KEYFACTOR

2023 | Keyfactor

Keyfactor Command 10.5

Reference Guide

Table of Contents

List of Tables

List of Figures

1.0 Introduction

The *Keyfactor Command Documentation Suite* includes:

- *Keyfactor Command Reference Guide*
- *Keyfactor Web APIs Reference Guide*
- *Keyfactor Command Server Installation Guide*
- *Keyfactor Orchestrators Installation and Configuration Guide*
- *Keyfactor Command Release Notes & Upgrading*

In addition, Keyfactor offers documentation for products that are not part of the *Keyfactor Command Documentation Suite*, including the *Keyfactor Command Upgrade Overview* and installation guides for third-party CA gateways that interface with Keyfactor, which are available upon request.

2.0 Reference Guide

The *Reference Guide* for the Keyfactor Command solution by Keyfactor provides comprehensive instructions on using the Keyfactor Command Management Portal and Policy Module. The Management Portal is the command and control center for Keyfactor Command. From here, you can get a quick glance at the health of your PKI and a sense of how it is being used by visiting the dashboard, or delve into details of certificates using the certificate search feature. The Management Portal is also used to configure workflow and email notifications, enroll for certificates, and configure options that are used across the whole of the Keyfactor Command product.

This reference guide covers advanced configuration of Keyfactor Command in addition to providing usage information.

This guide is organized in the order of the Management Portal menu panel:

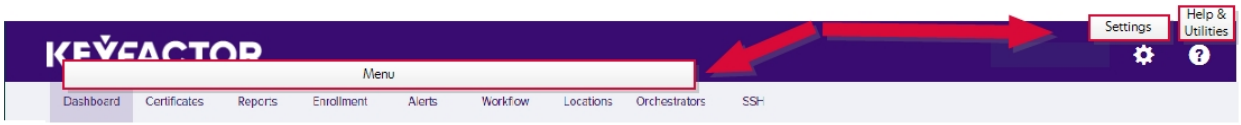


Figure 1: Management Portal Menu

2.1 Using the Management Portal

The Keyfactor Command Management Portal is a web-based application that you can open in any supported browser. The default URL for the Management Portal is (where KEYFACTOR_SERVER_FQDN is the FQDN of your Keyfactor Command administration server):

https://KEYFACTOR_SERVER_FQDN/keyfactorportal

In addition to the main URL, the pages in the Management Portal are available via deep link. To find the deep link for a page, just visit the page in your browser and copy the URL from the browser's URL line. For example, the deep link URL directly to the certificate search page in the Management Portal is available at:

https://KEYFACTOR_SERVER_FQDN/keyfactorportal/CertificateCollection/Edit?cid=0

You can change the number at the end of this deep link to direct the deep link to a specific saved collection instead of the main search. You can find the collection number by browsing to the collection and viewing the URL in your browser. You can also build links to specific searches, rather than saved collections. For more information, see Certificate Search and Collections on page 19.

The following is some information to help you understand and use the Management Portal successfully.

Navigating Keyfactor Command Grids

The grid includes the following features:

- **Action buttons** are used to perform actions on the data in the rows displayed in the grid. Some buttons are grayed out until you click on a grid row, or if that action is unavailable for the selected row. Which action buttons are displayed will depend on the function of the page.

  Note: On some grids the actions are also available from the context menu, which is accessible by right-clicking on the selected row.

- The **Total** in the upper right of the grid will be updated each time you refresh the grid.
- The **Refresh** button will poll the Keyfactor Command database and update the grid with the results of the current page query and update the Total.
- To change a **column width**, click, hold and drag the line separating two column headers (to the right of the column you want to change).
- To **rearrange columns**, click on the header of the column you want to move and hold and drag the column to your selected location.
- To change the **sort order** of the grid, click on the header of the column you wish to sort by. The first time you click, the grid will be sorted in ascending order by the selected column. Click the column header again to reverse the sort order. When a column is sorted, a purple caret will appear at the end of the column name showing the direction of the sort. Lack of a caret indicates the grid is sorted by the default column and order. On some grids only select columns are sortable.
- Click anywhere on the **row**, or on the tick box in the far left column of a grid row, to select that row. You may select multiple rows by utilizing the standard Windows selection functions of CRTL/Select and SHIFT/Select to select multiple rows at once. Selected rows will be highlighted purple. You may then perform actions on the selected row(s) depending on the functionality of the grid by right-clicking and selecting an action (if available) or selecting an action from the action buttons at the top of the grid. Tick boxes are found only on grids that support actions on multiple rows at once.
- Information in a grid field can be **copied** to the clipboard by highlighting text in a grid field and clicking **Ctrl+C**.
- Hovering over a row will change the row green to show which row the cursor is focused on.
- To open up the details pop-up for a row, or a search page, depending on the functionality of the screen, double click on a row, or select the row and then select an action button from the grid header or the context menu item, if available, by right-clicking.
- Grids use scroll bars to display grids with large quantities of data.
- Grid pages will re-size with the window size.

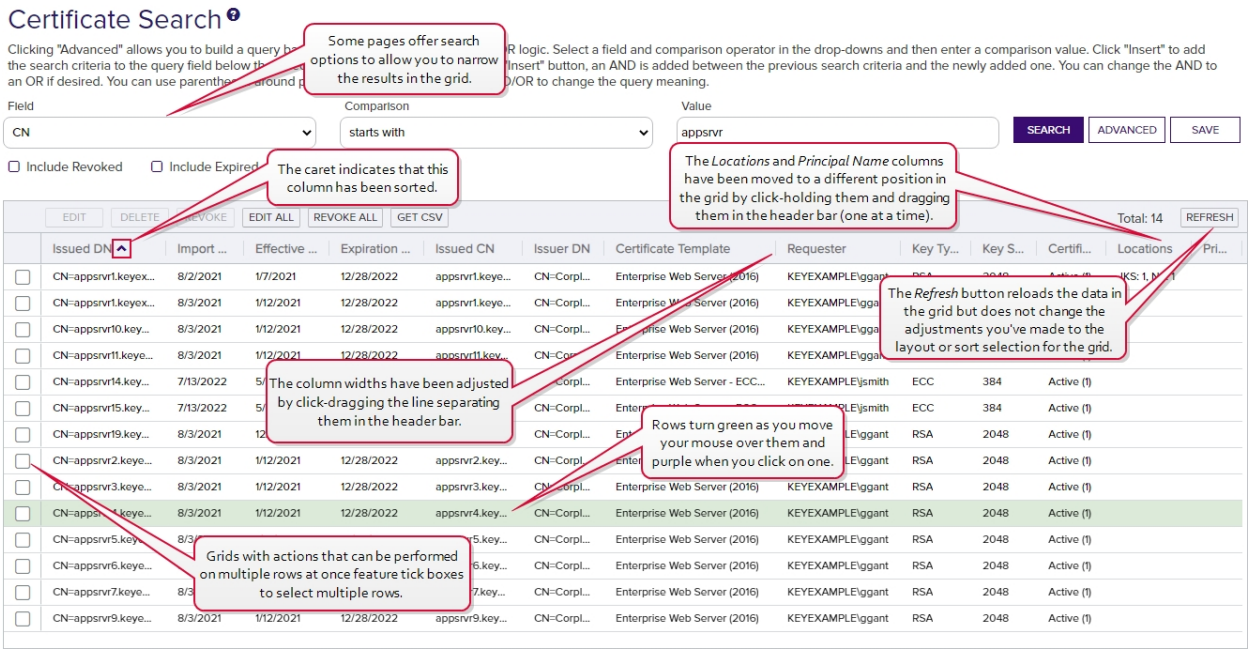


Figure 2: Using the Management Portal Grids

Validating Data Types

In data entry dialogs, fields in which the user is expected to enter certain data types will validate the user input against the expected data type and produce an error if the data entered is not valid. Fields that typically have validation include:

- email addresses (string fields)
- integers
- strings (alpha-numeric)

Further to this, regular expressions are supported on select entry fields for enrollment (see Certificate Template Operations on page 353).

Pop-up Dialogs

- When the cursor is focused on a field, the outline of the field will turn purple.
- Active/ available buttons will be bright purple. Inactive/ unavailable buttons will be faded to light purple. When data entered into the panes changes the conditions, the buttons may change between bright and light purple (active/inactive).
- At the bottom of most pop-up dialogs are the Save and Cancel buttons, and possibly other actions that can be performed on the data, depending on the purpose of the pane.
- The *X* in the top right corner is the close option which works like the cancel button.

- Many pop-up panes will have multiple tabs. The tab in which the cursor is focused will be underlined in green. When you point the cursor at another tab, it will temporarily change the underlining to green until you click into the tab.

Under Construction Icon

The under construction icon will display when an action of a transaction is *in process*.

Figure 3: Under Construction Icon

Confirmation Message

Messages appear at the bottom of the screen during processing at times. For example, an operation successful message will appear at the bottom of the screen when a selected action on a transaction is successful.

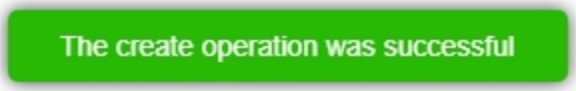


Figure 4: Confirmation Message

Tip: As of Keyfactor Command version 7.0, Internet Explorer is no longer supported for the Keyfactor Command Management Portal. Supported browsers are:

- Chrome version 65.0.3325 or higher
- Firefox version 59.0 or higher
- Microsoft Edge version 42.17134 or higher

2.1.1 Authentication and Authorization

Out of the box, Keyfactor Command is configured to support Windows integrated authentication so that users on domain-joined computers using domain accounts and browsers configured to support integrated authentication do not need to provide a username or password to authenticate to the Management Portal or Keyfactor API endpoints. Keyfactor Command can be configured to support only basic authentication, which requires entry of a username and password to authenticate to the Management Portal or Keyfactor API endpoints. This can be useful in environments where integrated authentication is not practical or desired, such as when users access the Management Portal using different accounts than they use to log on to their computers.

Keyfactor Command uses a system of security roles and security identities to provide access control to the Management Portal as a whole and to the features within it and the Keyfactor API. In order to access the Management Portal or Keyfactor API, your Active Directory account must be a member of one of the Active Directory groups granted access to the Management Portal during the Keyfactor

Command installation and configuration process (see the *Administration section* of the *Keyfactor Command Server Installation Guide*) or your Active Directory account must have been granted access either directly or via group membership later through the Management Portal (see Security Overview on page 605) or with the Keyfactor API (see *Security Roles & Identities* in the *Keyfactor Web APIs Reference Guide*).

2.1.2 Dashboard

The dashboard, at the top level of the Management Portal, provides you with a quick glance at the status of your PKI. It is a global representation of your PKI and does not filter data based on your access.

Risk Header

The top of the page shows a risk header, which is made up of a collection of sticky notes displaying active certificates, expiring and expired certificates, revoked certificates, and certificates with weak keys. The dashboard risk header displays by default and cannot be moved or removed (though it may be hidden with a security setting).

Figure 5: Dashboard Risk Header

The risk header panels are:

- Active Certificates

  This value reflects all active certificates in the database, including those with a certificate state of *unknown*, and excludes expired and revoked certificates.

- Certificates Expiring in Less Than 48 Hours

  This value includes all active certificates in the database with an expiration date between the current date/time and 48 hours from the current date/time.

- Certificates Expiring in Less Than 14 Days

  This value includes all active certificates in the database with an expiration date between the current date/time and 14 days (to the minute) from the current date/time. This value includes certificates shown in the *Expiring in < 48 Hours* panel.

- Certificates Expired in the Last 7 Days

  This value includes all certificates that have expired within the previous 7 days. This is the only panel that includes expired certificates.

- Certificates Revoked in the Last 7 Days

This value includes all certificates that have been revoked within the previous 7 days. This is the only panel that includes revoked certificates.

- Certificates with Weak Keys

  This value includes all certificates in the database that are deemed to have weak keys. Weak key certificates are those with signature algorithms SHA-1, MD5, RSA key size less than 2048, and ECC key size less than 224.

Tip: Access control to the risk header is controlled separately from the dashboard page as a whole, so a user could be granted access to the dashboard but not to the risk header and in this way see a dashboard that did not display the risk header. For more information, see Security Role Permissions on page 611.

Customizable Panels

A variety of panels are available to add to the dashboard, including:

- A separate panel for each of your certificate authorities (CAs) configured for synchronization can be displayed with graphs showing the activity over the last X weeks (24 by default) and a pie chart showing all active certificates by template. The number of weeks to display is configurable on a panel-by-panel basis. See Dashboard: CA Status on page 11.

  Note: Any CAs that have not been configured for synchronization will not appear as available for addition on the dashboard, or for reports which require selecting a CA.

- Certificate collections (see Certificate Collection Manager on page 80) can be configured to be included in a bar chart on the Certificate Collection dashboard panel. See Dashboard: Collections on page 12.
- The Certificates by Signing Algorithm panel displays a bar chart showing all active certificates broken down by signing algorithm. The CAs to include in the display are configurable. Both CAs that are currently configured for synchronization and any that were previously synchronized are available for inclusion. Certificates imported into Keyfactor Command via SSL scanning, certificate store inventorying, and manual import are also included and can be filtered out by unchecking the *Certificates Not Associated with CA* option. See Dashboard: Certificates by Signing Algorithm on page 13.
- The Recent Certificate Store Jobs panel displays the status of up to ten jobs. Both completed and in progress jobs are included. See Dashboard: Recent Certificate StoreJobs on page 15.
- If you configure certificate revocation list (CRL) or online certificate status protocol (OCSP) locations for monitoring and opt to display them on the dashboard (see Revocation Monitoring on page 199), these will appear with a status on the dashboard Revocation Monitoring panel. See Dashboard: Revocation Monitoring on page 16.
- The comprehensive SSL Endpoints panel includes a grid of changes found in existing SSL endpoints, a grid of endpoints with certificates expiring in the next X days, a pie chart showing SSL endpoints per defined SSL network, and a pie chart showing the results from the

last SSL scan broken out by result (e.g. certificate found, connection timed out, connection refused). The number of days for the expiring certificates grid is configurable. See Dashboard: SSL Endpoints on page 17.

- The status of SSL discovery and monitoring jobs can be displayed on an orchestrator-by-orchestrator basis on the SSL Orchestrator Job Status panel. The orchestrators to include are configurable. See Dashboard: SSL Orchestrator Job Status on page 18.
- The Number of SSH Keys per Type panel includes SSH keys found on discovery and those issued through the Management Portal and displays as a bar chart broken down by key type. See Dashboard: Number of SSH Keys per Type on page 14.

The panels on the dashboard are displayed in two columns. You can click and drag the dividing line between the two columns to change the width of the columns—for example, a wide left column and a narrower right column. The panels can be rearranged by dragging them up and down a column or from one column to the other. If you've chosen to change the column widths, you can arrange the wider panels in your wider column and the narrower panels in your narrower column.

The selected panels and their arrangement is unique to each user of the Management Portal. Out of the box, in addition to the risk header, the dashboard includes the Collections and Revocation Monitoring panels, so each new user to the dashboard will see these panels.

The latest version of the Logi reporting engine has functionality which avoids a system timeout issue by periodically pinging the IIS session behind the scenes so that the dashboard doesn't time out when the session has been idle. As a result, the dashboard no longer refreshes after 20 minutes, but invokes this new functionality instead. The settings used to control this depend on the **Session State Timeout** and **Session Auto Keep Alive** attribute settings in IIS. For more information on this see:

https://devnet.logianalytics.com/hc/en-us/articles/1500009515942-Manage-Session-Timeout

Add a Panel to the Dashboard Display

To add a panel for display on your dashboard:

1. Click the Add Panel button on the left just below the dashboard risk header.

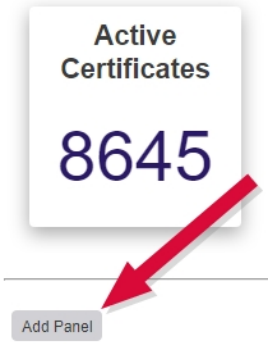


Figure 6: Click the Dashboard Add Panel Button

2. On the Add Panels dialog, select the panels you wish to display on the dashboard, click **Add** and then click **Done** at the bottom of the dialog.

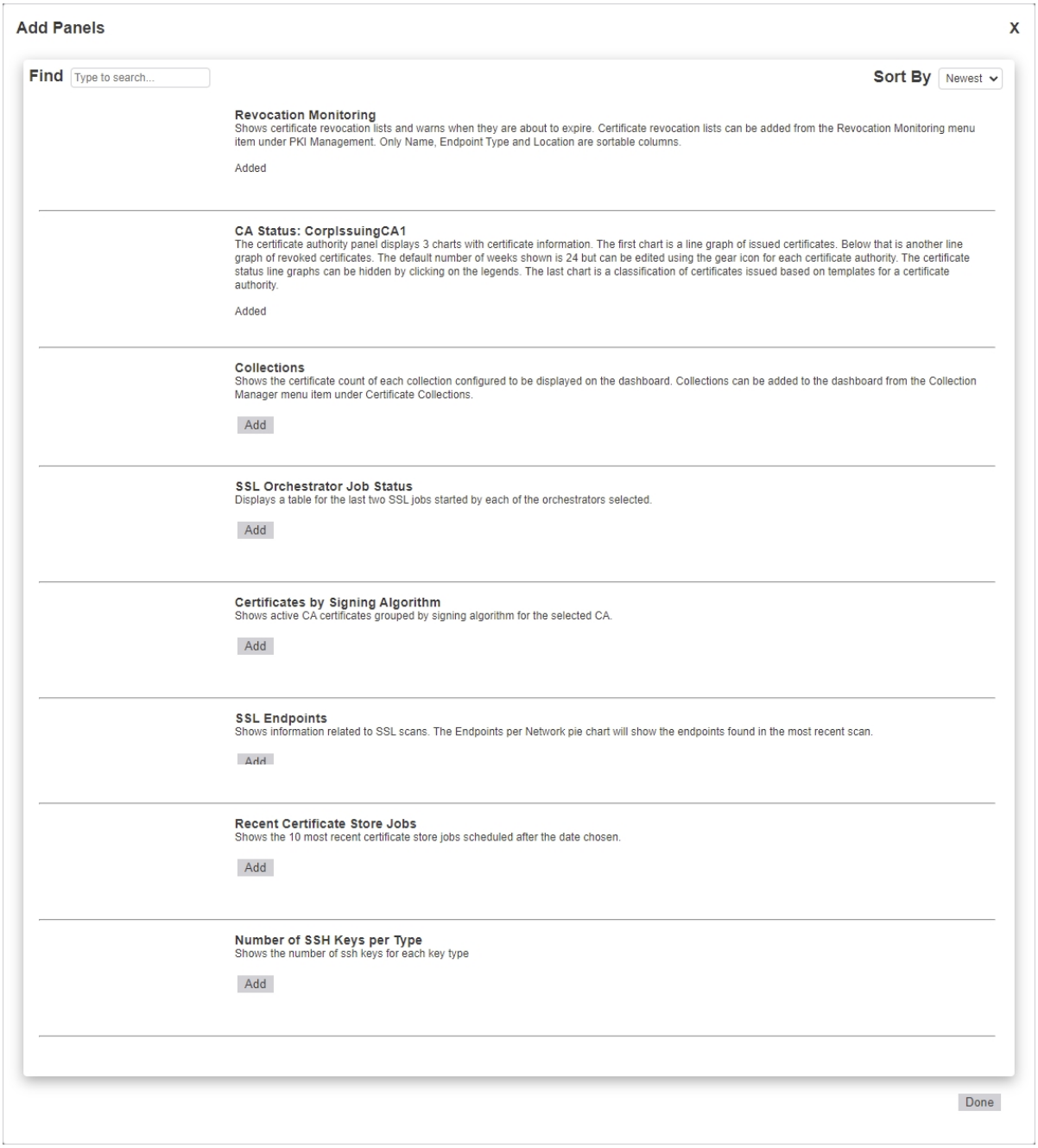


Figure 7: Add Panels to the Dashboard

Rename a Dashboard Panel

The panels displayed on the dashboard may be given user-defined names. To rename a displayed panel:

1. Click the panel **Settings** icon on the right of the panel you wish to rename and then click **Rename**.

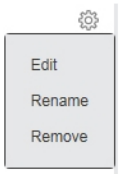


Figure 8: Dashboard Panel Settings

2. In the title field of the panel, type a new name. Click away from the field to save.

Figure 9: Type in a New Name for the Panel

Note: Only letters, numbers, spaces, and select punctuation marks are supported in the panel name field. Special characters, such as < and > (and therefore HTML markup), are not supported.

Remove a Dashboard Panel

To remove a panel from display on your dashboard:

1. Click the panel **Settings** icon on the right of the panel you wish to remove and then click **Remove**.

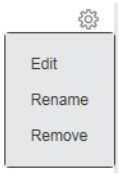


Figure 10: Dashboard Panel Settings

2. When prompted, confirm that you are sure that you want to remove the panel.

Tip: The **Edit** option only appears on the panel settings menu for selected panels.

2.1.2.1 Dashboard: CA Status

Each CA section of the dashboard includes two line graphs showing issued (top graph) and revoked and failed/denied certificate requests (bottom graph) over the last X weeks or days (24 weeks by default) on the left and a pie chart showing all active certificates by template on the right. To change the number of weeks displayed on the line graphs for **all** CAs, change the *Weeks of CA Stats* application setting (see Application Settings: Console Tab on page 584). To change the number of weeks or days displayed on the line graph on a CA-by-CA basis, click the panel **Settings** icon for the selected CA and choose **Edit**. A maximum of 52 weeks or 30 days may be configured when setting the time frame on a CA-by-CA basis.

The panel is interactive in a number of ways:

- Hover over a point on a line graph to see details for that point.
- Click on a point on a line graph to be taken to a new window with the certificate search page populated by the query of the selected CA and date.
- Click on a legend (e.g. Revoked) below a line graph to toggle add/remove that line from the chart.
- Click one of the labels below the pie chart to toggle add/remove that segment of the pie from the chart. This can be helpful, for example, if you remove a template that makes up the bulk of the chart, allowing you to just focus on the remaining templates (and making these pie segments bigger and easier to click on).
- Hover over a number for, or section of, the pie chart to see the template name associated with that section of the pie chart. This is the number of active certificates for that template.
- Click on a number for, or section of, the pie chart to be taken to a new window with the certificate search page populated by the query of the selected CA and template.

A status indicator appears at the top of the CA section showing when the CA was last contacted.

Click the **Hide** button to minimize the display. Click the panel **Settings** icon to remove or rename the panel or change the comparison date for the display (see Dashboard on page 6). Data for the CA sections of the dashboard is generated from certificates retrieved during CA synchronization tasks (see Certificate Authorities on page 325).

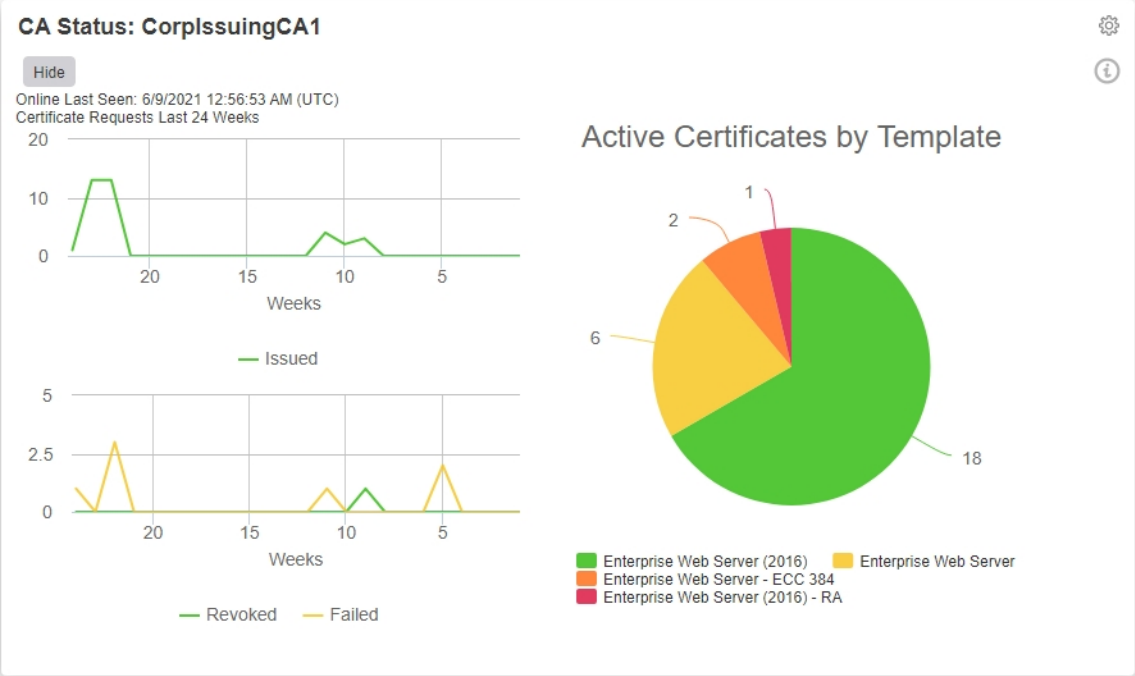


Figure 11: Dashboard CA Snapshot

2.1.2.2 Dashboard: Collections

If you opt to include any certificate collections for display on the dashboard (see Certificate Collection Manager on page 80), you will see the data on the Collections dashboard panel. This panel shows a bar representing the total number of active, expired and revoked certificates for each certificate collection configured for dashboard display. Hover over a bar to see the number of certificates in the collection. Click on a bar to open the certificate search page in a new window filtered for that certificate collection.

Note: The collections dashboard widget will only display the first 25 collections alphabetically.

Tip: If you **Save** a new certificate collection, or **Save** a change to an existing certificate collection, that change will be immediately reflected in the collection data used to display certificate collections on dashboards and reports. The data used by the dashboards and reports is stored in an intermediate table that is updated immediately. It will also continue to be updated periodically (approximately every 20 minutes by default as configured by the *Dashboard Collection Caching Interval* application setting) by the Keyfactor Command Service (see Application Settings: Console Tab on page 584).

Click the **Hide** button to minimize the display. Click the panel **Settings** icon to remove or rename the panel or change the comparison date for the display (see Dashboard on page 6).

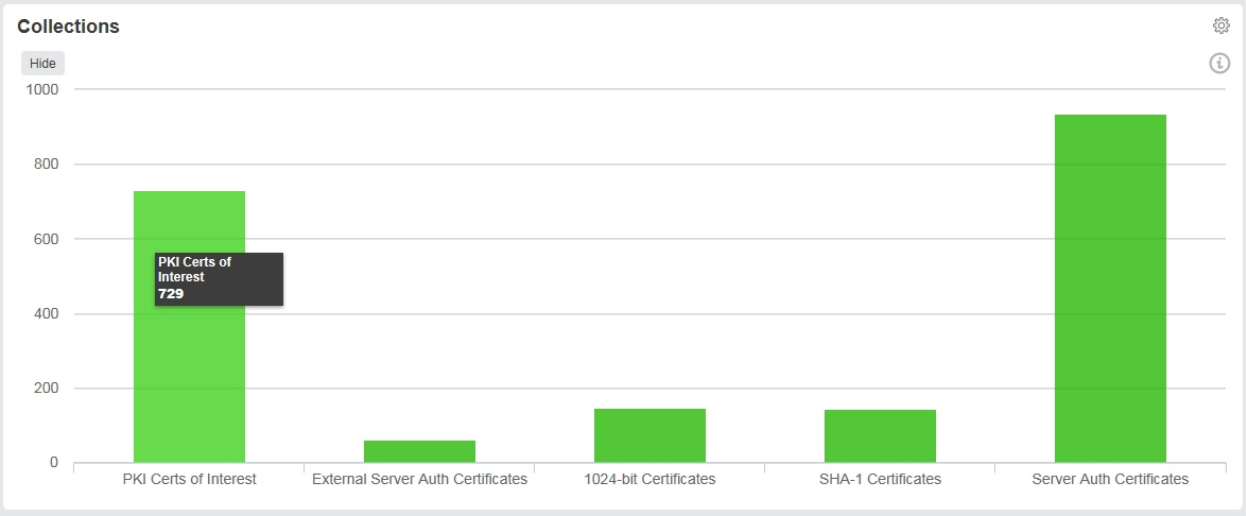


Figure 12: Dashboard Certificate Collections

2.1.2.3 Dashboard: Certificates by Signing Algorithm

The Certificates by Signing Algorithm panel on the dashboard shows a bar chart of all active certificates synchronized to Keyfactor Command from a Microsoft CA or Keyfactor CA gateway or imported via SSL scanning, certificate store inventorying, or manual import broken down by signing algorithm. Hover over a bar to see the number of active certificates in the category. By default, all certificates in the Keyfactor Command database are included. To include only selected CAs or gateways, click the panel **Settings** icon and choose **Edit**. In the Edit dialog, select the CAs you wish to include in the panel. To filter out certificates brought into the database via SSL scanning, certificate store inventorying, and manual import, select specific CAs and uncheck the *Certificates Not Associated with CA* option.

Click the **Hide** button to minimize the display. Click the panel **Settings** icon to remove or rename the panel or change the comparison date for the display (see Dashboard on page 6).

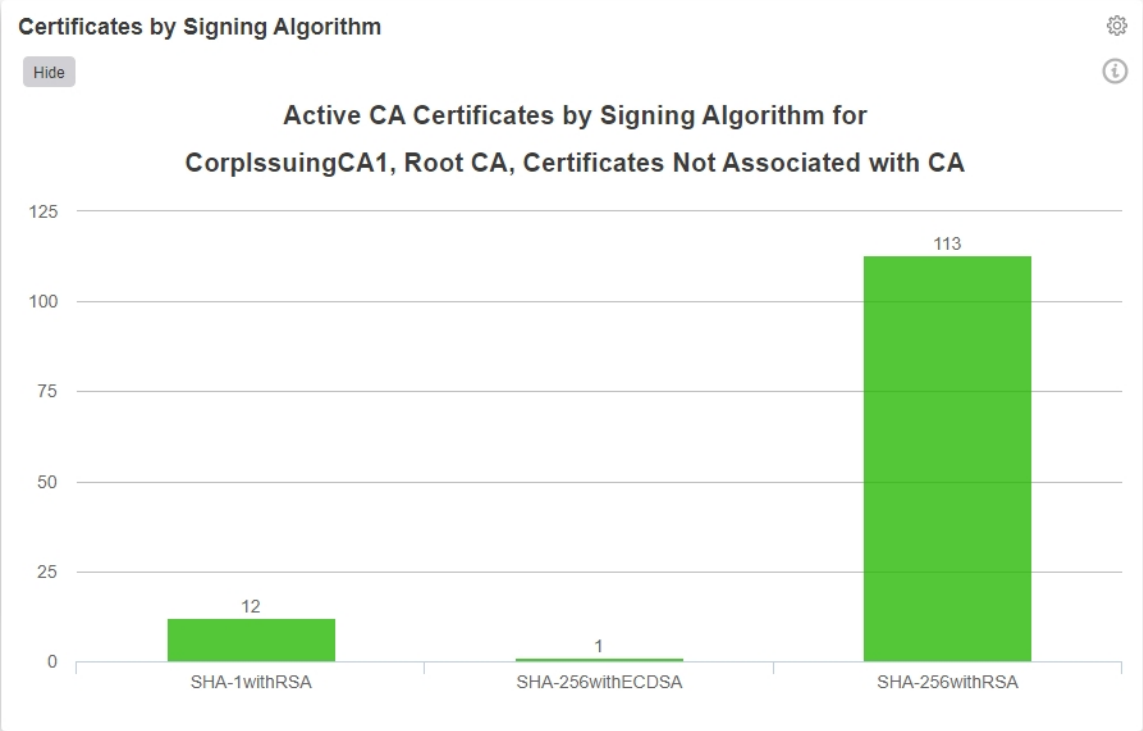


Figure 13: Dashboard Certificates by Signing Algorithm

2.1.2.4 Dashboard: Number of SSH Keys per Type

The Number of SSH Keys per Type panel on the dashboard shows a bar chart of all SSH keys in the Keyfactor Command database. The chart includes both managed keys (those generated within Keyfactor Command using My SSH Key (see My SSH Key on page 512) or the service account key page (see Service Account Keys on page 524) and unmanaged keys (see Unmanaged SSH Keys on page 538). Hover over a bar to see the number of SSH keys in the category.

Click the **Hide** button to minimize the display. Click the panel **Settings** icon to remove or rename the panel or change the comparison date for the display (see Dashboard on page 6).

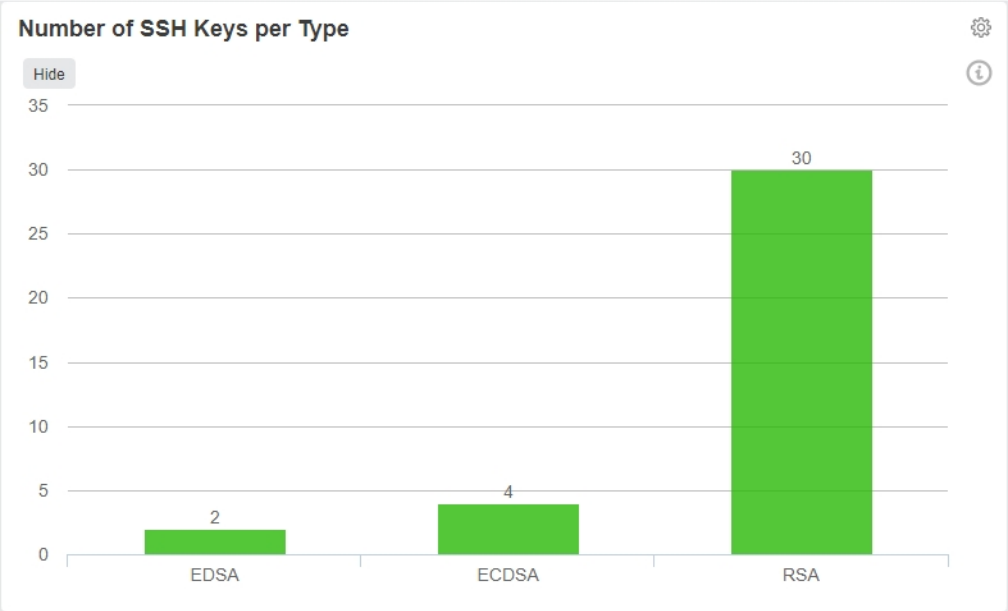


Figure 14: Dashboard SSH Keys per Type

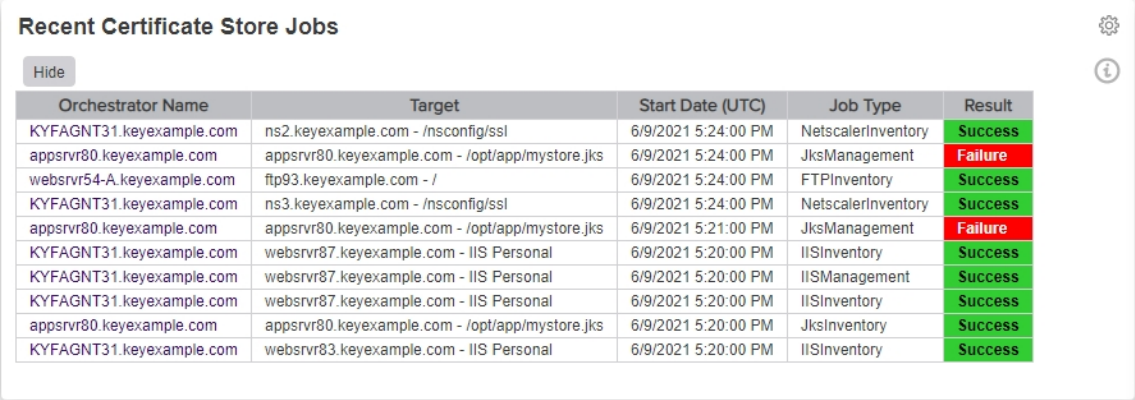
2.1.2.5 Dashboard: Recent Certificate StoreJobs

The Recent Certificate Store Jobs panel on the dashboard includes a grid showing the most recent job history for certificate stores. Both completed (successful or not) and in progress jobs are included. The grid includes the orchestrator name, the target for the job (which in most cases includes the host name and the certificate store name), the job start date, the job type (e.g. inventory or management for an IIS or FTP store), and color-coded results (errors appear in red) for the job.

Click on the name of the orchestrator in the grid to be taken to the orchestrator job history page with the query populated by the selected orchestrator.

To include only jobs that started on or after a selected date, click the panel **Settings** icon and choose **Edit**. In the Edit dialog, either enter a comparison date or use the calendar picker to select a date. Only jobs with a starting date on or after this date will be shown. A maximum of ten jobs are shown.

Click the **Hide** button to minimize the display. Click the panel **Settings** icon to remove or rename the panel or change the comparison date for the display (see Dashboard on page 6).



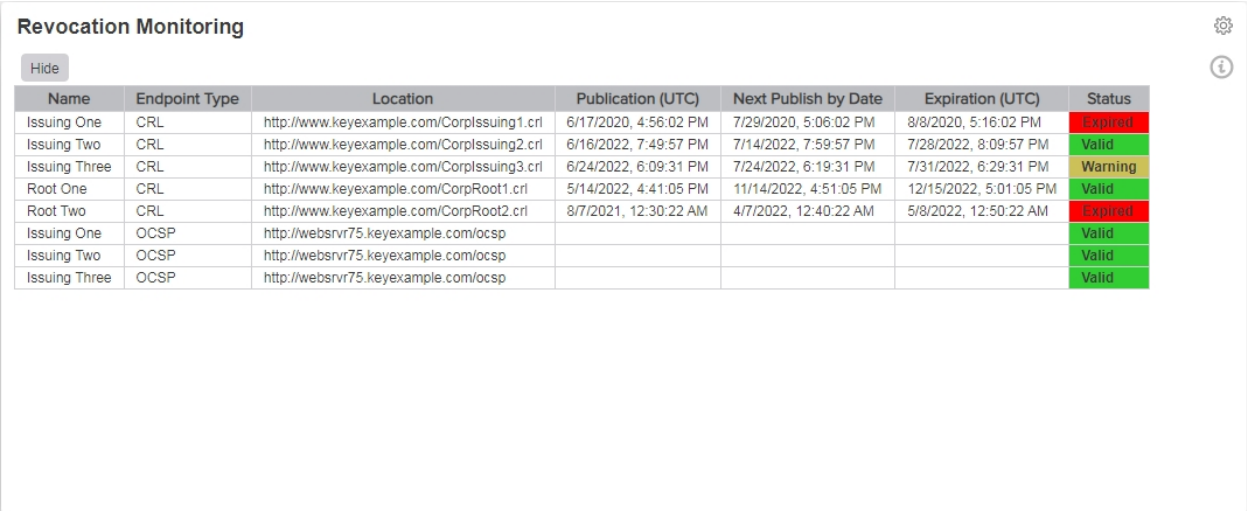
Orchestrator Name	Target	Start Date (UTC)	Job Type	Result
KYFAGNT31.keyexample.com	ns2.keyexample.com - /nsconfig/ssl	6/9/2021 5:24:00 PM	NetscalerInventory	Success
appsrvr80.keyexample.com	appsrvr80.keyexample.com - /opt/app/mystore.jks	6/9/2021 5:24:00 PM	JksManagement	Failure
websrvr54-A.keyexample.com	ftp93.keyexample.com - /	6/9/2021 5:24:00 PM	FTPInventory	Success
KYFAGNT31.keyexample.com	ns3.keyexample.com - /nsconfig/ssl	6/9/2021 5:24:00 PM	NetscalerInventory	Success
appsrvr80.keyexample.com	appsrvr80.keyexample.com - /opt/app/mystore.jks	6/9/2021 5:21:00 PM	JksManagement	Failure
KYFAGNT31.keyexample.com	websrvr87.keyexample.com - IIS Personal	6/9/2021 5:20:00 PM	IISInventory	Success
KYFAGNT31.keyexample.com	websrvr87.keyexample.com - IIS Personal	6/9/2021 5:20:00 PM	IISManagement	Success
KYFAGNT31.keyexample.com	websrvr87.keyexample.com - IIS Personal	6/9/2021 5:20:00 PM	IISInventory	Success
appsrvr80.keyexample.com	appsrvr80.keyexample.com - /opt/app/mystore.jks	6/9/2021 5:20:00 PM	JksInventory	Success
KYFAGNT31.keyexample.com	websrvr83.keyexample.com - IIS Personal	6/9/2021 5:20:00 PM	IISInventory	Success

Figure 15: Dashboard Recent Certificate Store Jobs

2.1.2.6 Dashboard: Revocation Monitoring

The Revocation Monitoring panel on the dashboard shows each configured CRL and OCSP location (if they have been configured to appear on the dashboard) with the path to the CRL or OCSP, the publication, next publish date, and expiration dates of the CRLs (these aren't relevant for OCSPs) and the status of the CRL or OCSP. The status for a CRL will show *Warning* if the expiration date of the CRL is within the warning period as defined by the number of weeks, days, or hours configured in the *Show on Dashboard* setting (see Revocation Monitoring Location Operations on page 200). For example, if you had a CRL that expired on June 30 and configured the warning period to 15 days before expiration, the Warning status would begin to appear on the dashboard for that CRL on June 15.

Some columns allow for sorting in ascending or descending order by clicking the column heading to toggle sort order. Click the **Hide** button to minimize the display. Click the panel **Settings** icon to remove or rename the panel or change the comparison date for the display (see Dashboard on page 6).



Name	Endpoint Type	Location	Publication (UTC)	Next Publish by Date	Expiration (UTC)	Status
Issuing One	CRL	http://www.keyexample.com/CorpIssuing1.crl	6/17/2020, 4:56:02 PM	7/29/2020, 5:06:02 PM	8/8/2020, 5:16:02 PM	Expired
Issuing Two	CRL	http://www.keyexample.com/CorpIssuing2.crl	6/16/2022, 7:49:57 PM	7/14/2022, 7:59:57 PM	7/28/2022, 8:09:57 PM	Valid
Issuing Three	CRL	http://www.keyexample.com/CorpIssuing3.crl	6/24/2022, 6:09:31 PM	7/24/2022, 6:19:31 PM	7/31/2022, 6:29:31 PM	Warning
Root One	CRL	http://www.keyexample.com/CorpRoot1.crl	5/14/2022, 4:41:05 PM	11/14/2022, 4:51:05 PM	12/15/2022, 5:01:05 PM	Valid
Root Two	CRL	http://www.keyexample.com/CorpRoot2.crl	8/7/2021, 12:30:22 AM	4/7/2022, 12:40:22 AM	5/8/2022, 12:50:22 AM	Expired
Issuing One	OCSP	http://websrvr75.keyexample.com/ocsp				Valid
Issuing Two	OCSP	http://websrvr75.keyexample.com/ocsp				Valid
Issuing Three	OCSP	http://websrvr75.keyexample.com/ocsp				Valid

Figure 16: Dashboard Revocation Monitoring Status

2.1.2.7 Dashboard: SSL Endpoints

The comprehensive SSL Endpoints panel includes several components:

- The Changes Found to Existing Endpoints grid displays up to ten SSL endpoints for which a change was found in the most recent scan from the previous scan status. The grid includes the endpoint address, scan time, and both the previous and current endpoint status. This grid only displays if there are endpoints that have been changed.
- The Endpoints Expiring in the Next X Days grid displays up to ten SSL endpoints with certificates expiring in the next X days. This grid only displays if there are endpoints that meet that criteria. If there are more than ten to display, the certificates expiring soonest are displayed. Out of the box, the number of days is configured to 30. To change the number of days, click the panel **Settings** icon, choose **Edit**, enter a number of days, and click **Done**. To clear the custom number of days and return to the default, click the panel **Settings** icon, choose **Edit**, clear the days field, and click **Done**. The grid includes the network name, the endpoint address, the certificate expiration date, and the certificate common name, if any.
- The Endpoints per Network pie chart shows discovered SSL endpoints broken down by SSL network. All discovered endpoints are included. This includes endpoints at which a certificate is currently being found, endpoints at which a certificate was found in the past but is no longer found, and endpoints that responded in some way on scan but did not present a certificate. Click on a section of the pie chart to be taken to the SSL Discovery Results page. Click any of the labels below the pie chart to toggle add/remove that segment of the pie from the chart.
- The Network Endpoint SSL Scanning Results pie chart shows the results from the most recent SSL scan (discovery or monitoring) broken out by result (e.g. certificate found, connection timed out, connection refused). Click on a section of the pie chart to be taken to the SSL Discovery Results page. Click any of the labels below the pie chart to toggle add/remove that segment of the pie from the chart. This can be helpful, for example, if you remove the certificate found section, allowing you to just focus on any errors (and making the error pie segments bigger and easier to click on).

Click the **Hide** button to minimize the display. Click the panel **Settings** icon to remove or rename the panel or change the comparison date for the display (see Dashboard on page 6).

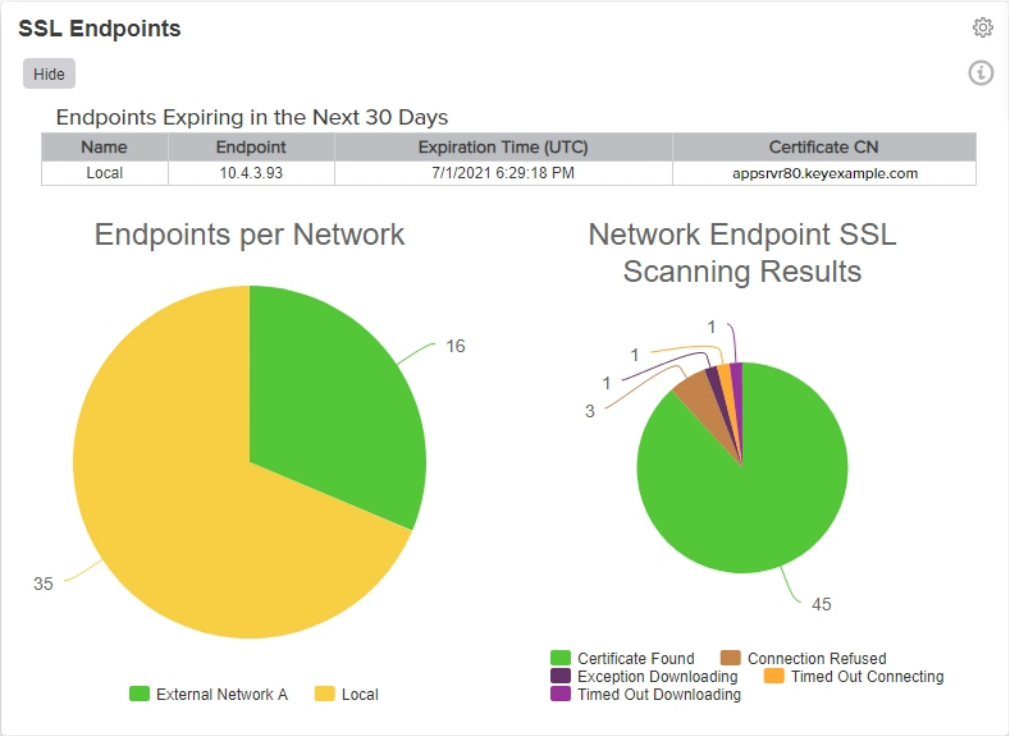


Figure 17: Dashboard SSL Endpoints

2.1.2.8 Dashboard: SSL Orchestrator Job Status

The SSL Orchestrator Job Status panel on the dashboard displays a grid showing the results of the two most recent SSL jobs for each active Keyfactor Universal Orchestrator and Windows Orchestrator with the SSL capability in the configured orchestrator pool (see Orchestrator Pools Definition on page 459). Both jobs in progress and completed jobs are included. The grid includes the names of the orchestrators in the selected pool(s), the job type, job start date and time, color-coded results (errors appear in red), and color-code status (jobs in progress are yellow). To change the orchestrator pools included in the display, click the panel **Settings** icon, choose **Edit**, select the desired orchestrator pools, and click **Done**.

Click on the name of an orchestrator in the grid to be taken to the orchestrator job history page with the query populated by the selected orchestrator.

Click the **Hide** button to minimize the display. Click the panel **Settings** icon to remove or rename the panel or change the comparison date for the display (see Dashboard on page 6).

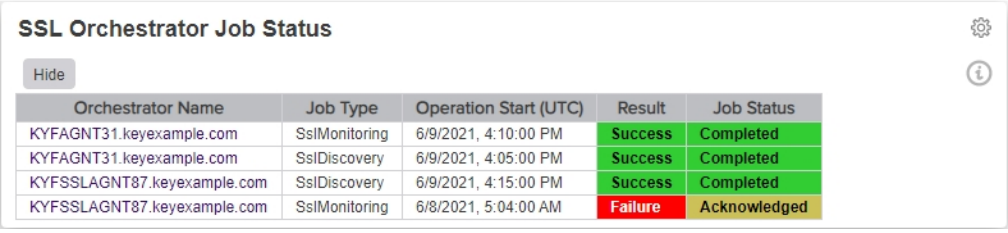


Figure 18: Dashboard SSL Orchestrator Job Status

2.1.3 Certificate Search and Collections

The Keyfactor Command database can include certificates from many locations—including certificates synchronized from your Microsoft CAs in both the primary forest and alternate forests, certificates synchronized from your EJBCA CAs, certificates synchronized from cloud-based certificate vendors via the Keyfactor certificate gateways, certificates automatically imported based on configured SSL endpoint locations (see SSL Discovery on page 443), certificates imported from certificate stores (see Certificate Stores on page 380), and manually imported certificates (see Add Certificate on page 69). The Certificate Search function allows you to query the database for certificates from any available source. You do not need to specify the source as part of the query.

A specific certificate search may be saved as a collection, which can then be revisited without needing to enter the search selections again. The saved collection can then be referenced from other parts of the Management Portal (e.g. expiration alerts, the dashboard, and select reports). Certificate collections may be added to the *Certificates* menu of the Management Portal for quick access. Several default certificate collections are created in new installations. For more information, see Certificate Collection Manager on page 80.

Note: The options shown and described in this section are available to full administrative users of the Management Portal. Users with limited access to the Management Portal will not see all the options (e.g. the recover buttons may not appear) and will see some slightly different buttons (e.g. the edit buttons shown may say *view* instead of *edit*).

2.1.3.1 Certificate Details

The cornerstones of the Keyfactor Command Management Portal are the Certificate Search and the Certificate Details pages. The Certificate Details page includes a comprehensive set of details about each certificate managed by Keyfactor Command. To access a certificate's details, double-click on a row of the certificate search grid, or highlight a row, right click and select **Edit** (**Display** for users with only Read permissions) from the action menu (see Certificate Search Page on page 32).

The following action buttons are conveniently located at the top of the Certificate Details page for users with the appropriate permissions: **Revoke**, **Download**, **Renew**. See Certificate Operations on page 42 for more information on these actions.

Content Tab

The Content tab shows the certificate attributes from the CA (Active Directory in the case of a Microsoft CA). These fields are not editable. The list of Subject Alternative Names (SANs) and SAN count are also included on this tab. For an ECC certificate, the elliptic curve algorithm is included on this tab.

Tip: Double-click any field on this dialog to open a pop-up showing just that detail.

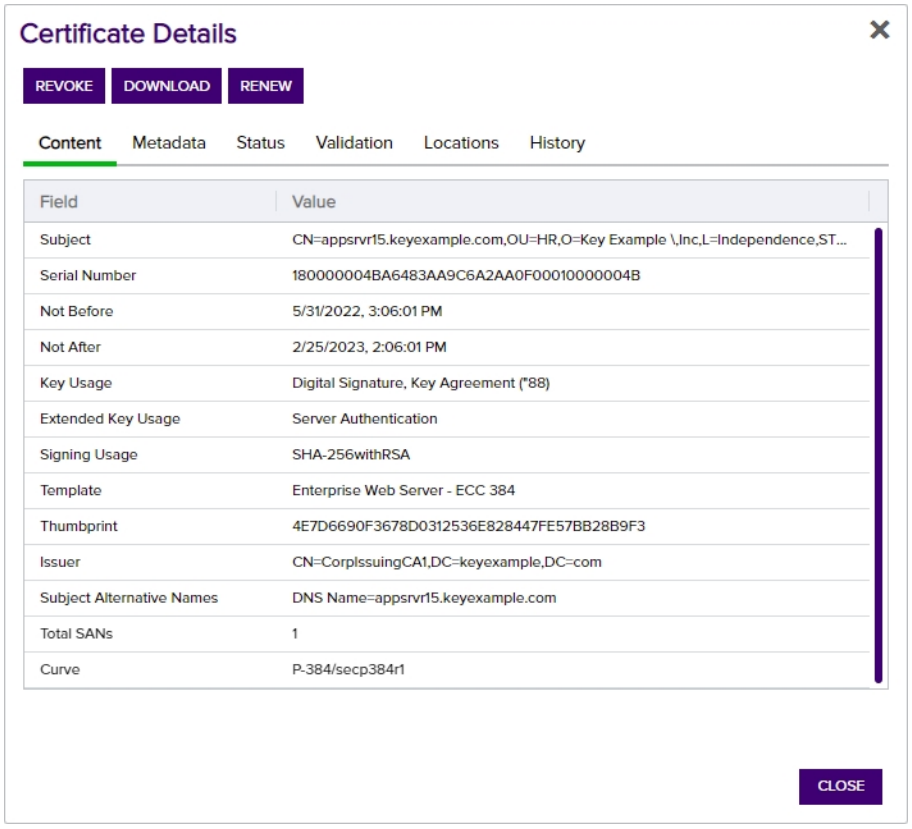


Figure 19: Certificate Details: Content Tab

Metadata Tab

The Metadata tab displays all metadata fields created for your Keyfactor Command implementation and shows any data in fields that have been populated with values specific to the certificate. Depending on the metadata type, these fields appear as text boxes, radio buttons, drop-downs, date fields, table or large text fields.

For users with edit permissions, on date fields a small popup calendar will appear that will allow you to select a date and will properly format it for you. You may edit values for any metadata fields to update the data at any time. You may also update multiple certificates' metadata with the same data by selecting multiple certificates from the certificates grid. Required fields will be marked with

*Required next to the field label. See Certificate Metadata on page 646 for information on this functionality.

Tip: The order of the metadata fields as they appear on this dialog is configurable using the certificate metadata display order option (see Sorting Metadata Fields on page 651).

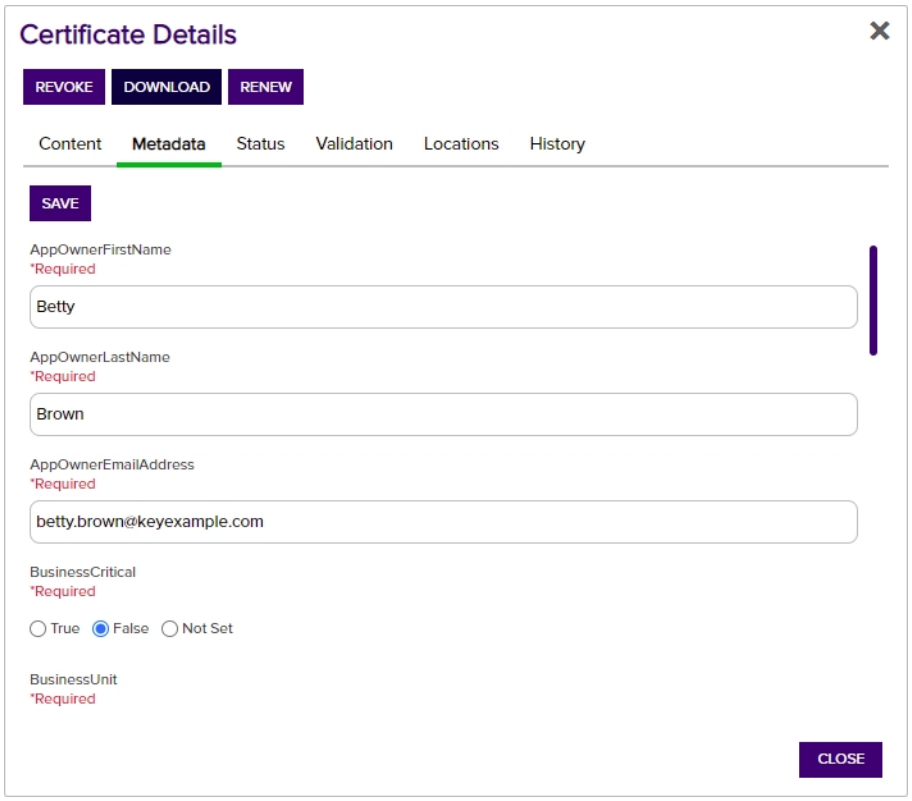


Figure 20: Certificate Details: Metadata Tab

Status Tab

The status tab displays some additional information about the certificate (see Table 1: Status Tab Descriptions).

The fields on this tab cannot be edited.

Tip: Double-click any field on this dialog to open a pop-up showing just that detail.

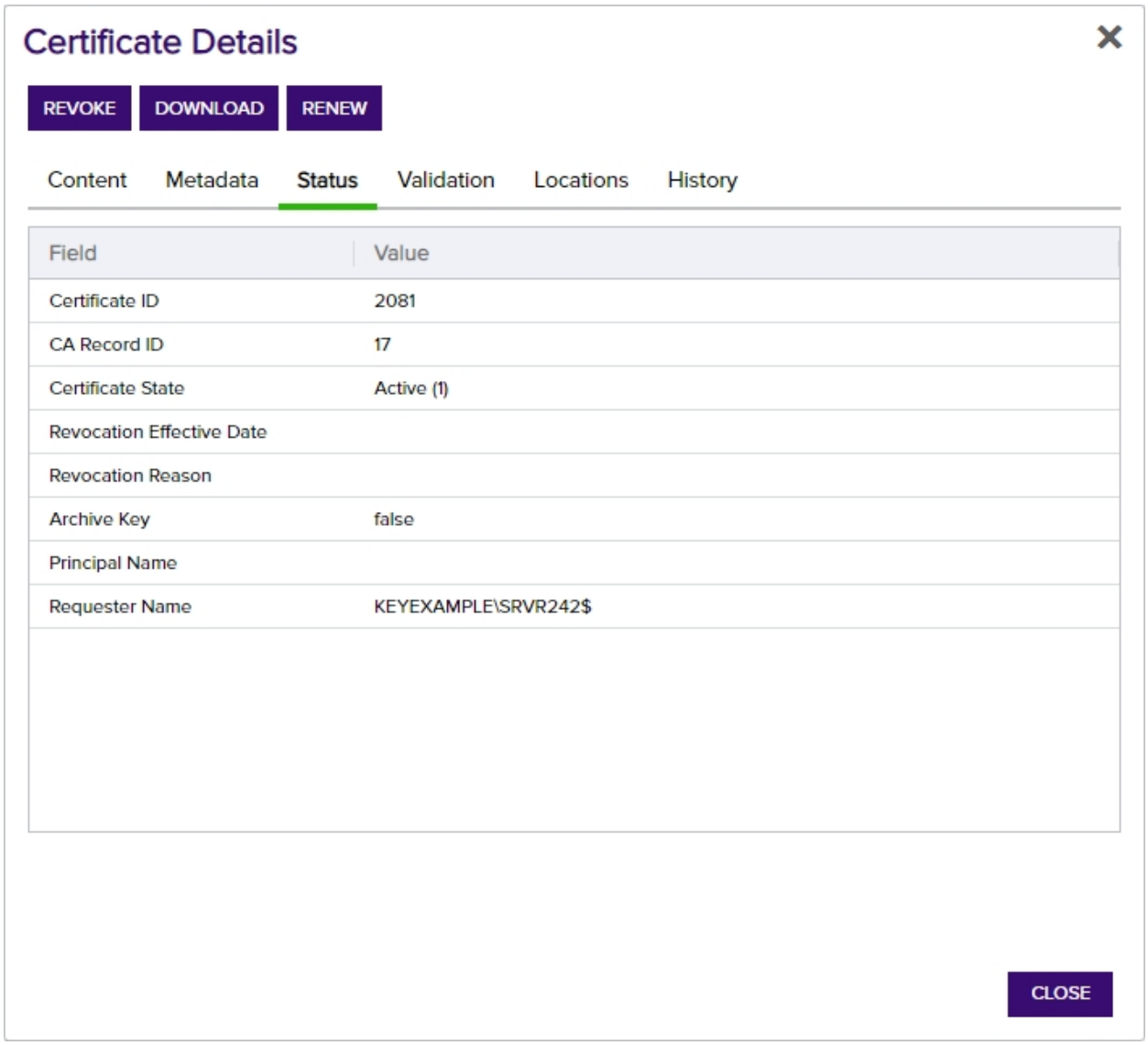


Figure 21: Certificate Details: Status Tab

Table 1: Status Tab Descriptions

Field	Description
Certificate ID	The Keyfactor Command reference ID for the certificate, which can be useful when referring to the certificate using API methods.
CA Record ID	The ID of the certificate in the CA (this has replaced CARequestID).
Certificate State	The state of the certificate. • Unknown (0)—This certificate entered the system in a manner other than a CA sync, so no status from a CA has been reported. • Active (1)—The "normal" state for certificates brought in via CA sync. The certificate has not been revoked. **Note:** Here we mimic the behavior of the Microsoft CA, which does not have a status for Expired, so certificates continue to be listed as Active or Revoked (as appropriate) after they expire. • Revoked (2)—The certificate has been revoked. • Failed (4)—The certificate has been denied approval. • Pending (5)—The certificate is awaiting approval. • Certificate Authority (6)—The certificate synced in from a CA sync that is indicated to be that CA's own certificate. • Parent Certificate Authority (7)—The certificate synced in from a CA sync that is indicated to be the certificate of a CA further up the chain. • Waiting for External Validation (8)—The certificate is pending, awaiting approval outside of Keyfactor Command. Generally, the certificate would have been added through one of the Keyfactor Command CA gateways using an EV certificate type.
Revocation Effective Date	If the certificate is revoked, the date it was revoked will be displayed here.
Revocation Reason	If the certificate is revoked, the reason will be displayed here. This is shown as a numeric value, which will be one of: • 0 — Unspecified • 1 — Key Compromised • 2 — CA Compromised • 3 — Affiliation Changed • 4 — Superseded • 5 — Cessation of Operation • 6 — Certificate Hold • 999 — Unknown

Field	Description
	See Revoke on page 66 for more information about revoking certificates.
Archive Key	If true, the certificate has a private key archived on the Microsoft CA to support CA key recovery. This flag is not an indicator for whether the certificate has a private key stored in Keyfactor Command. **Tip:** CA-level key recovery is supported for Microsoft CAs to allow recovery of private keys for certificates enrolled outside of Keyfactor Command. CA-level key archiving is not supported for enrollments done through Keyfactor Command. CA-level key recovery is not supported for EJBCA CAs. For enrollments done through Keyfactor Command for either Microsoft or EJBCA CAs, use Keyfactor Command private key retention (see Details Tab on page 360).
Principal Name	The user principal name (UPN) contained in the subject alternative name (SAN) field of the certificate, if present (e.g. username@keyexample.com).
Requester Name	The name of the requester in DOMAIN\User format.

Validation Tab

This tool will report on the certificate validity based on the criteria defining the status of an X509 chain shown in Table 2: Validation Tab Descriptions. This tab replaces the former **Validate** action from the certificate search grid. An alert symbol will show on the tab header if one or more tests have a result of *Fail*.

Tip: See Certificate Validation Errors on page 750 for assistance troubleshooting validation errors.

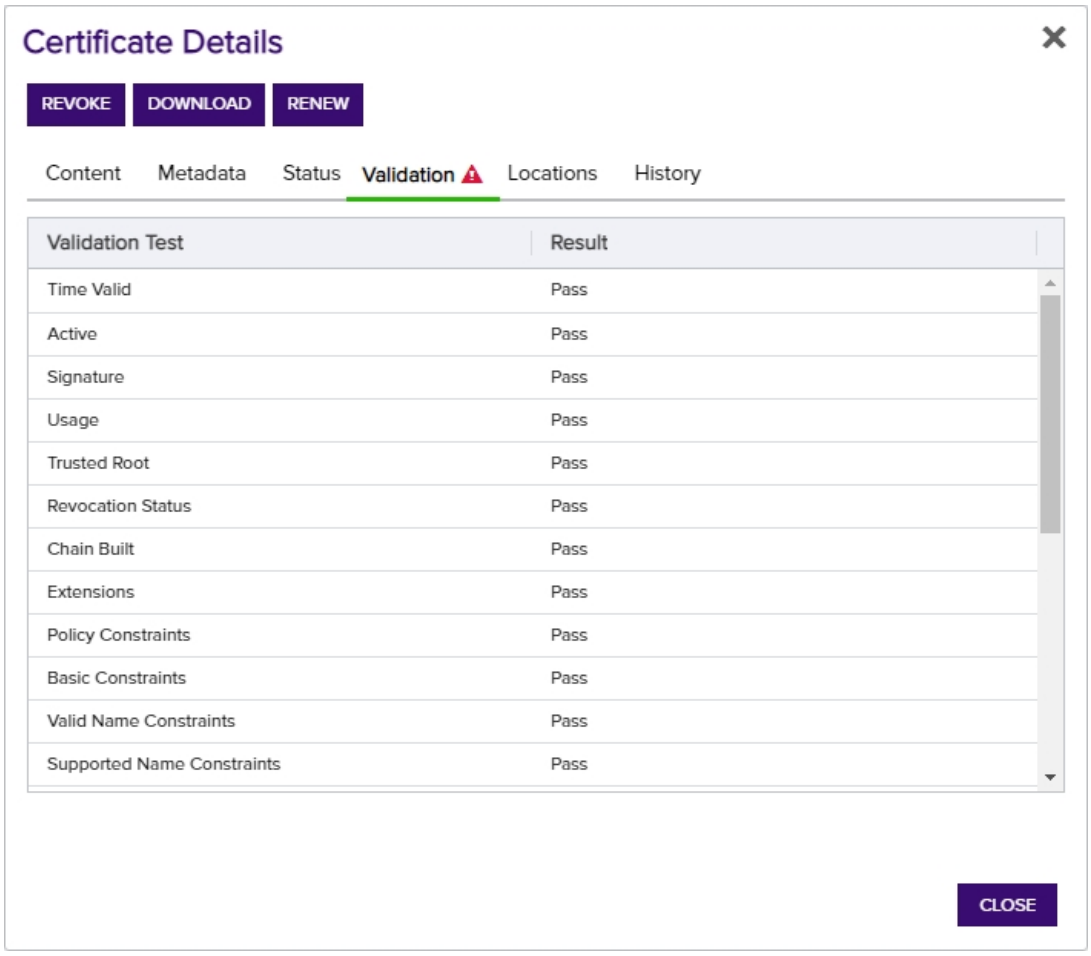


Figure 22: Certificate Details: Validation Tab

Table 2: Validation Tab Descriptions

Validation Test	Keyfactor API Equivalent[1]	Definition
Time Valid	NotTimeValid	A value of *Pass* indicates that the certificate time value is valid. A time can appear invalid (*Fail*) for a certificate that has expired.
Active	Revoked	A value of *Pass* indicates that the X509 certificate chain is valid for the certificate and contains no revoked certificates or errors.
Signature	NotSignatureValid	A value of *Fail* indicates that the X509 certificate chain is invalid as a result of an invalid certificate signature.
Usage	NotValidForUsage	A value of *Fail* indicates that the X509 certificate chain is invalid as a result of an invalid key usage.
Trusted Root	UntrustedRoot	A value of *Fail* indicates that the X509 certificate chain is invalid as a result of an untrusted root certificate.
Revocation Status	RevocationStatusUnknown	A value of *Pass* indicates that the revocation status can successfully be determined for the certificate. This may be the result of successful access to online certificate revocation lists (CRLs) and, if configured, authority information access (AIA) endpoints.
Chain Built	Cyclic	A value of *Pass* indicates that the certificate chain for the certificate could successfully be built.
Extensions	InvalidExtension	A value of *Fail* indicates that the X509 certificate chain is invalid as a result of an invalid extension.
Policy	InvalidPolicyConstraints	A value of *Fail* indicates that the X509 certi-

[1]The parameter names for results returned by the Keyfactor API ***GET /Certificates/{id}/Validate*** method.

Validation Test	Keyfactor API Equivalent[1]	Definition
Constraints		ficate chain is invalid as a result of an invalid policy constraint.
Basic Constraints	InvalidBasicConstraints	A value of *Fail* indicates that the X509 certificate chain is invalid as a result of an invalid basic constraint.
Valid Name Constraints	InvalidNameConstraints	A value of *Fail* indicates that the X509 certificate chain is invalid as a result of an invalid name constraint.
Supported Name Constraints	HasNotSupportedNameConstraint	A value of *Fail* indicates that a name constraint for the certificate is unsupported or that the certificate has no supported name constraints.
Defined Name Constraints	HasNotDefinedNameConstraint	A value of *Fail* indicates that a name constraint for the certificate is undefined.
Permitted Name Constraints	HasNotPermittedNameConstraint	A value of *Fail* indicates that a name constraint for the certificate is impermissible.
Excluded Name Constraints	HasExcludedNameConstraint	A value of *Fail* indicates that a name constraint for the certificate has been excluded.
Full Chain	PartialChain	A value of *Pass* indicates that the certificate chain for the certificate could successfully be built up to the root certificate.
CTL Time Valid	CtlNotTimeValid	A value of *Fail* indicates that the certificate trust list (CTL) is invalid because of an invalid time value (e.g. the CTL has expired).
CTL Signature Valid	CtlNotSignatureValid	A value of *Fail* indicates that the certificate trust list (CTL) contains an invalid signature.

[1]The parameter names for results returned by the Keyfactor API ***GET /Certificates/{id}/Validate*** method.

Validation Test	Keyfactor API Equivalent[1]	Definition
CTL Usage Valid	CtlNotValidForUsage	A value of *Fail* indicates that the certificate trust list (CTL) is not valid for this use.
Strong Signature	HasWeakSignature	A value of *Pass* indicates that the certificate has been signed with a secure hashing algorithm. A value of *Fail* can indicate that a hashing algorithm of MD2 or MD5 was used for the certificate.
CRL online	OfflineRevocation	A value of *Pass* indicates that the online certificate revocation list (CRL) the chain relies on is available.
Chain Policy	NoIssuanceChainPolicy	A value of *Pass* indicates that there is either no certificate policy by design in the certificate or that if a group policy has specified that all certificates must have a certificate policy, the certificate policy exists in the certificate.
No Explicit Distrust	ExplicitDistrust	A value of *Pass* indicates that the certificate is not explicitly distrusted.
Critical Extensions	HasNotSupportedCriticalExtension	A value of *Pass* indicates that the certificate has a critical extension that is supported or has no critical extensions.

Locations Tab

If you have added the certificate to any certificate store location(s) a number will appear in the **Count** column on the corresponding **Location Type** row. Users with limited permissions will only see locations for types of certificate stores to which they have been granted permissions either globally or via certificate store containers (see Container Permissions on page 624). Click the count number for more details regarding this certificate's location. See Add to Certificate Store on page 43 for more information. The *Total Cert Store Locations* appears at the end of the list. Clicking on the total will open a dialog with the list of locations with the columns: Store Path, Store Machine, Alias, IPAddress, Port, and Agent Pool which will be populated depending on the details of the individual stores.

Note: The SSL network name is searchable with certificate search and also appears in the location details grid of the certificate details, if the certificate was found during an SSL scan.

[1]The parameter names for results returned by the Keyfactor API ***GET /Certificates/{id}/Validate*** method.

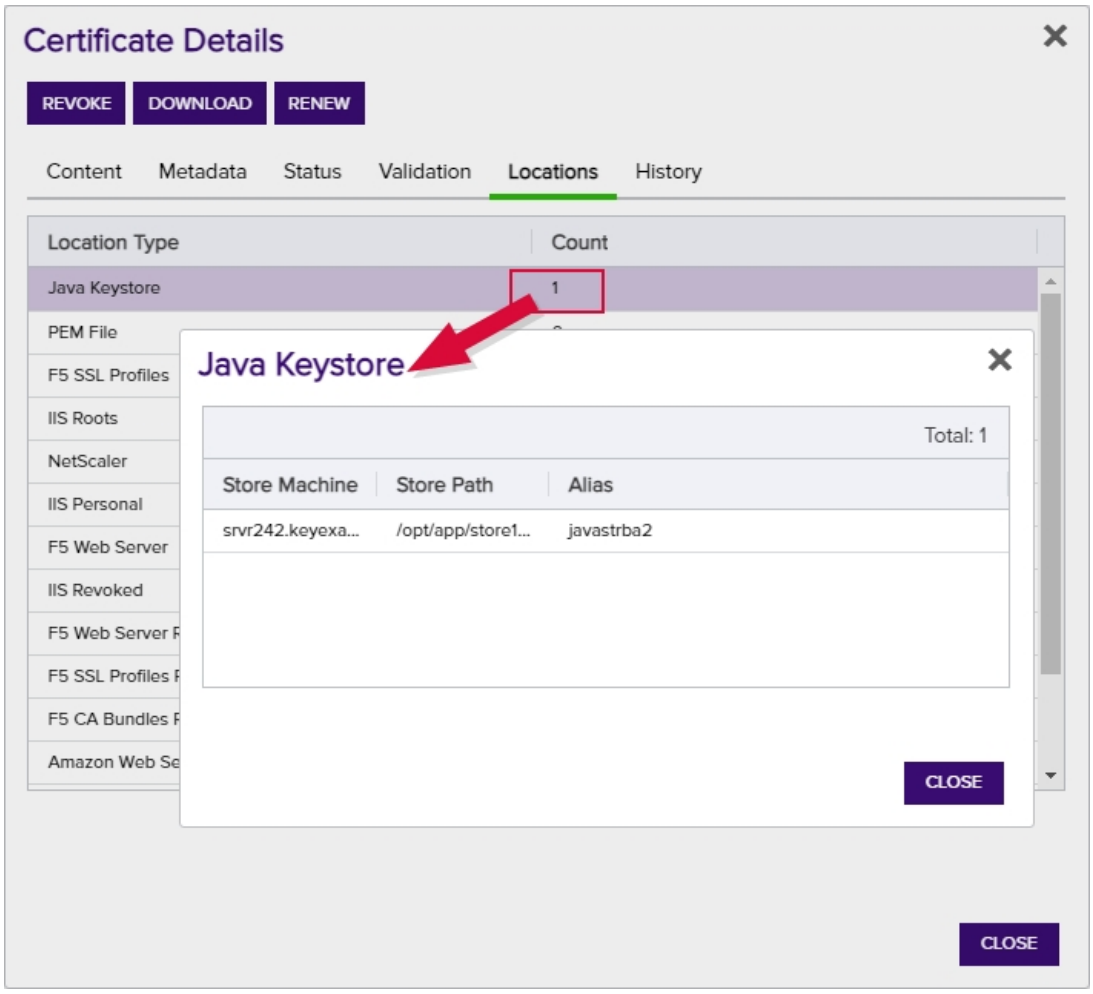


Figure 23: Location Details

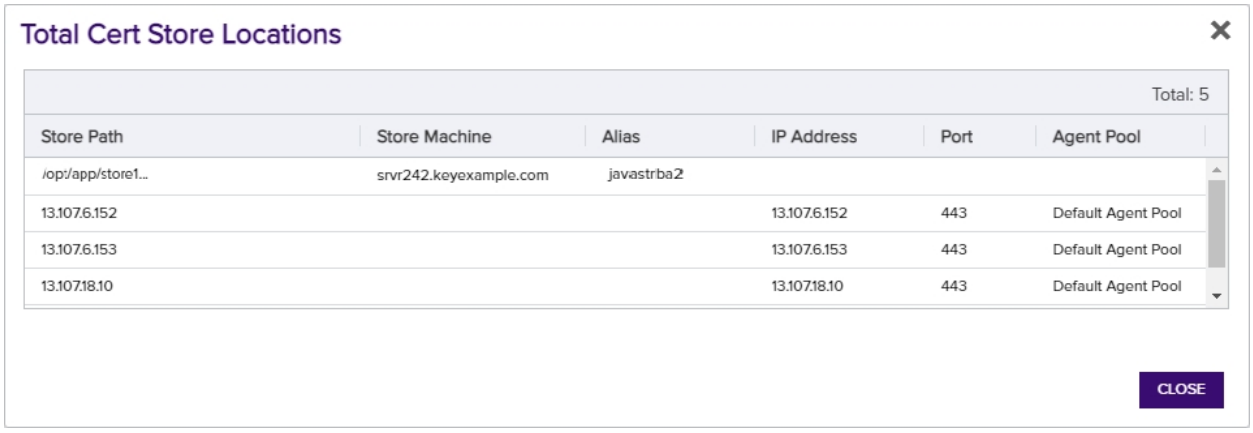


Figure 24: Total Certificate Store Location Details

History Tab

History about a certificate is recorded in the Keyfactor Command database for the following types of activities (see also Audit Log on page 652):

- Initial Import—A history entry is made on import via CA synchronization, SSL synchronization, certificate store synchronization or manual import.
- Certificate Enrollment—A history entry is made when a PFX or CSR enrollment is completed through the Keyfactor Command Management Portal. The source of the request (PFX or CSR) is indicated.
- Revocation—A history entry is made each time a certificate is revoked, so if a certificate is revoked multiple times, there will be multiple history entries.
- Key Recovery—A history entry is made each time the key for a certificate is recovered, so if the key for a given certificate is recovered multiple times, there will be multiple history entries. This type of record is generated when the private key for a certificate is downloaded from the Keyfactor Command database or when a private key is recovered from a CA using the CA's key recovery mechanism.
- Certificate Store Additions and Removals—A history entry is made each time a certificate is added to a certificate store or removed from a certificate store. These entries reference the specific certificate store type and whether the operation was an addition or removal—*Add ([store type])* and *Remove ([store type])*—and include details in the certificate history comments.
- Certificate Renewals—A history entry is made each time a certificate is renewed or reissued. The certificate renewal history record appears on the old certificate, not the new certificate.
- Certificate Store Inventory Discoveries—A history entry is made each time an inventory of a certificate store notices that a certificate that was in a certificate store no longer is or that a new certificate has appeared in the certificate store. These entries are referenced as *Certificate Appeared ([store type])* and *Certificate Disappeared ([store type])* with details in the certificate history comments.
- SSL Endpoint Inventory Discoveries—A history entry is made each time an inventory of an SSL endpoint notices that a certificate that was at an endpoint no longer is or that a new certificate has appeared at an endpoint during a monitoring task. These entries are referenced as *Certificate Appeared (SSL Sync)* and *Certificate Disappeared (SSL Sync)* with details in the certificate history comments.
- Metadata Updated—A history entry is made each time a metadata field is updated for the certificate. The changed data will be recorded in the *Comment* field.

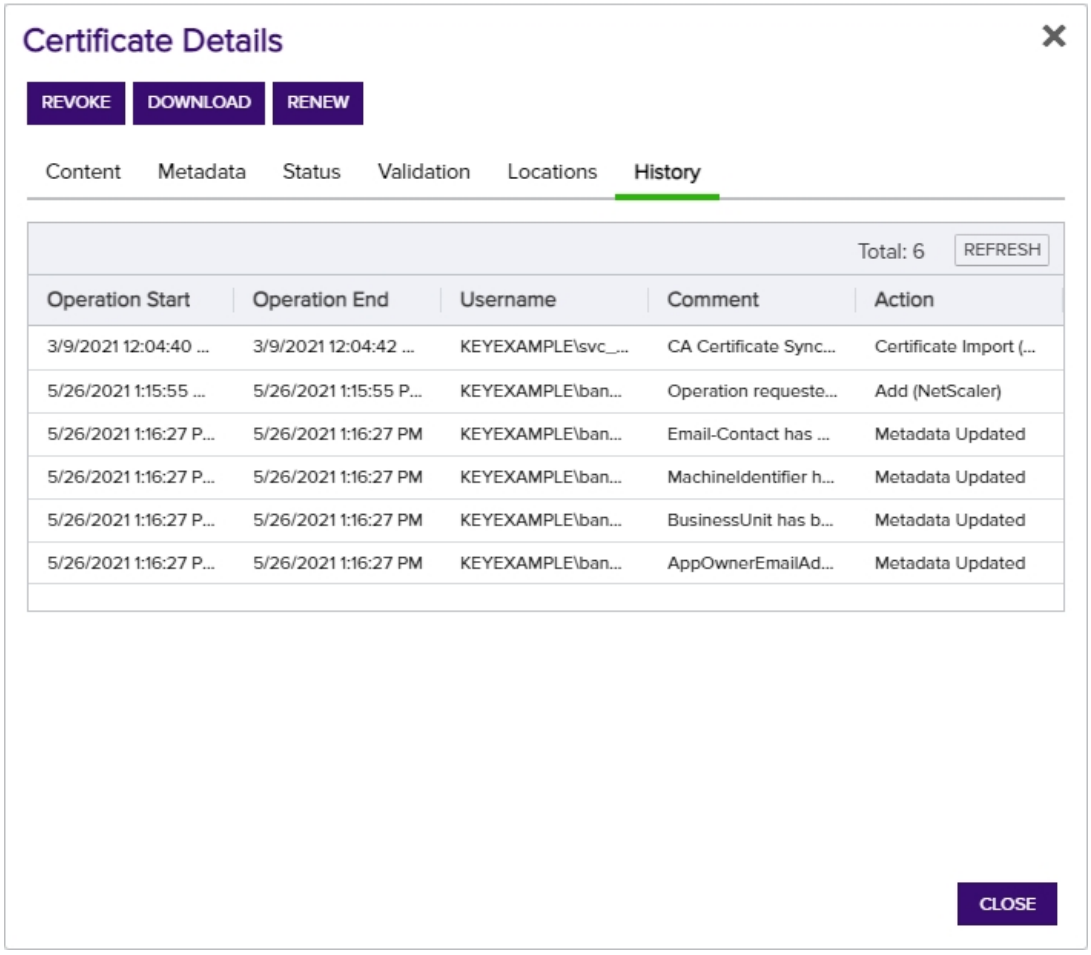


Figure 25: Certificate Operation: Certificate History Tab

Tip: Double-click a row on the History grid to see the content of that row in a more readable pop-up.

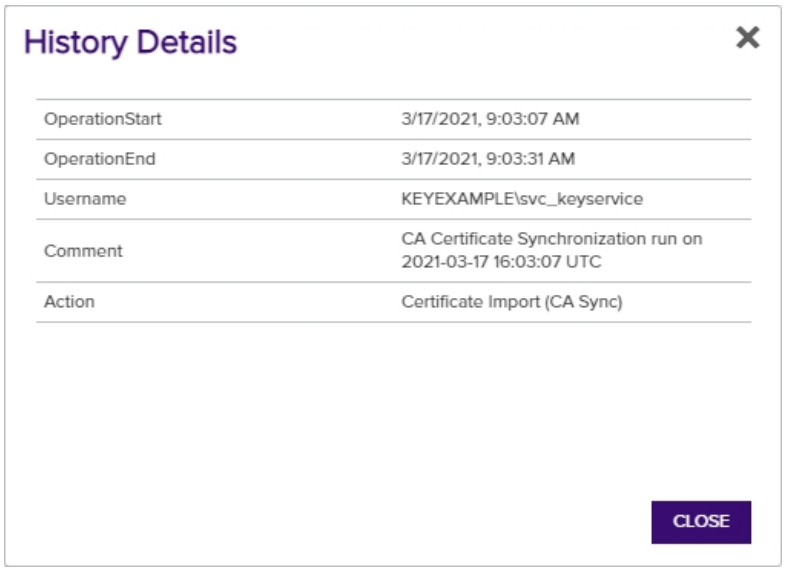


Figure 26: Certificate Operation: Certificate History Detail

2.1.3.2 Certificate Search Page

The search function allows you to query the database for information. The same query structure is used in multiple locations within the Keyfactor Command Management Portal.

When you first open the page, you will see the simple search option. To execute a search, select the field and comparison operators in the dropdowns and type something on which to search in the value field (if applicable). If you select an *is null* or *is not null* comparison operator, the value field will be grayed out. Click the **Search** button to execute the query.

Each query consists of three parts:

Query Field

The available fields for querying vary depending on the area of the Management Portal in which the search is used. On this page, the queries can be done on the following built-in fields:

ArchivedKey

The certificate's archived key has been encrypted and saved to the Keyfactor Command database (true/false).

CertId

Numeric matches with the Keyfactor Command reference ID for the certificate.

CA

KeyType

The selected certificate key type: Unknown, RSA, DSA, ECC, DH, Ed448, Ed25519, Dilithium2, Dilithium3, Dilithium5.

KeyUsage

Certificate includes or doesn't include (or is null or not null for) the selected key usage; CRLSign, DataEncipherment, DecipherOnly, DigitalSignature, EncipherOnly, KeyAgreement, KeyCer-

Complete or partial matches with the certificate issuing CA logical name.

CertState

The certificate state; Unknown, Active, Revoked, CertificateAuthority, ParentCertificateAuthority.

CertStoreFQDN

Complete or partial matches with the fully qualified domain name of the computer hosting one or more certificate stores.

This field has an alias of *JavaKeystoreFQDN* that may be used when querying the field from the Keyfactor API.

CertStorePath

Complete or partial matches on the full path to a certificate store—e.g. /opt/application/mystore.jks or c:\program files\application\mystore.jks.

This field has an alias of *JavaKeystorePath* that may be used when querying the field from the Keyfactor API.

CertStoreContainer

Certificate is in a certificate store that is included in the container criteria indicated.

CN

Complete or partial matches with the certificate common name.

This field has an alias of *IssuedCN* that may be used when querying the field from the Keyfactor API.

DN

Complete or partial matches with the certificate distinguished name.

This field has an alias of *IssuedDN* that may be used when querying the field from the Keyfactor API.

ExpirationDate

Certificate expiration before, after, or on a

tSign, KeyEncipherment, NonRepudiation.

NetBIOSPrincipal

Complete or partial matches with the certificate principal name in NetBIOS format (DOMAIN\username). Supports the %ME% token (see Advanced Searches on page 38).

This field has an alias of *PrincipalName* that may be used when querying the field from the Keyfactor API.

NetBIOSRequester

Complete or partial matches with the certificate requester's name in NetBIOS format (DOMAIN\username). Supports the %ME% token (see Advanced Searches on page 38).

This field has an alias of *RequesterName* that may be used when querying the field from the Keyfactor API.

OU

Complete or partial matches with the certificate organizational unit.

PublicKey

Exact matches with the certificate public key in hexadecimal or base64 format.

RevocationDate

Certificate revocation before, after, or on a specified date, or is null or not null. Be sure to check the *Include Revoked* checkbox to view revoked certificates. Supports the %TODAY% token (see Advanced Searches on page 38).

This field has an alias of *RevocationEffDate* that may be used when querying the field from the Keyfactor API.

Revoker

Complete or partial matches with the name of the user (DOMAIN\username format) who revoked the certificate. Be sure to check the *Include Revoked*

specified date. Supports the %TODAY% token (see Advanced Searches on page 38). Be sure to check the *Include Expired* checkbox to view expired certificates.

This field has an alias of *NotAfter* that may be used when querying the field from the Keyfactor API.

EKU

Complete or partial matches with the certificate template OID.

EKUName

Complete or partial matches with the certificate template Name.

HasPrivateKey

Certificate private key encrypted and stored in the Keyfactor Command database (true/false).

ImportDate

The certificate imported to Keyfactor Command before, after, or on a specified date.

IssuedDate

Certificate issuance before, after, or on a specified date. Supports the %TODAY% token (see Advanced Searches on page 38).

This field has aliases of *NotBefore* and *EffectiveDate* that may be used when querying the field from the Keyfactor API.

IssuerDN

Complete or partial matches with the certificate issuer's distinguished name.

KeyfactorRequestId

Numeric matches with the Keyfactor Command reference ID for the certificate request.

KeySize

Complete or partial matches with the certificate checkbox to view revoked certificates.

RFC2818Compliant

Certificate is compliant with RFC 2818 (contains a DNS SAN) (true/false).

SelfSigned

Certificate is self-signed (true/false).

SerialNumber

Complete, or starts/ends with, or null/not null matches with the certificate serial number.

SigningAlgorithm

Complete or partial matches with the certificate signing algorithm.

SSLDNSName

Complete or partial matches with the DNS name resolved for an SSL endpoint.

SSLIPAddress

Complete, or starts/ends with, or null/not null matches with the IP address defined for an SSL endpoint.

This field has an alias of *SslHostName* that may be used when querying the field from the Keyfactor API.

SSLNetworkName

Complete, or starts/ends with, or null/not null matches with the network name under which an SSL endpoint was found.

SSLPort

Complete or partial numeric matches with the port number defined for an SSL endpoint.

SAN

Complete or partial matches with the certificate

key size.

This field has an alias of *KeySizeInBits* that may be used when querying the field from the Keyfactor API.

subject alternate name(s).

TemplateDisplayName

Complete or partial matches with the certificate template display name.

This field has an alias of *TemplateName* that may be used when querying the field from the Keyfactor API.

TemplateShortName

Complete or partial matches with the certificate template name.

Thumbprint

Complete or partial matches with the certificate thumbprint value.

You can also do queries based on user-defined metadata fields (see Certificate Metadata on page 646).

Comparison Operator

The query comparison operators vary depending on the type of field selected and the specific properties of the field. The list below shows the dropdown list comparison operators, as well as the equivalent query language syntax (in parentheses).

Most string fields (the vast majority of the built-in fields) support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Contains (-contains)
- Does not contain (-notcontains)
- Starts with (-startswith)
- Ends with (-endswith)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Most date and integer fields support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Is less than (-lt)
- Is less than or equal to (-le)
- Is greater than (-gt)
- Is greater than or equal to (-ge)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Most Boolean (true/false) fields support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Comparison Value

The value you enter for comparison must match the field type. For example, integer fields only support numerical values. String fields support all alphanumeric characters. Boolean fields only support True or False. The value field is not case sensitive. Date fields support only properly formatted dates and will initially display as mm/dd/yyyy. You can choose to populate the date field by:

- Clicking in a date Value field to open a pop-up calendar to select a date that will populate the field.
- Clicking in a segment of the date format (i.e., mm/dd/yyyy) and entering a value. As you continue to type in any one segment, the cursor will keep moving onto the next segment.

The results that match your search criteria will be displayed in the results grid below the search selection options. The results grid includes these fields:

Issued DN

The distinguished name of the certificate subject.

Import Date

The date the certificate was imported to Keyfactor Command. This field will auto populate on any new imports/enrollments of certificates. On an upgrade, this field will be populated in existing certificates from the certificate operation history.

Effective Date

The date the certificate was issued or became active.

Expiration Date

The date the certificate expires.

Issued CN

The common name of the certificate subject.

Issuer DN

The distinguished name of the certificate issuer.

Certificate Template

The short name of the template used to issue the certificate.

Principal Name

The identity that the certificate represents. The principal name field is populated during certificate synchronization by the user principal name (UPN) extracted from Active Directory if there is a principal name in the certificate subject alternative name (SAN).

Requester

The user or entity that requested the certificate.

Locations

The server(s), if any, that the certificate is hosted on (e.g. for SSL certificates). If the certificate is found on multiple servers, this field will show the number of servers on which it was found and the location type (e.g. *4 SSL* or *6 JKS*). The specific server names can be found in the certificate details.

Key Type

The key type of the certificate.

Key Size

The key size of the certificate.

Certificate State

The certificate state options are:

- Unknown (0)

- Active (1)
- Revoked (2)
- Failed (4)
- Pending (5)
- Certificate Authority (6)
- Parent Certificate Authority (7)

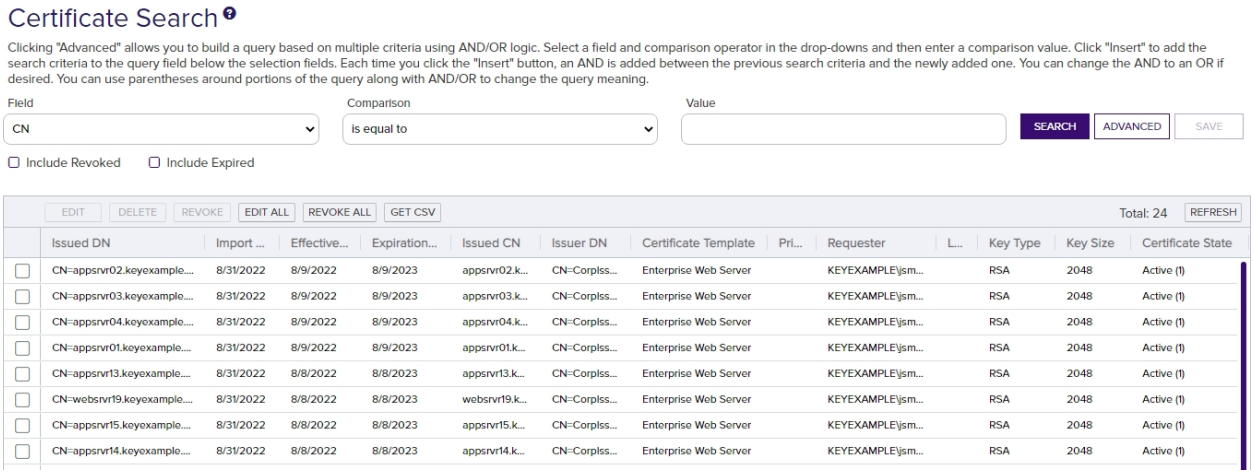


Figure 27: Certificate Search

The search results can be sorted by clicking on a column header in the results grid for every column (except Certificate Locations, Key Type, and Certificate State). Click the column header again to reverse the sort order. The grid columns can be arranged in any order desired by click-holding and dragging the header of the column you wish to move. The column widths may be adjusted by click-holding and dragging the line separating two column headers.

You can click the **Include Revoked** and/or **Include Expired** buttons at the top of the results grid to toggle inclusion of revoked or expired certificates in the results. By default they are excluded.

The rest of the buttons at the top of the display grid are used to interact with the certificates displayed in the results grid. Some buttons are grayed out until you click on a grid row. Other certificate functions are available on the right-click menu. To open the right-click menu, highlight a row in the results grid and right-click. You can also double-click a certificate row in the results grid to open the Certificate Details (see Certificate Details on page 19).

To select a single row in the grid, click to highlight it and then select an operation from either the top of the grid or the right-click menu. Some of the certificate operations support action on multiple certificates at once. To select multiple rows, hold down the CTRL key and click each row on which you would like to perform an operation, or tick the check box next to the row. Then select an operation from the top of the grid. The right-click menu supports limited operations on the multiple certificates.

Advanced Searches

On any search page you can click **Advanced** to the right of the Search button to display the advanced search options. Click **Simple** to close the advanced search options again.

Multiple Criteria

Using the advanced search options, you can build a query based on multiple criteria using AND/OR logic. As with a simple search, you select a field and comparison operator in the drop-downs and then enter a comparison value, if applicable. Click **Insert** to add the search criteria to the query field below the selection fields. Use the selection fields to build multiple search criteria. Each time you click the insert button, an AND is added between the previous search criteria and the newly added one. You can change the AND to an OR if desired. You can use parentheses around portions of the query along with AND/OR to change the query meaning.

For example, for certificate searches:

```
(CN -contains "appsrvr" AND IssuedDate -ge "01/01/2022") OR (CN -contains "appsrvr" AND
TemplateShortName -contains "web")
```

This query will return all the certificates issued on or after January 1, 2022 with the string appsrvr in the CN and also all certificates issued at any time with the string appsrvr in the CN using a template referencing web. When you have entered all the desired search criteria, click **Search** to execute the query. If you wish to clear the query field and start over, click the **Clear** button.

Note: Multiple *OR* queries can be slow due to the nature of the query not being indexed and potentially requiring multiple queries of the database. To mitigate this, we suggest you create a collection for the subset of certificates, using the *OR* statement as needed, then perform a search starting with that collection and adding any additional conditions using advanced search from the search page. See Saving Search Criteria as a Collection on page 40.

In addition to the options available in the query builder, three special values can be used in selected searches by typing them in directly:

- %TODAY%
  Use the TODAY special value in place of a specific date in date queries. This option supports math operations, so you can use TODAY-10 or TODAY+30. The built-in *Certificates Expiring in 7 Days* collection uses this special value (see Certificate Collection Manager on page 80).

  Example: Create a certificate search of IssuedDate -ge ”%TODAY-7%” and save it as a collection called *Certificates Issued in the Last Week*. Create another certificate search of ExpirationDate -lt ”%TODAY+60%” and save it as a collection called *Certificates Expiring in the Next 60 Days*. This allows you to have saved collections containing a comparison date without having to update the date in the collection.

- %ME%
  Use the ME special value in place of a specific domain\user name in queries that match a

domain\user name. The built-in *My Certificates* collection uses this special value (see Certificate Collection Manager on page 80).

Example: Create a certificate search of NetBIOSRequester -contains ”%ME%” and save it as a collection. Multiple users can now use this same collection to search for all the certificates on which they were the requester in the current domain.

Note: Certificate collections saved using the %ME% value are *not* supported for use in reports or on the dashboard.

- %ME-AN%
  Use the ME-AN special value in place of a specific user name excluding the domain. This is beneficial in environments with multiple domains where there is a desire to query for a user’s certificates even if they were requested across multiple domains.

  Example: Create a certificate search of NetBIOSRequester -contains ”%ME-AN%” and save it as a collection. Multiple users can now use this same collection to search for all the certificates on which they were the requester, regardless of domain.

  Note: Certificate collections saved using the %ME-AN% value are *not* supported for use in reports or on the dashboard.

Important: The special query options of %TODAY%, %ME%, and %ME-AN% are only supported in uppercase. Lowercase equivalents (e.g. %me%) cannot be substituted.

To build a deep link with your search criteria, begin with the following URL (where KEYFACTOR_SERVER_FQDN is the FQDN of your Keyfactor Command administration server):

https://KEYFACTOR_SERVER_FQDN/keyfactorportal/CertificateCollection/Query?query=YOUR_URL_ENCODED_QUERY

Your Management Portal may have been configured to use HTTP rather than HTTPS.

Replace YOUR_URL_ENCODED_QUERY with your search criteria as built using the advanced search. The search criteria needs to be URL encoded, so, for example, spaces need to be replaced with %20 and quotation marks with %22. However, many modern browsers will automatically do this for you. A deep link using part of the example search shown above would look something like this without URL encoding:

https://keyfactor.keyexample.com/keyfactorportal/CertificateCollection/Query?query=CN -contains ”appsrvr”

And with URL encoding, like this:

https://key-factor.keyexample.com/keyfactorportal/CertificateCollection/Query?query=CN%20-contains%20%22appsrvr%22

Tip: Click the help icon (?) next to the page title to open the embedded web copy of the *Keyfactor Command Documentation Suite* to this section.
You can also find the help icon at the top of the page next to the **Log Out** button. From here you can choose to open either the *Keyfactor Command Documentation Suite* at the home page or the *Keyfactor API Endpoint Utility*.

Saving Search Criteria as a Collection

To save your search criteria as a certificate collection:

1. Click the **Save** button.

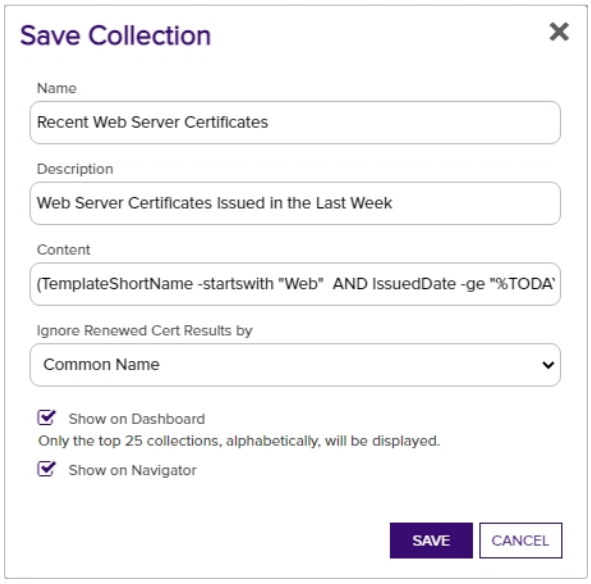


Figure 28: Save Certificate Collection

2. In the Save Certificate Search dialog, enter a name for the certificate collection. This name appears at the top of the page for this collection and can be configured to appear on the Management Portal menu under Certificates. It will also appear in other places within the Management Portal where you can reference certificate collections (e.g. expiration alerts and certain reports and dashboards). Because it can appear on the menu and in selection drop-downs, the name should be fairly short.

3. Enter a description for the collection. This description appears as a subtitle below the collection name on the page for this collection and can be more detailed than the collection name.

4. Select a setting in the *Ignore renewed certificate results by* dropdown. The *Ignore* dropdown applies to processing reports or expiration alerts and contains these options:

None

Do not eliminate duplicate certificates when processing reports or expiration alerts based on this certificate collection.

Common Name

Eliminate duplicate certificates based on the common name in the certificate when processing reports or expiration alerts. Certificates will be excluded from reports and expiration alerts if they share the same common name and enhanced key usage (EKU—e.g. Client Authentication). The certificate with the most recent issued date and the given common name and EKU will be included in the report or expiration alert.

Distinguished Name

Eliminate duplicate certificates based on the distinguished name in the certificate when processing reports or expiration alerts. Certificates will be excluded from reports and expiration alerts if they share the same distinguished name and EKU. The certificate with the most recent issued date and the given distinguished name and EKU will be included in the report or expiration alert.

Principal Name

Eliminate duplicate certificates based on the principal name in the certificate status data stored in the Keyfactor Command database for the certificate when processing reports or expiration alerts. The principal name is added to the certificate status data for the certificate during certificate synchronization if the certificate SAN contains a *user principal name* or *NT principal name*. Certificates will be excluded from reports and expiration alerts if they share the same principal name and EKU. The certificate with the most recent issued date and the given principal name and EKU will be included in the report or expiration alert.

Note: Regardless of the selection you make in the Ignore option, all certificates will appear in the search results grid. Duplicate certificates are not excluded on this page. When processing reports or expiration alerts based on this certificate collection, only certificates that share all the EKUs (e.g. Client Authentication and Server Authentication) as well as the same CN, DN or UPN will be eliminated as duplicates. If a certificate has more than one EKU and at least one EKU does not match an otherwise similar certificate with matching CN, DN or UPN, it will not be eliminated on reports or expiration alerts.

5. Check the **Show on Dashboard** box to include the results from this collection on the *Collection* dashboard (see Dashboard: Collections on page 12). You will not be able to change this setting once the collection is saved. If you need to change it, you would need to edit the collection and re-save it.

   Note: The collections dashboard widget will only display the first 25 collections alphabetically. A brief warning message explaining this will be shown on the collections save dialog when the **Show on Dashboard** box is checked.

6. Check the **Show in Navigator** box to include the collection on the Management Portal menu (on the *Certificates* top-level menu dropdown).

7. Click **Save** to save the collection. The search results will display immediately. If you didn't select the **Show in Navigator** option, you can find the collection again on the Certificate Collection Management page, accessed by navigating to *Certificates > Collection Manager* from the Management Portal.

Tip: If you **Save** a new certificate collection, or **Save** a change to an existing certificate collection, that change will be immediately reflected in the collection data used to display certificate collections on dashboards and reports. The data used by the dashboards and reports is stored in an intermediate table that is updated immediately. It will also continue to be updated periodically (approximately every 20 minutes by default as configured by the *Dashboard Collection Caching Interval* application setting) by the Keyfactor Command Service (see Application Settings: Console Tab on page 584).

2.1.3.3 Certificate Operations

Most common certificate operations (except enrollment) are available on the Certificate Search grid. The actions available on the grid header include: **Edit** (users with read-only permissions will see **Display** instead), **Delete**, **Revoke**, **Edit All**, **Revoke All**, **Delete All** (for collections only), and **Get CSV**. Secondary operations are shown on the context menu, accessed by right-clicking on a selected row on the Certificate Search grid. The context menu includes **Edit** (or **Display**), **Delete**, **Delete Private Key**, **Revoke**, **Download**, **Add to Certificate Store**, **Remove from Certificate Store**, **Renew**, and **Identity Audit**. There is also an operation to place a hold, or remove a hold, on a certificate, which is available from the Revoke operation through the Revocation Reason: Certificate Hold/Remove From Hold. When selecting multiple rows, only the operations Edit, Delete, Revoke and Delete Private Key (only if the private key is stored in the database) are enabled on the grid header and the context menu. For the edit commands, the only details that can be edited are the metadata fields.

Note: As of Keyfactor Command version 10, enrollment (PFX and CSR), renewal, and revocation requests all flow through Keyfactor Command workflow. This will result in no changes to the enrollment, renewal, and revocation user experience unless customizations have been added in workflow (see Workflow Definitions on page 218).

Full descriptions of the available certificate operations are below.

Add to Certificate Store

Before adding a certificate to a certificate store in Keyfactor Command, you must approve an orchestrator to handle the store and create a record for the store in Keyfactor Command. See Orchestrator Management on page 481 and Certificate Store Operations on page 385.

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:
Certificates: *Read*
Certificates: *Download with Private Key*
Certificate Store Management: *Read*
Certificate Store Management: *Schedule*

Permissions for certificates and certificate stores can be set at either the global or certificate collection and certificate store container level. See Certificate Permissions on page 621 and Container Permissions on page 624 for more information about global vs collection and container permissions.

Note: Certificates cannot be added to stores that require private keys (e.g. IIS personal stores) from this interface unless the selected certificate contains a private key stored in the database. If the selected certificate does not contain a stored private key, stores that require a private key will not appear on the Select Certificate Store Locations dialog.

To add a certificate to a certificate store:

1. Highlight the row in the results grid and right-click.
2. Choose **Add to a Certificate Store** from the right-click menu.
3. When you select the Add to Certificate Store option the *Select Certificate Store Locations* dialog opens. When you select the certificate stores to which you want to deploy your certificate and click **Include**, the *Add to Certificate Stores* dialog appears BEHIND the *Select Certificate Store Locations* dialog, holding your selection and leaving the *Select Certificate Store Locations* dialog open for you to continue selecting locations. The final list of selections will only be accessible once you close the *Select Certificate Store Locations* dialog using the **Include and Close** button.

Select Certificate Store Locations

The *Select Certificate Store Locations* dialog allows you to run queries against your certificate store list to select which store(s) to deploy a selected certificate to. **Check** the box next to each certificate store location to which you want to distribute the certificate.

Note: Only compatible certificate stores and only stores in containers to which you have permissions are shown on the grid.

Tip: You may change the search results by using the search fields at the top of the dialog. All of the Keyfactor Command grid search features are available to assist your search. See Using the Certificate Store Search Feature on page 382 for more information on the available search fields. The default search criteria is *AgentAvailable is equal to True*.

The actions on the *Select Certificate Store Locations* dialog are:

- **Include**

  Click this to add the selected certificate store(s) to your certificate selection and leave the search dialog open for further searches.

- **Include and Close**

  Click this to close the search dialog and add the selected certificate store(s) to your certificate selection, which will then be displayed and ready for updates as per the instructions in *Add to Certificate Stores*.

- **Close**

  Click this to cancel the operation and return to the main page with no certificate stores selected.

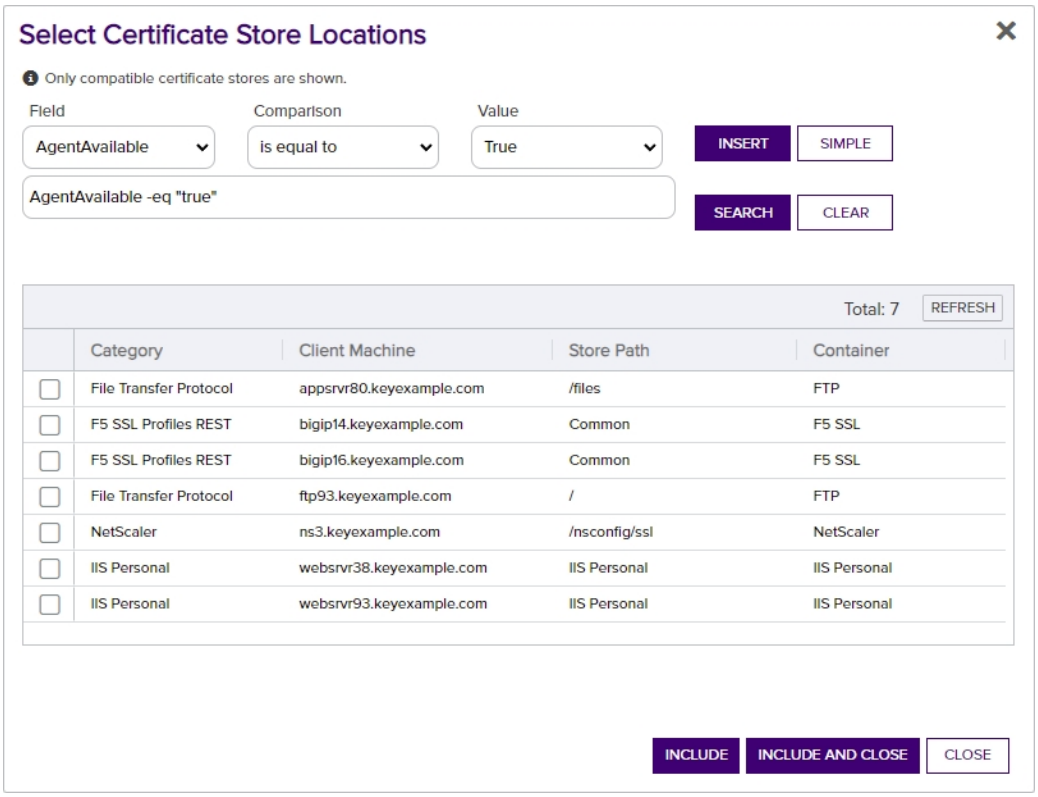


Figure 29: Select Certificate Store Locations Dialog

Add to Certificate Stores

The *Add to Certificate Stores* page appears once you select at least one certificate store to distribute your certificate to. It includes a grid section with a series of tabs that display a tab for each type of certificate store selected with a list of the selected stores under each tab. The header section of the dialog shows global options that apply to the add job as a whole:

- **Include Certificate Stores**

  You may return to the *Select Certificate Store Locations* dialog by clicking **Include Certificate Stores** above the grid. The current selections will be retained.

- **Schedule when to run the job for the certificate store**

  In the **Schedule** dropdown, select a time at which the job to add the certificate to the stores should run. The choices are *Immediate* or *Exactly Once* at a specified date and time. If you choose *Exactly Once*, enter the date and time for the job. A job scheduled for *Immediate* running will run within a few minutes of saving the operation. The default is *Immediate*.

- **Include Private Key on Certificate Stores when the Private Key is optional**

Check the **Include Private Key** box if you want to deliver the private key of the certificate to any selected certificate stores that do not require a private key (e.g. Java keystores). This option only appears for certificates that have a private key available for distribution.

Click **Remove** at the top of the grid to remove the selected certificate store from the page. The certificate will not be added to the store.

For each selected certificate store you can apply the following actions:

- **Overwrite**

  Check **Overwrite** below the grid to overwrite any existing certificate in the same location and with the same name or alias for the selected certificate store type.

- **Alias**

  Add an **Alias** below the grid, if applicable, for the certificate store type. See the **Information Required by Certificate Store** section, below, for more information.

  Note: The tab heading of the certificate location will display an alert if an alias is required for the location. If this is set to **Forbidden** on the certificate store type, the **Alias** field will not display unless "Overwrite" is checked on this page.

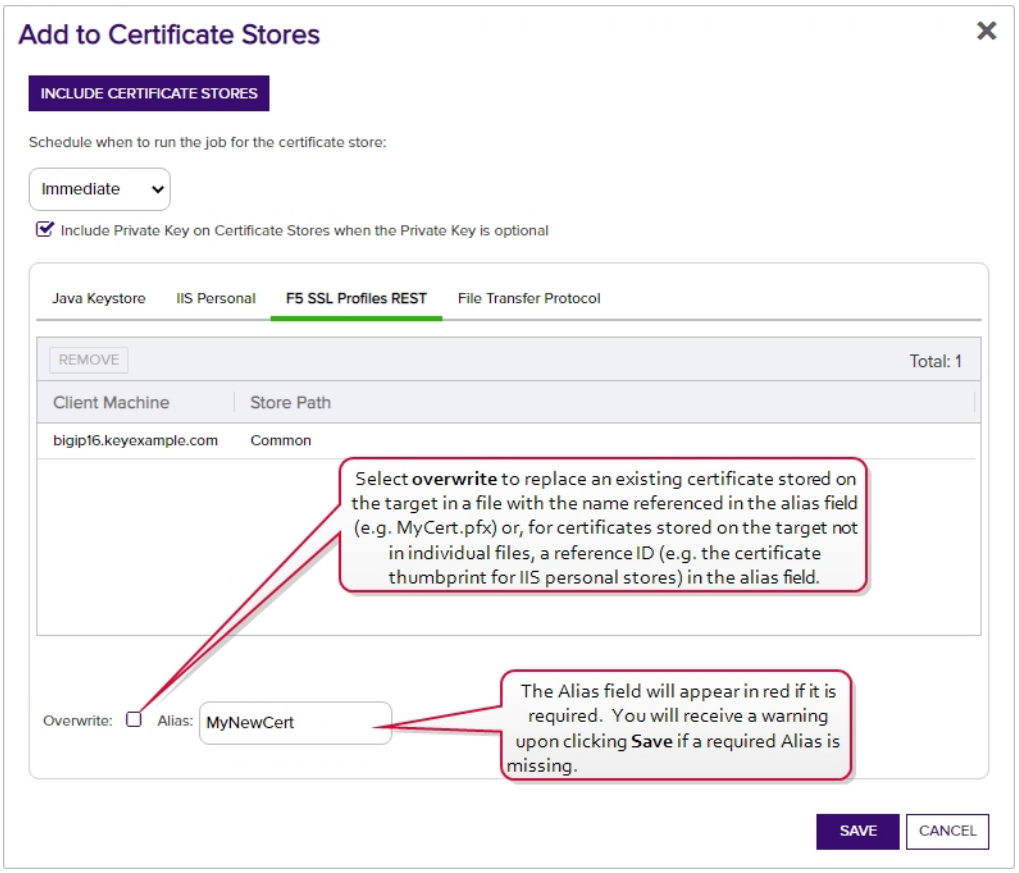


Figure 30: Add Certificate—Install into Certificate Locations

Figure 31: Alias Required Alert on Save

Information Required by Certificate Stores

Each type of certificate store has different requirements for providing an alias or other additional information. Table 3: Alias Requirements by Certificate Store Type provides a quick breakdown by certificate store of whether a certificate alias is required for new certificate additions or only for overwriting an existing certificate in the store.

Tip: When adding a certificate to a certificate store, you have the option to overwrite an existing certificate with the current certificate. If you choose this option, you will need to provide the alias of the certificate you wish to overwrite. Find the alias values by navigating to *Management Portal > Certificates > Certificate Search*. Select the certificate

you wish to overwrite and double-click, or click **Edit**, from the grid header or right-click menu. Choose the **Locations** tab and double-click on the Location Type (this must have a number other than zero in the *Count* column) to open the details dialog. The *Alias* field holds the information that may be required for an overwrite.

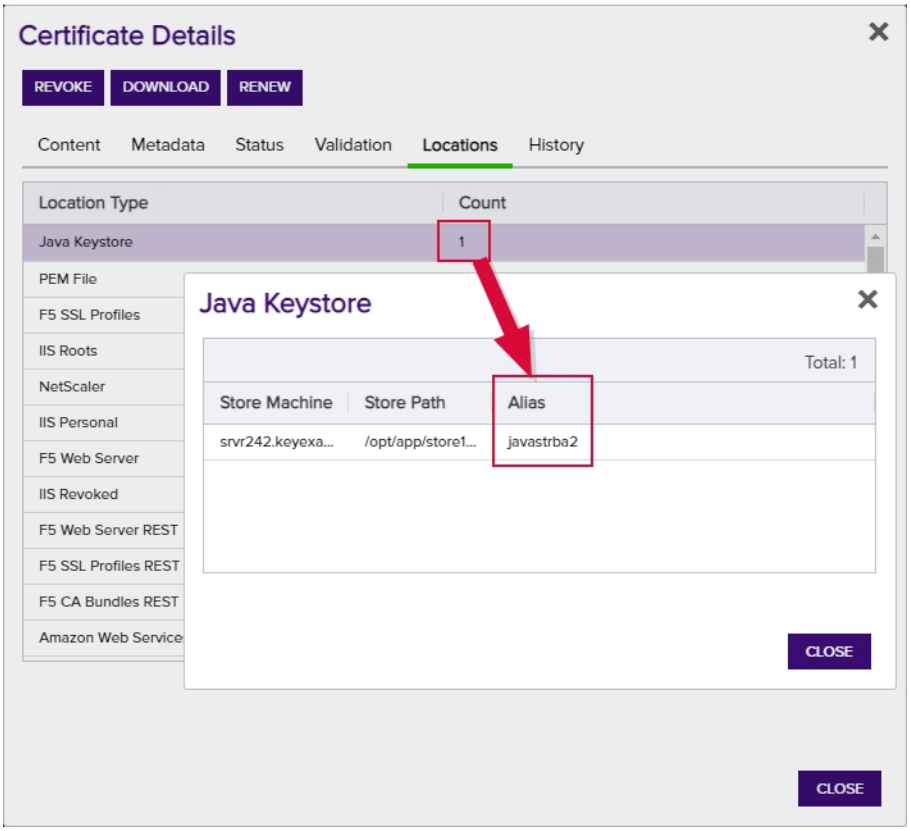


Figure 32: Example: Certificate Location Details for a JKS Location

Table 3: Alias Requirements by Certificate Store Type

Certificate Store Type	Alias Functionality
Amazon Web Services	Alias only required for overwrites
F5 CA Bundles REST	Alias required for new additions and overwrites

Certificate Store Type	Alias Functionality
F5 SSL Profiles	Alias required for new additions and overwrites
F5 SSL Profiles REST	Alias required for new additions and overwrites
F5 Web Server	Alias only required for overwrites
F5 Web Server REST	Alias only required for overwrites
File Transfer Protocol	Alias required for new additions and overwrites
IIS Personal	Alias only required for overwrites
IIS Revoked	Alias not needed
IIS Trusted Roots	Alias not needed
Java Keystore	Alias required for new additions and overwrites
NetScaler	Alias required for new additions and overwrites
PEM File	Alias only required for overwrites

Amazon Web Services (AWS)

Amazon Web Services (AWS) certificate stores require the addition of a private key and will only appear as an option when you select a certificate with a private key. With this type of store, you have the option to overwrite an existing certificate with the current certificate. If you choose this option, you will need to provide the alias of the certificate you wish to overwrite. The alias is the internal ID assigned by Amazon (the Amazon resource number or ARN). Provide the entire contents of the *Alias/IP* from this field when entering an alias for overwrite. For example:

arn:aws:acm:us-west-2:220531701668:certificate/88e5dcfb-a70b-4636-a8ab-e85e8ad88780

F5 CA Bundles REST

F5 CA Bundle REST certificate store additions do not require the addition of a private key and will appear for both certificates with a private key and those without. With this type of store, you will be prompted to add an alias for the certificate. The alias is the file name used to store the file in the device file system, minus the extension (e.g. use alias MyFile for a file named MyFile.crt). Aliases should be entered without spaces. Note that certificate names are case sensitive. You have the option to overwrite an existing certificate with the current certificate. If you choose this option, you will need to provide the alias of the certificate you wish to overwrite.

F5 SSL Profile

F5 SSL Profile certificate store additions do not require the addition of a private key and will appear for both certificates with a private key and those without. With this type of store, you will be prompted to add an alias for the certificate. The alias is the file name used to store the file in the device file system, minus the extension (e.g. use alias MyFile for a file named MyFile.pfx). Aliases should be entered without spaces. Note that certificate names are case sensitive. You have the option to overwrite an existing certificate with the current certificate. If you choose this option, you will need to provide the alias of the certificate you wish to overwrite.

F5 SSL Profile REST

F5 SSL Profile REST certificate store additions do not require the addition of a private key and will appear for both certificates with a private key and those without. With this type of store, you will be prompted to add an alias for the certificate. The alias is the file name used to store the file in the device file system, minus the extension (e.g. use alias MyFile for a file named MyFile.pfx). Aliases should be entered without spaces. Note that certificate names are case sensitive. You have the option to overwrite an existing certificate with the current certificate. If you choose this option, you will need to provide the alias of the certificate you wish to overwrite.

F5 Web Server

F5 Web Server certificate stores require the addition of a private key and will only appear as an option when you select a certificate with a private key. With this type of store, you have the option to overwrite an existing certificate with the current certificate. If you choose this option, you will need to provide the alias of the certificate you wish to overwrite. The alias for F5 device certificates is typically *server*.

F5 Web Server REST

F5 Web Server REST certificate stores require the addition of a private key and will only appear as an option when you select a certificate with a private key. With this type of store,

you have the option to overwrite an existing certificate with the current certificate. If you choose this option, you will need to provide the alias of the certificate you wish to overwrite. The alias for F5 device certificates is typically *server*.

File Transfer Protocol (FTP)

File Transfer Protocol (FTP) certificate store additions do not require the addition of a private key and will appear for both certificates with a private key and those without. With this type of store, you have the option to overwrite an existing certificate with the current certificate. If you choose this option, you will need to provide the alias of the certificate you wish to overwrite. In that case the new thumbprint should be passed in as the alias without any spaces between the octets (e.g. 81009c6e5465ecf343ba55ff9612122a5a4f6b33 not 81 00 9c 6e 54 65 ec f3 43 ba 55 ff 96 12 12 2a 5a 4f 6b 33).

IIS Personal

IIS Personal certificate stores require the addition of a private key and will only appear as an option when you select a certificate with a private key. With this type of store, you have the option to overwrite an existing certificate bound to an IIS web site with the current certificate. If you choose this option, you will need to provide the alias of the certificate you wish to overwrite. The alias is the thumbprint of the certificate bound to the IIS web site on the target. The thumbprint may be entered with or without spaces between each octet (e.g. 81 00 9c 6e 54 65 ec f3 43 ba 55 ff 96 12 12 2a 5a 4f 6b 33 or 81009c6e5465ecf343ba55ff9612122a5a4f6b33).

Tip: Choosing overwrite for a certificate **not** bound to an IIS web site will have no effect. No certificate will be overwritten.

IIS Revoked and Trusted Root

IIS Revoked and Trusted Root certificate store additions do not require the addition of a private key and will appear for both certificates with a private key and those without.

Tip: The overwrite functionality is not relevant for IIS Revoked and Trusted Root certificate stores and should be ignored.

Java Keystore

Java keystore certificate store additions do not require the addition of a private key and will appear for both certificates with a private key and those without. With this type of store, you will be prompted to add an alias for the certificate. This optional alias is stored in the keystore associated with the certificate. You have the option to overwrite an existing certificate with the current certificate. If you choose this option, you will need to provide the alias of the

certificate you wish to overwrite. Spaces *are* supported in the alias.

NetScaler

NetScaler certificate store additions do not require the addition of a private key and will appear for both certificates with a private key and those without. With this type of store, you will must add an **Alias** for the certificate. This serves as the file name used to store the file in the file system, so provide it with an appropriate extension (e.g. appserver17.crt or appserver17.pfx). Aliases should be entered without spaces. You must also enter the virtual server to associate the certificate with in the **NetscalerVserver** field. For a certificate with a private key, you are associating the certificate as a NetScaler Server Certificate. For a certificate without a private key, you are associating the certificate as a NetScaler CA Certificate and only CA certificates are supported for this purpose. You will receive an error if you attempt to associate a non-CA certificate without a private key with a virtual server. Entry of virtual server name is not case sensitive. You have the option to overwrite an existing certificate with the current certificate. If you choose this option, you will need to provide the alias (full file name with extension) of the certificate you wish to overwrite.

PEM File

PEM certificate store additions do not require the addition of a private key and will appear for both certificates with a private key and those without. With this type of store, you have the option to overwrite an existing certificate with the current certificate. If you choose this option, you will need to provide the alias of the certificate you wish to overwrite. The alias is the thumbprint of the certificate without any spaces between the octets (e.g. 81009c6e5465ecf343ba55ff9612122a5a4f6b33 not 81 00 9c 6e 54 65 ec f3 43 ba 55 ff 96 12 12 2a 5a 4f 6b 33).

Note: Keyfactor Command will automatically strip out any spaces between the octets in the alias field, so it does not matter whether you enter the thumbprint with or without spaces.

4. Click **Save** to submit the certificate store additions.

Delete

Select one or more certificates in the results grid and then click **Delete** at the top of the grid or **Delete** in the right-click menu to remove the selected certificate(s) from the Keyfactor Command database. If the selected certificates have associated private keys stored in the database, these private keys are also removed. The certificates will be returned to the Keyfactor Command database on the next full synchronization if synchronization for the certificate source (certificate authority, SSL endpoint, etc.) is still configured. Certificate history and private keys do not return when certificates re-synchronize.

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:

Certificates: *Read*
Certificates: *Delete*

Permissions for certificates can be set at either the global or certificate collection level. See *Certificate Permissions* in the *Keyfactor Command Reference Guide* for more information about global vs collection permissions.

Delete All

This option is available only in saved collections, not in standard certificate searches. Click the **Delete All** action button at the top of the collection grid. The button appears active only if no certificates are selected on the grid. A large deletion may take several minutes to complete. The certificates will be returned to the Keyfactor Command database on the next full synchronization if synchronization for the certificate source (certificate authority, SSL endpoint, etc.) is still configured.

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:
Certificates: *Read*
Certificates: *Delete*

Permissions for certificates can be set at either the global or certificate collection level. See *Certificate Permissions* in the *Keyfactor Command Reference Guide* for more information about global vs collection permissions.

Delete Private Key

Click the **Delete Private Key** in the right-click menu to remove the private key of the selected certificate(s) from the Keyfactor Command database. This option is only available if the private key is stored in the database.

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:
Certificates: *Read*
Certificates: *Delete*

Permissions for certificates can be set at either the global or certificate collection level. See *Certificate Permissions* in the *Keyfactor Command Reference Guide* for more information about global vs collection permissions.

Download

Click **Downland** in the right-click menu to download the selected certificate to the local computer with or without a private key. Only one certificate may be downloaded at a time.

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:
Certificates: *Read*
Certificates: *Download with Private Key*

The *Download with Private Key* permission is only needed for users who will be downloading certificates with private keys. To download a certificate without a private key, *Read* permission is sufficient.

Permissions for certificates can be set at either the global or certificate collection level. See *Certificate Permissions* in the *Keyfactor Command Reference Guide* for more information about global vs collection permissions.

Note: The Recover option that was found in previous versions of Keyfactor Command is now part of the Download option.

You will be able to download a certificate including its private key if one of the following is true:

- The certificate has been stored in the Keyfactor Command database with its private key.
- The certificate was issued using a template that had key archival enabled, issued from a Microsoft CA that has a valid Key Recovery Agent certificate, and that Key Recovery Agent certificate is configured on the Keyfactor Command server.

Important: In order to successfully download certificates and retrieve their associated private keys using Microsoft key recovery, the service account under which the Keyfactor Command application pool is running must be granted "Issue and Manage Certificates" permission to the CA database as per *Create Active Directory Groups to Control Access to Keyfactor Command Features* in the *Keyfactor Command Server Installation Guide*, or, if delegation is configured for the CA, the user executing the download must have these permissions.

In order to support key recovery within Keyfactor Command, you need to import at least one Key Recovery Agent certificate with a private key into the Keyfactor Command application pool user's personal certificate store on each Management Portal server. See Configuring Key Recovery for Keyfactor Command on page 745.

Tip: CA-level key recovery is supported for Microsoft CAs to allow recovery of private keys for certificates enrolled outside of Keyfactor Command. CA-level key archiving is not supported for enrollments done through Keyfactor Command. CA-level key recovery is not supported for EJBCA CAs. For enrollments done through Keyfactor Command for either Microsoft or EJBCA CAs, use Keyfactor Command private key retention (see Details Tab on page 360).

Note: Downloading of the private key is logged and reflected on the History tab of the certificate details (see History Tab on page 30).

To download a certificate that has the private key stored in the Keyfactor Command database:

1. Highlight the row in the results grid and right-click.
2. Choose **Download** from the right-click menu, or the action button on the Certificate Details dialog.

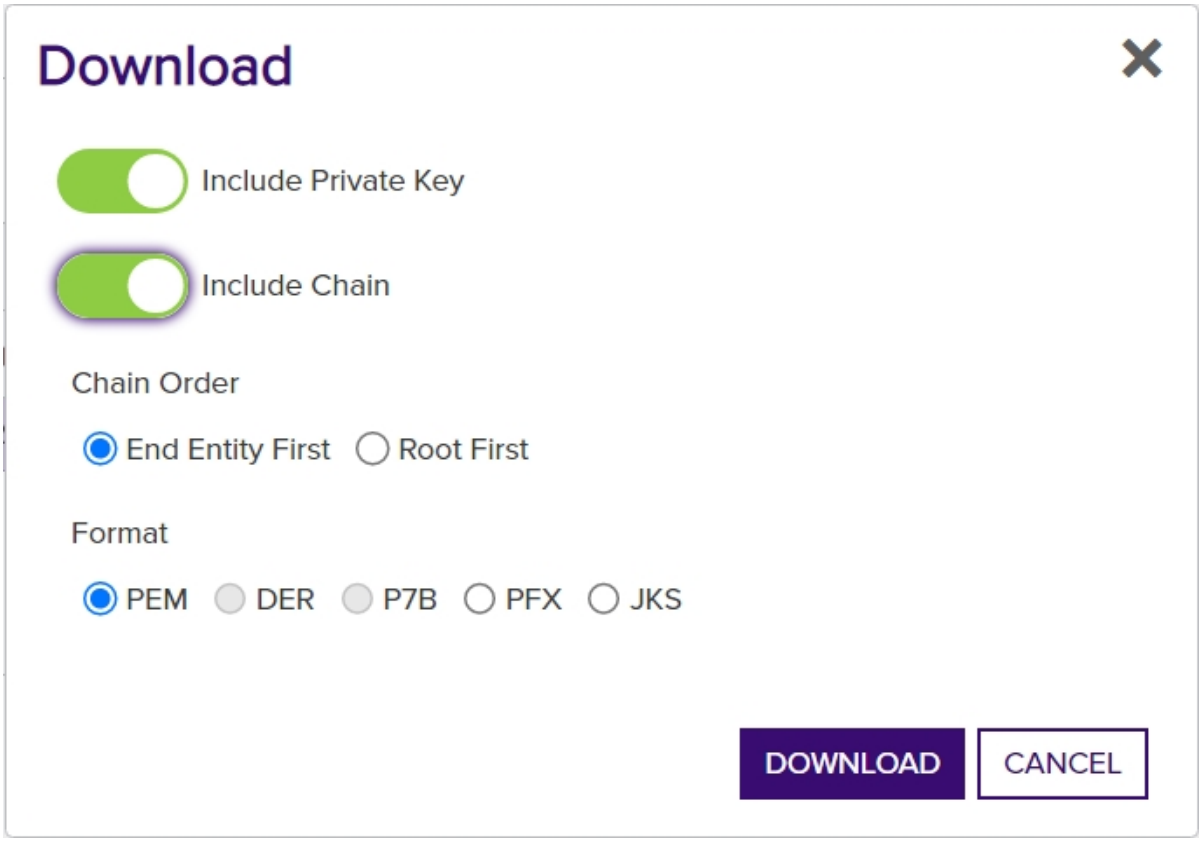


Figure 33: Certificate Operation: Download Certificate with Private Key

3. In the Download dialog, select the **Include Private Key** option to include the private key of the certificate in the download. The Include Private Key option is supported for PEM, PFX and JKS outputs.

Note: If you choose **Include Private Key**, *after* you click **Download** (step 7, below), a PFX/PEM/JKS Password dialog will pop-up with the one-time password and action buttons to **Copy Password** or **Close** the pop-up. Clicking **Copy Password** will copy the

password to the clipboard. As a security measure, the dialogue will close after 2 minutes. To secure the downloaded file, you will need this password in order to access the PFX, PEM, or JKS file generated by the download. Click **Close** to close the PFX/PEM/JKS Password dialog once you have copied the password.

Figure 34: Certificate Operation: Password for Certificate with Private Key

Important: The randomly generated password cannot be regenerated, so it must be copied prior to closing the dialog.

4. Select **Include Chain** to include the certificate chain (root and intermediate certificates) in the download, if required.
5. If you selected Include Chain, select a **Chain Order** for the certificates in the resulting output file—either **End Entity First** (at the beginning of the file) or **Root First**. Chain Order is supported for PEM and P7B outputs. PFX output always includes the end entity certificate first.
6. Chose an encoding format.

   Note: Selecting the *Include Private Key* and *Include Chain* options changes which formats are available.

7. Click **Download** to begin the download.

To download a certificate that does not have the private key stored in the Keyfactor Command database:

1. Highlight the row in the results grid and right-click.
2. Choose **Download** from the right-click menu.

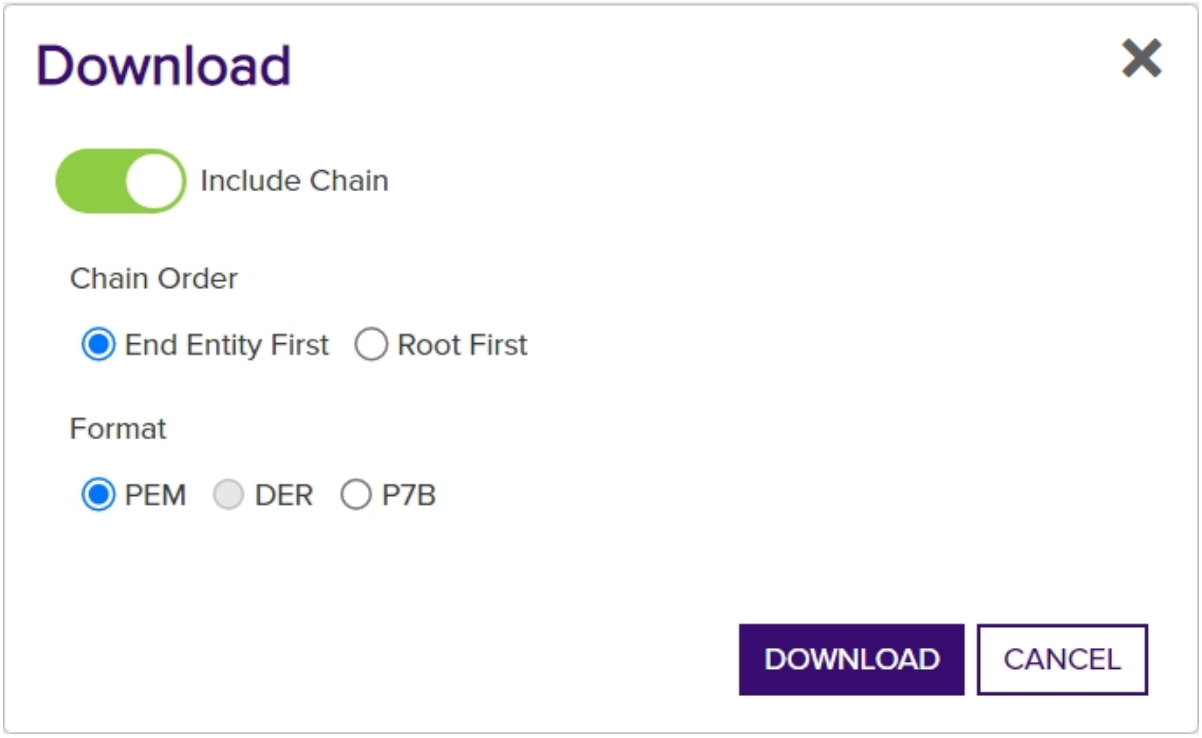


Figure 35: Certificate Operation: Download Certificate without Private Key

3. Chose **Include Chain** to include the certificate chain (root and intermediate certificates) in the download, if required. Include Chain is supported for PEM and P7B outputs.
4. If you selected Include Chain, select a **Chain Order** for the certificates in the resulting output file—either *End Entity First* (at the beginning of the file) or *Root First*. Chain Order is supported for PEM and P7B outputs.
5. Chose an encoding format.

   Note: Selecting the *Include Chain* option changes which formats are available.

6. Click **Download** to begin the download.

Edit (Display)

Select one certificate in the results grid and then click **Edit** at the top of the grid, or **Edit** in the right-click menu, or double-click the row, to pop up the certificate details dialog box in which you can view details of the certificate data and edit metadata fields for the certificate. Users without *Edit Metadata* permissions to certificates will see a **Display** option instead of an **Edit** option.

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:

Certificates: *Read*
Certificates: *Edit Metadata*
Certificate Store Management: *Read*

The *Edit Metadata* permission is only needed for users who will be modifying the values of metadata fields for certificates. Users with *Read* permissions may view the exiting metadata values.

The *Read* permission for *Certificate Store Management* is only needed for users who will be viewing values on the Locations tab.

Permissions for certificates and certificate stores can be set at either the global or certificate collection and certificate store container level. See *Certificate Permissions* and *Container Permissions* in the *Keyfactor Command Reference Guide* for more information about global vs collection and container permissions.

Note: When you open a certificate for editing, only the custom Keyfactor Command metadata fields are editable.

Note, the certificate details dialog also includes buttons for the **download**, **revoke**, and **renew** (if applicable) operations for users with appropriate permissions. You cannot change any of the certificate attributes from Certificate Authority (shown on the Content tab) or any of the certificate status, validation, locations, or history data tracked by Keyfactor Command (shown on the Status, Validation, Locations and History tabs).

See Certificate Details on page 19 for more detailed information about the certificate details dialog.

If you select multiple certificates to edit at once, only the metadata fields dialog will appear. See **Edit All**.

Edit All

Click **Edit All** at the top of the grid to open the metadata fields for all of the certificates in the query for editing. The button appears active only if no certificates are selected on the grid. All defined metadata fields—including those marked hidden—appear on the Edit All dialog. Each field includes an alert button that identifies whether the certificates in the query have all of same ( ) or different ( ) values for each metadata field. Click the alert button for an explanation of the impact the **Overwrite** settings for this field will have on the certificates.

See Metadata Tab on page 20 for more detailed information about the certificate details metadata.

Click **Allow Modifying** to enable the field for editing. Editing a field and selecting **Overwrite** will change the value for all certificates. Editing this field and not selecting **Overwrite** will only change the value for certificates that do not already have a value defined for this field.

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:

Certificates: *Read*
Certificates: *Edit Metadata*

Permissions for certificates can be set at either the global or certificate collection level. See *Certificate Permissions* in the *Keyfactor Command Reference Guide* for more information about global vs collection permissions.

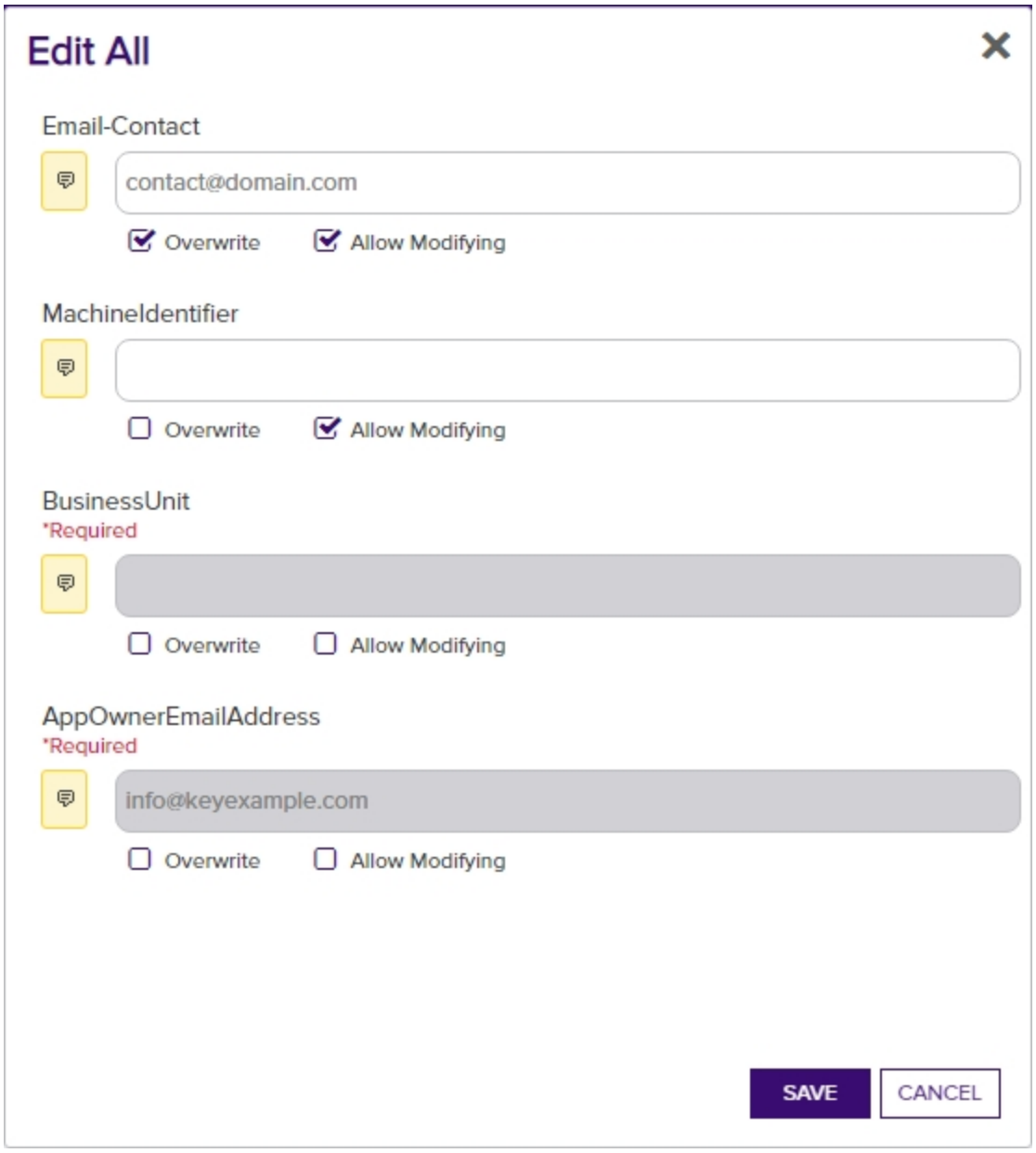


Figure 36: Certificate Operation: Edit All

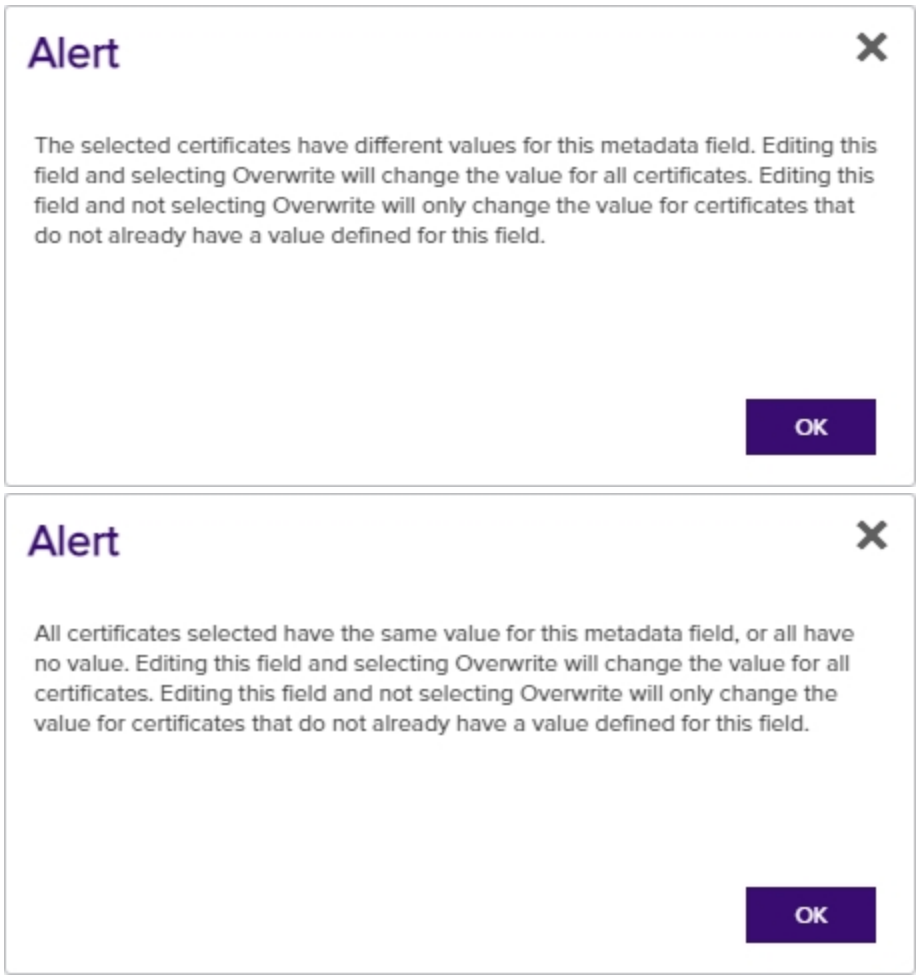


Figure 37: Certificate Operation: Edit All Alerts

Tip: The following setting will need to be configured to run 1+ million certificates in an *Edit All* request. In the IIS Management console, browse to *Default Web Site > Advanced Settings > Limits > Connection timeout*. Set this to a value higher than the default of 120, for example 360.

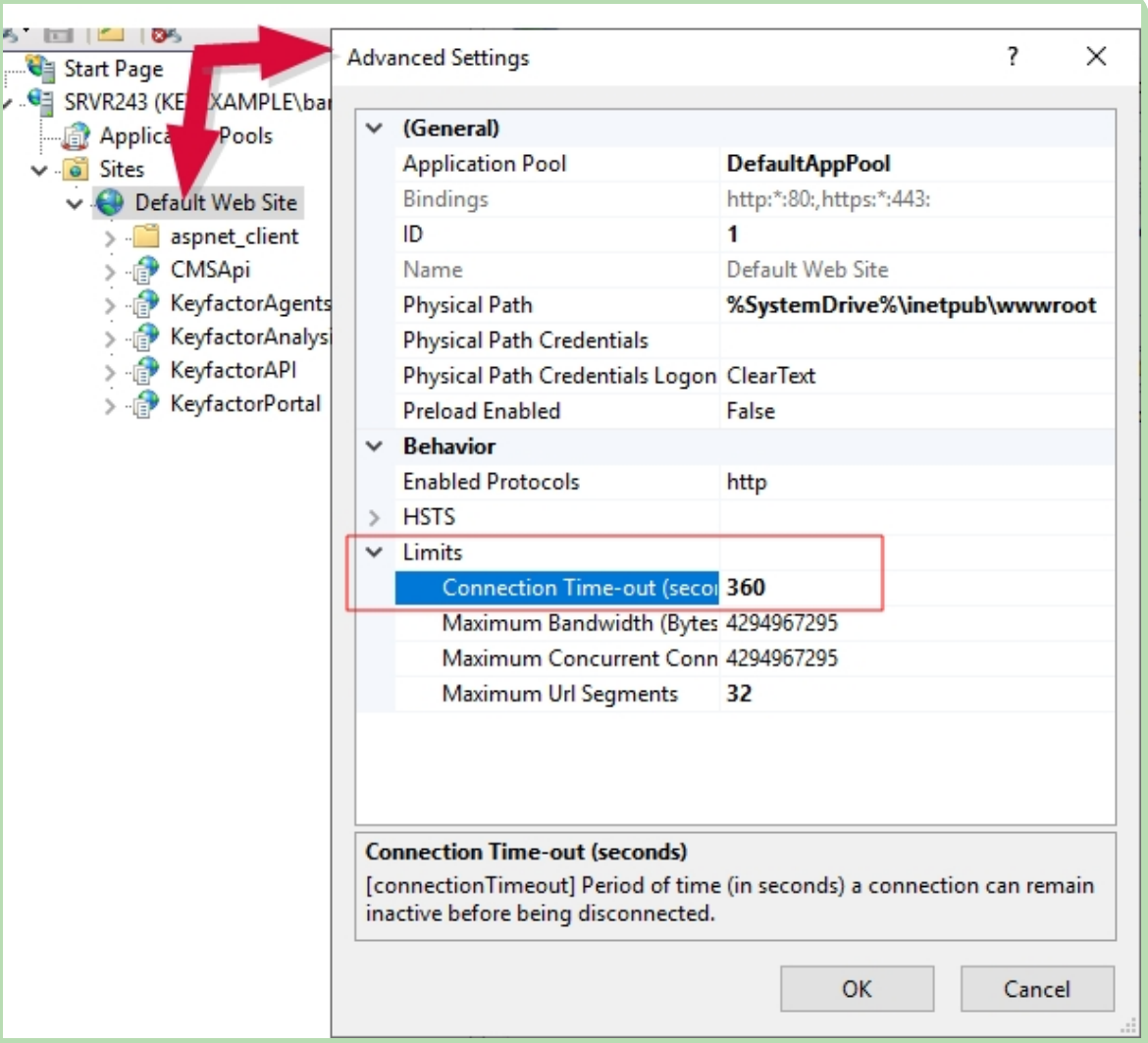


Figure 38: IIS Setting for 1+ Million Records - Certificate Operation: Edit All

Get CSV

Click **Get CSV** from the top of the grid to download all the certificates in the results grid to a comma-delimited CSV file. The button appears active only if no certificates are selected on the grid.

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:
Certificates: *Read*

Permissions for certificates can be set at either the global or certificate collection level. See *Certificate Permissions* in the *Keyfactor Command Reference Guide* for more information about global vs collection permissions.

The CSV file will contain the following information for each exported certificate:

- Issued DN
- Import Date
- Effective Date
- Expiration Date
- Issued CN
- Certificate Authority Name
- Template Display Name
- Principal
- Requester
- Key Type
- Key Size
- Certificate State
- Thumbprint

A confirmation dialog will pop up providing an approximate file size of the file that will be generated. A CSV file generated from a very large result set may take a long time to download or may be unwieldy to edit.

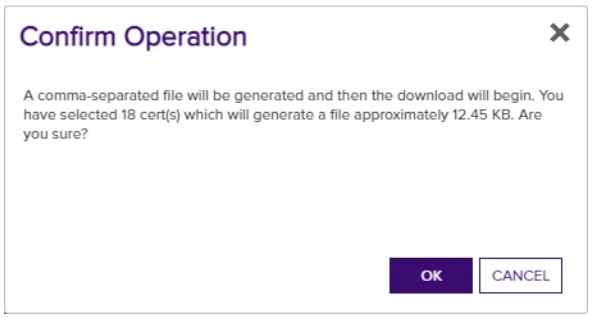


Figure 39: Certificate Operation: CSV Download

Identity Audit

Click **Identity Audit**in the right-click menu to view the certificate level permissions (read, edit metadata, download with private key, revoke, and delete) granted to all user roles defined in Keyfactor Command (see Security Roles and Identities on page 609) for the selected certificate.

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:
Auditing: *Read*
Certificates: *Read*
Security Settings: *Read*

Permissions for certificates can be set at either the global or certificate collection level. See *Certificate Permissions* in the *Keyfactor Command Reference Guide* for more information about global vs collection permissions.

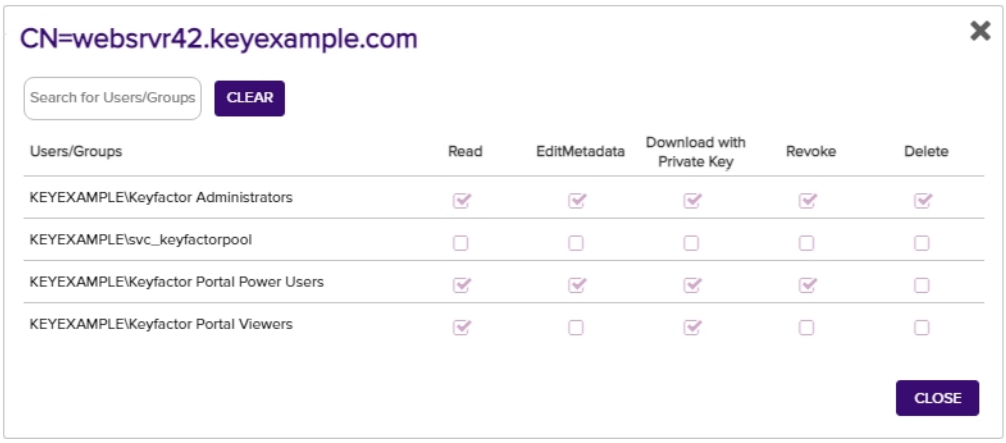


Figure 40: Certificate Operation: Identity Audit

Remove from Certificate Store

Click **Remove from Certificate Store** in the right-click menu to remove the selected certificate from a certificate store or stores. Two dialog boxes will pop up as per Add to Certificate Store on page 43 allowing you to select the certificate store(s) from which you wish to remove the certificate. In the first dialog, select the certificate store from which you want to remove the certificate and click the **Include and Close** button and then click **Save** in the second dialog. Only certificate stores that contain the certificate and to which the user has permissions will be shown.

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:
Certificates: *Read*
Certificate Store Management: *Read*
Certificate Store Management: *Schedule*

Permissions for certificates and certificate stores can be set at either the global or certificate collection and certificate store container level. See *Certificate Permissions* and *Container Permissions* in the *Keyfactor Command Reference Guide* for more information about global vs collection and container permissions.

Tip: The small *Remove* button at the top of the grid applies to managing the list in the grid only and will remove certificate stores from the selection of stores in the grid. Highlight a row and click *remove* to remove it from the list.

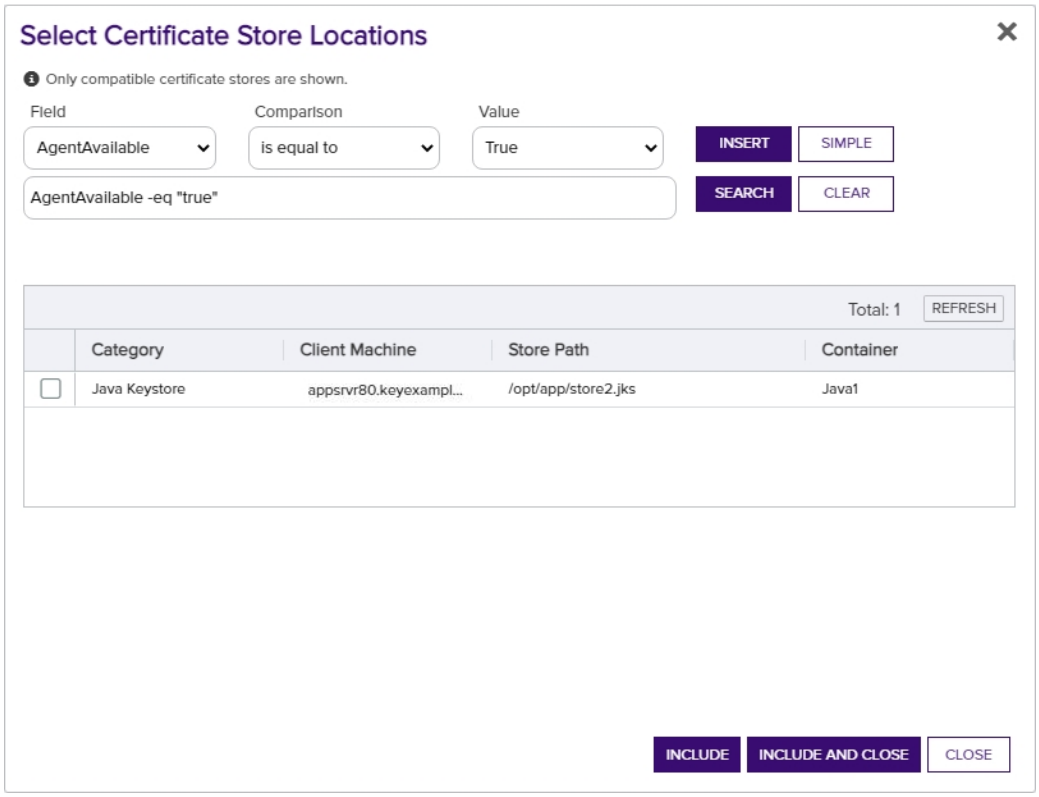


Figure 41: Certificate Operation: Select Stores for Remove from Certificate Store

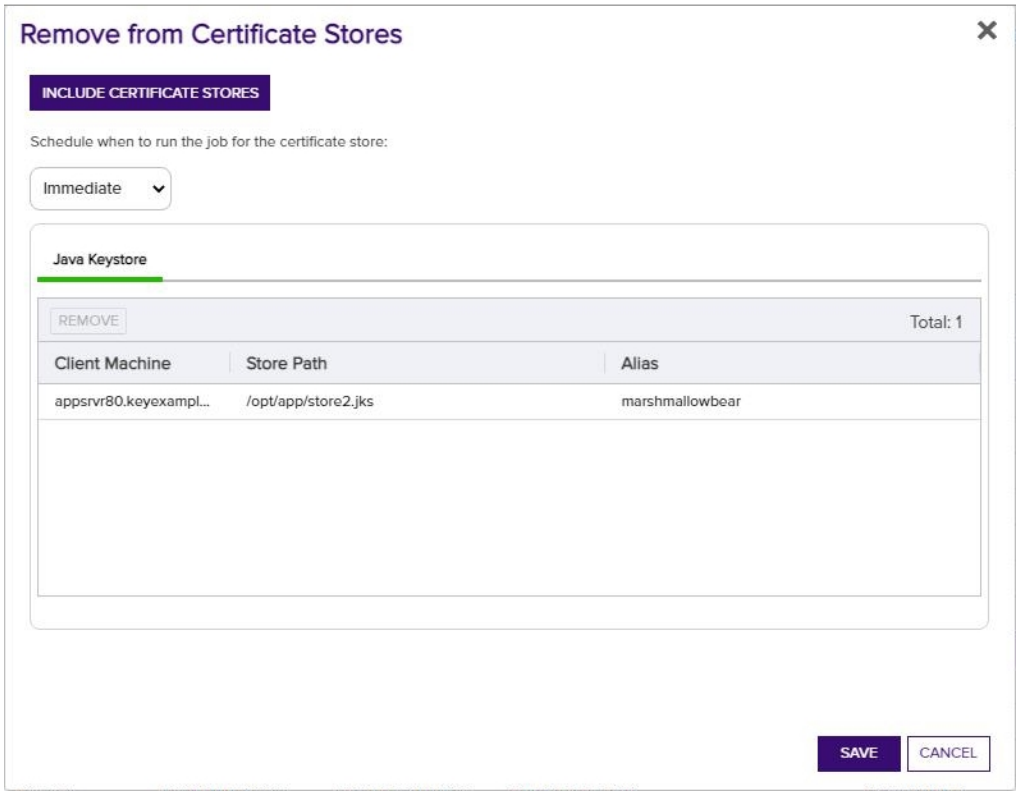


Figure 42:Remove from Cert Store Save Page

Renew

Click **Renew** in the right-click menu to renew or re-issue the selected certificate.

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:
Certificates: *Read*
Certificate Enrollment: *Enroll PFX*
Certificate Store Management: *Read*
Certificate Store Management: *Schedule*

Permissions for certificates and certificate stores can be set at either the global or certificate collection and certificate store container level. See *Certificate Permissions* and *Container Permissions* in the *Keyfactor Command Reference Guide* for more information about global vs collection and container permissions.

The renewal dialog includes the options of one-click renewal (the **Continue** option), which supports renewal with no further user interaction, or seeded PFX enrollment (the **Configure** option), to be redirected to the PFX Enrollment page with the information for the certificate pre-populated in the enrollment fields. The **Continue** option is only available if either one of the following is true:

- The certificate is located *together with its private key* in one or more managed certificate store (s).
- The certificate was enrolled with a template that has been configured in Keyfactor Command to allow private keys to be encrypted and stored in the Keyfactor Command database (see Certificate Template Operations on page 353).

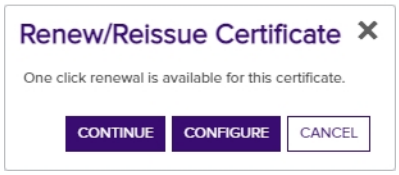


Figure 43: Certificate Operation: Renew/Reissue with the Continue Option

Note: The **Continue** option is only supported if the user performing the renewal has permissions to enroll using the template and CA associated with the original certificate.

From the seeded PFX Enrollment page, you can change the CA or template for enrollment, change the subject information or metadata for the certificate, set or remove SANs, or change the certificate store(s) to which the renewed certificate will be distributed. To change the certificate store(s) for distribution, on the PFX Enrollment page, scroll down to the Certificate Delivery Format section and click the **Include Certificate Stores** button. This will open the *Select Certificate Store Locations* dialog. For more information, see Add to Certificate Store on page 43 and PFX Enrollment on page 141.

Certificates issued by Microsoft CAs will be renewed (meaning the certificate will be issued with a different private key) regardless of how recently they were issued. Certificates issued by other certificate authorities will be renewed (typically retaining the same private key but with a new expiration date) if they are within the renewal window specified by the certificate template and re-issued (retaining the same expiration date) if they are not yet within the renewal window.

Note: As of Keyfactor Command version 10, enrollment (PFX and CSR), renewal, and revocation requests all flow through Keyfactor Command workflow. This will result in no changes to the enrollment, renewal, and revocation user experience unless customizations have been added in workflow (see Workflow Definitions on page 218).

Revoke

Select one or more certificates in the results grid and then click **Revoke** to revoke the selected certificate(s). When you select revoke, a dialog box pops up prompting for the effective revocation date, the reason for the revocation (for which there are dropdown choices), and comments (required). Upon completion of the revocation, the CRL for the CA in question is immediately republished to reflect the revocation. Unless you choose the revocation reason of *Certificate Hold*, there is no way to undo a revoke so care should be taken with this operation.

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:
Certificates: *Read*
Certificates: *Revoke*

Permissions for certificates can be set at either the global or certificate collection level. See *Certificate Permissions* in the *Keyfactor Command Reference Guide* for more information about global vs collection permissions.

Important: In order to successfully revoke certificates, the service account under which the Keyfactor Command application pool is running must be granted "Issue and Manage Certificates" and "Manage CA" permissions to the CA database as per *Create Active Directory Groups to Control Access to Keyfactor Command Features* in the *Keyfactor Command Server Installation Guide*, or, if delegation is configured for the CA, the user executing the revoke must have the "Issue and Manage Certificates" permissions while the application pool service account has the "Manage CA" permissions. If you are using explicit credentials to authenticate your CA (see Adding or Modifying a CA Record on page 330), it is the user specified on the CA configuration in Keyfactor Command who must have both these permissions on the CA.

Note: As of Keyfactor Command version 10, enrollment (PFX and CSR), renewal, and revocation requests all flow through Keyfactor Command workflow. This will result in no changes to the enrollment, renewal, and revocation user experience unless customizations have been added in workflow (see Workflow Definitions on page 218).

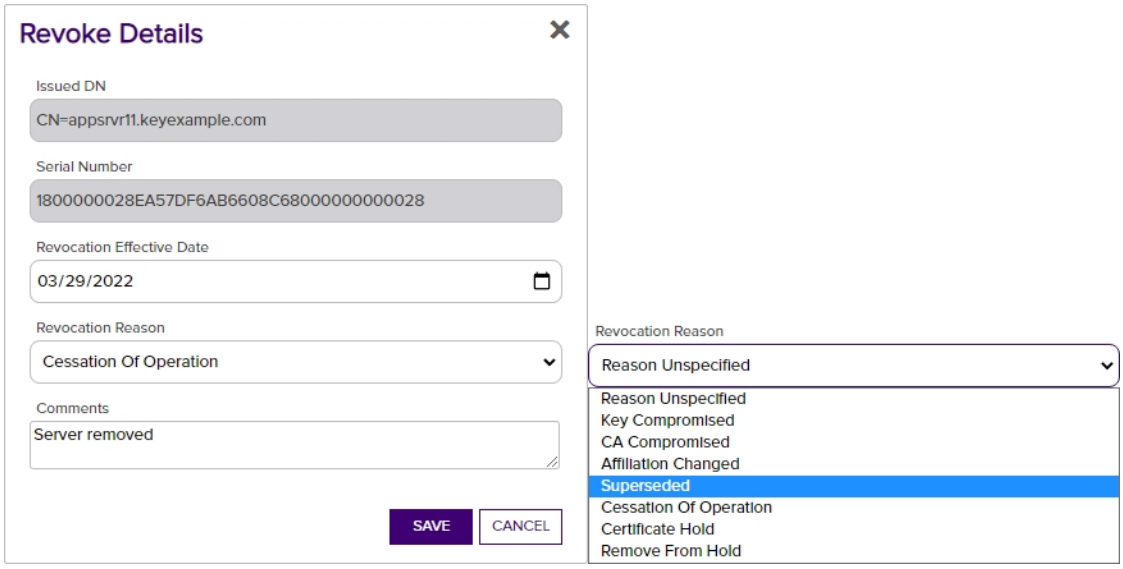


Figure 44: Certificate Operation: Revoke

Revoke: Certificate Hold / Remove from Hold

If you would like to suspend one or more certificates without permanently revoking them, select one or more certificates in the results grid and then click **Revoke** at the top of the grid or **Revoke** on the right-click menu. Select **Certificate Hold** as the revocation reason. You will be required to add a comment in the *Comments* field to **Save** the record change.

When you **Revoke** a certificate using the revocation reason of **Certificate Hold**, the certificate is in the revoked state, with the revocation reason of **Certificate Hold**. You will only be able to see the certificate on a certificate search with *Include Revoked* checked. To return the certificate to the Active state, **Revoke** it again with the reason **Remove from Hold**. You will be required to add a comment in the *Comments* field to **Save** the record change.

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:
Certificates: *Read*
Certificates: *Revoke*

Permissions for certificates can be set at either the global or certificate collection level. See *Certificate Permissions* in the *Keyfactor Command Reference Guide* for more information about global vs collection permissions.

Note: As of Keyfactor Command version 10, enrollment (PFX and CSR), renewal, and revocation requests all flow through Keyfactor Command workflow. This will result in no changes to the enrollment, renewal, and revocation user experience unless customizations have been added in workflow (see Workflow Definitions on page 218).

Revoke All

If you would like to revoke ALL the certificates in the current query results set, click **Revoke All** at the top of the grid. The button appears active only if no certificates are selected on the grid.

When you select revoke all, a dialog box pops up prompting for the effective revocation date, the reason for the revocation (for which there are dropdown choices), comments (required), and confirmation of the number of certificates being revoked. In the confirmation field, you must type the suggested message, which includes the number of certificates being revoked, exactly as indicated, including case (e.g. “REVOKE 52” not “revoke 52”).

If any certificates fail revocation, their certificate IDs will be listed in a dialog at the completion of the revocations.

Upon completion of the revocations, the CRL(s) for the CA(s) in question is immediately republished to reflect the revocations. Unless you choose the revocation reason of *Certificate Hold*, there is no way to undo a revoke so care should be taken with this operation.

A maximum of 1000 certificates can be revoked at once with this option. If the query contains more certificates than this, a warning dialog will appear and you will not be allowed to continue with the revocation.

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:
Certificates: *Read*
Certificates: *Revoke*

Permissions for certificates can be set at either the global or certificate collection level. See *Certificate Permissions* in the *Keyfactor Command Reference Guide* for more information about global vs collection permissions.

Note: As of Keyfactor Command version 10, enrollment (PFX and CSR), renewal, and revocation requests all flow through Keyfactor Command workflow. This will result in no changes to the enrollment, renewal, and revocation user experience unless customizations have been added in workflow (see Workflow Definitions on page 218).

Note: The Revoke All option can be removed from display on the certificate search pages using the *Revoke All Enabled* application setting (see Application Settings: Console Tab on page 584).

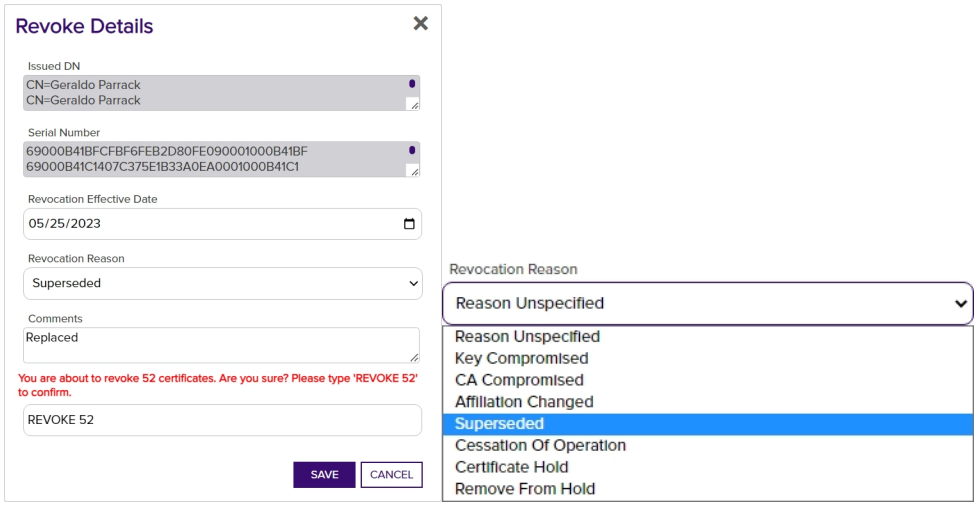


Figure 45: Certificate Operation: Revoke All

2.1.3.4 Add Certificate

The add certificate tool supports importing certificates with the following formats and extensions:

- PEM: .cer or.crt

  If your PEM file has an extension of .pem, rename it to .cer or .crt before using the Add Certificate tool.

- PKCS#12: .pfx or .p12
- PKCS#7: .p7b

This tool has several purposes, including:

- It can be used to import certificates generated outside the enterprise PKI environment—such as those purchased from a commercial certificate vendor or generated by a non-Microsoft or non-EJBCA CA.
- It can be used to import certificates that would not be automatically imported during a synchronization of configured Microsoft or EJBCA CAs such as root CA certificates or certificates with unusual key types (e.g. Dilithium) that aren't supported by synchronization.
- It can be used to import certificates acquired using CSRs generated by Keyfactor Command and issued by a CA not managed using Keyfactor Command to allow for ongoing management with Keyfactor Command.
- It can be used to push a certificate with the associated private key out to a certificate store when you have the appropriate .pfx or .p12 file available.
- It can be used as a quick shortcut to push a certificate without a private key out to a certificate store when you have the certificate file in hand and don't want to search for the certificate in Keyfactor Command in order to push it out to the certificate store.

  Before you can add a certificate to a certificate store with this option, you must first add the certificate store in Keyfactor Command (see Certificate Stores on page 380) and install, start, and approve the orchestrator (see Orchestrator Management on page 481 and the *Keyfactor Orchestrators Installation and Configuration Guide*.

If you import a certificate that has either already been imported via a synchronization task or has been manually imported previously, the certificate will not be re-imported. You will receive a notification message, when you save it, if the certificate already exists in the Keyfactor Command database. Any metadata currently stored in the database for that certificate will be displayed in the metadata fields on the page (for .cer and .crt format certificates), and any changes you make to the metadata on this page will overwrite the existing metadata for the certificate when you complete the import (for all certificate formats).

To use the add certificate tool

1. In the Management Portal, browse to *Certificates > Add Certificate.*
2. In the *Add Certificate* section of the page, click the **Upload** button to open a browse window.
3. In the browse window, browse to select the certificate you wish to import.
4. For a .pfx or .p12 file, when prompted enter the password for the file and **Save**. This will open the Add Certificate page, which will allow you to change/add metadata and choose certificate locations to deploy the certificate to. **Set PFX Password** allows you to reenter the password once you have uploaded the certificate.

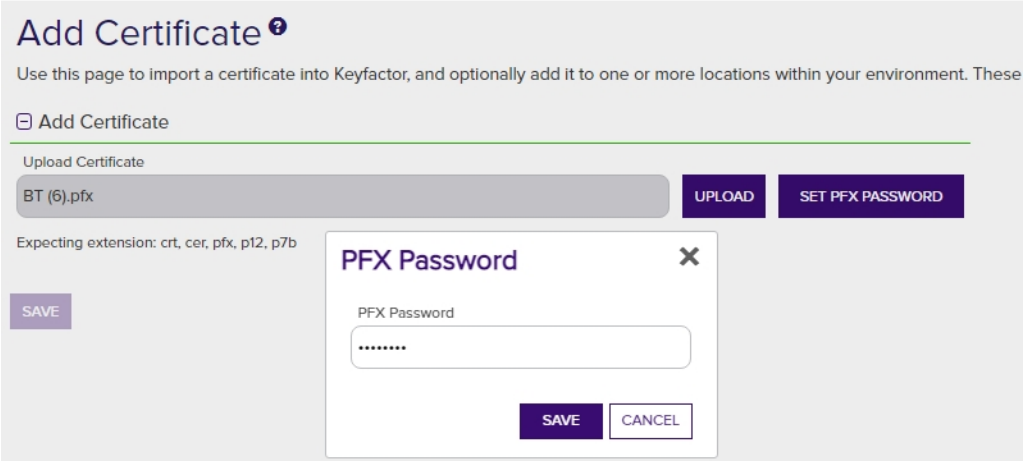


Figure 46: Add Certificate Password for PFX/p12

5. In the *Certificate/PFX Details* section of the page, review the certificate information.

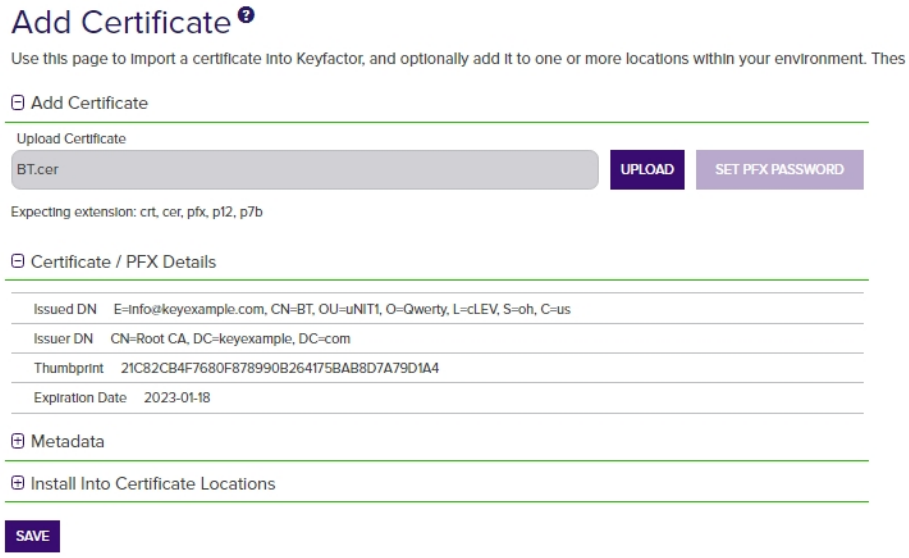


Figure 47: Add Certificate Information

6. In the *Metadata* section of the page, populate the metadata fields as appropriate for the certificate. Metadata fields that have been designated as required on a system-wide or template-level basis will be marked with *Required.

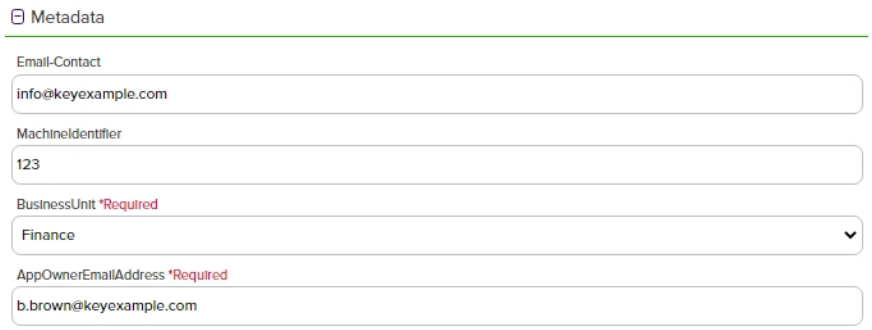


Figure 48: Add Certificate Metadata

7. In the *Install into Certificate Locations* section of the page, select each certificate store location to which you want to distribute the certificate, if desired. To do this, click the **Include Certificate Stores** button. This will cause the *Select Certificate Store Locations* dialog to appear. Make your certificate store selections in this dialog as described in *Select Certificate Store Locations*, below, and click **Include and Close**. You will then see some additional fields on the page. Populate these as per *Add to Certificate Stores* and *Information Required for Certificate Stores*, below.

Select Certificate Store Locations

The *Select Certificate Store Locations* dialog allows you to run queries against your certificate store list to select which store(s) to deploy a selected certificate to. **Check** the box next to each certificate store location to which you want to distribute the certificate.

Note: Only compatible certificate stores and only stores in containers to which you have permissions are shown on the grid.

Tip: You may change the search results by using the search fields at the top of the dialog. All of the Keyfactor Command grid search features are available to assist your search. See Using the Certificate Store Search Feature on page 382 for more information on the available search fields. The default search criteria is *AgentAvailable is equal to True*.

The actions on the *Select Certificate Store Locations* dialog are:

- **Include**

  Click this to add the selected certificate store(s) to your certificate selection and leave the search dialog open for further searches.

- **Include and Close**

Click this to close the search dialog and add the selected certificate store(s) to your certificate selection, which will then be displayed and ready for updates as per the instructions in *Add to Certificate Stores*.

- **Close**

  Click this to cancel the operation and return to the main page with no certificate stores selected.

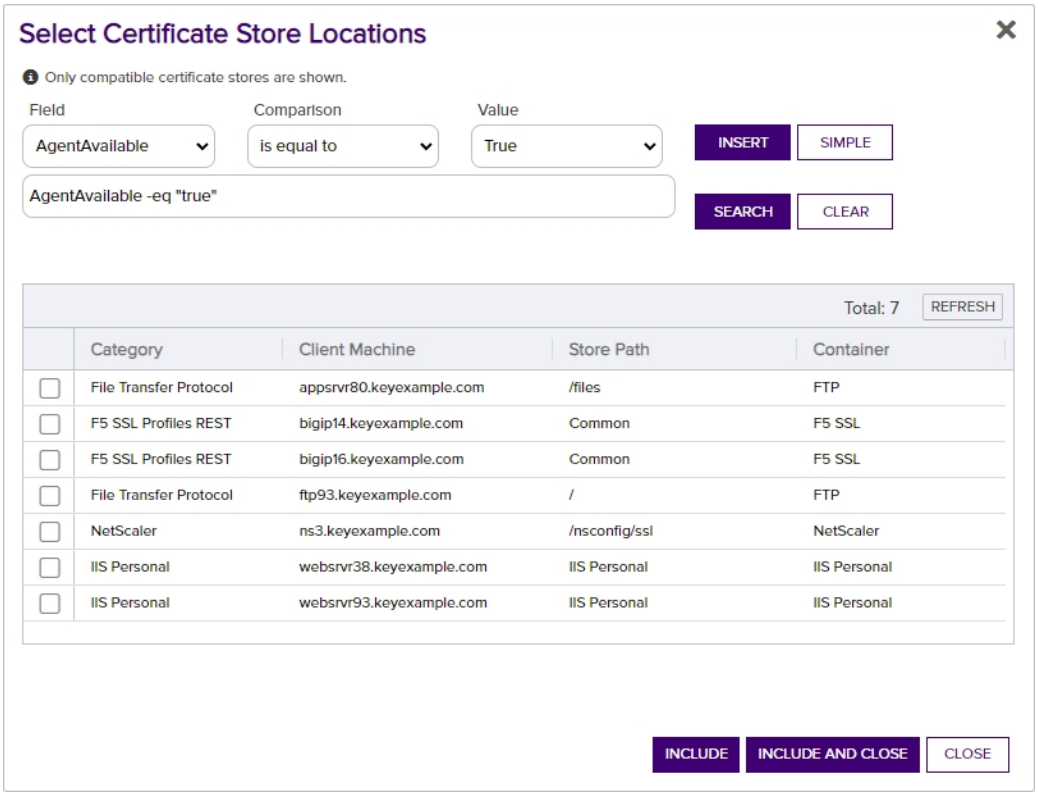


Figure 49: Select Certificate Store Locations Dialog

Add to Certificate Stores

The *Add to Certificate Stores* page appears once you select at least one certificate store to distribute your certificate to. It includes a grid section with a series of tabs that display a tab for each type of certificate store selected with a list of the selected stores under each tab. The header section of the dialog shows global options that apply to the add job as a whole:

- **Include Certificate Stores**

  You may return to the *Select Certificate Store Locations* dialog by clicking **Include Certificate Stores** above the grid. The current selections will be retained.

- **Schedule when to run the job for the certificate store**

In the **Schedule** dropdown, select a time at which the job to add the certificate to the stores should run. The choices are *Immediate* or *Exactly Once* at a specified date and time. If you choose *Exactly Once*, enter the date and time for the job. A job scheduled for *Immediate* running will run within a few minutes of saving the operation. The default is *Immediate*.

Click **Remove** at the top of the grid to remove the selected certificate store from the page. The certificate will not be added to the store.

For each selected certificate store you can apply the following actions:

- **Overwrite**

  Check **Overwrite** below the grid to overwrite any existing certificate in the same location and with the same name or alias for the selected certificate store type.

- **Alias**

  Add an **Alias** below the grid, if applicable, for the certificate store type. See the **Information Required by Certificate Store** section, below, for more information.

  Note: The tab heading of the certificate location will display an alert if an alias is required for the location. If this is set to **Forbidden** on the certificate store type, the **Alias** field will not display unless "Overwrite" is checked on this page.

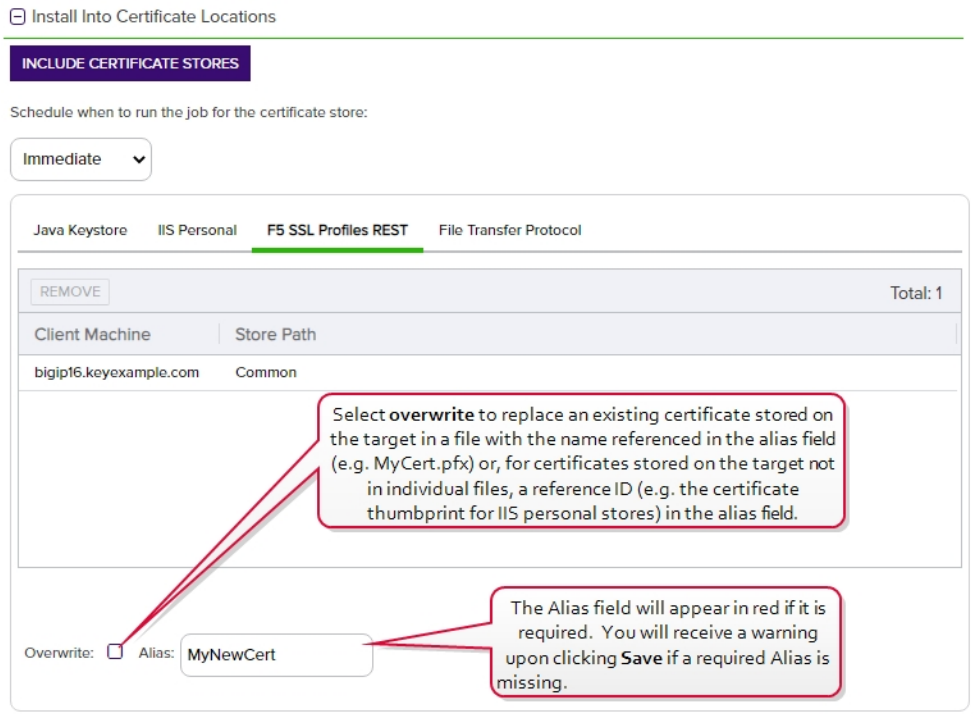


Figure 50: Add Certificate—Install into Certificate Locations

Figure 51: Alias Required Alert on Save

Information Required by Certificate Stores

Each type of certificate store has different requirements for providing an alias or other additional information. Table 4: Alias Requirements by Certificate Store Type provides a quick breakdown by certificate store of whether a certificate alias is required for new certificate additions or only for overwriting an existing certificate in the store.

Tip: When adding a certificate to a certificate store, you have the option to overwrite an existing certificate with the current certificate. If you choose this option, you will need to provide the alias of the certificate you wish to overwrite. Find the alias values by navigating to *Management Portal > Certificates > Certificate Search*. Select the certificate you wish to overwrite and double-click, or click **Edit**, from the grid header or right-click menu. Choose the **Locations** tab and double-click on the Location Type (this must have a number other than zero in the *Count* column) to open the details dialog. The *Alias* field holds the information that may be required for an overwrite.

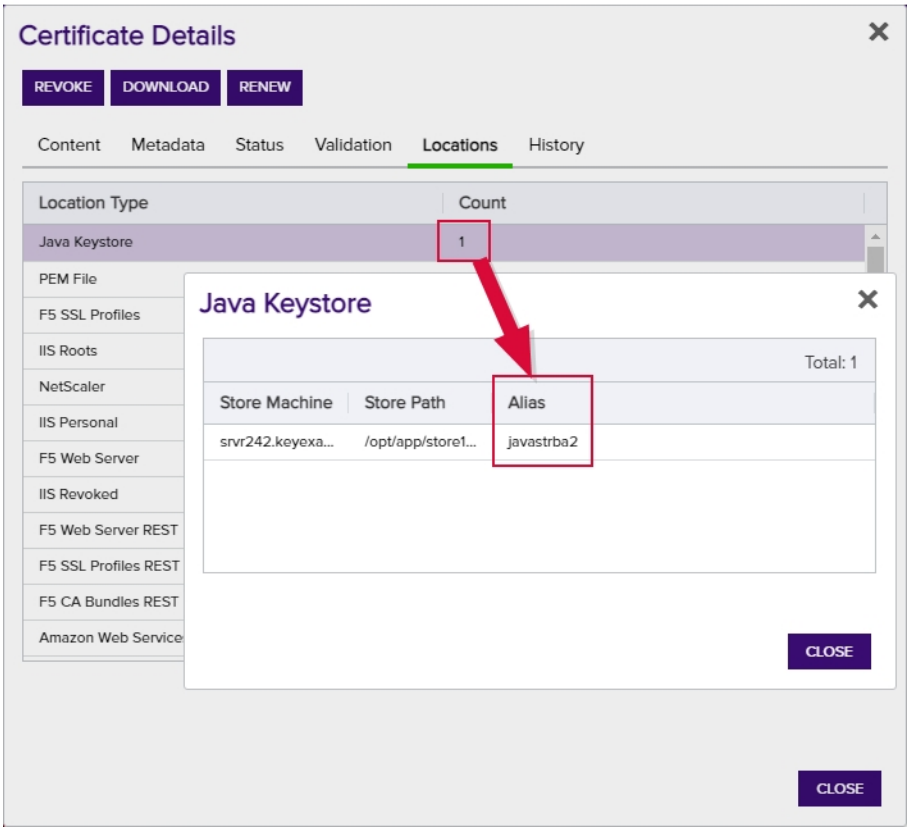


Figure 52: Example: Certificate Location Details for a JKS Location

Table 4: Alias Requirements by Certificate Store Type

Certificate Store Type	Alias Functionality
Amazon Web Services	Alias only required for overwrites
F5 CA Bundles REST	Alias required for new additions and overwrites
F5 SSL Profiles	Alias required for new additions and overwrites
F5 SSL Profiles REST	Alias required for new additions and overwrites
F5 Web Server	Alias only required for overwrites

Certificate Store Type	Alias Functionality
F5 Web Server REST	Alias only required for overwrites
File Transfer Protocol	Alias required for new additions and overwrites
IIS Personal	Alias only required for overwrites
IIS Revoked	Alias not needed
IIS Trusted Roots	Alias not needed
Java Keystore	Alias required for new additions and overwrites
NetScaler	Alias required for new additions and overwrites
PEM File	Alias only required for overwrites

Amazon Web Services (AWS)

Amazon Web Services (AWS) certificate stores require the addition of a private key and will only appear as an option when you select a certificate with a private key. With this type of store, you have the option to overwrite an existing certificate with the current certificate. If you choose this option, you will need to provide the alias of the certificate you wish to overwrite. The alias is the internal ID assigned by Amazon (the Amazon resource number or ARN). Provide the entire contents of the *Alias/IP* from this field when entering an alias for overwrite. For example:

arn:aws:acm:us-west-2:220531701668:certificate/88e5dcfb-a70b-4636-a8ab-e85e8ad88780

F5 CA Bundles REST

F5 CA Bundle REST certificate store additions do not require the addition of a private key and will appear for both certificates with a private key and those without. With this type of store, you will be prompted to add an alias for the certificate. The alias is the file name used to store the file in the device file system, minus the extension (e.g. use alias MyFile for a file named MyFile.crt). Aliases should be entered without spaces. Note that certificate names are case sensitive. You have the option to overwrite an existing certificate with the current certificate. If you choose this option, you will need to provide the alias of the certificate you wish to overwrite.

F5 SSL Profile

F5 SSL Profile certificate store additions do not require the addition of a private key and will appear for both certificates with a private key and those without. With this type of store, you will be prompted to add an alias for the certificate. The alias is the file name used to store the file in the device file system, minus the extension (e.g. use alias MyFile for a file named MyFile.pfx). Aliases should be entered without spaces. Note that certificate names are case sensitive. You have the option to overwrite an existing certificate with the current certificate. If you choose this option, you will need to provide the alias of the certificate you wish to overwrite.

F5 SSL Profile REST

F5 SSL Profile REST certificate store additions do not require the addition of a private key and will appear for both certificates with a private key and those without. With this type of store, you will be prompted to add an alias for the certificate. The alias is the file name used to store the file in the device file system, minus the extension (e.g. use alias MyFile for a file named MyFile.pfx). Aliases should be entered without spaces. Note that certificate names are case sensitive. You have the option to overwrite an existing certificate with the current certificate. If you choose this option, you will need to provide the alias of the certificate you wish to overwrite.

F5 Web Server

F5 Web Server certificate stores require the addition of a private key and will only appear as an option when you select a certificate with a private key. With this type of store, you have the option to overwrite an existing certificate with the current certificate. If you choose this option, you will need to provide the alias of the certificate you wish to overwrite. The alias for F5 device certificates is typically *server*.

F5 Web Server REST

F5 Web Server REST certificate stores require the addition of a private key and will only appear as an option when you select a certificate with a private key. With this type of store, you have the option to overwrite an existing certificate with the current certificate. If you choose this option, you will need to provide the alias of the certificate you wish to overwrite. The alias for F5 device certificates is typically *server*.

File Transfer Protocol (FTP)

File Transfer Protocol (FTP) certificate store additions do not require the addition of a private key and will appear for both certificates with a private key and those without. With this type of store, you have the option to overwrite an existing certificate with the current certificate. If you choose this option, you will need to provide the alias of the certificate you wish to overwrite. In that case the new thumbprint should be passed in as the alias without any spaces

between the octets (e.g. 81009c6e5465ecf343ba55ff9612122a5a4f6b33 not 81 00 9c 6e 54 65 ec f3 43 ba 55 ff 96 12 12 2a 5a 4f 6b 33).

IIS Personal

IIS Personal certificate stores require the addition of a private key and will only appear as an option when you select a certificate with a private key. With this type of store, you have the option to overwrite an existing certificate bound to an IIS web site with the current certificate. If you choose this option, you will need to provide the alias of the certificate you wish to overwrite. The alias is the thumbprint of the certificate bound to the IIS web site on the target. The thumbprint may be entered with or without spaces between each octet (e.g. 81 00 9c 6e 54 65 ec f3 43 ba 55 ff 96 12 12 2a 5a 4f 6b 33 or 81009c6e5465ecf343ba55ff9612122a5a4f6b33).

Tip: Choosing overwrite for a certificate **not** bound to an IIS web site will have no effect. No certificate will be overwritten.

IIS Revoked and Trusted Root

IIS Revoked and Trusted Root certificate store additions do not require the addition of a private key and will appear for both certificates with a private key and those without.

Tip: The overwrite functionality is not relevant for IIS Revoked and Trusted Root certificate stores and should be ignored.

Java Keystore

Java keystore certificate store additions do not require the addition of a private key and will appear for both certificates with a private key and those without. With this type of store, you will be prompted to add an alias for the certificate. This optional alias is stored in the keystore associated with the certificate. You have the option to overwrite an existing certificate with the current certificate. If you choose this option, you will need to provide the alias of the certificate you wish to overwrite. Spaces *are* supported in the alias.

NetScaler

NetScaler certificate store additions do not require the addition of a private key and will appear for both certificates with a private key and those without. With this type of store, you will must add an **Alias** for the certificate. This serves as the file name used to store the file in the file system, so provide it with an appropriate extension (e.g. appserver17.crt or appserver17.pfx). Aliases should be entered without spaces. You must also enter the virtual server to associate the certificate with in the **NetscalerVserver** field. For a certificate with a private key, you are associating the certificate as a NetScaler Server Certificate. For a certificate without a private key, you are associating the certificate as a NetScaler CA Certificate and

only CA certificates are supported for this purpose. You will receive an error if you attempt to associate a non-CA certificate without a private key with a virtual server. Entry of virtual server name is not case sensitive. You have the option to overwrite an existing certificate with the current certificate. If you choose this option, you will need to provide the alias (full file name with extension) of the certificate you wish to overwrite.

PEM File

PEM certificate store additions do not require the addition of a private key and will appear for both certificates with a private key and those without. When you check the box for a PEM store, a new PFX Password section will appear on the page. The password you enter here is used to encrypt the private key of the certificate when stored in the PEM file or separate password file. If you choose to uncheck the *Use Custom Password* box, the private key will be encrypted with a random password *which is not accessible to you*. For most use cases, you will need a known password for this purpose, so leave the *Use Custom Password* box checked and make note of the password you use for this purpose. With this type of store, you have the option to overwrite an existing certificate with the current certificate. If you choose this option, you will need to provide the alias of the certificate you wish to overwrite. The alias is the thumbprint of the certificate without any spaces between the octets (e.g. 81009c6e5465ecf343ba55ff9612122a5a4f6b33 not 81 00 9c 6e 54 65 ec f3 43 ba 55 ff 96 12 12 2a 5a 4f 6b 33).

Note: Keyfactor Command will automatically strip out any spaces between the octets in the alias field, so it does not matter whether you enter the thumbprint with or without spaces.

8. Click **Save** to import the certificate to Keyfactor Command

Note: When you import a certificate containing a private key (a .pfx or .p12 file), the private key for that certificate is stored in the Keyfactor Command database. Users with limited permissions to the Add Certificate function may have permissions to upload certificates but not store private keys. If a user with this permission model uploads a certificate containing a private key, the certificate itself will be imported (if it does not already exist in the database), but the private key will not be stored. The user will receive a message indicating this. For more information about setting permissions for importing certificates, see Security Roles and Identities on page 609.

Tip: Click the help icon (?) next to the page title to open the embedded web copy of the *Keyfactor Command Documentation Suite* to this section.
You can also find the help icon at the top of the page next to the **Log Out** button. From here you can choose to open either the *Keyfactor Command Documentation Suite* at the home page or the *Keyfactor API Endpoint Utility*.

2.1.3.5 Certificate Collection Manager

The Certificate Collection Manager is used to:

- View a list of certificate collections.
- Change whether or not the collections show in Navigator (the top menu, where they appear under *Certificates*).
- View whether or not the collections show in the dashboard widget (see Dashboard: Collections on page 12).
- Delete a certificate collection.
- Search for specific certificate collections from the list (see Using the Collection Manager Search Feature on page 84).
- View all the certificates in a collection.

  Highlight the collection from the Certificate Collection Manager grid and click the **View** action button. This will open a new window with the name of the collection in a certificate search grid (see Viewing an Existing Certificate Collection on page 83).

To open the Certificate Collection Management grid, browse to *Certificates > Collection Manager* in the Management Portal. The Certificate Collection Management page includes the following collection action buttons from the grid header:

- Set **Show in Navigator** on the collection to determine whether or not the collection appears in Navigator (the top menu under Certificates). To change this setting, highlight the row in the collection management grid and click **Show in Navigator** at the top of the grid, or right-click the collection in the grid and choose **Show in Navigator** from the right-click menu. This will toggle the Yes/No in the **Show in Navigator** grid column.
- To delete a collection, highlight the row (or rows) in the collection management grid and click **Delete** at the top of the grid or right-click the collection in the grid and choose **Delete** from the right-click menu.
- Highlight a row in the collection management grid and click **View** at the top of the grid, or right-click the collection in the grid and choose **View** from the right-click menu to be taken to the list of certificates in that collection. Choosing this option will open the certificate search page in a new window filtered with the specific collection.

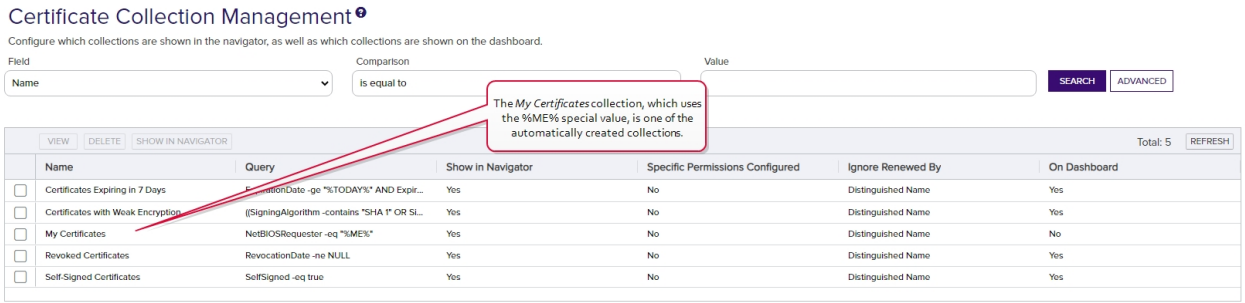


Figure 53: Certificate Collection Manager

Keyfactor Command Auto-Created Collections

Several collections are created automatically when Keyfactor Command is installed:

- Certificates Expiring in 7 Days
  This collection uses the special %TODAY% value in place of the current date to create a collection that can be used on any day to find the certificates that will expire within the next week. Only active certificates are included in this collection. The query for this collection is:

  ```
  ExpirationDate -ge "%TODAY%" AND ExpirationDate -le "%TODAY+7%" AND CertState -eq "1"
  ```

- Certificates with Weak Encryption
  This collection uses a variety of key type, key size, and signing algorithm queries to produce a collection that returns active certificates that have weak encryption. The query for this collection is:

  ```
  ((SigningAlgorithm -contains "SHA 1" OR SigningAlgorithm -contains "SHA1" OR SigningAlgorithm -contains "SHA-1") OR (SigningAlgorithm -contains "MD") OR (KeyType -eq 3 AND KeySize -lt 224) OR (KeyType -eq 1 AND KeySize -lt 2048)) AND CertState -eq "1"
  ```

- My Certificates
  This collection uses the special %ME% value in place of a specific user name to create a collection that any user can use to find the certificates on which they were the requester. The query for this collection is:

  ```
  NetBIOSRequester -eq "%ME%"
  ```

  Note: Certificate collections saved using the %ME% value are *not* supported for use in reports or on the dashboard.

- Revoked Certificates
  This collection returns revoked certificates by querying for certificates that have a non-null revocation date. The *Include Revoked* box is automatically checked for this collection when run. The query for this collection is:

  ```
  RevocationDate -ne NULL
  ```

- Self-Signed Certificates
  This collection returns all certificates that are self-signed. In environments with no certificates imported from external sources (e.g. SSL scanning), this would typically just be CA certificates. The query for this collection is:

  ```
  SelfSigned -eq true
  ```

Important: The special query options of %TODAY%, %ME%, and %ME-AN% are only supported in uppercase. Lowercase equivalents (e.g. %me%) cannot be substituted.

Important: All automatically created collections are included on the menu by default, and all are included in the Certificate Collections Management grid by default. They are created for

fresh installations of Keyfactor Command only, not upgrades, so as not to overwrite any user-defined collection for existing installations.

Tip: Click the help icon (?) next to the page title to open the embedded web copy of the *Keyfactor Command Documentation Suite* to this section.
You can also find the help icon at the top of the page next to the **Log Out** button. From here you can choose to open either the *Keyfactor Command Documentation Suite* at the home page or the *Keyfactor API Endpoint Utility*.

Viewing an Existing Certificate Collection

To view an existing certificate collection, either browse to the *Certificates* dropdown on the Management Portal menu and select the desired collection from the dropdown (if the collection has *Show in Navigator* set as **Yes**), or browse to *Certificates > Collection Manager* from the Management Portal and then select **View**, or double-click the row, from the Certificate Collection Management grid. When you select the collection for viewing, the search will begin immediately and the certificate search grid will open with the results from the collection. For information on using the certificate search grid, see Certificate Search Page on page 32.

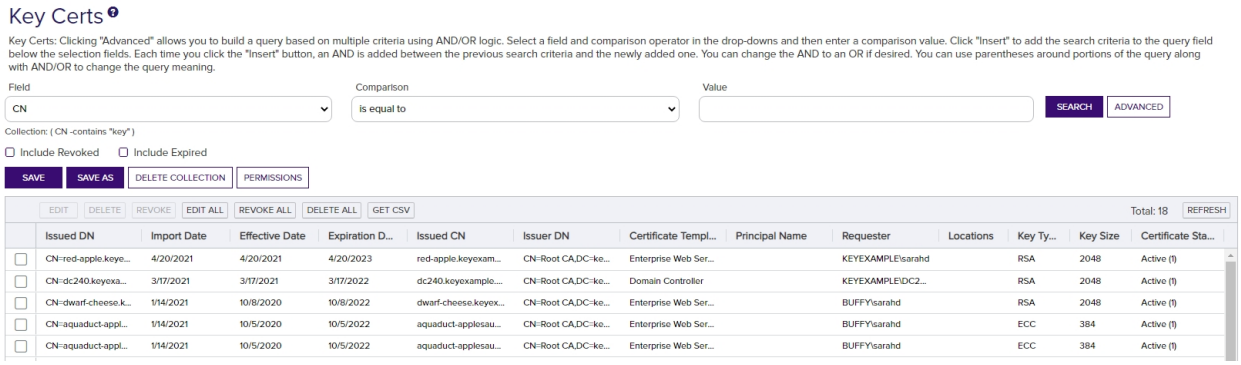


Figure 54: View Collection

Available operations on a certificate collection include; **Save**, **Save As**, **Delete Collection** or view **Permissions** on the certificate collection.

Click **Save** to edit the existing collection. You may change the following about the collection from this option:

- The collection *Name*.
- The collection *Description*.
- The collection query *Content*.
- The *Ignore Renewed Cert Results by* setting.

- The *Show on Dashboard* setting.
- The *Show on Navigator* setting.

For more information on these, see Saving Search Criteria as a Collection on page 40.

Note: Certificate collections that are configured for *Certificate Entered Collection* or *Certificate Left Collection* workflows (see Workflow Definition Operations in the *Keyfactor Command Reference Guide*) cannot be edited to prevent triggering a large number of entered/left workflows.

Click **Save As** to create a new collection based on the existing collection. You can then edit the search criteria for the new collection without affecting the existing collection. Click **Delete Collection** to delete the certificate collection. Click **Permissions** to view collection level permission for the collection (see Certificate Permissions on page 621).

Tip: If you **Save** a new certificate collection, or **Save** a change to an existing certificate collection, that change will be immediately reflected in the collection data used to display certificate collections on dashboards and reports. The data used by the dashboards and reports is stored in an intermediate table that is updated immediately. It will also continue to be updated periodically (approximately every 20 minutes by default as configured by the *Dashboard Collection Caching Interval* application setting) by the Keyfactor Command Service (see Application Settings: Console Tab on page 584).

Using the Collection Manager Search Feature

The search function allows you to query the database for information. The same query structure is used in multiple locations within the Keyfactor Command Management Portal.

When you first open the page, you will see the simple search option. To execute a search, select the field and comparison operators in the dropdowns and type something on which to search in the value field (if applicable). If you select an *is null* or *is not null* comparison operator, the value field will be grayed out. Click the **Search** button to execute the query.

Each query consists of three parts:

Query Field

The available fields for querying vary depending on the area of the Management Portal in which the search is used. On this page, the queries can be done on the following built-in fields:

Name	Query
Complete or partial matches with the name of the collection.	Complete or partial matches with the query.

Comparison Operator

The query comparison operators vary depending on the type of field selected and the specific properties of the field. The list below shows the dropdown list comparison operators, as well as the equivalent query language syntax (in parentheses).

Most string fields (the vast majority of the built-in fields) support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Contains (-contains)
- Does not contain (-notcontains)
- Starts with (-startswith)
- Ends with (-endswith)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Most date and integer fields support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Is less than (-lt)
- Is less than or equal to (-le)
- Is greater than (-gt)
- Is greater than or equal to (-ge)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Most Boolean (true/false) fields support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Comparison Value

The value you enter for comparison must match the field type. For example, integer fields only support numerical values. String fields support all alphanumeric characters. Boolean fields only support True or False. The value field is not case sensitive. Date fields support only properly formatted dates and will initially display as mm/dd/yyyy. You can choose to populate the date field by:

- Clicking in a date Value field to open a pop-up calendar to select a date that will populate the field.
- Clicking in a segment of the date format (i.e., mm/dd/yyyy) and entering a value. As you continue to type in any one segment, the cursor will keep moving onto the next segment.

The results that match your search criteria will be displayed in the results grid below the search selection options.

Advanced Searches

On any search page you can click **Advanced** to the right of the Search button to display the advanced search options. Click **Simple** to close the advanced search options again.

Multiple Criteria

Using the advanced search options, you can build a query based on multiple criteria using AND/OR logic. As with a simple search, you select a field and comparison operator in the drop-downs and

then enter a comparison value, if applicable. Click **Insert** to add the search criteria to the query field below the selection fields. Use the selection fields to build multiple search criteria. Each time you click the insert button, an AND is added between the previous search criteria and the newly added one. You can change the AND to an OR if desired. You can use parentheses around portions of the query along with AND/OR to change the query meaning.

For example, for certificate searches:

```
(CN -contains "appsrvr" AND IssuedDate -ge "01/01/2022") OR (CN -contains "appsrvr" AND
TemplateShortName -contains "web")
```

This query will return all the certificates issued on or after January 1, 2022 with the string appsrvr in the CN and also all certificates issued at any time with the string appsrvr in the CN using a template referencing web. When you have entered all the desired search criteria, click **Search** to execute the query. If you wish to clear the query field and start over, click the **Clear** button.

2.1.4 Reports

Keyfactor Command uses the Logi Analytics Platform to provide a number of built-in reports based on certificate data in the Keyfactor Command database. These reports are available for viewing through the Management Portal, if you configured that option during the installation and configuration process (see *Install the Main Keyfactor Command Components on the Keyfactor Command Server(s): Dashboard and Reports Tab* in the *Keyfactor Command Server Installation Guide*). The reports can also be configured to save to a network path or deliver via email periodically, if desired.

As of Keyfactor Command version 10, Logi has been upgraded to v14 SP2 and a new Logi license is included in the application.

Note: Any CAs that have not been configured for synchronization will not appear as an option for reports which require selecting a CA.

Tip: If you **Save** a new certificate collection, or **Save** a change to an existing certificate collection, that change will be immediately reflected in the collection data used to display certificate collections on dashboards and reports. The data used by the dashboards and reports is stored in an intermediate table that is updated immediately. It will also continue to be updated periodically (approximately every 20 minutes by default as configured by the *Dashboard Collection Caching Interval* application setting) by the Keyfactor Command Service (see Application Settings: Console Tab on page 584).

Once a report has been generated, you may be able to export it to either PDF, Excel, or CSV. The export file types available for each standard report are shown in Table 5: Chart of Available Exports per Standard Report.

Table 5: Chart of Available Exports per Standard Report

PDF and Excel	Excel and CSV	PDF, Excel and CSV
Certificate Count by Template	Certificates Found at TLS/SSL Endpoints	Certificate Count Grouped by Single Metadata Fields
Certificate Count by User per Template	Certificates in Collection	
Certificate by Key Strength	Expiration Report by Days	
Certificates by Revoker	Full Certificate Extract	
Certificates by Type and Java Keystores	Revoked Certificates in Certificate Stores	
Certificate Issuance Trends with Metadata	SSH Keys with Root Logon Access	
Expiration Report	SSH Trusted Public Keys with No Known Private Key	
Issued Certificates Per Certificate Authority	SSH Key Usage Report	
Monthly Executive Report		
PKI Status for Collection		
Statistical Report		
SSH Keys by Age		

Report Drill-down

Most reports now have drill-down capability. Clicking on a chart or graph segment in a report will open the corresponding query grid in a new browser window or tab populated with the query as defined by the selected graph segment. For example, for the *Certificates by Key Strength* report, clicking on a bar or pie will take you to the Certificate Search page pre-populated with the query that corresponds to that bar or pie.

Figure 55: Report Drill Down: Certificates by Key Strength Report

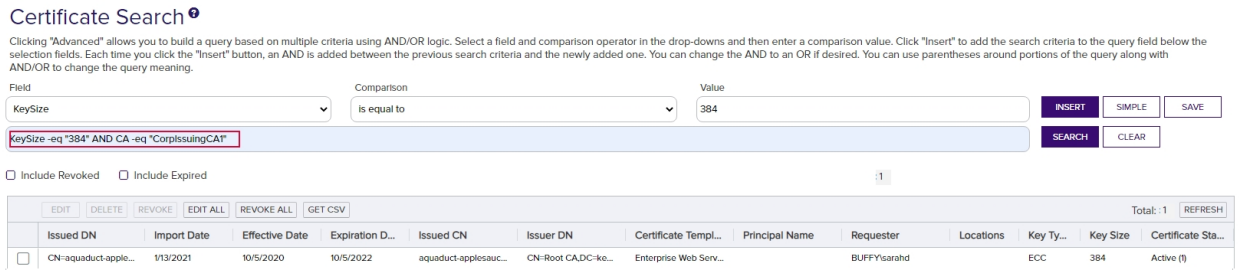


Figure 56: Report Drill Down: Certificate Search Results

List of Built-In Reports

The following reports are available as part of the standard Keyfactor Command installation. Those marked with a (*) have been configured to *Show in Navigator* by default, so they appear on the Management Portal top menu under Reports. The Report Manager page shows all the available reports.

- Certificate Count by Template
- Certificate Count by User per Template
- Certificate Count Grouped by Single Metadata Field
- Certificate Issuance Trends with Metadata
- Certificates by Key Strength
- Certificates by Revoker
- Certificates by Type and Java Keystores
- Certificates Found at TLS/SSL Endpoints
- Certificates in Collection (*)
- Expiration Report (*)
- Expiration Report by days (*)
- Full Certificate Extract (*)
- Issued Certificates per Certificate Authority
- Monthly Executive Report
- PKI Status for Collection (*)
- Revoked Certificates in Certificate Stores
- SSH Key Usage Report
- SSH Keys by Age
- SSH Keys with Root Logon Access
- SSH Trusted Public Keys with No Known Private Keys
- Statistical Report (*)

2.1.4.1 Certificate Count by Template

The Certificate Count by Template report includes bar graphs showing the number of certificates issued, failed and revoked by template in the selected date range for the selected CA(s). Separate graphs are generated for issued and revoked certificates and for each selected CA. Each graph contains all the templates that have had certificates issued or revoked for the period.

Note: Clicking on a bar on the graph, or a section of a pie chart or line graph, will open a new window as a drill down to the certificate search grid filtered for the exact criteria of that aspect of the graph. You can return to the original report by navigating to the original report window.

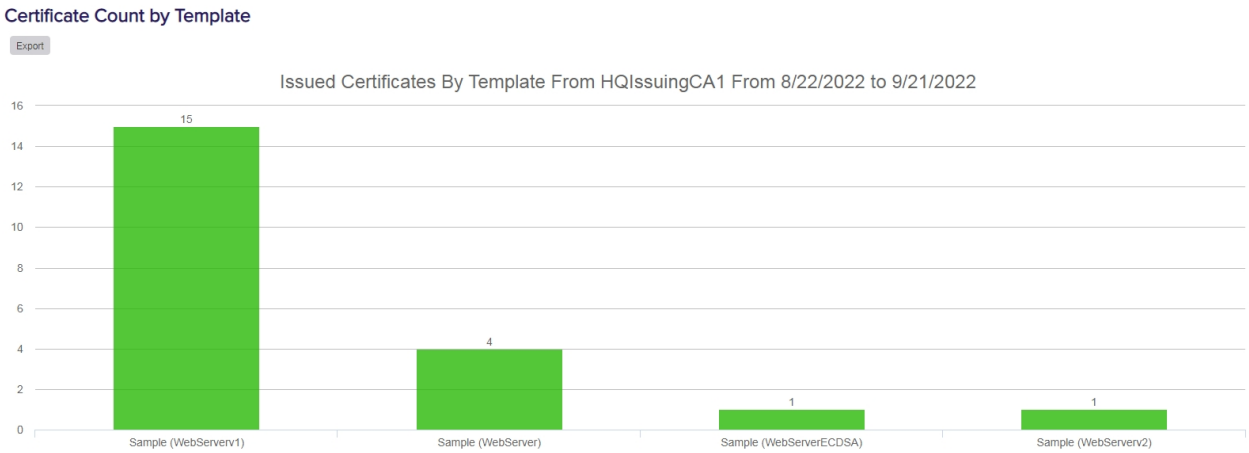


Figure 57: Certificate Count by Template: Issued Certificates

The export options for the Certificate Count by Template report are Excel and PDF.

The input parameters for this report are:

- The start date and end date for the report date range. The default date range is 30 days prior through the current date, meaning only certificates issued and revoked in that date range will be included in the report.
- The CA(s) to include in the report. Templates that are available for issuance from more than one CA are reported separately by CA.

Note: Only CAs configured for synchronization are available for reporting.

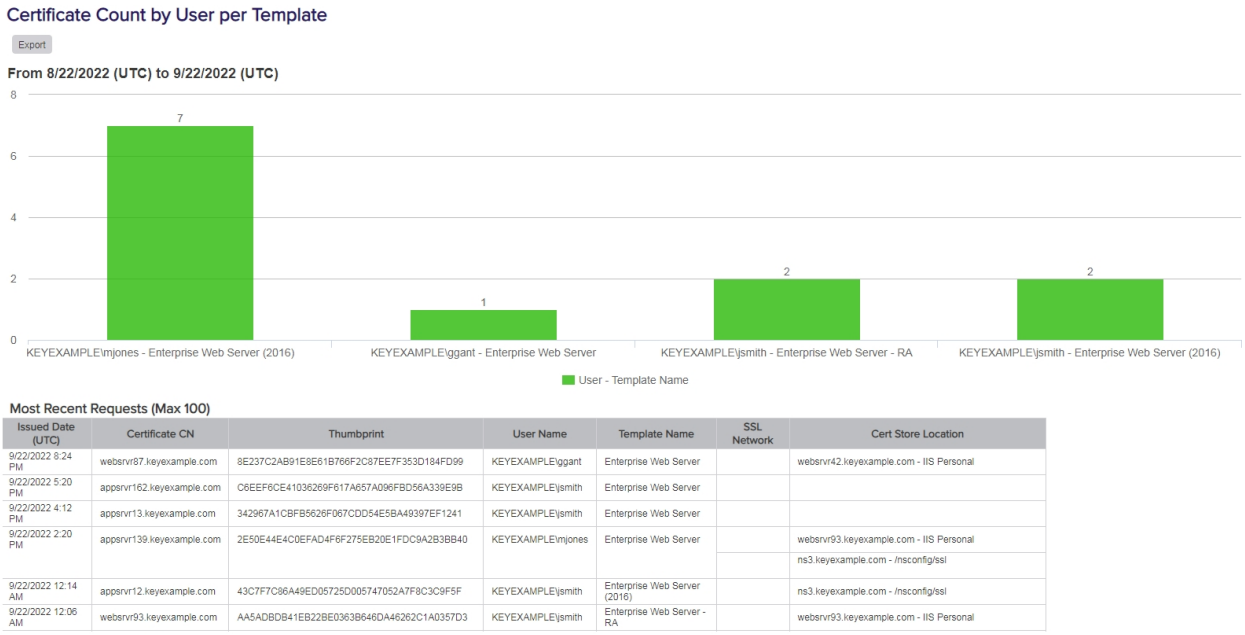
Note: By default, this report is configured not to appear on the top menu under Reports and can be found only in Report Manager. You can change this by modifying the *Show in Navigator* setting (see Report Manager Operations on page 122).

2.1.4.2 Certificate Count by User per Template

The Certificate Count by User per Template report includes a table and bar graphs.

The bar graphs show the number of certificates issued by the certificate requester and template in the selected date range for the selected template(s). The report shows one bar for each requester and template combination; for example, *KEYEXAMPLE\jsmith - Template One* would be one bar and *KEYEXAMPLE\mjones - Template One* would be another bar.

Note: Clicking on a bar on the graph, or a section of a pie chart or line graph, will open a new window as a drill down to the certificate search grid filtered for the exact criteria of that aspect of the graph. You can return to the original report by navigating to the original report window.



Most Recent Requests (Max 100)

Issued Date (UTC)	Certificate CN	Thumbprint	User Name	Template Name	SSL Network	Cert Store Location
9/22/2022 8:24 PM	websrvr87.keyexample.com	8E237C2AB91E8E61B766F2C87EE7F353D184FD99	KEYEXAMPLE\ggant	Enterprise Web Server		websrvr42.keyexample.com - IIS Personal
9/22/2022 5:20 PM	appsrvr162.keyexample.com	C6EEF6CE41036269F617A657A096FBD56A339E9B	KEYEXAMPLE\jsmith	Enterprise Web Server		
9/22/2022 4:12 PM	appsrvr13.keyexample.com	342967A1CBFB5626F067CDD54E5BA49397EF1241	KEYEXAMPLE\jsmith	Enterprise Web Server		
9/22/2022 2:20 PM	appsrvr139.keyexample.com	2E50E44E4C0EFAD4F6F275EB20E1FDC9A2B3BB40	KEYEXAMPLE\mjones	Enterprise Web Server		websrvr93.keyexample.com - IIS Personal
						ns3.keyexample.com - /nsconfig/ssl
9/22/2022 12:14 AM	appsrvr12.keyexample.com	43C7F7C86A49ED05725D005747052A7F8C3C9F5F	KEYEXAMPLE\jsmith	Enterprise Web Server (2016)		ns3.keyexample.com - /nsconfig/ssl
9/22/2022 12:06 AM	websrvr93.keyexample.com	AA5ADBDB41EB22BE0363B646DA46262C1A0357D3	KEYEXAMPLE\jsmith	Enterprise Web Server - RA		websrvr93.keyexample.com - IIS Personal

Figure 58: Certificate Count by User by Template

The table shows detailed information for the certificates issued in the selected time-frame (up to a maximum of 100).

The export options for the Certificate Count by User per Template report are Excel and PDF. The PDF exports in landscape format to accommodate the width of the report.

The certificate details grid includes these fields:

- Issued Date
  The certificate's effective date.
- Certificate CN
  Common name of the certificate.
- Thumbprint
  Thumbprint of the certificate.
- User Name
  The user who requested the certificate. In some cases (e.g. enrollment using the *Restrict Allowed Requesters* option), this will be a service account rather than an end user.
- Template Name
  Name of the template used for the certificate.
- SSL Network
  The name of the SSL network containing the endpoint at which the certificate is found, if any.
- Cert Store Location
  The certificate store or stores in which the certificate is found, if any.

The input parameters for this report are:

- The template names on which to report. Although you can select multiple templates, selecting more than one or two templates can make for a messy report, depending on how many unique users have requested certificates using the selected template(s) in the date range. Defaults for the template(s) on which to report can be configured in the report parameters (see Report Manager Operations on page 122).

- The start date and end date for the date range on which to report. The default date range is one month ending with the current date. These defaults can be changed in the report parameters (see Report Manager Operations on page 122).
- A requester and template combination bar will only be included in the bar chart, with corresponding details in the details grid, if the number of certificates issued for it in the selected date range exceeds the value selected for *Certificate count more than*.

  Example: You want to track down instances of duplicate certificates where user X has been issued a certain type of certificate more than once and more than one of these certificates is still valid (not revoked). To use this report for that, select the template or templates used for that particular type of certificate (say, a client authentication template), select a date range that would cover the full lifetime for certificates issued by that template, and select a value of 1 or greater in the *Certificate count more than* field. The report results will include all users who have multiple certificates issued with the selected template(s) in the selected date range.

Note: Certificates must have a certificate state of *Active* to be included in the report. The report output includes active and expired certificates but not revoked certificates.

Note: By default, this report is configured not to appear on the top menu under Reports and can be found only in Report Manager. You can change this by modifying the *Show in Navigator* setting (see Report Manager Operations on page 122).

2.1.4.3 Certificate Count Grouped by Single Metadata Field

The Certificate Count Grouped by Single Metadata Field report includes a data table with two columns:

- Metadata Value
  All the populated values for the selected metadata field for certificates issued in the selected date range.
- Certificate Count
  The number of certificates issued for each metadata value in the selected date range.

For example, if the selected metadata field is AppOwnerEmailAddress, the table will show a row for each unique email address populated in a certificate issued in the selected date range with a count of how many certificates share that same email address.

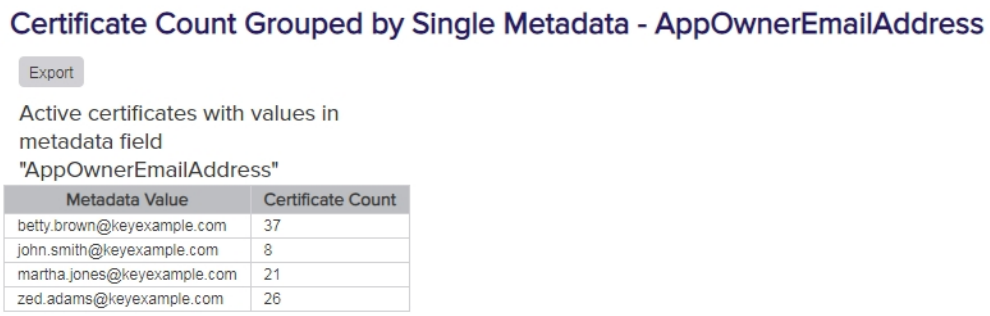


Figure 59: Certificate Count Grouped by Single Metadata Field

The export options for the Certificate Count Grouped by Single Metadata Field report are CSV, Excel, and PDF.

The input parameters for this report are:

- The metadata field on which to report. Only Boolean, integer, multiple choice, and string fields are available for reporting.
- The start date and end date for the date range on which to report. The default date range is one month ending with the current date. Only certificates issued within the time span will be counted.

Note: Certificates must have a certificate state of *Active* to be included in the report. The report output includes active and expired certificates but not revoked certificates. Only certificates issued within the time span will be counted.

Note: By default, this report is configured not to appear on the top menu under Reports and can be found only in Report Manager. You can change this by modifying the *Show in Navigator* setting (see Report Manager Operations on page 122).

2.1.4.4 Certificate Issuance Trends with Metadata

The Certificate Issuance Trends with Metadata report produces tables and pie charts showing currently active certificates based on the selected input parameters as follows: the number of certificates per requester and the number of certificates per metadata value for each of the metadata fields chosen, based on the certificate collection chosen. Multiple tables and charts will be produced when the report is generated.

Note: Clicking on a bar on the graph, or a section of a pie chart or line graph, will open a new window as a drill down to the certificate search grid filtered for the exact criteria of that aspect of the graph. You can return to the original report by navigating to the original report window.

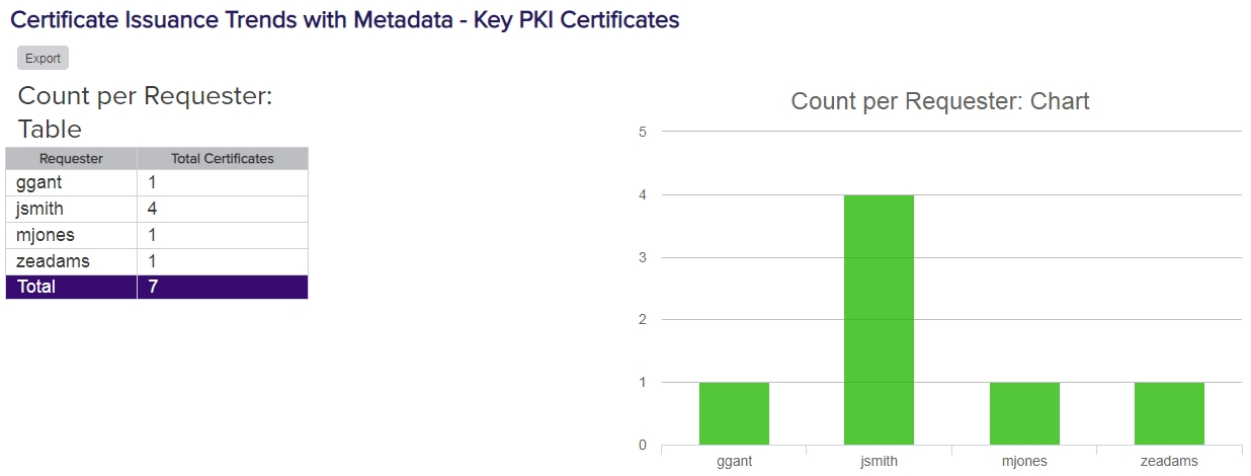


Figure 60: Certificate Issuance Trends with Metadata: Requesters

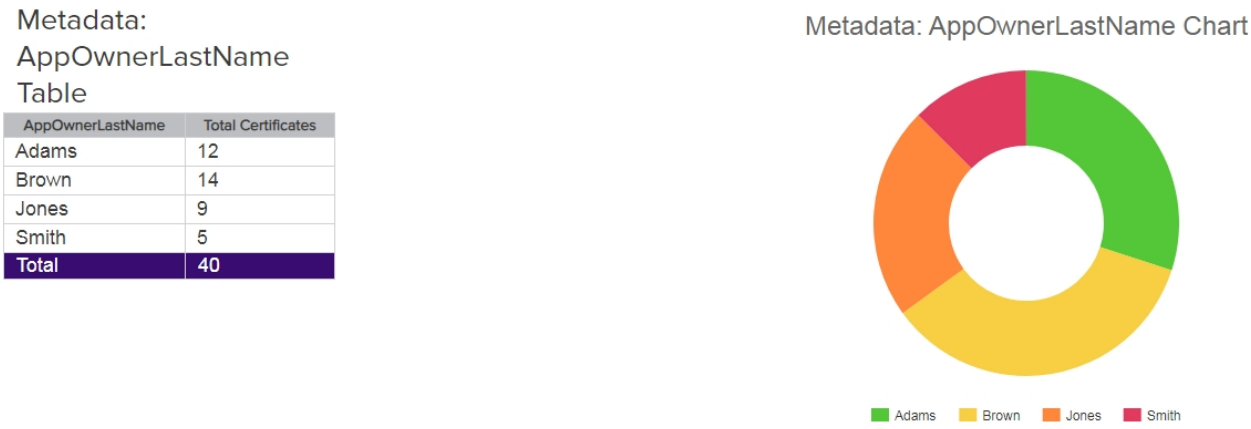


Figure 61: Certificate Issuance Trends with Metadata: Metadata Table and Chart

The export options for the Certificate Issuance Trends with Metadata report are Excel and PDF.

Note: When either scheduling or exporting this report as an Excel file, the output will not include the graphs.

The input parameters for this report are:

- Collections: The name of the collection to report on.
- The start date and end date for the report: The definition of the date range for the report.
- Metadata: Check a metadata field from the pop-up to select it for this report.
- Requesters: A comma-separated list of requester user names (do not included the domain name).

Tip: If you **Save** a new certificate collection, or **Save** a change to an existing certificate collection, that change will be immediately reflected in the collection data used to display

certificate collections on dashboards and reports. The data used by the dashboards and reports is stored in an intermediate table that is updated immediately. It will also continue to be updated periodically (approximately every 20 minutes by default as configured by the *Dashboard Collection Caching Interval* application setting) by the Keyfactor Command Service (see Application Settings: Console Tab on page 584).

Note: By default, this report is configured not to appear on the top menu under Reports and can be found only in Report Manager. You can change this by modifying the *Show in Navigator* setting (see Report Manager Operations on page 122).

Note: Other than the option of certificates with no associated CA, only CAs currently configured for synchronization are available for reporting.

2.1.4.5 Certificates by Key Strength

The Certificates by Key Strength report includes a bar graph showing the number of active certificates by key strength (e.g. sha-1, sha-256) for the selected CA(s), a bar graph showing the number of active certificates by key size for the selected CA(s), and a pie chart for each selected CA showing the active certificates by key size (e.g. 1024 bit, 2048 bit).

Note: Clicking on a bar on the graph, or a section of a pie chart or line graph, will open a new window as a drill down to the certificate search grid filtered for the exact criteria of that aspect of the graph. You can return to the original report by navigating to the original report window.

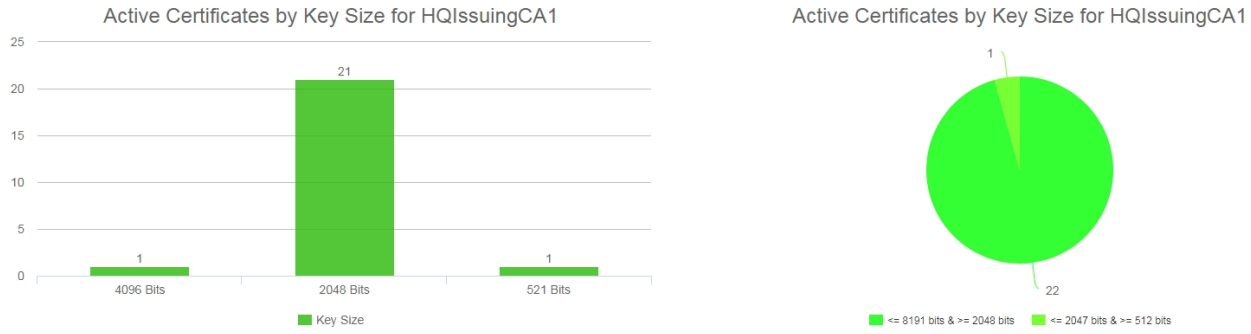


Figure 62: Certificates by Key Strength

The export options for the Certificates by Key Strength report are Excel and PDF.

This report takes as an input parameter the CA(s) on which to report and includes the option to report on certificates that have no associated CA. Typically, these would be certificates found via SSL scanning or inventory on certificate stores.

Note: By default, this report is configured not to appear on the top menu under Reports and can be found only in Report Manager. You can change this by modifying the *Show in Navigator* setting (see Report Manager Operations on page 122).

Note: Other than the option of certificates with no associated CA, only CAs currently or previously configured for synchronization are available for reporting.

2.1.4.6 Certificates by Revoker

The Certificates by Revoker report includes a bar graph showing the number of certificates revoked through Keyfactor Command in the selected date range for the selected CA(s) broken down by the user doing the revocation. The report shows one bar for each revoker.

Note: Clicking on a bar on the graph, or a section of a pie chart or line graph, will open a new window as a drill down to the certificate search grid filtered for the exact criteria of that aspect of the graph. You can return to the original report by navigating to the original report window.

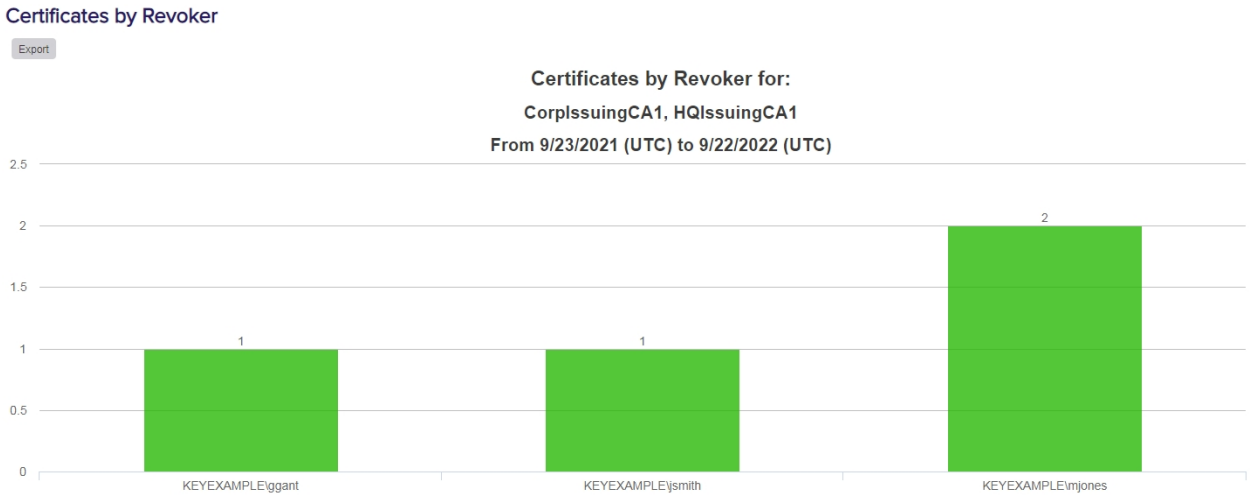


Figure 63: Certificates by Revoker

The export options for the Certificates by Revoker report are Excel and PDF.

Note: Certificates that have been revoked outside of Keyfactor Command (e.g. directly on the CA) appear with an *Unknown* revoker.

The input parameters for this report are:

- The evaluation date for the report. This report covers a specified number of days, weeks or months ending with this date. The default evaluation date is the current date, meaning

certificates revoked up to the current date will be included in the report. The default can be changed in the report parameters (see Report Manager Operations on page 122).

- The number of periods to include in the report. This is how many days, weeks or months of data to include in the report. The default is 52.
- The period length for the report. The options are days, weeks or months. The default is weeks.
- The CA(s) to include in the report. Certificates that were issued from CA(s) other than those selected will not be included in the counts of revoked certificates.

Note: By default, this report is configured not to appear on the top menu under Reports and can be found only in Report Manager. You can change this by modifying the *Show in Navigator* setting (see Report Manager Operations on page 122).

Note: Only CAs currently or previously configured for synchronization are available for reporting.

2.1.4.7 Certificates by Type and Java Keystore

The Certificates by Type and Java Keystore report provides a table with a summary of the number of certificates generated through Keyfactor Command in the selected date range broken down by PFX requests versus CSR requests for a selected CA or CAs. In addition, a count is provided of certificates that were added to Java Keystores in this timeframe (new or existing certificates from any source).

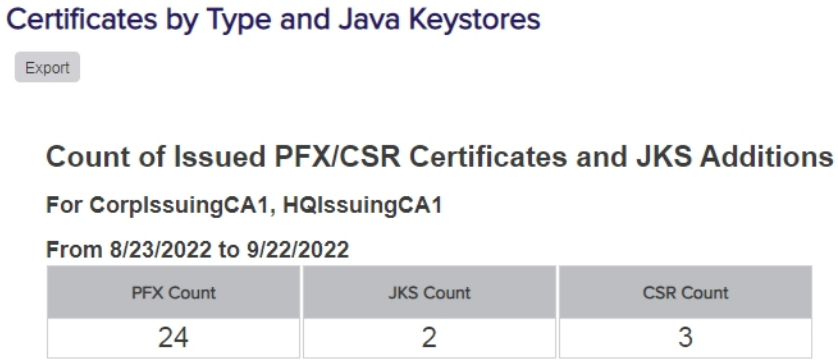


Figure 64: Certificates by Type and Java Keystore

The export options for the Certificates by Type and Java Keystore report are Excel and PDF.

The input parameters for this report are:

- The CA(s) to include in the report. Certificates that were issued from CAs other than those selected will not be included in the counts of PFXs and CSRs.
- The start date and end date for the date range on which to report. The default date range is one month ending with the current date. These defaults can be changed in the report parameters

(seeReport Manager Operations on page 122).

Note: By default, this report is configured not to appear on the top menu under Reports and can be found only in Report Manager. You can change this by modifying the *Show in Navigator* setting (see Report Manager Operations on page 122).

Note: Only CAs currently or previously configured for synchronization are available for reporting.

2.1.4.8 Certificates Found at TLS/SSL Endpoints

The Certificates Found at TLS/SSL Endpoints report provides a table which shows the IP Address and Port for any discovered endpoints with the Issued DN for the certificate or certificates discovered at the endpoint and the server name indication (SNI) configured on the endpoint, if available. The report table includes these fields:

- IP Address
- Port
- Issued DN
- SNI Name
- Reverse DNS

Certificates Found at TLS/SSL Endpoints

Export

Ip Address	Port	Issued DN	SNI Name	Reverse DNS
10.15.20.2	443	CN=pfSense-619d0859492a1,O=pfSense webConfigurator Self-Signed Certificate		10.15.20.2
10.15.20.1	443	C=DE\;ST\=Berlin\;L\=Berlin\;CN\=OpenWrt\;		10.15.20.1
10.4.3.183	8443	C=US,O=Key Example,CN=ManagementCA		ejbca2.keyother.com
10.4.3.175	443	CN=bigip16.keyexample.com,OU=IT,L=Independence,ST=Ohio,C=US		bigip16.keyexample.com
10.4.3.183	8443	C=US,O=Key Example,CN=ejbca2.keyother.com		ejbca2.keyother.com
10.4.3.154	443	CN=default SWFQOW,OU=NS Internal,O=Citrix ANG,L=San Jose,ST=California,C=US		ns3.keyexample.com
10.4.3.80	443	CN=appsrvr80.keyexample.com,OU=IT,L=Independence,ST=Ohio,C=US		appsrvr80.keyexample.com
10.4.3.1	443	CN=pfSense-619d0859492a1,O=pfSense webConfigurator Self-Signed Certificate		10.4.3.1
10.4.3.242	443	CN=keyfactor242.keyexample.com		srvr242.keyexample.com

Figure 65: Certificates Found at TLS/SSL Endpoints

The export options for the Certificates Found at TLS/SSL Endpoints report are CSV and Excel.

The input parameters for this report are:

- The orchestrator pool on which to report. Only one orchestrator pool can be selected. A default for the orchestrator pool on which to report can be configured in the report parameters (see Report Manager Operations on page 122).
- The start date and end date for the date range on which to report. The default date range is one month ending with the current date. These defaults can be changed in the report parameters (see Report Manager Operations on page 122).

Note: By default, this report is configured not to appear on the top menu under Reports and can be found only in Report Manager. You can change this by modifying the *Show in Navigator* setting (see Report Manager Operations on page 122).

2.1.4.9 Certificates in Collection

The Certificates in Collection report shows detailed information for the active, expired and revoked certificates in the selected collection.

Tip: If you **Save** a new certificate collection, or **Save** a change to an existing certificate collection, that change will be immediately reflected in the collection data used to display certificate collections on dashboards and reports. The data used by the dashboards and reports is stored in an intermediate table that is updated immediately. It will also continue to be updated periodically (approximately every 20 minutes by default as configured by the *Dashboard Collection Caching Interval* application setting) by the Keyfactor Command Service (see Application Settings: Console Tab on page 584).

The export options for the Certificates in Collection report are CSV and Excel.

The report table includes these fields:

- ID

  The Keyfactor Command reference ID for the certificate.
- Issued DN
- Effective Date (UTC)
- Expiration Date (UTC)
- Issued CN
- Issuer DN
- Principal

  The user principal name (UPN) contained in the subject alternative name (SAN) field of the certificate, if present (e.g. username@keyexample.com).
- Requester
- Thumbprint
- Template
- Cert State

  The state of the certificate (e.g. Active, Revoked, Unknown).
- Key Type
- Key Size in Bits
- Key Usage
- Signing Algorithm
- Serial Number
- CA Record ID

  The ID of the certificate in the CA database.
- Issued OU

  The OU from the certificate subject, if any.
- Issued Email

  The email address from the certificate subject, if any.
- Revocation Effective Date
- Revocation Reason
- Metadata (Optional)

Column handling on this report grid has the following features:

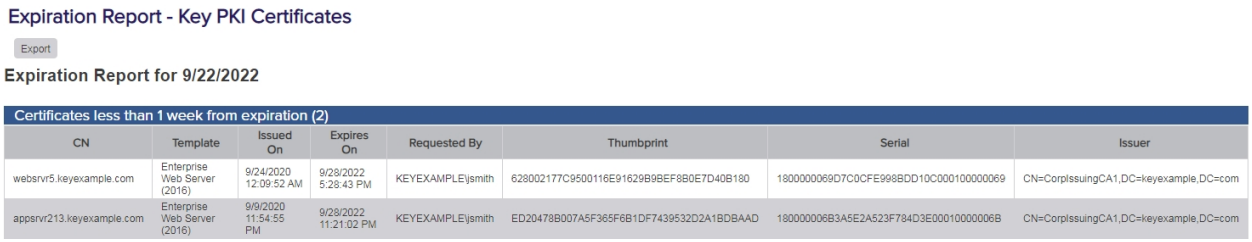
- To change the width of a column of the report, hover over the triangle of dots on the right side of the selected column header (). Click, hold and drag the triangle to change the width of the column.
- To rearrange columns on the report display, hover over the rectangle of dots on the left side of the selected column header (). Click, hold, and drag the rectangle to move the column to your selected location.
- Most columns can be sorted in ascending order by clicking on the header of the column. Click the column header again to reverse the sort order. When a column is sorted, a caret will appear at the end of the column name showing the direction of the sort. Lack of a triangle indicates the report is sorted by the default column and order.

The input parameter for this report is:

- The certificate collection to report on, including the built-in option, *All Certificate*s collection. The default is *All Certificates*.
- The metadata field(s) to include, if desired.

2.1.4.10 Expiration Report

The Expiration Report includes table(s) showing detailed information for certificates expiring and expired within the next 12 weeks and CA certificates expiring and expired within the next 2 1/2 years. Expired certificates are only included if they have expired within the last 4 weeks.



Expiration Report - Key PKI Certificates

Export

Expiration Report for 9/22/2022

Certificates less than 1 week from expiration (2)

CN	Template	Issued On	Expires On	Requested By	Thumbprint	Serial	Issuer
websrvr5.keyexample.com	Enterprise Web Server (2016)	9/24/2020 12:09:52 AM	9/28/2022 5:28:43 PM	KEYEXAMPLE\jsmith	628002177C9500116E91629B9BEF8B0E7D40B180	1800000069D7C0CFE998BDD10C000100000069	CN=CorpIssuingCA1,DC=keyexample,DC=com
appsrvr213.keyexample.com	Enterprise Web Server (2016)	9/9/2020 11:54:55 PM	9/28/2022 11:21:02 PM	KEYEXAMPLE\jsmith	ED20478B007A5F365F6B1DF7439532D2A1BDBAAD	180000006B3A5E2A523F784D3E00010000006B	CN=CorpIssuingCA1,DC=keyexample,DC=com

Figure 66: Certificate Expiration Report: Certificates Expiring within One Week

The export options for the Expiration report are Excel and PDF. The PDF exports in landscape format to accommodate the wide width of the report.

The report includes the following tables:

- Expired Certificates (within the last 4 weeks)
- Certificates less than 1 week from expiration
- Certificates less than 2 weeks from expiration
- Certificates less than 4 weeks from expiration
- Certificates less than 6 weeks from expiration
- Certificates less than 8 weeks from expiration
- Certificates less than 12 weeks from expiration

In addition, tables are shown for CA certificates expiring in the following timeframes relative to the selected report date:

- CA certificates less than 6 months from expiration
- CA certificates less than 12 months from expiration
- CA certificates less than 18 months from expiration
- CA certificates less than 24 months from expiration
- CA certificates less than 30 months from expiration

A table is only shown if a certificate or CA in the collection matches the expiration time window. A certificate or CA appears in only one table, so, for example, a certificate expiring within 4 weeks does not also appear as expiring within 6 weeks.

The report tables include these fields:

- CN (Common Name)
- Template
- Issued On
- Expires On (this is the default sort order)
- Requested By
- Thumbprint
- Serial (Number)
- Issuer (Distinguished Name)
- Metadata (optional)

Column handling on this report grid has the following features:

- To change the width of a column of the report, hover over the triangle of dots on the right side of the selected column header (). Click, hold and drag the triangle to change the width of the column.
- To rearrange columns on the report display, hover over the rectangle of dots on the left side of the selected column header (). Click, hold, and drag the rectangle to move the column to your selected location.
- Most columns can be sorted in ascending order by clicking on the header of the column. Click the column header again to reverse the sort order. When a column is sorted, a caret will appear at the end of the column name showing the direction of the sort. Lack of a triangle indicates the report is sorted by the default column and order.

The input parameters for this report are:

- The certificate collection to report on, including the built-in *All Certificates* collection. The default is *All Certificates*.
- The evaluation date to report on. The default is the current date.
- The metadata field(s) to include, if desired.

Tip: This report makes use of the optional certificate de-duplication logic by default. When de-duplication is enabled for a report, the report results will include only the most recently issued certificate if there is more than one certificate that matches the de-duplication criteria. De-duplication is enabled for a report by checking the *Ignore Renewed Certificates* box on the Details tab of the report configuration (see Report Manager Operations on page 122). De-duplication can only be enabled for reports that use certificate collections—the *Uses Collection* box on the Details tab. The *Uses Collection* setting is not user-configurable.

De-duping is configured on a certificate collection by setting the *Ignore renewed certificate results by* option when saving a certificate collection (see Saving Search Criteria as a Collection on page 40). Certificate collections may be configured to be de-duplicated based on the certificate common name, distinguished name, or principal name (or not at all). Only certificates that share all the EKUs (e.g. Client Authentication and Server Authentication) as well as the same CN, DN or UPN will be eliminated as duplicates. If a certificate has more than one EKU and at least one EKU does not match an otherwise similar certificate with matching CN, DN or UPN, it will not be eliminated.

For example, if the de-duplication logic was set to DN and the report would include these two certificates:

- Certificate one:
  - DN: CN=apps-srvr14.keyexample.com,OU=IT,O=Key Example, Inc.,L=Chicago,ST=IL,C=US
  - EKUs: Server Authentication
  - Issued Date: December 1, 2020
  - Expiration Date: January 1, 2022
- Certificate two:
  - DN: CN=apps-srvr14.keyexample.com,OU=IT,O=Key Example, Inc.,L=Chicago,ST=IL,C=US
  - EKUs: Server Authentication
  - Issued Date: December 15, 2020
  - Expiration Date: December 14, 2021

The de-duplication logic would be triggered because the DNs and EKUs match. The report would include certificate two and leave out certificate one. Notice that certificate two is retained even through certificate one expires after certificate two. This is because certificate two was issued after certificate one.

Now imagine that the de-duplication logic is set to CN and the report would include these two certificates:

- Certificate one:
  - DN: CN=appsrvr14.keyexample.com,OU=IT,O=Key Example, Inc.,L-L=Chicago,ST=IL,C=US
  - EKUs: Server Authentication
  - Issued Date: December 1, 2020
  - Expiration Date: January 1, 2022
- Certificate two:
  - DN: CN=appsrvr14.keyexample.com,OU=HR,O=Key Example, Inc.,L-L=Chicago,ST=IL,C=US
  - EKUs: Server Authentication, Client Authentication
  - Issued Date: December 15, 2020
  - Expiration Date: December 14, 2021

Although the DNs for these certificates do not match, the CNs still do, so this matches the de-duplication logic of CN. However, the EKUs for these two certificates do not match, since only one of them includes Client Authentication. In this case, both certificates would appear on the report.

Note: This report is limited to a maximum of 10,000 expiring and recently expired (within the last 4 weeks) certificates on which to report. Selecting a certificate collection containing more expiring and recently expired certificates than this, based on the evaluation date, will result in an error. Selecting a certificate collection containing a large number of certificates to report on can cause the report to take a long time to generate.

2.1.4.11 Expiration Report by Days

The Expiration Report by Days shows details for certificates expiring after a given start date with a time span chosen in days. It can be used, for example, to show you all the certificates in a certificate collection expiring within the next few days.

The Expiration Report includes a table showing detailed information for certificates expiring in the time frames identified by the parameters start date and number of days. The number of days parameter value must be between 0 and 100.

The export options for the Expiration Report by Days are CSV and Excel.

The report tables include these fields:

- CN (Common Name)
- Template
- Issued On
- Expires On (this is the default sort order)
- Requested By
- Thumbprint
- Serial (Number)
- Issuer (Distinguished Name)
- Metadata (optional)

Column handling on this report grid has the following features:

- To change the width of a column of the report, hover over the triangle of dots on the right side of the selected column header (). Click, hold and drag the triangle to change the width of the column.
- To rearrange columns on the report display, hover over the rectangle of dots on the left side of the selected column header (). Click, hold, and drag the rectangle to move the column to your selected location.

- Most columns can be sorted in ascending order by clicking on the header of the column. Click the column header again to reverse the sort order.

The input parameters for this report are:

- The certificate collection to report on, including the built-in *All Certificates* collection. The default is *All Certificates*.
- The start date of the reporting period. The default is the current date.
- The number of days in the reporting period (must be between 0 and 100). The default is 6.
- The metadata field(s) to include, if desired.

Tip: If you **Save** a new certificate collection, or **Save** a change to an existing certificate collection, that change will be immediately reflected in the collection data used to display certificate collections on dashboards and reports. The data used by the dashboards and reports is stored in an intermediate table that is updated immediately. It will also continue to be updated periodically (approximately every 20 minutes by default as configured by the *Dashboard Collection Caching Interval* application setting) by the Keyfactor Command Service (see Application Settings: Console Tab on page 584).

Tip: This report makes use of the optional certificate de-duplication logic by default. When de-duplication is enabled for a report, the report results will include only the most recently issued certificate if there is more than one certificate that matches the de-duplication criteria. De-duplication is enabled for a report by checking the *Ignore Renewed Certificates* box on the Details tab of the report configuration (see Report Manager Operations on page 122). De-duplication can only be enabled for reports that use certificate collections—the *Uses Collection* box on the Details tab. The *Uses Collection* setting is not user-configurable.
De-duping is configured on a certificate collection by setting the *Ignore renewed certificate results by* option when saving a certificate collection (see Saving Search Criteria as a Collection on page 40). Certificate collections may be configured to be de-duplicated based on the certificate common name, distinguished name, or principal name (or not at all). Only certificates that share all the EKUs (e.g. Client Authentication and Server Authentication) as well as the same CN, DN or UPN will be eliminated as duplicates. If a certificate has more than one EKU and at least one EKU does not match an otherwise similar certificate with matching CN, DN or UPN, it will not be eliminated.

For example, if the de-duplication logic was set to DN and the report would include these two certificates:

- Certificate one:
  - DN: CN=apps-srvr14.keyexample.com,OU=IT,O=Key Example, Inc.,L=Chicago,ST=IL,C=US
  - EKUs: Server Authentication
  - Issued Date: December 1, 2020
  - Expiration Date: January 1, 2022
- Certificate two:
  - DN: CN=apps-srvr14.keyexample.com,OU=IT,O=Key Example, Inc.,L=Chicago,ST=IL,C=US
  - EKUs: Server Authentication
  - Issued Date: December 15, 2020
  - Expiration Date: December 14, 2021

The de-duplication logic would be triggered because the DNs and EKUs match. The report would include certificate two and leave out certificate one. Notice that certificate two is retained even through certificate one expires after certificate two. This is because certificate two was issued after certificate one.

Now imagine that the de-duplication logic is set to CN and the report would include these two certificates:

- Certificate one:
  - DN: CN=appsrvr14.keyexample.com,OU=IT,O=Key Example, Inc.,L-L=Chicago,ST=IL,C=US
  - EKUs: Server Authentication
  - Issued Date: December 1, 2020
  - Expiration Date: January 1, 2022
- Certificate two:
  - DN: CN=appsrvr14.keyexample.com,OU=HR,O=Key Example, Inc.,L-L=Chicago,ST=IL,C=US
  - EKUs: Server Authentication, Client Authentication
  - Issued Date: December 15, 2020
  - Expiration Date: December 14, 2021

Although the DNs for these certificates do not match, the CNs still do, so this matches the de-duplication logic of CN. However, the EKUs for these two certificates do not match, since only one of them includes Client Authentication. In this case, both certificates would appear on the report.

Note: This report is limited to a maximum of 10,000 expiring certificates on which to report. Selecting a certificate collection containing more expiring certificates than this, within the selected reporting period, will result in an error. Selecting a certificate collection containing a large number of certificates to report on can cause the report to take a long time to generate.

2.1.4.12 Full Certificate Extract Report

The Full Certificate Extract Report shows detailed information for the active, expired and revoked certificates in the selected collection.

The export options for the Full Certificate Extract Report are CSV and Excel.

The report table includes these fields:

- Common Name
  The common name of the certificate.
- Valid From
  The date on which the certificate became valid (typically the issuance date).
- Valid To
  The date on which the certificate expires.
- Total SANs
  The total number of subject alternative names (SANs) for the certificate.
- SANs
  Any subject alternative names (SANs) of type DNS name, UPN, or email.
- SANs IP

- Days to Expiration

  The number of days remaining until the certificate expires. This will be a negative value for expired certificates.
- Signature Algorithm

  The cryptographic algorithm used to sign the certificate.
- Key Size

  The key length used to create the certificate.
- Validity Period

  The number of days for which the certificate was issued.
- Serial Number

  The serial number of the certificate.
- DN

  The distinguished name (subject) of the certificate.
- Issuer DN

  The distinguished name of the issuer (CA) for the certificate.
- User Name

  The name of the identity that requested the certificate.

  Any subject alternative names (SANs) of type IP address.
- Port

  The port where the certificate was found on an SSL scan.
- IP Address

  The IP address where the certificate was found on an SSL scan.
- DNS Name

  The DNS name resolved for the IP address where the certificate was found on an SSL scan.
- Alias

  The alias of the certificate in the certificate store.
- Client Machine

  Depending on the type of certificate store, either the name of the server on which the orchestrator is installed or the name of the server on which the certificate store is located.
- Store Path

  The location of the certificate store. The format of this value will vary depending on the type of certificate store.
- Template

  The certificate template used to issue the certificate.

Column handling on this report grid has the following features:

- To change the width of a column of the report, hover over the triangle of dots on the right side of the selected column header (). Click, hold and drag the triangle to change the width of the column.
- To rearrange columns on the report display, hover over the rectangle of dots on the left side of the selected column header (). Click, hold, and drag the rectangle to move the column to your selected location.
- Most columns can be sorted in ascending order by clicking on the header of the column. Click the column header again to reverse the sort order.

This report takes the input parameters:

- The certificate collection to report on, including the built-in option, *All Certificates* collection. The default is *All Certificates*.
- The metadata field(s) to include, if desired. This will append the selected metadata columns to the end of the report.

Tip: If you **Save** a new certificate collection, or **Save** a change to an existing certificate collection, that change will be immediately reflected in the collection data used to display certificate collections on dashboards and reports. The data used by the dashboards and reports is stored in an intermediate table that is updated immediately. It will also continue to be updated periodically (approximately every 20 minutes by default as configured by the *Dashboard Collection Caching Interval* application setting) by the Keyfactor Command Service (see Application Settings: Console Tab on page 584).

2.1.4.13 Issued Certificates per Certificate Authority

The Issued Certificates per Certificate Authority report includes line graphs showing the number of certificates issued for each template in the selected date range for the selected template(s) on the selected CA. A separate line graph is generated for each template. An option to report on certificates that are not associated with any CA is included.

Note: Clicking on a bar on the graph, or a section of a pie chart or line graph, will open a new window as a drill down to the certificate search grid filtered for the exact criteria of that aspect of the graph. You can return to the original report by navigating to the original report window.

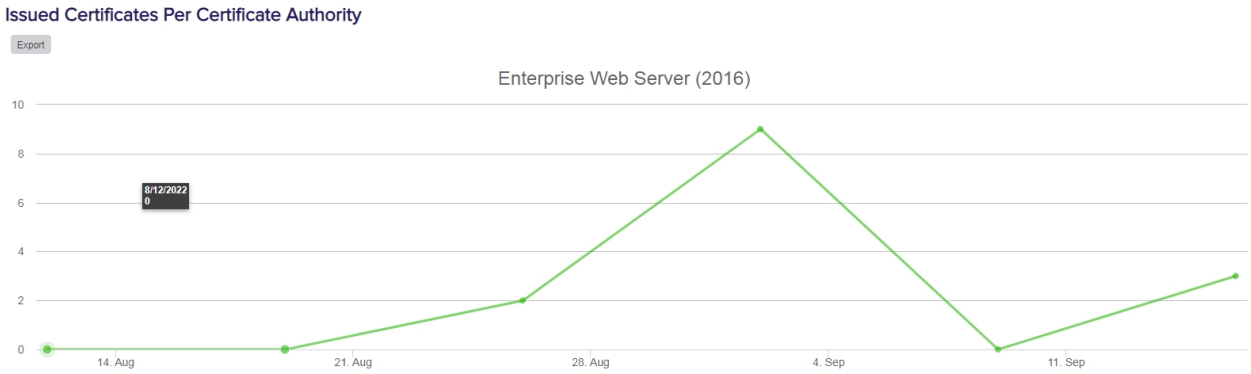


Figure 67: Issued Certificates per CA

The export options for the Issued Certificates per Certificate Authority report are Excel and PDF.

The input parameters for this report are:

- The evaluation date for the report. This report covers a specified number of days, weeks or months ending with this date. The default evaluation date is the current date, meaning certificates issued up to the current date will be included in the report.
- The number of periods to include in the report. This is how many days, weeks or months of data to include in the report. The default is 6.
- The period length for the report. The options are days, weeks or months. The default is weeks.

- Which CA to include in the report. This includes the option to report on certificates that have no associated CA. Typically, these would be certificates found via SSL scanning or inventory on certificate stores. Only one CA option can be reported on at a time.
- The template(s) to include in the report. A separate line graph is generated for each template selected for reporting. Templates that are available for issuance from more than one CA are reported separately by CA, so only certificates issued for the selected template *and* the selected CA will be shown. When the *Certificates Not Associated with CA* option is selected for the CA, the *No Template* option should be selected for the template.

Note: By default, this report is configured not to appear on the top menu under Reports and can be found only in Report Manager. You can change this by modifying the *Show in Navigator* setting (see Report Manager Operations on page 122).

Note: Other than the option of certificates with no associated CA, only CAs currently configured for synchronization are available for reporting.

2.1.4.14 Monthly Executive Report

The Monthly Executive report provides a dashboard-like summary including bar and pie charts with counts of certificates created, renewed and approaching expiration for a selected CA or CAs. Data for certificates approaching expiration is presented in a pie chart broken out into certificates that will expire in the next 15 days, in 16-30 days, 31-60 days and 61-90 days. Data for certificates that have been recently created or renewed is presented in a bar chart that includes data for the current month and the previous month, broken out by month and renewed versus newly created. In addition, a summary pie chart is included that shows all the active certificates for the selected CAs broken out by CA.

Note: Clicking on a bar on the graph, or a section of a pie chart or line graph, will open a new window as a drill down to the certificate search grid filtered for the exact criteria of that aspect of the graph. You can return to the original report by navigating to the original report window.

The export options for the Monthly Executive report are Excel and PDF.

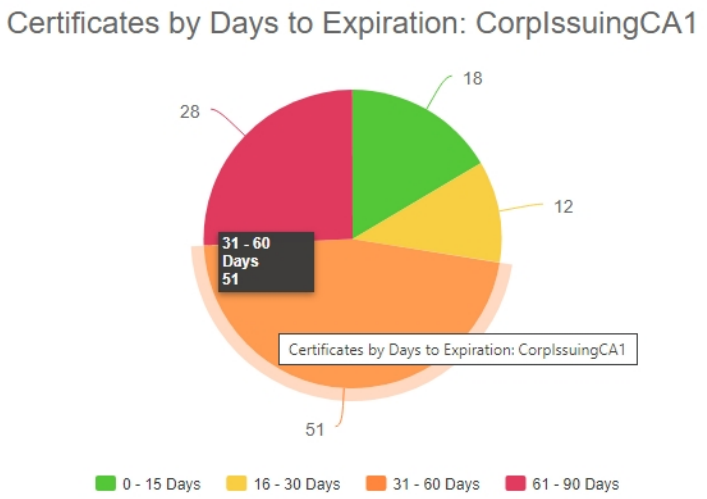


Figure 68: Example Pie Chart from Monthly Executive Report

This report takes as an input parameter the CA or CAs to report on and includes the option to report on certificates that have no associated CA. Typically, these would be certificates found via SSL scanning or inventory on certificate stores.

Note: By default, this report is configured not to appear on the top menu under Reports and can be found only in Report Manager. You can change this by modifying the *Show in Navigator* setting (see Report Manager Operations on page 122).

Note: Only CAs currently or previously configured for synchronization are available for reporting.

2.1.4.15 PKI Status for Collection

The PKI Status for Collection report is a multi-page report incorporating tables and charts that provides an overview of the status of the certificates in the selected collection.

Note: Clicking on a bar on the graph, or a section of a pie chart or line graph, will open a new window as a drill down to the certificate search grid filtered for the exact criteria of that aspect of the graph. You can return to the original report by navigating to the original report window.

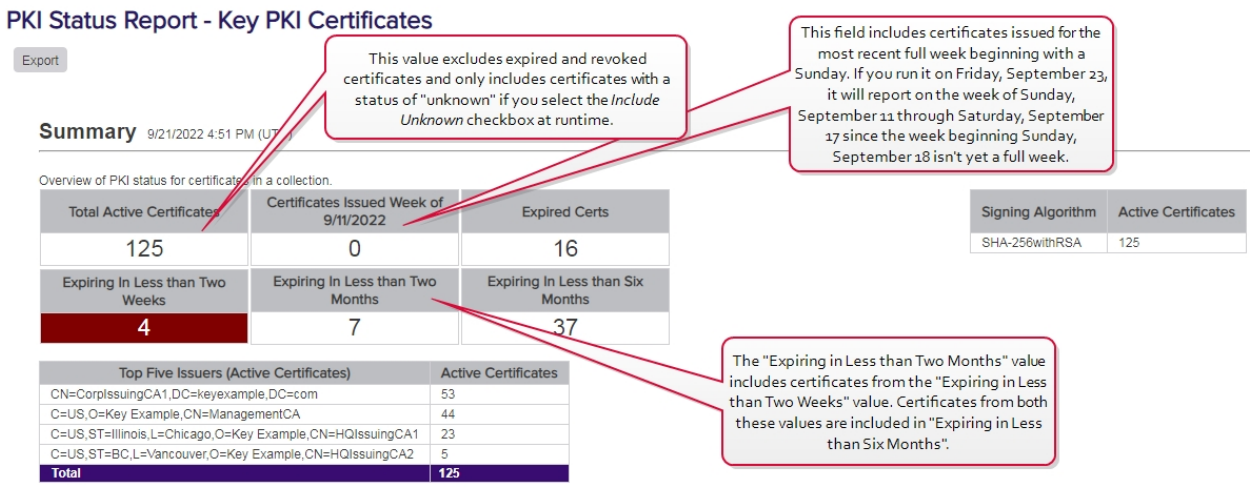


Figure 69: PKI Status for Collection Summary

The export options for the PKI Status for Collection report are Excel and PDF.

This report takes as an input parameter the certificate collection to report on, including the built-in *All Certificates* collection, and has the option to include or exclude certificates that have a status of unknown (certificates found on SSL scans and in certificate stores often have this status). The default collection is *All Certificates*, and unknown certificates are excluded by default.

Tip: If you **Save** a new certificate collection, or **Save** a change to an existing certificate collection, that change will be immediately reflected in the collection data used to display certificate collections on dashboards and reports. The data used by the dashboards and reports is stored in an intermediate table that is updated immediately. It will also continue to be updated periodically (approximately every 20 minutes by default as configured by the *Dashboard Collection Caching Interval* application setting) by the Keyfactor Command Service (see Application Settings: Console Tab on page 584).

Sections of the report include:

Summary Page

The summary page provides certificate counts for the following:

- Total number of active certificates

  This value excludes expired and revoked certificates and only includes non-expired, non-revoked certificates with an unknown state if the *Include Unknown* checkbox is selected at runtime.
- Number of certificates issued in the most recently completed week, beginning with a Sunday
- Number of expired certificates
- Number of certificates coming up for expiration within two weeks

- Number of certificates coming up for expiration within two months (including those expiring within two weeks)
- Number of certificates coming up for expiration within six months (including those expiring within two weeks and two months)
- A breakdown of the number of active certificates by signing algorithm (only the top five signing algorithms are shown)
- The top five issuers of active certificates with the number of active certificates

Next Ten Certificates to Expire Page

This table shows details of the ten certificates expiring within the shortest timeframe (for any time-frame under two years) and includes the certificate CN, issuer CN, certificate validity period in UTC time, template name, thumbprint and serial number. Grid columns may be rearranged by click-holding and dragging the grid arrangement control icon ( ) at the left of the column header. Click a column header to sort the grid by ascending values; click again to sort descending (columns already in ascending order will switch to descending on the first click). The screen will redraw when you sort. Not all columns are sortable.

PKI Health Metrics—Lifetime Remaining Page

This donut chart shows the percentage of certificates that are expired, near expiration (90% or more of lifetime used) or active and not near expiration along with a table showing the specific numbers in these categories. Hover over a segment in the donut chart to see details for that segment. Click one of the labels below the donut chart to toggle add/remove the segment on the chart. Grid columns may be rearranged by click-holding and dragging the grid arrangement control icon ( ) at the left of the column header. Click a column header to sort the grid by ascending values; click again to sort descending (columns already in ascending order will switch to descending on the first click). The screen will redraw when you sort. Not all columns are sortable.

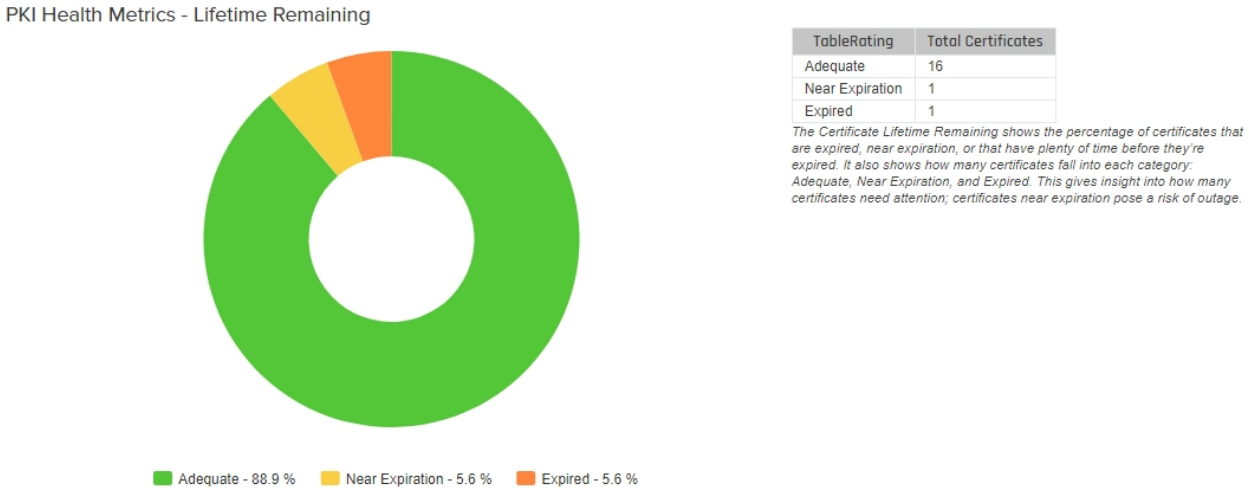


Figure 70: PKI Status for Collection Lifetime Remaining

PKI Health Metrics—Algorithm Strength

This donut chart shows the percentage of certificates (active and expired) with strong (SHA2 and SSA), weak (SHA1) or critically weak (MD5 and older) signature algorithms along with a table showing the specific numbers in these categories. Hover over a segment in the donut chart to see details for that segment. Click one of the labels below the donut chart to toggle add/remove the segment on the chart. Grid columns may be rearranged by click-holding and dragging the grid arrangement control icon () at the left of the column header. Click a column header to sort the grid by ascending values; click again to sort descending (columns already in ascending order will switch to descending on the first click). The screen will redraw when you sort. Not all columns are sortable.

PKI Health Metrics—RSA Key Strength

This donut chart shows the percentage of certificates (active and expired) with strong (2048+), weak (1024-2047), and critically weak (<1024) RSA keys along with a table showing the specific numbers in these categories. Hover over a segment in the donut chart to see details for that segment. Click one of the labels below the donut chart to toggle add/remove the segment on the chart. Grid columns may be rearranged by click-holding and dragging the grid arrangement control icon () at the left of the column header. Click a column header to sort the grid by ascending values; click again to sort descending (columns already in ascending order will switch to descending on the first click). The screen will redraw when you sort. Not all columns are sortable.

Certificates by Signing Algorithm

This donut chart shows the percentage of active certificates broken down by signing algorithm (RSA SHA-1, RSA SHA-256, etc.) along with a table showing the specific numbers in these categories. Hover over a segment in the donut chart to see details for that segment. Click one of the labels below the donut chart to toggle add/remove the segment on the chart.

Top Certificate Issuers

This donut chart shows the percentage of certificates (active and expired) broken down by the top five issuers plus an *other* bucket along with a table showing the specific numbers in these categories. Hover over a segment in the donut chart to see details for that segment. Click one of the labels below the donut chart to toggle add/remove the segment on the chart. Grid columns may be rearranged by click-holding and dragging the grid arrangement control icon () at the left of the column header. Click a column header to sort the grid by ascending values; click again to sort descending (columns already in ascending order will switch to descending on the first click). The screen will redraw when you sort. Not all columns are sortable.

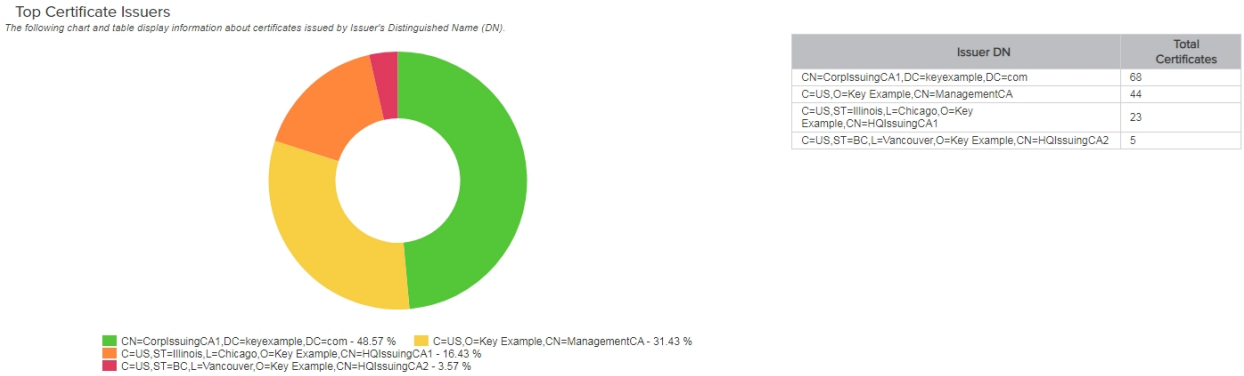


Figure 71: PKI Status for Collection Top Issuers

Certificates Issued in Previous 10 Weeks

This bar chart shows the number of certificates (active and expired) issued per week for the ten weeks leading up to and through the full week prior to the run date of the report. Hover over a bar to see the number of issued certificates for the week with that date.

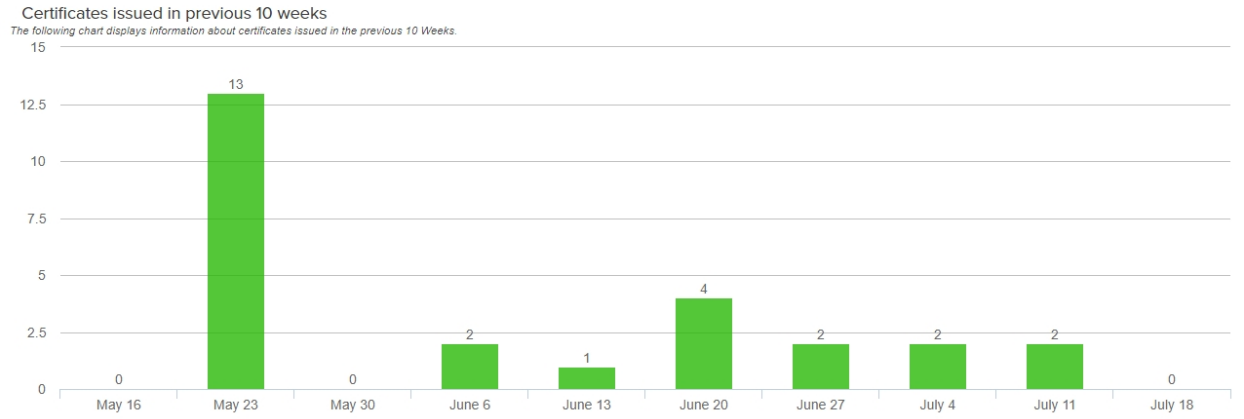


Figure 72: PKI Status for Certificates issued in previous 10 weeks

Certificates Issued in Previous 12 Months

This bar chart shows the number of certificates (active and expired) issued per month for the twelve months leading up to and through the full month prior to the run date of the report, broken down by internally issued certificates (from sources managed by Keyfactor Command such as synchronization of CAs in the primary forest and any trusted forests, any certificate vendors synced using a Keyfactor gateway, and any CAs synced using the remote CA agent) and externally issued certificates (from sources not managed by Keyfactor Command such as certificates located during SSL scans or uploaded using the Add Certificate option). Hover over a bar to see the number of issued certificates for that month and source. Click one of the labels below the chart to toggle add/remove the segment on the chart.

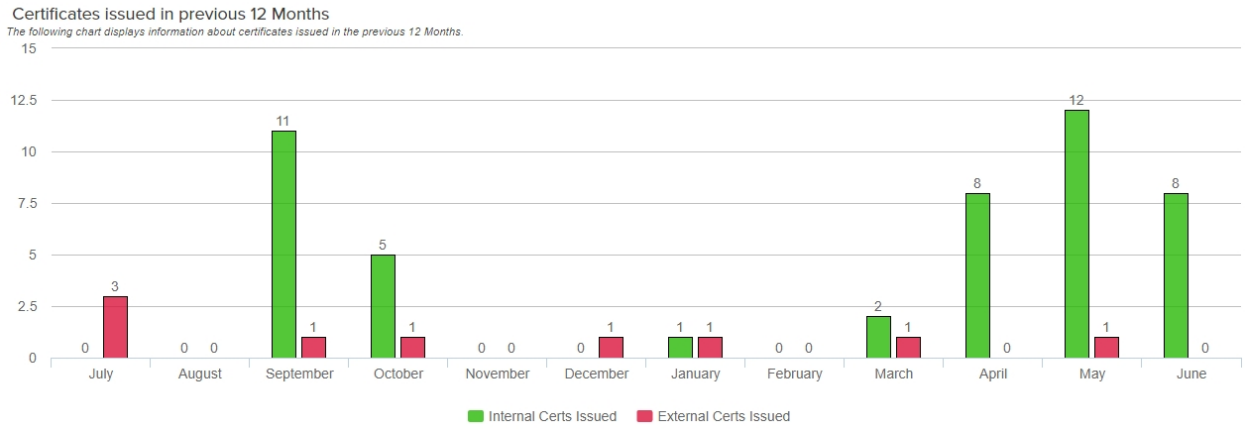


Figure 73: PKI Status for Certificates issued in previous 12 months

Weak RSA Certificates

This table shows details of the certificates with weak (under 2048) RSA keys and includes the certificate CN, issuer CN, certificate validity period in UTC time, key size, thumbprint and serial number. A maximum of 1000 certificates is shown. Grid columns may be rearranged by click-holding and dragging the grid arrangement control icon ( ) at the left of the column header. Click a column header to sort the grid by ascending values; click again to sort descending (columns already in ascending order will switch to descending on the first click). The screen will redraw when you sort. Not all columns are sortable.

Deprecated Signing Algorithms

This table shows details of the certificates with deprecated (MD5 and older) signing algorithms and includes the certificate CN, issuer CN, certificate validity period in UTC time, signing algorithm, thumbprint and serial number. A maximum of 1000 certificates is shown. Grid columns may be rearranged by click-holding and dragging the grid arrangement control icon ( ) at the left of the column header. Click a column header to sort the grid by ascending values; click again to sort descending (columns already in ascending order will switch to descending on the first click). The screen will redraw when you sort. Not all columns are sortable.

Self-Signed Certificates

This table shows details of the certificates that are self-signed or root CA certificates and includes the certificate DN, certificate validity period in UTC time, thumbprint and serial number. A maximum of 1000 certificates is shown. Grid columns may be rearranged by click-holding and dragging the grid arrangement control icon ( ) at the left of the column header. Click a column header to sort the grid by ascending values; click again to sort descending (columns already in ascending order will switch to descending on the first click). The screen will redraw when you sort. Not all columns are sortable.

2.1.4.16 Revoked Certificates in Certificate Stores

The Revoked Certificates in Certificate Stores report displays a table of all certificates that have been revoked, either in Keyfactor Command or externally, that are found in at least one certificate store or SSL scan location, and for which the revocation effective date is less than or equal to the date and time when the report is run (not in the future). The report is included in the report manager Certificate Locations and Certificate Lifecycle categories.

The export options for the Revoked Certificates in Certificate Stores report are CSV and Excel.

The report table includes these fields:

- Certificate CN

  The common name of the certificate.
- Thumbprint

  The thumbprint of the certificate.
- User

  The username (DOMAIN\username format) of the user who revoked the certificate.
- Expiration Date (UTC)

  The date on which the certificate expires.
- Issued Date (UTC)

  The date on which the certificate became valid (typically the issuance date).
- Template Name

  The certificate template used to issue the certificate.
- SSL Location

  The DNS name(s) resolved for the IP address(es) where the certificate was found on an SSL scan. Due to query constraints, the maximum length of text allowed in each of these fields is 10,000 characters.
- Cert Store Location

  The name(s) of the server(s) on which the certificate is found in one or more certificate stores and the location of the certificate store(s). The format of this value will vary depending on the type of certificate store. Due to query constraints, the maximum length of text allowed in each of these fields is 10,000 characters.
- Revocation Date (UTC)

  The date on which the certificate was revoked in UTC.
- Revocation Reason

  The reason given for the certificate revocation.
- Revocation Comment

  The comment entered at revocation.

Column handling on this report grid has the following features:

- To change the width of a column of the report, hover over the triangle of dots on the right side of the selected column header (). Click, hold and drag the triangle to change the width of the column.
- To rearrange columns on the report display, hover over the rectangle of dots on the left side of the selected column header (). Click, hold, and drag the rectangle to move the column to your selected location.
- Most columns can be sorted in ascending order by clicking on the header of the column. Click the column header again to reverse the sort order. When a column is sorted, a caret will appear at the end of the column name showing the direction of the sort. Lack of a triangle indicates the report is sorted by the default column and order.

This report takes as an input parameter the certificate collection to report on, including the built-in *All Certificates* collection. The default is *All Certificates*.

Tip: If you **Save** a new certificate collection, or **Save** a change to an existing certificate collection, that change will be immediately reflected in the collection data used to display certificate collections on dashboards and reports. The data used by the dashboards and reports is stored in an intermediate table that is updated immediately. It will also continue to be updated periodically (approximately every 20 minutes by default as configured by the *Dashboard Collection Caching Interval* application setting) by the Keyfactor Command Service (see Application Settings: Console Tab on page 584).

Note: By default, this report is configured not to appear on the top menu under Reports and can be found only in Report Manager. You can change this by modifying the *Show in Navigator* setting (see Report Manager Operations on page 122).

Note: This report is limited to a maximum of 100,000 revoked certificates in certificate stores on which to report. Selecting a certificate collection containing more certificates than this will result in an error.

2.1.4.17 SSH Key Usage

The SSH Key Usage report shows a table which displays a list of SSH keys that have not been used to log on in the given minimum number of days.

The export options for the SSH Key Usage report are CSV and Excel.

The grid includes:

- Key Fingerprint
  The fingerprint of the SSH public key.
- Discovered Date
  The date and time (in local server time) on which the SSH key was discovered.
- Date Last Used
  The date and time (in local server time) on which the SSH key was last used.
- Key Length
  The key length of the SSH public key.
- Logon Username
  The Linux logon username associated with the key.
- Logon Server
  The IP address of the Linux server last used to logon.

This report takes as an input parameter; number of *Days Since Last Used*. You must select a number between 0 and 100.

Note: By default, this report is configured not to appear on the top menu under Reports and can be found only in Report Manager. You can change this by modifying the *Show in Navigator* setting (see Report Manager Operations on page 122).

2.1.4.18 SSH Keys by Age

The SSH Keys by Age report shows one or more table(s) with detailed information for SSH keys generated in Keyfactor Command broken down by age—as defined by the *Key Lifetime (days)* application setting (see Application Settings: SSH Tab on page 604).

The export options for the SSH Keys by Age report are PDF and Excel.

The report aging categories are:

- Stale keys (within the last 4 weeks)
- Keys less than 1 week from being stale
- Keys less than 4 weeks from being stale
- Keys less than 8 weeks from being stale
- Keys less than 6 months from being stale
- Keys less than 12 months from being stale

A table is only shown if an SSH key with one of the selected key types matches the age window. An SSH key appears only in one table, so, for example, a key that will become stale within 4 weeks and appears in the 4-week table does not also appear as becoming stale within the 8-week table.

The grid includes:

- Account Name
  For user keys, the Active Directory user account associated with the key being reported on. For service account keys, the username and client hostname entered when the service account key was created (e.g. myapp@appsrvr.keyexample.com).
- Creation Date
  The date (in UTC time) on which the SSH key was created.
- Fingerprint
  The fingerprint of the SSH public key.
- Key Type
  The key type of the SSH public key.
- Key Length
  The key length of the SSH public key.
- Associated Logons
  The number of Linux logons associated with the SSH public key.

This report takes as an input parameter the SSH Key Types to include in the report. You must select at least one key type using the **Select SSH Key Types** button.

Note: By default, this report is configured not to appear on the top menu under Reports and can be found only in Report Manager. You can change this by modifying the *Show in Navigator* setting (see Report Manager Operations on page 122).

2.1.4.19 SSH Keys with Root Logon Access

The SSH Keys with Root Logon Access report shows a list of SSH public keys found associated with root logon authorized_keys files on servers managed with the SSH orchestrator. Holders of the matching private keys for these public keys can gain root access without providing the root password.

The export options for the SSH Keys with Root Logon Access report are CSV and Excel.

The grid includes the fields:

- Account Name
  The Active Directory user account associated with the key found to have root access on the target machine, if any. This field will only be populated for keys created in Keyfactor Command.
- Fingerprint
  The fingerprint of the SSH public key found associated with the root logon on the target machine.
- Hostname
  The host name of the server on which the root logon was found to have an SSH public key providing logon access.
- Creation Date
  The date (in UTC time) on which the SSH key was created. This field will only be populated for keys created in Keyfactor Command.
- Date Found
  The date (in UTC time) on which Keyfactor Command found the root logon SSH public key on the target server. This field will only be populated for keys discovered outside of Keyfactor Command (as opposed to created in Keyfactor Command).
- Key Type
  The key type of the SSH public key found to have root access on the target machine.
- Key Length
  The key length of the SSH public key found to have root access on the target machine.

The input parameter for this report is:

- The start date and end date range for the report. This is the date range during which SSH keys that allow root logon were created or discovered by Keyfactor Command. The default start date is one month prior to the current date. The default end date is the current date, meaning only SSH keys with root access discovered or created within the last month will be included in the report.
- The SSH Key Types to include in the report.

Note: By default, this report is configured not to appear on the top menu under Reports and can be found only in Report Manager. You can change this by modifying the *Show in Navigator* setting (see Report Manager Operations on page 122).

2.1.4.20 SSH Trusted Public Keys with No Known Private Keys

The SSH Trusted Public Keys with No Known Private Keys report shows a list of SSH public keys found in authorized_keys files on servers managed with the SSH orchestrator that do not have a matching private key in Keyfactor Command.

The export options for the SSH Trusted Public Keys with No Known Private Keys report are CSV and Excel.

The grid includes:

- Logon Name
  The Linux user account associated with the SSH public key found on the target machine.
- Fingerprint
  The fingerprint of the SSH public key found associated with the referenced logon on the target machine.
- Date Found
  The date (in UTC time) on which Keyfactor Command found the SSH public key on the target machine.
- Key Type
  The key type of the SSH public key found on the target machine.
- Key Length
  The key length of the SSH public key found on the target machine.
- Hostname
  The host name of the server on which the root logon was found to have an SSH public key providing logon access.
- Server Group
  The server group to which the server on which the root logon was found belongs.

The input parameters for this report are:

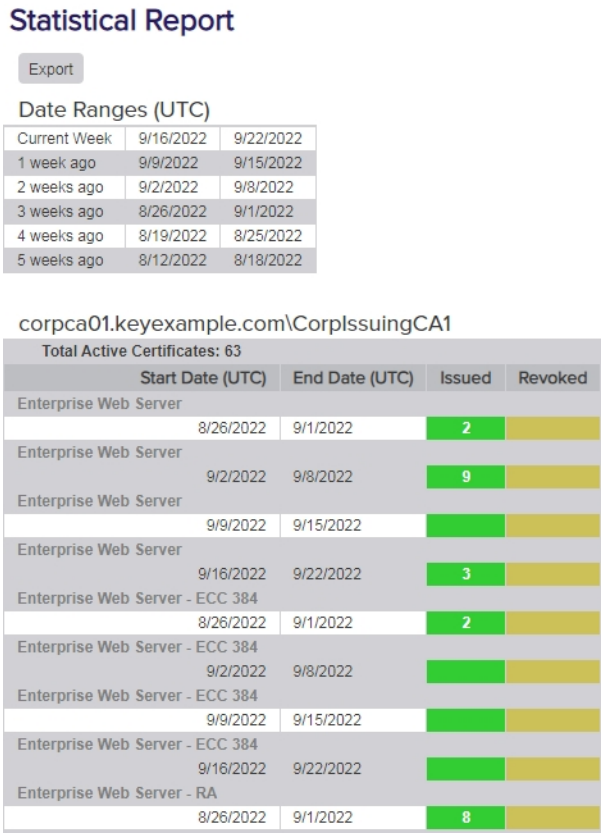
- The start date and end date range for the report. This is the date range during which SSH keys were discovered by Keyfactor Command. The default start date is one month prior to the current date. The default end date is the current date, meaning only SSH keys that have no matching private key discovered within the last month will be included in the report.
- The SSH Key Types to include in the report. You must select at least one key type using the **Select SSH Key Types** button.

Note: By default, this report is configured not to appear on the top menu under Reports and can be found only in Report Manager. You can change this by modifying the *Show in Navigator* setting (see Report Manager Operations on page 122).

2.1.4.21 Statistical Report

The Statistical Report shows the number of issued, revoked, and failed (includes denied) certificates for a user-definable period of time leading up to a user-definable date broken down by CA, certificate template and reporting period length (day, week or month). The report includes sections titled "No Template Associated" for certificates with no associated template. This may be the case with certificates issued from a standalone CA as well as select failed certificate requests from enterprise CAs.

The export options for the Statistical Report are PDF and Excel.



Statistical Report

Export

Date Ranges (UTC)

Current Week	9/16/2022	9/22/2022
1 week ago	9/9/2022	9/15/2022
2 weeks ago	9/2/2022	9/8/2022
3 weeks ago	8/26/2022	9/1/2022
4 weeks ago	8/19/2022	8/25/2022
5 weeks ago	8/12/2022	8/18/2022

corpca01.keyexample.com\CorpIssuingCA1

Total Active Certificates: 63

	Start Date (UTC)	End Date (UTC)	Issued	Revoked
Enterprise Web Server				
	8/26/2022	9/1/2022	2	
Enterprise Web Server				
	9/2/2022	9/8/2022	9	
Enterprise Web Server				
	9/9/2022	9/15/2022		
Enterprise Web Server				
	9/16/2022	9/22/2022	3	
Enterprise Web Server - ECC 384				
	8/26/2022	9/1/2022	2	
Enterprise Web Server - ECC 384				
	9/2/2022	9/8/2022		
Enterprise Web Server - ECC 384				
	9/9/2022	9/15/2022		
Enterprise Web Server - ECC 384				
	9/16/2022	9/22/2022		
Enterprise Web Server - RA				
	8/26/2022	9/1/2022	8	

Figure 74: Example Portion of the Statistical Report

The input parameters for this report are:

- The evaluation date of the reporting period. The default is the current date.
- The number of periods to report on. The default is six.

  Note: A maximum of 100 periods may be selected (e.g. 100 weeks).

- The period length—day, week or month. The default is week.

Tip: The *Total Active Certificates* count for each CA section in the report includes all certificates issued by that CA which are still active (not revoked and not expired), not just those issued in the time period for the report.

2.1.4.22 Report Manager

The Report Manager is used to run reports and manage existing reports, including scheduling delivery of reports. The Report Manager page shows all the available reports, not just those that have been configured to appear on the Management Portal top menu under *Reports*. Built-In Reports and Custom Reports are shown on separate tabs on the Report Manager page. Built-In reports have been organized into categories to allow you to filter the search results on the Report Manager grid by category of report.

With the Report Manager, custom Logi Analytics reports or custom reports from other external reporting solutions can be added into the portal to allow for easy running and scheduling. If you would like assistance creating a custom report in the new reporting engine, Logi Analytics, or displaying a custom report in the Report Manager, please contact your Client Success representative.

Tip: Be sure to check the filter on the category if you are not seeing all of the reports you expect to see. The default filter is *All* unless you have favorited some reports, in which case it is *Favorite*.

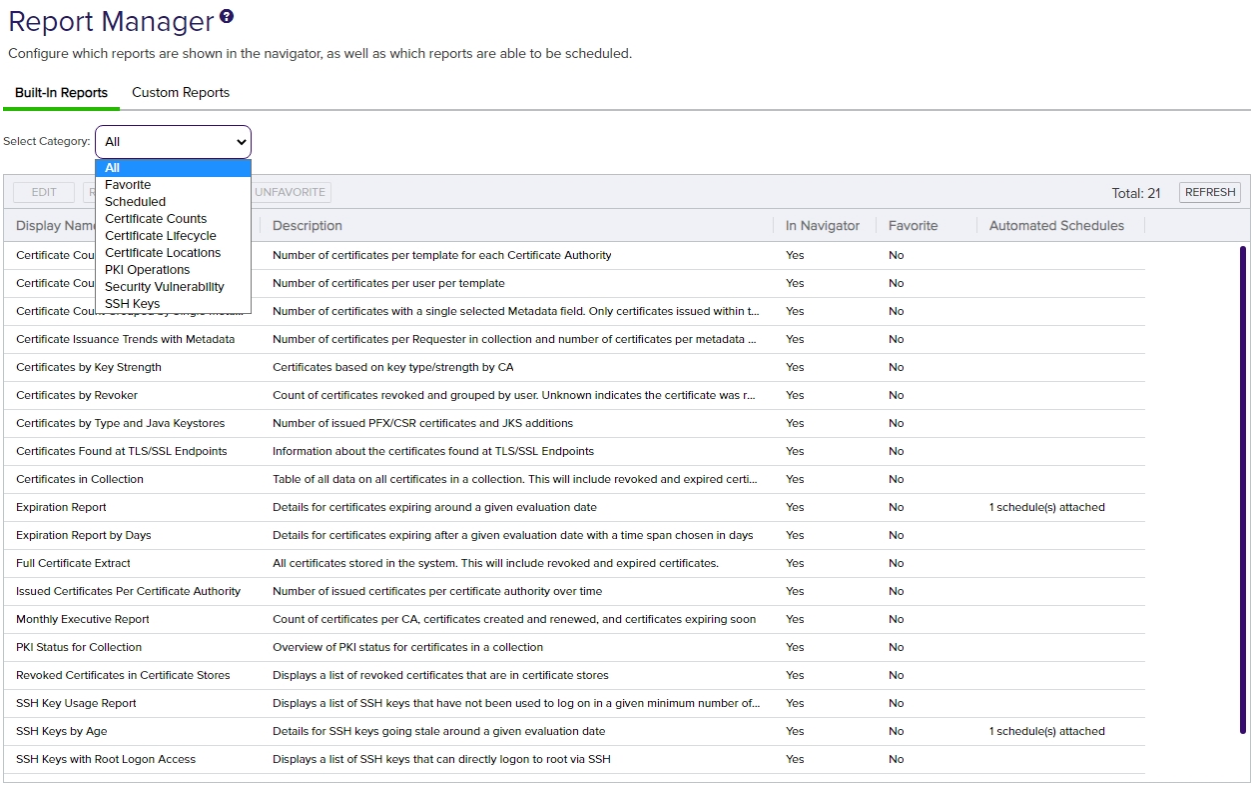


Figure 75: Report Manager Grid

Tip: If you **Save** a new certificate collection, or **Save** a change to an existing certificate collection, that change will be immediately reflected in the collection data used to display certificate collections on dashboards and reports. The data used by the dashboards and reports is stored in an intermediate table that is updated immediately. It will also continue to be updated periodically (approximately every 20 minutes by default as configured by the *Dashboard Collection Caching Interval* application setting) by the Keyfactor Command Service (see Application Settings: Console Tab on page 584).

Report Manager Operations

From the Report Manager you can run reports on demand, edit reports (modify how a report displays, change the parameter definitions and add or change the schedule(s) used to run the report), or delete reports. From the top grid menu you can also quickly change the *Favorite* setting for a report.

Run a Report

You can run a report on demand from the Report Manager page.

1. In the Management Portal, browse to *Reports > Report Manager*.
2. On the Report Manager page, highlight the report you wish to run in the grid and click **Run Report** from the top grid menu or the right click menu.
3. Populate the parameters as desired (see Parameters Tab on page 125 for more information on parameters).
4. Click **Generate**. The report will display immediately in the open window. The report can be exported to Excel, PDF or CSV, as available for that report, via the **Export** button at the end of the report.

Editing a Report and Scheduling a Report for Delivery

You can modify how a report displays, change the parameter definitions for running a report and add or change the schedule(s) used to deliver the report.

To edit an existing report:

1. In the Management Portal, browse to *Reports > Report Manager*.
2. On the Report Manager page, highlight the report you wish to modify in the grid and click **Edit** from the grid menu or the right click menu.
3. In the Report Manager dialog, edit the available options as needed.
4. Click **OK** to save the new or changed report details.

Details Tab

The most common edit to make on an existing report would be to check or uncheck the **Show in Navigator** box to add or remove the report from display on the Reports top menu, or to check or uncheck the **Favorites** box on the **Details** tab. The **Ignore Renewed Certificates** box will be available for reports that use collections to enable de-duplication (see the tip below). The **Uses Collection** box is for information only. It will be grayed out and checked for reports that use collections.

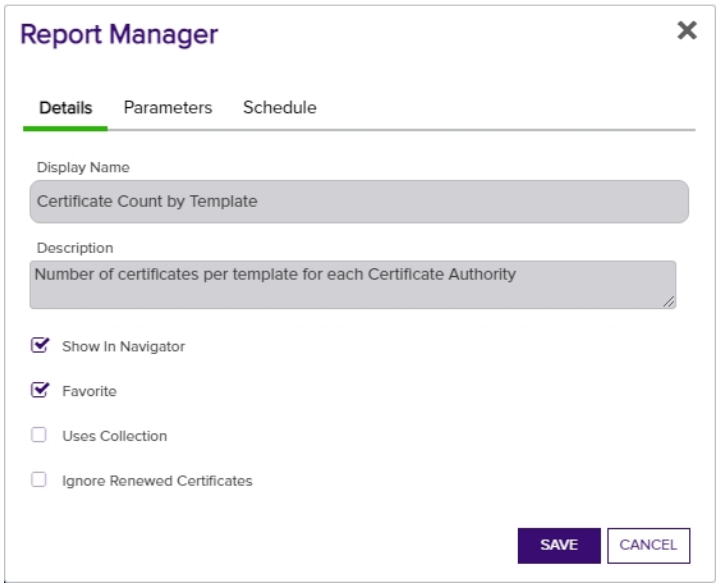


Figure 76: Edit a Report in Report Manager Details Tab

Tip: When de-duplication is enabled for a report, the report results will include only the most recently issued certificate if there is more than one certificate that matches the de-duplication criteria. De-duplication is enabled for a report by checking the *Ignore Renewed Certificates* box on the Details tab of the report configuration. De-duplication can only be enabled for reports that use certificate collections—the *Uses Collection* box on the Details tab. The *Uses Collection* setting is not user-configurable.
De-duping is configured on a certificate collection by setting the *Ignore renewed certificate results by* option when saving a certificate collection (see Saving Search Criteria as a Collection on page 40). Certificate collections may be configured to be de-duplicated based on the certificate common name, distinguished name, or principal name (or not at all). Only certificates that share all the EKUs (e.g. Client Authentication and Server Authentication) as well as the same CN, DN or UPN will be eliminated as duplicates. If a certificate has more than one EKU and at least one EKU does not match an otherwise similar certificate with matching CN, DN or UPN, it will not be eliminated.

For example, if the de-duplication logic was set to DN and the report would include these two certificates:

- Certificate one:
  - DN: CN=apps-srvr14.keyexample.com,OU=IT,O=Key Example, Inc.,L=Chicago,ST=IL,C=US
  - EKUs: Server Authentication
- Certificate two:
  - DN: CN=apps-srvr14.keyexample.com,OU=IT,O=Key Example, Inc.,L=Chicago,ST=IL,C=US
  - EKUs: Server Authentication

- Issued Date: December 1, 2020
- Expiration Date: January 1, 2022

- Issued Date: December 15, 2020
- Expiration Date: December 14, 2021

The de-duplication logic would be triggered because the DNs and EKUs match. The report would include certificate two and leave out certificate one. Notice that certificate two is retained even through certificate one expires after certificate two. This is because certificate two was issued after certificate one.

Now imagine that the de-duplication logic is set to CN and the report would include these two certificates:

- Certificate one:
  - DN: CN=appsrvr14.keyexample.com,OU=IT,O=Key Example, Inc.,L-L=Chicago,ST=IL,C=US
  - EKUs: Server Authentication
  - Issued Date: December 1, 2020
  - Expiration Date: January 1, 2022
- Certificate two:
  - DN: CN=appsrvr14.keyexample.com,OU=HR,O=Key Example, Inc.,L-L=Chicago,ST=IL,C=US
  - EKUs: Server Authentication, Client Authentication
  - Issued Date: December 15, 2020
  - Expiration Date: December 14, 2021

Although the DNs for these certificates do not match, the CNs still do, so this matches the de-duplication logic of CN. However, the EKUs for these two certificates do not match, since only one of them includes Client Authentication. In this case, both certificates would appear on the report.

Parameters Tab

The Parameters tab will display all of the parameters for that specific report and allow you to configure default values to be used when the report is run from the Report Manager **Run Report** action button and what values default when adding a new schedule. You may also change the display name and description of the parameter.

To edit a parameter, select the **Parameters** tab, highlight the desired parameter in the parameters grid and click **Edit**, or double click the row. The *Parameters* dialog will open. Only those fields which can be edited will be enabled on the parameters details page. A change of the **Display Name** will change the name of parameter on the *Parameters* tab . A change of the **Description** will change the name of the description field on the *Schedule* tab. A change to the **Default Value** will define the value to use when the report is run from the Report Manager **Run Report** action button and what values default when adding a new schedule.

Tip: Some reports parameters use the **Add**/**Edit** button at the bottom of the dialog to open a Default Value dialog for to populate that parameter.

Note: The parameter fields will vary depending on the report selected. The parameters shown correspond to the specific parameters for each report. For more information on the parameters for a specific report, see the individual report under Reports on page 86.

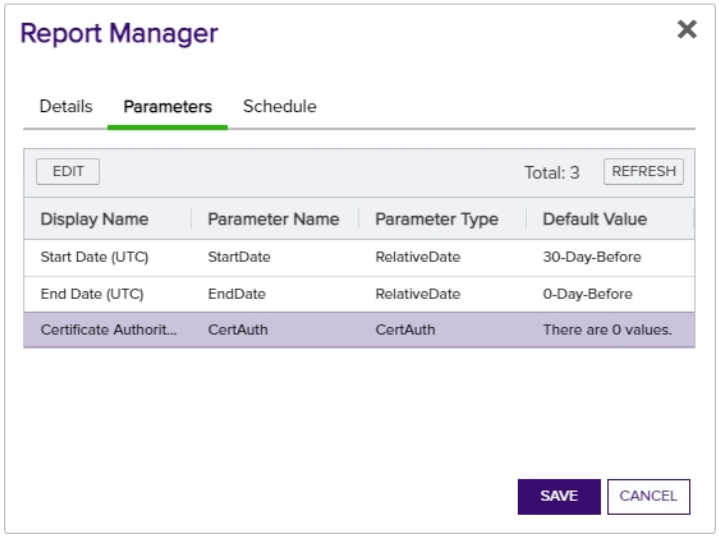


Figure 77: Edit a Report in Report Manager Parameters Tab

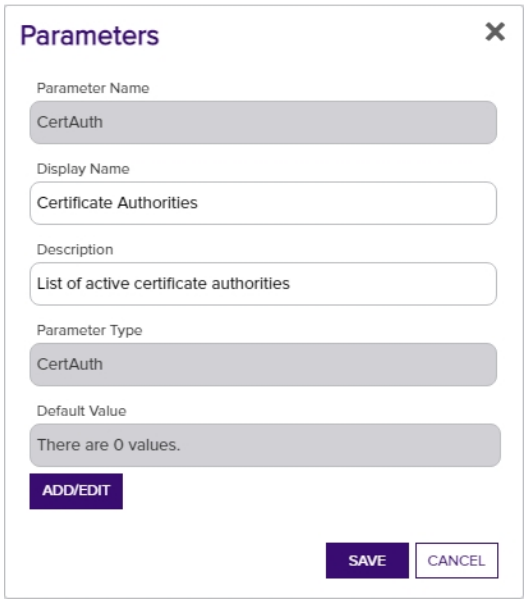


Figure 78: Report Manager Parameters Tab: Parameter Details

Schedule Tab

To add, edit, or delete a report delivery schedule, select the **Schedule** tab and choose the desired action. Any scheduled reports will appear on the schedule tab page. You can create multiple schedules with different parameters and recipients for the same report.

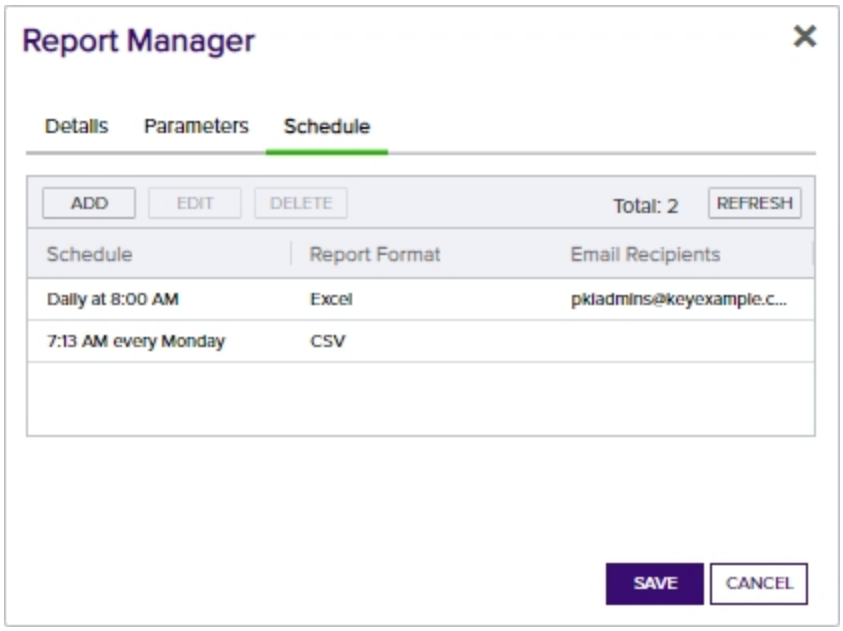


Figure 79: Edit a Report in Report Manager Schedule Tab

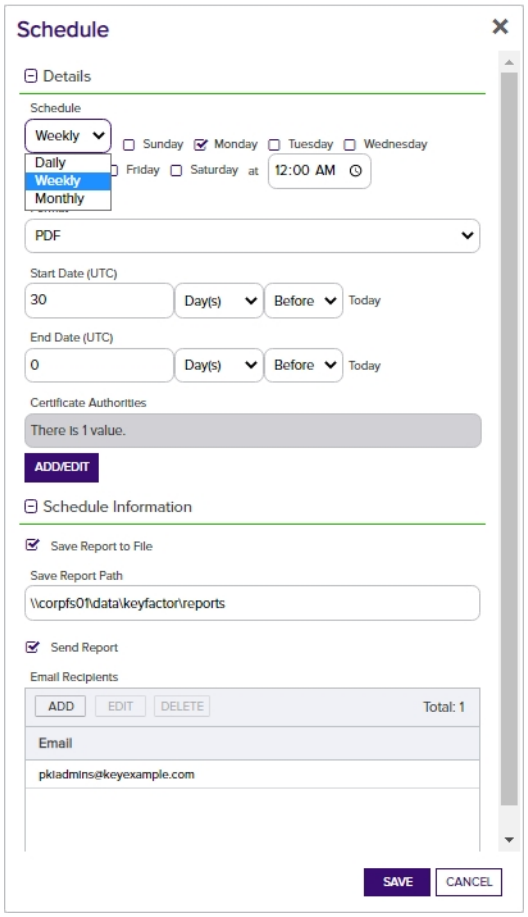


Figure 80: Edit a Report in Report Manager Schedule Tab - Add/Edit page

Note: Report scheduling is limited by collection permissions. Users in roles that have *Reports: Read and Modify* permissions will also need to have *Read* collection permissions on individual collections or global *Read* permissions for Certificates to have the ability to add, edit and delete schedules associated with collections. Any users without global *Read* permissions for Certificates will not have access to add, edit and delete schedules for any collections for which they do not have collection *Read* permissions in addition to *Reports* permissions.

Details section

- **Schedule**: Choose the schedule by selecting Daily, Weekly or Monthly from the dropdown, then choosing the day or date, and the time to run the report.

- **Report Format**: The available report formats are PDF, Excel and CSV*.

  Note: *The CSV format is only available on reports that contain all the data within a single section (such as the Certificates in Collection report) rather than broken out into multiple sections (such as the Expiration Report).

  Note: *CSV format is not available for custom reports with multiple tables.

- **Dynamic Parameters**:

  Depending on the parameters specific to the report, you will use either a entry field, a dropdown or click the **Add**/**Edit** to open the selection window for the report parameters for the specific schedule you are working on.

  - Some reports are based on a certificate collection, so one must be selected.
  - Some reports allow you to set an evaluation date for the report other than the current date so that you can, for example, run an Expiration Report time shifted to 1 month in the future to see what the expiration picture will look like in a month's time or compare last year to this year.
  - Some reports allow you to include custom metadata (see Certificate Metadata on page 646) in the report output.
  - Some reports allow you to select specific templates or CAs for reporting.

Schedule Information Section

- **Save Report to File**: You can choose to save your report to file by ticking the **Save Report to File** box, in which case you must provide a network path to which the file will be written in the **Save Report Path (relative to the server)** field. You will be given a warning message if the network path cannot be resolved. Although the record can still be saved with a path that doesn't resolve correctly, the report may fail to run if the path still does not resolve at the time the report runs.

  Note: The path for saved reports must be provided in UNC format (\\server-name\sharename\path) and must be accessible from the Keyfactor Command administration server. In addition:

  - Do not use a trailing "\" in the report path.
  - Ensure that the service account for the Keyfactor Command Service has permission to write to the location where you want the outputted report to be saved.

- When scheduling a report, schedule it for at least 10 minutes in advance of the current time if you wish it to run soon. If you want to run it faster than that, the Keyfactor Command Service will need to be restarted.

- **Send Report**: You can choose to deliver your report via email by ticking the **Send Report** box, in which case you must provide at least one recipient in the **Recipients** field at the bottom of the dialog.

Tip: For an explanation of the parameters specific to each report, see the section in the documentation for that specific report under Reports on page 86.

Important: Scheduled reports will not run if the Keyfactor Command Service is stopped.

Deleting a Report

To delete a report

1. In the Management Portal, browse to *Reports > Report Manager*.
2. On the Report Manager page, highlight the report you wish to delete in the grid and click **Delete** from the right-click menu.

Note: Only user-defined reports can be deleted. Built-in reports cannot be deleted. If you prefer not to see a built-in report, you may opt to remove the report from the menu by unchecking the **Show in Navigator** option.

2.1.5 Enrollment

The enrollment function in the Keyfactor Command Management Portal allows PKI administrators to request certificates by either submitting a certificate signing request (see CSR Enrollment on the next page) or by directly entering request information to receive a certificate delivered as a PFX file (see PFX Enrollment on page 141). The certificate file is available for immediate download via the browser or installation into a certificate store providing that the enrollment succeeds and the template used does not require manager approval. An option is also provided to generate a certificate signing request within Keyfactor Command. When you do this, the private key generated as part of the CSR generation process is stored—encrypted—in the Keyfactor Command database (see CSR Generation on page 138).

Note: As of Keyfactor Command version 10, enrollment (PFX and CSR), renewal, and revocation requests all flow through Keyfactor Command workflow. This will result in no changes to the enrollment, renewal, and revocation user experience unless customizations have been added in workflow (see Workflow Definitions on page 218).

See Application Settings: Enrollment Tab for configuration settings that apply to the enrollment functions in the Keyfactor Command Management Portal. Some enrollment functions are also affected by template settings. See Configuring System-Wide Settings on page 355 and Configuring Template Options on page 360 for more information.

Note: The app pool service account must be set with permissions on the CA itself, in order to enroll via the CA in Keyfactor Command.

Important: Direct enrollment (without use of a Keyfactor CA gateway) is only supported for CAs in the forest in which Keyfactor Command is installed and any forests in a two-way trust with this forest. To do a cross-forest enrollment (with a forest in a two-way trust with the Keyfactor Command forest), Keyfactor Command requires that the root and intermediate CA certificates from the trusted forest are installed in the trusted root/intermediate stores in the Keyfactor Command server.

2.1.5.1 CSR Enrollment

The certificate signing request (CSR) enrollment page provides the ability to submit a CSR and download the resulting certificate.

Important: Before you can use the CSR enrollment function, you must configure at least one template for enrollment by checking the **CSR Enrollment** box under **Allowed Enrollment Types** in the certificate template details. See Configuring Template Options on page 360.

Note: As of Keyfactor Command version 10, enrollment (PFX and CSR), renewal, and revocation requests all flow through Keyfactor Command workflow. This will result in no changes to the enrollment, renewal, and revocation user experience unless customizations have been added in workflow (see Workflow Definitions on page 218).

To request a certificate via CSR:

1. Generate a CSR. This can be done within the target application (e.g. Microsoft IIS), by using a tool such as certutil or OpenSSL, or by using the Keyfactor Command CSR generation tool (see CSR Generation on page 138).
2. In the Management Portal, browse to *Enrollment > CSR Enrollment*.
3. Paste your CSR into the **CSR Content** text area, with or without the BEGIN REQUEST/END REQUEST delimiters.

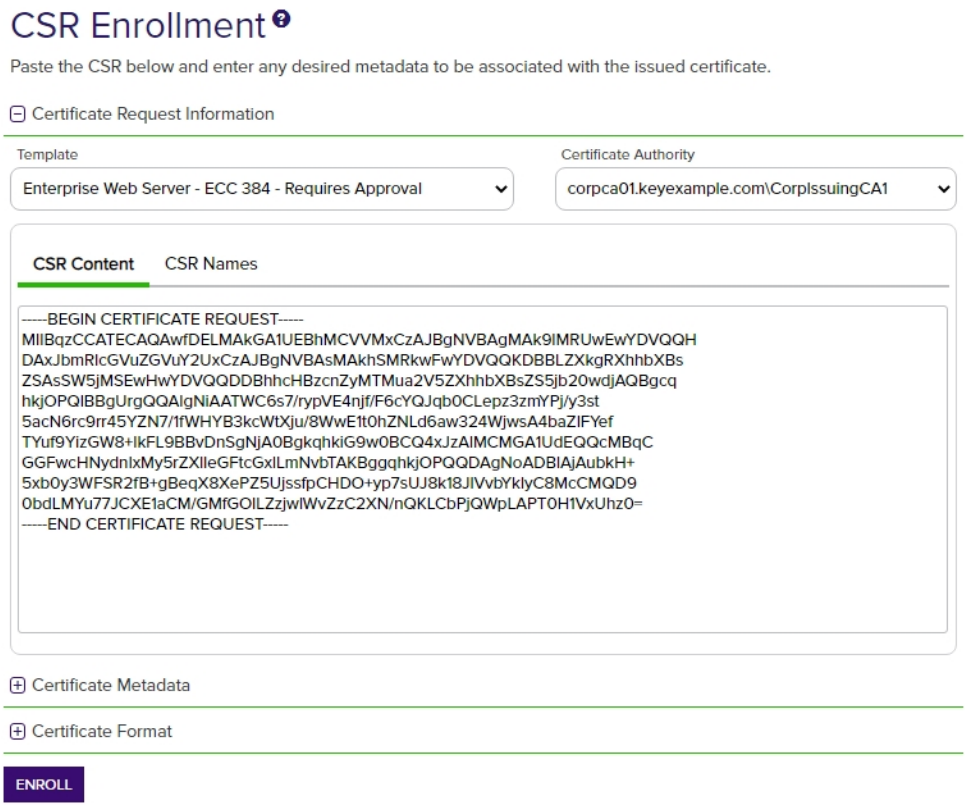


Figure 81: CSR Enrollment: CSR Content

4. The CSR contents will be parsed, and you will automatically be switched to the **CSR Names** view. Review the data to be sure it is as expected.

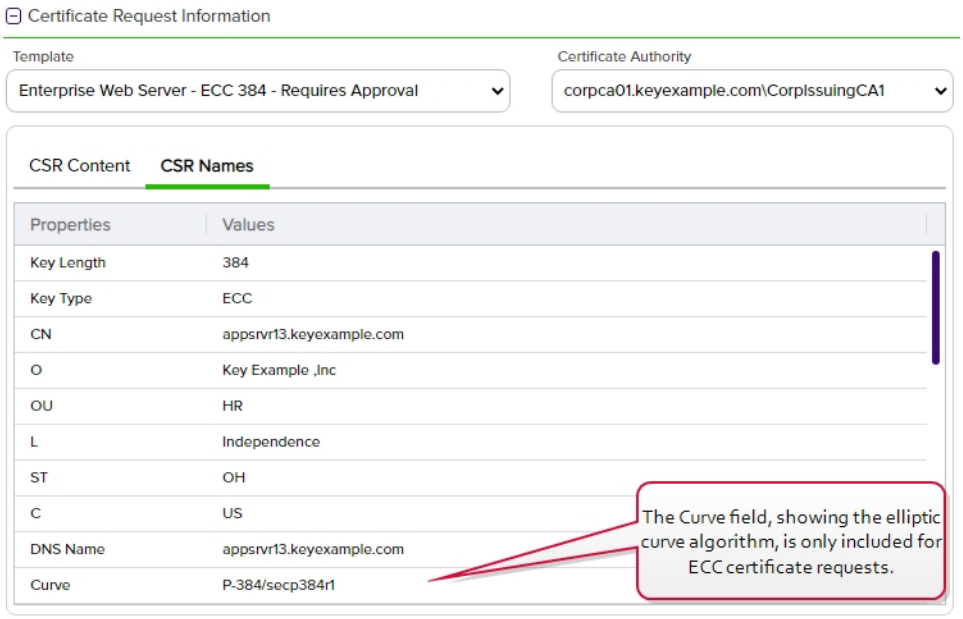


Figure 82: CSR Enrollment: CSR Names

Note: If a system-wide or template-level regular expression exists for a subject part or SAN, and the subject part or SAN is left blank, the regular expression will be applied to an empty string for that part. For example, if you have a regular expression on organization, but do not supply an organization, the regular expression will be applied to a blank string as if that were supplied as the organization.

5. If you are enrolling from an enterprise CA, select a certificate template from the **Template** drop-down. The templates are organized by configuration tenant (formerly known as forest). If you have multiple configuration tenants and templates with similar names, be sure to select the template in the correct configuration tenant.

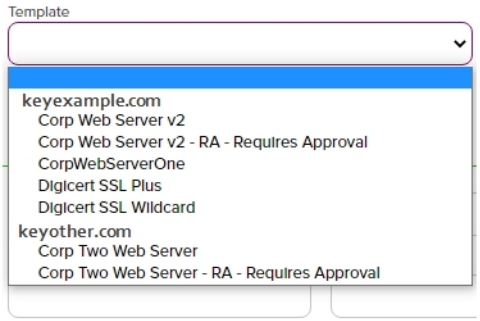


Figure 83: Select a Certificate Template

Note: When enrolling with the template, the key size of the request is validated against the template key size. This allows for a key size to be set on a template in Keyfactor Command for validation purposes that can be different than the CA template key size setting. Care should be taken to make sure any template policy settings take into consideration CA template key size settings so that errors do not occur at the CA level.

- If a CSR Enrollment request is made with a key size that is not valid, per the template policy settings, an error will be displayed when you click the **Enroll** button (for example, the CSR has a key size of 2048 but the template policy supports only 4096).
- For PFX Enrollment, the request will contain the minimum settings from the Keyfactor Command presiding template settings.

6. Select the **Certificate Authority** from which the certificate should be requested. Only CAs that have the selected template available for enrollment or are standalone, if you check the stand-alone CA box, will be shown.

Tip: If you are enrolling from a standalone CA, check the **Use a stand-alone CA** box instead of selecting a template. The check box for stand-alone CAs only appears if you have a stand-alone CA configured for enrollment.

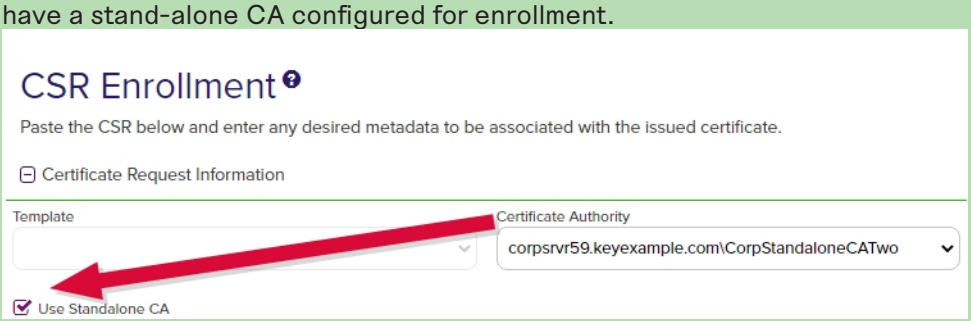


Figure 84: CSR Enrollment for Stand-Alone CA

7. The SAN section of the page appears if you enable the *Allow CSR SAN Entry* application setting (see Application Settings: Enrollment Tab on page 591). This option is disabled by default. In the Subject Alternative Names section of the page, click **Add** and select from the dropdown to enter one or more SANs for your CSR. Use the **Remove** action button to remove an existing SAN. The SAN field supports:

    - DNS name
    - IP version 4 address
    - IP version 6 address
    - User Prinicpal Name
    - Email

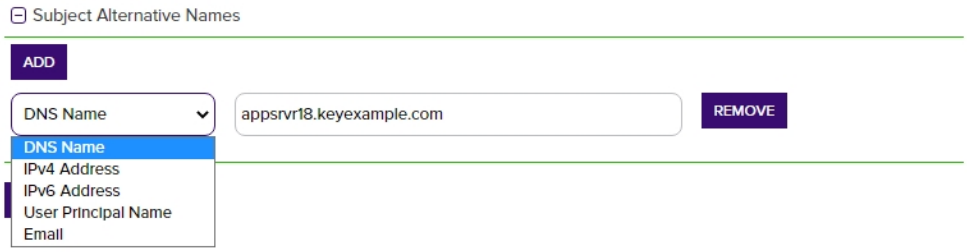


Figure 85: CSR Enrollment SAN options

Important: If the RFC 2818 compliance setting is enabled for the selected template (see Certificate Template Operations on page 353), your request must have at least one SAN either included in the original CSR or entered separately in this field, which matches the CN in the request.

Note: Entering SANs here may either append or overwrite the SANs in the CSR request depending on how the issuing CA is configured. Please be sure to check that the certificate has the correct SANs after issuance. Any SAN added automatically as a result of RFC 2818 compliance settings at the policy handler level will still be added alongside anything you add here. For more information, review the SAN Attribute Policy Handler for the Keyfactor CA Policy Module (see *Installing the Keyfactor CA Policy Module Handlers* in the *Keyfactor Command Server Installation Guide*).

8. If template-specific enrollment fields have been defined (see Enrollment Fields Tab on page 363) for the selected template, the fields will display in the Additional Enrollment Fields section. The types of fields shown could be either blank (string) fields or multiple choice drop-down fields depending on how they were configured on the template. **All additional enrollment fields are mandatory.**

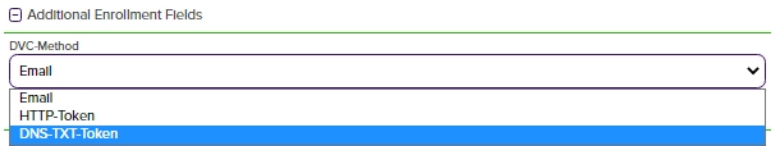


Figure 86: Populate Enrollment Fields

9. In the Certificate Metadata section of the page, populate any defined certificate metadata fields (see Certificate Metadata on page 646 and Metadata Tab on page 366) as appropriate for the template. These fields may be required or optional depending on your metadata configuration. Required fields will be marked with *Required next to the field label. Any completed values will be associated with the certificate once it has been synchronized with Keyfactor Command. The order in which the metadata fields appear can be changed (see Sorting Metadata Fields on page 651).

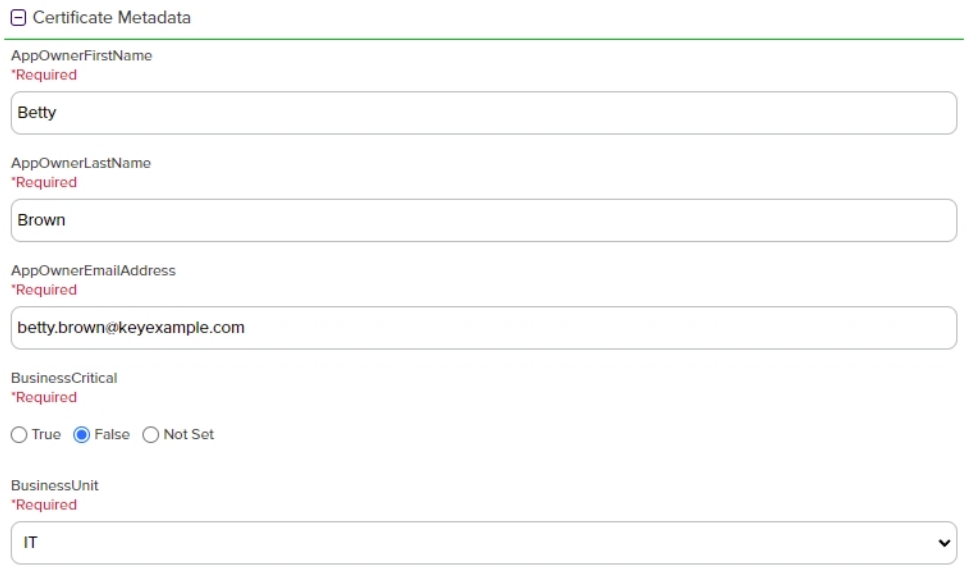


Figure 87: Populate Metadata Fields

10. At the bottom of the page, select the radio button for the desired encoding format (PEM or DER).

Figure 88: Select a Certificate Format

11. Click the **Enroll** button to begin the certificate request process.

    - If the request completes successfully, you'll see a success message and you'll be prompted by your browser to begin download of your certificate.

- If the template you selected requires approval at the Keyfactor Command workflow level, you'll see a message that your request is suspended and is awaiting one or more approvals. The user(s) responsible for approving the request will be notified (if the workflow has been configured this way, see Adding or Modifying a Workflow Definition on page 223). You can use the My Workflows *Created by Me* tab (see Workflows Created by Me Operations on page 313) to check on the status of your request. If the Management Portal feature has been configured to send notification alerts when a certificate is issued following approval, you may receive an email message when your certificate is available for download. The email message may contain a download link. See Issued Certificate Request Alerts on page 181.

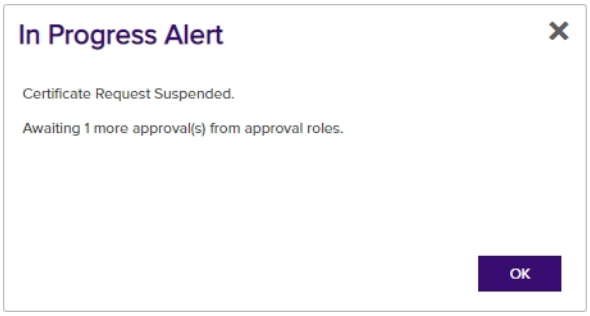


Figure 89: CSR Enrollment Completed Successfully—Awaiting Workflow Approval(s)

- If the template you selected requires manager approval at the CA level, you'll see a message that your request is pending. The user responsible for approving issuance of pending certificates will be notified (if that Management Portal feature is configured, see Pending Certificate Request Alerts on page 171). You can use the Certificate Requests page (see Certificate Requests on page 157) to check on the status of your pending request and complete the certificate download. If the Management Portal feature has been configured to send notification alerts when a pending certificate request is approved or denied, you may receive an email message when your certificate is available for download. The email message may contain a download link. See Issued Certificate Request Alerts on page 181 and Denied Certificate Request Alerts on page 188.

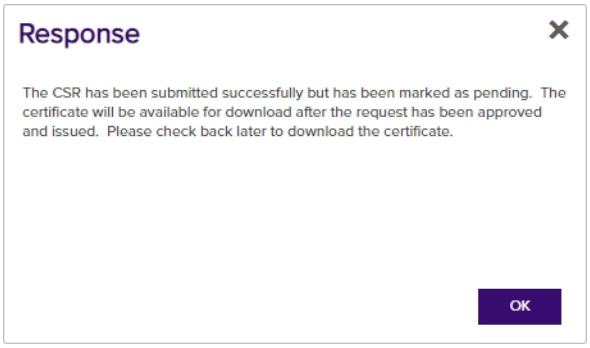


Figure 90: CSR Enrollment Completed Successfully—Pending Status

Tip: Click the help icon (?) next to the page title to open the embedded web copy of the *Keyfactor Command Documentation Suite* to this section.

You can also find the help icon at the top of the page next to the **Log Out** button. From here you can choose to open either the *Keyfactor Command Documentation Suite* at the home page or the *Keyfactor API Endpoint Utility*.

2.1.5.2 CSR Generation

The Certificate Signing Request (CSR) generation page provides the ability to enter a subject, SAN, key size, and template information and generate a CSR based on this information. You can then use this CSR to request a certificate using the CSR enrollment function (see CSR Enrollment on page 131) or any other enrollment method requiring a CSR.

When you use the CSR generation option, the encrypted private key of the request is stored in the Keyfactor Command database. When you generate a certificate using that CSR, it will be married together with the private key when the certificate synchronizes into the Keyfactor Command database. The certificate enrollment with the CSR does not need to be completed in Keyfactor Command (using CSR Enrollment) in order for the private key to be married with the certificate. Certificates enrolled outside of Keyfactor Command using CSRs generated within Keyfactor Command and synchronized via the CA synchronization process (see Certificate Authorities on page 325) or manually imported using the Add Certificate option (see Add Certificate on page 69) will also be married with their private keys.

To generate a CSR:

1. In the Keyfactor Command Management Portal, browse to *Enrollment > CSR Generation*.
2. In the Certificate Request Details section of the page:
    a. Select a **Template**, if desired. The templates are organized by configuration tenant (formerly known as forest). If you have multiple configuration tenants and templates with similar names, be sure to select the template in the correct configuration tenant.

    Important: The template will not be included in the CSR. The template is referenced in order to retrieve key size and other information to help populate the CSR. Also, the CSR generation page supports template-level regular expressions for both subject parts and SANs. If system-wide and template-level regular expressions exists for the same field and you select a template, the template-level regular expression is applied.
    If you choose to select a template during CSR generation, you will need to choose the same template during CSR Enrollment (see CSR Enrollment on page 131) because the CSR file will contain elements from the template which may conflict with other template configurations.

    b. Select a **Key Length** for your CSR. If you have selected a template, the dropdown will be limited to the value supplied by the template. When enrolling with the template, the key size of the request is validated against the template key size.

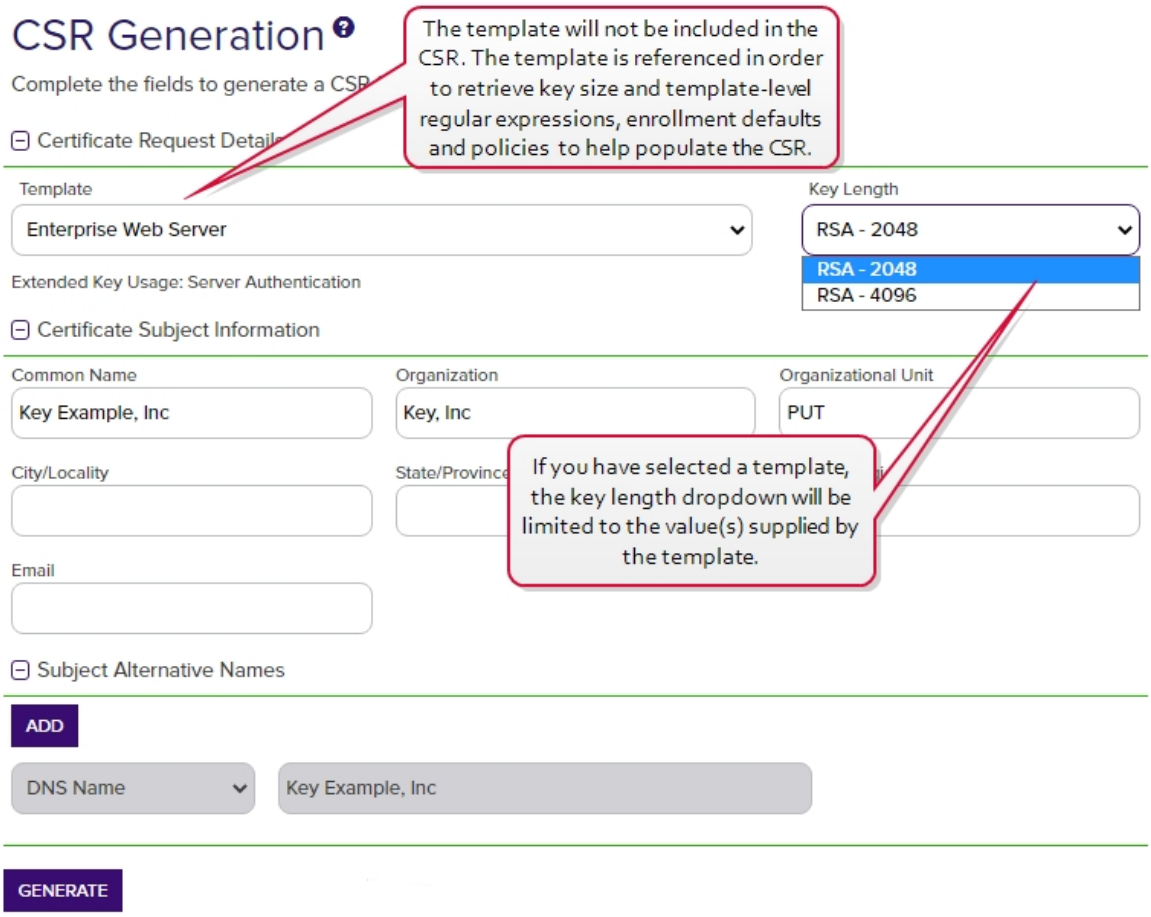


Figure 91: CSR Generation

3. In the Certificate Subject Information section of the page, enter appropriate subject information for your CSR.

   Note: Some subject fields may be automatically populated by system-wide or template-level enrollment defaults. You may override the system-populated data, if desired. Any system-wide or template-level regular expressions will be used to validate the data entered in the subject fields. System-wide or template-level policies will affect the request. For more information, see Certificate Template Operations on page 353. Subject data may also be overridden after an enrollment request is submitted either as part of a workflow (see Update Certificate Request Subject\SANs for Microsoft CAs on page 261) or using the *Subject Format* application setting (see Application Settings: Enrollment Tab on page 591).

4. In the Subject Alternative Names section of the page, click **Add** and select from the dropdown to enter one or more SANs for your CSR. Use the **Remove** action button to remove an existing

SAN.

Important: If the template you selected has the RFC 2818 compliance setting enabled, the DNS name will be automatically populated with the Common Name (CN) and will be set to read only.

Note: If the CSR generated has multiple SANs, they will not be overridden by the template default settings, nor the RFC 2818 compliance settings.

The SAN field supports:

- DNS name
- P version 4 address
- IP version 6 address
- User Prinicpal Name
- Email

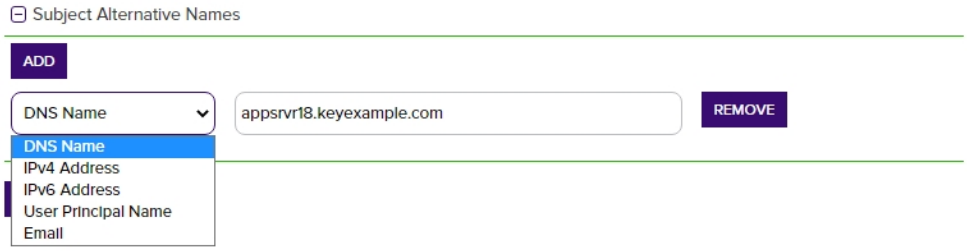


Figure 92: CSR Generation SAN Options

5. At the bottom of the page, click the **Generate** button. You will see a success message. If any template-level or system-wide regexes have been applied to any fields on the CSR and failed you will receive a notice at the top of the CSR generation page indicating the error as defined on the template (whether template or system-wide settings prevail).

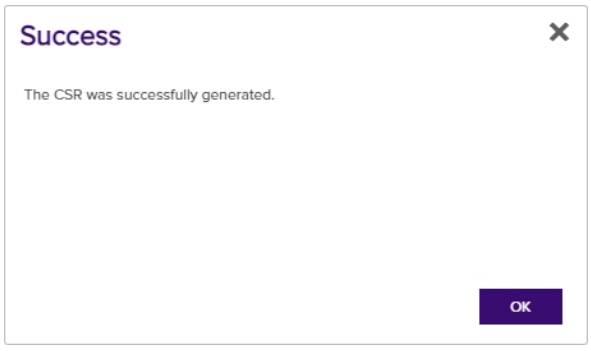


Figure 93: CSR Generation Success

6. Save or open your CSR once it has been successfully generated.

Tip: Click the help icon (?) next to the page title to open the embedded web copy of the *Keyfactor Command Documentation Suite* to this section.
You can also find the help icon at the top of the page next to the **Log Out** button. From here you can choose to open either the *Keyfactor Command Documentation Suite* at the home page or the *Keyfactor API Endpoint Utility*.

2.1.5.3 Pending CSRs

The Pending CSRs page allows you to see if you have any outstanding certificate signing requests that have been generated but not used for enrollment. From here, you can download them so that you can use them for enrollment or delete them if they are no longer needed. To download, highlight the selected row, right-click and choose **Download** from the right-click menu, or choose the **Download** action button at the top of the grid.

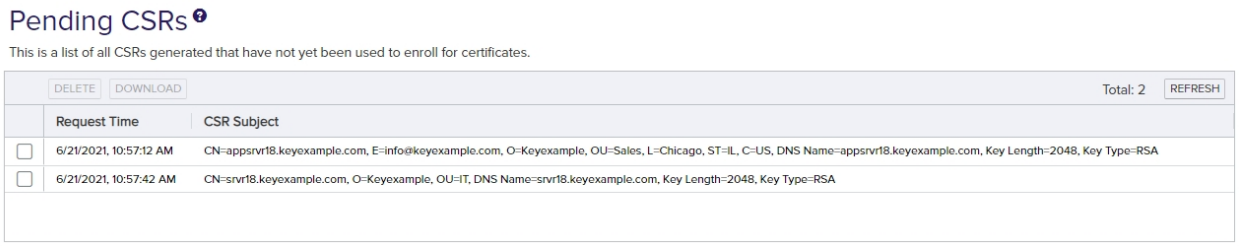


Figure 94: Pending CSRs

The pending certificate grid includes these fields:

- Request Time
  The date and time the CSR request was submitted in Keyfactor Command.
- Subject Name
  The subject name of the CSR, including key size, key type, and SANs, if applicable.

The CSRs can be sorted by clicking on the **Request Time** column header in the results grid. Click the column header again to reverse the sort order. The results grid columns can be arranged in any order desired by click-holding and dragging the header of the column you wish to move. The column widths may also be adjusted by click-holding and dragging the line separating two column headers.

2.1.5.4 PFX Enrollment

The PFX Enrollment page provides the ability to submit a certificate request and download the resulting PFX certificate file. Given the power involved in allowing a user to generate his or her own subject name and automatically receive a certificate in this subject name, Keyfactor recommends that permissions for this feature are only given to very trusted users and/or that you consider making use of Keyfactor Command workflow with a RequireApproval step (see Adding or Modifying a Workflow Definition on page 223).

Important: Before you can use the PFX enrollment function, you must configure at least one template for enrollment by checking the **PFX Enrollment** box under **Allowed Enrollment Types** in the certificate template details. In addition, if you wish to use a template that requires *CA certificate manager approval*, you must enable one of the **Private Key Retention** options in the certificate template details. See Certificate Template Operations on page 353.

Note: As of Keyfactor Command version 10, enrollment (PFX and CSR), renewal, and revocation requests all flow through Keyfactor Command workflow. This will result in no changes to the enrollment, renewal, and revocation user experience unless customizations have been added in workflow (see Workflow Definitions on page 218).

You can expand and collapse sections of the PFX enrollment page by clicking on the plus/minus icon to the left of each section title.

To request a certificate via PFX:

1. In the Keyfactor Command Management Portal, browse to *Enrollment > PFX Enrollment*.
2. If you are enrolling from an enterprise CA, select a certificate template from the **Template** dropdown. The templates are organized by configuration tenant (formerly known as forest). If you have multiple configuration tenants and templates with similar names, be sure to select the template in the correct configuration tenant. If you are enrolling from a standalone CA, check the **Use a stand-alone CA** box instead of selecting a template.

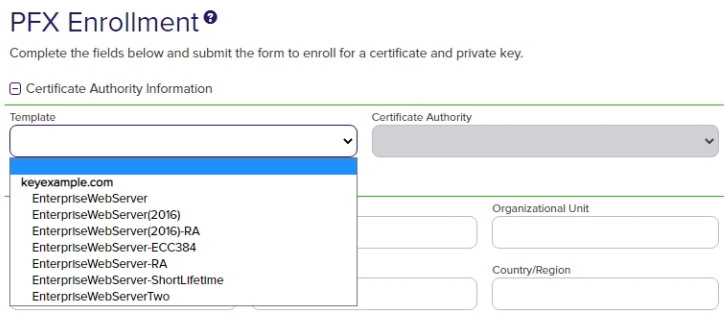


Figure 95: Select a Certificate Template

Note: When enrolling with the template, the key size of the request is validated against the template key size. This allows for a key size to be set on a template in Keyfactor Command for validation purposes that can be different than the CA template key size setting. Care should be taken to make sure any template policy settings take into consideration CA template key size settings so that errors do not occur at the CA level.

- If a CSR Enrollment request is made with a key size that is not valid, per the template policy settings, an error will be displayed when you click the **Enroll** button (for example, the CSR has a key size of 2048 but the template policy supports only

4096).

- For PFX Enrollment, the request will contain the minimum settings from the Keyfactor Command presiding template settings.

Tip: The check box for stand-alone CAs only appears if you have a stand-alone CA configured for enrollment.

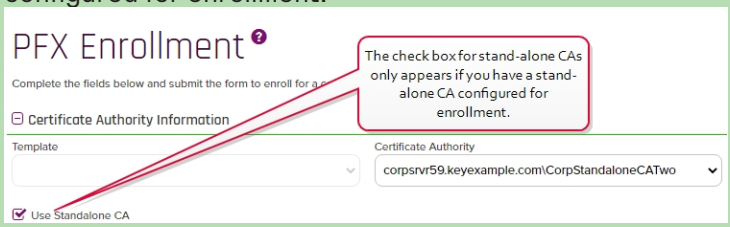


Figure 96: PFX Enrollment for Stand-Alone CA

Tip: If you select an ECC template, the elliptic curve algorithm for the template appears below the Template dropdown.

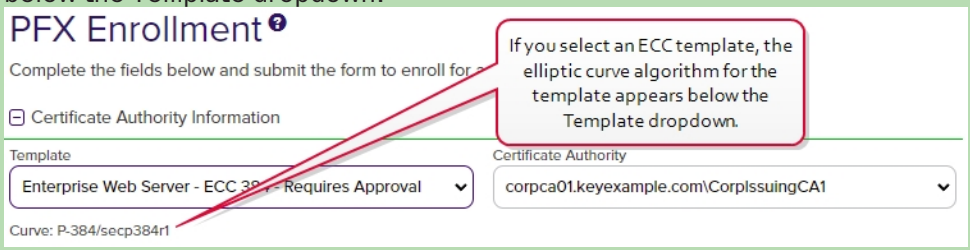


Figure 97: PFX Enrollment for ECC Template Displaying Elliptic Curve

3. Select the **Certificate Authority** from which the certificate should be requested. Only CAs that have the selected template available for enrollment or are standalone, if you check the stand-alone CA box, will be shown.

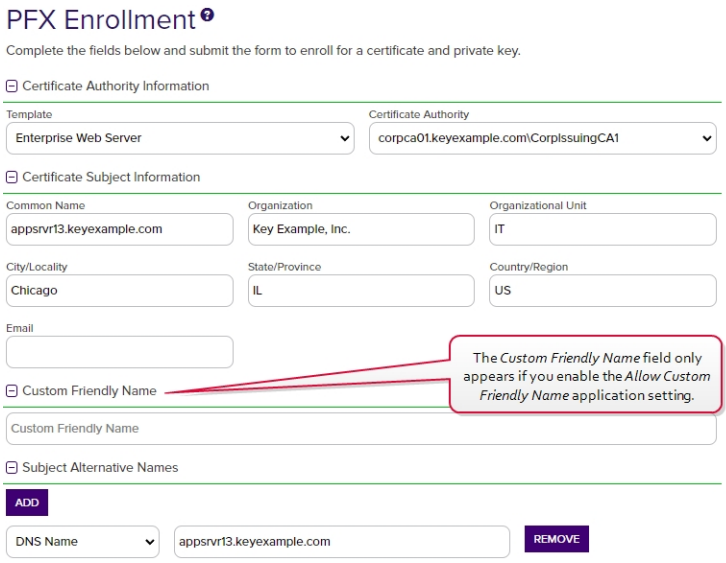


Figure 98: PFX Enrollment

> **Note:** If a system-wide or template-level regular expression exists for a subject part or SAN, and the subject part or SAN is left blank, the regular expression will be applied to an empty string for that part. For example, if you have a regular expression on organization, but do not supply an organization, the regular expression will be applied to a blank string as if that were supplied as the organization

4. In the Certificate Subject Information section of the page, populate the fields as appropriate for the certificate being requested. Although Keyfactor Command does not require the **Common Name**, it is typical for a CA to require this unless the template is set to populate the subject from Active Directory.

   > **Note:** Some subject fields may be automatically populated by system-wide or template-level enrollment defaults. You may override the system-populated data, if desired. Any system-wide or template-level regular expressions will be used to validate the data entered in the subject fields. System-wide or template-level policies will affect the request. For more information, see Certificate Template Operations on page 353. Subject data may also be overridden after an enrollment request is submitted either as part of a workflow (see Update Certificate Request Subject\SANs for Microsoft CAs on page 261) or using the *Subject Format* application setting (see Application Settings: Enrollment Tab on page 591).

5. If enabled, add a friendly name in the Custom Friendly Name section of the page. This section only appears if the *Allow Custom Friendly Name* application setting is set to *True*. If the *Require Custom Friendly Name* application is set to *True*, a value is required in this field. For more information, see Application Settings: Enrollment Tab on page 591.

6. In the Subject Alternative Names (SANs) section of the page, add SANs if needed. If the RFC 2818 compliance option has been enabled for the template (seeCertificate Template Operations on page 353), the first SAN field will automatically populate with a DNS SAN matching the CN when you enter the CN be set to *Read Only*. Click the **Add** button to add SAN fields.

   The SAN field supports:

   - DNS name
   - IP version 4 address
   - IP version 6 address
   - User Prinicpal Name
   - Email

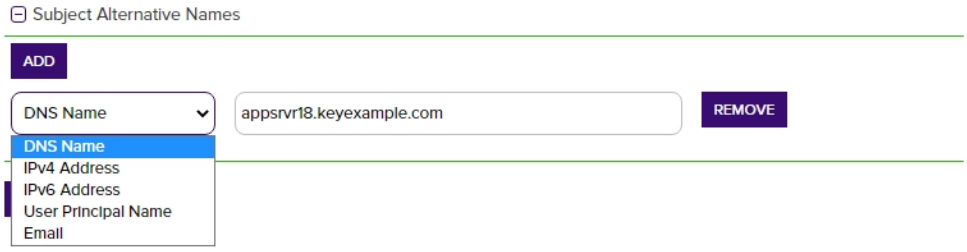


Figure 99: PFX Enrollment: SAN Options

   This field is not required unless the RFC 2818 compliance option on the CA has been configured.

7. If template-specific enrollment fields have been defined (see Enrollment Fields Tab on page 363) for the selected template, the fields will display in the Additional Enrollment Fields section. Additional enrollment fields have a data type of either string or multiple choice. String fields will appear as a text box; Multiple choice fields will appear as a dropdown. All additional enrollment fields are required.

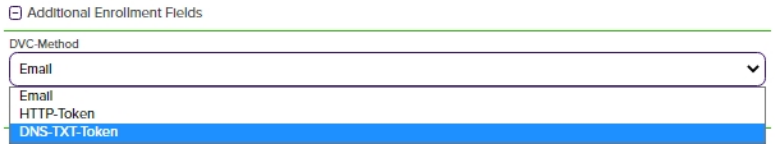


Figure 100: Populate Enrollment Fields

8. In the Certificate Metadata section of the page, populate any defined certificate metadata fields (see Certificate Metadata on page 646 and Certificate Template Operations on page 353) as appropriate for the template. These fields may be required or optional depending on your metadata configuration. Required fields will be marked with *Required next to the field label. Any completed values will be associated with the certificate once it has been imported into Keyfactor Command. The order in which the metadata fields appear can be changed (see Sorting Metadata Fields on page 651).

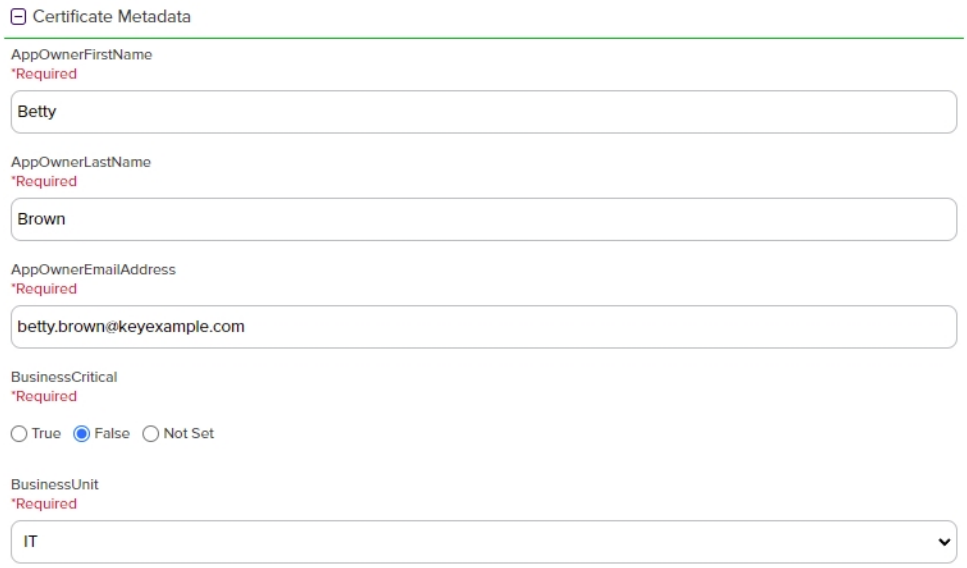


Figure 101: Populate Metadata Fields

9. If enabled, in the Password section of the page, check the **Use Custom Password** box and enter and confirm a custom password to use in securing the PFX file. This section only appears if the *Allow Custom Password* application setting is set to *True*. For more information, see Application Settings: Enrollment Tab on page 591.

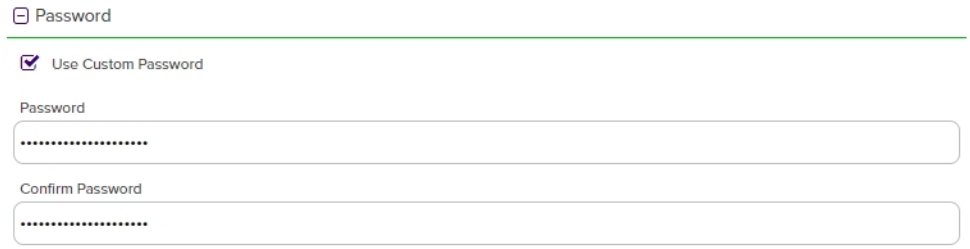


Figure 102: Set a Custom Password

10. In the Certificate Delivery Format section of the page, specify either **End Entity First** or **Root First** order when opting to include the chain in the returned certificate. The option to specify the order will only be available if the selected format supports it and you have specified to include the chain, otherwise the order will always be **End Entity First**.

    The supported formats are: PFX, ZIP PEM and JKS.

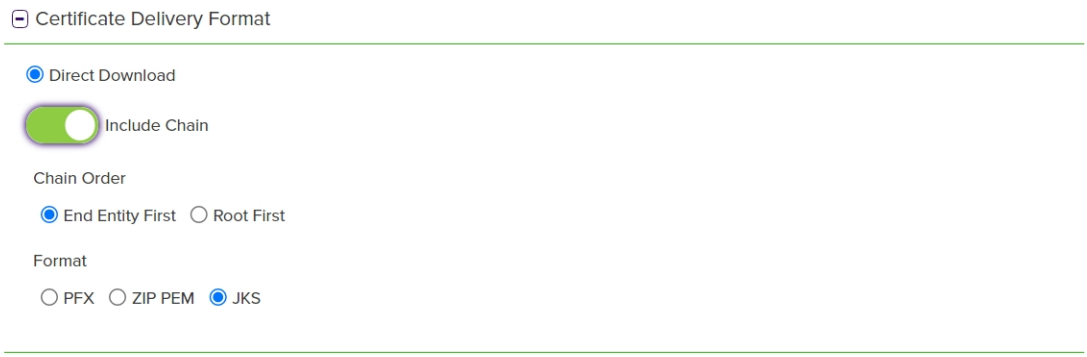


Figure 103: Delivery Format PFX Enrollment

11. To install a certificate into a certificate store, select the *Install into Certificate Stores* radio button and then click the **Include Certificate Stores** button. This will cause the *Select Certificate Store Locations* dialog to appear. Make your certificate store selections in this dialog as described in *Select Certificate Store Locations*, below, and click **Include and Close**. You will then see some additional fields on the enrollment page. Populate these as per *Add to Certificate Stores* and *Information Required for Certificate Stores*, below.

Select Certificate Store Locations

The *Select Certificate Store Locations* dialog allows you to run queries against your certificate store list to select which store(s) to deploy a selected certificate to. **Check** the box next to each certificate store location to which you want to distribute the certificate.

Note: Only compatible certificate stores and only stores in containers to which you have permissions are shown on the grid.

Tip: You may change the search results by using the search fields at the top of the dialog. All of the Keyfactor Command grid search features are available to assist your search. See Using the Certificate Store Search Feature on page 382 for more information on the available search fields. The default search criteria is *AgentAvailable is equal to True*.

The actions on the *Select Certificate Store Locations* dialog are:

- **Include**

  Click this to add the selected certificate store(s) to your certificate selection and leave the search dialog open for further searches.

- **Include and Close**

  Click this to close the search dialog and add the selected certificate store(s) to your certificate selection, which will then be displayed and ready for updates as per the instructions in *Add to Certificate Stores*.

- **Close**

  Click this to cancel the operation and return to the main page with no certificate stores selected.

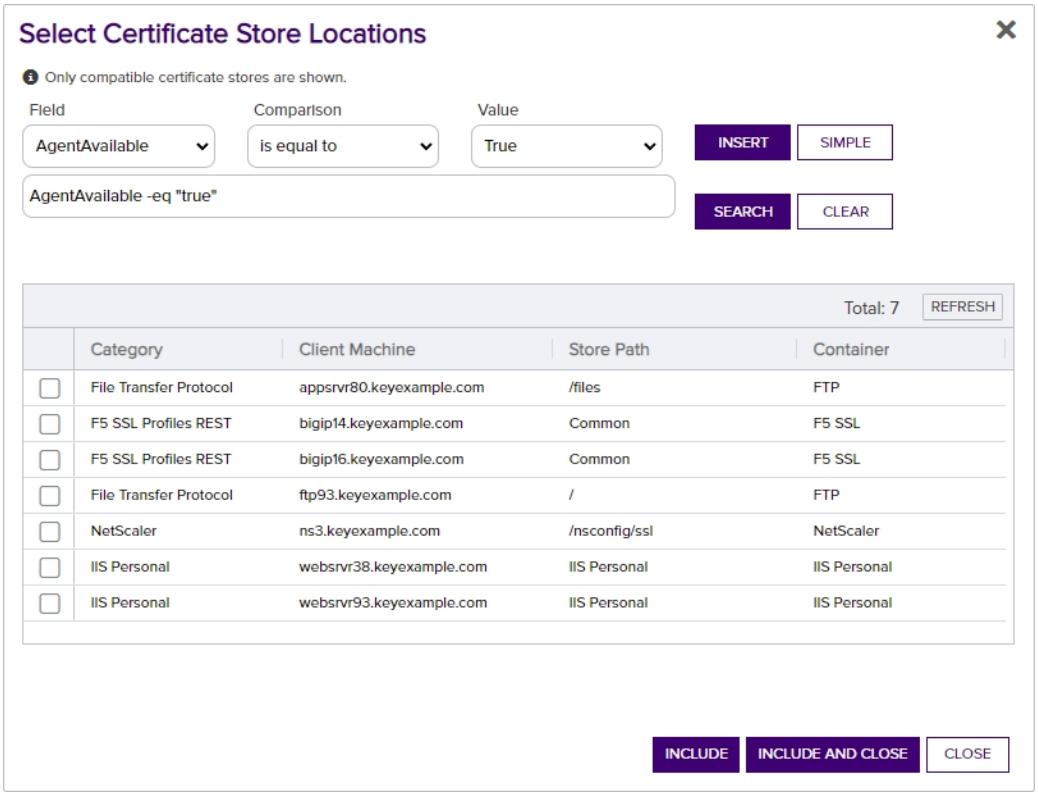


Figure 104: Select Certificate Store Locations Dialog

Add to Certificate Stores

The additional fields that appear on the page once you select at least one certificate store to distribute your certificate to include a grid section with a series of tabs that displays a tab for each type of certificate store selected with a list of the selected stores under each tab.

Above this section are global options that apply to the add job as a whole:

- **Schedule when to run the job for the certificate store**

  In the **Schedule** dropdown, select a time at which the job to add the certificate to the stores should run. The choices are *Immediate* or *Exactly Once* at a specified date and time. If you choose *Exactly Once*, enter the date and time for the job. A job scheduled for *Immediate* running will run within a few minutes of saving the operation. The default is *Immediate*.

- **Include Certificate Stores**

  Open the *Select Certificate Store Locations* dialog again.

For each selected certificate store you can apply the following actions:

- **Overwrite**

  Check **Overwrite** below the grid to allow the selected certificate to overwrite any existing certificate in the same location with the same name or alias.

- **Alias**

  Add an **Alias** below the grid, if applicable, for the certificate store type. See the **Information Required by Certificate Store** section, below, for more information.

  > **Note:** The tab heading of the certificate location will display an alert if an alias is required for the location.

- **Remove**

  Click **Remove** at the top of the grid to remove the selected certificate store from the page. The certificate will not be added to the store.

You may return to the *Select Certificate Store Locations* dialog by clicking **Include Certificate Stores** above the grid. The current selections will be retained.

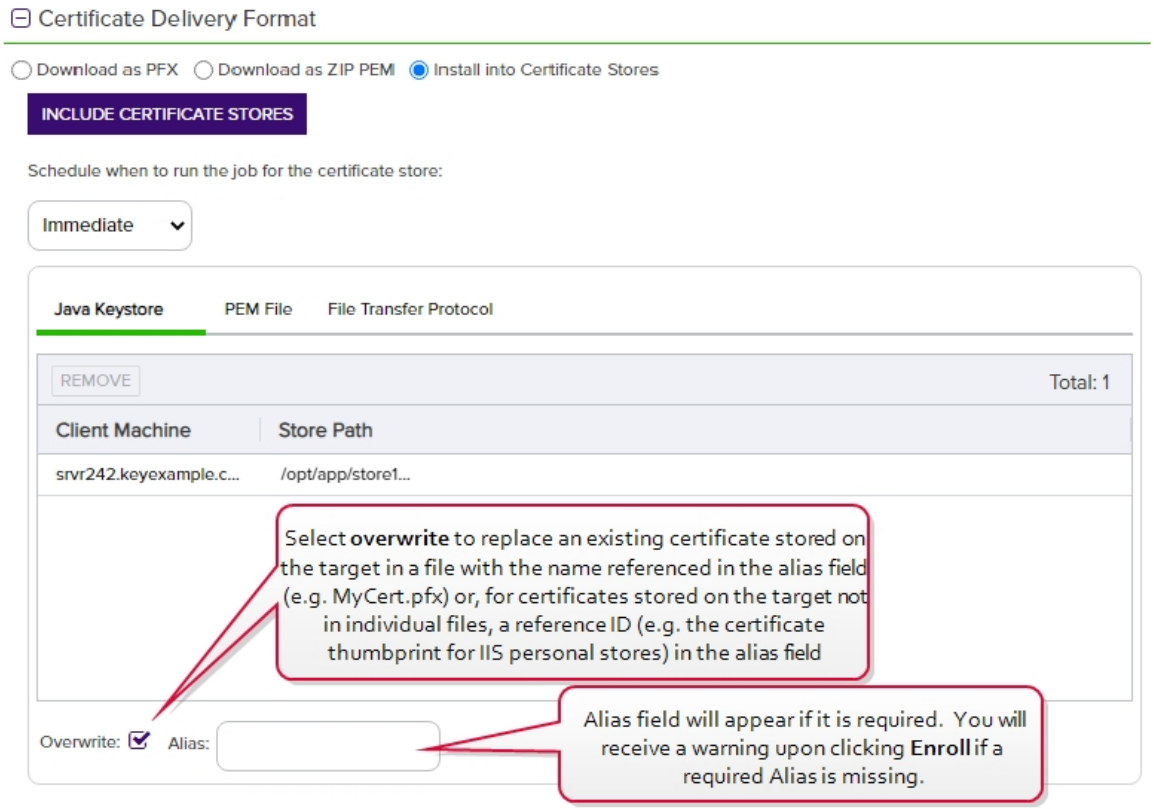


Figure 105: PFX Enrollment: Certificate Delivery Format

Figure 106: Alias Required System Alert on Enrolling

Information Required by Certificate Stores

Each type of certificate store has different requirements for providing an alias or other additional information. Table 6: Alias Requirements by Certificate Store Type provides a quick breakdown by certificate store of whether a certificate alias is required for new certificate additions

or only for overwriting an existing certificate in the store.

Tip: When adding a certificate to a certificate store, you have the option to overwrite an existing certificate with the current certificate. If you choose this option, you will need to provide the alias of the certificate you wish to overwrite. Find the alias values by navigating to *Management Portal > Certificates > Certificate Search*. Select the certificate you wish to overwrite and double-click, or click **Edit**, from the grid header or right-click menu. Choose the **Locations** tab and double-click on the Location Type (this must have a number other than zero in the *Count* column) to open the details dialog. The *Alias* field holds the information that may be required for an overwrite.

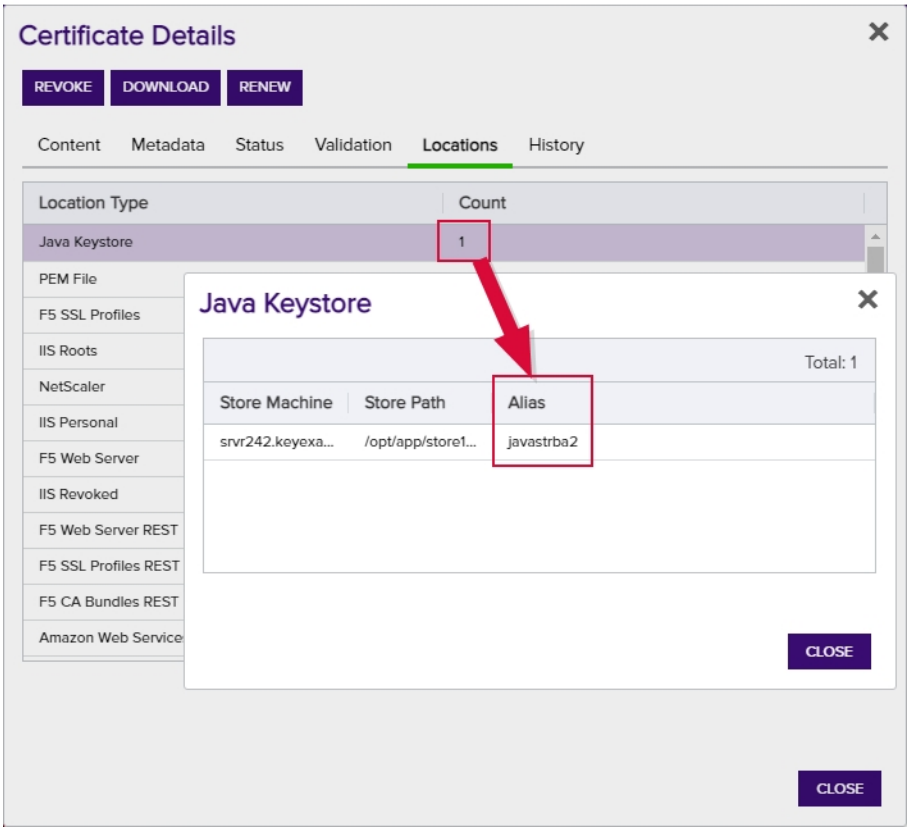


Figure 107: Example: Certificate Location Details for a JKS Location

Table 6: Alias Requirements by Certificate Store Type

Certificate Store Type	Alias Functionality
Amazon Web Services	Alias only required for overwrites
F5 CA Bundles REST	Alias required for new additions and overwrites
F5 SSL Profiles	Alias required for new additions and overwrites
F5 SSL Profiles REST	Alias required for new additions and overwrites
F5 Web Server	Alias only required for overwrites
F5 Web Server REST	Alias only required for overwrites
File Transfer Protocol	Alias required for new additions and overwrites
IIS Personal	Alias only required for overwrites
IIS Revoked	Alias not needed
IIS Trusted Roots	Alias not needed
Java Keystore	Alias required for new additions and overwrites
NetScaler	Alias required for new additions and overwrites
PEM File	Alias only required for overwrites

Amazon Web Services (AWS)

With this type of store, you have the option to overwrite an existing certificate with the current certificate. If you choose this option, you will need to provide the alias of the certificate you wish to overwrite. The alias is the internal ID assigned by Amazon (the Amazon resource number or ARN). Provide the entire contents of the *Alias/IP* from this field when entering an alias for overwrite. For example:

arn:aws:acm:us-west-2:220531701668:certificate/88e5dcfb-a70b-4636-a8ab-e85e8ad88780

F5 CA Bundles REST

With this type of store, you will be prompted to add an alias for the certificate. The alias is the file name used to store the file in the device file system, minus the extension (e.g. use alias MyFile for a file named MyFile.crt). Aliases should be entered without spaces. Note that certificate names are case sensitive. You have the option to overwrite an existing certificate with the current certificate. If you choose this option, you will need to provide the alias of the certificate you wish to overwrite.

F5 SSL Profile

With this type of store, you will be prompted to add an alias for the certificate. The alias is the file name used to store the file in the device file system, minus the extension (e.g. use alias MyFile for a file named MyFile.pfx). Aliases should be entered without spaces. Note that certificate names are case sensitive. You have the option to overwrite an existing certificate with the current certificate. If you choose this option, you will need to provide the alias of the certificate you wish to overwrite.

F5 SSL Profile REST

With this type of store, you will be prompted to add an alias for the certificate. The alias is the file name used to store the file in the device file system, minus the extension (e.g. use alias MyFile for a file named MyFile.pfx). Aliases should be entered without spaces. Note that certificate names are case sensitive. You have the option to overwrite an existing certificate with the current certificate. If you choose this option, you will need to provide the alias of the certificate you wish to overwrite.

F5 Web Server

With this type of store, you have the option to overwrite an existing certificate with the current certificate. If you choose this option, you will need to provide the alias of the certificate you wish to overwrite. The alias for F5 device certificates is typically *server*.

F5 Web Server REST

With this type of store, you have the option to overwrite an existing certificate with the current certificate. If you choose this option, you will need to provide the alias of the certificate you wish to overwrite. The alias for F5 device certificates is typically *server*.

File Transfer Protocol (FTP)

With this type of store, you have the option to overwrite an existing certificate with the current certificate. If you choose this option, you will need to provide the alias of the certificate you wish to overwrite. In that case the new thumbprint should be passed in as the alias without any spaces between the octets (e.g. 81009c6e5465ecf343ba55ff9612122a5a4f6b33 not 81 00 9c 6e 54 65 ec f3 43 ba 55 ff 96 12 12 2a 5a 4f 6b 33).

IIS Personal

With this type of store, you have the option to overwrite an existing certificate bound to an IIS web site with the current certificate. If you choose this option, you will need to provide the alias of the certificate you wish to overwrite. The alias is the thumbprint of the certificate bound to the IIS web site on the target. The thumbprint may be entered with or without spaces between each octet (e.g. 81 00 9c 6e 54 65 ec f3 43 ba 55 ff 96 12 12 2a 5a 4f 6b 33 or 81009c6e5465ecf343ba55ff9612122a5a4f6b33).

Tip: Choosing overwrite for a certificate **not** bound to an IIS web site will have no effect. No certificate will be overwritten.

IIS Revoked and Trusted Root

Tip: The overwrite functionality is not relevant for IIS Revoked and Trusted Root certificate stores and should be ignored.

Java Keystore

With this type of store, you will be prompted to add an alias for the certificate. This optional alias is stored in the keystore associated with the certificate. You have the option to overwrite an existing certificate with the current certificate. If you choose this option, you will need to provide the alias of the certificate you wish to overwrite. Spaces *are* supported in the alias.

NetScaler

With this type of store, you will must add an **Alias** for the certificate. This serves as the file name used to store the file in the file system, so provide it with an appropriate extension (e.g. appserver17.pfx). Aliases should be entered without spaces. You must also enter the virtual server to associate the certificate with in the **NetscalerVserver** field. For a certificate with a private key, you are associating the certificate as a NetScaler Server Certificate. Entry of virtual server name is not case sensitive. You have the option to overwrite an existing certificate with the current certificate. If you choose this option, you will need to provide the alias (full file name with extension) of the certificate you wish to overwrite.

PEM File

When you check the box for a PEM store, a new PFX Password section will appear on the page. The password you enter here is used to encrypt the private key of the certificate when stored in the PEM file or separate password file. If you choose to uncheck the *Use Custom Password* box, the private key will be encrypted with a random password *which is not accessible to you*. For most use cases, you will need a known password for this purpose, so leave the *Use Custom Password* box checked and make note of the password you use for this purpose. With this type of store, you have the option to overwrite an existing certificate with the current

certificate. If you choose this option, you will need to provide the alias of the certificate you wish to overwrite. The alias is the thumbprint of the certificate without any spaces between the octets (e.g. 81009c6e5465ecf343ba55ff9612122a5a4f6b33 not 81 00 9c 6e 54 65 ec f3 43 ba 55 ff 96 12 12 2a 5a 4f 6b 33).

Note: Keyfactor Command will automatically strip out any spaces between the octets in the alias field, so it does not matter whether you enter the thumbprint with or without spaces.

If you have any certificate stores defined, you may opt to install the certificate directly into one or more certificate stores on enrollment. If you choose to do this, the certificate will not be available for download on this page. The *Install Into Certificate Stores* option does not appear if no certificate stores have been defined.

12. At the bottom of the page, click **Enroll** to begin the certificate request process.

    - If the request completes successfully, you'll see a success message and you'll be prompted by your browser to begin download of your certificate unless you chose to install it directly into a certificate store. If you've configured PFX enrollment to use Windows authentication (the default) and have not selected the option to enter a custom password, you'll see a one-time password that has been generated to secure the PFX file. You will need this password in order to open the PFX file.

      Important: The randomly generated password cannot be regenerated, so it must be copied prior to closing the page. If you do not retain this password, you will not be able to open the PFX file. However, if you have configured private key retention for the template used for this enrollment (see Certificate Template Operations on page 353), you will be able to download the certificate with private key from certificate search at a later time.

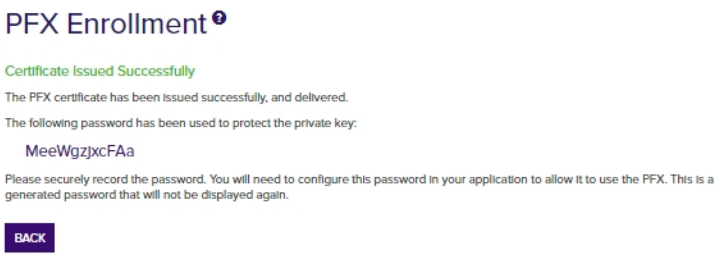
      

      Figure 108: PFX Request Completed Successfully—Windows Authentication

    - If you've configured the Keyfactor Command Management Portal to use basic authentication and you've configured the *Use Active Directory Password* application setting option to True, the message will indicate that the PFX file can be opened using the Active Directory domain password of the user making the request. For more information about

configuring basic authentication versus Windows authentication, see Application Settings: Enrollment Tab on page 591.

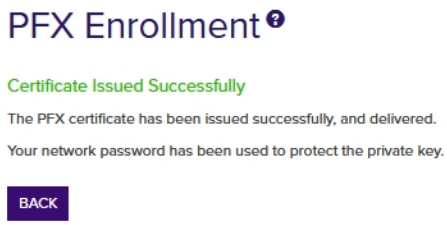


Figure 109: PFX Enrollment Completed Successfully—Network Password Used

Note: This option does not work when you authenticate to the Management Portal using Kerberos because Keyfactor Command does not have access to your credentials to apply your password to the PFX file.

- If the template you selected requires approval at the Keyfactor Command workflow level, you'll see a message that your request is suspended and is awaiting one or more approvals. The user(s) responsible for approving the request will be notified (if the workflow has been configured this way, see Adding or Modifying a Workflow Definition on page 223). You can use the My Workflows *Created by Me* tab (see Workflows Created by Me Operations on page 313) to check on the status of your request. If the Management Portal feature has been configured to send notification alerts when a certificate is issued following approval, you may receive an email message when your certificate is available for download. The email message may contain a download link. See Issued Certificate Request Alerts on page 181.

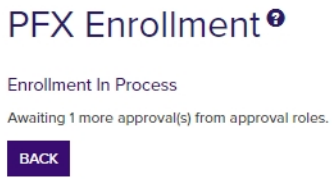


Figure 110: PFX Enrollment Completed Successfully—Awaiting Workflow Approval(s)

- If the template you selected requires manager approval at the CA level, you'll see a message that your request is pending. The user responsible for approving issuance of pending certificates will be notified (if that Management Portal feature is configured, see Pending Certificate Request Alerts on page 171). You can visit the Certificate Requests page (see Certificate Requests on the next page) to check on the status of your pending request and certificate search (see Certificate Search and Collections on page 19) to complete the certificate download. If the Management Portal feature has been configured to send notification alerts when a pending certificate request is approved or denied, you may receive an email message when your certificate is available for download. The email message may contain a download link. See Issued Certificate Request Alerts on page 181 and Denied Certificate Request Alerts on page 188.

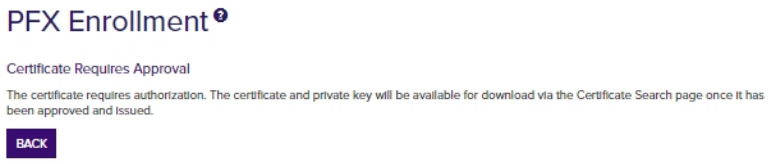


Figure 111: PFX Enrollment Completed Successfully—Pending Status

Tip: Click the help icon (?) next to the page title to open the embedded web copy of the *Keyfactor Command Documentation Suite* to this section.
You can also find the help icon at the top of the page next to the **Log Out** button. From here you can choose to open either the *Keyfactor Command Documentation Suite* at the home page or the *Keyfactor API Endpoint Utility*.

2.1.5.5 Certificate Requests

The Certificate Requests page shows certificate requests made to certificate authorities that have been configured to synchronize to the Keyfactor Command database and which have a status of pending, external validation or denied/failed. You can approve or deny pending certificates from this page (see Approving or Denying a Pending Certificate Request on page 159).

Tip: Click the help icon (?) next to the page title to open the embedded web copy of the *Keyfactor Command Documentation Suite* to this section.
You can also find the help icon at the top of the page next to the **Log Out** button. From here you can choose to open either the *Keyfactor Command Documentation Suite* at the home page or the *Keyfactor API Endpoint Utility*.

Viewing Certificate Requests

The Certificate Requests grid has three tabs: **Pending**, **External Validation** and **Denied/Failed**. Select the appropriate tab to the view desired certificate requests. You may also filter the list shown by entering all or part of a **Requester Name** and clicking **Filter** to change which requests are displayed.

Note: Certificate requests that require approval at the Keyfactor Command workflow level (see Workflow Definitions on page 218) do not appear on this page.

- **Pending**

  Typically a request in this state has been made using a template that requires manager approval at the CA level before issuance. The request may be approved or denied from this tab of the certificate requests page or though action on a *Pending Request Alert* (see Pending Certificate Request Alerts on page 171). When the pending requests tab is selected, you will see **Approve** and **Deny** buttons activated at the top of the grid. By clicking **Details**, you can view the

certificate details and **Approve** or **Deny** the request from the Certificate Request Details dialog. See Approving or Denying a Pending Certificate Request on the next page for more information.

- **External Validation**

  Certificate requests in this state require approval outside of Keyfactor Command. Certificates appearing on this tab generally are for requests made through one of the Keyfactor Command CA gateways using an EV certificate type. The requests appear here for reference only and cannot be approved or denied. Once a request has been approved using the cloud provider's EV approval process, the Keyfactor Command CA gateway and Keyfactor Command will import the issued certificate on the next synchronization. The synced certificate will move to the Certificate Search grid (see Certificate Search and Collections on page 19) and can be viewed there.

- **Denied/Failed**

  The denied/failed view shows requests that have been denied through Keyfactor Command as an action on the certificate requests page **Pending** tab though action on a *Pending Request Alert* (see Pending Certificate Request Alerts on page 171), or through a *POST /Workflow/Certificates/Deny* API request (see *POST Workflow Certificates Deny* in the *Keyfactor Web APIs Reference Guide*), but does not include requests denied directly from the CA outside of Keyfactor Command.

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:
Alerts: *Read*

The certificate requests grid includes these fields:

Keyfactor Request ID
The reference ID of the request from the Keyfactor database.

Common Name
The requested common name of the request.

Distinguished Name
The requested distinguished name of the request.

Submission Date
The date on which the request was submitted.

Certificate Authority
The CA against which the request was made.

Template
The short name of the template used to make the request.

Requester
The user or entity that made the request.

State
The request status—failed, pending or external validation as per the tab selected.

By default, the grid sorts in descending order with the most recent certs at the top. The grid can be sorted in ascending or descending Submission Date order by clicking on the column header. he grid columns can be arranged in any order desired by click-holding and dragging the header of the column you wish to move. The column widths may also be adjusted by click-holding and dragging the line separating two column headers.

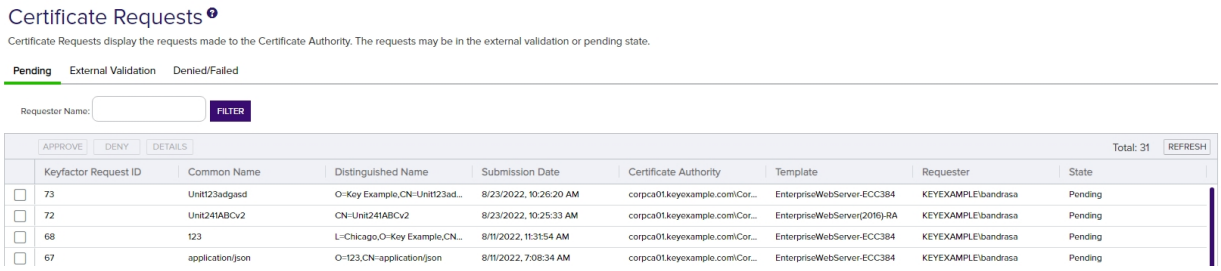


Figure 112: Certificate Requests Grid

The **Details** button appears activated for all views. The details page includes the SANs, metadata, and certificate stores scheduled for distribution for the request, in addition to the information shown on the main grid.

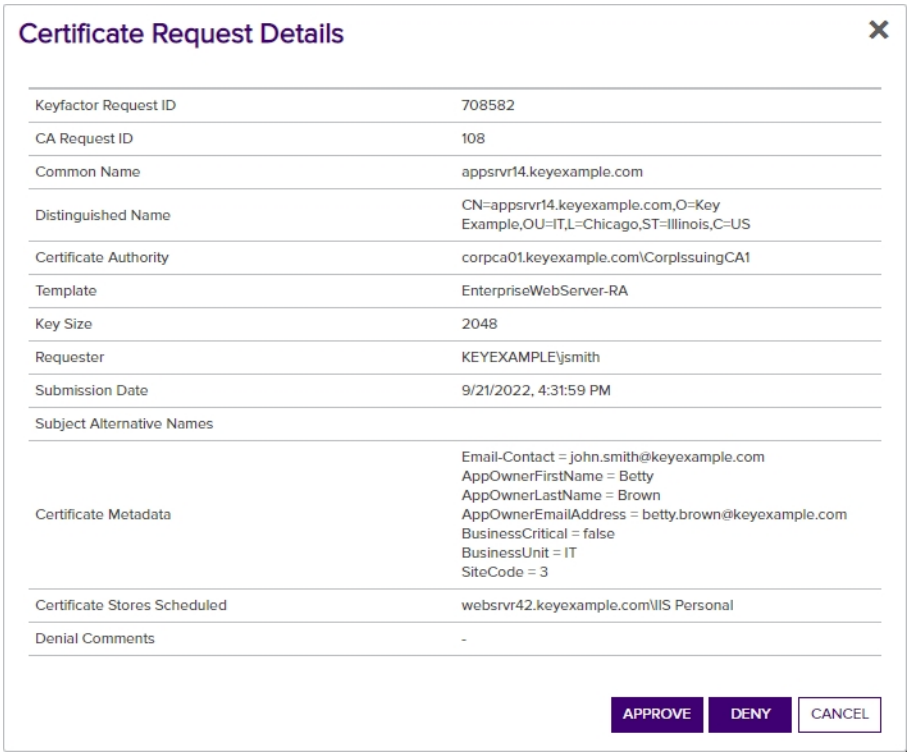


Figure 113: Certificate Request Details

Approving or Denying a Pending Certificate Request

On the **Pending** tab of the certificates requests grid you can view the **Details** of a certificate request that required manager approval at the CA level and choose to **Approve** or **Deny** it by clicking the action buttons at the top of the grid. You can also **Approve** or **Deny** the request from the Certificate Request Details dialog. The approve and deny operations can be done on multiple requests at once. To select multiple rows, click the checkbox for each row on which you would like to perform an oper-

ation, then select an operation from the top of the grid. The right-click menu only supports operations on one request at a time.

- When you deny a request, you will be prompted to enter a comment regarding the denial. These comments can be delivered to the requester or other interested party using a denied request alert (see Denied Certificate Request Alerts on page 188). When a certificate is denied, its status will change to failed and it will move from the pending grid tab to the denied/failed grid tab. The denial comments will display in the Certificate Request Details dialogue.
- When a request is approved on this page, the certificate will move to the Certificate Search grid (see Certificate Search and Collections on page 19) and can be viewed there. If you have configured issued certificate alerts (see Issued Certificate Request Alerts on page 181), the requester or other interested party will be notified immediately on approval.

Note: Certificate requests that require approval at the Keyfactor Command workflow level (see Workflow Definitions on page 218) do not appear on this page.

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:
Alerts: *Read*
Certificate Requests: *Manage*

Certificate requests with a pending status have generally either been requested using certificate templates requiring manager approval at the CA level or from a CA configured to send all requests to pending automatically.

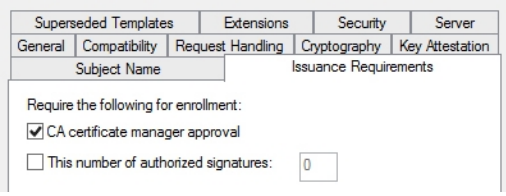


Figure 114: Certificate Template Requiring Manager Approval

Note: Certificate requests that require approval at the CA level are supported only for Microsort CAs and select CA gateways. This feature is not supported for EJBCA CAs. Use workflow for configuring Keyfactor Command-level approvals for EJBCA CAs (see Workflow Definitions on page 218).

2.1.6 Alerts

The options available in the Alerts section of the Management Portal are:

- Expiration Alerts below
  Create email notifications that alert administrators and/or end users when certificates are coming up for expiration.
- Pending Certificate Request Alerts on page 171
  Create email notifications that alert PKI administrators when a new pending certificate request is made.
- Issued Certificate Request Alerts on page 181
  Create email notifications that alert a certificate requester when a certificate he or she requested has been issued.
- Denied Certificate Request Alerts on page 188
  Create email notifications that alert a certificate requester when a certificate he or she requested has been denied.
- Key Rotation Alerts on page 193
  Create email notifications that alert end users and PKI administrators when an SSH key is nearing the end of its lifetime.
- Revocation Monitoring on page 199
  Define locations where certificate revocation lists (CRLs) and online certificate status protocol (OCSP) locations may be found and enable expiration notification alerts for them.

2.1.6.1 Expiration Alerts

Expiration alerts are used to send email notifications to certificate owners, users and/or administrators when a certificate is nearing or at expiration. The alerts can be customized to provide detailed information about the certificates along with, for example, instructions to end users on how to enroll for a replacement certificate.

Expiration Alert Operations

Expiration alerts are based on certificate collections. Before you can work with expiration alerts, you need to have created a certificate collection on which to base the alert (see Certificate Search and Collections on page 19).

Adding or Modifying an Expiration Alert

1. In the Management Portal, browse to *Alerts* > *Expiration*.
2. On the Expiration Alerts page, click **Add** from the top menu to create a new alert, or **Edit** from either the top or right click menu, to modify an existing one.
3. In the Certificate Expiration Alert Settings dialog, select your **Certificate Collection** in the first dropdown.

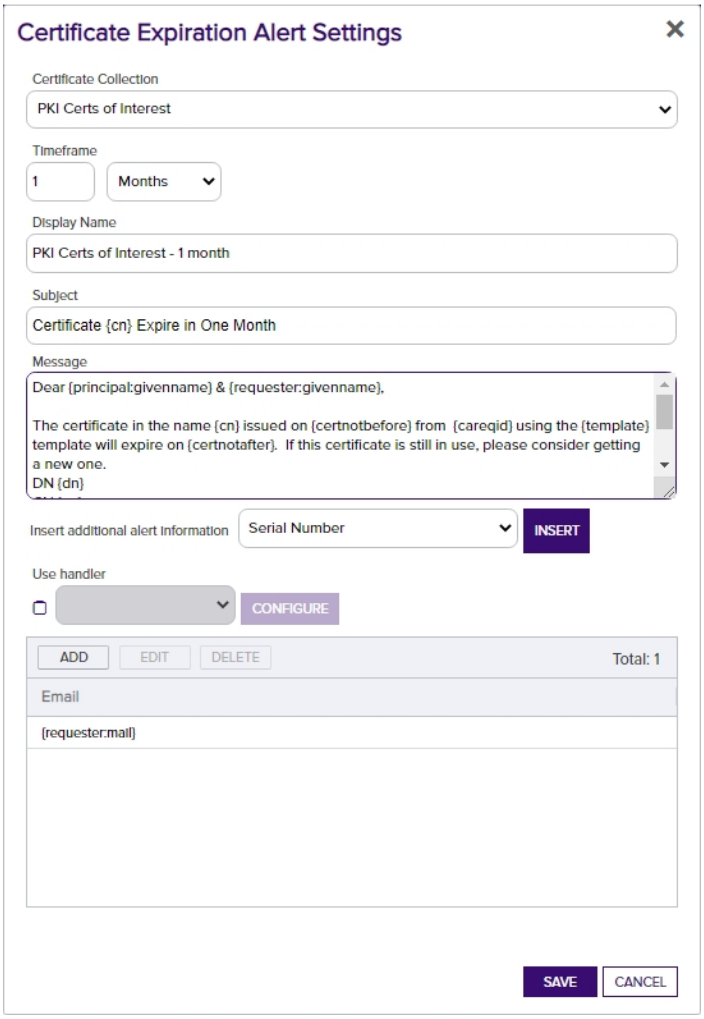


Figure 115: Create a New Expiration Alert

4. In the **Timeframe** fields, select the warning timeframe by defining a number for either days, weeks, or months for the alert. For example, if you select three weeks, the expiration alerts will be sent automatically three weeks ahead of certificate expiration.

Note: When the alert is stored in the database, weeks are converted to 7 days and months are converted to 30 days.

Example: When alerts run, the alert engine reports on all the certificates expiring within the next X days (e.g. 30 days) from the execution time that have not previously been reported on. This means that if the alerts run daily and have been running daily regularly

for some time, only a single day of expiring certificates will be reported on by any given alert run.
For example, say you create a new alert that has never run before for collection A and set it to 30 days. You configure it to run daily at 5:00 am. The alert runs for the first time at 5:00 am on July 1st. All the certificates in collection A that will expire between July 1st at 12:oo am UTC and July 31 at 12:00 am UTC will be alerted on. The next day when the alert runs again at 5:00 am on July 2nd, the certificates in collection A expiring between July 31st at 12:00 am UTC and August 1st at 12:oo am UTC will be alerted on.

If alerts are missed for a period of time (due to an outage, for example), the next run of the alerts will check the previous successful run date for the alerts and report on certificates expiring X days from that outage window. For example, using the collection A alert referenced above, say an outage caused the alerts not to run on August 1 and August 2. On August 3, the alert would run again at 5:00 am, and the certificates in collection A expiring between August 30th at 12:00 am UTC and September 2nd at 12:oo am UTC would be alerted on.

5. In the **Display Name** field, enter a name for the alert. This name appears in the list of expiration alerts in the Management Portal.

6. In the **Subject** field, enter a subject line for the email message that will be delivered when the alert is triggered. You can use substitutable special text in the subject line. Substitutable special text uses a variable in the alert definition that is replaced by data from the certificate or certificate metadata at processing time. For example, you can enter {cn} in the alert definition and each alert generated at processing time will contain the specific common name of the given certificate instead of the variable {cn}.

   To add substitutable special text to the subject line; place your cursor where you would like the text to appear on the subject line, select the appropriate variable from the *Insert special text* dropdown, and click **Insert**. Alternately, type the special text variable enclosed in curly braces (e.g. {cn}).

7. In the **Message** box, enter the body of the email message that will be delivered when the alert is triggered. You can use the *Insert special text* dropdown below the message window to add substitutable special text to the message. The metadata that appears in the dropdown will depend upon the custom metadata you have defined (see Certificate Metadata on page 646). Place your cursor where you would like the text to appear, select the appropriate variable from the dropdown, and click **Insert**. Alternately, you can type the special text variable enclosed in curly braces directly. In addition to the substitutable special text fields available in the dropdown, you can also build your own substitutable fields for the principal and/or requester based on string values from the user or computer Active Directory record. See Table 7: Substitutable Special Text for Expiration Alerts. If desired, you can format the message body using HTML. For example, you could place certificate detail information into a table by replacing this text:

   DN: {dn}
   CN: {cn}

UPN: {upn}
Thumbprint: {thumbprint}
Serial Number: {serial}

With this HTML code:

```
<table>
<tr><td>DN:</td><td>{dn}</td></tr>
<tr><td>CN:</td><td>{cn}</td></tr>
<tr><td>UPN:</td><td>{upn}</td></tr>
<tr><td>Thumbprint:</td><td>{thumbprint}</td></tr>
<tr><td>Serial Number:</td><td>{serial}</td></tr>
</table>
```

8. Check the **Use handler** box if you would like the alert to trigger an event handler at processing time, select the appropriate handler in the dropdown, and click the **Configure** button to configure the handler. See Using Event Handlers on page 207 for more information on using event handlers.

   Note: As of version 9.0 of Keyfactor Command, PowerShell scripts for alert handlers need to be in the extension path or a subdirectory of it specified by the *Extension Handler Path* application setting (see Application Settings: Console Tab on page 584). By default this is:

   ```
   C:\Program Files\Keyfactor\Keyfactor Platform\ExtensionLibrary\
   ```

   For example, create a directory called *Scripts* under the ExtensionLibrary directory and then reference your PowerShell script as *Scripts\MyPowerShell.ps1*. Any scripts referenced by PowerShell handlers that are outside this path will fail to run.

9. In the Recipients section of the page, click **Add** to add a recipient to the alert. Each alert can have multiple recipients. Recipients should be added one at a time. You can enter specific email addresses and/or use substitutable special text to replace an email address variable with actual email addresses at processing time. The built-in variable can be selected in the Recipient dialog **Use a variable from the certificate** dropdown. In addition, you can type a special text variable enclosed in curly braces in the Email field if you have, for example, a metadata field that contains an email address.

   Keyfactor Command sends SMS (text) messages by leveraging the email to text gateways that many major mobile carriers provide. Check with your carrier for specific instructions. Keyfactor has tested that AT&T can be addressed using 10-digit-number@txt.att.net (e.g. 4155551212@txt.att.net) and Verizon can be addressed using 10-digit-number@vtext.com (e.g. 2125551212@vtext.com). T-Mobile can be addressed using 10-digit-number@tmomail.net (e.g. 2065551212@tmomail.net), but functionality can be spotty. Reliability of alerting via this method depends on the reliability of the carrier's gateways.

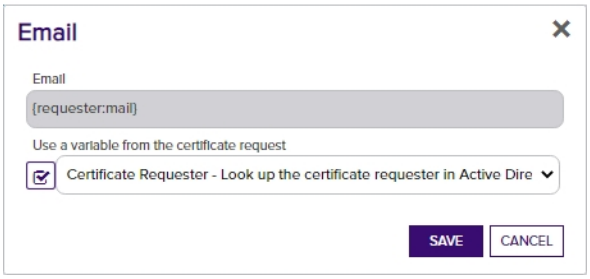


Figure 116: Expiration Alerts Recipients

10. Click **Save** to save your expiration alert, or your changes.

Copying an Expiration Alert

You may use the copy operation to create multiple similar alerts—for example, several alerts for the same certificate collection but with different warning timeframes.

1. In the Management Portal, browse to *Alerts* > *Expiration*.
2. On the Expiration Alerts page, highlight the row in the expiration alerts grid and click **Copy** at the top of the grid, or from the right click menu.
3. The Certificate Expiration Alert Settings dialog will pop-up with the details from the selected alert. The display name field will have - *Copy* tagged to the end of it to indicate it is a new alert. You may modify the alert as needed and click **Save** to add the new alert, or **Cancel** to cancel the operation.

Deleting an Expiration Alert

You may delete one expiration alert at a time.

1. In the Management Portal, browse to *Alerts* > *Expiration*.
2. On the Expiration Alerts page, highlight the row in the Expiration Alerts grid and click **Delete** at the top of the grid, or from the right click menu.
3. On the Confirm Operation alert, click **OK** to confirm or **Cancel** to cancel the operation.

Configuring an Expiration Alert Schedule

After adding your desired Certificate Expiration Alerts, you may configure an alert schedule.

1. In the Management Portal, browse to *Alerts* > *Expiration*.
2. On the Expiration Alerts page, click the **Configure** button at the top of the Expiration Alerts page to configure a monitoring execution schedule. This will apply for all the expiration alerts. This defines the frequency with which alerts are sent. This type of alert is scheduled for daily delivery at a specified time.

Example: When alerts run, the alert engine reports on all the certificates expiring within the next X days (e.g. 30 days) from the execution time that have not previously been reported on. This means that if the alerts run daily and have been running daily regularly for some time, only a single day of expiring certificates will be reported on by any given alert run.
For example, say you create a new alert that has never run before for collection A and set it to 30 days. You configure it to run daily at 5:00 am. The alert runs for the first time at 5:00 am on July 1st. All the certificates in collection A that will expire between July 1st at 12:oo am UTC and July 31 at 12:00 am UTC will be alerted on. The next day when the alert runs again at 5:00 am on July 2nd, the certificates in collection A expiring between July 31st at 12:00 am UTC and August 1st at 12:oo am UTC will be alerted on.

If alerts are missed for a period of time (due to an outage, for example), the next run of the alerts will check the previous successful run date for the alerts and report on certificates expiring X days from that outage window. For example, using the collection A alert referenced above, say an outage caused the alerts not to run on August 1 and August 2. On August 3, the alert would run again at 5:00 am, and the certificates in collection A expiring between August 30th at 12:00 am UTC and September 2nd at 12:oo am UTC would be alerted on.

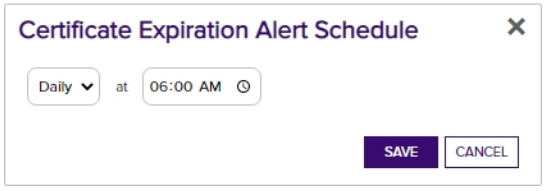


Figure 117: Expiration Alert Schedule

Testing Expiration Alerts

Once the alerts are configured, you may run a test of all, or selected, alerts to see if they are configured correctly.

1. In the Management Portal, browse to *Alerts* > *Expiration*.
2. On the Expiration Alerts page, either highlight one row in the expiration alert grid and click the **Test** button at the top of the grid or click the **Test All** button at the top of the grid to test all the alerts.
3. In the Expiration Alert Test dialog in the Alert Parameters section, select a **Start Date** and **End Date** for testing. You can use this option to simulate running the alerts a month from now instead of today, for example, or put in a broad date range to be sure you pick up some expiring certificates for testing purposes.

   Example: Say you had experienced an outage and alerts that normally run daily at 5:00 pm did not run for two days. You wanted to test to see what to expect of the alerts once the system was up and running again. You are running your test on August 3rd for an alert

that's configured to report at 30 days for collection A. The alert last ran on July 31. This means the alert has a *Previous Evaluation Date* of July 31. When running your test, set the **Start Date** to July 31st to match the *Previous Evaluation Date*. Set the **End Date** to the current date, August 2nd in this example, to simulate the results when the alerts are run today. The test results will include up to 100 certificates in collection A expiring between August 30th at 12:00 am UTC and September 1st at 12:00 am UTC.

4. In the Expiration Alert Test dialog in the Alert Parameters section, click the toggle button for **Send Alerts** if you would like to deliver email messages as part of the test.

5. Click the **Generate** button to begin generating alerts. Depending on the number of certificates to process, this may take a few seconds.

6. In the Expiration Alert Test dialog in the Alert Data and Alert Message sections, you can review the certificates found to confirm that the expected certificates are appearing and that the substitutable special text is being replaced as expected. Scroll through the alerts using the **First**, **Previous**, **Next** and **Last** buttons at the bottom of the dialog. The number of alerts generated will display between the navigation buttons.

Note: You may see fewer alerts than you have certificates expiring in the selected time window for the certificate collection if you enabled one of the options to ignore duplicate certificates on the certificate collection (see Saving Search Criteria as a Collection on page 40).

Tip: Alerts are generated when a certificate has expired or is approaching expiration as defined by the timeframe configured in the alert.
By default, a maximum of 100 alerts will be generated during a test. The maximum value is configurable with the *Expiration Alert Test Result Limit* setting in Keyfactor Command application settings (see Application Settings: Console Tab on page 584 in the *Keyfactor Command Reference Guide*). If more than 100 alerts are generated, no email messages will be sent and you'll have the opportunity to view the first 100 alerts generated.

If you're using an event handler, the event handler is run and the handler actions taken (PowerShell script run, event log message written, certificates renewed) when the test is run. This is true whether or not you click the *Send Alerts* toggle.

Note: HTML does not render in the alert viewer.

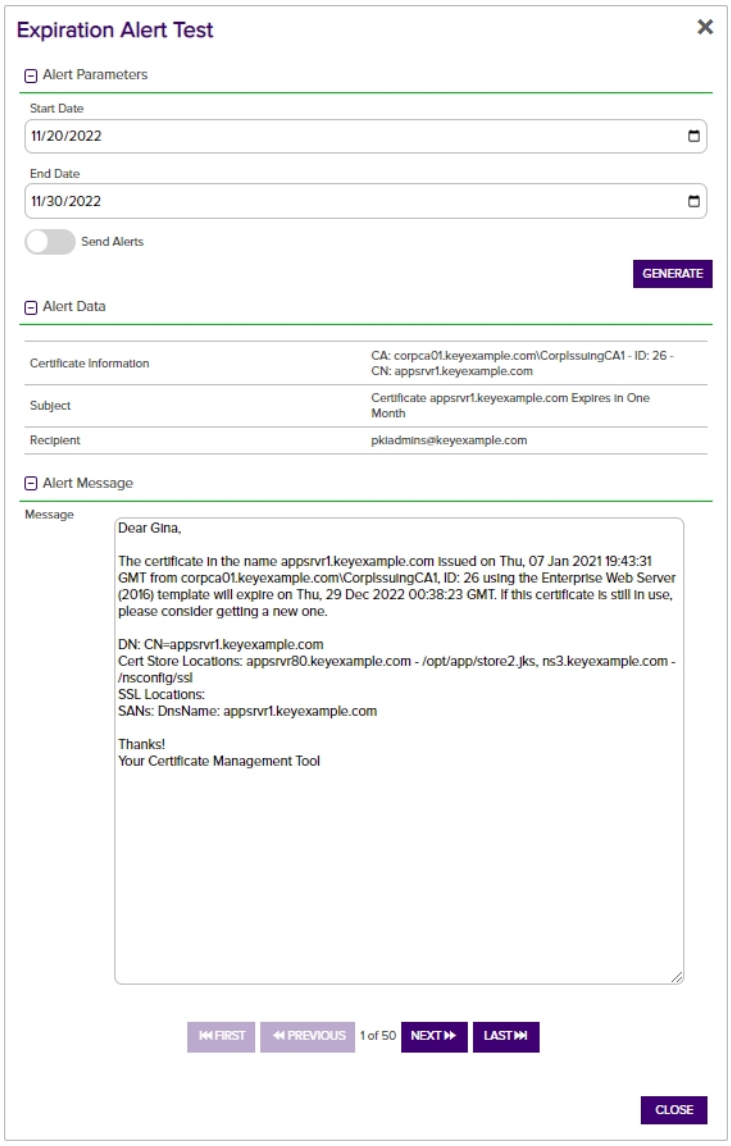


Figure 118: Expiration Alert Test

Refer to the following table for a complete list of the substitutable special text that can be used to customize alert messages.

Table 7: Substitutable Special Text for Expiration Alerts

Variable	Name	Description
{certemail}	Email Address in Certificate	Email address contained in the certificate, if present
{cn}	Common Name	Common name contained in the certificate

Variable	Name	Description
{dn}	Distinguished Name	Distinguished name contained in the certificate
{certnotbefore}	Issue Date	Validity date of the certificate
{certnotafter}	Expiration Date	Expiration date of the certificate
{issuerDN}	Issuer DN	Distinguished name of the certificate's issuer
{locations:certstore}	Certificate Store Locations	The server and path location to the certificate store (s) where the certificate resides, if any, for certificates found in certificate stores (e.g. server1.keyexample.com – /opt/test/mystore.jks)
{principal:mail}	Principal's Email	Email address retrieved from Active Directory of the user whose UPN is contained in the SAN field of the certificate, if present
{principal:givenname}	Principal's First Name	First name retrieved from Active Directory of the user whose UPN is contained in the SAN field of the certificate, if present
{principal:sn}	Principal's Last Name	Last name retrieved from Active Directory of the user whose UPN is contained in the SAN field of the certificate, if present
{principal:displayname}	Principal's Display Name	Display name retrieved from Active Directory of the user whose UPN is contained in the SAN field of the certificate, if present
{requester}	Requester	The user account that requested the certificate from the CA, in the form *DOMAIN\username*
{requester:mail}	Requester's Email	Email address retrieved from Active Directory of the user account that requested the certificate from the CA, if present
{requester:givenname}	Requester's First Name	First name retrieved from Active Directory of the user account that requested the certificate from the CA, if present
{requester:sn}	Requester's Last Name	Last name retrieved from Active Directory of the user account that requested the certificate from the CA, if present
{requester:displayname}	Requester's	Display name retrieved from Active Directory of the

Variable	Name	Description
	Display Name	user account that requested the certificate from the CA, if present
{careqid}	Issuing CA / Request ID	A string containing the Issuing CA name and the certificate's Request ID from the CA
{serial}	Serial Number	The serial number of the certificate
{locations:ssl}	SSL Locations	The server location(s) where the certificate resides, if any, for certificates synchronized using SSL synchronization
{san}	Subject Alternative Name	Subject alternative name(s) contained in the certificate
{template}	Template Name	Name of the certificate template used to create the certificate
{templateshortname}	Template Short Name	Short name (often the name with no spaces) of the certificate template used to create the certificate
{thumbprint}	Thumbprint	The thumbprint (hash) of the certificate
{upn}	User Principal Name	The user principal name (UPN) contained in the subject alternative name (SAN) field of the certificate, if present (e.g. username@keyexample.com)
{metadata: Email-Contact}	Email-Contact	Example of a custom metadata field
{principal:field}	String Value from AD	Locates the object in Active Directory identified by the UPN in the certificate (if present), and substitutes the contents of the attribute named by *field*. For example: • {principal:department} • {principal:sAMAccountName} • {principal:manager} • {principal:co} **Note:** This substitutable special text field is partially user defined—you pick the field out of AD to include—and is therefore not available in the *Insert special text* dropdown; it needs to be typed manually.

Variable	Name	Description
{requester:field}	String Value from AD	Locates the object in Active Directory identified by the user or computer account that requested the certificate from the CA, and substitutes the contents of the attribute named by *field*. For example, for users: • {requester:department} • {requester:sAMAccountName} For computers: • {requester:operatingSystem} • {requester:location} • {requester:managedBy} **Note:** This substitutable special text field is partially user defined—you pick the field out of AD to include—and is therefore not available in the *Insert special text* dropdown; it needs to be typed manually.

2.1.6.2 Pending Certificate Request Alerts

Pending certificate request alerts are used to send email notifications to certificate administrators when a new certificate request that requires approval based on policy on the CA is generated. The alerts can be customized to provide detailed information about the certificate requests.

Important: These alerts are **not** used to provide email alerts or run event handlers for certificate requests that require approval based on policies configured in Keyfactor Command workflows. Pending request notification for requests handled by Keyfactor Command workflow are configured within the workflow (see Adding or Modifying a Workflow Definition on page 223).

Pending certificate requests are generated, for the most part, based on templates that are configured to require manager approval at the CA level.

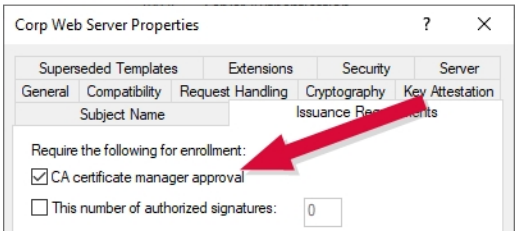


Figure 119: Certificate Template Requiring Manager Approval

The functionality of pending alerts for certificates requested within Keyfactor Command has been largely replaced by the new Keyfactor Command workflow added in Keyfactor Command version 10 (see Workflow on page 218). When alerting with Keyfactor Command workflow, templates do not need to be configured to require manager approval. This is because the approval handling is fully controlled within Keyfactor Command. In fact, templates generally should not be configured to require manager approval when using Keyfactor Command workflow, since this would generally require approval both at the Keyfactor Command level and at the CA level, depending on workflow configuration.

Pending alerts are retained for use in these scenarios:

- For customers not wishing to make use of Keyfactor Command workflow.
- For customers still in the process of migrating from CA-based workflow to Keyfactor Command workflow.
- For certificates requested outside of Keyfactor Command using templates that require manager approval.

Note: Pending request alerts are supported only for Microsort CAs and select CA gateways. This feature is not supported for EJBCA CAs.

Pending Request Alert Operations

Pending certificate request alerts are designed to send an email notification to certificate approvers when a certificate request is received that requires approval based on policy on the CA. Pending request alerts can also be sent to the original certificate requesters alerting them that their certificate requests have been sent.

Important: These alerts are **not** used to provide email alerts or run event handlers for certificate requests that require approval based on policies configured in Keyfactor Command workflows. Pending request notification for requests handled by Keyfactor Command workflow are configured within the workflow (see Adding or Modifying a Workflow Definition on page 223).

Pending Request Alert operations include:

- Creating, editing or deleting a pending alert
- Configuring an alert schedule
- Copying alerts to create similar alerts for different recipients or situations
- Testing alerts

Tip: In order to be used for PFX enrollment, a template that requires manager approval must be configured with private key retention to allow the private key generated for the request to be downloaded with the certificate after the certificate request is approved (see Certificate Template Operations on page 353).

Adding or Modifying a Pending Request Alert

1. In the Management Portal, browse to *Alerts > Pending Request*.
2. On the Pending Certificate Request Alerts page, click **Add** from the top menu to create a new alert, or **Edit** from either the top or right click menu, to modify an existing one.
3. In the Pending Request Alert Settings dialog, select your **Certificate Template** (or select **All Templates**) in the first dropdown.

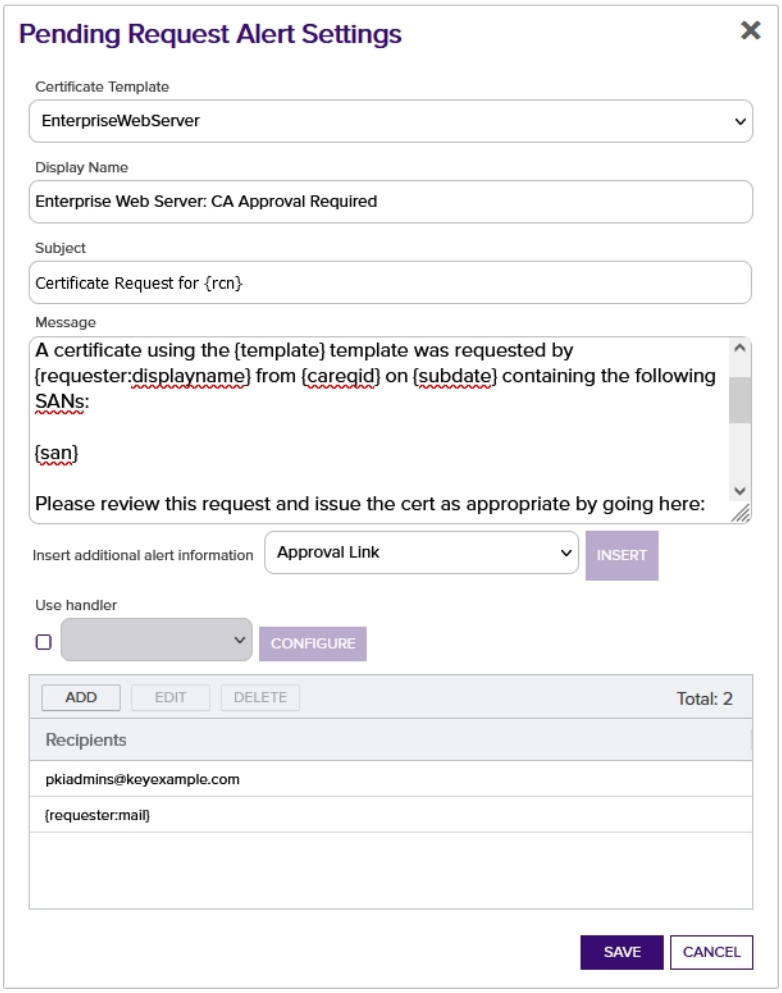


Figure 120: Create a New Pending Request Alert

4. In the **Display Name** field, enter a name for the alert. This name appears in the pending request alerts grid in the Management Portal.

5. In the **Subject** field, enter a subject line for the email message that will be delivered when the alert is triggered. You can use substitutable special text in the subject line. Substitutable special text uses a variable in the alert definition that is replaced by data from the certificate or certificate metadata at processing time. For example, you can enter {rcn} in the alert definition and each alert generated at processing time will contain the specific requested common name of the given certificate request instead of the variable {rcn}.

   To add substitutable special text to the subject line; place your cursor where you would like the text to appear on the subject line, select the appropriate variable from the *Insert special text* dropdown, and click **Insert**. Alternately, type the special text variable enclosed in curly braces (e.g. {cn}).

6. In the **Message** box, enter the body of the email message that will be delivered when the alert is triggered. You can use the **Insert special text** dropdown below the message window to add substitutable special text to the message. The metadata that appears in the dropdown will depend upon the custom metadata you have defined (see Certificate Metadata on page 646). Place your cursor where you would like the text to appear, select the appropriate variable from the dropdown, and click **Insert**. Alternately, you can type the special text variable enclosed in curly braces directly. In addition to the substitutable special text fields available in the drop-down, you can also build your own substitutable fields for the requester based on string values from the user or computer Active Directory record. See Table 8: Substitutable Special Text for Pending Request Alerts. If desired, you can format the message body using HTML. For example, you could place the certificate detail information into a table by replacing this text:

   ```
   CN: {rcn}
   DN: {rdn}
   SAN: {san}
   ```

   With this HTML code:

   ```
   <table>
   <tr><td>CN:</td><td>{rcn}</td></tr>
   <tr><td>DN:</td><td>{rdn}</td></tr>
   <tr><td>SAN:</td><td>{san}</td></tr>
   </table>
   ```

7. The **Approval Link** substitutable special text field is an important one to include in your alert intended for the administrator responsible for approving or denying the certificate request. This provides a link in the email message that the administrator can click to be taken to an approve/deny page for the certificate in the Management Portal to either approve or deny the request. This certificate-specific approval page cannot be directly accessed within the Management Portal (though you can approve certificate requests in the Management Portal from the Certificate Requests page (see Certificate Requests on page 157).

8. Check the **Use handler** box if you would like the alert to trigger an event handler at processing time, select the appropriate handler in the dropdown, and click the **Configure** button to configure the event handler. See Using Event Handlers on page 207 for more information on

using event handlers.

> **Note:** As of version 9.0 of Keyfactor Command, PowerShell scripts for alert handlers need to be in the extension path or a subdirectory of it specified by the *Extension Handler Path* application setting (see Application Settings: Console Tab on page 584). By default this is:
>
> ```
> C:\Program Files\Keyfactor\Keyfactor Platform\ExtensionLibrary\
> ```
>
> For example, create a directory called *Scripts* under the ExtensionLibrary directory and then reference your PowerShell script as *Scripts\MyPowerShell.ps1*. Any scripts referenced by PowerShell handlers that are outside this path will fail to run.

9. In the Recipients section of the page, click **Add** to add a recipient to the alert. Each alert can have multiple recipients. Recipients should be added one at a time. You can enter specific email addresses and/or use substitutable special text to replace an email address variable with actual email addresses at processing time. The built-in variable can be selected in the Recipient dialog **Use a variable from the certificate request** dropdown. In addition, you can type a special text variable enclosed in curly braces in the Email field if you have, for example, a metadata field that contains an email address.

   Keyfactor Command sends SMS (text) messages by leveraging the email to text gateways that many major mobile carriers provide. Check with your carrier for specific instructions. Keyfactor has tested that AT&T can be addressed using 10-digit-number@txt.att.net (e.g. 4155551212@txt.att.net) and Verizon can be addressed using 10-digit-number@vtext.com (e.g. 2125551212@vtext.com). T-Mobile can be addressed using 10-digit-number@tmomail.net (e.g. 2065551212@tmomail.net), but functionality can be spotty. Reliability of alerting via this method depends on the reliability of the carrier's gateways.

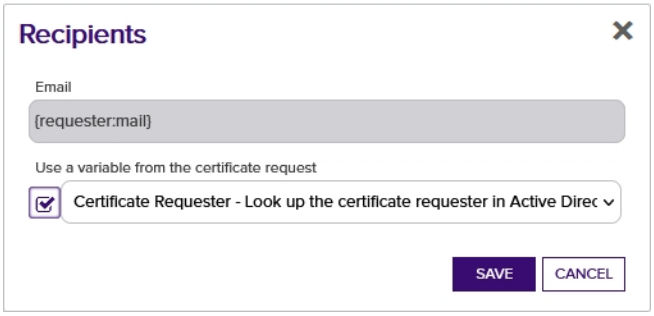


Figure 121: Pending Request Alerts Recipients

10. Click **Save** to save your pending request alert.

Copying a Pending Request Alert

You may use the copy operation to create multiple similar alerts—for example, one to the requester of the certificate and one to the administrator(s) responsible for approving it.

1. In the Management Portal, browse to *Alerts > Pending Request*.
2. On the Pending Certificate Request Alerts page, highlight the row in the alerts grid and click **Copy** at the top of the grid, or from the right click menu.
3. The Pending Request Alert Settings dialog will pop-up with the details from the selected alert. The display name field will have - *Copy* tagged to the end of it to indicate it is a new alert. You may modify the alert as needed and click **Save** to add the new alert, or **Cancel** to cancel the operation.

Deleting a Pending Request Alert

1. In the Management Portal, browse to *Alerts > Pending Request*.
2. On the Pending Certificate Request Alerts page, highlight the row in the alerts grid and click **Delete** at the top of the grid, or from the right click menu.
3. On the Confirm Operation alert, click **OK** to confirm or **Cancel** to cancel the operation.

Configuring a Pending Request Alert Schedule

After adding your desired pending request alerts, you may configure a schedule to send the alerts.

1. In the Management Portal, browse to *Alerts > Pending Request*.
2. On the Pending Certificate Request Alerts page, click the **Configure** button at the top of the Pending Request Alerts page to open the **Pending Certificate Request Alert Schedule** dialog and configure a monitoring execution schedule. This defines the frequency with which alerts are sent. You can choose to schedule the alerts for:

- **Daily** delivery at a specified time
- An **Interval** of anywhere from every 1 minute to every 12 hours
- Turn **Off** a previously configured schedule

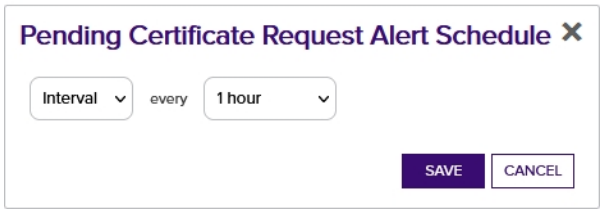


Figure 122: Pending Request Alert Schedule

Testing Pending Request Alerts

Once the alerts are configured, you may run a test of all or selected alerts to see if they are configured correctly.

1. In the Management Portal, browse to *Alerts > Pending Request*.
2. On the Pending Certificate Request Alerts page, either highlight one row in the pending request alerts grid and click the **Test** button at the top of the grid or click the **Test All** button at the top of the grid to test all the alerts.
3. In the Pending Alert Test dialog in the Alert Parameters section, click the toggle button for **Send Alerts** , if you would like to deliver email messages as part of the test.
4. Click the **Generate** button to begin generating alerts. Depending on the number of certificate requests to process, this may take a few seconds.
5. In the Pending Alert Test dialog in the Alert Data and Alert Message sections, you can review the certificate requests found to confirm that the expected requests are appearing and that the substitutable special text is being replaced as expected. Scroll the **First**, **Previous**, **Next** and **Last** buttons at the bottom of the dialog. The number of alerts generated will display between the navigation buttons.

Tip: Alerts are generated for all certificate requests that have not previously been alerted on, unless the system has been configured to send multiple alerts per request. By default, one alert is sent to each recipient for any given request. The number of alerts to send for a given request is configurable with the *Pending Alert Max Reminders* setting in Keyfactor Command application settings (see Application Settings: Console Tab on page 584). If a certificate remains in a pending state after the configured number of alerts has been sent, no further alerts will be sent.
By default, a maximum of 100 alerts will be generated during a test. The maximum value is configurable with the *Pending Alert Test Result Limit* setting in Keyfactor Command application settings (see Application Settings: Console Tab on page 584). If more than 100 alerts are generated, no email messages will be sent and you'll have the opportunity to view the first 100 alerts generated.

If you're using an event handler, the event handler is run and the handler actions taken (PowerShell script run, event log message) when the test is run. This is true whether or not you click the *Send Alerts* toggle.

Note: HTML does not render in the alert viewer.

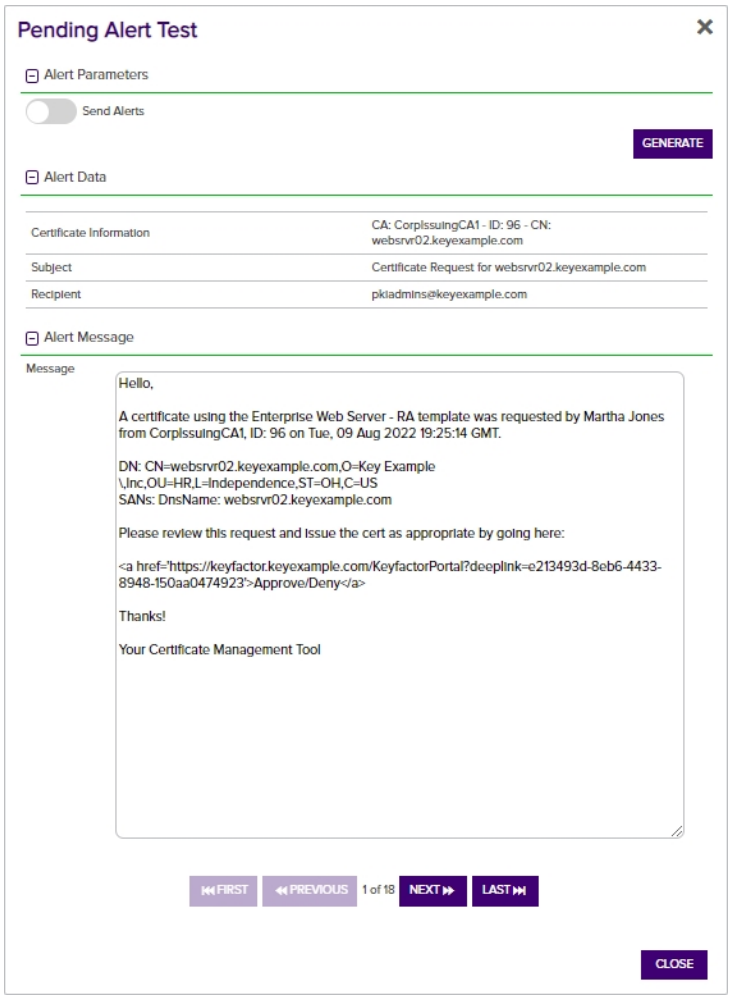


Figure 123: Pending Alert Test

Refer to the following table for a complete list of the substitutable special text that can be used to customize alert messages.

Table 8: Substitutable Special Text for Pending Request Alerts

Variable	Name	Description
{apprlink}	Approval Link	Link pointing to the certificate-specific approval page in the Management Portal where the person responsible for approving the request can go to approve or deny the request
{reqid}	CMS Request Id	The request ID for the certificate as stored in the Keyfactor Command database. This is not the same as the request ID issued by the CA.

Variable	Name	Description
{rcn}	Requested Common Name	Common name contained in the certificate request
{rdn}	Requested Distinguished Name	Distinguished name contained in the certificate request
{requester}	Requester	The user account that requested the certificate from the CA, in the form *DOMAIN\username*
{requester:mail}	Requester's Email	Email address retrieved from Active Directory of the user account that requested the certificate from the CA, if present
{requester:givenname}	Requester's First Name	First name retrieved from Active Directory of the user account that requested the certificate from the CA, if present
{requester:sn}	Requester's Last Name	Last name retrieved from Active Directory of the user account that requested the certificate from the CA, if present
{requester:displayname}	Requester's Display Name	Display name retrieved from Active Directory of the user account that requested the certificate from the CA, if present
{careqid}	Issuing CA / Request ID	A string containing the Issuing CA name and the certificate's Request ID from the CA
{san}	Subject Alternative Name	Subject alternative name(s) contained in the certificate request. There are four possible sources for the SANs that appear here: • For CSR enrollment, the original SANs included in the CSR. • Any SANs added through the Keyfactor Command Management Portal. For CSR enrollment, these take the place of the SANs in the CSR if the ATTRIBUTESUBJECTALTNAME2 option is enabled on the CA. See CSR Enrollment on page 131. • A SAN matching the CN added automatically during enrollment as a result of setting the RFC 2818 compliance flag in

Variable	Name	Description
		the CA configuration. See Adding or Modifying a CA Record on page 330. For PFX enrollment, the user has the option of editing this entry at enrollment time; entry of something is required. • A SAN matching the CN added automatically by the Keyfactor Command policy module on the CA if the Keyfactor Command RFC 2818 Policy Handler is enabled, if one was not included in the CSR or added manually. See *Installing the Keyfactor CA Policy Module Handlers* in the *Keyfactor Command Server Installation Guide*.
{subdate}	Submission Date	Date the certificate request was submitted
{template}	Template Name	Name of the certificate template used to create the certificate request
{templateshortname}	Template Short Name	Short name (often the name with no spaces) of the certificate template used to create the certificate request
{metadata: Email-Contact}	Email-Contact	Example of a custom metadata field
{requester:field}	String Value from AD	Locates the object in Active Directory identified by the user or computer account that requested the certificate from the CA, and substitutes the contents of the attribute named by *field*. For example, for users: • {requester:department} • {requester:sAMAccountName} For computers: • {requester:operatingSystem} • {requester:location} • {requester:managedBy} **Note:** This substitutable special text field is partially user defined—you pick the field out of AD to include—and is therefore not available in the *Insert special text* dropdown; it needs to be typed manually.

2.1.6.3 Issued Certificate Request Alerts

Issued certificate request alerts are used to send email notifications to certificate requesters, or other relevant parties, when a new certificate is issued through any CA that syncs to Keyfactor Command. The alerts can be customized to provide detailed information about the certificates.

Note: Because Issued Certificate Request Alerts are sent for any CAs synced to Keyfactor Command, it is recommended that any CAs are synced first and then the Issued Certificate Request Alerts set up afterward to avoid a lot of unnecessary emails, upon syncing.

Issued Request Alert Operations

An issued certificate request alert is designed to send an email notification to a certificate requester when a certificate request he or she made using a certificate template that required manager approval is approved.

Issued Request Alert operations include: creating, editing or deleting an issued request alerts, configuring an alert schedule, and copying alerts to create similar alerts for different recipients or collections.

The issued alert handler runs immediately when an enrollment is approved within the Keyfactor Command platform and also runs via a schedule to pick up any approvals done outside of Keyfactor Command.

Adding or Modifying an Issued Request Alert

1. In the Management Portal, browse to *Alerts > Issued Request*.
2. On the Issued Certificate Request Alerts page, click **Add** from the top menu to create a new alert, or **Edit** ,from either the top or right click menu, to modify an existing one.
3. In the Issued Certificate Alert Settings dialog, select your **Certificate Template** (or select **All Templates**) in the first dropdown.

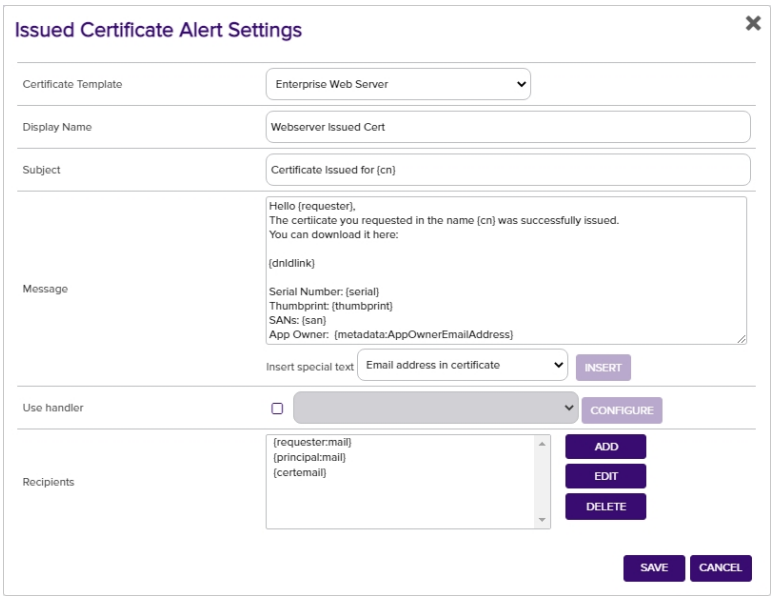


Figure 124: Create a New Issued Certificate Alert

4. In the **Display Name** field, enter a name for the alert. This name appears in the list of issued certificate alerts in the Management Portal.

5. In the **Subject** field, enter a subject line for the email message that will be delivered when the alert is triggered. You can use substitutable special text in the subject line. Substitutable special text uses a variable in the alert definition that is replaced by data from the certificate or certificate metadata at processing time. For example, you can enter {cn} in the alert definition and each alert generated will contain the specific common name of the given certificate instead of the variable {cn}.

   To add substitutable special text to the subject line; place your cursor where you would like the text to appear on the subject line, select the appropriate variable from the *Insert special text* dropdown, and click **Insert**. Alternately, type the special text variable enclosed in curly braces (e.g. {cn}).

6. In the **Message** box, enter the body of the email message that will be delivered when the alert is triggered. You can use the **Insert special text** dropdown below the message window to add substitutable special text to the message. The metadata that appears in the dropdown will depend upon the custom metadata you have defined (see Certificate Metadata on page 646). Place your cursor where you would like the text to appear, select the appropriate variable from the dropdown, and click **Insert**. Alternately, you can type the special text variable enclosed in curly braces directly. In addition to the substitutable special text fields available in the dropdown, you can also build your own substitutable fields for the requester based on string values from the user or computer Active Directory record. See Substitutable Special Text for Issued Certificate Alerts on page 186. If desired, you can format the message body using HTML. For

example, you could place the certificate detail information into a table by replacing this text:

```
Serial Number: {serial}
Thumbprint: {thumbprint}
SANs: {san}
App Owner: {metadata:AppOwnerFirstName} {metadata:AppOwnerLastName}
```

With this HTML code:

```
<table>
<tr><td>Serial Number: </td><td>{serial}</td></tr>
<tr><td>Thumbprint: </td><td>{thumbprint}</td></tr>
<tr><td>SANs: </td><td>{san}</td></tr>
<tr><td>App Owner: </td><td>{metadata:AppOwnerFirstName} {metadata:Ap-
pOwnerLastName}</td></tr>
</table>
```

7. The **Download Link** substitutable special text field is an important one to include in your alert intended for the requester of the certificate or the person responsible for installing the certificate. This provides a link in the email message that the user can click to be taken to the Keyfactor Command Management Portal to download the certificate.

Tip: If the users who will receive the issued alerts do not have global *Read* permissions for *Certificates*, they will not be able to use the built-in download link. To resolve this, you can build a custom download link as follows:

a. If you do not already have a *My Certificates* collection, create one using the %ME% special value with a search string of:

```
NetBIOSRequester -eq "%ME%"
```

b. In the Management Portal, browse to the *My Certificates* collection page and look in the browser's address bar at the end of the URL for the number that has been assigned to the collection. For example, the following URL points to collection 9:

```
https://keyfactor.keyexample.com/KeyfactorPortal/CertificateCollection/Edi
t?cid=9
```

c. Grant the users who will receive the issued alerts *Read* permissions on the *My Certificates* collection (see Certificate Permissions on page 621).

d. In the message body of the issued alert, create a link that looks like the following, where keyfactor.keyexample.com is the name of your Keyfactor Command server and ID is the correct collection ID for your *My Certificates* collection (e.g. 9):

```
<a
href="https://
keyfactor.keyexample.com
```

```
/KeyfactorPortal/CertificateCollection/Edit?cid=ID&query=Thumbprint+-
eq+%22{thumbprint}%22">Download Now</a>
```

8. Check the **Use handler** box if you would like the alert to trigger an event handler at processing time, select the appropriate handler in the dropdown, and click the **Configure** button to configure the event handler. See Using Event Handlers on page 207 for more information on using event handlers.

   Note: As of version 9.0 of Keyfactor Command, PowerShell scripts for alert handlers need to be in the extension path or a subdirectory of it specified by the *Extension Handler Path* application setting (see Application Settings: Console Tab on page 584). By default this is:

   ```
   C:\Program Files\Keyfactor\Keyfactor Platform\ExtensionLibrary\
   ```

   For example, create a directory called *Scripts* under the ExtensionLibrary directory and then reference your PowerShell script as *Scripts\MyPowerShell.ps1*. Any scripts referenced by PowerShell handlers that are outside this path will fail to run.

9. In the Recipients section of the page, click **Add** to add a recipient to the alert. Each alert can have multiple recipients. Recipients should be added one at a time. You can enter specific email addresses and/or use substitutable special text to replace an email address variable with actual email addresses at processing time. There are three built-in variables that can be selected in the Recipient dialog **Use a variable from the certificate request** dropdown. In addition, you can type a special text variable enclosed in curly braces in the Email field if you have, for example, a metadata field that contains an email address.

   Keyfactor Command sends SMS (text) messages by leveraging the email to text gateways that many major mobile carriers provide. Check with your carrier for specific instructions. Keyfactor has tested that AT&T can be addressed using 10-digit-number@txt.att.net (e.g. 4155551212@txt.att.net) and Verizon can be addressed using 10-digit-number@vtext.com (e.g. 2125551212@vtext.com). T-Mobile can be addressed using 10-digit-number@tmomail.net (e.g. 2065551212@tmomail.net), but functionality can be spotty. Reliability of alerting via this method depends on the reliability of the carrier's gateways.

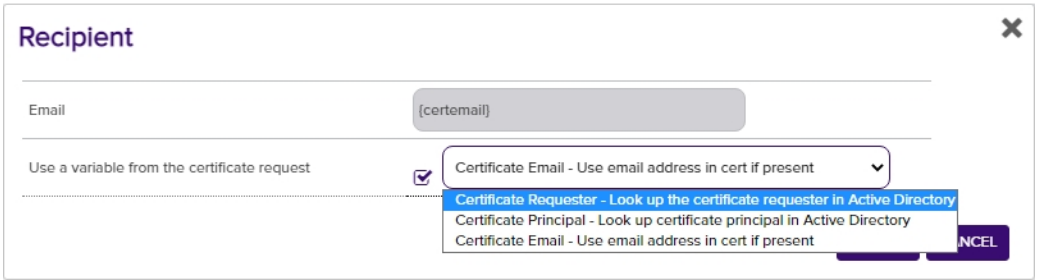


Figure 125: Issued Certificate Alerts Recipients

10. Click **Save** to save your issued certificate alert.

Copying an Issued Request Alert

You may use the copy operation to create multiple similar alerts—for example, one to the requester of the certificate and another with a different message to the person responsible for installing it.

1. In the Management Portal, browse to *Alerts > Issued Request*.
2. On the Issued Certificate Request Alerts page, highlight the row in the alerts grid and click **Copy** at the top of the grid, or from the right click menu.
3. The Issued Certificate Alert Settings dialog will pop-up with the details from the selected alert. The display name field will have - *Copy* tagged to the end of it to o indicate it is a new alert. You may modify the alert as needed and click **Save** to add the new alert, or **Cancel** to cancel the operation.

Deleting an Issued Request Alert

1. In the Management Portal, browse to *Alerts > Issued Request*.
2. On the Issued Certificate Request Alerts page, highlight the row in the alerts grid and click **Delete** at the top of the grid, or from the right click menu.
3. On the Confirm Operation alert, click **OK** to confirm or **Cancel** to cancel the operation.

Configuring an Issued Request Alert Schedule

After adding your desired issued alerts, you may configure a schedule to send the alerts.

1. In the Management Portal, browse to *Alerts > Issued Request*.
2. On the Issued Certificate Request Alerts page, click the **Configure** button at the top of the Issued Certificate Request Alerts page to configure a monitoring execution schedule. This defines the frequency with which alerts are sent. You can choose to schedule the alerts either for daily delivery at a specified time or at intervals of anywhere from every 1 minute to every 12 hours. A short interval is the most common configuration.

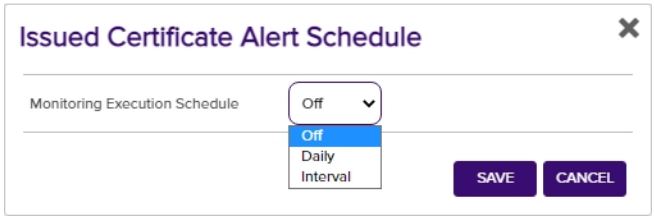


Figure 126: Issued Alert Schedule

Refer to the following table for a complete list of the substitutable special text that can be used to customize alert messages.

Table 9: Substitutable Special Text for Issued Certificate Alerts

Variable	Name	Description
{dnldlink}	Download Link	Link pointing to the Certificate Requests page in the Keyfactor Command Management Portal where the certificate requester or the person responsible for installing the certificate can go to download the certificate. The certificate will be available only in a .cer-/.crt format (without the private key) unless private key retention has been enabled on the template (see Certificate Templates on page 352).
{certemail}	Email Address in Certificate	Email address contained in the certificate, if present
{cn}	Common Name	Common name contained in the certificate
{dn}	Distinguished Name	Distinguished name contained in the certificate
{certnotbefore}	Issue Date	Validity date of the certificate
{certnotafter}	Expiration Date	Expiration date of the certificate
{issuerDN}	Issuer DN	Distinguished name of the certificate's issuer
{principal:mail}	Principal's Email	Email address retrieved from Active Directory of the user whose UPN is contained in the SAN field of the certificate, if present
{principal:givenname}	Principal's First Name	First name retrieved from Active Directory of the user whose UPN is contained in the SAN field of the certificate, if present
{principal:sn}	Principal's Last Name	Last name retrieved from Active Directory of the user whose UPN is contained in the SAN field of the certificate, if present
{principal:displayname}	Principal's Display Name	Display name retrieved from Active Directory of the user whose UPN is contained in the SAN field of the certificate, if present
{requester}	Requester	The user account that requested the certificate from the CA, in the form *DOMAIN\username*

Variable	Name	Description
{requester:mail}	Requester's Email	Email address retrieved from Active Directory of the user account that requested the certificate from the CA, if present
{requester:givenname}	Requester's First Name	First name retrieved from Active Directory of the user account that requested the certificate from the CA, if present
{requester:sn}	Requester's Last Name	Last name retrieved from Active Directory of the user account that requested the certificate from the CA, if present
{requester:displayname}	Requester's Display Name	Display name retrieved from Active Directory of the user account that requested the certificate from the CA, if present
{careqid}	Issuing CA / Request ID	A string containing the Issuing CA name and the certificate's Request ID from the CA
{serial}	Serial Number	The serial number of the certificate
{san}	Subject Alternative Name	Subject alternative name(s) contained in the certificate
{template}	Template Name	Name of the certificate template used to create the certificate
{templateshortname}	Template Short Name	Short name (often the name with no spaces) of the certificate template used to create the certificate request
{thumbprint}	Thumbprint	The thumbprint (hash) of the certificate
{upn}	User Principal Name	The user principal name (UPN) contained in the subject alternative name (SAN) field of the certificate, if present (e.g. username@keyexample.com)
{metadata:Email-Contact}	Email-Contact	Example of a custom metadata field
{requester:field}	String Value from AD	Locates the object in Active Directory identified by the user or computer account that requested the certificate from the CA, and substitutes the contents of the attribute named by "field". For example, for users: • {requester:department}

Variable	Name	Description
		• {requester:sAMAccountName} For computers: • {requester:operatingSystem} • {requester:location} • {requester:managedBy} **Note:** This substitutable special text field is partially user defined—you pick the field out of AD to include—and is therefore not available in the *Insert special text* dropdown; it needs to be typed manually.

2.1.6.4 Denied Certificate Request Alerts

Denied certificate request alerts are used to send email notifications to certificate requesters or other relevant parties when a certificate request that required approval is denied through Keyfactor Command. The alerts can be customized to provide detailed information about the certificate requests.

Important: These alerts are **not** used to provide email alerts or run event handlers for certificate requests that require approval based on policies configured in Keyfactor Command workflows. Denial notification for requests handled by Keyfactor Command workflow are configured within the workflow (see Adding or Modifying a Workflow Definition on page 223).

Unlike pending certificate request alerts that are sent on a configurable schedule, denied certificate request alerts are sent immediately after the certificate request is denied through Keyfactor Command.

Tip: Click the help icon (?) next to the page title to open the embedded web copy of the *Keyfactor Command Documentation Suite* to this section.
You can also find the help icon at the top of the page next to the **Log Out** button. From here you can choose to open either the *Keyfactor Command Documentation Suite* at the home page or the *Keyfactor API Endpoint Utility*.

Denied Certificate Request Alert Operations

A denied certificate request alert is designed to send an email notification to a certificate requester when a certificate request he or she made using a certificate template that required manager approval is denied. It can include a comment from the administrator who denied the request indicating why the request was denied. From the Denied Certificate Request Alert page you can add a

new alert, edit an existing one, delete an alert and copy an existing alert to form a template for a new alert.

Adding or Modifying a Denied Certificate Request Alert

1. In the Management Portal, browse to *Alerts > Denied Request*.
2. On the Denied Certificate Requests Alerts page, click **Add** at the top of the grid to create a new alert, or click **Edit** to modify an existing one (**Edit** is also available from the right click menu).
3. In the Denied Certificate Request Alert Settings dialog, select your Certificate Template (or select **All Templates**) in the first dropdown.

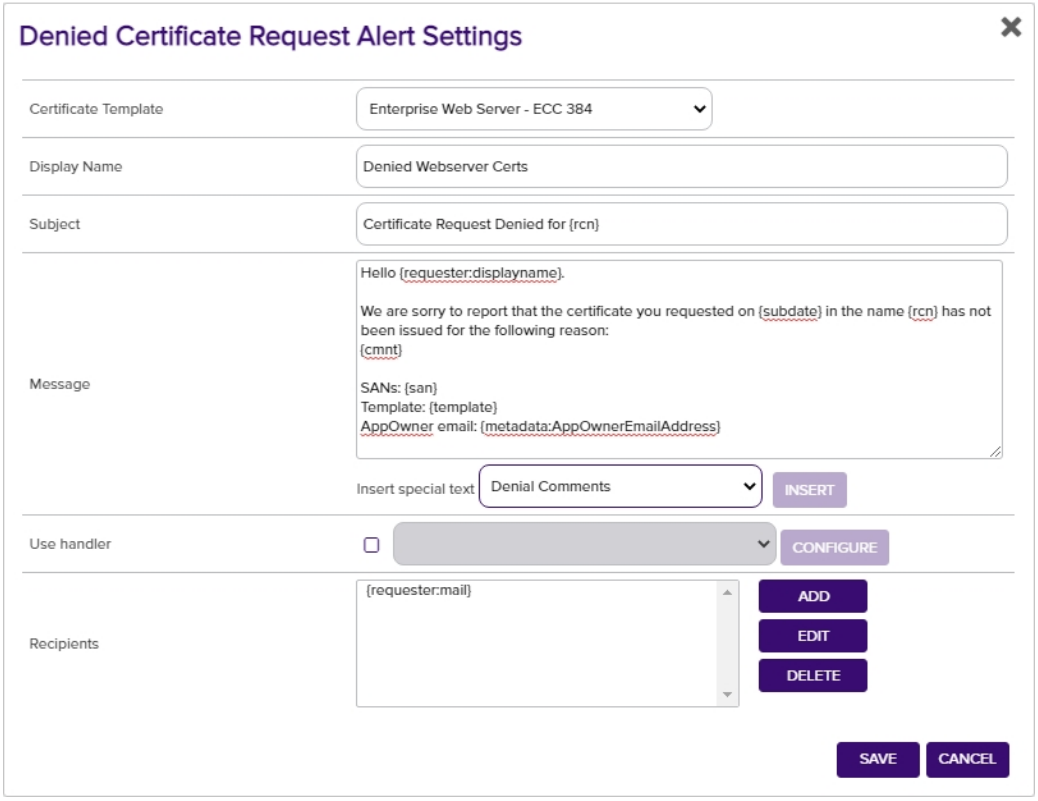


Figure 127: Create a New Denied Certificate Request Alert

4. In the **Display Name** field, enter a name for the alert. This name appears in the list of denied certificate request alerts in the Management Portal.
5. In the **Subject** field, enter a subject line for the email message that will be delivered when the alert is triggered. You can use substitutable special text in the subject line. Substitutable special text uses a variable in the alert definition that is replaced by data from the certificate or certificate metadata at processing time. For example, you can enter {rcn} in the alert definition and each alert generated will contain the specific requested common name of the given request

instead of the variable {rcn}.

To add substitutable special text to the subject line; place your cursor where you would like the text to appear on the subject line, select the appropriate variable from the *Insert special text* dropdown, and click **Insert**. Alternately, type the special text variable enclosed in curly braces (e.g. {cn}).

6. In the **Message** box, enter the body of the email message that will be delivered when the alert is triggered. You can use the **Insert special text** dropdown below the message window to add substitutable special text to the message. The metadata that appears in the dropdown will depend upon the custom metadata you have defined (see Certificate Metadata on page 646). Place your cursor where you would like the text to appear, select the appropriate variable from the dropdown, and click **Insert**. Alternately, you can type the special text variable enclosed in curly braces directly. In addition to the substitutable special text fields available in the drop-down, you can also build your own substitutable fields for the requester based on string values from the user or computer Active Directory record. See Table 10: Substitutable Special Text for Denied Certificate Request Alerts. If desired, you can format the message body using HTML.

7. The **Denial Comments** substitutable special text field is an important one to include in your alert intended for the requester of the certificate. This provides the comment the administrator made at the time he or she denied the certificate request (see Certificate Requests on page 157).

8. Check the **Use handler** box if you would like the alert to trigger an event handler at processing time, select the appropriate handler in the dropdown, and click the **Configure** button to configure the event handler. See Event Handler Registration on page 674 for more information on using event handlers.

   Note: As of version 9.0 of Keyfactor Command, PowerShell scripts for alert handlers need to be in the extension path or a subdirectory of it specified by the *Extension Handler Path* application setting (see Application Settings: Console Tab on page 584). By default this is:

   ```
   C:\Program Files\Keyfactor\Keyfactor Platform\ExtensionLibrary\
   ```

   For example, create a directory called *Scripts* under the ExtensionLibrary directory and then reference your PowerShell script as *Scripts\MyPowerShell.ps1*. Any scripts referenced by PowerShell handlers that are outside this path will fail to run.

9. In the Recipients section of the page, click **Add** to add a recipient to the alert. Each alert can have multiple recipients. Recipients should be added one at a time. You can enter specific email addresses and/or use substitutable special text to replace an email address variable with actual email addresses at processing time. There are three built-in variables that can be selected in the Recipient dialog **Use a variable from the certificate request** dropdown. In addition, you can type a special text variable enclosed in curly braces in the Email field if you have, for example, a metadata field that contains an email address.

Keyfactor Command sends SMS (text) messages by leveraging the email to text gateways that many major mobile carriers provide. Check with your carrier for specific instructions. Keyfactor has tested that AT&T can be addressed using 10-digit-number@txt.att.net (e.g. 4155551212@tx-t.att.net) and Verizon can be addressed using 10-digit-number@vtext.com (e.g. 2125551212@v-text.com). T-Mobile can be addressed using 10-digit-number@tmomail.net (e.g. 2065551212@tmomail.net), but functionality can be spotty. Reliability of alerting via this method depends on the reliability of the carrier's gateways.

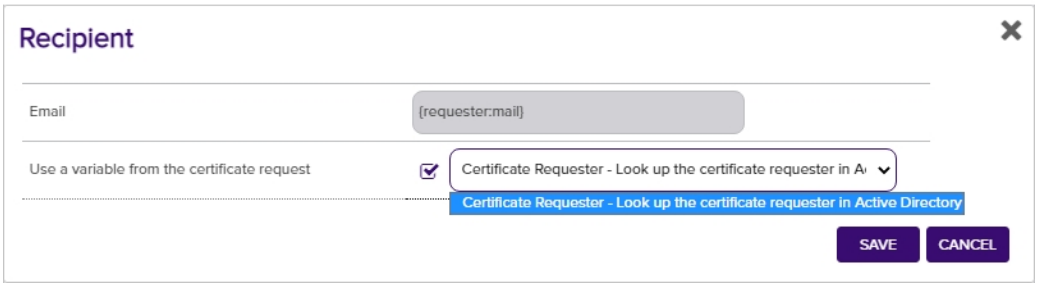


Figure 128: Denied Certificate Request Alerts Recipients

10. Click **Save** to save your denied certificate request alert.

Copying a Denied Certificate Request Alert

You may use the copy operation to create multiple similar alerts—for example, one to the requester of the certificate and another with a different message to the application owner for whom it was intended.

1. In the Management Portal, browse to *Alerts > Denied Request*.
2. On the Denied Certificate Requests Alerts page, highlight the row in the denied certificate request alerts grid and click **Copy** at the top of the grid, or from the right click menu.
3. The Denied Certificate Request Alert Settings dialog will pop-up with the details from the selected alert. The display name field will have - *Copy* tagged to the end of it to indicate it is a new alert. You may modify the alert as needed and click **Save** to add the new alert, or **Cancel** to cancel the operation.

Deleting a Denied Certificate Request Alert

1. In the Management Portal, browse to *Alerts > Denied Request*.
2. On the Denied Certificate Requests Alerts page, highlight the row in the denied certificate request alerts grid and click **Delete** at the top of the grid, or from the right click menu.
3. On the Confirm Operation alert, click **OK** to confirm or **Cancel** to cancel the operation.

Refer to the following table for a complete list of the substitutable special text that can be used to customize alert messages.

Table 10: Substitutable Special Text for Denied Certificate Request Alerts

Variable	Name	Description
{cmnt}	Denial Comments	Comments provided by the administrator responsible for approving or denying the certificate request at the time the request was denied
{rcn}	Requested Common Name	Common name contained in the certificate request
{rdn}	Requested Distinguished Name	Distinguished name contained in the certificate request
{requester:mail}	Requester's Email	Email address retrieved from Active Directory of the user account that requested the certificate from the CA, if present
{requester:givenname}	Requester's First Name	First name retrieved from Active Directory of the user account that requested the certificate from the CA, if present
{requester:sn}	Requester's Last Name	Last name retrieved from Active Directory of the user account that requested the certificate from the CA, if present
{requester:displayname}	Requester's Display Name	Display name retrieved from Active Directory of the user account that requested the certificate from the CA, if present
{careqid}	Issuing CA / Request ID	A string containing the Issuing CA name and the certificate's Request ID from the CA
{san}	Subject Alternative Name	Subject alternative name(s) contained in the certificate request
{subdate}	Submission Date	Date the certificate request was submitted
{template}	Template Name	Name of the certificate template used to create the certificate request
{templateshortname}	Template Short Name	Short name (often the name with no spaces) of the certificate template used to create the certificate request
{metadata:Email-Contact}	Email-Contact	Example of a custom metadata field
{requester:field}	String Value	Locates the object in Active Directory identified by

Variable	Name	Description
	from AD	the user or computer account that requested the certificate from the CA, and substitutes the contents of the attribute named by *field*. For example, for users: • {requester:department} • {requester:sAMAccountName} For computers: • {requester:operatingSystem} • {requester:location} This substitutable special text field is partially user defined—you pick the field out of AD to include—and is therefore not available in the *Insert special text* drop-down; it needs to be typed manually.

2.1.6.5 Key Rotation Alerts

Key rotation alerts are used to send email notifications to SSH key users and/or administrators when a key is nearing the end of the key lifetime. The default key lifetime is 365 days, but this setting is configurable (see Application Settings: SSH Tab on page 604). Key rotation alerts apply to both user keys (see My SSH Key on page 512) and service account keys (see Service Account Keys on page 524) generated within Keyfactor Command.

The alerts can be customized to provide detailed information about the keys along with, for example, instructions to users on how to enroll for a replacement key.

Key Rotation Alert Operations

Key Rotation alert operations include: creating, editing or deleting a key rotation alert, configuring an alert schedule, copying alerts to create similar alerts for different recipients or collections, and testing alerts.

Adding or Modifying a Key Rotation Alert

1. In the Management Portal, browse to *Alerts > Key Rotation*.
2. On the Key Rotation Alerts page, click **Add** from the top menu to create a new alert, or **Edit** ,from either the top or right click menu, to modify an existing one.
3. In the Key Rotation Alert Settings dialog, select a **Timeframe** for the alert by choosing the number of days, weeks, or months to define the alert period.

Note: When the alert is stored in the database, weeks are converted to 7 days and months are converted to 30 days.

4. In the Key Rotation Alert Settings dialog, enter a **Display Name** for the alert. This name appears in the list of key rotation alerts in the Management Portal.

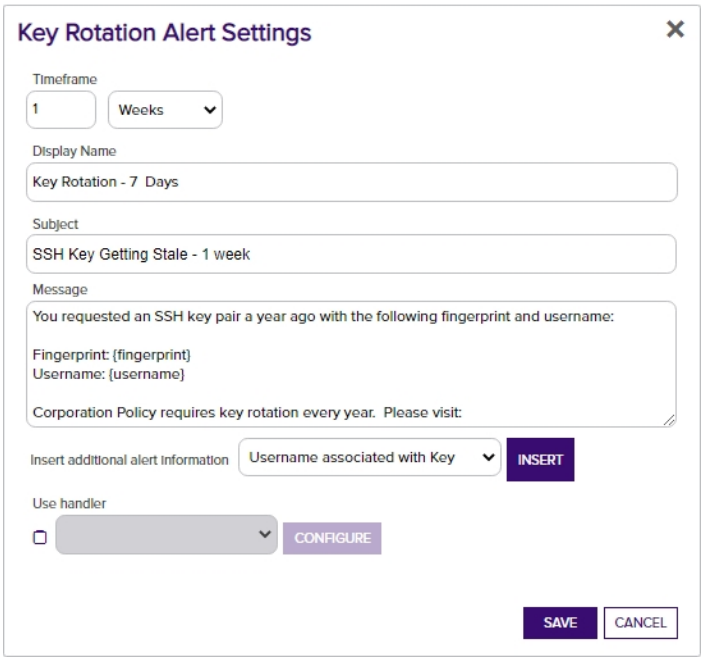


Figure 129: Key Rotation Alerts Recipients

5. In the **Subject** field, enter a subject line for the email message that will be delivered when the alert is triggered. You can use substitutable special text in the subject line. Substitutable special text uses a variable in the alert definition that is replaced by data from the key record at processing time. For example, you can enter {fingerprint} in the alert definition and each alert generated at processing time will contain the specific fingerprint of the given key instead of the variable {fingerprint}. To add substitutable special text to the subject line, type the special text variable enclosed in curly braces (e.g. {fingerprint}).

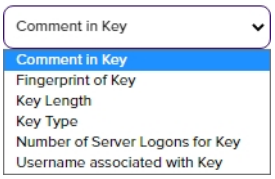


Figure 130: Substitutable Special Text for Key Rotation Alerts

6. In the **Message** box, enter the body of the email message that will be delivered when the alert is triggered. You can use the **Insert special text** dropdown below the message window to add substitutable special text to the message. Place your cursor where you would like the text to appear, select the appropriate variable from the dropdown, and click **Insert**. Alternately, you can type the special text variable enclosed in curly braces directly. If desired, you can format the message body using HTML. For example, you could place the key detail information into a table by replacing this text:

   Fingerprint: {fingerprint}

   Username: {username}

   Comment: {comment}

   With this HTML code:

   ```
   <table>

   <tr><td>Fingerprint:</td><td>{fingerprint}</td></tr>

   <tr><td>Username:</td><td>{username}</td></tr>

   <tr><td>Comment:</td><td>{comment}</td></tr>

   </table>
   ```

7. Check the **Use handler** box if you would like the alert to trigger an event handler at processing time, select the appropriate handler in the dropdown, and click the **Configure** button to configure the event handler. See Using Event Handlers on page 207 for more information on using event handlers.

   Note: As of version 9.0 of Keyfactor Command, PowerShell scripts for alert handlers need to be in the extension path or a subdirectory of it specified by the *Extension Handler Path* application setting (see Application Settings: Console Tab on page 584). By default this is:

   ```
   C:\Program Files\Keyfactor\Keyfactor Platform\ExtensionLibrary\
   ```

   For example, create a directory called *Scripts* under the ExtensionLibrary directory and then reference your PowerShell script as *Scripts\MyPowerShell.ps1*. Any scripts referenced by PowerShell handlers that are outside this path will fail to run.

8. Click **Save** to save your key rotation alert.

Copying an existing key rotation alert:

You may use the copy operation to create multiple similar alerts—for example, one for a warning a month in advance of the stale date of keys and another shortly before the keys become stale.

1. In the Management Portal, browse to *Alerts > Key Rotation.*
2. On the Key Rotation Alerts page, highlight the row in the alerts grid and click **Copy** at the top of the grid, or from the right click menu.
3. The Key Rotation Alert Settings dialog will pop-up with the details from the selected alert. The display name field will have - *Copy* tagged to the end of it to indicate it is a new alert. You may modify the alert as needed and click **Save** to add the new alert, or **Cancel** to cancel the operation.

Deleting a Key Rotation Alert

1. In the Management Portal, browse to *Alerts > Key Rotation.*
2. On the Key Rotation Alerts page, highlight the row in the alerts grid and click **Delete** at the top of the grid, or from the right click menu.
3. On the Confirm Operation alert, click **OK** to confirm or **Cancel** to cancel the operation.

Configuring a Key Rotation Alert Schedule

After adding your desired key rotation alerts, you may configure a schedule to send the alerts.

1. In the Management Portal, browse to *Alerts > Key Rotation.*
2. On the Key Rotation Alerts page, click the **Configure** button at the top of the Key Rotation Alerts page to configure an alert execution schedule. This defines the frequency with which key rotation alerts are sent. This type of alert is scheduled for daily delivery at a specified time.

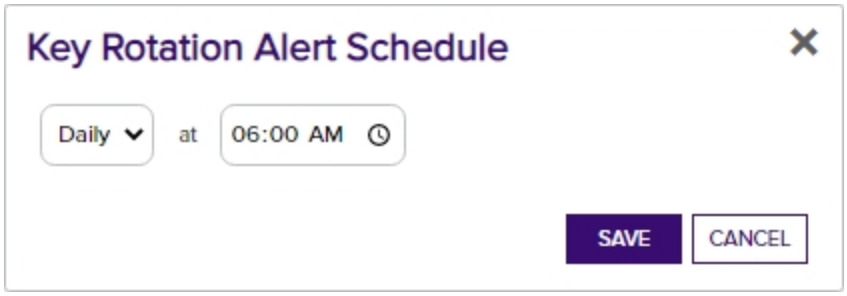


Figure 131: Key Rotation Alert Schedule

Testing Key Rotation Alerts

Once the alerts are configured, you may run a test of all or selected alerts to see if they are configured correctly.

1. In the Management Portal, browse to *Alerts > Key Rotation*.
2. On the Key Rotation Alerts page, either highlight one row in the expiration alert grid and click the **Test** button at the top of the grid or click the **Test All** button at the top of the grid to test all the alerts.
3. In the Key Rotation Alert Viewer dialog in the Alert Parameters section, select a **Start Date** and **End Date** for testing. You can use this option to simulate running the alerts a month from now instead of today, for example, or put in a broad date range to be sure you pick up some expiring certificates for testing purposes.
4. In the Key Rotation Alert Viewer dialog in the Alert Parameters section, click the toggle button for **Send Alerts** if you would like to deliver email messages as part of the test.
5. Click the **Generate** button to begin generating alerts. Depending on the number of keys to process, this may take a few seconds.
6. In the Key Rotation Alert Viewer dialog in the Alert Data and Alert Message sections, you can review the keys found to confirm that the expected keys are appearing and that the substitutable special text is being replaced as expected. Scroll through the alerts using the **First**, **Previous**, **Next** and **Last** buttons at the bottom of the dialog. The number of alerts generated will display between the navigation buttons.

Tip: Alerts are generated when an SSH key is approaching or has reached its stale date as defined by the timeframe configured in the alert and the SSH key lifetime (the *Key Lifetime (days)* application setting).
By default, a maximum of 100 alerts will be generated during a test. The maximum value is configurable with the *Key Rotation Alert Test Result Limit* setting in Keyfactor Command application settings (see Application Settings: Console Tab on page 584 in the *Keyfactor Command Reference Guide*). If more than 100 alerts are generated, no email messages will be sent and you'll have the opportunity to view the first 100 alerts generated.

If you're using an event handler, the event handler is run and the handler actions taken (PowerShell script run, event log message written) when the test is run. This is true whether or not you click the *Send Alerts* toggle.

Note: HTML does not render in the alert viewer.

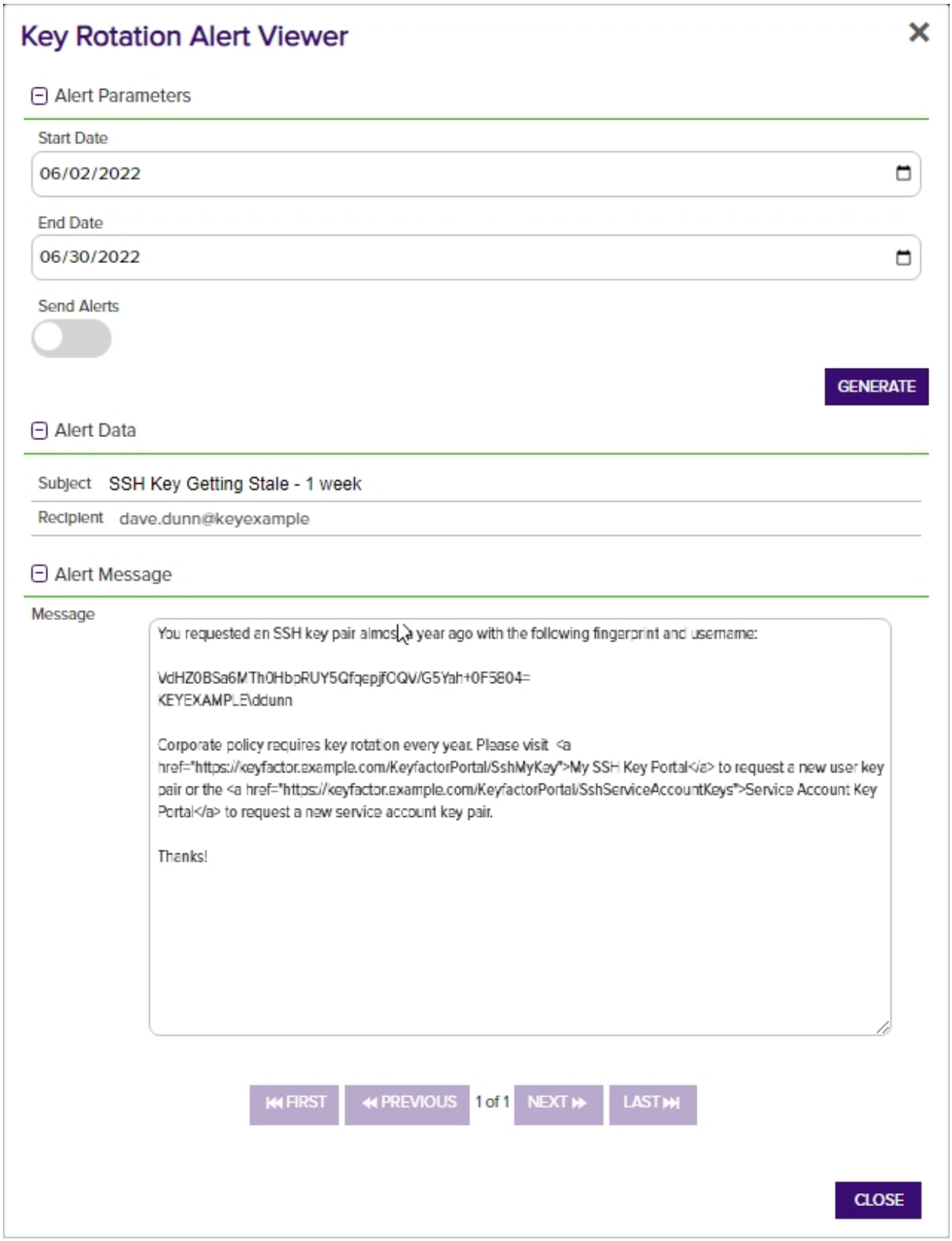

Key Rotation Alert Viewer
Alert Parameters
Start Date
06/02/2022
End Date
06/30/2022
Send Alerts
GENERATE
Alert Data
Subject SSH Key Getting Stale - 1 week
Recipient dave.dunn@keyexample
Alert Message
Message
You requested an SSH key pair almost a year ago with the following fingerprint and username:
VdHZ0BSa6MTh0HbpRUY5QfqepjfCQV/G5Yah+0F5804=
KEYEXAMPLE\ddunn
Corporate policy requires key rotation every year. Please visit My SSH Key Portal to request a new user key pair or the Service Account Key Portal to request a new service account key pair.
Thanks!
FIRST
PREVIOUS
1 of 1
NEXT
LAST
CLOSE

Figure 132: Key Rotation Alert Viewer

Refer to the following table for a complete list of the substitutable special text that can be used to customize alert messages.

Table 11: Substitutable Special Text for Key Rotation Alerts

Variable	Name	Description
{comment}	Comment in Key	The user-defined descriptive comment, if any, on the key. Although entry of an email address in the comment field of an SSH key is traditional, this is not a required format. The comment may can contain any characters supported for string fields, including spaces and most punctuation marks.
{fingerprint}	Fingerprint of Key	The fingerprint of the public key. Each SSH public key has a single cryptographic fingerprint that can be used to uniquely identify the key.
{keylength}	Key Length	The key length for the key. The key length depends on the key type selected. Keyfactor Command supports 256 bits for Ed25519 and ECDSA and 2048 or 4096 bits for RSA.
{keytype}	Key Type	A number of cryptographic algorithms can be used to generate SSH keys. Keyfactor Command supports RSA, Ed25519, and ECDSA. RSA keys are more universally supported, and this is the default key type when generating a new key.
{serverlogons}	Number of Server Logons for Key	The number of Linux logons associated with the key, if any, granting the holder of the private key pair logon access on the server where the Linux logon resides.
{username}	Username associated with Key	The username of the user or service account associated with the key. For a user, the username is in the form of an Active Directory account (e.g. DOMAIN\username). For a service account, the username is made up of the username and client hostname entered when the service account key was created (e.g. myapp@appsrvr75).

2.1.6.6 Revocation Monitoring

Certificate revocation list (CRL) and online certificate status protocol (OCSP) locations are configured in the Revocation Monitoring section of the Management Portal to allow for email notifications when CRLs are near or at expiration, and for display on the Revocation Monitoring dashboard (see Dashboard: Revocation Monitoring on page 16). When revocation notifications are sent via email, matching events are written to the Windows event log on the Keyfactor Command server. The alert time-frame is calculated based on the date that the CRL expires, rather than the Next

Publish date. This allows for users to define their own alerts and log entries (thus determining their own definition of *stale*).

CRL monitoring and notification provides information on:

- The status of the CRL endpoint's responsiveness (e.g. is the file missing or the web site unreachable).
- Warning of upcoming expiration for a CRL.
- Notification of expired CRLs.

OCSP monitoring and notification provides only information on whether or not the OCSP endpoint is responsive. Expiration is not relevant for OSCP.

Tip: Click the help icon (?) next to the page title to open the embedded web copy of the *Keyfactor Command Documentation Suite* to this section.
You can also find the help icon at the top of the page next to the **Log Out** button. From here you can choose to open either the *Keyfactor Command Documentation Suite* at the home page or the *Keyfactor API Endpoint Utility*.

Revocation Monitoring Location Operations

From the Revocation Monitoring page on the Keyfactor Command Management Portal you can view and edit existing location endpoints, add new locations, delete an endpoint, test revocation monitoring location alert email notifications, and monitor location endpoint responsiveness.

Adding or Modifying a Revocation Monitoring Location

1. In the Management Portal, browse to *Alerts > Revocation Monitoring*.

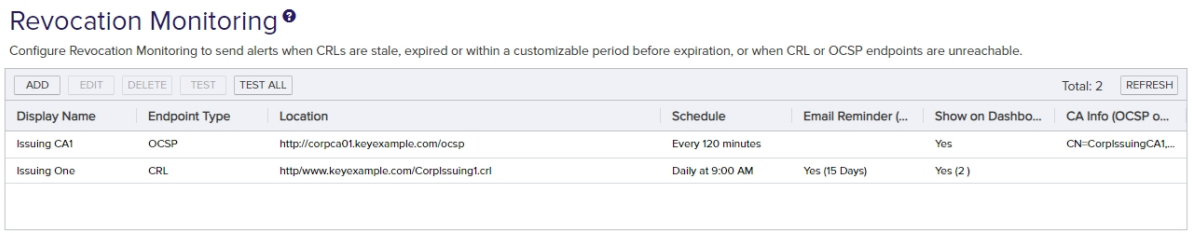


Figure 133: Revocation Monitoring Grid

2. On the Revocation Monitoring page, click **Add** to create a new monitoring location, or **Edit** to modify an existing one, and then populate the *Revocation Endpoint Settings* dialog appropriately for the type of revocation endpoint using the information below:

For a CRL location:

a. In the Revocation Endpoint Settings dialog, type a **Display Name** for the CRL location. This name appears on the Revocation Monitoring grid and on the Management Portal dashboard.

b. Select CRL in the **Endpoint Type** dropdown.

c. In the **Location** field, type a URL for the CRL location. This can be either an HTTP location or an LDAP location. Be sure to monitor the CRL locations that are in use by applications in your environment—if you're monitoring LDAP locations but applications are using an HTTP location, you're not going to receive any warning if a CRL fails to publish to the HTTP location.

> ⚠ **Important:** Because a "+" (plus sign) in a URL can represent either a space or a "+" Keyfactor Command has chosen to read "+" as a space. For CRL URLs that require a "+" (plus sign), rather than a space, replace plus signs in your CRL's URL with "`%2B`". Only replace the plus signs you don't wish to be treated as a space.

d. In the **Email Reminder** section of the page, check the **Warn** box and set the number of days ahead of expiration that email reminders should begin to be sent.

e. In the **Show on Dashboard** section of the page, check the **Warn** box and set the number of weeks, days or hours ahead of expiration for warning flags to begin appearing on the Management Portal dashboard (see Dashboard: Revocation Monitoring on page 16).

f. In the **Monitoring Execution Schedule** section of the page, configure a monitoring execution schedule. This defines the frequency with which locations are checked and alerts sent. You can choose to schedule the alert for this location either for daily delivery at a specified time or at intervals of anywhere from every 1 minute to every 12 hours. A daily schedule is the most common configuration. Schedules are configured separately for each endpoint.

g. In the **Recipients** section of the page, add email addresses of the users and/or groups who should receive email notifications when CRLs are approaching expiration or are unreachable. Recipient lists are configured separately for each endpoint.

   Keyfactor Command sends SMS (text) messages by leveraging the email to text gateways that many major mobile carriers provide. Check with your carrier for specific instructions. Keyfactor has tested that AT&T can be addressed using 10-digit-number@txt.att.net (e.g. 4155551212@txt.att.net) and Verizon can be addressed using 10-digit-number-@vtext.com (e.g. 2125551212@vtext.com). T-Mobile can be addressed using 10-digit-number@tmomail.net (e.g. 2065551212@tmomail.net), but functionality can be spotty. Reliability of alerting via this method depends on the reliability of the carrier's gateways.

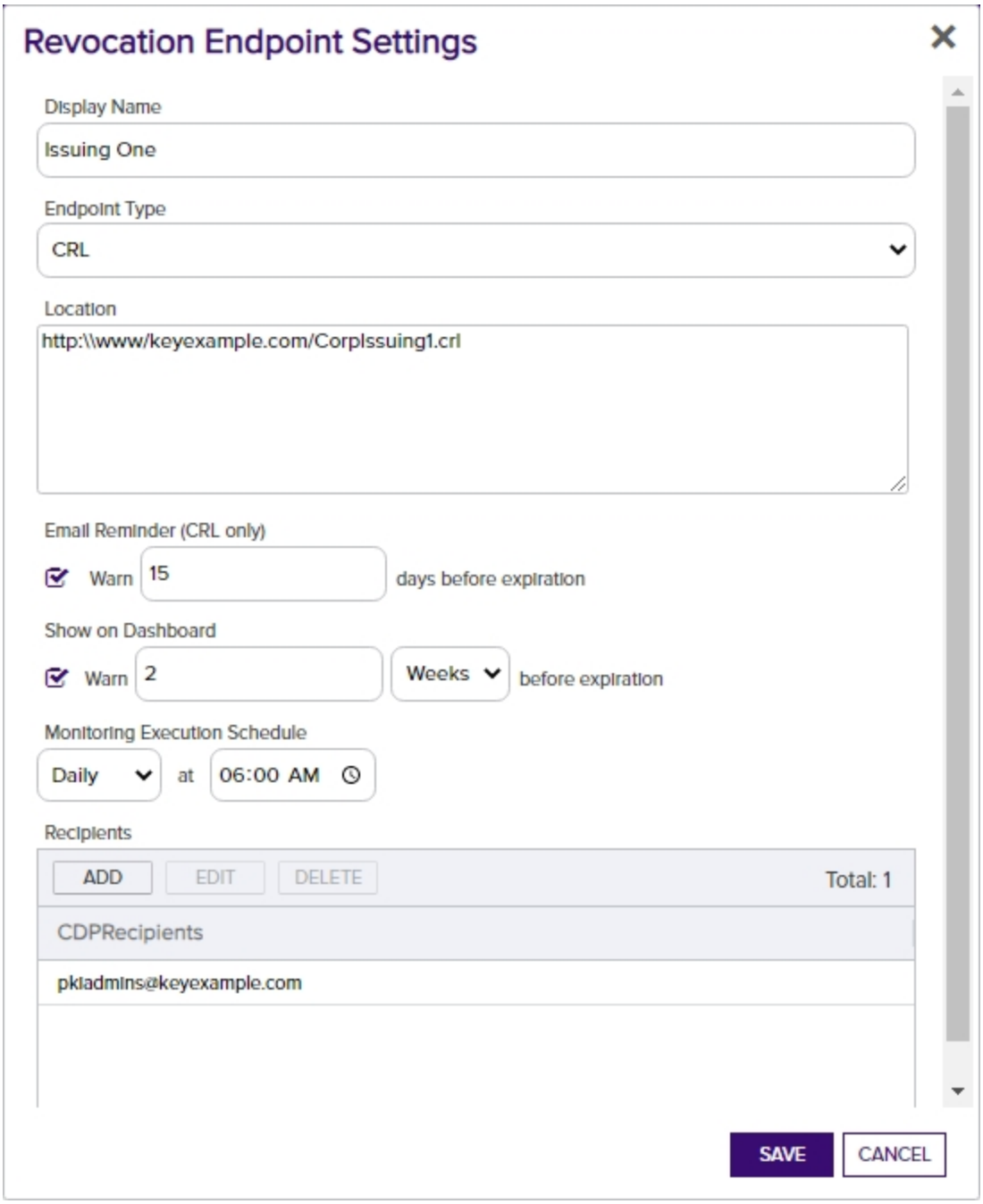


Figure 134: CRL Monitoring Details

For an OCSP location:

a. In the Revocation Endpoint Settings dialog, type a **Display Name** for the OCSP location. This name appears on the Revocation Monitoring grid and on the Management Portal dashboard.

b. Select OCSP in the **Endpoint Type** dropdown.

c. Keyfactor Command offers two options to retrieve endpoint information for OCSP:

- Resolve it based on a certificate authority defined in Keyfactor Command (see Adding or Modifying a CA Record on page 330). This option is only available for Microsoft CAs in the forest in which Keyfactor Command is installed or EJBCA CAs installed on the same network as the Keyfactor Command server. When you use this option, a request is sent for information from the Keyfactor Command server to the CA. For Microsoft CAs, this a DCOM request. For EJBCA CAs, this is a REST request.
- Import it from a certificate issued by the certificate authority to be monitored. This can be any certificate issued by the CA and containing the OCSP information. The certificate needs to be a base-64 encoded PEM file (.cer/.crt).

In the **CA Info** field, select the **CMS** radio button to automatically retrieve the CA certificate information from Keyfactor Command or select the **File** radio button to upload a file with the CA certificate information.

- If you select CMS, pick the desired CA from the CA dropdown and then click the **Resolve** button to retrieve the certificate authority information.
- If you select File, click the **Upload** button, browse to locate the file containing a certificate issued by the desired CA and open it.

  With either method of retrieving the information, you should see the full certificate authority name and authority key ID populate below the CA dropdown. The serial number field will populate for uploaded files.

d. In the **Location** section of the page, enter the full URL to the OCSP responder servicing this certificate authority's CRL.

e. In the **Show on Dashboard** section of the page, check the box to include this OCSP location on the Management Portal dashboard (see Dashboard: Revocation Monitoring on page 16).

f. In the **Monitoring Execution Schedule** section of the page, configure a monitoring execution schedule. This defines the frequency with which locations are checked and alerts sent. You can choose to schedule the alert for this location either for daily delivery at a specified time or at intervals of anywhere from every 1 minute to every 12 hours. A daily

schedule is the most common configuration. Schedules are configured separately for each endpoint.

g. In the **Recipients** section of the page, add email addresses of the users and/or groups who should receive email notifications when OCSP endpoints are unreachable. Recipient lists are configured separately for each endpoint.

   Keyfactor Command sends SMS (text) messages by leveraging the email to text gateways that many major mobile carriers provide. Check with your carrier for specific instructions. Keyfactor has tested that AT&T can be addressed using 10-digit-number@txt.att.net (e.g. 4155551212@txt.att.net) and Verizon can be addressed using 10-digit-number-@vtext.com (e.g. 2125551212@vtext.com). T-Mobile can be addressed using 10-digit-number@tmomail.net (e.g. 2065551212@tmomail.net), but functionality can be spotty. Reliability of alerting via this method depends on the reliability of the carrier's gateways.

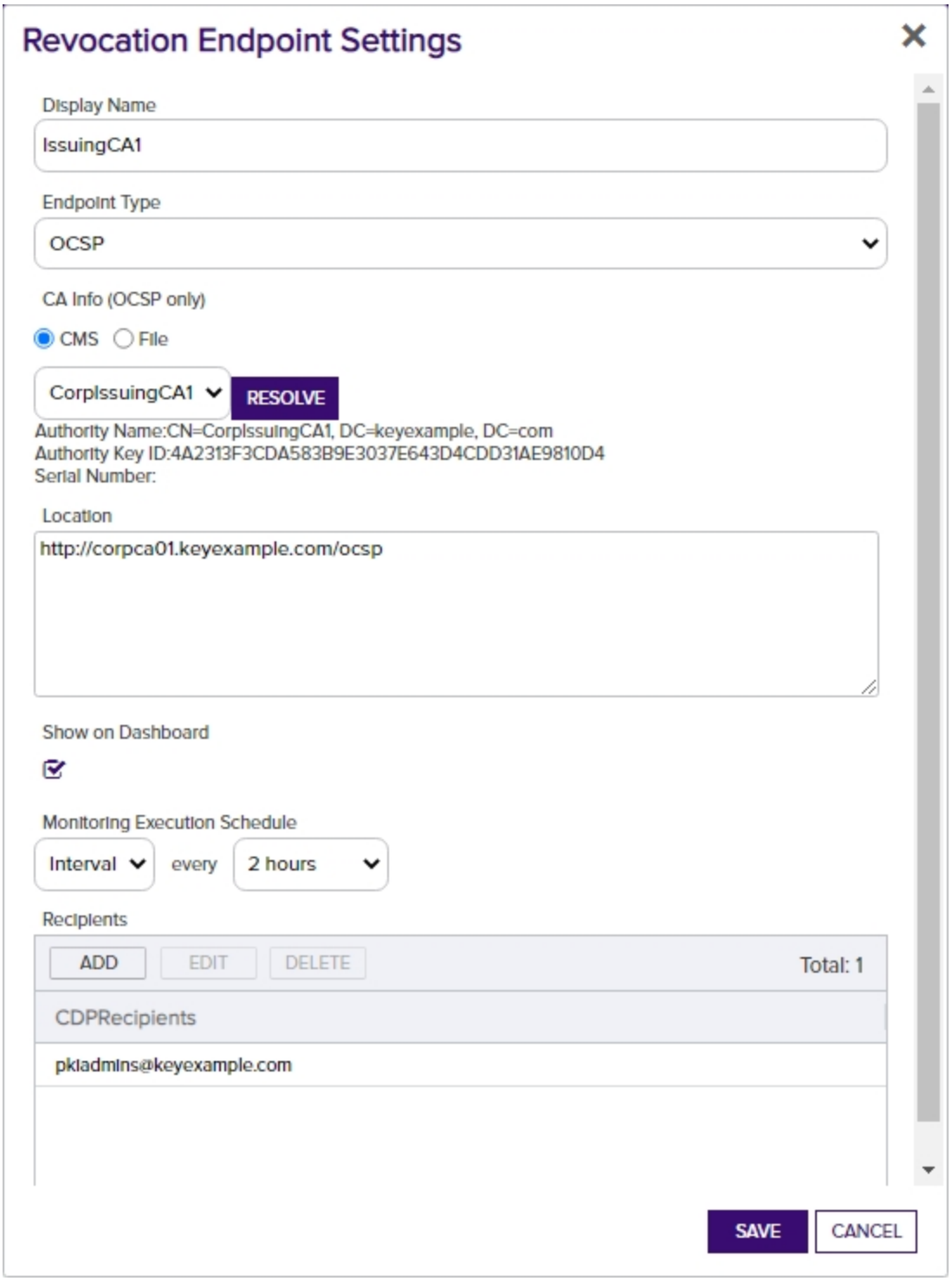

Revocation Endpoint Settings
Display Name
IssuingCA1
Endpoint Type
OCSP
CA Info (OCSP only)
CMS
File
CorpIssuingCA1
RESOLVE
Authority Name:CN=CorpIssuingCA1, DC=keyexample, DC=com
Authority Key ID:4A2313F3CDA583B9E3037E643D4CDD31AE9810D4
Serial Number:
Location
http://corpca01.keyexample.com/ocsp
Show on Dashboard
Monitoring Execution Schedule
Interval
every
2 hours
Recipients
ADD
EDIT
DELETE
Total: 1
CDPRecipients
pkiadmins@keyexample.com
SAVE
CANCEL

Figure 135: OCSP Monitoring Details

3. Click **Save** to save the endpoint location, or the changes. Click **Cancel** to cancel.

Deleting a Revocation Monitoring Location

1. In the Management Portal, browse to *Alerts > Revocation Monitoring*.
2. On the Revocation Monitoring page, highlight the row in the grid and click **Delete** at the top of the grid, or from the right click menu.
3. On the Confirm Operation alert, click **OK** to confirm or **Cancel** to cancel the operation.

Testing Revocation Alerts

1. In the Management Portal, browse to *Alerts > Revocation Monitoring*.
2. On the Revocation Monitoring page, click the **Test All** button at the top of the grid, or select a specific location from the grid and click **Test** from the top of the grid or the right click menu.
3. In the Revocation Monitoring Test dialog in the Alert Parameters section, select an **End Date** for testing. You can use this option to simulate running the alerts a month from now instead of today, for example, or put in a date far in the future to be sure you pick up some expiring CRLs for testing purposes.
4. In the Revocation Monitoring Test dialog in the Alert Parameters section, click the toggle button for **Send Alerts** if you would like to deliver email messages as part of the test.
5. Click the **Generate** button to begin generating alerts. Depending on the number of endpoints to process, this may take a few seconds.
6. In the Revocation Monitoring Test dialog in the Alert Data and Alert Message sections, you can review the alerts to confirm that the expected CRLs and OCSP endpoints are appearing. Scroll through the alerts using the **First**, **Previous**, **Next** and **Last** buttons at the bottom of the dialog. The number of alerts generated will display between the navigation buttons.

Tip: Alerts are generated when a CRL is expired or in the warning period as defined by the number of days configured in the *Email Reminder* setting. For example, if you had a CRL that expired on June 30 and configured the email reminder period to 15 days before expiration, the warning status would begin for that CRL on June 15 and CRL alerts would be generated. A warning will also appear for any CRL or OCSP locations that produced an error or couldn't be resolved.
When alerts are tested or sent on a schedule, corresponding message are also written to the system event log on the server where the Keyfactor Command service runs. For testing, this is true whether or not you click the *Send Alerts* toggle. Information is logged to the event log for both locations that are in a good state (e.g. CRL resolves and is not in a warning or expired state or response from OCSP) and locations that are in an error state (e.g. CRL resolves but is in the warning period or expired, CRL is expired, CRL or OCSP location does not resolve).

For specific Windows event ID information, see Keyfactor Command Windows Event IDs on page 727.

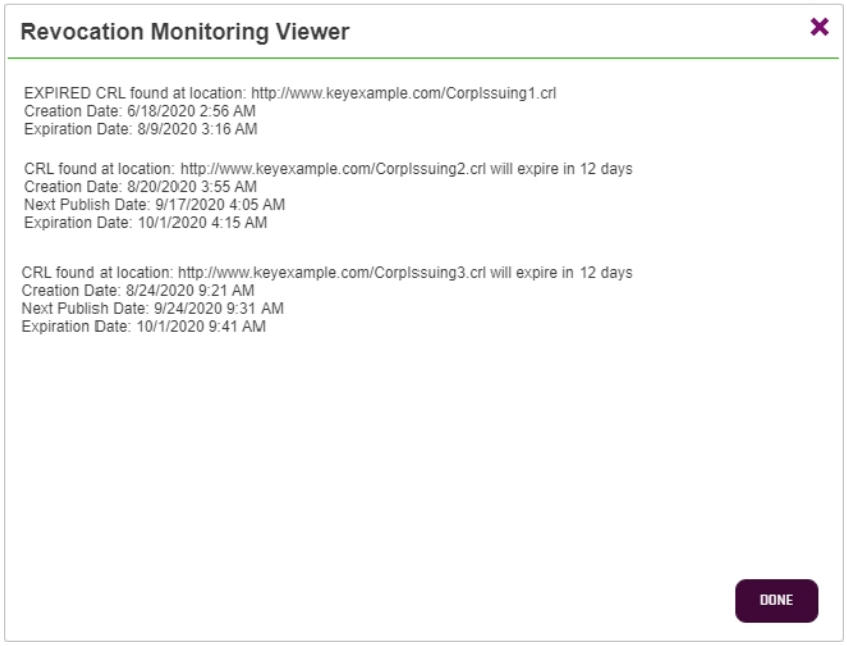


Figure 136: Test Revocation Monitoring

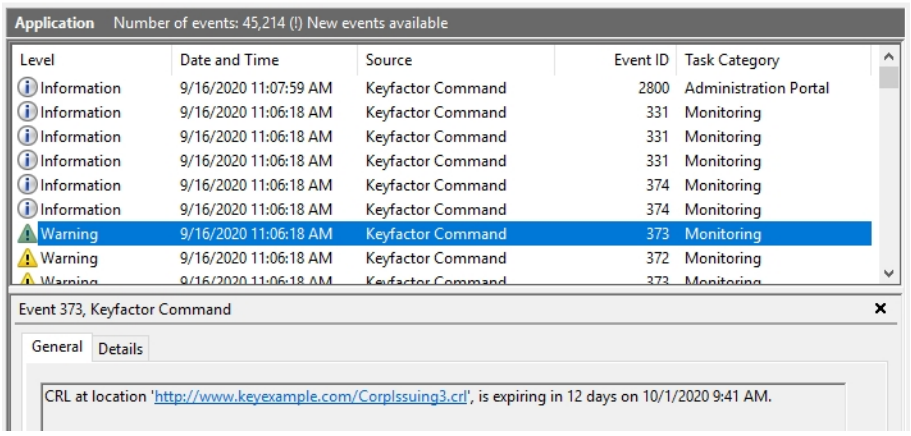


Figure 137: Revocation Monitoring Event Log Messages

2.1.6.7 Using Event Handlers

A given expiration, pending, issued or denied alert can have only one event handler action associated with it. For example, an alert can run one PowerShell script but not also a second PowerShell script or also an event logging task. Alerts configured with a PowerShell or renewal event handler can also send out email messages. However, be aware that your PowerShell script will run once for

every certificate and every email recipient, so if your alert has three email recipients, your script will run three times for each certificate. If this is not the desired behavior, you can set up separate alerts for email messages and your PowerShell script. Alerts configured with an event logger event handler will log events to the event log instead of sending email messages. If you want to both log to the event log and send email messages for a given alert configuration, you need to set up two separate alerts.

Tip: PowerShell handlers will run in different security contexts depending on how they are triggered. If they are triggered by the Management Portal/Keyfactor API they will run in the context of the Keyfactor API application pool account. If they are triggered by a task scheduled in the Keyfactor Command Management Portal, they will run in the context of the Keyfactor Command Service account. Keep this in mind if your configuration of the PowerShell script is going to use Windows Authentication to reach back into Keyfactor Command,or elsewhere.

Adding PowerShell Handlers to Alerts

To add a PowerShell handler to an alert, the alert must first be created and saved. See Alerts on page 160 for more information on creating various alerts. The example below uses an expiration alert, but the process applies to all types of alters.

1. Select the alert to which you want to add the event handler from the respective alert grid.
2. Check the **Use handler** box and select the PowerShell event handler in the dropdown.

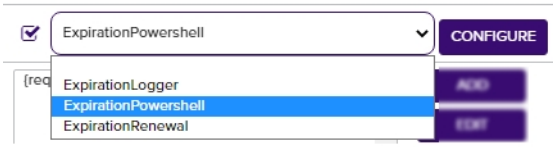


Figure 138: Use PowerShell Expiration Event Handler

Tip: If the expected event handler types do not appear, confirm that they exist and are enabled on the Event Handler Registration page (see Event Handler Registration on page 674).

3. Click the **Configure** button in the Use handler section of the page to open the Configure Event Handler dialog and then click **Add**.

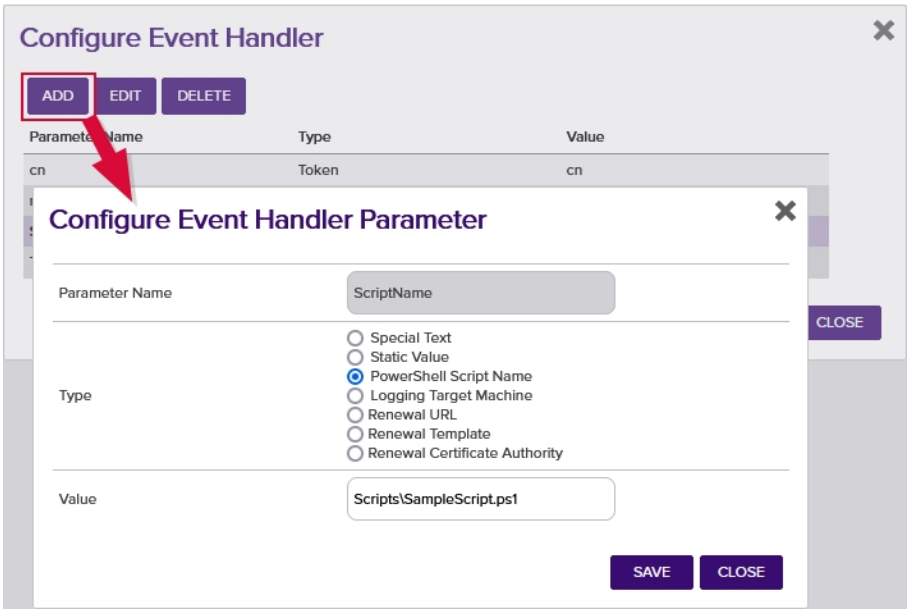


Figure 139: Expiration Alert with PowerShell Event Handler

4. In the Configure Event Handler Parameter dialog, select **PowerShell Script Name** as the parameter Type, and enter the filename and optional relative path to the PowerShell script, located in the extensions directory on the Keyfactor Command server, in the Value field.

   Note: As of version 9.0 of Keyfactor Command, PowerShell scripts for alert handlers need to be in the extension path or a subdirectory of it specified by the *Extension Handler Path* application setting (see Application Settings: Console Tab on page 584). By default this is:

   ```
   C:\Program Files\Keyfactor\Keyfactor Platform\ExtensionLibrary\
   ```

   For example, create a directory called *Scripts* under the ExtensionLibrary directory and then reference your PowerShell script as *Scripts\MyPowerShell.ps1*. Any scripts referenced by PowerShell handlers that are outside this path will fail to run.

5. Click **Save** to save your first parameter.

6. If desired, you can pass one or more parameters into your PowerShell script—either fixed text (type Static Value) or substitutable special text (type Special Text). To pass in fixed text, enter a name for the parameter (e.g. MyName), select the **Static Value** radio button, and type your fixed text in the Value field. To pass in special text, enter a name for the parameter (e.g. MyOtherName), select the **Special Text** radio button, and select your desired substitutable special text field in the Value dropdown. When referring to these parameters in your PowerShell script, refer to them using a *$context* hashtable parameter passed to the script, whose keys are the names entered in the event handler configuration. See Figure 140: PowerShell Event Handler with

Multiple Parameters. For example, for the parameter named “cn” in the event handler configuration, you might use this line in a PowerShell script:

```
if ($context.ContainsKey("cn")) { Add-Content -Path "C:\Stuff\MyOutput.txt" -Value $context["cn"] }
```

In addition to the parameters you opt to pass in the event handler configuration, there are several built-in parameters that are always passed. These can be found in Table 12: PowerShell Event Handler Special Fields. You can reference these in your PowerShell script without having to specify them in your event handler configuration.

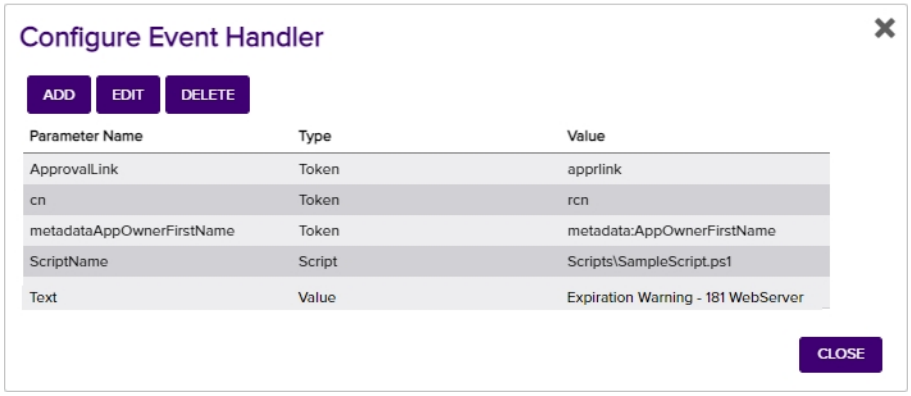


Figure 140: PowerShell Event Handler with Multiple Parameters

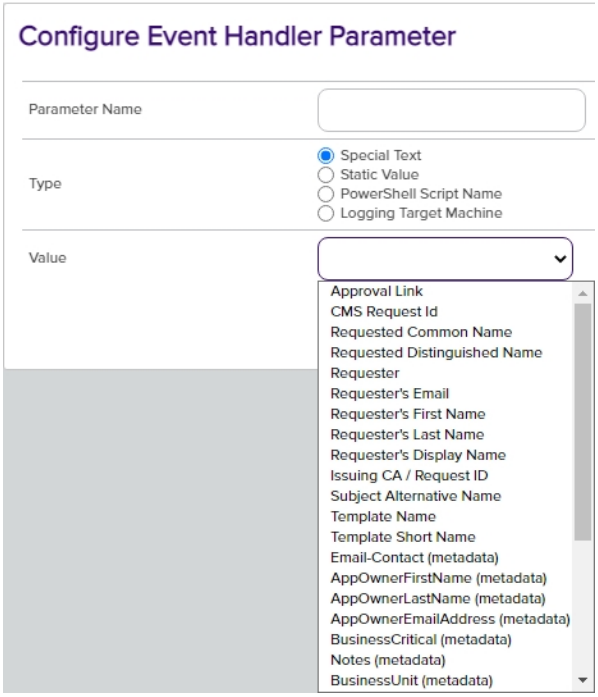


Figure 141: Example of a List of Special Text Parameters

7. Click **Close** to return to the alert configuration and then save the alert.
8. If your PowerShell script is unsigned, you may need to enable execution of unsigned PowerShell scripts on the Keyfactor Command server with this PowerShell command:

    ```
    Set-ExecutionPolicy RemoteSigned
    ```

9. Test the alert as described in Expiration Alert Operations on page 161. It is not necessary to check the **Send Alerts** box during the test to cause the PowerShell script to run.

Table 12: PowerShell Event Handler Special Fields

Name	Alert Type	Description
SendEmail	All	If true, email messages are sent in addition to processing of the Power-Shell script.
Subject	All	The full subject line of the alert.
Message	All	The full message body of the alert.
Recipient	All	The recipient of the alert. Alerts configured with more than one recip-ient will execute the PowerShell script multiple times—once for each recipient and each certificate or request.

Name	Alert Type	Description
Certificate	Expiration Only	For internal Keyfactor use only.
First Recipient	Expiration Only	If true and the alert has multiple recipients configured, this output is for the first recipient for the given certificate. Subsequent output for the same certificate and different recipients will show false for this value.

To create a PowerShell script that works with the event handlers, there are just a few things to keep in mind:

- You need to declare the $context hashtable at the start of the script with this line:

```
[hashtable]$context
```

- Parameters you want to use in your script are referenced using the $context syntax as follows (where MyName is the name you gave to the parameter in the event handler configuration or the name of the built-in parameter from Table 12: PowerShell Event Handler Special Fields):

```
$context["MyName"]
```

Here is a simple script that takes as inputs all the parameters you defined in your event handler configuration as well as the built-in parameters and outputs them to a file along with a comment and the date, with configuration to skip output of a defined list of the built-in parameters:

```
# This is a sample script that can be set up as a Keyfactor Command event handler. The script will
output
# data passed to the handler to a text file. This script will be called for the combination of each
# certificate involved in the corresponding event and each configured email recipient.

# In order to communicate with the extension script, the Keyfactor Command event handler framework
injects
# a hashtable into the PowerShell runspace. This hashtable will include the fields configured by the
# administrator when setting up the handler as well as some built-in system fields used for commu-
nication
# with the handler.

# The following fields are provided for communication with the handler:
#   Subject -        Email subject line that will be sent if the alert has the email subject
configured
#   Message -        Email body that will be sent if the alert has the email message body configured
#   Recipient -      Email address where the alert will be sent if the alert has this configured
#   Certificate -    For internal use only
#   SendEmail -      Boolean (true/false) indicating if Keyfactor Command is planning on sending an
email
```

```
#                   for this certificate / recipient combination
#   FirstRecipient - Boolean (true/false) indicating if this extension invocation is the first recip-
ient
#                   for a given certificate
#                   This can be used in the event it is desired to execute some logic once per certi-
ficate
#                   This field applies only to expiration alerts

[hashtable]$context

# Four of the built-in context fields can be modified and used as output fields to change how (and
if)
# Keyfactor Command will send emails related to the alert being processed:
#   Subject - If an email is produced this new value will be used to create the email subject.
#   Message - If an email is produced this new value will be used to create the email message body.
#   Recipient - If an email is produced this new value will be used as the email recipient.
#   SendEmail - This value can be used to override whether an email will be sent.
#     A value of "true" will cause an email to be sent, while "false" will cause the associated email
#     to not be sent.
#     Examples:
#       $context["Subject"] = "new subject line"
#       $context["Message"] = "new message line"
#       $context["Recipient"] = "newRecipient@keyexample.com"
#       $context["SendEmail"] = "false"

# Typically output values would be used with some form of logic. As an example, to change the recip-
ient
# of the email based on a metadata field provided to the handler, uncomment the following, provide
# appropriate values (including a metadata field that's being passed in to the handler in place of
# "SampleMetadataField"), and remove Recipient from ignoreKeys:
#
#      if ($context["SampleMetadataField"] -eq "SomeValue") {
#              $context["Recipient"] = "newRecipient@keyexample.com"
#              }

# This example will output to a file the $context values for the user configured fields and skip the
system
# supplied ones. To output the system supplied fields, remove the desired items from the $ignoreKeys
array.
$ignoreKeys = "Subject", "Message", "SendEmail", "Certificate", "FirstRecipient", "Recipient"

# Path to the output file
$outputFile = ("C:\PSScripts\Output\SampleScriptOutput" + (get-date -UFormat "%Y%m%d%H%M") + ".txt")

# Add a comment and the date at the start of each output block
```

```
Add-Content -Path $outputFile -Value "Starting Output: $(Get-Date -format G)"

# Loop through all passed in key/value keys and process
$context.GetEnumerator() | % {
	if (-not $ignoreKeys.Contains($_.key)) {
		Add-Content -Path $outputFile -Value ($_.key + ": " + $_.value)
	}
}

# Add a blank line between output blocks
Add-Content -Path $outputFile -Value ""
```

Tip: A sample PowerShell script is installed with Keyfactor Command in the ExtensionLibrary directory.

Adding Logging Handlers to Alerts

To add a logging handler to an alert:

1. Edit an existing alert or create a new one. An alert cannot both send emails and write to the event log, so if you need to do both of these for the same alert configuration, you will need two separate alerts.
2. Configure the message body as you would for an email message, including substitutable special text. The text from the message body is written to the event log. Note that HTML is not supported in the message body for event logging. The contents of the *Subject* line do not appear in the event log.
3. Check the **Use handler** box and select the logger event handler in the dropdown.

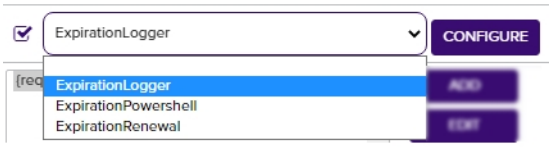


Figure 142: Expiration Alert with Event Logging Event Handler

Tip: If the expected event handler types do not appear, confirm that they exist and are enabled on the Event Handler Registration page (see Event Handler Registration on page 674).

4. Click the **Configure** button in the Use handler section of the page to open the Configure Event Handler dialog and then click **Add**.

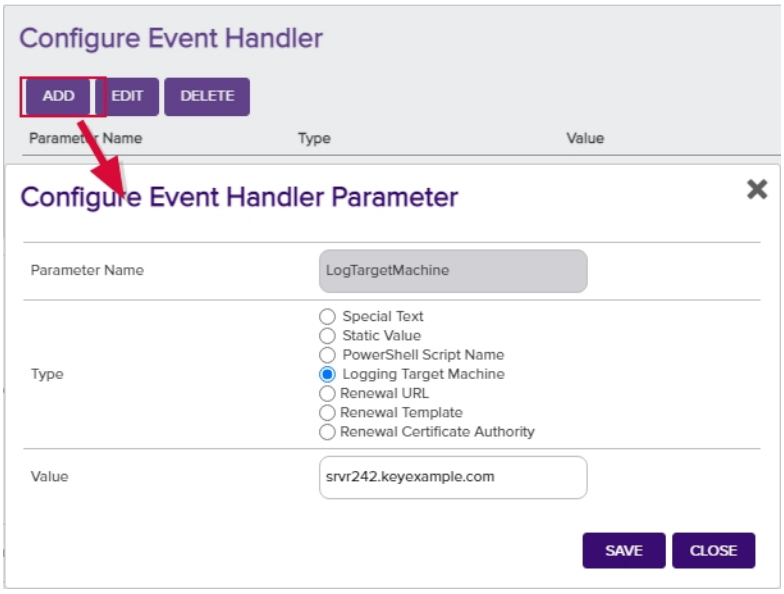


Figure 143: Expiration Alert with Logging Event Handler

5. In the Configure Event Handler Parameter dialog, select **Logging Target Machine** as the parameter Type, and enter the fully qualified domain name of the server to which you wish to send the event log message in the Value field.

   By default, the service accounts under which the Keyfactor Command application pool and Keyfactor Command service run have sufficient permissions to write to the event log on the Keyfactor Command server. If your target computer is not the Keyfactor Command server, you will need to grant appropriate permissions on that computer to one or both of these service accounts in order to write to the event log on that computer. When alerts containing event handlers are run in test most, the application pool service account is used. When alerts containing event handlers are run as a scheduled task, the Keyfactor Command service account is used. Local administrator permissions are needed initially to allow the service account to create the event log source types on the target machine. After that has been completed (on the first successful write of event logs to the server), permissions for the service account can be dialed back to “Generate security audits” or “Manage auditing and security log” in the local security policy.

   If you wish to use a DNS alias for the target machine value, you may need to disable loopback checking on the Keyfactor Command server and reference the target machine. See Disable Loopback Checking on page 745.

6. Click **Save** to save and then **Close** to return to the alert configuration. No other parameters are needed (or functional) for an event logging event handler.

7. Test the alert as described in Expiration Alerts on page 161. It is not necessary to check the **Send Alerts** box during the test. Alerts are written to the Application event log.

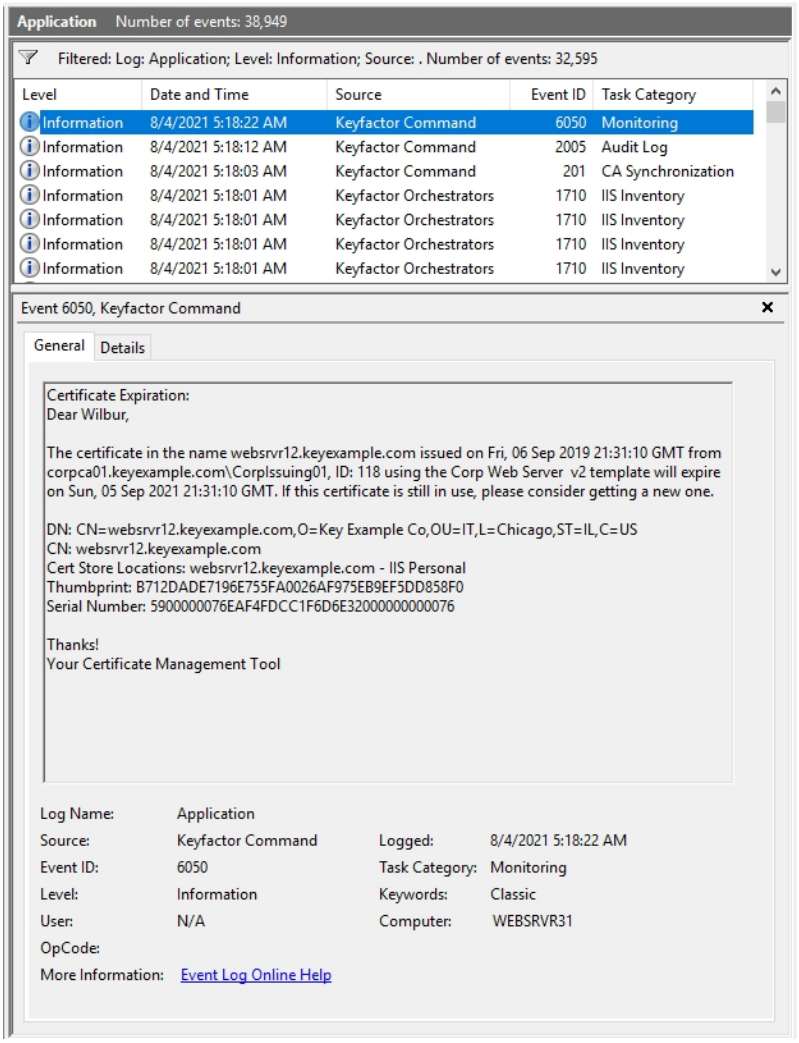


Figure 144: Expiration Alert Event Log

Adding Renewal Handlers to Expiration Alerts

Important: Renewal alerts will not function until you configure security permissions for the renewal handler as per *Configure Renewal Handler Permission* in the *Keyfactor Command Server Installation Guide*.

To add a renewal handler to an expiration alert:

1. Edit an existing expiration alert or create a new one. See Expiration Alert Operations on page 161.
2. Check the **Use handler** box and select the renewal event handler in the dropdown.

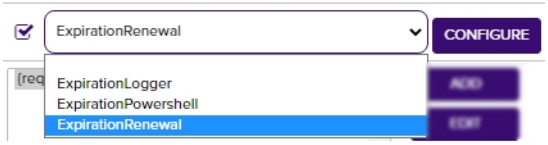


Figure 145: Use Renewal Event Handler on Expiration Alert

Tip: If the expected event handler types do not appear, confirm that they exist and are enabled on the Event Handler Registration page (see Event Handler Registration on page 674).

3. Click the **Configure** button in the Use handler section of the page to open the Configure Event Handler dialog and then click **Add**.

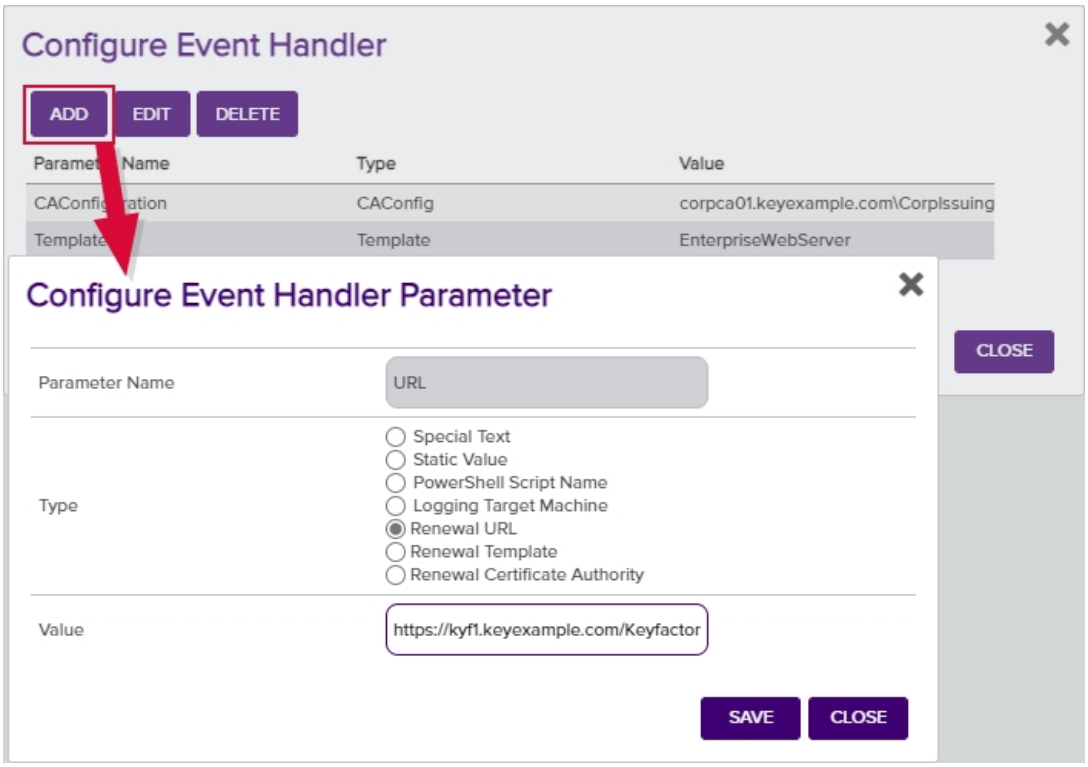


Figure 146: Expiration Alert with URL Event Handler

4. In the Configure Event Handler Parameter dialog, select **Renewal URL** as the parameter Type, and enter the URL to the Keyfactor Command server hosting the Keyfactor API component followed by /KeyfactorApi in the Value field. Click **Save** to save your first parameter.

5. If desired, you can configure a renewal template and CA for use with the renewal event handler. These settings are optional. If you don't set these, the renewal will be done using the template

and CA originally used on the certificate. If you set only one of these—for example, the template—it will use the setting from the renewal event handler for that and retrieve the other—for example, the CA—from the certificate.

6. Test the alert as described in Expiration Alerts on page 161. It is not necessary to check the **Send Alerts** box during the test.

   Important: Renewals **are** processed and new certificates **are issued** during expiration alert tests with associated renewal handlers.

2.1.7 Workflow

The options available in the Workflow section of the Management Portal are:

- **Workflow Definitions**

  Create workflows that manage certificate enrollments, renewals, or revocations end-to-end to require approvals, send emails, run PowerShell scripts and/or execute API requests as part of the process and workflows that are initiated by an automated task that runs periodically (every 10 minutes by default) to identify additions and removals of certificates from a specified certificate collection.

- **Workflow Instances**

  Manage initiated instances of workflows to view active, suspended (requiring approval) and completed enrollments, renewals, revocations, and additions and removals of certificates from a specified certificate collection. This page allows you to view the steps in a given instance of a workflow (which may be different from the current configuration of the workflow definition), restart failed workflow instances, and delete workflow instances.

- **My Workflows**

  Review initiated instances of workflows awaiting action by you and take action (e.g. approve or deny enrollment or revocation requests) or created by you.

2.1.7.1 Workflow Definitions

The workflow builder in Keyfactor Command allows you to easily automate event-driven tasks when a certificate is requested, revoked, or added or removed from a certificate collection. The workflows can be configured with multiple steps between the start and end of the operation that offer a simple way to configure notifications, approvals, and end-to-end automation throughout the environment. This provides for operational agility in an intuitive and easy-to-configure manner.

When a user begins one of the types of actions managed with workflow in Keyfactor Command on the usual Management Portal page (e.g. PFX Enrollment) or using the Keyfactor API or a certificate collection membership change is detected by an automated task, the workflow kicks in behind the scenes and executes however many steps have been configured in the workflow definition to bring the action to the appropriate conclusion along the desired path. In the current version of workflows, the following workflow types are supported:

- **Certificate Entered Collection**

  The workflow is initiated by an automated task that runs periodically to identify certificates that now meet the query criteria of the specified certificate collection. For example, when a certificate discovered on an SSL scan becomes part of the Weak Keys collection, an email message can be generated notifying the PKI administrators that a new certificate with a weak key has been discovered.

- **Certificate Left Collection**

  The workflow is initiated by an automated task that runs periodically to identify certificates that no longer meet the query criteria of the specified certificate collection. For example, when a certificate in the Web Server Certificates collection disappears, a REST request can be made to open a support ticket request to investigate the removal of a web server certificate.

- **Enrollment (Including Renewals)**

  The workflow is initiated by enrollment for a new or renewed certificate. Steps during the workflow can be used to do things such as require manager approval for the enrollment or manipulate the subject and/or SANs for the certificate request.

- **Revocation**

  The workflow is initiated by revoking a certificate. Steps during the workflow can be configured to do things such as modify the revocation comment entered when the certificate is revoked, append an additional comment, and store the resulting extended comment in a metadata field.

The following customizable workflow steps are supported within the workflows:

- **Send Email**

  Send an email message. This is a separate email message from those typically sent as part of a *Require Approval* step. You might send an email message as part of an enrollment request to notify approvers that a new request needs approval. The email messages can be customized to provide detailed information about, for example, the certificate request.

- **Set Variable Data**

  Run PowerShell commands within the confines of the workflow to populate variables with information to pass back to the workflow. The PowerShell script contents are embedded within the step. This step does not call out to an external file. This provides a high level of security by greatly limiting the number of standard PowerShell cmdlets that can be executed by the workflow step. A small number of PowerShell cmdlets have been white listed to allow them to be included in workflow steps of this type, including:

  - Where-Object
  - ForEach-Object
  - Get-Command

- **Use Custom PowerShell**

  Run a PowerShell script. The script contents are in a file placed in the ExtensionLibrary\Workflow directory or a subdirectory of it on the Keyfactor Command server under the install directory for Keyfactor Command. By default, this is:

C:\Program Files\Keyfactor\Keyfactor Platform\ExtensionLibrary\Workflow

The file must have an extension of .ps1. A sample PowerShell script is provided in the Workflow directory (CustomPowershellExample.ps1).

- **Require Approval**

  Require approval for a workflow step before the step can be completed. The require approval step can require approval from just one approver or multiple approvers. The workflow will be suspended at this point until the correct number of approvals from users with the correct security roles is received or until one deny is received before continuing to the next step. As part of this step, an email message is sent indicating whether the step was approved or denied—typically to the requester. This step does not include logic to send an email initiating the approval process (letting users know something needs approval). Use a *Send Email* type step for this.

  Important: Workflows are not supported with CA delegation when they contain steps that require approval. For more information, see the CA configuration *Authorization Methods Tab*.

  Note: The users that you send email to initiating the approval process must be members of a security role that is allowed to submit signals (approve/deny) for the workflow in order to approve or deny the request.

  Tip: The workflow builder does not include a step to send a notification to the requester of a certificate on an enrollment once the certificate is issued by the CA (as opposed to approved in Keyfactor Command). Use the issued alerts for this (see *Issued Request Alert Operations*).

- **Invoke REST Request**

  Run a REST (API) request. The REST request contents are embedded within the step. It does not call out to an external file.

- **Update Certificate Request Subject\SANs for Microsoft CAs (Enrollment Only)**

  On an enrollment (either CSR or PFX), create a resigned CSR to prepare an updated enrollment request for delivery to a Microsoft CA after a previous step in the workflow has been used to update either the SANs in the initial request, subject (DN) in the initial request or both. This step must be placed later in the workflow than the step(s) to modify the SANs and/or subject. The SANs and subject may be modified with either of the PowerShell step types or a custom step type. The step creates a new CSR using the same public key as the original CSR using the updated SAN and/or subject values. It signs the new CSR with the certificate provided in the step's configuration.

  For this type of step you will need an enrollment agent certificate available as a PKCS#12 (.PFX) file with included private key to import into Keyfactor Command. This can be a user certificate or a computer certificate (e.g. generated from a copy of the *Enrollment Agent* template or the

Enrollment Agent (Computer) template) and must have a Certificate Request Agent EKU. Note that the built-in *Enrollment Agent* and *Enrollment Agent (Computer)* templates do not allow private keys to be exported by default. You will need a template that allows private key export or will need to manually override private key export to create a certificate with an exportable private key in order to create a PKCS#12 (.PFX) file.

> ⚠ **Important:** This step applies to Microsoft CAs only. If this step is added to workflow for requests directed to an EJBCA CA, it will fail on enrollment. Note that EJBCA supports submission of updated SAN or subject details as part of standard functionality.

- **Windows Enrollment Gateway - Populate from AD (Enrollment Only)**

  On an enrollment done through the Keyfactor Windows Enrollment Gateway using a client-side template configured with the *Build from this Active Directory information* option on the template, this workflow step handles formatting the incoming subject, SANs, and/or SID in the certificate request appropriately such that the enrollment will complete successfully with the target CA and Keyfactor Command template, which is not configured to build from AD. Any Keyfactor Windows Enrollment Gateway using a client-side template configured with the subject as *Build from this Active Directory information* must be configured with a workflow step of this type on the Keyfactor Command template that has been mapped in the gateway to that template in order to complete an enrollment through the gateway. There are no configuration parameters for the step.

  > ⚠ **Important:** The template in Keyfactor Command that is mapped to the client-side template configured to build the subject from Active Directory also needs to be configured with three enrollment fields to support handling the incoming subject, SANs, and/or SID. For more information about configuring this, see the *Keyfactor Windows Enrollment Gateway Installation and Configuration Guide*.

In addition to these customizable types of steps, there are built-in steps that you won't see unless you're using the Keyfactor API to view or edit the workflows (see *Workflow Definitions* in the *Keyfactor Web APIs Reference Guide*). At the end of their respective workflow types there are an enroll step and a revoke step to initiate the actual enrollment or revocation if the workflow reaches the end without being denied or failing. These built-in steps cannot be modified or moved to a different location in the workflow. There are also NOOP steps that indicate the start and end of the workflow for housekeeping purposes.

There are two types of workflow definition:

- **Global**

  The global workflow definitions are built into the product and cannot be deleted, though they can be modified to add workflow steps, if desired. Global workflow definitions do not have a specific associated *key*—in the case of the currently available workflows, this is a certificate template—and apply to all requests of the workflow's type (e.g. enrollment) that are not otherwise handled by a custom workflow specifying a *key*.

- **Custom**

Custom workflow definitions are any additional workflow definitions you define beyond the built-in ones. Custom workflows are associated with a specific *key* (certificate template or certificate collection) and each workflow only applies to requests made using that *key*.

Note: All certificate enrollment, renewal, and revocation requests go through workflow even if you haven't created any workflow steps or added any custom workflow definitions. In the absence of customization, the global workflow definitions are used. The addition and removal of certificates from certificate collections only go through workflow if you create custom workflows for them.

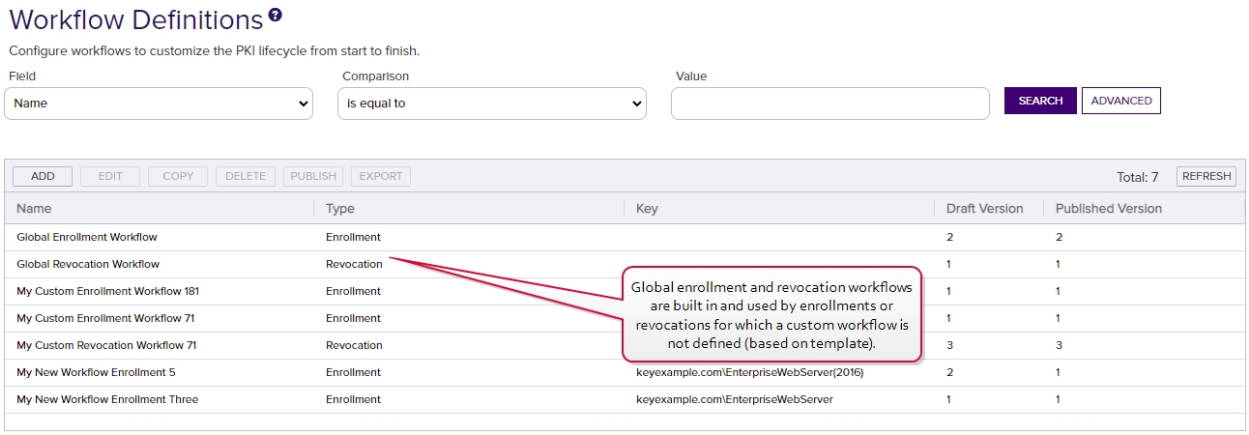


Figure 147: Workflow Definitions

When requiring approval for enrollment using workflow definitions in Keyfactor Command, templates do not need to be configured to require manager approval at the CA level in the certificate template. This is because the approval handling is fully controlled within Keyfactor Command. In fact, templates generally should not be configured to require CA manager approval when using Keyfactor Command workflow, since this would generally require approval both at the Keyfactor Command level and at the CA level.

Tip: Click the help icon (?) next to the page title to open the embedded web copy of the *Keyfactor Command Documentation Suite* to this section.
You can also find the help icon at the top of the page next to the **Log Out** button. From here you can choose to open either the *Keyfactor Command Documentation Suite* at the home page or the *Keyfactor API Endpoint Utility*.

Workflow Definition Operations

The workflow builder in Keyfactor Command is a powerful feature that allows you to manage certificate enrollments, renewals, revocations, and additions or removals from a certificate collection end-to-end. Out of the box, there are workflow builder steps such as requiring approvals for actions like certificate enrollment and revocation requests, sending email notifications, and running PowerShell scripts and API requests as part of the request flow.

Workflow definition operations include:

- Creating, editing or deleting a workflow definition
- Publishing a workflow definition to make it active and available for use
- Importing and exporting workflow definitions for backup, duplication and customization purposes

Tip: There are two built-in workflow definitions—Global Enrollment Workflow and Global Revocation Workflow—that are used to manage enrollment and revocation requests which are not otherwise handled by custom workflows. These workflows can be configured with steps (see Adding or Modifying a Workflow Definition below), but they cannot be deleted. There are no built-in workflow definitions for the addition and removal of certificates from certificate collections. These actions only go through workflow if you create custom workflows for them.

Adding or Modifying a Workflow Definition

The workflow builder workspace is laid out with the workflow steps running from top to bottom in the middle (initially), the Workflow Definition dialog in a collapsible window on the right, and workspace controls at the bottom left. If you create several steps in a workflow or are working on a smaller browser screen, you may have more workflow steps than will fit in the configuration window. To navigate around the workspace and personalize it:

- Click and drag the workspace background to move the steps around the workspace. In this way you can reach steps at the top or bottom of the workflow that do not initially appear.
- Click the open button () to open the Workflow Definition dialog and the close button () to close the Workflow Definition dialog.
- Click the plus button with a circle around it () to add a new workflow step at that point in the workflow.
- Click the plus button in the lower left of the workspace () to zoom in on the steps.
- Click the minus button in the lower left of the workspace () to zoom out on the steps.
- Click the auto size button in the lower left of the workspace () to recenter and fit the steps to the window.

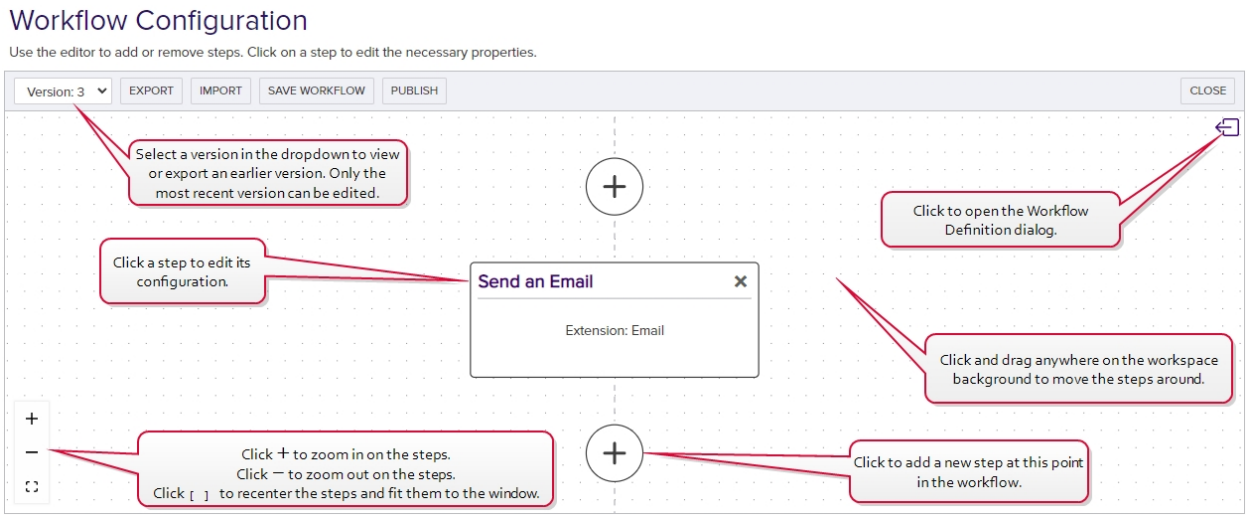


Figure 148: Using the Workflow Workspace

Tip: At any point while editing your workflow definition, you can click **Undo** at the bottom of the Add/Edit Workflow Definition dialog to undo changes made since the last save to the current workflow step you are editing or **Undo All** at the top of the workflow builder workspace to undo all changes made to the workflow definition since the last save.

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:
Workflow Definitions: *Read*
Workflow Definitions: *Modify*

To add a new workflow definition or modify an existing one:

1. In the Management Portal, browse to *Workflow > Workflow Definitions*.
2. On the Workflow Definitions page, click **Add** from the top menu to create a new blank workflow definition, **Copy** from either the top or right click menu to copy an existing workflow to create a new one, or **Edit** from either the top or right click menu, to modify an existing one. This will open the workflow in the workflow builder workspace with the Workflow Definition dialog open on the right.

   Note: When you create a new workflow definition by copying an existing one, the word *copy* will be appended to the end of the definition name and the workflow key (template or certificate collection) will be cleared. Other data from the copied workflow will be retained.

3. In the Add/Edit Workflow Definition dialog on the Definition tab, enter a **Name** for your workflow.

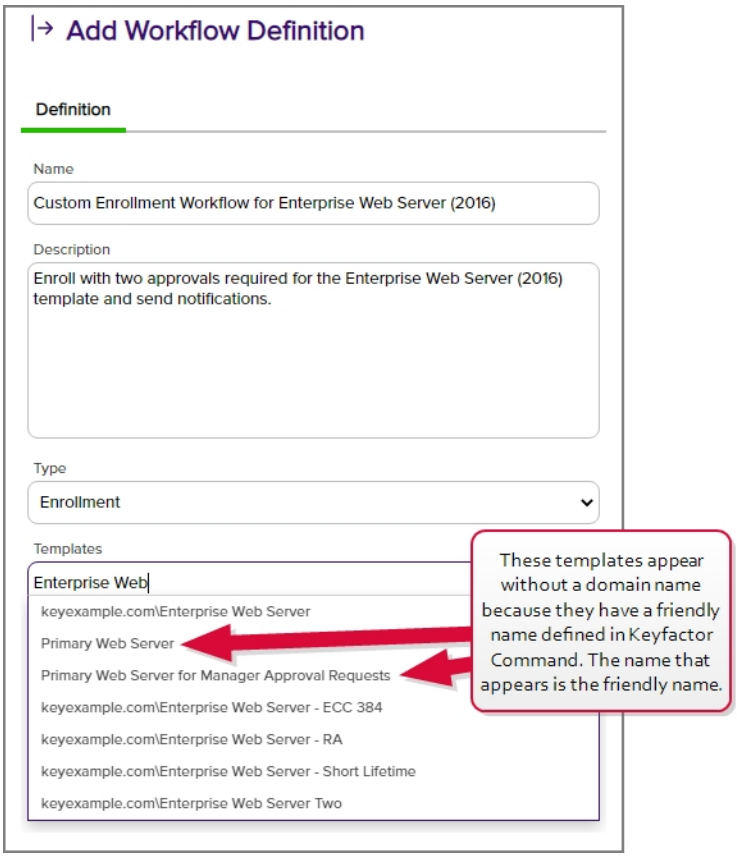


Figure 149: Create a New Workflow Definition

4. In the **Description** field, enter a description for the workflow definition.

5. In the **Type** dropdown, select the type of requests this workflow will handle. The following types are supported:

    - **Certificate Entered Collection**

      The workflow is initiated by an automated task that runs periodically to identify certificates that now meet the query criteria of the specified certificate collection. For example, when a certificate discovered on an SSL scan becomes part of the Weak Keys collection, an email message can be generated notifying the PKI administrators that a new certificate with a weak key has been discovered.

    - **Certificate Left Collection**

      The workflow is initiated by an automated task that runs periodically to identify certificates that no longer meet the query criteria of the specified certificate collection. For example, when a certificate in the Web Server Certificates collection disappears, a REST request can be made to open a support ticket request to investigate the removal of a web server certificate.

- **Enrollment (Including Renewals)**

  The workflow is initiated by enrollment for a new or renewed certificate. Steps during the workflow can be used to do things such as require manager approval for the enrollment or manipulate the subject and/or SANs for the certificate request.

- **Revocation**

  The workflow is initiated by revoking a certificate. Steps during the workflow can be configured to do things such as modify the revocation comment entered when the certificate is revoked, append an additional comment, and store the resulting extended comment in a metadata field.

The workflow type cannot be changed on an edit.

6. Once you have selected a type, a key field will appear. If you selected a type of Enrollment or Revocation, the key field is **Templates**. If you selected a type of Certificate Entered Collection or Certificate Left Collection, the key field is **Certificate Collections**. Begin typing in the **Templates** or **Certificate Collections** field to search for available templates or certificate collections or click in the field and scroll down to locate your desired template or certificate collection. Templates that have been configured with a template friendly name will appear by friendly name.

   The key cannot be changed on an edit.

   Tip: A given workflow can only apply to one key. If you need to run the same workflow steps for more than one key (e.g. the same enrollment steps for more than one template), you can either add these steps to the global workflow or, if you want to run the steps for more than one type of enrollment, for example, but not all, you can configure one custom workflow and then export and re-import that workflow to duplicate it (see Importing or Exporting a Workflow Definition on page 271) and edit the copy to change the key.

7. On the Workflow Configuration page, click the plus button in between two workflow steps where you want to add a new step. A new step box will be added below the plus that you clicked.

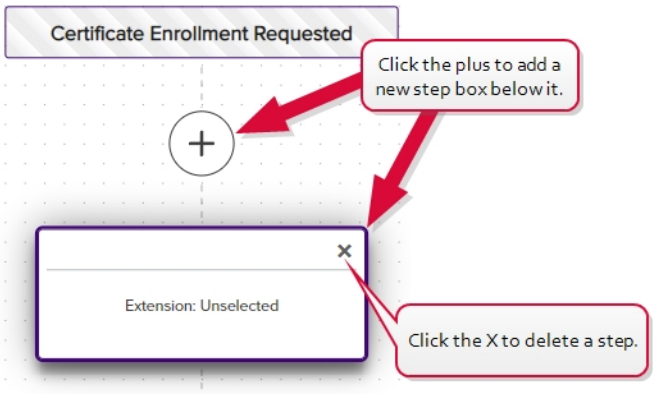


Figure 150: Click Plus to Add a New Workflow Definition Step

> **Tip:** To delete a step, click the X at the top right of the step box and confirm that you want to delete the step.

8. Click the new step box to load the step in the Add/Edit Workflow Definition dialog. If the dialog is not already open, clicking a step will open it, or you can open a step by clicking the open button ( ) and then clicking the desired step to load it into the dialog.

9. In the Add/Edit Workflow Definition dialog on the Step tab in the General section, select a **Step Type** for the step in the dropdown. To narrow the list of step types in the dropdown, begin typing a search string in the Search field. The built-in step types are:

    - **Send Email**

      Send an email message. This is a separate email message from those typically sent as part of a *Require Approval* step. You might send an email message as part of an enrollment request to notify approvers that a new request needs approval. The email messages can be customized to provide detailed information about, for example, the certificate request.

    - **Set Variable Data**

      Run PowerShell commands within the confines of the workflow to populate variables with information to pass back to the workflow. The PowerShell script contents are embedded within the step. This step does not call out to an external file. This provides a high level of security by greatly limiting the number of standard PowerShell cmdlets that can be executed by the workflow step. A small number of PowerShell cmdlets have been white listed to allow them to be included in workflow steps of this type, including:

        - Where-Object
        - ForEach-Object
        - Get-Command

    - **Use Custom PowerShell**

      Run a PowerShell script. The script contents are in a file placed in the ExtensionLibrary\Workflow directory or a subdirectory of it on the Keyfactor Command server under the install directory for Keyfactor Command. By default, this is:

      C:\Program Files\Keyfactor\Keyfactor Platform\ExtensionLibrary\Workflow

      The file must have an extension of .ps1. A sample PowerShell script is provided in the Workflow directory (CustomPowershellExample.ps1).

    - **Require Approval**

      Require approval for a workflow step before the step can be completed. The require approval step can require approval from just one approver or multiple approvers. The workflow will be suspended at this point until the correct number of approvals from users with the correct security roles is received or until one deny is received before continuing to the next step. As part of this step, an email message is sent indicating whether the step

was approved or denied—typically to the requester. This step does not include logic to send an email initiating the approval process (letting users know something needs approval). Use a *Send Email* type step for this.

Important: Workflows are not supported with CA delegation when they contain steps that require approval. For more information, see the CA configuration *Authorization Methods Tab*.

Note: The users that you send email to initiating the approval process must be members of a security role that is allowed to submit signals (approve/deny) for the workflow in order to approve or deny the request.

Tip: The workflow builder does not include a step to send a notification to the requester of a certificate on an enrollment once the certificate is issued by the CA (as opposed to approved in Keyfactor Command). Use the issued alerts for this (see *Issued Request Alert Operations*).

- **Invoke REST Request**

  Run a REST (API) request. The REST request contents are embedded within the step. It does not call out to an external file.

- **Update Certificate Request Subject\SANs for Microsoft CAs (Enrollment Only)**

  On an enrollment (either CSR or PFX), create a resigned CSR to prepare an updated enrollment request for delivery to a Microsoft CA after a previous step in the workflow has been used to update either the SANs in the initial request, subject (DN) in the initial request or both. This step must be placed later in the workflow than the step(s) to modify the SANs and/or subject. The SANs and subject may be modified with either of the PowerShell step types or a custom step type. The step creates a new CSR using the same public key as the original CSR using the updated SAN and/or subject values. It signs the new CSR with the certificate provided in the step's configuration.

  For this type of step you will need an enrollment agent certificate available as a PKCS#12 (.PFX) file with included private key to import into Keyfactor Command. This can be a user certificate or a computer certificate (e.g. generated from a copy of the *Enrollment Agent* template or the *Enrollment Agent (Computer)* template) and must have a Certificate Request Agent EKU. Note that the built-in *Enrollment Agent* and *Enrollment Agent (Computer)* templates do not allow private keys to be exported by default. You will need a template that allows private key export or will need to manually override private key export to create a certificate with an exportable private key in order to create a PKCS#12 (.PFX) file.

> **Important:** This step applies to Microsoft CAs only. If this step is added to workflow for requests directed to an EJBCA CA, it will fail on enrollment. Note that EJBCA supports submission of updated SAN or subject details as part of standard functionality.

- **Windows Enrollment Gateway - Populate from AD (Enrollment Only)**

  On an enrollment done through the Keyfactor Windows Enrollment Gateway using a client-side template configured with the *Build from this Active Directory information* option on the template, this workflow step handles formatting the incoming subject, SANs, and/or SID in the certificate request appropriately such that the enrollment will complete successfully with the target CA and Keyfactor Command template, which is not configured to build from AD. Any Keyfactor Windows Enrollment Gateway using a client-side template configured with the subject as *Build from this Active Directory information* must be configured with a workflow step of this type on the Keyfactor Command template that has been mapped in the gateway to that template in order to complete an enrollment through the gateway. There are no configuration parameters for the step.

  > **Important:** The template in Keyfactor Command that is mapped to the client-side template configured to build the subject from Active Directory also needs to be configured with three enrollment fields to support handling the incoming subject, SANs, and/or SID. For more information about configuring this, see the *Keyfactor Windows Enrollment Gateway Installation and Configuration Guide*.

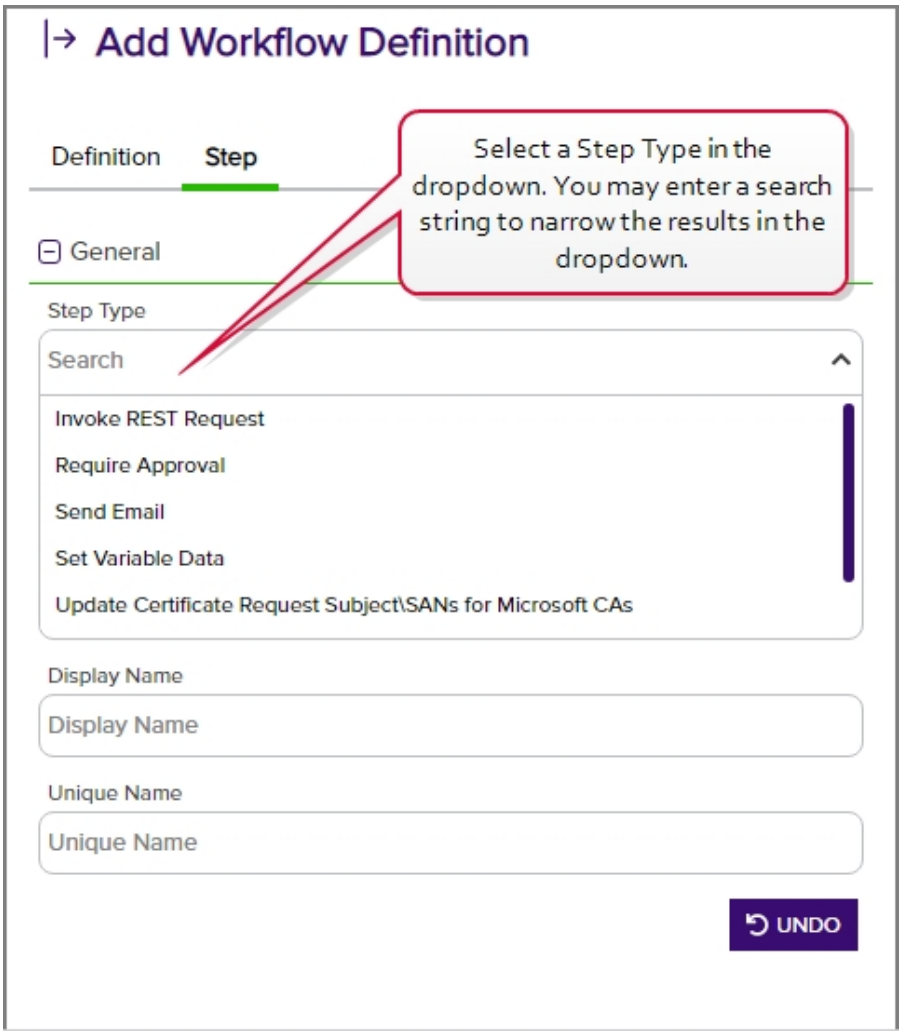


Figure 151: Select a Workflow Definition Step

Note: On an edit, if you change the workflow step type, you must also change the **Unique Name**. Changing the workflow step type without changing the unique name will result in an error similar to the following:

```
System.Collections.Generic.KeyNotFoundException: The given key was not present
in the dictionary
```

Instead of changing both the workflow step type and unique name, you may be prefer to delete the step and create a new step of the desired type.

10. In the Add/Edit Workflow Definition dialog on the Step tab in the General section, enter a **Display Name** for the step. This name appears as the title of the step box on the workflow

workspace page.

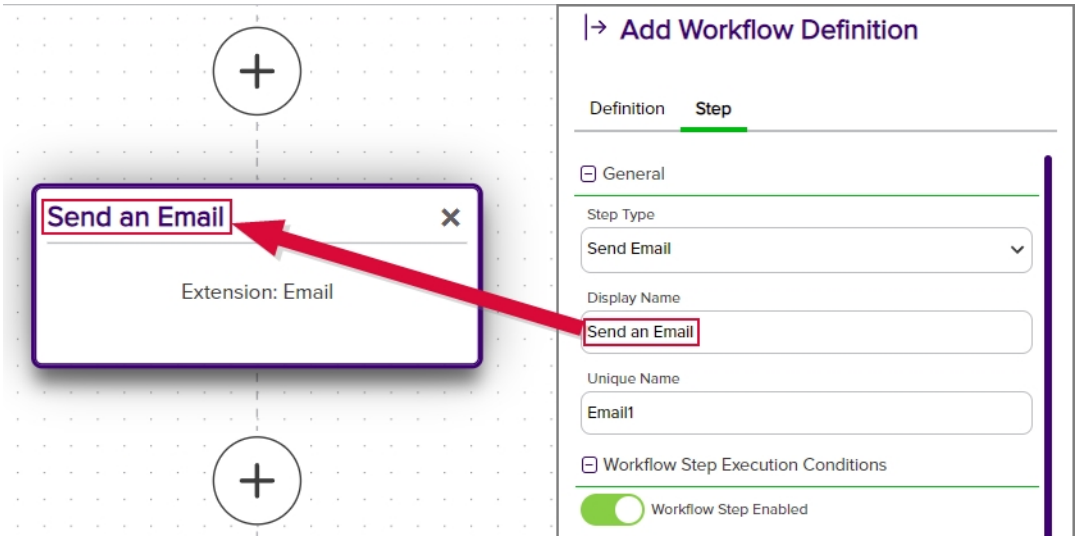


Figure 152: Display Name is Step Name Title

11. In the Add/Edit Workflow Definition dialog on the Step tab in the General section, either accept the automatically generated **Unique Name** for the step or modify it. This name must be unique among the steps within the particular workflow. It is intended to be used as a user-friendly reference ID.

12. In the Add/Edit Workflow Definition dialog on the Step tab in the Workflow Step Execution Conditions section, click the **Workflow Step Enabled** toggle to enable or disable the workflow. It is enabled by default.

13. In the Add/Edit Workflow Definition dialog on the Step tab in the Workflow Step Execution Conditions section, click **Add** in the Optional Workflow Step Conditions for Execution section to create a new condition for the step. Conditions are true/false statements indicating whether the step should run and can be based on tokens.

    Tip: Tokens (a.k.a. substitutable special text) may be used in the condition field. Tokens use a variable in the workflow definition that is replaced by data from the certificate request, certificate, or certificate metadata at processing time. For example, you can create a token in a PowerShell step that has a value of True or False based on something determined in the step and then evaluate that token in a subsequent require approval step to determine whether to execute the require approval step based on the results from the PowerShell step. Fields that support tokens are indicated with $() at the top right of the field. To use a token in a field, begin typing at the location where you want the token to appear, starting with **$(**. Once you have typed **$(**, a second **)** will appear automatically along with a dropdown of available tokens to choose from. You may continue

typing to narrow the values in the dropdown (e.g. type **$(req** to see only tokens that begin "req").

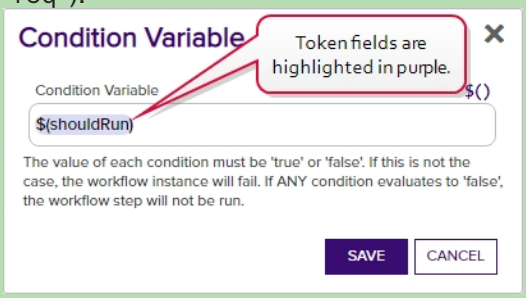


Figure 153: Tokens are Highlighted

To add a new condition, click Add and in the Condition Variable field enter either a static value of True or False or a token that will have a value of True or False at the time the step is run. More than one condition may be added. If multiple conditions are used in the same step, all conditions must have a value of True at the time the step is evaluated to be run in order for the step to run. If any single condition evaluates to False, the step will not run.

Example: The following example takes the common name entered during an enrollment and evaluates it to determine whether the domain name on it matches "keyexample.com" or not. If the domain is "keyexample.com", the enrollment is allowed to proceed without requiring approval. If the domain does not match "keyexample.com", the request requires approval. This example uses both a PowerShell Set Variable Data step and a Require Approval step.

To do this, first create the PowerShell step. Here we use a *Set Variable Data* step (see Set Variable Data on page 246) since no functions need to be called outside the confines of Keyfactor Command, though you could use a *Custom PowerShell Script* step instead. Add a Script Parameter to pull the request CN into the script.

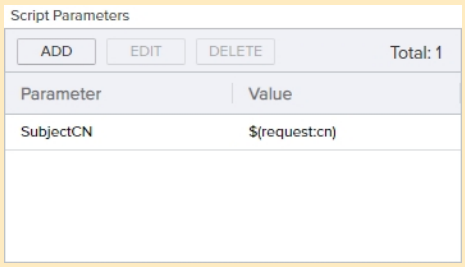


Figure 154: Conditions Example: Add Parameters

In the Insert PowerShell Script field, enter a script similar to the following:

```
# Declare your parameter at the beginning
param(
[string]$SubjectCN
)

# Initialize a variable for the response
$shouldRun = @()

# Check to see if the requested CN ends with keyexample.com and require approval in the
next step if it does not
$Suffix = "keyexample.com"

if ($SubjectCN.EndsWith($Suffix))
{
   $shouldRun = "False"
}else {
   $shouldRun = "True"
}

# Return the true/false value to the workflow as a hashtable
$result = @{ "shouldRun" = $shouldRun; }
return $result
```

Next, create the require approval request step (see Require Approval on page 241) with $(shouldRun) as a condition like so:

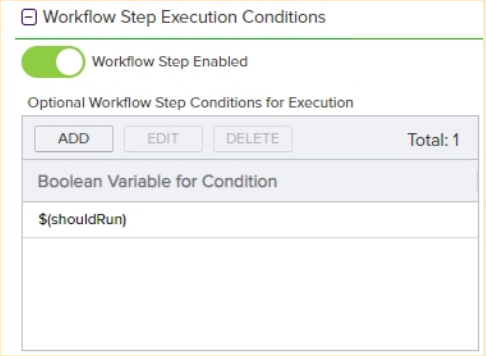


Figure 155: Conditions Example: Add Conditions for Require Approval Step

This condition on the require approval step will cause the approvals configured in the step to be required only if the CN submitted in the request does not end with

"keyexample.com", so a request for "CN=mycert.keyother.com" will require approval but a request for "CN=mycert.keyexample.com" will not.

14. The fields in the Configuration Parameters section of the Add/Edit Workflow Definition dialog on the Step tab will vary depending on the type of step you're configuring.

Tip: To open a pop-out dialog with more real-estate for editing content in large text areas, like scripts and email messages:

a. Navigate to the field you want to edit on the workflow definition.

b. Click at the top right above the large text field.

c. An *Edit Content* or *Edit PowerShell* window will open to accept your input. The *Edit Content* window supports token replacement. The *Edit PowerShell* window will open with a text editor. Enter your information.

d. Click at the top right to close the edit window and return to the workflow definition, populated with your text.

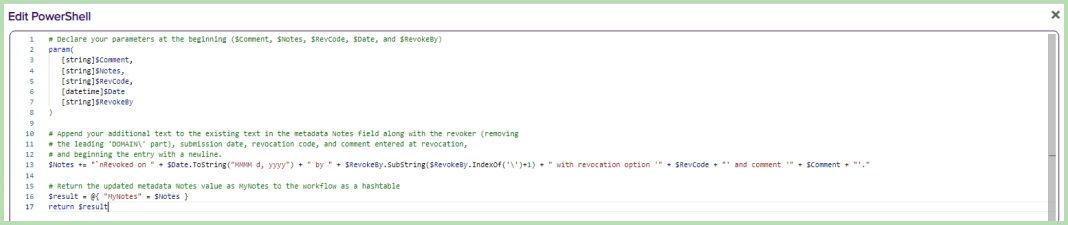


Figure 156: Edit PowerShell Window

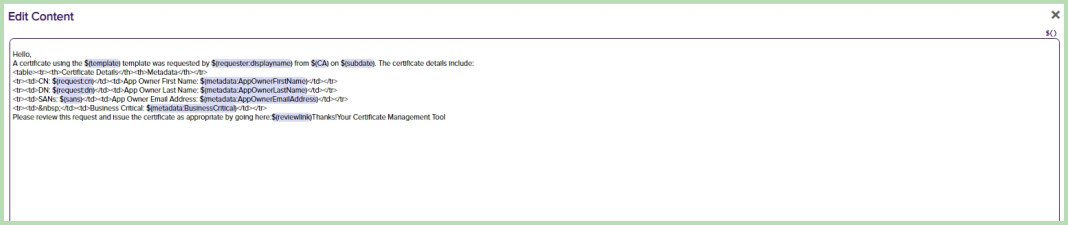


Figure 157: Edit Content Window

Invoke REST Request

Tip: Tokens (a.k.a. substitutable special text) may be used in the URL and request content fields. Tokens use a variable in the workflow definition that is replaced by data from the certificate request, certificate, or certificate metadata at processing time. For

example, you can take the revocation comment entered when the revocation request is approved—$(cmnt)—and insert it into a custom metadata field in the certificate by doing a PUT /Certificates/Metadata request for the $(id). Fields that support tokens are indicated with $() at the top right of the field. To use a token in a field, begin typing at the location where you want the token to appear, starting with **$(**. Once you have typed **$(**, a second **)** will appear automatically along with a dropdown of available tokens to choose from. You may continue typing to narrow the values in the dropdown (e.g. type **$(req** to see only tokens that begin "req").

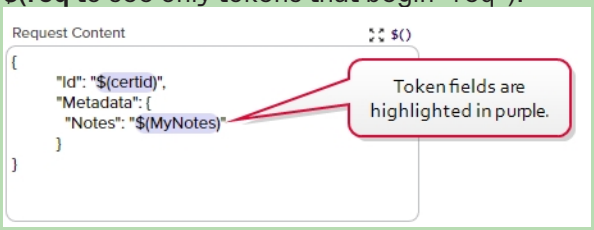


Figure 158: Tokens are Highlighted

- **Headers**: Enter any headers needed for your request. For a Keyfactor API request, this might look like:

```
x-keyfactor-requested-with: APIClient
x-keyfactor-api-version: 1
```

Tip: For a Keyfactor API request, version 1 is assumed if no version is specified. Content type and authorization headers do not need to be specified, since those are addressed elsewhere in the configuration.

- **Variable to Store Response in**: Provide a name for the parameter in which to store the response data from your request. You can then reference this parameter from subsequent steps in the workflow.

Tip: The response is stored as a serialized JObject. To make use of only a portion of the response data in your subsequent step, use JSON path syntax. For example, say you returned the data from a GET /Agents request in a variable called *MyResponse* and you wanted to reference the *ClientMachine* name for the orchestrator in a subsequent email message. To limit the data to the first result (0) and only the ClientMachine name, in the email message you would enter the following:

```
$(MyResponse.[0].ClientMachine)
```

- **Verb**: In the dropdown, select the type of request you wish to make (e.g. GET, POST).
- **Use Basic Authentication**: Check this box to use Basic authentication for the request. If you do not check this box, Windows authentication in the context of the Keyfactor Command application pool user will be used (see *Create Active Directory Service Accounts for Keyfactor Command* in the *Keyfactor Command Server Installation Guide*).
- **Username** and **[Password]**: Enter the username and password to use for authentication if *Use Basic Authentication* is checked. In the Username and Password dialogs, the options are Load From Keyfactor Secrets or Load From PAM Provider.
  A Keyfactor secret is a user-defined password or other information that is encrypted and stored securely in the Keyfactor Command database. Although Keyfactor recommends using Privileged Access Management (see Privileged Access Management (PAM) on page 677) as a more secure solution to secure information, Keyfactor Secret is an option for customers that do not already have a relationship with a PAM provider such as CyberArk or Delinea (formerly Thycotic).

  Select the **Load From Keyfactor Secrets** radio button as the *Secret Source* if you want Keyfactor Command to encrypt and store the password in the Keyfactor Command database. Enter and confirm a password.

  Select the **Load from PAM Provider** radio button as the *Secret Source* if you want to store the password in a supported third-party PAM solution (see Privileged Access Management (PAM) on page 677). The remaining fields on the dialog will vary depending on the PAM provider.

  ### CyberArk

  Select CyberArk in the **Providers** dropdown if your PAM provider is CyberArk. The remaining fields in the dialog will then be:

  - PrivateArk Protected Password Name—The name of the username or password in the safe (see Create a CyberArk Password on page 683).
  - PrivateArk Folder Name—The path and name of the folder that stores the CyberArk Password (e.g. Root or Root\MyDir).

  ### Delinea (formerly Thycotic)

  Select Delinea in the **Providers** dropdown if your PAM provider is Delinea. The remaining field in the dialog will then be:

  - Delinea Secret ID—The numeric ID of the secret to retrieve from Secret Server (see Create a Delinea Secret Server Secret on page 687).
- **URL**: Enter the request URL for the request, including tokens if desired. For a Keyfactor API request, this might look like (with query parameters):

```
https://keyfactor.keyexample.com/KeyfactorAPI/Certificates?pq.queryString=CN
%20-contains%20%22appsrvr14%22%20AND%20CertStorePath%20-ne%20NULL
```

Or, with tokens:

```
https://keyfactor.keyexample.com/KeyfactorAPI/Certificates/$(certid)
```

Note: To prevent REST requests from being made to inappropriate locations by malicious users, configure a system environment variable of KEYFACTOR_BLOCKED_OUTBOUND_IPS on your Keyfactor Command server pointing to the IP address or range of addresses in CIDR format that you wish to block. Both IPv4 and IPv6 addresses are supported. More than one address or range may be specified in a comma-delimited list. For example:

```
192.168.12.0/24,192.168.14.22/24
```

When a REST request is made where the URL is either configured to a blocked IP address or resolves via DNS to a blocked IP address, the REST request will fail.

- **Content-Type**: In the dropdown, select the content type for the request:
  - application/json
- **Request Content**: The request body of the REST request, if required, with tokens, if desired. For a Keyfactor API request, this will vary depending on the request and might look like (for a PUT /Certificates/Metadata request):

```
{
   "Id": "$(certid)",
   "Metadata":{
      "RevocationComment":"$(cmnt)"
   }
}
```

Note: This example assumes you have a metadata field called *RevocationComment* (see Certificate Metadata on page 646).

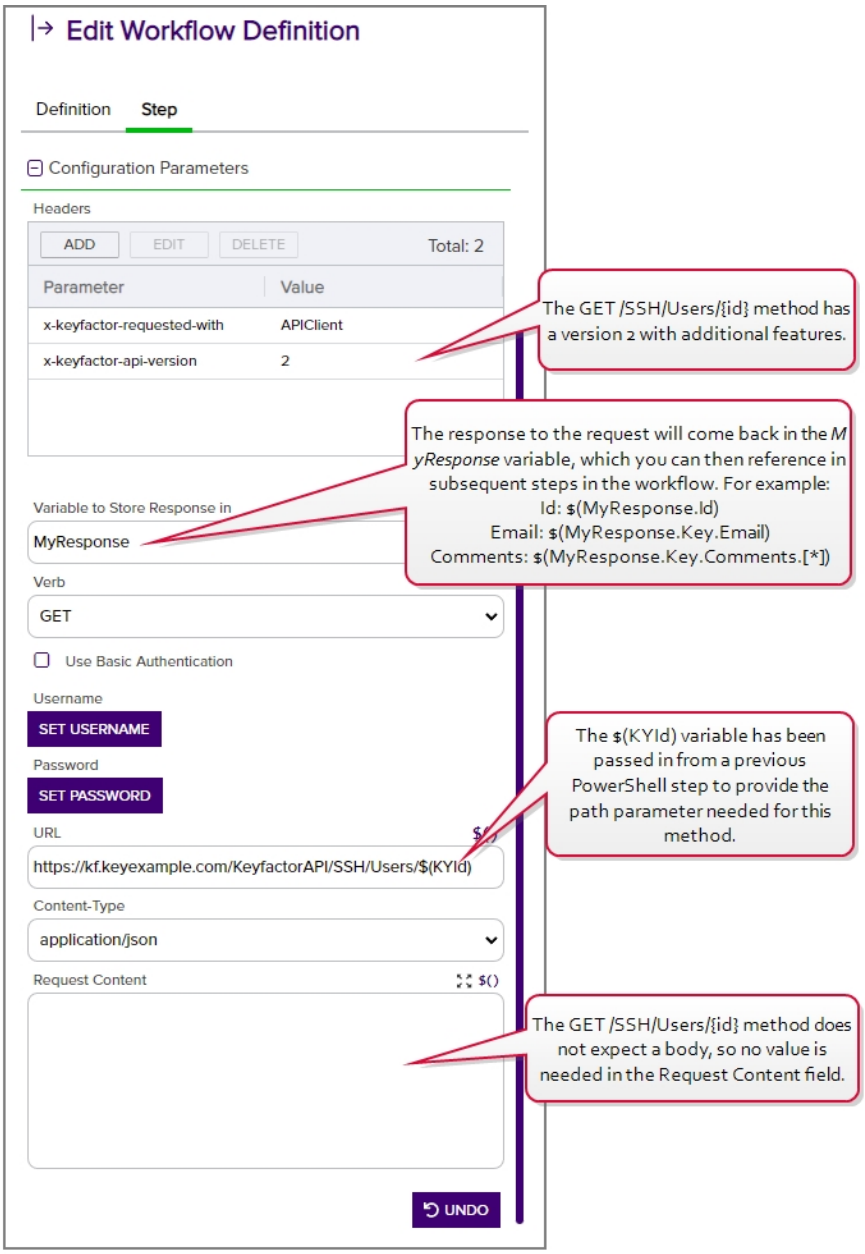


Figure 159: Configuration Parameters for an Invoke REST Request Workflow Definition Step

Example: The following example takes the revocation comment entered when a certificate is revoked and puts it together with some other information into a custom

metadata field, retaining any existing data in that metadata field. This example uses both a PowerShell step and a REST Request step to demonstrate passing of information from one step to the other.
To do this, first create the PowerShell step. Here we use a *Set Variable Data* step (see Set Variable Data on page 246) since no functions need to be called outside the confines of Keyfactor Command, though you could use a *Custom PowerShell Script* step instead. Add Script Parameters to pull the revocation comment, submission date, revocation code, user making the revocation request, and the metadata field into which you will place your updated comment ("Notes" in this example) into the script. Figure 160: Metadata Update Example: Add Parameters shows only four of these. The metadata field "Notes" is a BigText type field in this example (see Metadata Field Operations on page 646).

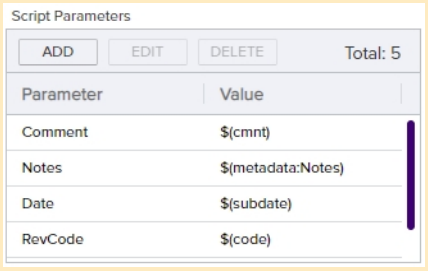


Figure 160: Metadata Update Example: Add Parameters

In the Insert PowerShell Script field, enter a script similar to the following:

```
# Declare your parameters at the beginning ($Comment, $Notes, $RevCode, $Date, and
$RevokeBy)
param(
   [string]$Comment,
   [string]$Notes,
   [string]$RevCode,
   [datetime]$Date
   [string]$RevokeBy
)

# Append your additional text to the existing text in the metadata Notes field along
with the revoker (removing
# the leading 'DOMAIN\' part), submission date, revocation code, and comment entered at
revocation,
# and beginning the entry with a newline.
```

```
$Notes += "`nRevoked on " + $Date.ToString("MMMM d, yyyy") + " by " +
$RevokeBy.SubString($RevokeBy.IndexOf('\')+1) + " with revocation option '" + $RevCode +
"' and comment '" + $Comment + "'."

# Return the updated metadata Notes value as MyNotes to the workflow as a hashtable
$result = @{ "MyNotes" = $Notes }
return $result
```

Next, create the REST request step with the following values:

- **Headers**:

```
{
   "x-keyfactor-requested-with": [
      "APIClient"
   ]
}
```

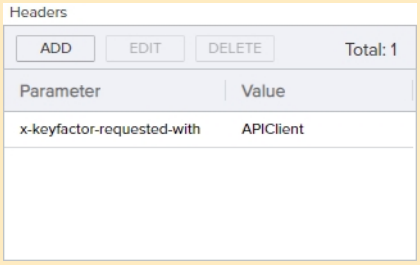


Figure 161: Metadata Update Example: Add Headers for REST Request

- **Variable to Store Response in**: None (there is no output from this command on a success)
- **Verb**: PUT
- **URL**: (Where *keyfactor.keyexample.com* is your Keyfactor Command server name.)

```
https://keyfactor.keyexample.com/KeyfactorAPI/Certificates/Metadata
```

- **Content-Type**: application/json

- **Request Content**:

```
{
   "Id": "$(certid)",
   "Metadata": {
      "Notes": "$(MyNotes)"
   }
}
```

This REST step takes the MyNotes output from the PowerShell step and updates the metadata Notes field to match that value. The resulting value in your Notes field will look something like this (assuming lines one, two and three were preexisting):

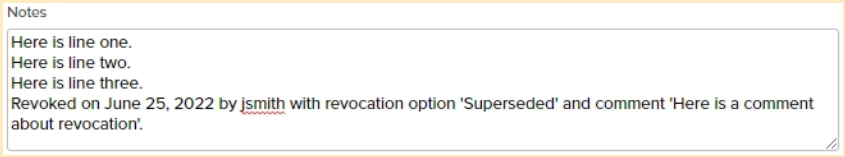


Figure 162: Metadata Update Example: Results

Note: You can achieve this same result of updating a metadata field entirely within PowerShell without using the REST step. This example uses both PowerShell and REST steps to demonstrate passing a value from one to the other.

Note: If your REST request takes a long time to complete, the step may time out and the workflow instance fail. The default timeout is 60 seconds and is configurable with the *Workflow Step Run Timeout* application setting (see Application Settings: Workflow Tab on page 605).

Require Approval

Tip: Tokens (a.k.a. substitutable special text) may be used in the subject line, message and email recipient fields. Tokens use a variable in the workflow definition that is replaced by data from the certificate request, certificate, or certificate metadata at processing time. For example, you can select $(requester) in the workflow definition for an enrollment request and the email message will contain the specific certificate requester name instead of the variable $(requester). Fields that support tokens are indicated with $() at the top right of the field. To use a token in a field, begin typing at the location where you want the token to appear, starting with **$(**. Once you have typed

$(, a second **)** will appear automatically along with a dropdown of available tokens to choose from. You may continue typing to narrow the values in the dropdown (e.g. type **$(req** to see only tokens that begin "req").

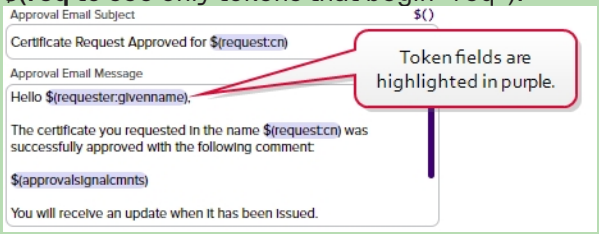


Figure 163: Tokens are Highlighted

Note: The users who will approve or deny the request must be members of a security role that is allowed to submit signals (e.g. approve requests) for the workflow in order to approve or deny the request.

- **Minimum Approvals**: Enter the minimum number of users who must approve the request to consider the request approved.
- **Denial Email Subject**: Enter the subject line for the email message that will be delivered if the request is denied, including tokens if desired.
- **Denial Email Message**: Enter the email message that will be delivered if the request is denied. The email message can be made up of regular text and tokens. If desired, you can format the message body using HTML. See Table 13: Tokens for Workflow Definitions for a complete list of available tokens.
- **Denial Email Recipients**: Click **Add**, enter a recipient for the denial email, and **Save**. Each email message can have multiple recipients. You can use specific email addresses and/or use tokens to replace an email address variable with actual email addresses at processing time. Available email tokens include:
    - $(requester:mail)

      The certificate requester, based on a lookup in Active Directory of the email address associated with the requester on the certificate.
    - Your custom email-based metadata field, which would be specified similarly to $(metadata:AppOwnerEmailAddress).
- **Approval Email Subject**: Enter the subject line for the email message that will be delivered if the request is approved, including tokens if desired.
- **Approval Email Message**: Enter the email message that will be delivered if the request is approved. The email message can be made up of regular text and tokens. If desired, you

can format the message body using HTML. See Table 13: Tokens for Workflow Definitions for a complete list of available tokens.

- **Approval Email Recipients**: Click **Add**, enter a recipient for the approval email, and **Save**. Each email message can have multiple recipients. You can use specific email addresses and/or use tokens to replace an email address variable with actual email addresses at processing time. Available email tokens include:
    - $(requester:mail)

      The certificate requester, based on a lookup in Active Directory of the email address associated with the requester on the certificate.
    - Your custom email-based metadata field, which would be specified similarly to $(metadata:AppOwnerEmailAddress).

Tip: The approval message is delivered before the enrollment actually takes place. To send an email alerting interested parties that the certificate was issued, including a link to download the certificate, use an issued certificate alert (see Issued Certificate Request Alerts on page 181).

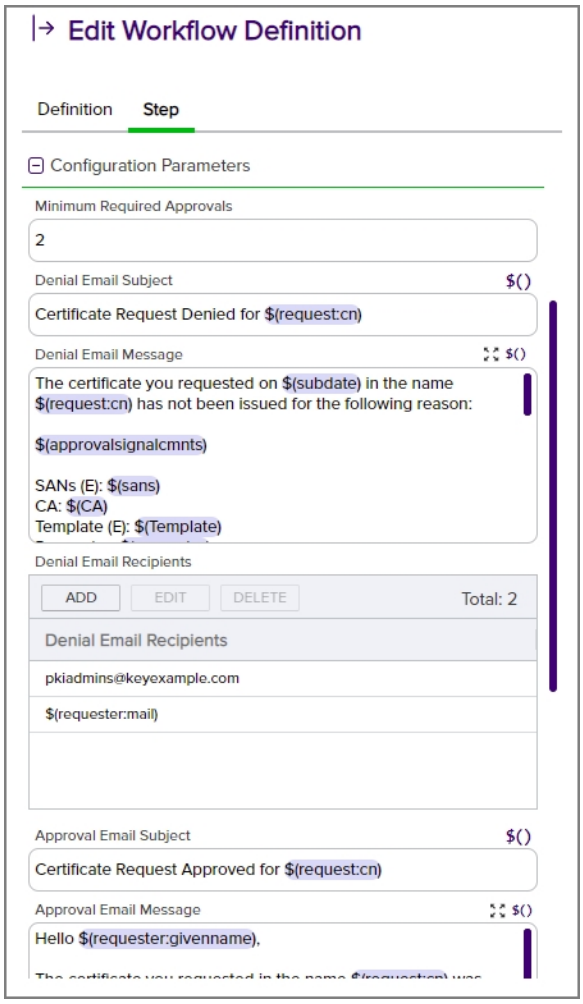


Figure 164: Configuration Parameters for a Require Approval Workflow Definition Step

Send Email

Tip: Tokens (a.k.a. substitutable special text) may be used in the subject line, message and email recipient fields. Tokens use a variable in the workflow definition that is replaced by data from the certificate request, certificate, or certificate metadata at processing time. For example, you can select $(requester) in the workflow definition for an enrollment request and the email message will contain the specific certificate requester name instead of the variable $(requester). Fields that support tokens are indicated with $() at the top right of the field. To use a token in a field, begin typing at the location where you want the token to appear, starting with **$(**. Once you have typed **$(**, a second **)** will appear automatically along with a dropdown of available tokens to

choose from. You may continue typing to narrow the values in the dropdown (e.g. type **$(req** to see only tokens that begin "req").

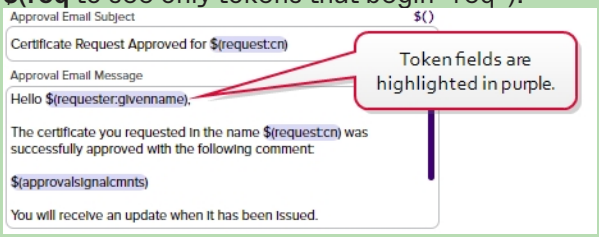


Figure 165: Tokens are Highlighted

- **Subject**: Enter the subject line for the email message that will be delivered when the workflow definition step is executed, including tokens if desired.
- **Message**: Enter the email message that will be delivered when the workflow definition step is executed. The email message can be made up of regular text and tokens. If desired, you can format the message body using HTML. For example, for an enrollment pending request notification:

  ```
  Hello,
  A certificate using the $(template) template was requested by $(requester:displayname) from $(CA) on $(subdate). The certificate details include:
  <table>
  <tr><th>Certificate Details</th><th>Metadata</th></tr>
  <tr><td>CN: $(request:cn)</td><td>App Owner First Name: $(metadata:AppOwnerFirstName)</td></tr>
  <tr><td>DN: $(request:dn)</td><td>App Owner Last Name: $(metadata:AppOwnerLastName)</td></tr>
  <tr><td>SANs: $(sans)</td><td>App Owner Email Address: $(metadata:AppOwnerEmailAddress)</td></tr>
  <tr><td> </td><td>Business Critical: $(metadata:BusinessCritical)</td></tr>
  Please review this request and issue the certificate as appropriate by going here: $(reviewlink)
  Thanks!
  Your Certificate Management Tool
  ```

  See Table 13: Tokens for Workflow Definitions for a complete list of available tokens.
- **Recipients**: Click **Add**, enter a recipient for the email, and **Save**. Each email message can have multiple recipients. You can use specific email addresses and/or use tokens to replace an email address variable with actual email addresses at processing time. Available email tokens include:

- $(requester:mail)

  The certificate requester, based on a lookup in Active Directory of the email address associated with the requester on the certificate.

- Your custom email-based metadata field, which would be specified similarly to $(metadata:AppOwnerEmailAddress).

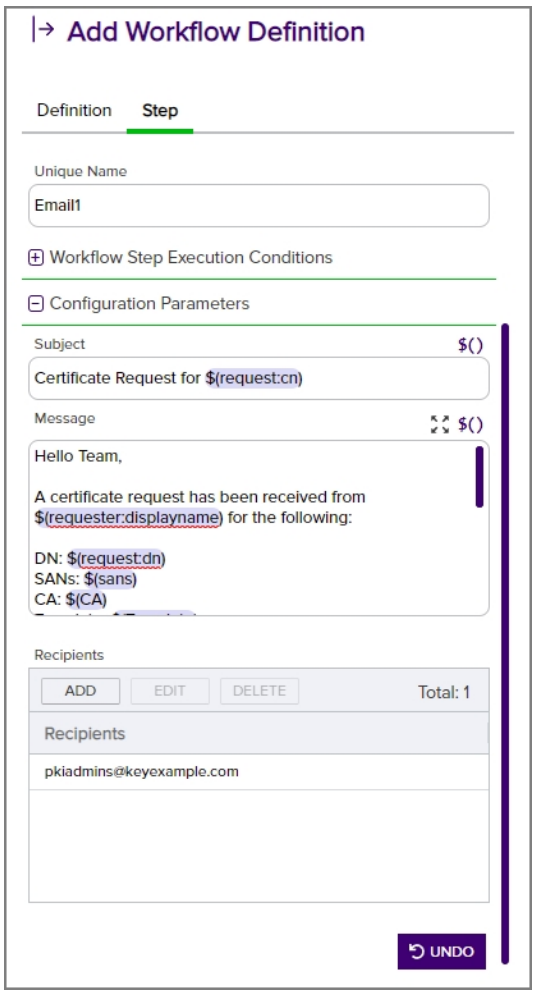


Figure 166: Step Configuration for an Email Workflow Definition Step

Set Variable Data

Tip: Tokens (a.k.a. substitutable special text) may be used in the script parameter value field. Tokens use a variable in the workflow definition that is replaced by data from the certificate request, certificate, or certificate metadata at processing time. For example,

you can take the revocation comment entered when the revocation request is approved—$(cmnt)—and append additional data to it using PowerShell.

- **Script Parameters**: Add any parameters you will use to pass data into your script. These can contain static values or tokens (see Table 13: Tokens for Workflow Definitions). To add a parameter:

  a. In the Script Parameters section, click **Add**.

  b. In the Add/Edit Parameter dialog, enter a name for the parameter in the **Parameter** field. In the **Value** field, enter either a static value to be passed into the PowerShell script or select from the available tokens to pass the token value into the Power-Shell in your parameter.

  c. Click **Save** to save your parameter.

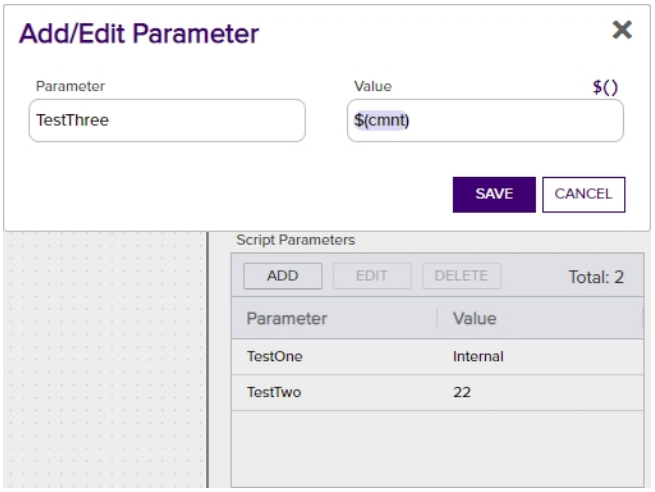


Figure 167: Add Parameters for PowerShell

- **Insert PowerShell Script**: Enter the PowerShell commands to execute. This should be the actual contents of the PowerShell script (the PowerShell commands and supporting components), not a path and filename to an external file.

  To receive your defined parameters from the previous step into the PowerShell script, begin the script by declaring the expected parameters like so (referencing the three parameters—TestOne, TestTwo, and TestThree):

```
param(
[string]$TestOne,
[int]$TestTwo,
```

```
[string]$TestThree
)
```

You may then use these parameters within the script.

To return data from the PowerShell script, create a hashtable of the data you wish to return like so (where $MyField1 and $MyField2 are parameters introduced within the script and the new value in $TestThree is reloaded back into that parameter and used to update that field if the original parameter was set to a token):

```
$result = @{ "MyFieldOne" = $MyField1; "MyFieldTwo" = $MyField2; "TestThree" =
$TestThree }
return $result
```

This will result in the following dictionary entries being added to the database and available for output or use in subsequent steps in the workflow:

```
{["MyFieldOne", "[your value as defined in the script"], ["MyFieldTwo", "[your value as
defined in the script"], ["TestThree", "[your value as defined in the script"],]}
```

You can reference these as tokens in subsequent steps as follows: $(MyFieldOne), $(MyFieldTwo), $(TestThree).

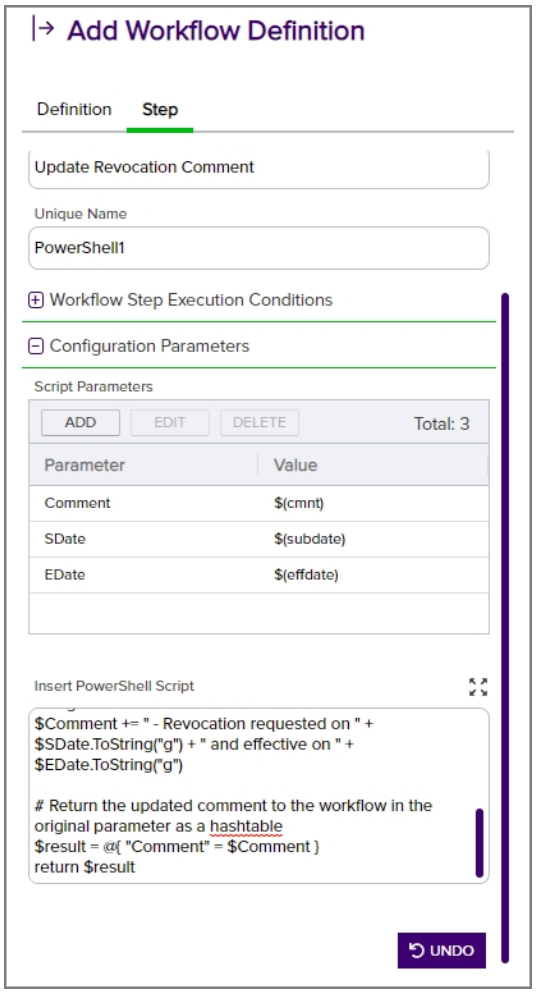


Figure 168: Configuration Parameters for a Set Variable Data Workflow Definition Step

Example: The following example takes the revocation comment entered when a certificate is revoked and appends an additional comment, including dates, to it. To create this, add Script Parameters to pull the revocation comment, submission date and effective date into the script as shown in Figure 160: Metadata Update Example: Add Parameters.

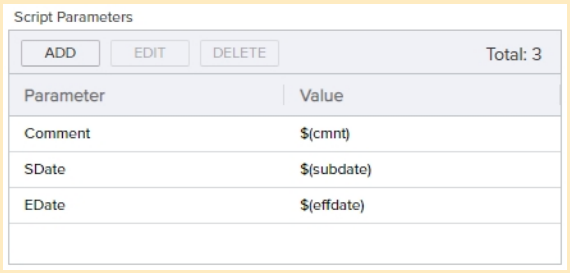


Figure 169: Revocation Comment Update Example: Add Parameters

In the Insert PowerShell Script field, enter a script similar to the following:

```
# Declare your parameters at the beginning ($Comment, $SDate, and $Edate)
param(
   [string]$Comment,
   [datetime]$SDate,
   [datetime]$EDate
)

# Append your additional text to the existing comment along with the submission and
effective dates
$Comment += " - Revocation requested on " + $SDate.ToString("g") + " and effective on "
+ $EDate.ToString("g")

# Return the updated comment to the workflow in the original parameter as a hashtable
$result = @{ "Comment" = $Comment }
return $result
```

The resulting comment will look something like:

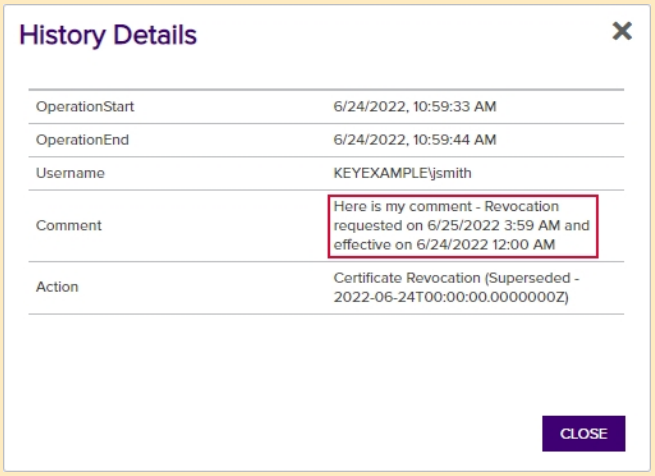


Figure 170: Revocation Comment Update Example: Results

You may reference the updated comment using the standard revocation comment token ($(cmnt)) in subsequent steps in your workflow and may view the updated comment wherever the revocation comment is available for viewing within Keyfactor Command.

Example: The following example takes two additional enrollment fields submitted on an enrollment and sets the value of one to a fixed value if the value of the other (a multi-value field) is a given value. In other words, the possible values for Department (a multi-value field) are:

- Accounting
- E-Commerce
- HR
- IT
- Marketing
- R & D
- Sales

If the value of Department is anything other than Accounting, the value of Code (a string field) can be any value. If the value of Department is Accounting, anything submitted in the Code field by the end user is discarded and replaced by the fixed value for Code provided in the script.

This example provides a solution using a *Set Variable Data* step type, which necessitates manually unpacking the JSON attribute string. One possible method of doing

this is provided in the example. If you prefer, you may instead use a *Use Custom PowerShell* step with the *ConvertFrom-Json* cmdlet similarly to the example for putting approval comments in a metadata field and avoid the manual string manipulation steps.

To create this, add Script Parameters to pull the additional attributes into the script as shown in Figure 171: Additional Attribute Update Example: Add Parameters

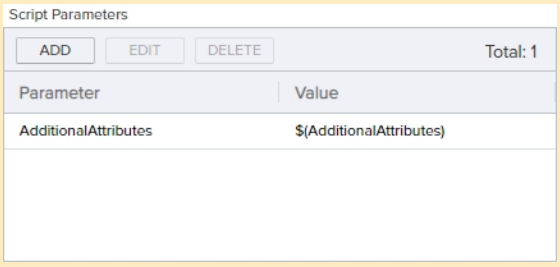


Figure 171: Additional Attribute Update Example: Add Parameters

In the Insert PowerShell Script field, enter a script similar to the following:

```
# Declare your parameters at the beginning
param(
[string]$AdditionalAttributes
)

# Trim brackets off incoming attribute string
$TrimmedAttributes = $AdditionalAttributes.Substring(1,$AdditionalAttributes.Length-2)

# Replace commas bracketed by quotes in attribute string with a temporary string to
facilitate splitting (assumes no incoming values contain temp string)
$TempString = "`"######`""
$CleanAttributes = $TrimmedAttributes -replace "`",`"", $TempString

# Split the incoming attribute string into its component values at the temporary string
$SplitAttributes = $CleanAttributes.Split('######')

# Split the incoming attribute string key/value pairs
foreach($attribute in $SplitAttributes){
   $attributeComponents = $attribute.Trim() -split ":"
   $attributeComponents
   Switch($attributeComponents[0].Trim()){
```

```
      '"Department"' {$Department = $attributeComponents[1].Substring(1,$at-
tributeComponents[1].Length-2)}
      '"Code"' {$Code = $attributeComponents[1].Substring(1,$attributeComponents
[1].Length-2)}
   }
}

# Initialize a hashtable
$UpdatedAttributes = @{}

# Load original attributes in UpdatedAttributes for the else case
if(![string]::IsNullOrWhiteSpace($Code)) {
   $UpdatedAttributes['Code'] = $Code
}
if(![string]::IsNullOrWhiteSpace($Department)) {
   $UpdatedAttributes['Department'] = $Department
}

# If the value of Department is "Accounting", then the value of Code must be "G5N145";
override submitted value--if any--and use fixed value
if($UpdatedAttributes['Department'] -eq "Accounting") {
   $UpdatedAttributes['Code'] = "G5N145"
}

# Return the updated attributes to the workflow in the original parameter as a hashtable
$result = @{ "AdditionalAttributes" = $UpdatedAttributes }
return $result
```

The updated attributes will be submitted to the CA as part of the enrollment package and can be viewed in the workflow instance (see Viewing a Workflow Instance on page 285).

Use Custom PowerShell

Tip: Tokens (a.k.a. substitutable special text) may be used in the script parameter value field. Tokens use a variable in the workflow definition that is replaced by data from the certificate request, certificate, or certificate metadata at processing time. For example, you can take the revocation comment entered when the revocation request is approved—$(cmnt)—and append additional data to it using PowerShell.

- **Script Parameters**: Add any parameters you will use to pass data into your script. These can contain static values or tokens (see Table 13: Tokens for Workflow Definitions). To

add a parameter:

a. In the Script Parameters section, click **Add**.

b. In the Add/Edit Parameter dialog, enter a name for the parameter in the **Parameter** field. In the **Value** field, enter either a static value to be passed into the PowerShell script or select from the available tokens to pass the token value into the Power-Shell in your parameter.

c. Click **Save** to save your parameter.

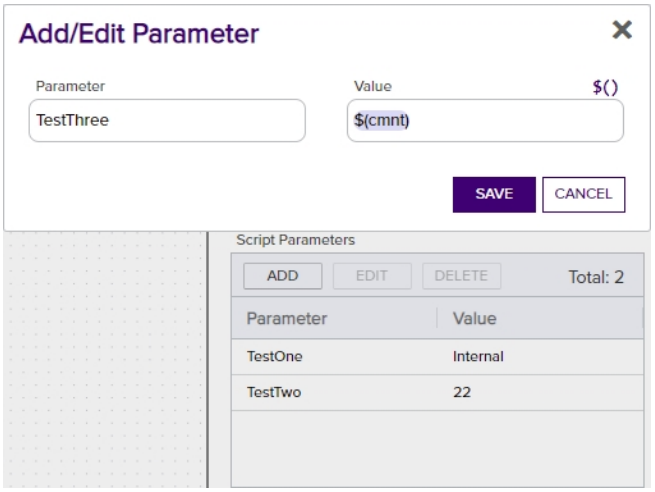


Figure 172: Add Parameters for PowerShell

- **PowerShell Script Name**: Select a script in the dropdown. The script needs to be in the ExtensionLibrary\Workflow directory or a subdirectory of it on the Keyfactor Command server under the install directory. By default, this is:

  C:\Program Files\Keyfactor\Keyfactor Platform\ExtensionLibrary\Workflow

  The file must have an extension of .ps1.

  The script should use the same input and output method for parameters as described for the Set Variable Data step type (see Set Variable Data on page 246). A sample Power-Shell script is provided in the Workflow directory (CustomPowershellExample.ps1).

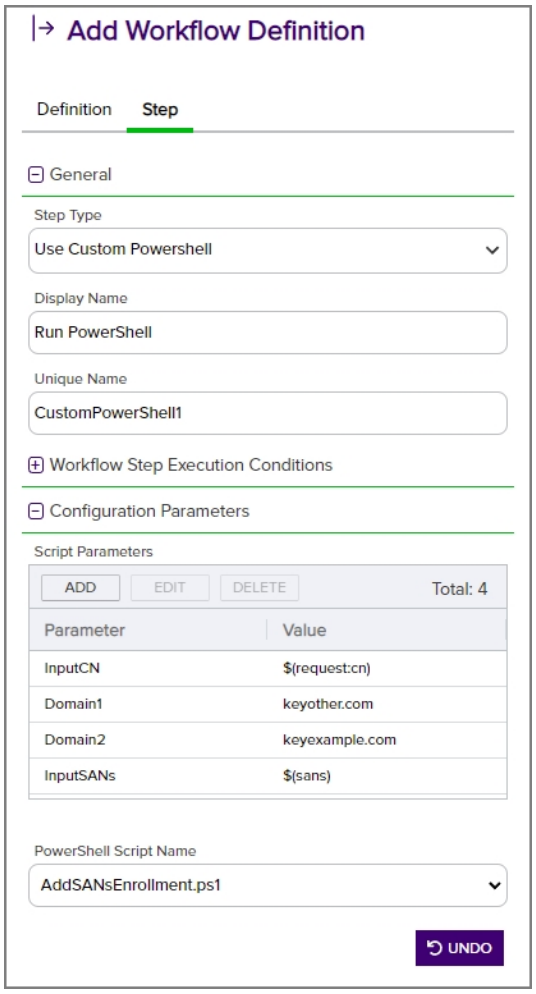


Figure 173: Step Configuration for a Custom PowerShell Workflow Definition Step

Example: The following example takes the common name entered during an enrollment and evaluates it to determine whether the domain suffix ends with “keyexample.com”. If it does, the script does a DNS lookup of the full CN to find the IPv4 address for that name and, if found, adds that value as a SAN to the request. Two additional SANs are added to the request by removing the “keyexample.com” domain suffix and instead appending the domain suffixes provided in the Domain1 and Domain2 parameters (e.g. mycert.keyother.com and mycert.keyother2.com). If the CN does not have a domain suffix ending with “keyexample.com”, the PowerShell script does nothing.

This step needs to be a *Use Custom PowerShell* step rather than a *Set Variable Data* step because it calls a PowerShell command (*Resolve-DnsName*) that exists outside the confines of Keyfactor Command.

To create this, add Script Parameters to pull the CN and SANs into the script as shown in Metadata Update Example: Add Parameters on page 239 and add to static values to pass in your two additional domain names.

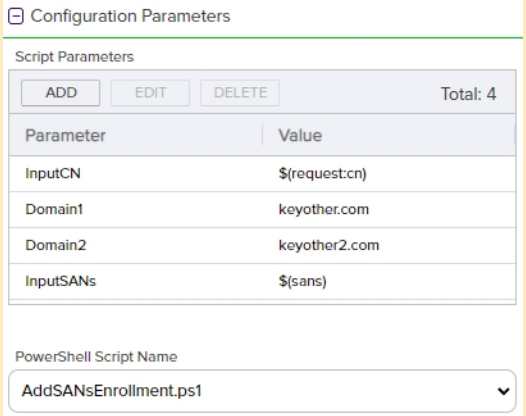


Figure 174: Update SANs Example: Add Parameters

In the *PowerShell Script Name* field, in the dropdown select the script containing content similar to the following:

```
# Declare your parameters at the beginning ($InputCN, $Domain1, $Domain2, and
$InputSANs)
param(
   [string]$InputCN,
   [string]$Domain1,
   [int]$Domain2,
   [string]$InputSANs
)

# Split the incoming SANs string into its component values
$SplitSANs = $InputSANs.Split(',')

# Initialize variables for the two types of SANs we're handling
$DnsSans = @()
$IpSans = @()
```

```
# Add the incoming SANs to the correct list (assumes only IPv4 addresses or DNS SANs
will be encountered)
foreach($san in $SplitSANs){
   $sanComponents = $san.Trim() -split ":"
   Switch ($sanComponents[0].Trim()){
      "DnsName" {$DnsSans += ,$sanComponents[1].Trim()}
      "IPAddress" {$IpSans += $sanComponents[1].Trim()}
   }
}

# Check to see if the incoming CN ends with keyexample.com and, if so, add some SANs.
$Suffix = "keyexample.com"

if ($InputCN.EndsWith($Suffix))
{
   # Load just the portion of the CN without the domain name into a variable.
   $CNName = $InputCN.SubString(0,$InputCN.Length - $Suffix.Length)

   # Do a lookup on the requested CN to find its IPv4 address.
   $IPResult = Resolve-DnsName -Name $InputCN -Type A -ErrorAction SilentlyContinue

   # If an address is found, add that address as a SAN.
   # Also add SANs built with the contents of Domain1, Domain2, and the leading part of
the CN
   # (e.g. mycert.my-first-other-domain.com and mycert.my-second-other-domain.com).
   if ($IPResult -ne $null)
   {
      $SAN1 = $IPResult.IPAddress
      $SAN2 = $CNName + $Domain1
      $SAN3 = $CNName + $Domain2
      $DnsSans += ,$SAN2
      $DnsSans += ,$SAN3
      $IpSans += ,$SAN1
   # If an IP address is not found, add only the SANs featuring Domain1 and Domain2.
   else {
      $SAN2 = $CNName + $Domain1
      $SAN3 = $CNName + $Domain2
      $DnsSans += ,$SAN2
```

```
      $DnsSans += ,$SAN3
   }
}

# Load the resulting IPv4 and DNS SANs into the SANS variable
$UpdatedSANs = @{}

if(![string]::IsNullOrWhiteSpace($DnsSans)) {
   $UpdatedSANs['dns'] = $DnsSans
}

if(![string]::IsNullOrWhiteSpace($IpSans)) {
   $UpdatedSANs['ip4'] = $IpSans
}

# Return the updated SANs to the workflow as a hashtable (case matters in the return
value name "SANs" in order
# to reload the results back into the SANs token)
$result = @{ "SANs" = $UpdatedSANs; }
return $result
```

Your enrollment will complete using the updated list of SANs, including any SANs you added manually on the PFX enrollment page or in the CSR. You may reference the updated SANs using the standard SANs token ($(sans)) in subsequent steps in your workflow and may view the complete SAN list wherever the SANs are available for viewing within Keyfactor Command.

Note: If you're using a Microsoft CA, in order to add SANs in the workflow you will need to do one of the following:

- Include an Update Certificate Request Subject\SANs step in your workflow (see Update Certificate Request Subject\SANs for Microsoft CAs on page 261). This is Keyfactor's preferred solution for workflow due to the limited risk profile.
- Use Keyfactor's SAN Attribute Policy Handler (see *Installing the Keyfactor CA Policy Module Handlers*). This opens security risks as well, which can be mitigated, however, this is not Keyfactor's preferred solution for workflow.

- Configure your CA to support the addition of SANs outside the initial request (enable the EDITF_ATTRIBUTESUBJECTALTNAME2 flag). Keyfactor does not recommend this solution due to the inherent security risks.

Example: The following example takes the approval comment entered when a certificate is enrolled or the approval or denial comment entered when a certificate is revoked using a require approval step and stores the comment in a metadata field. There will be no certificate to associate the metadata field with for an enrollment request that is denied. Normally, approval and denial comments are discarded after a workflow instance is complete, so this allows the comment to be retained.
To create this, after the Require Approval step(s) in the workflow, add a *Use Custom PowerShell* step. A Use Custom PowerShell step is used here because we are calling the external command *ConvertFrom-Json*. If you wanted to use a Set Variable Data step instead, you would need to go through a process of extracting all your metadata values from the incoming metadata string and placing them in a hashtable instead of using *ConvertFrom-Json* (see the additional attributes example).

In the Use Custom PowerShell step, add Script Parameters to pull any approval comments and the metadata field you're planning to store them in (in this example, a field called ApprovalComments) into the script , along with the metadata bucket to include any remaining metadata values, as shown in Figure 175: Approval Comment Update Example: Add Parameters.

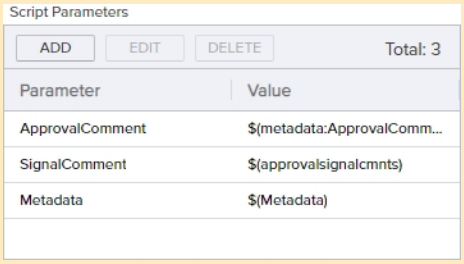


Figure 175: Approval Comment Update Example: Add Parameters

In the *PowerShell Script Name* field, in the dropdown select the script containing content similar to the following:

```
# Declare your parameters at the beginning
param(
```

```
[string]$ApprovalComment,
[string]$SignalComment,
[string]$Metadata
)

# Initialize a hashtable to contain your metadata fields and populate it
$UpdatedMetadata = @{}
$jsonobject = $Metadata | ConvertFrom-Json
foreach( $property in $jsonobject.PSObject.Properties )
{
$UpdatedMetadata[$property.Name] = $property.Value
}

# Append your signal comment(s) to any existing comment in the ApprovalComment metadata
field
if([string]::IsNullOrWhiteSpace($ApprovalComment)) {
$UpdatedMetadata['ApprovalComment'] = $SignalComment
}else {
$UpdatedMetadata['ApprovalComment'] = $ApprovalComment + ", " + $SignalComment
}

# Return the updated metadata fields, including ApprovalComment, to the workflow in the
original parameter as a hashtable
$result = @{ "ApprovalComment" = $UpdatedMetadata }
return $result
```

The resulting comment will look something like:

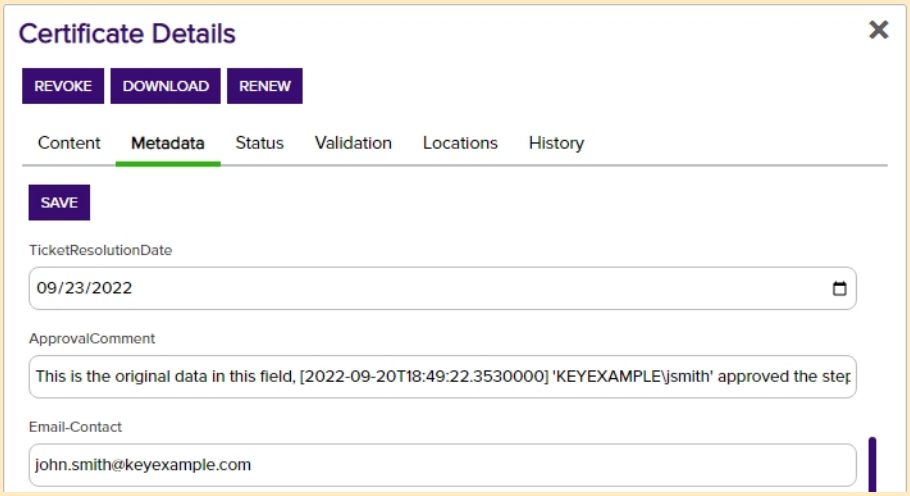


Figure 176: Approval Comment Update Example: Results

If the workflow requires multiple approvals or has multiple require approval steps, all the approval comments entered in the given workflow instance prior to the PowerShell step will be added to the metadata field. If you expect to have multiple comments, you may prefer to use a big text field rather than the string type fields shown here.

Note: If your PowerShell script takes a long time to execute, the step may time out and the workflow instance fail. The default timeout is 60 seconds and is configurable with the *Workflow Step Run Timeout* application setting (see Application Settings: Workflow Tab on page 605).

Update Certificate Request Subject\SANs for Microsoft CAs

This step is used to create a new signed CSR to prepare an updated enrollment request for delivery to a Microsoft CA after a previous step in the workflow has been used to update either the SANs in the initial request, subject (DN) in the initial request or both. This step must be placed later in the workflow than the step(s) that modify the SANs and/or subject. The SANs and subject may be modified with either of the PowerShell step types (see Set Variable Data on page 246 and Use Custom PowerShell on page 253) or a custom step type. This step is used for both PFX enrollment and CSR enrollment, since both use a CSR that is generated at the start of the workflow. A Microsoft CA will not accept a CSR for enrollment if the subject has been modified and will only accept a CSR for enrollment with modified SANs if the EDITF_ATTRIBUTESUBJECTALTNAME2 flag has been enabled on the CA—a security risk Keyfactor does not recommend. EJBCA doesn't support enroll on behalf of (EOBO), so this step type does not apply to EJBCA CAs. EJBCA is able to handle subject and SAN changes without the need for this type of step based on end entity profile constraints.

- **Enrollment Agent Certificate**: Click **Browse** to search for the desired base-64 encoded PKCS#12 (.PFX) enrollment agent certificate with private key to sign the CSR. This can be either a user certificate or a computer certificate and must have a Certificate Request Agent EKU.
- **Set Private Key Password**: The password for the enrollment agent certificate. Click **Set Private Key Password** to open the *Private Key Password* dialog. Choose the *No Value* checkbox to not assign a password, or choose from Load From Keyfactor Secrets or Load From PAM Provider.

  A Keyfactor secret is a user-defined password or other information that is encrypted and stored securely in the Keyfactor Command database. Although Keyfactor recommends using Privileged Access Management (see Privileged Access Management (PAM) on page 677) as a more secure solution to secure information, Keyfactor Secret is an option for customers that do not already have a relationship with a PAM provider such as CyberArk or Delinea (formerly Thycotic).

  Select the **Load From Keyfactor Secrets** radio button as the *Secret Source* if you want Keyfactor Command to encrypt and store the password in the Keyfactor Command database. Enter and confirm a password.

  Select the **Load from PAM Provider** radio button as the *Secret Source* if you want to store the password in a supported third-party PAM solution (see Privileged Access Management (PAM) on page 677). The remaining fields on the dialog will vary depending on the PAM provider.

  ### CyberArk

  Select CyberArk in the **Providers** dropdown if your PAM provider is CyberArk. The remaining fields in the dialog will then be:

  - PrivateArk Protected Password Name—The name of the username or password in the safe (see Create a CyberArk Password on page 683).
  - PrivateArk Folder Name—The path and name of the folder that stores the CyberArk Password (e.g. Root or Root\MyDir).

  ### Delinea (formerly Thycotic)

  Select Delinea in the **Providers** dropdown if your PAM provider is Delinea. The remaining field in the dialog will then be:

  - Delinea Secret ID—The numeric ID of the secret to retrieve from Secret Server (see Create a Delinea Secret Server Secret on page 687).

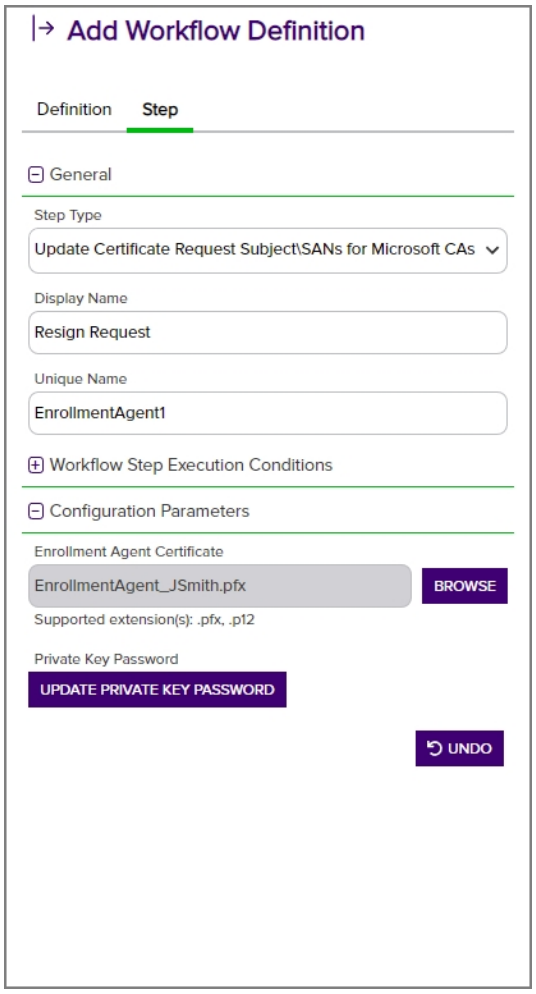


Figure 177: Update Certificate Request Subject\SANs for Microsoft CAs Workflow Definition Step

Example: The following example uses PowerShell to take the distinguished name (subject) and SANs entered during an enrollment along with two static domain names and evaluates the domain name of the common name in the subject to determine whether the domain suffix ends with the "original" domain name provided in the static value ("keyexample.com"). If it does, the script replaces the domain name in the subject with the value provided by the "new" static value and adds a SAN with CN prefix and the new domain name (e.g. CN=mycert.keyexample.com becomes CN=m-mycert.keyother.com and a SAN is added for mycert.keyother.com). If the CN does not have a domain suffix ending with "keyexample.com", the PowerShell script does nothing. Here we use a *Set Variable Data* step (see Set Variable Data on page 246)

since no functions need to be called outside the confines of Keyfactor Command, though you could use a *Custom PowerShell Script* step instead. Then an Update Certificate Subject\SANs for Microsoft CAs step is used to re-sign the request before it is submitted to the CA.
To create this, add Script Parameters to pull the DN and SANs into the script as shown in Metadata Update Example: Add Parameters on page 239 and add two static values to pass in your two domain names.

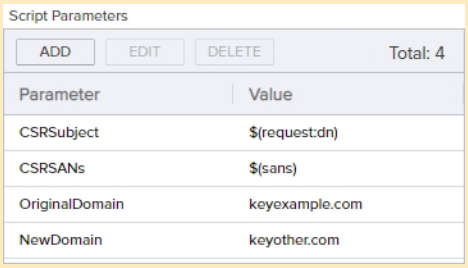


Figure 178: Update SANs and Subject Example: Add Parameters

In the *Insert PowerShell Script* field, enter a script similar to the following:

```
# Declare your parameters at the beginning
param(
   [string]$CSRSubject,
   [string]$CSRSANs,
   [string]$OriginalDomain,
   [string]$NewDomain
)

# Split the incoming SANs string into its component values
$SplitSANs = $CSRSANs.Split(',')

# Initialize variables for the two types of SANs we're handling
$DnsSANs = @()
$IpSANs = @()

# Add the incoming SANs to the correct list (assumes only IPv4 addresses or DNS SANs
will be encountered)
foreach($san in $SplitSANs){
   $sanComponents = $san.Trim() -split ":"
   Switch ($sanComponents[0].Trim()){
```

```
      "DnsName" {$DnsSANs += ,$sanComponents[1].Trim()}
      "IPAddress" {$IpSANs += $sanComponents[1].Trim()}
   }
}

# Load original SANs in UpdatedSANs for the else case
$UpdatedSANs = @{}

if(![string]::IsNullOrWhiteSpace($DnsSANs)) {
   $UpdatedSANs['dns'] = $DnsSANs
}

if(![string]::IsNullOrWhiteSpace($IpSANs)) {
   $UpdatedSANs['ip4'] = $IpSANs
}

# Load original subject in NewSubject for the else case
$NewSubject = $CSRSubject

# Replace escaped commas in the subject temporarily with a string to facilitate split-
ting
$TempString = "######"
$CleanSubject = $CSRSubject -replace "\\,", $TempString

# Split the incoming Subject string into its component values
$SplitSubject = $CleanSubject.Split(',')

# Initialize variables for the components of the subject
$SubjectCN = @()
$SubjectO = @()
$SubjectOU = @()
$SubjectL = @()
$SubjectST = @()
$SubjectC = @()
$SubjectE = @()

# Load subject values
foreach($element in $SplitSubject){
   $SplitElement = $element.Split('=')
```

```
   Switch($SplitElement[0]){
      "CN" {$SubjectCN = $SplitElement[1]}
      "O" {$SubjectO = $SplitElement[1]}
      "OU" {$SubjectOU = $SplitElement[1]}
      "E" {$SubjectE = $SplitElement[1]}
      "L"{$SubjectL = $SplitElement[1]}
      "ST"{$SubjectST = $SplitElement[1]}
      "C"{$SubjectC = $SplitElement[1]}
   }
}

# Check to see if the incoming CN ends with $OriginalDomain and, if so, add it as a SAN
with $NewDomain and update the Subject with $NewDomain (assumes non-null CN)
if ($SubjectCN.EndsWith($OriginalDomain))
{
   # Load just the portion of the CN without the domain name into a variable.
   $CNName = $SubjectCN.SubString(0,$SubjectCN.Length - ($OriginalDomain.Length + 1)) #
+1 to account for the '.'

   # Build new DNS SAN
   $NewSAN = $CNName + "." + $NewDomain

   # Add new SAN to DNS SANs
   $DnsSans += ,$NewSAN

   # Build new Subject with $NewDomain
   $NewSubject = "";

   if(![string]::IsNullOrWhiteSpace($SubjectCN)){
      $NewSubject += "CN=" + $CNName + "." + $NewDomain + ","
   }

   if(![string]::IsNullOrWhiteSpace($SubjectO)){
      $NewSubject += "O=" + $SubjectO + ","
   }

   if(![string]::IsNullOrWhiteSpace($SubjectOU)){
      $NewSubject += "OU=" + $SubjectOU + ","
   }
```

```
   if(![string]::IsNullOrWhiteSpace($SubjectL)){
      $NewSubject += "L=" + $SubjectL + ","
   }

   if(![string]::IsNullOrWhiteSpace($SubjectST)){
      $NewSubject += "ST=" + $SubjectST + ","
   }

   if(![string]::IsNullOrWhiteSpace($SubjectC)){
      $NewSubject += "C=" + $SubjectC + ","
   }

   if(![string]::IsNullOrWhiteSpace($SubjectE)){
      $NewSubject += "E=" + $SubjectE + ","
   }

   $NewSubject = $NewSubject.Remove($NewSubject.Length - 1) # remove the last ','

   # Replace temporary string with escaped commas in Subject
   $NewSubject = $NewSubject -replace $TempString, "\,"

   # Load the resulting IPv4 and updated DNS SANs into the SANs variable
   $UpdatedSANs = @{}

   if(![string]::IsNullOrWhiteSpace($DnsSANs)) {
      $UpdatedSANs['dns'] = $DnsSANs
   }

   if(![string]::IsNullOrWhiteSpace($IpSANs)) {
      $UpdatedSANs['ip4'] = $IpSANs
   }
}

# Return the updated subject and SANs as NewSubject and NewSANs to the workflow as a
hashtable
$result = @{ "Subject" = $NewSubject; "SANs" = $UpdatedSANs }
return $result
```

Add an Update Certificate Request Subject\SANs for Microsoft CAs step at a point in the workflow after your PowerShell step to allow the request to be re-signed before it is submitted to the Microsoft CA for enrollment.

Your enrollment will complete using the updated list of SANs, including any SANs you added manually on the PFX enrollment page or in the CSR, and the updated subject. You may reference the updated SANs using the standard SANs token ($(sans)) and updated subject using the standard DN token ($(request:dn)) in subsequent steps in your workflow and may view the subject and complete SAN list wherever the subject and SANs are available for viewing within Keyfactor Command.

Windows Enrollment Gateway - Populate from AD

This step is needed for any Keyfactor Windows Enrollment Gateway requests where the incoming template (the template from the client side) is configured to build the subject of the certificate request from Active Directory. It has no configuration parameters.

15. For Require Approval steps or custom steps requiring signals, in the Workflow Step Editor in the Signals section, select one or more security roles (see Security Overview on page 605) in the **Approval Status** dropdown. To narrow the list of security roles in the dropdown, begin typing a search string in the Search field. Click the erase icon ( ) to clear your selections.

    Users who hold the security role(s) selected here will be able to submit signals (e.g. approve requests) for this workflow.

    Tip: Signals represent data used at the point in the workflow step where the workflow needs to continue based on user input. Here, you're configuring which users are allowed to provide that input.

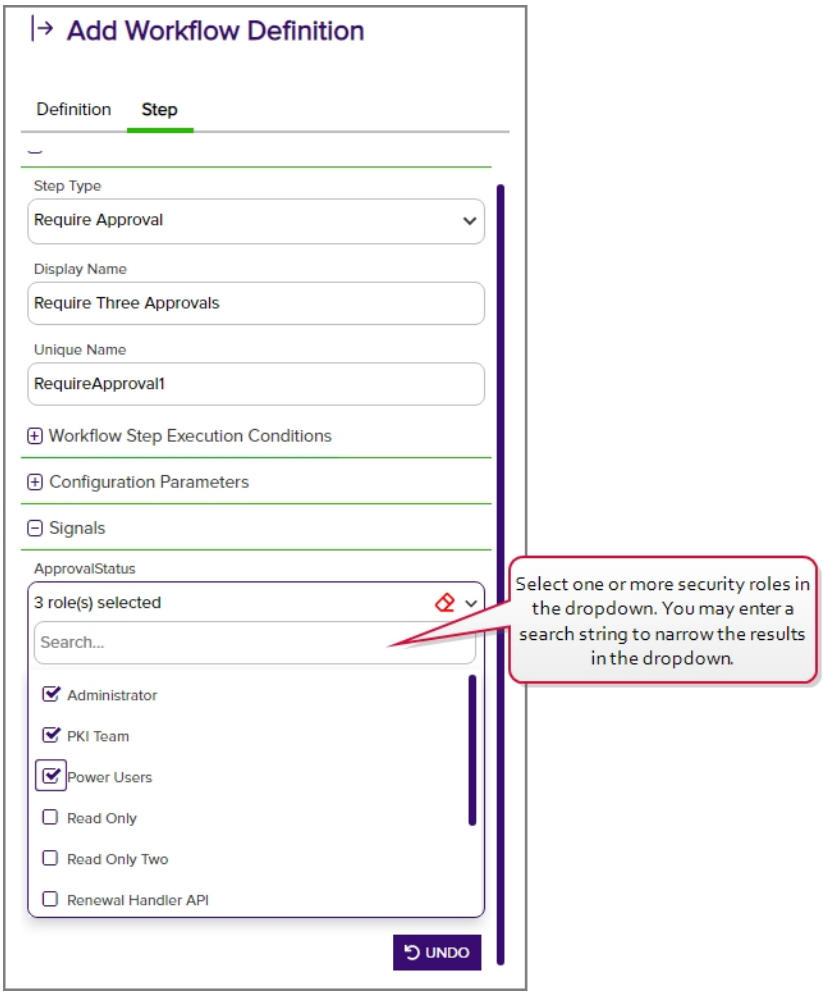


Figure 179: Signals Configuration for a Requires Approval Workflow Definition Step

Important: If all the security roles configured for a workflow step are deleted from Keyfactor Command, no users will be able to submit signals for workflow instances initiated with that workflow definition. To remedy this, update the workflow definition with one or more current security roles, re-publish it, and then restart any outstanding workflow instances.

16. Click **Save Workflow** at the top of the workflow workspace to save the workflow step.

17. On the Workflow Configuration page, click the plus button in between two workflow steps to add another step in the workflow or click **Save Workflow** to save the workflow with its current steps.

18. Before you can use the workflow, it must be published to activate it. Click the **Publish** button at the top of the workflow workspace to publish it immediately or return to the workflow definitions

page and publish it later, if desired (see Publishing a Workflow Definition below).

> **Tip:** Clicking **Publish** automatically saves the workflow.

19. To close the workflow workspace and return to the workflow definitions page, click the **Close** button at the top of the workflow workspace.

> **Note:** If you edit an existing *published* workflow definition, a new version of the workflow definition will be created. If you edit an existing workflow definition which has *never been published*, the existing configuration will be overwritten with the changes you've made—a new version will not be created.

An audit log entry is created when you add or edit a workflow definition (see Audit Log on page 652).

Deleting a Workflow Definition

> **Tip:** The following permissions (see Security Overview on page 605) are required to use this feature:
> Workflow Definitions: *Read*
> Workflow Definitions: *Modify*

To delete a workflow definition:

1. In the Management Portal, browse to *Workflow > Workflow Definitions*.
2. On the Workflow Definitions page, select a workflow definition and click **Delete** from either the top or right-click menu.
3. On the Confirm Operation alert, click **OK** to confirm or **Cancel** to cancel the operation.

> **Note:** The built-in global workflow definitions (*Global Revocation Workflow* and *Global Enrollment Workflow*) cannot be deleted. A workflow definition cannot be deleted if there is an active or suspended workflow instance for the workflow definition.

An audit log entry is created when you delete a workflow definition (see Audit Log on page 652).

Publishing a Workflow Definition

Workflow definitions are drafts that cannot be actively used until you take the step to publish them. This allows you to add new workflows or update existing ones without interrupting the flow of activity. Then, once the workflow definition is complete and ready for use, you can activate it. This can be done on the workflow workspace page while editing the workflow (see Adding or Modifying a Workflow Definition on page 223) or from the workflow definitions page.

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:
Workflow Definitions: *Read*
Workflow Definitions: *Modify*

To publish a workflow definition from the workflow definitions page:

1. In the Management Portal, browse to *Workflow > Workflow Definitions*.
2. On the Workflow Definitions page, select a workflow definition and click **Publish** from either the top or right-click menu.
3. On the Confirm Operation alert, click **OK** to confirm or **Cancel** to cancel the operation.

Importing or Exporting a Workflow Definition

You may wish to use the import and export functions to:

- Import a new workflow customized for you by the Keyfactor team.
- Export a workflow for backup purposes.
- Export a workflow that you've fully configured and which you need to replicate and then import under another name to create a duplicate of it.
- Export a previous version of a workflow and import it as the current version to revert to using the previous version.

Exporting a Workflow

Workflow definitions can be exported either from the workflow workspace page while viewing or editing the workflow (see Adding or Modifying a Workflow Definition on page 223) or from the workflow definitions page.

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:
Workflow Definitions: *Read*

To export a workflow definition from the workflow workspace:

1. In the Management Portal, browse to *Workflow > Workflow Definitions*.
2. On the Workflow Definitions page, click **Edit** from either the top or right click menu. This will open the workflow in the workflow workspace with the Workflow Definition dialog open on the right.
3. At the top of the workflow workspace, select a different **Version** of the workflow in the drop-down, if desired (see Workflow Versions on page 274).

4. At the top of the workflow workspace, click **Export**.
5. Browse to place the exported file on the local computer. The file will have an extension of .json.

To export a workflow definition from the workflow definitions page:

1. In the Management Portal, browse to *Workflow > Workflow Definitions*.
2. On the Workflow Definitions page, select a workflow definition and click **Export** from either the top or right-click menu.
3. In the Export Workflow Definition dialog, select a **Version** and click **Export**.

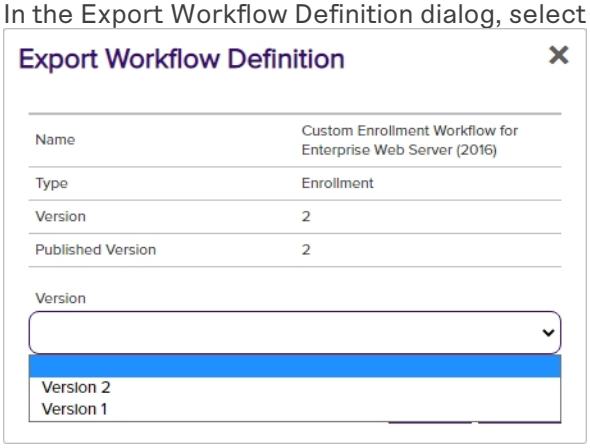


Figure 180: Export Workflow Definition

4. Browse to place the exported file on the local computer. The file will have an extension of .json.

Note: The following information is removed on export and will not be in the exported file:

- **Secrets**
  Some types of workflow steps include secret values (e.g. passwords). Secret values are not exported. If your workflow includes steps with secret values, these will need to be re-entered if you choose to import the exported file.
- **Roles for Signals**
  Some types of workflow steps make use of signals to allow users to provide input to the workflow midstream (e.g. provide approvals). This requires configuration of security roles that define who is allowed to provide this input. These security role values are not exported. You will need to set appropriate security roles on any workflow steps that use signals if you choose to import the exported file.

Importing a Workflow

Workflow definitions can be imported either to create a new workflow or to replace an existing workflow (e.g. to revert to a backup). When you import a workflow definition while editing an existing

workflow definition, it will overwrite any changes you have made to the existing workflow since the last time it was published. Previously published versions of the workflow—including the most recent—will be retained. This is useful in cases where you want to export a previous version of a workflow and reimport it to make it the currently active version.

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:
Workflow Definitions: *Read*
Workflow Definitions: *Modify*

To import a workflow definition:

1. In the Management Portal, browse to *Workflow > Workflow Definitions*.
2. On the Workflow Definitions page, click **Add** from the top menu to create a new workflow definition into which you will import, or **Edit** from either the top or right click menu, to import into an existing one to revert to a previous version. This will open the workflow in the workflow workspace with the Workflow Definition dialog open on the right.
3. At the top of the workflow workspace, click **Import**.
4. Browse to locate the workflow definition file you wish to import. Only files with an extension of *.json* will appear.

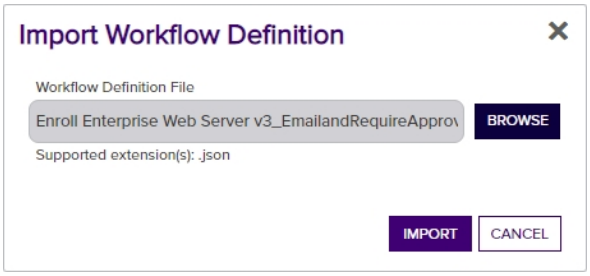


Figure 181: Browse to Locate a Workflow Definition to Import

Tip: In order to be successfully imported, the file must be correctly formatted JSON with at least *WorkflowType* and *Steps* properties. The maximum file upload size is 2 MB.

5. Click **Import** to import the workflow definition and populate it into the workflow workspace.
6. On the Confirm Operation alert, click **OK** to confirm or **Cancel** to cancel the operation.
7. In the workflow workspace, edit and save the workflow definition as needed as per Adding or Modifying a Workflow Definition on page 223. The following values will need attention:

- **Key (Template or Certificate Collection)**

  When the workflow definition is imported into a new workflow definition, the key is cleared. You will need to set an appropriate key (template for enrollment or revocation type workflows, certificate collection for workflows of type certificate entered or left collection) on the imported workflow definition before saving. The key is not cleared for imports into workflows with existing published versions.

  This is done both to support export of workflow definitions from one environment and import into another where the key set likely would be different and to support copying of workflow definitions, since you can't have two definitions for the same key.

- **Secrets**

  Some types of workflow steps include secret values (e.g. passwords). Secret values are not imported. If your workflow includes steps with secret values, these will need to be re-entered. This is true for imports into new workflow definitions and workflow definitions with existing published versions.

- **Roles for Signals**

  Some types of workflow steps make use of signals to allow users to provide input to the workflow midstream (e.g. provide approvals). This requires configuration of security roles that define who is allowed to provide this input. These security role values are not imported. You will need to set appropriate security roles on any workflow steps that use signals before saving. This is true for imports into new workflow definitions and workflow definitions with existing published versions.

  This is done to support export of workflow definitions from one environment and import into another where the security role set likely would be different.

Important: If you're importing a copy of a workflow definition that already exists in Keyfactor Command and you want to save it as a separate copy, be sure to change the **Name** of the workflow before saving the imported workflow to avoid overwriting the existing version of the workflow.

Workflow Versions

When you open a workflow definition for editing, you will see the version of the workflow shown at the upper left of the workflow workspace in a dropdown. By default, the current version will be shown.

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:
Workflow Definitions: *Read*

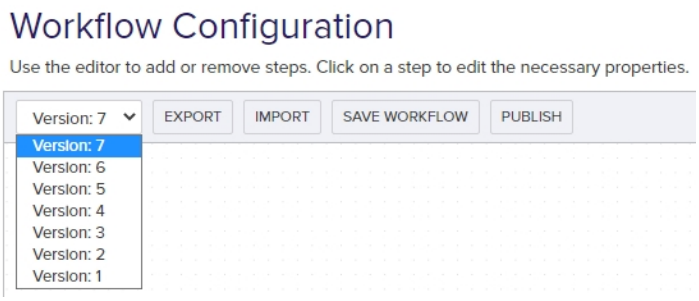


Figure 182: Workflow Definition Versions: View Current Version

When you have the current, most recent, version of the workflow loaded, you will see several options in the button bar at the top of the workflow workspace (if you have appropriate permissions) and the Add/Edit Workflow Definition Dialog will be active. If you select an older version in the dropdown, only the Version, Export, and Close options will appear on the workflow workspace button bar and the Add/Edit Workflow Definition Dialog will be read only.

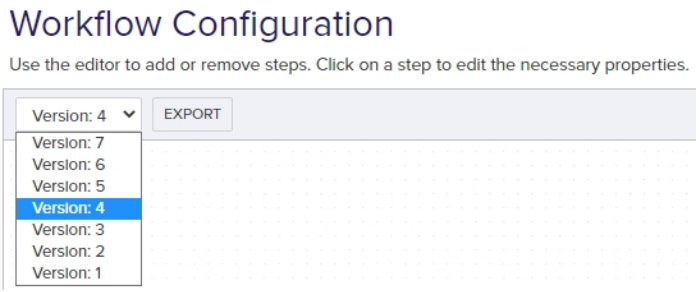


Figure 183: Workflow Definition Versions: View Previous Version

This option is designed to allow you to review previous versions of a workflow or export them as backups or to be re-imported to be used as a base for generating new workflows.

Refer to the following table for a list of the substitutable special text tokens that are available in the dropdown to customize workflow email messages.

Tip: In addition to these tokens, any data in the current data bucket can be referenced by entering an appropriate reference string. For example, to return the CSR for an enrollment request you can use **$(CSR)**. Refer to the *CurrentStateData* field in the response to the GET /Workflow/Instances/{instanceId} API method for information on all the data found in the current (as opposed to initial) data bucket (see GET Workflow Instances Instance ID in the *Keyfactor Web APIs Reference Guide*).

Table 13: Tokens for Workflow Definitions

Variable	Name	Request Type	Description
$(approvalsignalcmnts)	Workflow	Certificate	The comment provided when a workflow

Variable	Name	Request Type	Description
	Approval or Denial Comment	Collection, Enrollment and Revocation	request that requires approval is approved or denied.
$(CA)	Issuing CA	Certificate Collection, Enrollment and Revocation	A string containing the Issuing CA logical name and hostname.
$(certid)	Request ID	Certificate Collection and Revocation	The request ID for the certificate as stored in the Keyfactor Command database. This is not the same as the request ID issued by the CA.
$(cmnt)	Revocation Comment	Revocation	The comment entered at revocation time to explain the revocation.
$(code)	Revocation Reason	Revocation	The reason selected at revocation time to explain the revocation.
$(cn)	Common Name	Certificate Collection and Revocation	The certificate common name.
$(dn)	Distinguished Name	Certificate Collection and Revocation	The certificate distinguished name.
$(effdate)	Revocation Effective Date	Revocation	Date on which the revocation becomes effective.
$(issuerdn)	Issuer DN	Certificate Collection and Revocation	The distinguished name of the issuer of the certificate.
$(keysize)	Key Size	Certificate Collection and Revocation	The key size of the certificate.

Variable	Name	Request Type	Description
$(keytype)	Key Type	Certificate Collection and Revocation	The key type of the certificate.
$(locations)	Certificate Store Locations	Certificate Collection, Enrollment and Revocation	The certificate store locations to which the certificate will be deployed following enrollment, for enrollment requests, or in which the certificate is found, for revocation requests.
$(request:cn)	Requested Common Name	Enrollment	The common name contained in the certificate request.
$(request:dn)	Requested Distinguished Name	Enrollment	The distinguished name contained in the certificate request.
$(request:keysize)	Request Key Size	Enrollment	The key size contained in the certificate request.
$(request:keytype)	Request Key Type	Enrollment	The key type contained in the certificate request.
$(requester)	Requester	Enrollment and Revocation	The user account that requested the certificate from the CA, in the form *DOMAIN\username*.
$(requester:mail)	Requester's Email	Enrollment and Revocation	The email address retrieved from Active Directory of the user account that requested the certificate from the CA, if present.
$(requester:givenname)	Requester's First Name	Enrollment and Revocation	The first name retrieved from Active Directory of the user account that requested the certificate from the CA, if present.
$(requester:sn)	Requester's Last Name	Enrollment and Revocation	The last name retrieved from Active Directory of the user account that requested the certificate from the CA, if present.

Variable	Name	Request Type	Description
$(requester:displayname)	Requester's Display Name	Enrollment and Revocation	The display name retrieved from Active Directory of the user account that requested the certificate from the CA, if present.
$(reviewlink)	Review Link	Certificate Collection, Enrollment and Revocation	Link pointing to the review page in the Management Portal for the workflow instance where the person responsible for providing signal input (e.g. approving the request) can go to review the request and provide the input. **Note:** This option is only useful in workflows that contain a step that requires signal input (e.g. requires approval).
$(sans)	Subject Alternative Names	Enrollment	Subject alternative name(s) contained in the certificate request. There are four possible sources for the SANs that appear here: • For CSR enrollment, the original SANs included in the CSR. • Any SANs added through the Keyfactor Command Management Portal. For CSR enrollment, these take the place of the SANs in the CSR if the ATTRIBUTESUBJECTALTNAME2 option is enabled on the CA. See CSR Enrollment on page 131. • A SAN matching the CN added automatically during enrollment as a result of setting the RFC 2818 compliance flag in the CA configuration. See Adding or Modifying a CA Record on page 330. For PFX enrollment, the user has the option of editing this entry at

Variable	Name	Request Type	Description
			enrollment time; entry of something is required. • A SAN matching the CN added automatically by the Keyfactor Command policy module on the CA if the Keyfactor Command RFC 2818 Policy Handler is enabled, if one was not included in the CSR or added manually. See *Installing the Keyfactor CA Policy Module Handlers* in the *Keyfactor Command Server Installation Guide*.
$(serial)	Serial Numer	Certificate Collection and Revocation	Certificate serial number.
$(subdate)	Submission Date	Enrollment and Revocation	Date the workflow was initiated.
$(template)	Template Name	Certificate Collection and Enrollment	The short name (often the name with no spaces) of the certificate template used to create the certificate request.
$(thumbprint)	Thumbprint	Certificate Collection and Revocation	Thumbprint of the certificate.
$(metadata:Email-Contact)	Email-Contact	Certificate Collection, Enrollment and Revocation	Example of a custom metadata field.

Using the Workflow Definitions Search Feature

The search function allows you to query the database for information. The same query structure is used in multiple locations within the Keyfactor Command Management Portal.

When you first open the page, you will see the simple search option. To execute a search, select the field and comparison operators in the dropdowns and type something on which to search in the value field (if applicable). If you select an *is null* or *is not null* comparison operator, the value field will be grayed out. Click the **Search** button to execute the query.

Each query consists of three parts:

Query Field

The available fields for querying vary depending on the area of the Management Portal in which the search is used. On this page, the queries can be done on the following built-in fields:

Display Name

Complete or partial matches with the name of the workflow definition.

Id

The Keyfactor Command reference GUID for the workflow definition.

Is Published

The workflow has been published yes/no.

Workflow Type

The type of workflow (enrollment or revocation).

Comparison Operator

The query comparison operators vary depending on the type of field selected and the specific properties of the field. The list below shows the dropdown list comparison operators, as well as the equivalent query language syntax (in parentheses).

Most string fields (the vast majority of the built-in fields) support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Contains (-contains)
- Does not contain (-notcontains)
- Starts with (-startswith)
- Ends with (-endswith)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Most date and integer fields support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Is less than (-lt)
- Is less than or equal to (-le)
- Is greater than (-gt)
- Is greater than or equal to (-ge)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Most Boolean (true/false) fields support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Comparison Value

The value you enter for comparison must match the field type. For example, integer fields only support numerical values. String fields support all alphanumeric characters. Boolean fields only support True or False. The value field is not case sensitive. Date fields support only properly formatted dates and will initially display as mm/dd/yyyy. You can choose to populate the date field by:

- Clicking in a date Value field to open a pop-up calendar to select a date that will populate the field.
- Clicking in a segment of the date format (i.e., mm/dd/yyyy) and entering a value. As you continue to type in any one segment, the cursor will keep moving onto the next segment.

The results that match your search criteria will be displayed in the results grid below the search selection options.

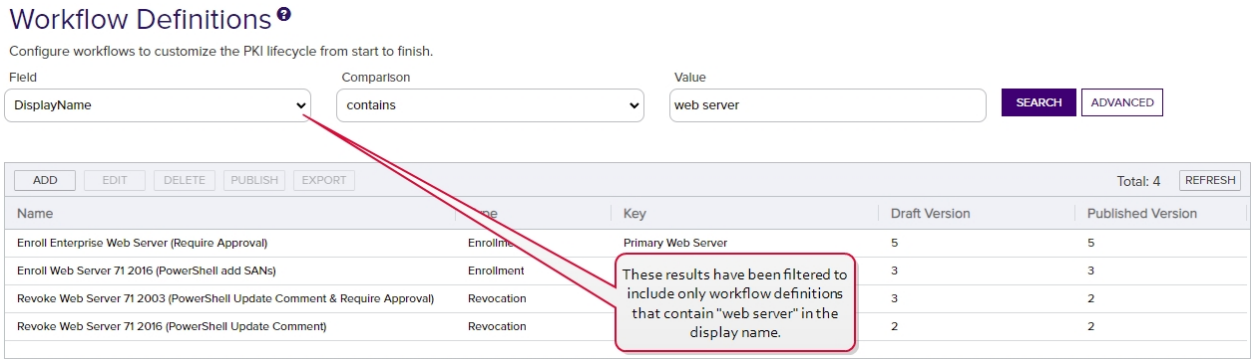


Figure 184: Simple Workflow Definitions Search

The search results can be sorted by clicking on a column header in the results grid for several of the columns. Click the column header again to reverse the sort order. The grid columns can be arranged in any order desired by click-holding and dragging the header of the column you wish to move. The column widths may be adjusted by click-holding and dragging the line separating two column headers.

Advanced Searches

On any search page you can click **Advanced** to the right of the Search button to display the advanced search options. Click **Simple** to close the advanced search options again.

Multiple Criteria

Using the advanced search options, you can build a query based on multiple criteria using AND/OR logic. As with a simple search, you select a field and comparison operator in the drop-downs and then enter a comparison value, if applicable. Click **Insert** to add the search criteria to the query field below the selection fields. Use the selection fields to build multiple search criteria. Each time you click the insert button, an AND is added between the previous search criteria and the newly added one. You can change the AND to an OR if desired. You can use parentheses around portions of the query along with AND/OR to change the query meaning.

For example, for certificate searches:

```
(CN -contains "appsrvr" AND IssuedDate -ge "01/01/2022") OR (CN -contains "appsrvr" AND
TemplateShortName -contains "web")
```

This query will return all the certificates issued on or after January 1, 2022 with the string appsrvr in the CN and also all certificates issued at any time with the string appsrvr in the CN using a template referencing web. When you have entered all the desired search criteria, click **Search** to execute the query. If you wish to clear the query field and start over, click the **Clear** button.

2.1.7.2 Workflow Instances

Whether you've chosen to create custom workflow definitions (see Workflow Definitions on page 218) or are relying on the built-in global workflow definitions, all certificate enrollments, renewals, and revocations go through workflow and create workflow instances. Certificate collection additions and removals only go through workflows if you create custom workflows for these actions, as there aren't built-in global workflows for these functions. The workflow instance is the combination of the certificate action and the workflow definition for that action as defined at the time that action took place.

Example: You have a custom enrollment workflow definition for the EnterpriseWebServer template. It contains a couple of steps including RequireApproval, which requires approval from at least two PKI admins before a certificate with this template may be issued. The workflow definition has been edited and published a few times and is now at version 3. John enrolls for a certificate using the Management Portal PFX Enrollment option and selects this template. When the enrollment completes, he receives a message indicating that the request is awaiting approval.

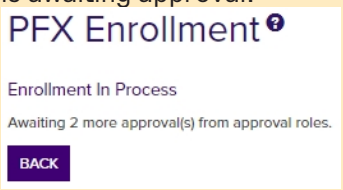


Figure 185: PFX Enrollment Complete for a Template Requiring Approval via Workflow

A workflow instance has now been created for his request. Users with appropriate permissions can view the instance in *Workflow Instances*.

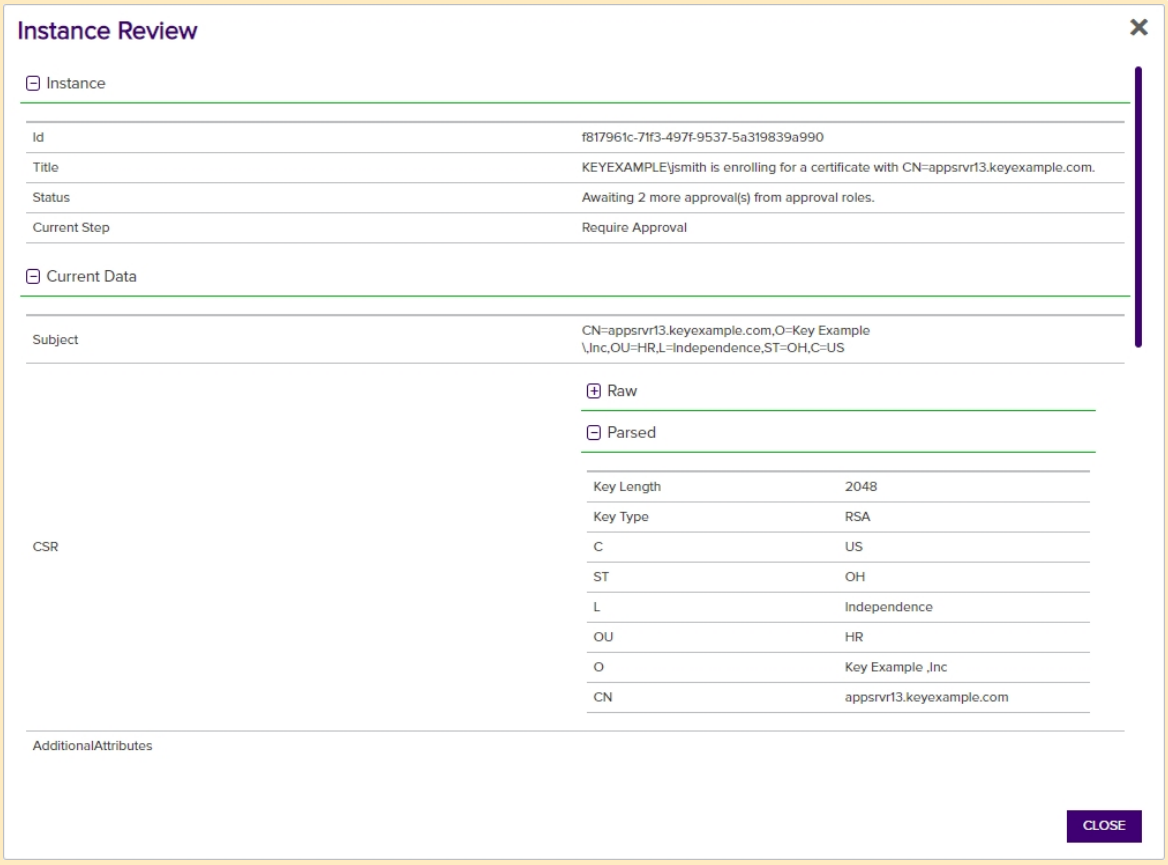


Figure 186: View Workflow Instance for a PFX Enrollment

Users with permissions to approve the request can do so through their *My Workflows* page and the *Assigned to Me* tab (see My Workflows on page 301).

After John completes his enrollment and before it is approved, an administrator makes a change to the workflow for the EnterpriseWebServer template and publishes the new version. The current workflow is now at version 4. However, John's request remains outstanding and valid with version 3 of the workflow. Any change made for version 4 of the template will not be reflected in John's request.

The only circumstance under which John's request might complete using version 4 of the workflow definition would be:

- If the administrator observed the suspended workflow (suspended because it is awaiting approvals), knew there was a new version of the workflow, and pro-actively restarted the workflow instance. A workflow instance restarted from a suspended state will always restart (from the beginning) with the currently active version of the workflow definition.
- If the administrator observed the suspended workflow, stopped the workflow knowing it should not be allowed to complete with the workflow definition it was submitted with, made

a further update to the workflow definition, and then restarted the workflow with the newly updated version of the workflow definition. One common reason to stop and restart rather than just restarting would be to allow time to make changes to the workflow.

- If the original request failed for some reason (e.g. the CA was not responding when the final approval was received and the request was submitted to the CA) and the administrator chose to restart the failed request with the currently active version of the workflow definition (the default) rather than the original version of the workflow after resolving the reason for the failure.

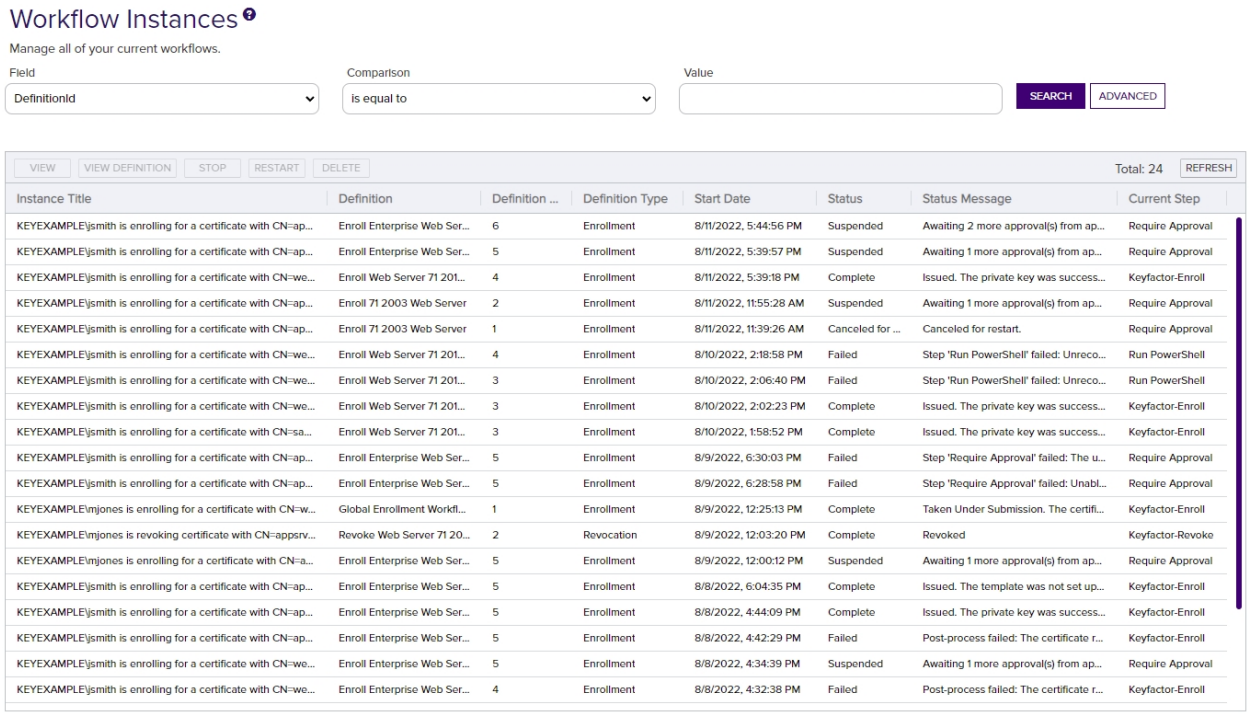


Figure 187: Workflow Instances

Tip: Click the help icon (?) next to the page title to open the embedded web copy of the *Keyfactor Command Documentation Suite* to this section.
You can also find the help icon at the top of the page next to the **Log Out** button. From here you can choose to open either the *Keyfactor Command Documentation Suite* at the home page or the *Keyfactor API Endpoint Utility*.

Workflow Instances Operations

A workflow instance is created for *every* certificate enrollment, renewal, or revocation request you make through the Keyfactor Command Management Portal. The addition and removal of certificates from certificate collections can be configured to flow through workflow as well, but these create workflow instances only if configured. If a given request is made using a workflow definition (see

Workflow Definitions on page 218) that has been configured with steps to require approvals for the request, run a PowerShell script, or make an API request as part of the request flow, you may find yourself on the Workflow Instances page needing to manage the instances.

Workflow instance operations include:

- Viewing a workflow instance to review details of the instance
- Viewing the workflow definition as configured for the particular workflow instance to understand the configuration at the time the instance was initiated
- Stopping a workflow instance
- Restarting a workflow instance after correcting a failure (e.g. the CA was not responding on an enrollment) or to introduce a different workflow definition
- Deleting workflow instances to clean house

Viewing a Workflow Instance

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:
Workflow Instances: *Read - All*

To view a workflow instance:

1. In the Management Portal, browse to *Workflow > Workflow Instances*.
2. On the Workflow Instances page, double-click or click **View** from either the top or right click menu.
3. The Instance Review dialog includes the following information:.

   Instance Section

   - **Id**

     A GUID indicating the Keyfactor Command reference ID for the instance.
   - **Title**

     A description for the action taking place in the step. For example:

     ```
     "KEYEXAMPLE\jsmith is enrolling for a certificate with
     CN=appsrvr12.keyexample.com."
     ```

     Or:

     ```
     "KEYEXAMPLE\mjones is revoking certificate with CN=appsrvr14.keyexample.com."
     ```

   - **Status**

     The current status message of the workflow instance.

     For example, for an enrollment that succeeded, the status message might be:

```
Issued. The private key was successfully retained.
```

For a workflow suspended and awaiting approval, the status message might be:

```
Awaiting 2 more approval(s) from approval roles.
```

For an enrollment that could not be submitted because a regular expression rule was not met, the status message might be something like:

```
Pre-process failed: Invalid ST provided: Value must be one of California, Washington,
Texas, New York, Illinois or Ohio.
```

For an enrollment that failed due to rejection by the CA, the status message might be:

```
The certificate request failed with the reason '[CA reason]'
```

A workflow that failed at a PowerShell step might include the PowerShell error in the status message:

```
Step 'Run PowerShell' failed: At line:5 char:19
+    [datetime]$Date
+                   ~
Missing ')' in function parameter list.
At line:7 char:1
+ )
+ ~
Unexpected token ')' in expression or statement.
```

- **Current Step**

  The display name defined for the workflow instance step at which the instance has paused or stopped. For a successfully completed enrollment or revocation workflow, this will be either *Keyfactor-Revoke* or *Keyfactor-Enroll*. For a suspended workflow, this will be the custom step that is awaiting user input to continue the workflow. For a failed workflow, this will be the step at which the workflow failed.

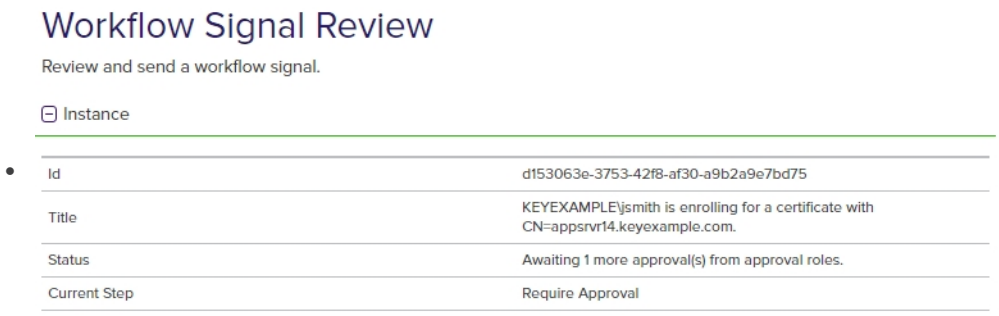


Figure 188: Workflow Instance Review

Current Data Section

The data included in this section will vary depending on the request type, the status of the request, and the configuration of the workflow.

Enrollment

For an enrollment, this section may include:

- Subject

  The distinguished name of the certificate.
- CSR:Raw

  The unparsed version of the certificate signing request generated for the certificate request.
- CSR: Parsed

  The parsed version of the certificate signing request generated for the certificate request. The CSR may include:
  - Key Length

    The desired key size for the certificate.
  - Key Type

    The desired key encryption for the certificate.
  - C

    The country (two characters) of the certificate.
  - ST

    The state or province of the certificate.
  - L

    The city or locality of the certificate.
  - OU

    The organizational unit of the certificate.

- O

  The organization of the certificate.

- E

  The email address of the certificate.

- CN

  The common name of the certificate.

- DNS Name

  A SAN value containing a DNS name.

- IP Address

  A SAN value containing an IP v4 or IP v6 address.

- RFC822 Name

  A SAN value containing an email address.

- Other name:Principal
  A SAN value containing a user principal name (UPN).

- Additional Attributes

  Values for any custom enrollment fields set on the certificate template to supply custom request attributes to the CA during the enrollment process.

- CA Certificate
  The certificate information returned from the CA for the certificate that is being requested, including:

  - CA Certificate ID

    The ID assigned to the certificate by the CA.

  - CA Request ID

    The ID assigned to the certificate request by the CA.

  - Status

    The numeric status for the certificate as returned by the CA.

  - Certificate Template

    The certificate template used to issue the certificate.

  - Revocation Date

    The revocation date for the certificate as returned by the CA, if applicable (generally not for newly enrolled certificates).

  - Revocation Reason

The revocation reason for the certificate as returned by the CA, if applicable (generally not for newly enrolled certificates).

- Archived Key

  A flag indicating whether the certificate is configured for key archival on the CA (true) or not (false).

Note: This field is populated only after the certificate has been issued by the CA.

- CA Certificate Data: Raw

  The certificate as returned by the CA in base-64 encoded binary format.
- CA Certificate Data: Parsed
  - Issued DN

    The distinguished name of the certificate.
  - Issuer DN

    The distinguished name of the issuer.
  - Thumbprint

    The thumbprint of the certificate.
  - Not After

    The date, in UTC, on which the certificate expires.
  - Not Before

    The date, in UTC, on which the certificate was issued by the certificate authority.
  - Metadata

    The metadata fields populated for the certificate.
- CA Certificate Request

  The certificate request information returned from the CA for the certificate that is being requested, including:
  - CA Request ID

    The ID assigned to the certificate request by the CA.
  - CSR

    The certificate signing request for the certificate request as returned by the CA.
  - Status

    The status for the certificate as returned by the CA.

- Requester Name

  The requester name on the certificate request as returned by the CA.

  Note: This field is populated only if the certificate request fails at the CA level or requires manager approval at the CA level.

- Certificate Authority

  The certificate authority that will be used to enroll against in *hostname\logical name* format.

- Custom Name

  A custom friendly name for the certificate, if entered at enrollment.

- Disposition Message

  A message about the certificate request.

  Note: This field is populated only after the certificate request has been submitted to the CA.

- Format

  The desired output format for the certificate. A value of STORE indicates that the certificate is intended to be delivered into one or more certificate stores.

- Include Chain

  A flag indicating whether to include the certificate chain in the enrollment response (true) or not (false).

- Initiating User Name

  The name of the user who initiated the workflow in DOMAIN\username format.

- Is PFX

  A flag indicating whether the certificate enrollment type that initiated the workflow instance was PFX (true) or CSR (false).

- Issuer DN

  The distinguished name of the issuer.

- Key Retention

  A flag indicating whether the private key for the certificate resulting from the enrollment will be retained in Keyfactor Command (true) or not (false).

- Key Status

A numeric value indicating the status of the private key retention for the certificate within Keyfactor Command. Possible values are:

    - 0—Unknown
    - 1—Saved
    - 2—Expected
    - 3—NoRetention
    - 4—Failure
    - 5—Temporary

- Keyfactor Id

  The Keyfactor Command reference ID for the certificate.

- Management Job Time

  The schedule for the management job to add the certificate to any certificate store(s).

- Metadata

  Values for the metadata fields that will be associated with the certificate once it is in Keyfactor Command.

- PFX Password Secret Instance Id

  The Keyfactor Command reference ID for the PFX password used to secure the PFX file on download.

- Private Key Converter

  An internally used Keyfactor Command field.

- Renewal Certificate

    - Certificate Id

      The Keyfactor Command reference ID of the certificate this certificate replaces on a renewal.

- Renewal Certificate Data: Raw

  The certificate that this certificate replaces on a renewal as returned by the CA in base-64 encoded binary format.

- Renewal Certificate Data: Parsed

  The certificate details for the certificate that this certificate replaces on a renewal, including:

    - Issued DN

      The distinguished name of the certificate.

    - Issuer DN

The distinguished name of the issuer.

- Thumbprint

  The thumbprint of the certificate.

- Not After

  The date, in UTC, on which the certificate expires.

- Not Before

  The date, in UTC, on which the certificate was issued by the certificate authority.

- Metadata

  The metadata fields populated for the certificate.

- SANs: Type

  The subject alternate names defined for the certificate. Possible types that can be entered within Keyfactor Command are DNS Name, IPv4 Address, IPv6 Address, User Principal Name, and Email. Within each type is a list of entries for that type shown with a key name of the entry number and the actual value. For example, if you had two DNS SANs, the DNS Name section would look something like:

  ```
  Entry 1: myfirstsan.keyexample.com
  Entry 2: mysecondsan.keyexample.com
  ```

- Serial Number

  The serial number of the certificate.

- Stores

  The certificate stores to which the certificate should be distributed, if applicable.

- Template

  The template that was used when requesting the certificate.

- Thumbprint

  The thumbprint of the certificate.

- (Custom)

  Optional user-generated custom fields returning response data from PowerShell scripts or REST requests. These will be sorted alphabetically in among the other fields on the page.

Revocation

For a revocation, this section may include:

- Certificate Authority

  The certificate authority that that issued the certificate.
- Certificate Id

  The Keyfactor Command reference ID for the certificate being revoked.
- Comment

  A freeform reason or comment to explain why the certificate is being revoked.
- Delegate

  A flag indicating whether delegation was enabled for the certificate authority that issued the certificate at the time revocation was requested (true) or not (false). For more information, see Authorization Methods Tab on page 341.
- Effective Date

  The date and time when the certificate will be revoked.
- Initiating User Name

  The name of the user who initiated the workflow in DOMAIN\\username format.
- Operation Start

  The time at which the revocation workflow was initiated.
- RevokeCode

  The specific reason that the certificate is being revoked. Possible values are:
  - -1—Remove from Hold
  - 0—Unspecified
  - 1—Key Compromised
  - 2—CA Compromised
  - 3—Affiliation Changed
  - 4—Superseded
  - 5—Cessation of Operation
  - 6—Certificate Hold
  - 7—Remove from CRL. Only valid in the case that a cert is already on a CRL in a manner that it can be removed, such as Certificate Hold.
- Serial Number

  The serial number of the certificate being revoked.
- Thumbprint

  The thumbprint of the certificate being revoked.
- (Custom)

Optional user-generated custom fields returning response data from PowerShell scripts or REST requests. These will be sorted alphabetically in among the other fields on the page.

Certificate Entered Collection and Certificate Left Collection

For a certificate that entered or left a certificate collection, this section generally includes:

- Certificate Id

  The Keyfactor Command reference ID for the certificate added to or removed from the certificate collection.

- Initiating User Name

  The name of the user who initiated the workflow—generally *Timer Service* in this case.

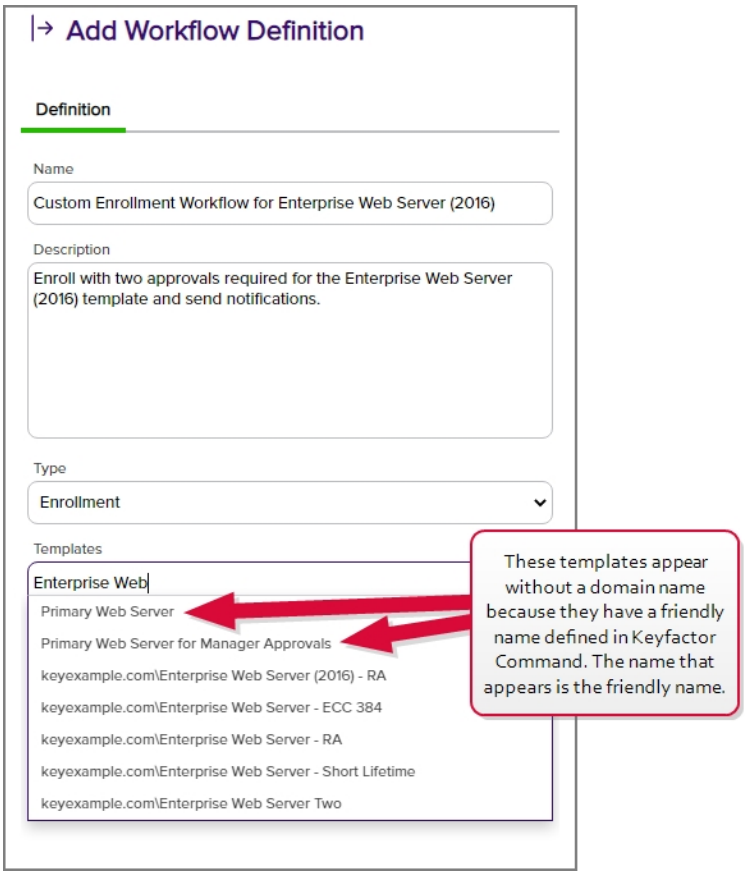


Figure 189: View a Workflow Instance

4. Click **Close** to close the viewer.

Viewing a Workflow Instance Definition

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:
Workflow Instances: *Read - All*
Workflow Definitions: *Read*

The workflow definition as it existed at the time a particular workflow instance was generated may not necessarily match the current workflow definition. Using the Workflow Definition option on the Workflow Instances page, you can view the workflow definition for the selected instance as it was at the time the instance was initiated using the workflow workspace.

To view a workflow instance definition:

1. In the Management Portal, browse to *Workflow > Workflow Instances*.
2. On the Workflow Instances page, select a workflow instance and click **View Definition** from either the top or right-click menu.
3. A read-only copy of the workflow definition at the time the instance was initiated will open in the workflow definition workspace. For information about using the workflow definition workspace, see Adding or Modifying a Workflow Definition on page 223.

Stopping a Workflow Instance

If a workflow instance has been initiated in error or with a workflow definition that is not configured correctly, you have the option to stop the workflow instance.

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:
Workflow Instances: *Read - All*
Workflow Instances: *Manage*

To stop a workflow instance:

1. In the Management Portal, browse to *Workflow > Workflow Instances*.
2. On the Workflow Instances page, select a workflow instance and click **Stop** from either the top or right-click menu.
3. On the Confirm Operation alert, click **OK** to confirm or **Cancel** to cancel the operation.

Note: Only workflow instances with a Status of *Suspended* can be stopped.

Restarting a Workflow Instance

If a workflow instance has failed or been stopped to correct an issue, you may restart it to reinitialize the request after correcting whatever issue caused the failure (e.g. a PowerShell script failed or a

CA was not responding on enrollment). You may also choose to use restart if a workflow instance was initiated with a workflow definition that had an incorrect definition that can easily be corrected—for example, the definition requires approval from just one user and that user is no longer available. In this case, you can update the definition, republish it, and then restart the workflow with the latest published version.

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:
Workflow Instances: *Read - All*
Workflow Instances: *Manage*
Workflow Definitions: *Read*

When you restart a workflow instance, it starts over from the beginning, not from the failure point.

To restart a workflow instance:

1. In the Management Portal, browse to *Workflow > Workflow Instances*.
2. On the Workflow Instances page, select a workflow instance and click **Restart** from either the top or right-click menu.
3. On the Confirm Operation alert, click **OK** to confirm or **Cancel** to cancel the operation.

Note: Only workflow instances with a Status of *Failed* or *Suspended* can be restarted.

After restarting a workflow instance, you can view any differences between the original instance and the newly restarted instance by looking at the audit log record (see Audit Log Operations on page 657) for the workflow instance restart. The Related Entries in the audit log record do not include the original workflow instance that failed since restarting a workflow instance generates a new workflow instance.

Tip: If user John Smith restarts a workflow instance that was originally started by user Martha Jones, the audit log message for this will look something like:

```
"The user 'KEYEXAMPLE\jsmith' restarted workflow instance, 'KEYEXAMPLE\mjones is
enrolling for a certificate with CN=appsrvr12.keyexample.com.'"
```

In a scenario like this, the user listed at the top of the audit log details will be the user who restarted the instance, not the user who originally started the request.

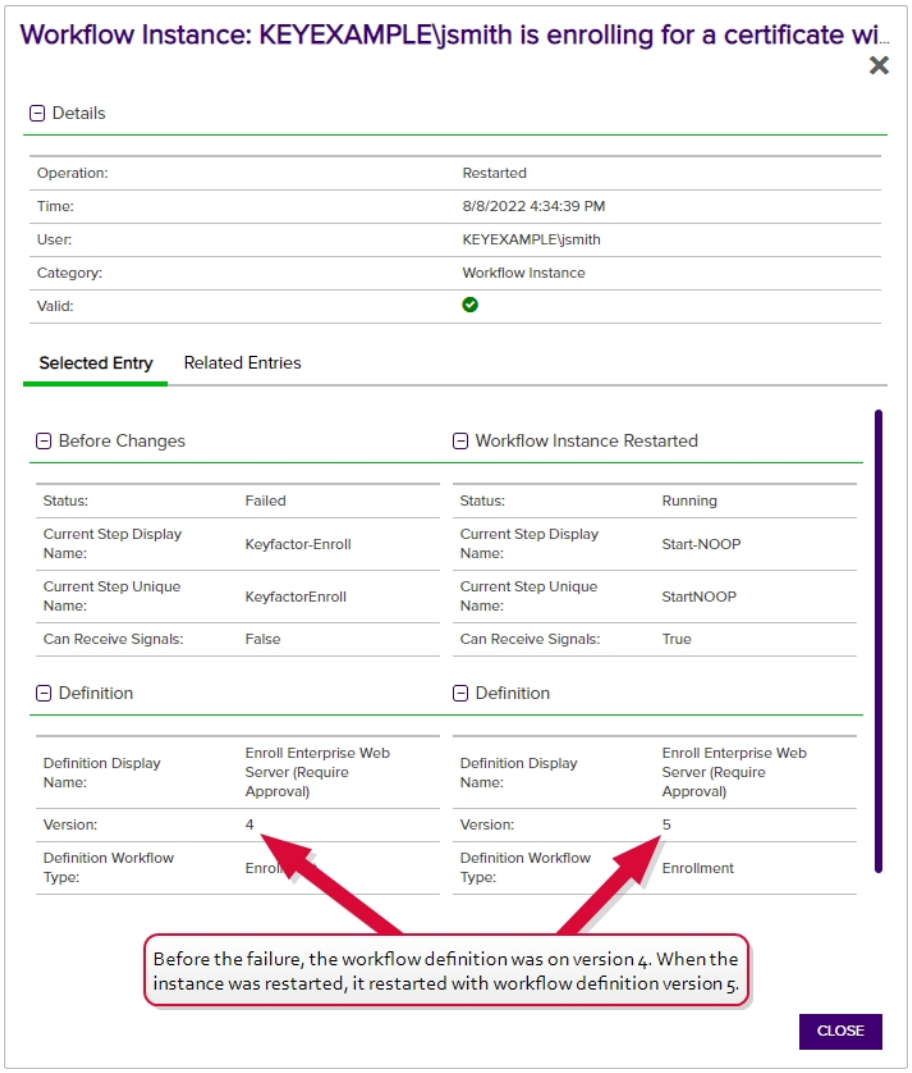


Figure 190: View an Audit Log Entry for a Restarted Workflow Instance

Deleting a Workflow Instance

If a workflow instance has failed, you may wish to remove the failed instance from the grid.

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:
Workflow Instances: *Read - All*
Workflow Instances: *Manage*

To delete a workflow instance:

1. In the Management Portal, browse to *Workflow > Workflow Instances*.
2. On the Workflow Instances page, select a workflow instance and click **Delete** from either the top or right-click menu.
3. On the Confirm Operation alert, click **OK** to confirm or **Cancel** to cancel the operation.

An audit log entry is created when you delete a workflow instance (see Audit Log on page 652). Instances deleted as the result of system action (e.g. purging old records) are not audited.

Using the Workflow Instances Search Feature

The search function allows you to query the database for information. The same query structure is used in multiple locations within the Keyfactor Command Management Portal.

When you first open the page, you will see the simple search option. To execute a search, select the field and comparison operators in the dropdowns and type something on which to search in the value field (if applicable). If you select an *is null* or *is not null* comparison operator, the value field will be grayed out. Click the **Search** button to execute the query.

Each query consists of three parts:

Query Field

The available fields for querying vary depending on the area of the Management Portal in which the search is used. On this page, the queries can be done on the following built-in fields:

DefinitionId

The Keyfactor Command reference GUID for the workflow *definition*.

Id

The Keyfactor Command reference GUID for the workflow *instance*.

Initiating User Name

Complete or partial matches with the name of the user who initiated the workflow instance in domain\username format.

Last Modified

The date and time on which an initiated instance was last updated. The instance is updated each time a step in the workflow is completed, when signals are received for a step that accepts signals (e.g. a requires approval step), or when an instance is stopped or restarted.

Start Date

The date and time when an instance was initiated.

Status

Status matches or doesn't match the selected value—Unknown, Running, Suspended, Failed, Complete, Rejected, CanceledforRestart

Title

Complete or partial matches with the description for the action taking place in the workflow instance step. The values in the title will vary and generally include the user initiating the request and the CN of the certificate or certificate request involved.

Workflow Type

The type of workflow (enrollment or revocation).

Comparison Operator

The query comparison operators vary depending on the type of field selected and the specific properties of the field. The list below shows the dropdown list comparison operators, as well as the equivalent query language syntax (in parentheses).

Most string fields (the vast majority of the built-in fields) support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Contains (-contains)
- Does not contain (-notcontains)
- Starts with (-startswith)
- Ends with (-endswith)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Most date and integer fields support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Is less than (-lt)
- Is less than or equal to (-le)
- Is greater than (-gt)
- Is greater than or equal to (-ge)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Most Boolean (true/false) fields support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Comparison Value

The value you enter for comparison must match the field type. For example, integer fields only support numerical values. String fields support all alphanumeric characters. Boolean fields only support True or False. The value field is not case sensitive. Date fields support only properly formatted dates and will initially display as mm/dd/yyyy. You can choose to populate the date field by:

- Clicking in a date Value field to open a pop-up calendar to select a date that will populate the field.
- Clicking in a segment of the date format (i.e., mm/dd/yyyy) and entering a value. As you continue to type in any one segment, the cursor will keep moving onto the next segment.

The results that match your search criteria will be displayed in the results grid below the search selection options.

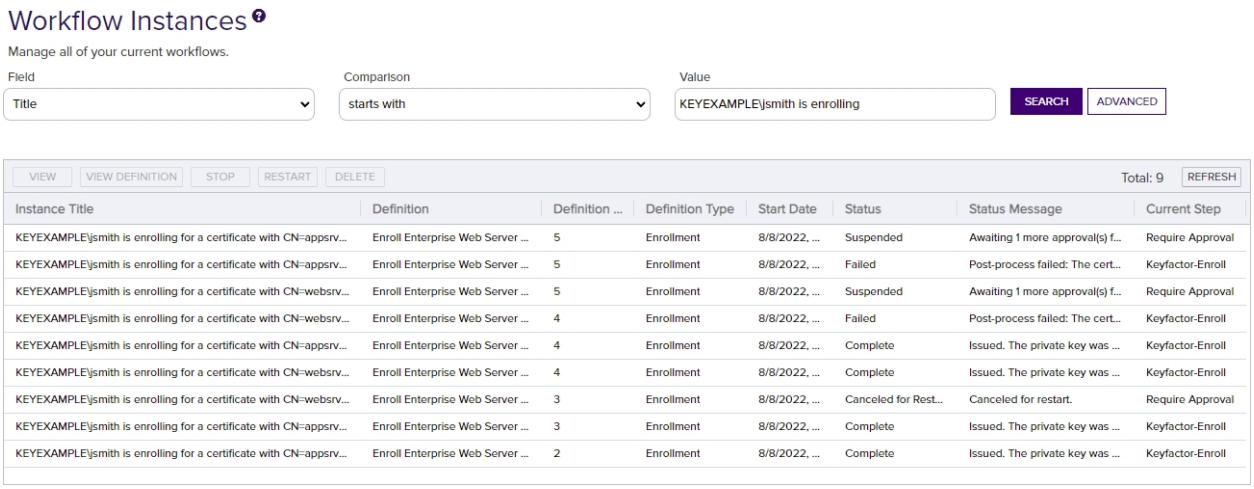


Figure 191: Simple Workflow Instance Search

The search results can be sorted by clicking on a column header in the results grid for several of the columns. Click the column header again to reverse the sort order. The grid columns can be arranged in any order desired by click-holding and dragging the header of the column you wish to move. The column widths may be adjusted by click-holding and dragging the line separating two column headers.

Advanced Searches

On any search page you can click **Advanced** to the right of the Search button to display the advanced search options. Click **Simple** to close the advanced search options again.

Multiple Criteria

Using the advanced search options, you can build a query based on multiple criteria using AND/OR logic. As with a simple search, you select a field and comparison operator in the drop-downs and then enter a comparison value, if applicable. Click **Insert** to add the search criteria to the query field below the selection fields. Use the selection fields to build multiple search criteria. Each time you click the insert button, an AND is added between the previous search criteria and the newly added one. You can change the AND to an OR if desired. You can use parentheses around portions of the query along with AND/OR to change the query meaning.

For example, for certificate searches:

```
(CN -contains "appsrvr" AND IssuedDate -ge "01/01/2022") OR (CN -contains "appsrvr" AND
TemplateShortName -contains "web")
```

This query will return all the certificates issued on or after January 1, 2022 with the string appsrvr in the CN and also all certificates issued at any time with the string appsrvr in the CN using a template referencing web. When you have entered all the desired search criteria, click **Search** to execute the query. If you wish to clear the query field and start over, click the **Clear** button.

2.1.7.3 My Workflows

When a workflow is initiated by a certificate enrollment, renewal, revocation request, or automated task (for workflows of types Certificate Entered Collection and Certificate left Collection), that workflow instance may appear in as many as two places:

- If the workflow definition for the instance requires signal input (e.g. approval), every Keyfactor Command user who holds a security role that has been defined in the workflow definition as allowed to send signals to the workflow (see Workflow Definitions on page 218) will see that instance appear on the *Assigned to Me* tab of the My Workflows page. The users can provide signal input (e.g. approve or deny the request) from here. The workflow does not necessarily need to receive signal input from all these users, depending on how many users with this role there are and how many users were required to provide signal input in the workflow definition. Once the workflow instance is complete, it disappears from the *Assigned to Me* tab for all users.
- The user who initiated the workflow (e.g. by beginning a certificate enrollment or revoking a certificate) will see that instance appear on the *Created by Me* tab of the My Workflows page. When the workflow instance is complete, it will still appear on the *Created by Me* tab and be searchable.

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:
Workflow Instances: *Read - All* OR
Workflow Instances: *Read - Assigned To Me* OR
Workflow Instances: *Read - Started By Me*

Users with only *Read - Started By Me* or *Read - Assigned To Me* will only be able to see the *Created by Me* or *Assigned to Me* tab, respectively. A user with either both *Read - Started By Me* and *Read - Assigned To Me* or *Read - All* will be able to see both tabs.

Example: The enrollment workflow definition for the *EnterpriseWebServer* template requires two approvals from users with the *Enrollment Approvers* security role. There are five users with this role: Anne, Charles, John, Mary, and Sam. Martha enrolls for a certificate using the Keyfactor Command Management Portal PFX Enrollment method and the *EnterpriseWebServer* template.

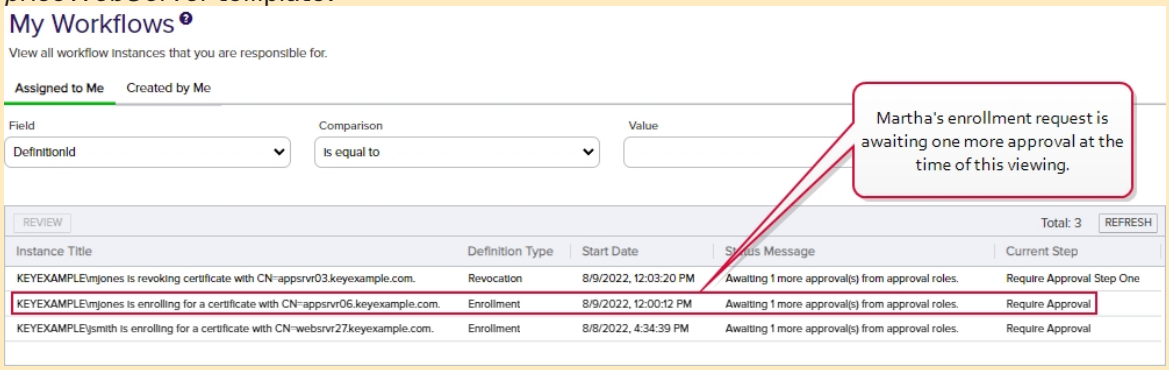


Figure 192: Workflows Assigned to Mary

The new workflow instance appears on the *Assigned to Me* tab of all users with the *Enrollment Approvers* role and on Martha's *Created by Me* tab. Approvers Mary and John approve the instance on their respective *Assigned to Me* tab and the certificate is issued. The workflow instance disappears from the *Assigned to Me* tab for all users. It's still visible on the main *Workflow Instances* page and on Martha's *Created by Me* tab as a completed instance.

Note: A locking conflict may occur if two (or more) users attempt to provide input to a workflow instance (e.g. approve a request) at exactly the same time. If this happens, input from only one of the users will be reflected in the Management Portal, and the workflow instance will not be moved along to the next step if it should have been with input from the two users. The other input is still accepted, however, and there is a scheduled task that runs daily and attempts to continue all suspended workflows that may be eligible to continue but have not done so due to locking conflicts.

Tip: Click the help icon (?) next to the page title to open the embedded web copy of the *Keyfactor Command Documentation Suite* to this section.
You can also find the help icon at the top of the page next to the **Log Out** button. From here you can choose to open either the *Keyfactor Command Documentation Suite* at the home page or the *Keyfactor API Endpoint Utility*.

Workflows Assigned to Me Operations

Only workflow instances that are in a Suspended state and that the current user has permissions to submit signals for (e.g. approve or deny) appear on the Assigned to Me tab of the My Workflows page. Once the user submits a signal to a workflow instance on this page, it is removed from the page.

Note: If a workflow instance is initiated for a workflow definition that has more than one step requiring input (signals), a user can only provide that input (e.g. approve or deny a require approval request) at the step in the workflow instance where the workflow instance was suspended pending input. The user cannot jump ahead and provide input for future steps in the workflow that have not yet occurred.

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:
Workflow Instances: *Read - Assigned to Me*
Or:
Workflow Instances: *Read - All*

To review a workflow instance and potentially submit a signal for it:

1. In the Management Portal, browse to *Workflow > My Workflows*.
2. On the Assigned to Me tab of the My Workflows page, double-click or click **Review** from either the top or right click menu.
3. On the Workflow Signal Review page, review the information in the instance before submitting a signal for the request. Information on the review page includes:

   Instance Section

   - **Id**

     A GUID indicating the Keyfactor Command reference ID for the instance.
   - **Title**

     A description for the action taking place in the step. For example:

     ```
     "KEYEXAMPLE\jsmith is enrolling for a certificate with
     CN=appsrvr12.keyexample.com."
     ```

     Or:

     ```
     "KEYEXAMPLE\mjones is revoking certificate with CN=appsrvr14.keyexample.com."
     ```

   - **Status**

     The current status message of the workflow instance.

     For a workflow suspended and awaiting approval, the status message might be:

     ```
     Awaiting 2 more approval(s) from approval roles.
     ```

   - **Current Step**

     The display name defined for the workflow instance step at which the instance has paused. For a suspended workflow, this will be the custom step that is awaiting user input to continue the workflow.

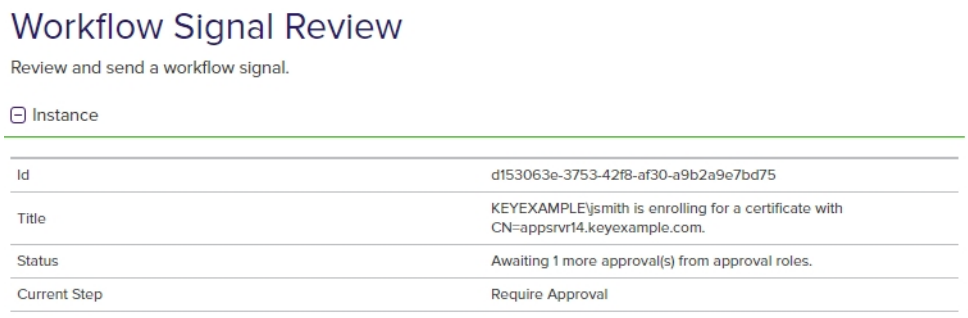
   

   Figure 193: Workflow Instance Review

   Current Data Section

The data included in this section will vary depending on the request type and the configuration of the workflow.

Enrollment

For an enrollment, this section may include:

- Subject

  The distinguished name of the certificate.
- CSR:Raw

  The unparsed version of the certificate signing request generated for the certificate request.
- CSR: Parsed

  The parsed version of the certificate signing request generated for the certificate request. The CSR may include:
  - Key Length

    The desired key size for the certificate.
  - Key Type

    The desired key encryption for the certificate.
  - C

    The country (two characters) of the certificate.
  - ST

    The state or province of the certificate.
  - L

    The city or locality of the certificate.
  - OU

    The organizational unit of the certificate.
  - O

    The organization of the certificate.
  - E

    The email address of the certificate.
  - CN

    The common name of the certificate.
  - DNS Name

    A SAN value containing a DNS name.
  - IP Address

    A SAN value containing an IP v4 or IP v6 address.

- RFC822 Name

  A SAN value containing an email address.

- Other name:Principal
  A SAN value containing a user principal name (UPN).

- Additional Attributes

  Values for any custom enrollment fields set on the certificate template to supply custom request attributes to the CA during the enrollment process.

- Certificate Authority

  The certificate authority that will be used to enroll against in *hostname\logical name* format.

- Custom Name

  A custom friendly name for the certificate, if entered at enrollment.

- Format

  The desired output format for the certificate. A value of STORE indicates that the certificate is intended to be delivered into one or more certificate stores.

- Include Chain

  A flag indicating whether to include the certificate chain in the enrollment response (true) or not (false).

- Initiating User Name

  The name of the user who initiated the workflow in DOMAIN\username format.

- Is PFX

  A flag indicating whether the certificate enrollment type that initiated the workflow instance was PFX (true) or CSR (false).

- Key Retention

  A flag indicating whether the private key for the certificate resulting from the enrollment will be retained in Keyfactor Command (true) or not (false).

- Management Job Time

  The schedule for the management job to add the certificate to any certificate store(s).

- Metadata

  Values for the metadata fields that will be associated with the certificate once it is in Keyfactor Command.

- PFX Password Secret Instance Id

  The Keyfactor Command reference ID for the PFX password used to secure the PFX file on download.

- Renewal Certificate

- Certificate Id

  The Keyfactor Command reference ID of the certificate this certificate replaces on a renewal.

- Renewal Certificate Data: Raw

  The certificate that this certificate replaces on a renewal as returned by the CA in base-64 encoded binary format.

- Renewal Certificate Data: Parsed

  The certificate details for the certificate that this certificate replaces on a renewal, including:

  - Issued DN

    The distinguished name of the certificate.

  - Issuer DN

    The distinguished name of the issuer.

  - Thumbprint

    The thumbprint of the certificate.

  - Not After

    The date, in UTC, on which the certificate expires.

  - Not Before

    The date, in UTC, on which the certificate was issued by the certificate authority.

  - Metadata

    The metadata fields populated for the certificate.

- SANs: Type

  The subject alternate names defined for the certificate. Possible types that can be entered within Keyfactor Command are DNS Name, IPv4 Address, IPv6 Address, User Principal Name, and Email. Within each type is a list of entries for that type shown with a key name of the entry number and the actual value. For example, if you had two DNS SANs, the DNS Name section would look something like:

  ```
  Entry 1: myfirstsan.keyexample.com
  Entry 2: mysecondsan.keyexample.com
  ```

- Stores

  The certificate stores to which the certificate should be distributed, if applicable.

- Template

  The template that was used when requesting the certificate.

- (Custom)

  Optional user-generated custom fields returning response data from PowerShell scripts or REST requests. These will be sorted alphabetically in among the other fields on the page.

Revocation

For a revocation, this section may include:

- Certificate Authority

  The certificate authority that that issued the certificate.
- Certificate Id

  The Keyfactor Command reference ID for the certificate being revoked.
- Comment

  A freeform reason or comment to explain why the certificate is being revoked.
- Delegate

  A flag indicating whether delegation was enabled for the certificate authority that issued the certificate at the time revocation was requested (true) or not (false). For more information, see Authorization Methods Tab on page 341.
- Effective Date

  The date and time when the certificate will be revoked.
- Initiating User Name

  The name of the user who initiated the workflow in DOMAIN\\username format.
- Operation Start

  The time at which the revocation workflow was initiated.
- RevokeCode

  The specific reason that the certificate is being revoked. Possible values are:
  - -1—Remove from Hold
  - 0—Unspecified
  - 1—Key Compromised
  - 2—CA Compromised
  - 3—Affiliation Changed
  - 4—Superseded
  - 5—Cessation of Operation
  - 6—Certificate Hold
  - 7—Remove from CRL. Only valid in the case that a cert is already on a CRL in a manner that it can be removed, such as Certificate Hold.

- Serial Number

  The serial number of the certificate being revoked.
- Thumbprint

  The thumbprint of the certificate being revoked.
- (Custom)

  Optional user-generated custom fields returning response data from PowerShell scripts or REST requests. These will be sorted alphabetically in among the other fields on the page.

Certificate Entered Collection and Certificate Left Collection

For a certificate that entered or left a certificate collection, this section generally includes:

- Certificate Id

  The Keyfactor Command reference ID for the certificate added to or removed from the certificate collection.
- Initiating User Name

  The name of the user who initiated the workflow—generally *Timer Service* in this case.

Signal Input

In the Signal Input section of the page, you can submit one or more signals for the step. For the built-in require approval workflow step type, this is where you send an approval or denial for the request along with a comment about the approval or denial.

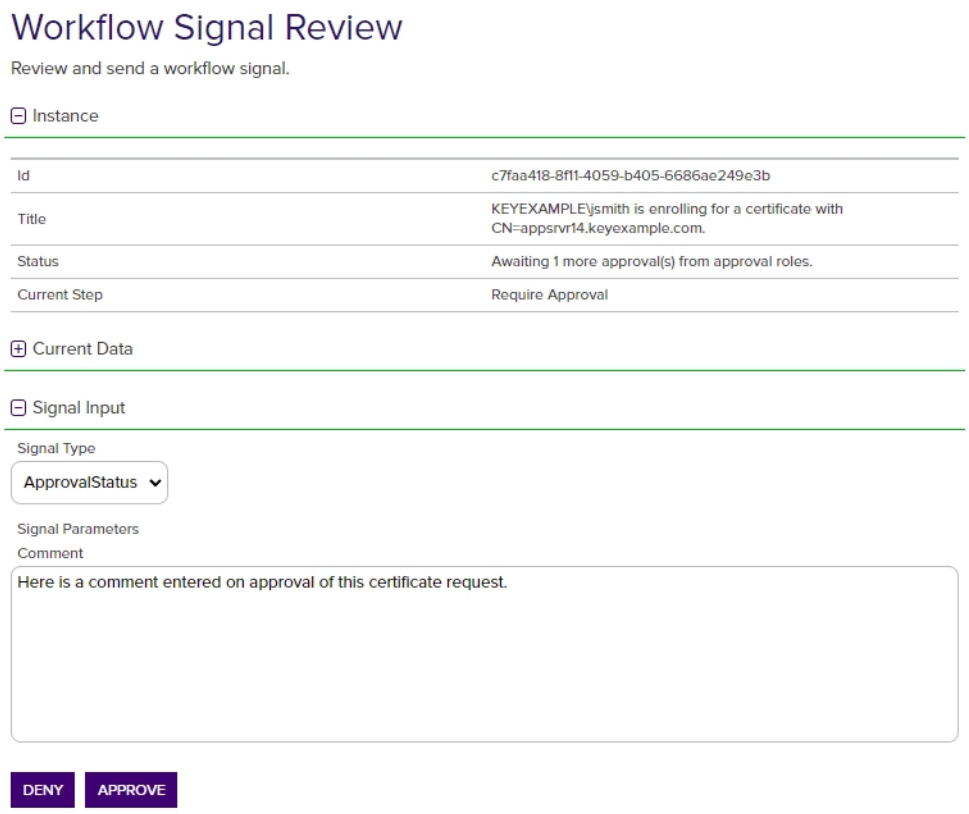


Figure 194: Approve or Deny a Workflow Instance

A custom workflow step requiring signal input may have more than one signal type to select from in the dropdown, may have input fields to submit data with the signal, and will likely have buttons with labels other than *Deny* or *Approve*.

4. At the bottom of the Workflow Signal Review page in the Signal Input section, select an option in the Signal Type dropdown, enter any required signal data, and click an appropriate signal button to submit the signal. For the built-in require approval workflow step type, select *ApprovalStatus* in the dropdown (there is only one choice), enter an optional **Comment** (the maximum comment length is 500 characters), and click either **Approve** to add your approval to the workflow or **Deny** to deny the workflow instance.

> **Tip:** If you reference the approve/deny comments using the $(approvalsignalcmnts) token, the included comments will vary depending on where you use the token. If you use the token in an email message within a require approval step, only comments from that require approval step will be included. If you use the token in a separate email step within the same workflow, all comments from any require approval steps within the workflow will be included.

Important: Comments entered when approving or denying a built-in require approval workflow step can be included in emails delivered either as part of the require approval step or in subsequent steps within the workflow, but they are not retained for future reference. If you would like to retain them for future reference, use a workflow step that copies the comment(s) to a metadata field (see Use Custom PowerShell on page 253).

5. On the Confirm Operation alert, click **OK** to confirm or **Cancel** to cancel the operation.

Note: The workflow definition may require more than one approval to be completed and so may not be immediately completed when you click Approve. However, a single denial is enough to reject the workflow instance.

An audit log entry is created when you provide input to a workflow instance (see Audit Log on page 652).

Using the Workflow Assigned to Me Search Feature

The search function allows you to query the database for information. The same query structure is used in multiple locations within the Keyfactor Command Management Portal.

When you first open the page, you will see the simple search option. To execute a search, select the field and comparison operators in the dropdowns and type something on which to search in the value field (if applicable). If you select an *is null* or *is not null* comparison operator, the value field will be grayed out. Click the **Search** button to execute the query.

Each query consists of three parts:

Query Field

The available fields for querying vary depending on the area of the Management Portal in which the search is used. On this page, the queries can be done on the following built-in fields:

Definition Id	Start Date
Complete or partial matches with the Keyfactor Command reference GUID of the workflow *definition*.	The date and time when an instance was initiated.
Id	Status
Complete or partial matches with the Keyfactor Command reference GUID of the workflow *instance*.	Status matches or doesn't match the selected value—Unknown, Running, Suspended, Failed, Complete, Rejected, CanceledforRestart
Initiating User Name	Title
Complete or partial matches with the name of the user who initiated the workflow instance in domain\username format.	Complete or partial matches with the description for the action taking place in the workflow instance step. The values in the title will vary and generally

include the user initiating the request and the CN of the certificate or certificate request involved.

Last Modified

The date and time on which an initiated instance was last updated. The instance is updated each time a step in the workflow is completed, when signals are received for a step that accepts signals (e.g. a requires approval step), or when an instance is stopped or restarted.

Workflow Type

The type of workflow (enrollment or revocation).

Comparison Operator

The query comparison operators vary depending on the type of field selected and the specific properties of the field. The list below shows the dropdown list comparison operators, as well as the equivalent query language syntax (in parentheses).

Most string fields (the vast majority of the built-in fields) support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Contains (-contains)
- Does not contain (-notcontains)
- Starts with (-startswith)
- Ends with (-endswith)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Most date and integer fields support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Is less than (-lt)
- Is less than or equal to (-le)
- Is greater than (-gt)
- Is greater than or equal to (-ge)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Most Boolean (true/false) fields support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Comparison Value

The value you enter for comparison must match the field type. For example, integer fields only support numerical values. String fields support all alphanumeric characters. Boolean fields only support True or False. The value field is not case sensitive. Date fields support only properly formatted dates and will initially display as mm/dd/yyyy. You can choose to populate the date field by:

- Clicking in a date Value field to open a pop-up calendar to select a date that will populate the field.

- Clicking in a segment of the date format (i.e., mm/dd/yyyy) and entering a value. As you continue to type in any one segment, the cursor will keep moving onto the next segment.

The results that match your search criteria will be displayed in the results grid below the search selection options.

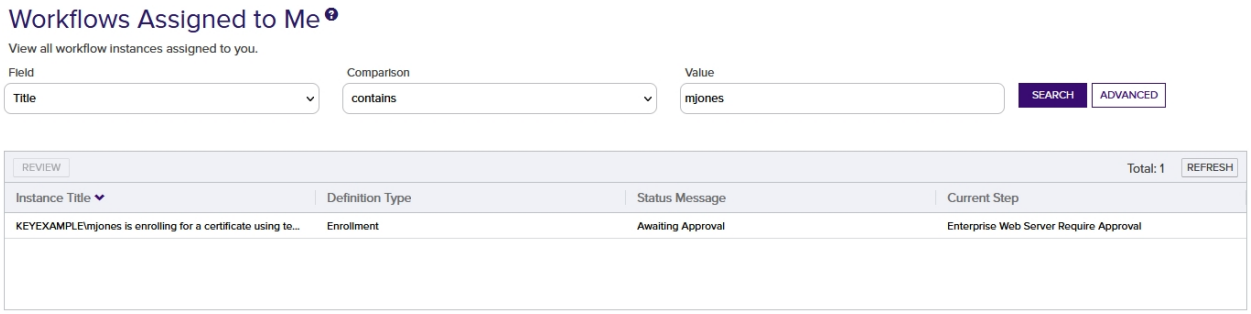


Figure 195: Simple Workflows Assigned to Me Search

The search results can be sorted by clicking on a column header in the results grid. Only the Instance Title column sortable. Click the column header again to reverse the sort order. The grid columns can be arranged in any order desired by click-holding and dragging the header of the column you wish to move. The column widths may be adjusted by click-holding and dragging the line separating two column headers.

Advanced Searches

On any search page you can click **Advanced** to the right of the Search button to display the advanced search options. Click **Simple** to close the advanced search options again.

Multiple Criteria

Using the advanced search options, you can build a query based on multiple criteria using AND/OR logic. As with a simple search, you select a field and comparison operator in the drop-downs and then enter a comparison value, if applicable. Click **Insert** to add the search criteria to the query field below the selection fields. Use the selection fields to build multiple search criteria. Each time you click the insert button, an AND is added between the previous search criteria and the newly added one. You can change the AND to an OR if desired. You can use parentheses around portions of the query along with AND/OR to change the query meaning.

For example, for certificate searches:

```
(CN -contains "appsrvr" AND IssuedDate -ge "01/01/2022") OR (CN -contains "appsrvr" AND
TemplateShortName -contains "web")
```

This query will return all the certificates issued on or after January 1, 2022 with the string appsrvr in the CN and also all certificates issued at any time with the string appsrvr in the CN using a template referencing web. When you have entered all the desired search criteria, click **Search** to execute the query. If you wish to clear the query field and start over, click the **Clear** button.

Workflows Created by Me Operations

On the Created by Me tab of the My Workflows page you can view all the workflows that the current user initiated.

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:
Workflow Instances: *Read - Started by Me*
Or:
Workflow Instances: *Read - All*

To view details of a workflow instance:

1. In the Management Portal, browse to *Workflow > My Workflows*.
2. On the Created by Me tab of the My Workflows page, double-click or click **View** from either the top or right click menu.
3. On the Workflow Signal Review page, review the information in the instance. Information on the review page includes:

   Instance Section

   - **Id**

     A GUID indicating the Keyfactor Command reference ID for the instance.
   - **Title**

     A description for the action taking place in the step. For example:

     ```
     "KEYEXAMPLE\jsmith is enrolling for a certificate with
     CN=appsrvr12.keyexample.com."
     ```

     Or:

     ```
     "KEYEXAMPLE\mjones is revoking certificate with CN=appsrvr14.keyexample.com."
     ```

   - **Status**

     The current status message of the workflow instance.

     For example, for an enrollment that succeeded, the status message might be:

     ```
     Issued. The private key was successfully retained.
     ```

     For a workflow suspended and awaiting approval, the status message might be:

     ```
     Awaiting 2 more approval(s) from approval roles.
     ```

For an enrollment that could not be submitted because a regular expression rule was not met, the status message might be something like:

```
Pre-process failed: Invalid ST provided: Value must be one of California, Washington,
Texas, New York, Illinois or Ohio.
```

For an enrollment that failed due to rejection by the CA, the status message might be:

```
The certificate request failed with the reason '[CA reason]'
```

A workflow that failed at a PowerShell step might include the PowerShell error in the status message:

```
Step 'Run PowerShell' failed: At line:5 char:19
+    [datetime]$Date
+                   ~
Missing ')' in function parameter list.
At line:7 char:1
+ )
+ ~
Unexpected token ')' in expression or statement.
```

- **Current Step**

  The display name defined for the workflow instance step at which the instance has paused or stopped. For a successfully completed enrollment or revocation workflow, this will be either *Keyfactor-Revoke* or *Keyfactor-Enroll*. For a suspended workflow, this will be the custom step that is awaiting user input to continue the workflow. For a failed workflow, this will be the step at which the workflow failed.

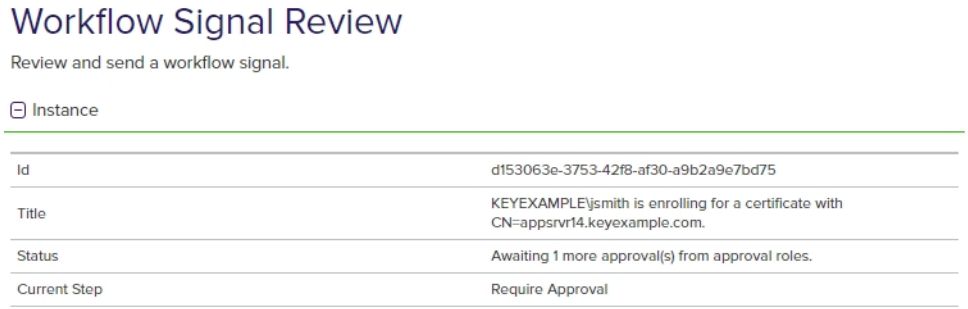


Figure 196: Workflow Instance Review

Current Data Section

The data included in this section will vary depending on the request type, the status of the request, and the configuration of the workflow.

Enrollment

For an enrollment, this section may include:

- Subject

  The distinguished name of the certificate.
- CSR:Raw

  The unparsed version of the certificate signing request generated for the certificate request.
- CSR: Parsed

  The parsed version of the certificate signing request generated for the certificate request. The CSR may include:
  - Key Length

    The desired key size for the certificate.
  - Key Type

    The desired key encryption for the certificate.
  - C

    The country (two characters) of the certificate.
  - ST

    The state or province of the certificate.
  - L

    The city or locality of the certificate.
  - OU

    The organizational unit of the certificate.
  - O

    The organization of the certificate.
  - E

    The email address of the certificate.
  - CN

    The common name of the certificate.
  - DNS Name

    A SAN value containing a DNS name.
  - IP Address

    A SAN value containing an IP v4 or IP v6 address.

- RFC822 Name

  A SAN value containing an email address.

- Other name:Principal
  A SAN value containing a user principal name (UPN).

- Additional Attributes

  Values for any custom enrollment fields set on the certificate template to supply custom request attributes to the CA during the enrollment process.

- CA Certificate
  The certificate information returned from the CA for the certificate that is being requested, including:

  - CA Certificate ID

    The ID assigned to the certificate by the CA.

  - CA Request ID

    The ID assigned to the certificate request by the CA.

  - Status

    The numeric status for the certificate as returned by the CA.

  - Certificate Template

    The certificate template used to issue the certificate.

  - Revocation Date

    The revocation date for the certificate as returned by the CA, if applicable (generally not for newly enrolled certificates).

  - Revocation Reason

    The revocation reason for the certificate as returned by the CA, if applicable (generally not for newly enrolled certificates).

  - Archived Key

    A flag indicating whether the certificate is configured for key archival on the CA (true) or not (false).

  Note: This field is populated only after the certificate has been issued by the CA.

- CA Certificate Data: Raw

  The certificate as returned by the CA in base-64 encoded binary format.

- CA Certificate Data: Parsed

  - Issued DN

    The distinguished name of the certificate.

- Issuer DN

  The distinguished name of the issuer.
- Thumbprint

  The thumbprint of the certificate.
- Not After

  The date, in UTC, on which the certificate expires.
- Not Before

  The date, in UTC, on which the certificate was issued by the certificate authority.
- Metadata

  The metadata fields populated for the certificate.

- CA Certificate Request

  The certificate request information returned from the CA for the certificate that is being requested, including:
  - CA Request ID

    The ID assigned to the certificate request by the CA.
  - CSR

    The certificate signing request for the certificate request as returned by the CA.
  - Status

    The status for the certificate as returned by the CA.
  - Requester Name

    The requester name on the certificate request as returned by the CA.

  Note: This field is populated only if the certificate request fails at the CA level or requires manager approval at the CA level.

- Certificate Authority

  The certificate authority that will be used to enroll against in *hostname\logical name* format.
- Custom Name

  A custom friendly name for the certificate, if entered at enrollment.
- Disposition Message

  A message about the certificate request.

Note: This field is populated only after the certificate request has been submitted to the CA.

- Format

  The desired output format for the certificate. A value of STORE indicates that the certificate is intended to be delivered into one or more certificate stores.

- Include Chain

  A flag indicating whether to include the certificate chain in the enrollment response (true) or not (false).

- Initiating User Name

  The name of the user who initiated the workflow in DOMAIN\username format.

- Is PFX

  A flag indicating whether the certificate enrollment type that initiated the workflow instance was PFX (true) or CSR (false).

- Issuer DN

  The distinguished name of the issuer.

- Key Retention

  A flag indicating whether the private key for the certificate resulting from the enrollment will be retained in Keyfactor Command (true) or not (false).

- Key Status

  A numeric value indicating the status of the private key retention for the certificate within Keyfactor Command. Possible values are:

  - 0—Unknown
  - 1—Saved
  - 2—Expected
  - 3—NoRetention
  - 4—Failure
  - 5—Temporary

- Keyfactor Id

  The Keyfactor Command reference ID for the certificate.

- Management Job Time

  The schedule for the management job to add the certificate to any certificate store(s).

- Metadata

Values for the metadata fields that will be associated with the certificate once it is in Keyfactor Command.

- PFX Password Secret Instance Id

  The Keyfactor Command reference ID for the PFX password used to secure the PFX file on download.

- Private Key Converter

  An internally used Keyfactor Command field.

- Renewal Certificate
  - Certificate Id

    The Keyfactor Command reference ID of the certificate this certificate replaces on a renewal.

- Renewal Certificate Data: Raw

  The certificate that this certificate replaces on a renewal as returned by the CA in base-64 encoded binary format.

- Renewal Certificate Data: Parsed

  The certificate details for the certificate that this certificate replaces on a renewal, including:
  - Issued DN

    The distinguished name of the certificate.
  - Issuer DN

    The distinguished name of the issuer.
  - Thumbprint

    The thumbprint of the certificate.
  - Not After

    The date, in UTC, on which the certificate expires.
  - Not Before

    The date, in UTC, on which the certificate was issued by the certificate authority.
  - Metadata

    The metadata fields populated for the certificate.

- SANs: Type

  The subject alternate names defined for the certificate. Possible types that can be entered within Keyfactor Command are DNS Name, IPv4 Address, IPv6 Address, User Principal Name, and Email. Within each type is a list of entries for that type shown with a key name of the entry number and the actual value. For example, if you had two DNS SANs, the DNS Name section would look something like:

```
Entry 1: myfirstsan.keyexample.com
Entry 2: mysecondsan.keyexample.com
```

- Serial Number

  The serial number of the certificate.
- Stores

  The certificate stores to which the certificate should be distributed, if applicable.
- Template

  The template that was used when requesting the certificate.
- Thumbprint

  The thumbprint of the certificate.
- (Custom)

  Optional user-generated custom fields returning response data from PowerShell scripts or REST requests. These will be sorted alphabetically in among the other fields on the page.

Revocation

For a revocation, this section may include:

- Certificate Authority

  The certificate authority that that issued the certificate.
- Certificate Id

  The Keyfactor Command reference ID for the certificate being revoked.
- Comment

  A freeform reason or comment to explain why the certificate is being revoked.
- Delegate

  A flag indicating whether delegation was enabled for the certificate authority that issued the certificate at the time revocation was requested (true) or not (false). For more information, see Authorization Methods Tab on page 341.
- Effective Date

  The date and time when the certificate will be revoked.
- Initiating User Name

  The name of the user who initiated the workflow in DOMAIN\\username format.
- Operation Start

  The time at which the revocation workflow was initiated.
- RevokeCode

The specific reason that the certificate is being revoked. Possible values are:

- -1—Remove from Hold
- 0—Unspecified
- 1—Key Compromised
- 2—CA Compromised
- 3—Affiliation Changed
- 4—Superseded
- 5—Cessation of Operation
- 6—Certificate Hold
- 7—Remove from CRL. Only valid in the case that a cert is already on a CRL in a manner that it can be removed, such as Certificate Hold.

- Serial Number

  The serial number of the certificate being revoked.

- Thumbprint

  The thumbprint of the certificate being revoked.

- (Custom)

  Optional user-generated custom fields returning response data from PowerShell scripts or REST requests. These will be sorted alphabetically in among the other fields on the page.

Certificate Entered Collection and Certificate Left Collection

For a certificate that entered or left a certificate collection, this section generally includes:

- Certificate Id

  The Keyfactor Command reference ID for the certificate added to or removed from the certificate collection.

- Initiating User Name

  The name of the user who initiated the workflow—generally *Timer Service* in this case.

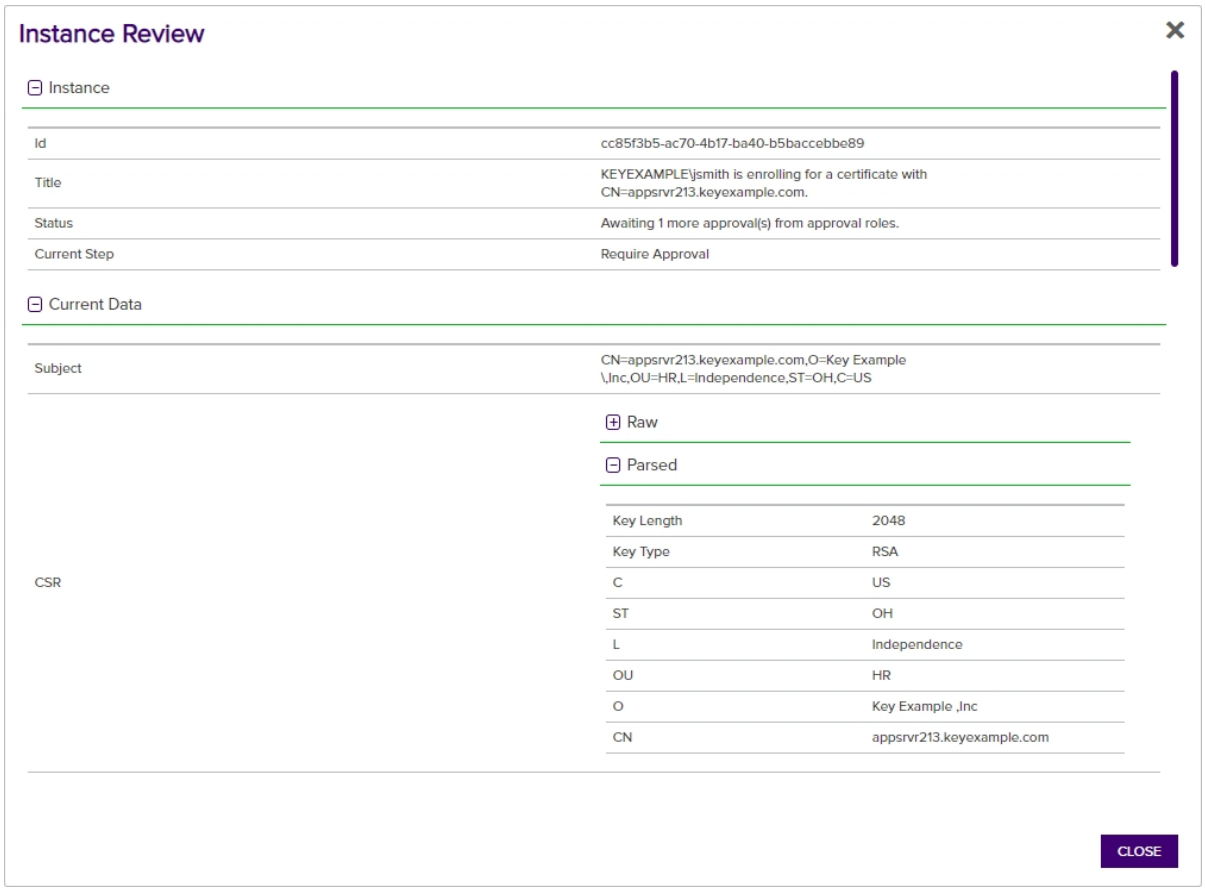


Figure 197: View Details for the Workflow Instance

4. Click **Close** to close the viewer.

Using the Workflow Created by Me Search Feature

The search function allows you to query the database for information. The same query structure is used in multiple locations within the Keyfactor Command Management Portal.

When you first open the page, you will see the simple search option. To execute a search, select the field and comparison operators in the dropdowns and type something on which to search in the value field (if applicable). If you select an *is null* or *is not null* comparison operator, the value field will be grayed out. Click the **Search** button to execute the query.

Each query consists of three parts:

Query Field

The available fields for querying vary depending on the area of the Management Portal in which the search is used. On this page, the queries can be done on the following built-in fields:

Definition Id

Complete or partial matches with the Keyfactor Command reference GUID of the workflow *definition*.

Id

Complete or partial matches with the Keyfactor Command reference GUID of the workflow *instance*.

Initiating User Name

Complete or partial matches with the name of the user who initiated the workflow instance in domain\username format.

Last Modified

The date and time on which an initiated instance was last updated. The instance is updated each time a step in the workflow is completed, when signals are received for a step that accepts signals (e.g. a requires approval step), or when an instance is stopped or restarted.

Start Date

The date and time when an instance was initiated.

Status

Status matches or doesn't match the selected value—Unknown, Running, Suspended, Failed, Complete, Rejected, CanceledforRestart

Title

Complete or partial matches with the description for the action taking place in the workflow instance step. The values in the title will vary and generally include the user initiating the request and the CN of the certificate or certificate request involved.

Workflow Type

The type of workflow (enrollment or revocation).

Comparison Operator

The query comparison operators vary depending on the type of field selected and the specific properties of the field. The list below shows the dropdown list comparison operators, as well as the equivalent query language syntax (in parentheses).

Most string fields (the vast majority of the built-in fields) support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Contains (-contains)
- Does not contain (-notcontains)
- Starts with (-startswith)
- Ends with (-endswith)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Most date and integer fields support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Is less than (-lt)
- Is less than or equal to (-le)
- Is greater than (-gt)
- Is greater than or equal to (-ge)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Most Boolean (true/false) fields support:

- Is equal to (-eq)
- Is null (-eq NULL)

- Is not equal to (-ne)
- Is not null (-ne NULL)

Comparison Value

The value you enter for comparison must match the field type. For example, integer fields only support numerical values. String fields support all alphanumeric characters. Boolean fields only support True or False. The value field is not case sensitive. Date fields support only properly formatted dates and will initially display as mm/dd/yyyy. You can choose to populate the date field by:

- Clicking in a date Value field to open a pop-up calendar to select a date that will populate the field.
- Clicking in a segment of the date format (i.e., mm/dd/yyyy) and entering a value. As you continue to type in any one segment, the cursor will keep moving onto the next segment.

The results that match your search criteria will be displayed in the results grid below the search selection options.

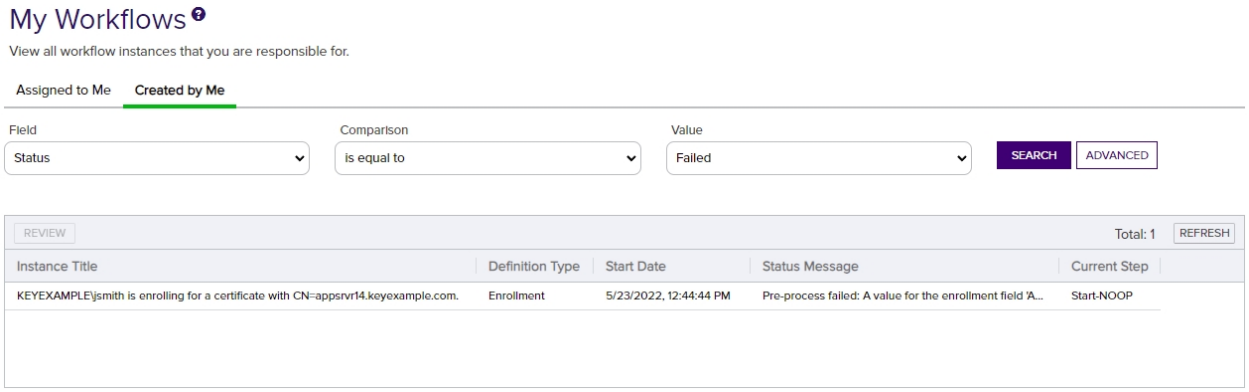


Figure 198: Simple Workflows Created by Me Search

The search results can be sorted by clicking on a column header in the results grid. Only the Instance Title column sortable. Click the column header again to reverse the sort order. The grid columns can be arranged in any order desired by click-holding and dragging the header of the column you wish to move. The column widths may be adjusted by click-holding and dragging the line separating two column headers.

Advanced Searches

On any search page you can click **Advanced** to the right of the Search button to display the advanced search options. Click **Simple** to close the advanced search options again.

Multiple Criteria

Using the advanced search options, you can build a query based on multiple criteria using AND/OR logic. As with a simple search, you select a field and comparison operator in the drop-downs and then enter a comparison value, if applicable. Click **Insert** to add the search criteria to the query field below the selection fields. Use the selection fields to build multiple search criteria. Each time you

click the insert button, an AND is added between the previous search criteria and the newly added one. You can change the AND to an OR if desired. You can use parentheses around portions of the query along with AND/OR to change the query meaning.

For example, for certificate searches:

```
(CN -contains "appsrvr" AND IssuedDate -ge "01/01/2022") OR (CN -contains "appsrvr" AND
TemplateShortName -contains "web")
```

This query will return all the certificates issued on or after January 1, 2022 with the string appsrvr in the CN and also all certificates issued at any time with the string appsrvr in the CN using a template referencing web. When you have entered all the desired search criteria, click **Search** to execute the query. If you wish to clear the query field and start over, click the **Clear** button.

2.1.8 Locations

The options available in the Locations section of the Management Portal are:

- **Certificate Authorities**
  Import CAs from Active Directory and/or define remote CAs, configure synchronization and monitoring tasks for them, set authorization methods and configure enrollment details.
- **Certificate Templates**
  Import certificate templates from Active Directory or EJBCA, view certificates and configure template-specific enrollment details such as; enrollment fields, authorization methods, metadata, template regular expressions, enrollment defaults and policies. Also, set system-wide template enrollment regular expressions, enrollment defaults and policies.
- **Certificate Stores**
  Configure paths to certificate stores on multiple machines and devices in the environment, group them into containers for organization and configure inventory schedules to synchronize the certificates in the stores to Keyfactor Command, and view certificate inventory.
- **SSL Discovery**
  Configure SSL endpoint groups on which to run discovery and monitoring jobs and then import certificates from the endpoints for monitoring, reporting and alerting purposes. Define orchestrator pools and view scan results.

2.1.8.1 Certificate Authorities

Your Microsoft and EJBCA certificate authorities (CAs) are defined in the Management Portal to support synchronization to the Keyfactor Command database and support enrollment. Microsoft CAs in the local forest in which Keyfactor Command is installed or in a forest in a two-way trust with this forest may be imported from Active Directory or manually configured. Other Microsoft CAs and EJBCA CAs need to be manually configured. During initial provisioning, any domain-joined Microsoft CAs in the primary Active Directory forest will be imported automatically by the Keyfactor Command configuration wizard.

Important: In order for CAs to successfully synchronize to the Keyfactor Command database and perform other functions (e.g. enrollment), the service account under which Keyfactor Command is making the request to the CA must be granted appropriate permission to the CA database as per *Grant the Keyfactor Command Users and Service Account(s) Permissions on the CAs* in the *Keyfactor Command Server Installation Guide*.

CAs that need to be configured manually include:

- Domain-joined enterprise or standalone Microsoft CA in a forest with a one-way trust (either direction) with the forest in which Keyfactor Command is installed
- Domain-joined enterprise or standalone Microsoft CA in a forest that has no trust with the forest in which Keyfactor Command is installed
- EJBCA CA
- Non-domain-joined standalone Microsoft CA
- Keyfactor CA gateway in the forest in which Keyfactor Command is installed

  The CA gateways are used to access cloud certificate providers (e.g. the Entrust CA Gateway) or to support Microsoft CAs in remote or cloud environments (e.g. the Cross-Forest Gateway).

  Note: Keyfactor CA gateways are not supported in any configuration other than in the same forest in which Keyfactor Command is installed.

- On-premise Microsoft CA accessed via the Keyfactor CA Management Gateway using a managed instance of Keyfactor Command
- On-premise EJBCA CA accessed via the Keyfactor CA Management Gateway using a managed instance of Keyfactor Command
- Microsoft CA accessed via the Keyfactor Universal Orchestrator or Windows Orchestrator

  Note: You must install and configure the Keyfactor Universal Orchestrator or Windows Orchestrator on a machine in the same forest where the Microsoft CA resides and configure it with CA Support and approve the orchestrator in the Management Portal before creating the CA record.

The majority of CA-related functions within Keyfactor Command are supported by both EJBCA and Microsoft CAs. Table 14: CA Function Matrix includes a list of CA-related functions and the support provided by EJBCA and Microsoft CAs.

Important: EJBCA integration with Keyfactor Command requires EJBCA version 7.8.1 or higher.

Table 14: CA Function Matrix

	EJBCA CA	Microsoft CA
CA Synchronization	✓	✓
Template[1] Import	✓	✓
CA Threshold Monitoring (Issuance)	✓	✓
CA Threshold Monitoring (Failures)		✓
CA Health Monitoring	✓	✓
Certificate Enrollment (PFX)	✓	✓
Certificate Enrollment (CSR)	✓	✓
Certificate Revocation	✓	✓
CRL Publishing Following Certificate Revocation	✓	✓
Keyfactor Command Private Key Retention and Key Recovery	✓	✓
CA-Level Key Archiving (* no longer supported as of Keyfactor Command v10)		
CA-Level Key Recovery		✓
Approvals in Workflow Builder	✓	✓
CA-Level Approvals with Pending, Issued and Denied Alerts		✓
Supports use of *Restrict Allowed Requesters* for access control	✓	✓
Requires use of *Restrict Allowed Requesters* for access control	✓	
Requests to the CA can be done in the context of the user initiating the		✓

[1]When EJBCA templates are imported, they are named using a naming scheme of <end entity profile name>_<certificate profile name> for the template name (short name). New templates do not need to be created for Keyfactor Command.

	EJBCA CA	Microsoft CA
request		
Requests to the CA can be done in the context of a single service account[1]	✔	✔
Supports use of Universal Orchestrator to access remote CA		✔

Tip: Click the help icon (?) next to the page title to open the embedded web copy of the *Keyfactor Command Documentation Suite* to this section.
You can also find the help icon at the top of the page next to the **Log Out** button. From here you can choose to open either the *Keyfactor Command Documentation Suite* at the home page or the *Keyfactor API Endpoint Utility*.

Certificate Authority Operations

During installation of Keyfactor Command, CA records are created for any Microsoft CAs found in the local forest in which Keyfactor Command is installed. If you have Microsoft CAs in separate forests in a two-way trust with the forest in which Keyfactor Command is installed, you will need to use the import option to import CA records from those forests. If you have Microsoft CAs in any other configuration or EJBCA CAs, you will need to manually configure CA records for them.

Importing Trusted Forest CAs

Microsoft CA and Keyfactor CA gateway records from the Active Directory forest in which Keyfactor Command is installed and any Active Directory forests in a two-way trust with this forest may be imported using the Import option.

To import CA records:

1. In the Management Portal, browse to *Locations > Certificate Authorities*.
2. On the Certificate Authorities grid, click the **Import** action button to import local or two-way trusted forest CAs and Keyfactor CA gateways.
3. In the Import Certificate Authorities dialog, select the forest from which you want to import in the dropdown and click **Import**.

[1]For EJBCA, this is the end entity associated with the client certificate used to authenticate to the EJBCA CA.

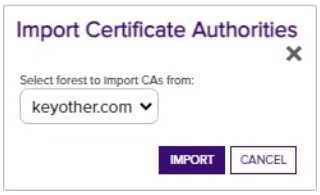


Figure 199: Import Certificate Authorities

Your certificate authorities and CA gateways will be retrieved from Active Directory in the trusted forest and will populate the CA grid. Import once for each forest containing Microsoft CAs that you want to synchronize or use for enrollment.

Once the records are imported, use the **Edit** option (see Adding or Modifying a CA Record on the next page) to configure synchronization and other optional settings for the CA.

Tip: This step does not need to be completed for the forest in which Keyfactor Command is installed because those records are imported during the installation process.

Note: Keyfactor CA gateways are not supported in any configuration other than in the same forest in which Keyfactor Command is installed.

Note: The import option only works for Microsoft CAs or Keyfactor CA gateways that have been registered in Active Directory.

Test a CA Connection

As of Keyfactor Command version 10, CA connections can be tested from the Certificate Authority page. There are two new action buttons on the Certificate Authority dialog, **Test Connection** and **Save and Test**, in addition to the Cancel button.

Certificate Authorities will be tested before they are saved to the database and must be valid and reachable to be saved. If the CA can't be verified, an error message with an explanation of the issue will be displayed and added to the Command_API_Log.

- For EJBCA, the test checks that the CA name provided is valid for the given EJBCA instance. It validates the hostname, enabled APIs, and authentication certificate. The version is validated (7.8.1 or greater) and connecting to both the REST v1 and SOAP APIs is also validated.
- For Microsoft, the test checks the forest, logical name, CA host, and explicit credentials by using a certutil ping.
- Remote CAs (managed by an orchestrator) will not have the connection tested before saving the CA. The **Test Connection** button will be active, but you will receive a message that the connection cannot be tested if you click it. The **Save and Test** button will skip the test when saving.

Note: As a result of this functionality, it is not possible to add offline root or policy CAs, as they will not be able to be verified. Add any certificates for offline root or policy CAs manually to the Keyfactor Command database using the Add Certificate option (see Add Certificate on page 69).

To test a CA record:

1. In the Management Portal, browse to *Locations > Certificate Authorities*.
2. On the Certificate Authorities grid, click **Add** to add a new CA, or click **Edit** to modify an existing CA, from either the top or right-click menu.
3. Follow the instructions for adding or modifying a CA (see Adding or Modifying a CA Record below). Once you have entered the details you want to test, click **Test Connection** or **Save and Test**. Upon a successful test, you will receive a green success notification at the bottom of the page. Upon a test failure, you will receive a pop-up message with the details of the failure; a message will also be added to the log.

Adding or Modifying a CA Record

Tip: When adding or editing your CAs, the connection can now be tested and must be valid and reachable for the CA to be saved. See Test a CA Connection on the previous page.

Whether your CA has been imported or added manually, you'll need to update it to configure synchronization and other optional settings.

Certificate Authorities that need to be added manually include:

- A Microsoft enterprise or standalone CA that is installed on a machine that is domain-joined to a forest that is in a one-way trust with the forest in which Keyfactor Command is installed
- A Microsoft enterprise or standalone CA that is installed on a machine that is domain-joined to a forest that has no trust with the forest in which Keyfactor Command is installed
- An EJBCA CA
- A non-domain-joined Microsoft standalone CA
- A CA accessed via the Keyfactor Universal Orchestrator or Windows Orchestrator
- A Microsoft enterprise or standalone CA that is installed on a machine that is domain-joined to the forest in which Keyfactor Command is installed or a forest that is in a two-way trust with the forest in which Keyfactor Command is installed but has not be registered in Active Directory
- A Keyfactor CA gateway or CA management gateway that has not been registered in Active Directory

If your Microsoft CA or Keyfactor CA gateway is domain-joined in the forest in which Keyfactor Command is installed or a forest in a two-way trust with this forest and has been registered in Active Directory, you can opt to add a record for it manually, but it is generally easier to use the import option (see Importing Trusted Forest CAs on page 328).

Important: In order for CAs to successfully synchronize to the Keyfactor Command database and perform other functions (e.g. enrollment), the service account under which Keyfactor Command is making the request to the CA must be granted appropriate permission to the CA database as per *Grant the Keyfactor Command Users and Service Account(s) Permissions on the CAs* in the *Keyfactor Command Server Installation Guide*.

To create a CA record manually or edit an existing one:

1. In the Management Portal, browse to *Locations > Certificate Authorities*.
2. On the Certificate Authorities grid, click **Add** to add a new CA, or click **Edit** from either the top or right-click menu to modify an existing one.
3. At the top of the dialog, choose an appropriate CA communication protocol in the **Select CA Communication Protocol** dropdown. The options are:
   - DCOM—Select this option for Microsoft CAs and CA gateways.
   - HTTPS—Select this option for EJBCA CAs.

   This field cannot be modified on an edit.
4. The remainder of the Certificate Authority dialog shows four tabs. Only the first three are used for EJBCA CAs. Complete the Certificate Authority dialog with the appropriate data using the following instructions:

The Basic Tab

In the *Details* section populate the **Logical Name**, **Host Name** and **Configuration Tenant** fields with the appropriate information for the CA. (The **Enforce Unique DN** checkbox applies only to the HTTPS Certificate Authorities).

The **Configuration Tenant** field cannot be modified on an edit.

Tip: Previous versions of Keyfactor Command referred to the **Configuration Tenant** as the **Template Forest**.

Domain-Joined Enterprise or Standalone Microsoft CA in a Forest with a One-Way Trust (either direction) with the Forest in which Keyfactor Command is Installed

- **Logical Name**—The logical name of the CA in the remote forest. For example: Corp2Ls-suingCA1
- **Host Name**—The fully qualified domain name of the server on which the CA in the remote forest is installed. For example: corp2ca01.keyother.com
- **Configuration Tenant**—The DNS domain name for the Active Directory forest in which the CA resides. For example: keyother.com

Domain-Joined Enterprise or Standalone Microsoft CA in a Forest that has No Trust with the Forest in which Keyfactor Command is Installed

- **Logical Name**—The logical name of the CA in the remote forest. For example: Corp3IssuingCA1
- **Host Name**—The fully qualified domain name of the server on which the CA in the remote forest is installed. For example: corp3ca01.keyother2.com
- **Configuration Tenant**—The DNS domain name for the Active Directory forest in which the CA resides. For example: keyother2.com

EJBCA CA

- **Logical Name**—The logical name of the EJBCA CA. For example: CorpCA1

  Note: EJBCA CA logical names are case sensitive (e.g. CorpCA1 is not the same as CORPCA1).

- **Host URL**—The URL pointing to the EJBCA CA. For example: https://ejbca01.keyother3.com. If the URL provided does not have a virtual directory (/ejbca or otherwise) the /ejbca will be provided, otherwise it will use what is supplied in the URL.
- **Configuration Tenant**—A reference ID for the EJBCA CA server. For EJBCA CAs, this does not need to be the DNS domain name. The short hostname of the EJBCA CA server makes a good reference ID.

  Important: EJBCA and Microsoft CAs cannot be configured with the same *Configuration Tenant*, so do not set this to the DNS domain name if you will also be configuring Microsoft CAs in the same DNS domain.

- **Enforce Unique DN**
  Checking this will cause Keyfactor Command, upon enrollment, to search the EJBCA CA for end entities with DNs that match the DN in the certificate request. If a matching DN is found, the process will update the existing end entity in EJBCA with the new certificate request information rather than creating a new end entity. If you enable this option in Keyfactor Command, it must also be enabled on the matching EJBCA CA. A mismatch in these settings can result in enrollment failures.

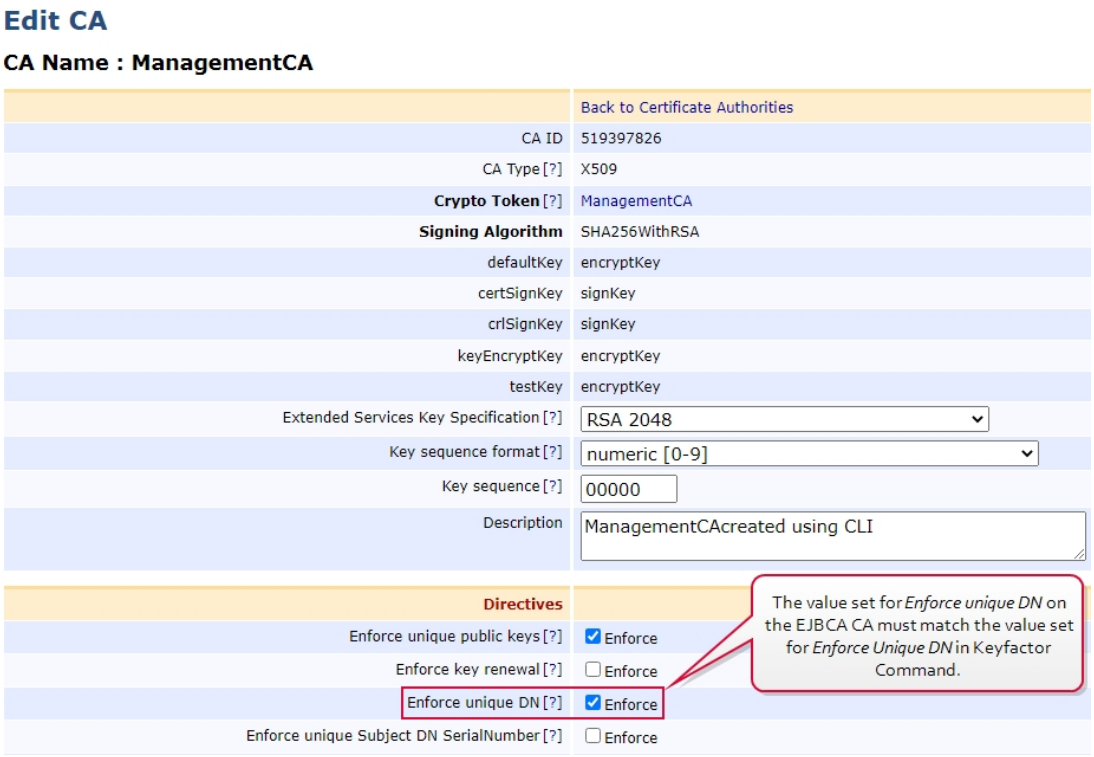


Figure 200: Enforce unique DN Setting on the EJBCA CA

The value of the Keyfactor Command **Enforce Unique DN** setting is verified for each certificate request:

- If unset, enrollment proceeds as usual.
- If set, EJBCA is searched for an end entity associated with the DN and CA in the certificate request and:
  - If none is found, the enrollment proceeds as usual.
  - If one or more is found, the end entity in EJBCA is updated with the information from the certificate request, so that the new certificate request is tied to the same end entity as the existing certificate (or the first one found, if multiple are found). A new password is generated and the enrollment proceeds as usual.

Non-Domain-Joined Standalone Microsoft CA

- **Logical Name**—The logical name of the standalone CA. For example: CorpSARootCA1
- **Host Name**—The fully qualified domain name of the server on which the standalone CA is installed. For example: saroot01.keyexample.com

- **Configuration Tenant**—The DNS domain name for the standalone CA. For example: keyexample.com

Remote CA Accessed via a Keyfactor Universal Orchestrator or Windows Orchestrator

- **Logical Name**—The logical name of the CA in the remote forest to which the orchestrator will be connecting for synchronization. For example: Corp4IssuingCA1
- **Host Name**—The fully qualified domain name of the CA in the remote forest to which the orchestrator will be connecting for synchronization. For example: corp4ca01.keyother4.com
- **Configuration Tenant**—The DNS domain name for the Active Directory forest in which the orchestrator is operating and in which the CA resides. For example: keyother4.com

Note: You must install and configure the Keyfactor Universal Orchestrator or Windows Orchestrator on a machine in the same forest where the CA resides, configure it with CA Support and approve the orchestrator in the Management Portal before creating the CA record.

Domain-Joined Enterprise or Standalone Microsoft CA in the Forest in which Keyfactor Command is Installed

- **Logical Name**—The logical name of the CA in the local forest. For example: CorpIssuingCA1
- **Host Name**—The fully qualified domain name of the server on which the CA in the local forest is installed. For example: corpca01.keyexample.com
- **Configuration Tenant**—The DNS domain name for the Active Directory forest in which the CA resides. For example: keyexample.com

Keyfactor CA Gateway

- **Logical Name**—The logical name of the CA gateway in the local forest. For example: EntrustGateway
- **Host Name**—The fully qualified domain name of the server on which the CA gateway in the local forest is installed. For example: entgtw1.keyexample.com
- **Configuration Tenant**—The DNS domain name for the Active Directory forest in which the CA resides. For example: keyexample.com

Keyfactor CA Management Gateway

- **Logical Name**—The logical name created when the gateway was configured. The logical name is unique for each CA gateway. For a gateway providing a bridge to an on-premise Microsoft CA, the name configured as the gateway logical name should match the logical

name of the Microsoft CA.

- **Host Name**—The fully qualified domain name of the server in the managed forest environment in which the Keyfactor CA Management Gateway is installed.
- **Configuration Tenant**—The DNS domain for the Active Directory forest in the managed forest environment in which the Keyfactor CA Management Gateway is installed.

In the *Scan* section, choose when to schedule full and incremental scans. You can choose to run each scan **Weekly**, **Daily** or on an **Interval**:

- If you select **Weekly**, you can select one or more days of the week on which to run the scan and a time when the scan should begin.
- If you select **Daily**, you can set the time of day when the scan should begin.
- If you select **Interval**, you can select a scan frequency of anywhere from every 1 minute to every 12 hours.
- Select **Off** in the dropdown to disable a scan job.

  There are two types of synchronization schedules available for CAs—Full and Incremental. You do not necessarily need to configure both types. A full scan reads all the certificates and certificate requests in the CA database and synchronizes them to Keyfactor Command regardless of their current state in Keyfactor Command. An incremental scan reads the certificates and certificate requests in the CA database that have been generated since the last full or incremental scan and synchronizes them to Keyfactor Command. A common configuration would be a full scan once or twice a week to provide a clean image of the CA database with a frequent incremental scan to provide timely updates to Keyfactor Command. For a large CA database, a full scan can take a long time to complete. Since an incremental scan only synchronizes updates that have occurred to the CA database since the last synchronization was run, this process is generally quick (other than for the initial synchronization when Keyfactor Command is first installed). The frequency of the incremental scans would depend on the volume of certificate requests coming into the CA.

  Note: For EJBCA CAs, if the certificate profile has a *Validity Offset* configured to a value greater than the value configured in the *CA Sync Backward Offset Minutes* application setting (15 minutes by default), certificates requested outside of Keyfactor Command will not be picked up on incremental scans. These certificates will only appear in Keyfactor Command on a full synchronization. The *CA Sync Backward Offset Minutes* application setting should be set to the same number of minutes as the *Validity Offset* value, if *Validity Offset* is configured.

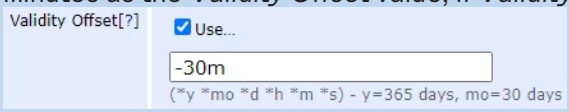
  

  Figure 201: EJBCA Certificate Profile Validity Offset Greater than 15 Minutes

Note: For EJBCA CAs, if the certificate profile has *Allow Backdated Revocation* configured and a revocation is completed outside of Keyfactor Command with a backdate of greater than 10 minutes, the revocation will not be picked up on incremental scans. These revocations will only appear in Keyfactor Command on a full synchronization.

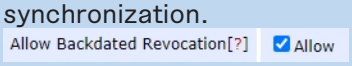


Figure 202: EJBCA Certificate Profile Backdated Revocation

For Microsoft CAs, if desired check the **Sync External Certificates** box to allow foreign certificates that have been imported into a Microsoft CA to be synchronized to Keyfactor Command along with the certificates issued by the Microsoft CA. This option does not appear for HTTPS CAs.

In the *Enrollment* section, check the **Enable PFX Enrollment** and/or **Enable CSR Enrollment** box to enable enrollment for the CA through Keyfactor Command.

Note: In order to perform enrollment through Keyfactor Command, the account making the request to the CA must be granted appropriate enroll permissions on the CA itself. Which account this is depends on the authorization configuration (see Authorization Methods Tab on page 341):

- If **Use Explicit Credentials** is set to *true* (box checked), enrollment is done in the context of that explicit user and that user needs permission.
- If **Use Explicit Credentials** is set to *false* (box not checked), enrollment is done in the context of the user authenticated to Keyfactor Command using Kerberos or Basic authentication.

Enrollment is not supported using NTLM authentication.

If desired, check the **Require Subscriber Terms** box to add a checkbox on the enrollment pages to force users to agree to a custom set of terms before enrolling. Configure a link to the custom terms using the *URL to Subscriber Terms* application setting (see Application Settings: Enrollment Tab on page 591).

Tip: To fully configure enrollment for the CA, you will also need to configure access on the Authorization Methods tab (see Authorization Methods Tab on page 341) and configure templates (see Certificate Template Operations on page 353).

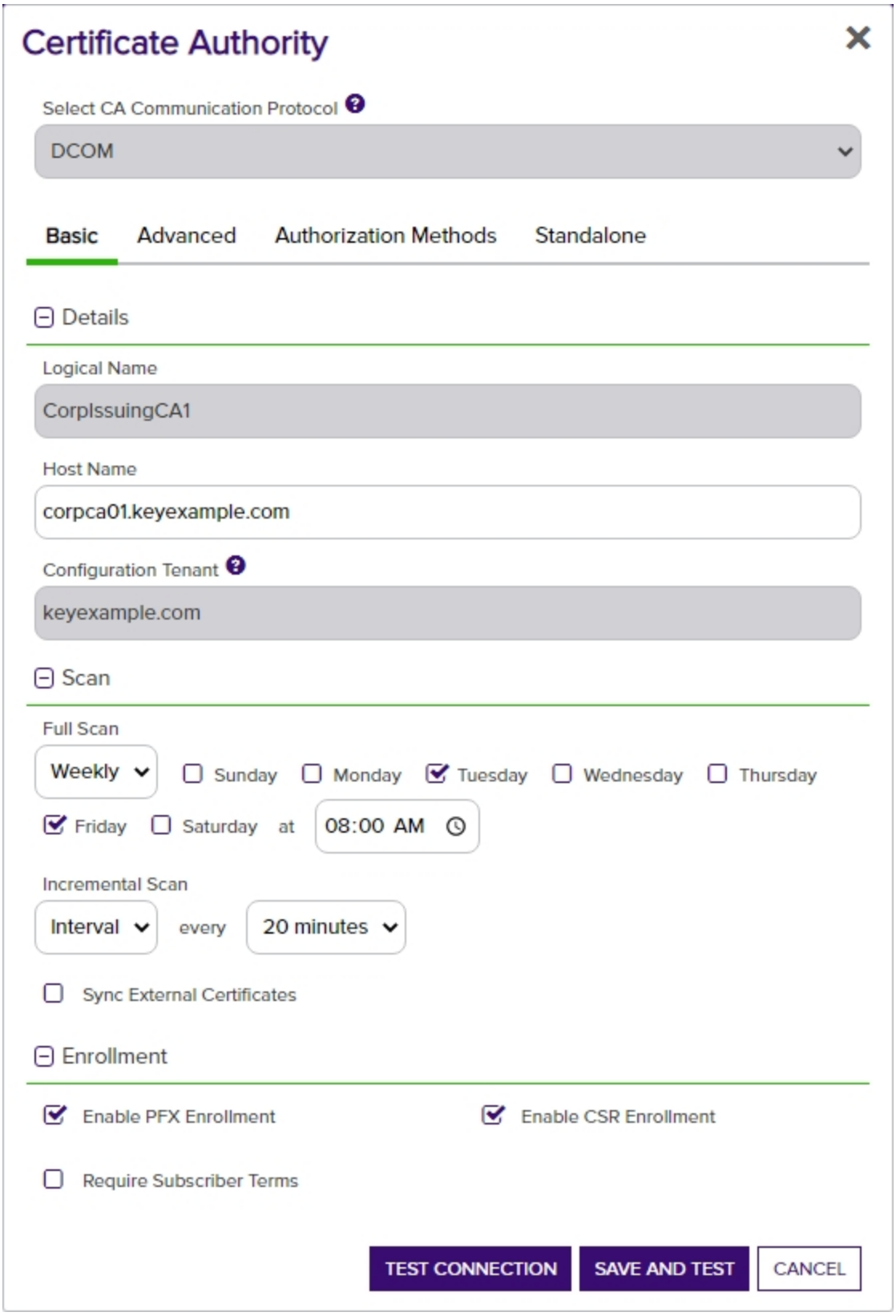

Certificate Authority
Select CA Communication Protocol
DCOM
Basic
Advanced
Authorization Methods
Standalone
Details
Logical Name
CorpIssuingCA1
Host Name
corpca01.keyexample.com
Configuration Tenant
keyexample.com
Scan
Full Scan
Weekly
Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
at
08:00 AM
Incremental Scan
Interval
every
20 minutes
Sync External Certificates
Enrollment
Enable PFX Enrollment
Enable CSR Enrollment
Require Subscriber Terms
TEST CONNECTION
SAVE AND TEST
CANCEL

Figure 203: Certificate Authority Basic Tab for a Microsoft CA

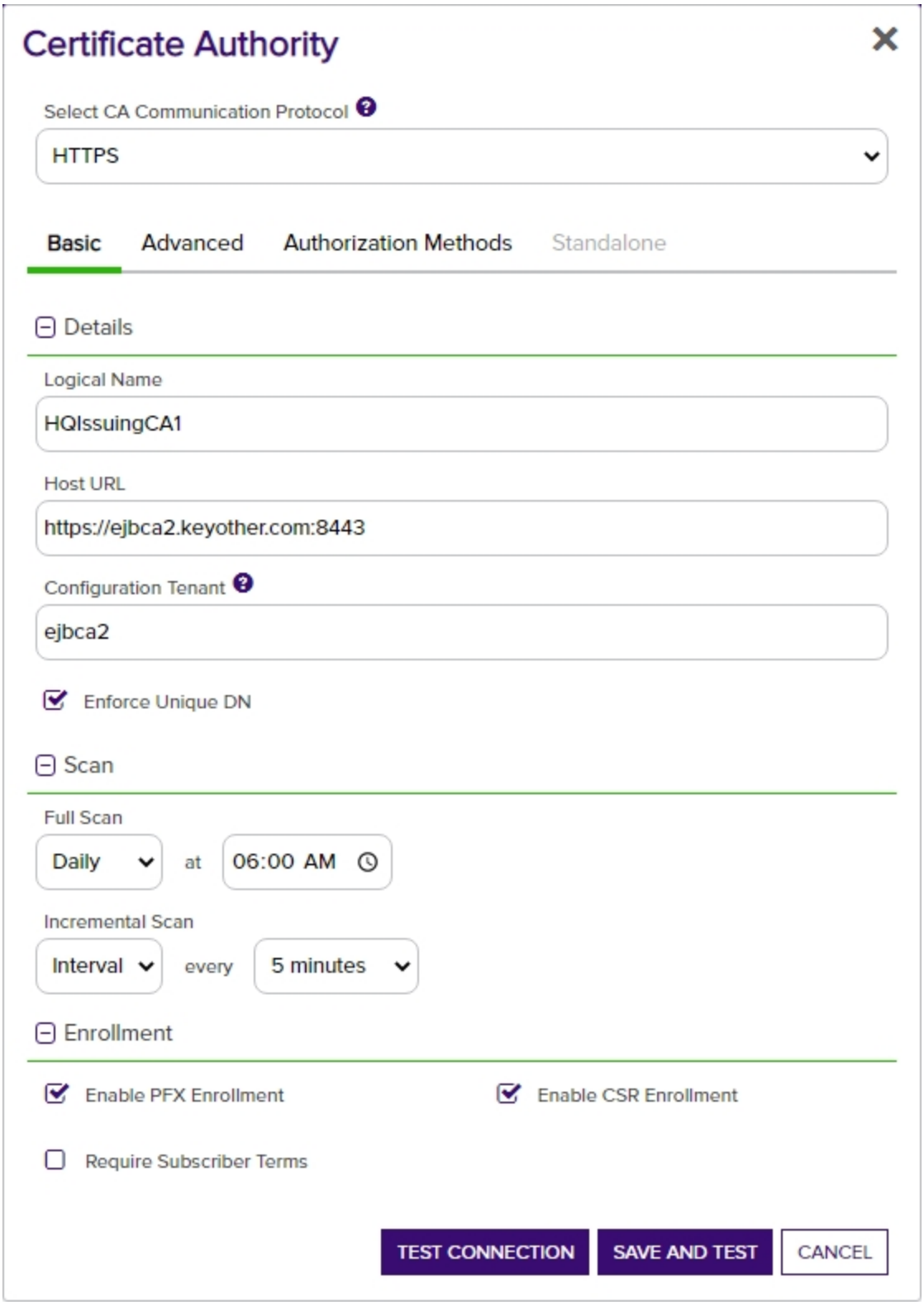

Certificate Authority
Select CA Communication Protocol
HTTPS
Basic
Advanced
Authorization Methods
Standalone
Details
Logical Name
HQIssuingCA1
Host URL
https://ejbca2.keyother.com:8443
Configuration Tenant
ejbca2
Enforce Unique DN
Scan
Full Scan
Daily
at
06:00 AM
Incremental Scan
Interval
every
5 minutes
Enrollment
Enable PFX Enrollment
Enable CSR Enrollment
Require Subscriber Terms
TEST CONNECTION
SAVE AND TEST
CANCEL

Figure 204: Certificate Authority Basic Tab for an EJBCA CA

Advanced Tab

In the *Details* section, if you've opted to use the Keyfactor Universal Orchestrator or Windows Orchestrator to communicate with a remote CA, check the **Use Orchestrator** box and choose the appropriate orchestrator from the dropdown.

Note: The Orchestrator dropdown is only active if the **Use Orchestrator** box is checked. If **Use Orchestrator** is checked, the Orchestrator dropdown will populate with any orchestrators approved in Keyfactor Command with the CA capability. The Keyfactor Universal Orchestrator or Windows Orchestrator must be installed on a machine in the forest where the remote CA resides, installed and configured as per *Universal Orchestrator* in the *Keyfactor Orchestrators Installation and Configuration Guide*. In addition, in the Management Portal, the Keyfactor Universal Orchestrator or Windows Orchestrator must be configured as per Orchestrator Management on page 481.

In the *Monitoring* section, check the **Enable Monitoring** box to turn on email alerting when certificate issuance or failures (including denials) since the last threshold alert was sent falls outside the configured limits. You can choose to schedule the alerts either for daily delivery at a specified time or at intervals of anywhere from every 1 minute to every 12 hours. Daily is the most common configuration. Set the thresholds for:

- **Issuance Greater Than**—You will receive an alert if more certificates are issued by this CA in the time period between executions of the alert than the number you set here. The value set here must be greater than, or equal to, the value set for *Issuance Less Than*.
- **Issuance Less Than**—You will receive an alert if fewer certificates are issued by this CA in the time period between executions of the alert than the number you set here. The minimum allowed value for *Issuance Less Than* is 1.
- **Failures Greater Than**—You will receive an alert if more certificate requests fail or are denied by this CA in the time period between executions of the alert than the number you set here. Zero is a valid setting (meaning you will receive an alert for a single failure).

  Note: EJBCA CAs do not return failure counts using the API, so failures cannot be reported on with threshold monitoring for EJBCA CAs.

In addition to configuring the thresholds for each CA, you must also configure the email recipients on the Alert Recipients tab (see Certificate Authority Monitoring on page 351) of the Certificate Authorities page. Monitoring is not supported for CAs accessed with the Keyfactor Universal Orchestrator or Windows Orchestrator.

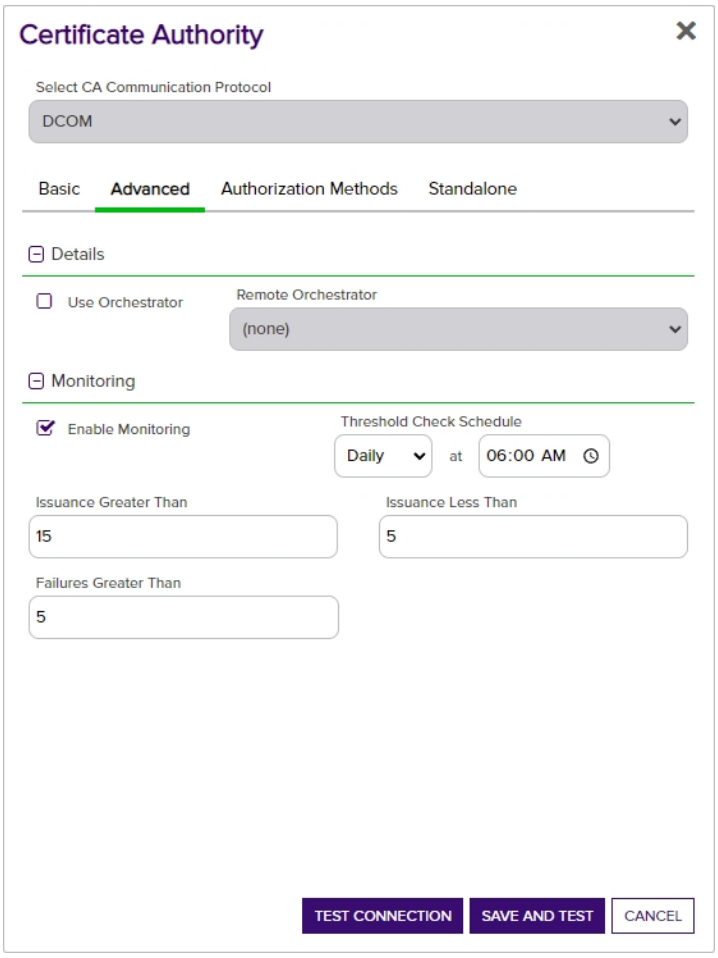


Figure 205: Certificate Authority Advanced Tab for Microsoft CA

Authorization Methods Tab

On the Authorization Methods tab, you configure how access for management tasks and enrollment occurs for the CA.

Tip: Keyfactor recommends the following configuration for most CAs to support access control within Keyfactor Command:

- **Use Explicit Credentials**: True or false as required by the environment
- **Delegate Management Operations**: False (box unchecked)
- **Delegate Enrollment**: False (box unchecked)
- **Restrict Allowed Requesters**: Set to the Keyfactor security roles allowed to perform certificate enrollment for this CA. If you're using workflow (see Workflow

Definitions on page 218), the users who hold these roles are the ones who are able to initiate workflows. This is entirely separate from the roles configured within workflows, which control the users who are able to approve workflows.

Note: If **Use Explicit Credentials**, **Delegate Management Operations** and **Delegate Enrollment** are all set to *false* (box unchecked), requests to the CA are made in the context of the Keyfactor Command application pool user. For more information, see *Grant the Keyfactor Command Users and Service Account(s) Permissions on the CAs* in the *Keyfactor Command Server Installation Guide*.

Use Explicit Credentials (Microsoft CAs)

The **Use Explicit Credentials** option allows you to configure specific credentials that will be used to make requests to the CA for management tasks and enrollment. This is generally used for Microsoft CAs where Windows integrated authentication is not supported. Integrated authentication is generally supported for Microsoft CAs, Keyfactor CA gateways, or Keyfactor CA management gateways on servers joined to the local Active Directory forest in which Keyfactor Command is installed and any Active Directory forests in a two-way trust with this forest.

To configure this option, check the **Use Explicit Credentials** box and enter a username in the format DOMAIN\username for a service account user in the forest in which the CA resides or, for non-domain-joined machines, a local machine account on the machine on which the CA is installed. Click the **Set Explicit Password** button and in the Set Explicit Password dialog, choose from No Value, Load from Keyfactor Secrets or Load From PAM Provider.

A Keyfactor secret is a user-defined password or other information that is encrypted and stored securely in the Keyfactor Command database. Although Keyfactor recommends using Privileged Access Management (see Privileged Access Management (PAM) on page 677) as a more secure solution to secure information, Keyfactor Secret is an option for customers that do not already have a relationship with a PAM provider such as CyberArk or Delinea (formerly Thycotic).

Select the **Load From Keyfactor Secrets** radio button as the *Secret Source* if you want Keyfactor Command to encrypt and store the password in the Keyfactor Command database. Enter and confirm a password.

Select the **Load from PAM Provider** radio button as the *Secret Source* if you want to store the password in a supported third-party PAM solution (see Privileged Access Management (PAM) on page 677). The remaining fields on the dialog will vary depending on the PAM provider.

CyberArk

Select CyberArk in the **Providers** dropdown if your PAM provider is CyberArk. The remaining fields in the dialog will then be:

- PrivateArk Protected Password Name—The name of the username or password in the safe (see Create a CyberArk Password on page 683).
- PrivateArk Folder Name—The path and name of the folder that stores the CyberArk Password (e.g. Root or Root\MyDir).

Delinea (formerly Thycotic)

Select Delinea in the **Providers** dropdown if your PAM provider is Delinea. The remaining field in the dialog will then be:

- Delinea Secret ID—The numeric ID of the secret to retrieve from Secret Server (see Create a Delinea Secret Server Secret on page 687).

This service account user needs appropriate permissions in the CA security settings to accomplish the tasks you plan to carry out for this CA through the Management Portal. For example:

- Certificate enrollment
- Certificate revocation
- Certificate key recovery
- Certificate request approval and denial

These tasks will be carried out on the CA in the context of the credentials you provide here. Access control for these tasks is controlled with Keyfactor Command security (see Security Roles and Identities on page 609) and the **Restrict Allowed Requesters** option, below.

Note: When this option is configured, enrollment and other tasks (e.g. revocation) are done in the context of the user configured here, not the user making the request in Keyfactor Command. This overrides the existing AD security policy used by Keyfactor Command.

Note: Once you have established explicit credentials to a forest for a CA, the forest will be included in the forest dropdown on the *Import Templates* dialog (see Certificate Templates on page 352).

Tip: The **Use Explicit Credentials** option is not needed if you are accessing your CA using a Keyfactor Universal Orchestrator or Keyfactor Windows Orchestrator. Enrollment is not supported when accessing a CA using an orchestrator, so the **Restrict Allowed Requesters** option is not relevant for this type of CA configuration.

The **Use Explicit Credentials** option is not used for EJBCA CAs.

Delegate Management Operations & Delegated Enrollment (Microsoft CAs & CA Gateways)

The **Delegate Management Operations** and **Delegate Enrollment** boxes are used for CAs that support integrated authentication to allow interactions with the CAs via Keyfactor Command to be done in the context of the user authenticated to Keyfactor Command using Kerberos authentication. Integrated authentication is generally supported for Microsoft CAs, Keyfactor CA gateways, or Keyfactor CA management gateways on servers joined to the local Active Directory forest in which Keyfactor Command is installed and any Active Directory forests in a two-way trust with this forest. If delegation is enabled, when a user authenticates with Kerberos to Keyfactor Command, the Keyfactor Command server can delegate the user's credentials to the CA to provide end-to-end authentication without unpacking the credentials at the Keyfactor Command layer.

These options also apply to users who authenticate to Keyfactor Command using Basic authentication, since Keyfactor Command performs pseudo delegation for these users. These options are not supported for users who authenticate using NTLM authentication.

If you choose to disable one or both of the delegation options and have not enabled the *Use Explicit Credentials* option, interaction with the CA for the type of activity that is not delegated (e.g. management operations) is done in the context of the service account under which the Keyfactor Command application pool is running. For more information, see *Grant the Keyfactor Command Users and Service Account(s) Permissions on the CAs* in the *Keyfactor Command Server Installation Guide*.

Note: Use of explicit credentials is mutually exclusive of delegation.

Important: If you configure CA delegation and are using Kerberos authentication, you must also configure Kerberos constrained delegation for the CAs as per *Configure Kerberos Constrained Delegation (Optional)* in the *Keyfactor Command Server Installation Guide*.

The types of interactions affected by these settings include:

- Approval of pending certificate requests (Delegate Management Operations)
- Denial of pending certificate requests (Delegate Management Operations)

- Revocation of certificates (Delegate Management Operations)
- Certificate key recovery (Delegate Management Operations)
- Certificate enrollment (Delegate Enrollment)

Note: If a workflow (see Workflow Definitions on page 218) is configured with a step that will result in a suspended state (e.g. pausing to wait for approvals) and the CA for the request is configured for delegation, the enrollment or revocation request made via the workflow will fail with an error indicating that the failure occurred because CA delegation is enabled. Workflows are not supported with CA delegation in the case where a suspended state may occur because it's possible that the initiating user's context may not be available all the way to the conclusion of the workflow.
When using workflow with steps that will result in a suspended state, do not use CA delegation. Instead, use the Keyfactor Command access control model provided by the **Restrict Allowed Requesters** option for enrollment (see Restrict Allowed Requesters (Microsoft and EJBCA CAs) below) and the Revoke permission for certificates at both the global and collection levels (see Certificate Permissions on page 621).

If you choose to enable delegation, be aware that each user performing one of these delegable operations through the Management Portal must have the appropriate permissions to accomplish this task configured in the CA security settings.

Important: Granting users permissions in the CA security settings for certificate revocation, certificate key recovery, or certificate request approval and denial—e.g. the *Issue and Manage Certificates* permission—in order to support delegation of these operations through the Management Portal also grants these permissions to the users when operating outside the Keyfactor Command Management Portal. Any risk associated with this can be mitigated by implementing the Keyfactor Whitelist Policy Handler on each CA where such permissions are granted (see *Installing the Keyfactor CA Policy Module Handlers* in the *Keyfactor Command Server Installation Guide*).

The **Delegate Management Operations** and **Delegate Enrollment** options are not used for EJBCA CAs.

Restrict Allowed Requesters (Microsoft and EJBCA CAs)

The **Restrict Allowed Requesters** option is used to select Keyfactor Command security roles that a user must belong to in order to successfully enroll for certificates in Keyfactor Command via this CA. (*NOTE: With this option checked, you must include at least one role in the **Allowed Requester Security Roles** table for enrollment to work*). This option is supported for all CAs, but it must be used for Microsoft CAs where integrated authentication is not supported and EJBCA CAs. Integrated authentication is generally supported for Microsoft CAs, Keyfactor CA gateways, or Keyfactor CA management gateways on servers joined to the

local Active Directory forest in which Keyfactor Command is installed and any Active Directory forests in a two-way trust with this forest. Since Keyfactor Command cannot make use of the access control model of the CA itself to determine which users can enroll for certificates at either a template or CA level without using integrated authentication, this setting replaces that functionality. This setting is similar to setting *request certificates* for the selected security roles at the CA level on a Microsoft CA.

The **Restrict Allowed Requesters** check box must be checked—and the **Allowed Requester Security Roles** populated—if the **Use Explicit Credentials** box is checked for a Microsoft CA that isn't accessed using integrated authentication.

Tip: For Microsoft CAs in a two-way trust environment you don't necessarily need to enable **Restrict Allowed Requesters** on the CA, though this may be required in some circumstances depending on the security configuration in the environment. However, templates for a two-way trust environment always require configuration of this option at a template level to support enrollment (see Certificate Template Operations on page 353).

In addition to granting permissions at the CA level using this option, you need enable the **Restrict Allowed Requesters** option to grant permissions on a template-by-template basis (see Certificate Templates on page 352).

Note: Access control for other types of interactions with the CA (e.g. revocation) is managed with standard security roles (e.g. the certificate revoke permission) at both the global and certificate collection level.

Authentication Certificate (EJBCA CAs)

Click the **Select Authentication Certificate** button to upload a client certificate in PKCS#12 format used to provide authentication to the EJBCA CA. This certificate is used to authenticate to the EJBCA database for synchronization, enrollment and management of certificates.

Note: Once you have established a connection to the EJBCA CA, it will be included in the forest dropdown on the *Import Templates* dialog (see Certificate Templates on page 352).

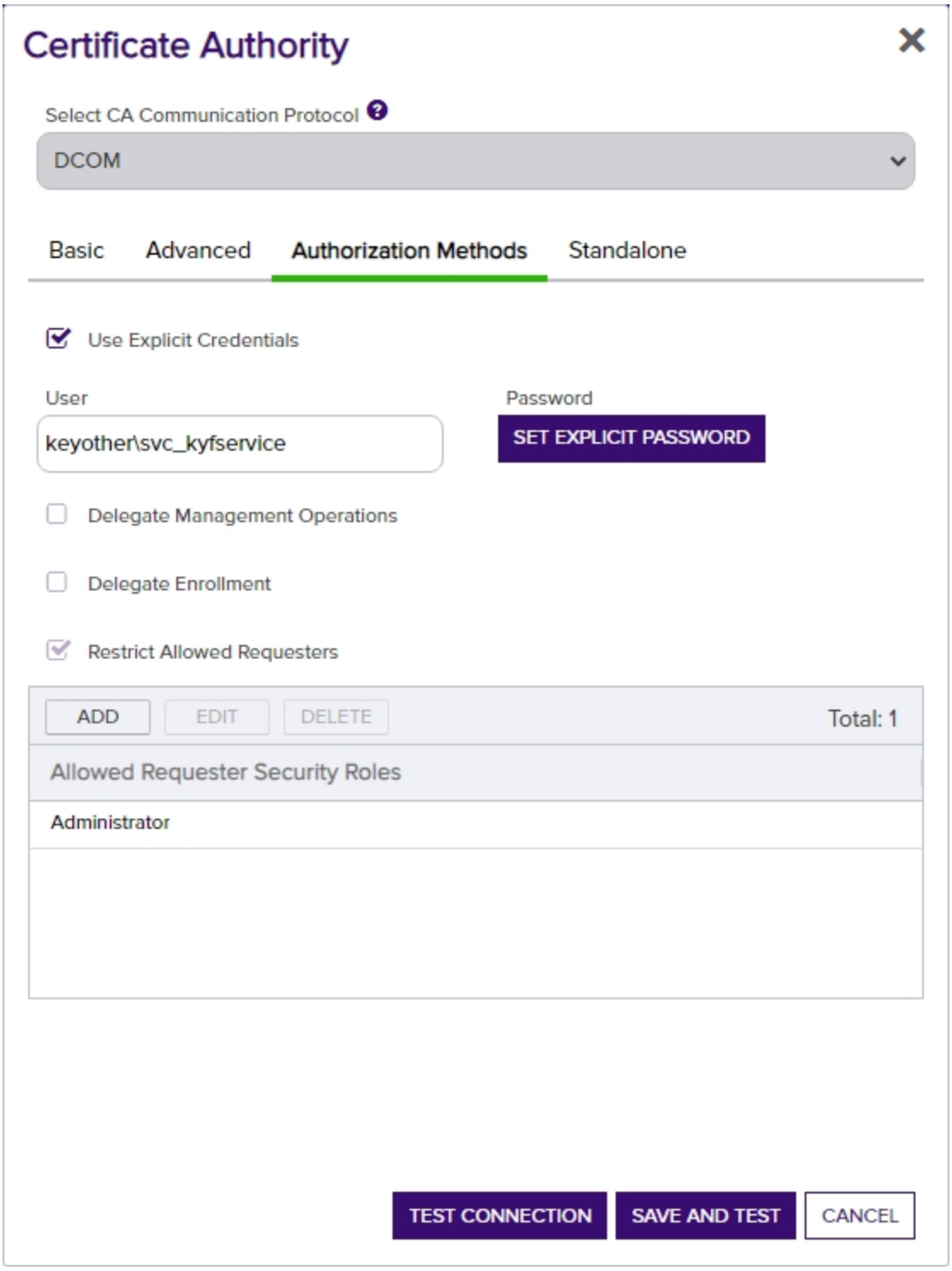

Certificate Authority
Select CA Communication Protocol
DCOM
Basic
Advanced
Authorization Methods
Standalone
Use Explicit Credentials
User
keyother\svc_kyfservice
Password
SET EXPLICIT PASSWORD
Delegate Management Operations
Delegate Enrollment
Restrict Allowed Requesters
ADD
EDIT
DELETE
Total: 1
Allowed Requester Security Roles
Administrator
TEST CONNECTION
SAVE AND TEST
CANCEL

Figure 206: Certificate Authority Authentication Methods Tab for a Microsoft CA

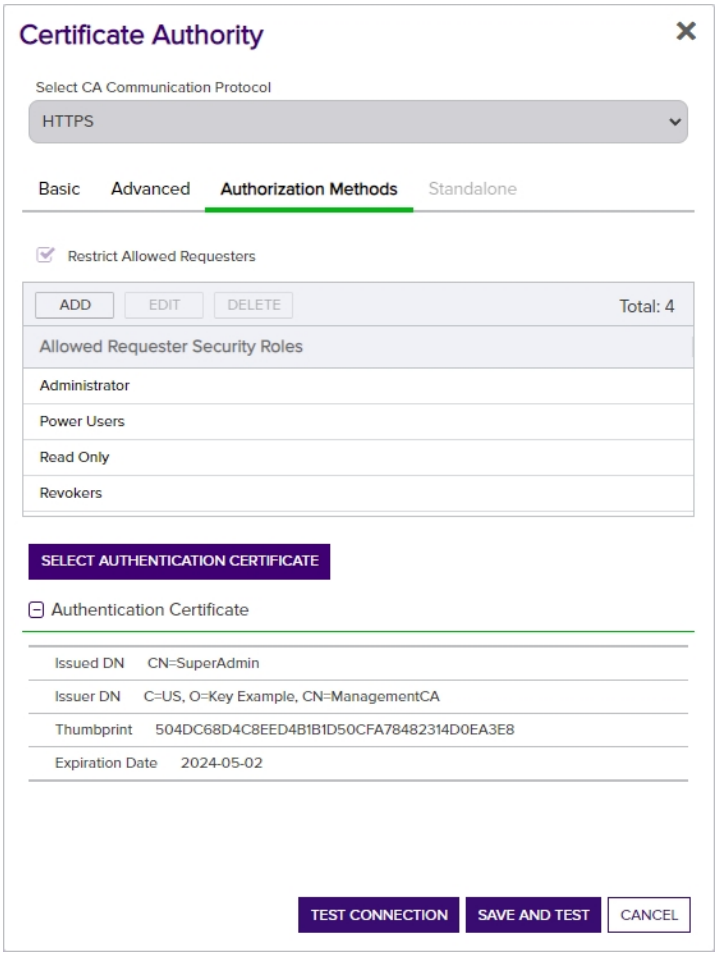


Figure 207: Certificate Authority Authentication Methods Tab for an EJBCA CA

Standalone Tab (Microsoft CAs)

To configure a standalone Microsoft CA, check the **Standalone** box.

Check the **Enforce RFC 2818 Compliance** box to require that certificate enrollments made through the Keyfactor Command Management Portal for this CA include at least one DNS SAN. This causes the CN entered in PFX enrollment to automatically be replicated as a SAN, which the user can either change or accept. For CSR enrollment, if the CSR does not have a SAN that matches the CN, one will automatically be added to the certificate if this is set.

If you have configured the CA for PFX enrollment on the Basic tab, the *Key Retention* field drop-down will display. Select a retention type. Enter the number of days, weeks, months, or years to keep the encrypted private key stored in the Keyfactor Command database based on the type

selected, then select the desired time frame (Day(s), Week(s), Month(s), or Year(s)). You will not have the option to choose a retention timeframe if you choose **Indefinite**.

Configuring private key retention allows the private keys for certificates enrolled through Keyfactor Command to be stored, encrypted, in the Keyfactor Command database for a user-definable period of time.

The private key retention configuration options are:

- Blank

  The private key will not be retained if the box is unchecked, or the *blank* option is selected.
- Indefinite

  The private key will be retained until it is explicitly deleted.
- After Expiration

  The private key will be retained until the specified number of days, weeks, months or years after the certificate expires, at which point it will be scheduled for deletion.
- From Issuance

  The private key will be retained until the specified number of days, weeks, months or years after the date on which the certificate was issued, at which point it will be scheduled for deletion.

Note: When the retention period is stored in the database, weeks are converted to 7 days, months are converted to 30 days, and years are converted to 365 days.

Tip: Setting the retention period to 0 will cause the private keys to be purged by the private key clean up job when it next runs, after the certificate expires or after the certificate is issued.

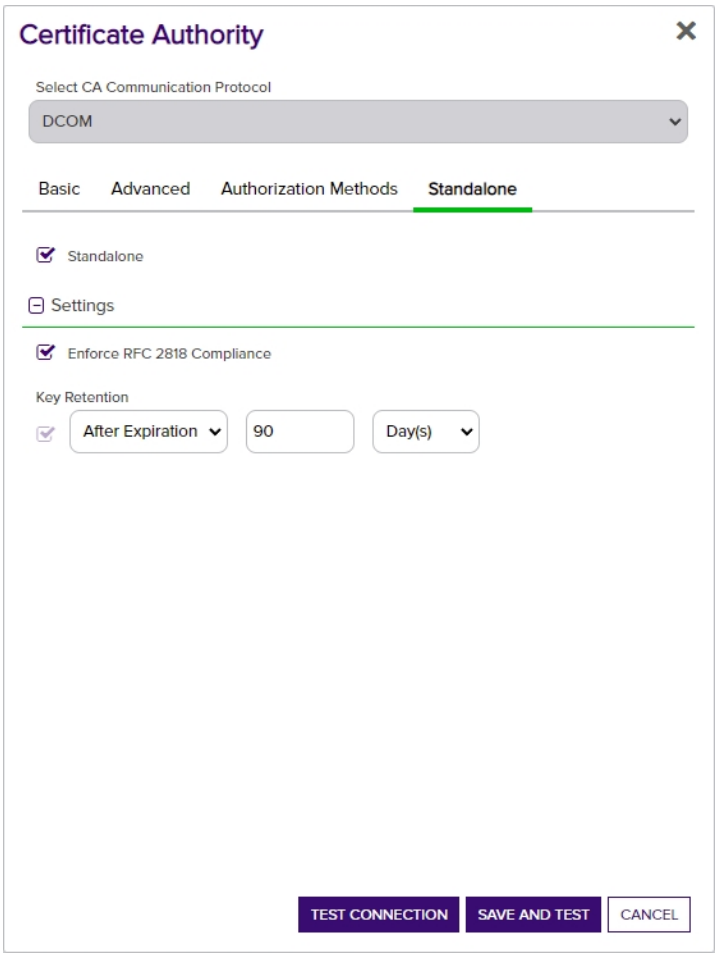


Figure 208: Certificate Authority Standalone Tab

5. Click **Test and Save** to add or update the CA, or click **Test Connection** to test the CA prior to saving (see Test a CA Connection on page 329).

Once a CA record has been created for your CA, go to certificate templates (see Certificate Templates on page 352) and import templates for the CA. Template import is supported for both Microsoft and EJBCA CAs. Template import is not supported for the following:

- Non-domain-joined standalone Microsoft CAs (these don't use templates)
- CAs accessed via the Keyfactor Universal Orchestrator or Windows Orchestrator

Deleting a CA Record

To delete a CA record:

1. In the Management Portal, browse to *Locations* > *Certificate Authorities*.
2. On the Certificate Authorities grid, highlight the row in the CA grid and click **Delete** at the top of

the grid or right-click the CA and choose **Delete** from the right-click menu.

3. On the Confirm Operation alert, click **OK** to confirm or **Cancel** to cancel the operation.

A CA cannot be deleted if:

- It has scanning tasks enabled.
- It has certificates associated with it in the Keyfactor Command database.
- It is the last CA for its *Configuration Tenant* and there are certificate templates (see Certificate Templates on the next page) for that *Configuration Tenant* in Keyfactor Command.

Certificate Authority Monitoring

The two types of monitoring which Keyfactor Command offers for certificate authorities are configured on the Alert Recipients tab of the Certificate Authorities page at *Locations > Certificate Authorities*. Monitoring is not supported for CAs accessed with the Keyfactor Windows Orchestrator or Keyfactor Universal Orchestrator.

Certificate Authority Health Monitoring

Enable certificate authority health monitoring to receive email alerts when one or more of your CAs is not responding. Only CAs configured for synchronization will be monitored for health. To enable health monitoring, configure one or more recipients to receive the email messages and configure a health check schedule. You can choose to schedule the health checks either for daily at a specified time or at intervals of anywhere from every one minute to every 12 hours.

Certificate Authority Threshold Alerts

Enable threshold alerting to receive email alerts when a CA issues more or fewer certificates or experiences more failures or denials than configured for monitoring on the CA (see Advanced Tab on page 340). Setting threshold monitoring is a two-step process:

1. Configure monitoring on the advanced tab (see links above) for each CA.
2. Set the email recipients for the alerts on the alert recipients tab of the certificate authorities page.

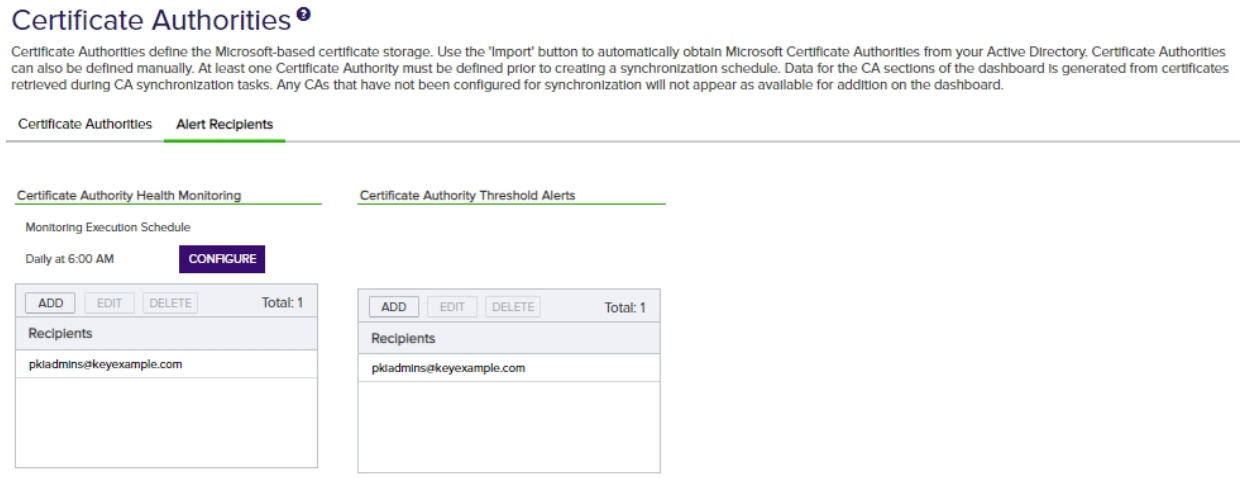


Figure 209: Certificate Authority Monitoring Recipients

2.1.8.2 Certificate Templates

During initial provisioning, the certificate templates in the primary Active Directory forest (the forest in which Keyfactor Command is installed) will be imported automatically by the Keyfactor Command configuration wizard. Templates for additional forests can be imported in a number of ways:

- For Microsoft CAs domain-joined to forests in a two-way trust with the primary forest, you can use the *Import Templates* option at any time.
- For Microsoft CAs domain-joined to forests in a one-way trust with the primary forest or to a forest having no trust with the primary forest, you can use the *Import Templates* option after you have configured a CA record for at least one Microsoft CA in the non-primary forest and enabled the *Use Explicit Credentials* option with credentials for the non-primary forest.
- For EJBCA CAs, you can use the *Import Templates* option after you have configured a CA record for at least one EJBCA CA.
- Templates that are associated with certificates that have been requested from a Microsoft CA in a forest other than the primary forest will appear in the templates grid as those certificates are synchronized to Keyfactor Command if you configure CA synchronization for the CA even if you don't use the import option.
- There's an automated process to import templates once every hour, on the hour. Templates are imported for Microsoft CAs in the primary forest, Microsoft CAs in any forests in a two-way trust with the primary forest, and any CAs that can be reached using the credentials configured in the CA record (the *Use Explicit Credentials* option for Microsoft CAs or the client certificate for EJBCA CAs). The automated template import only runs for CAs for which there is an active CA synchronization job configured. This automated sync is only enabled if the *Sync Templates* option on the **Service tab** of the Configuration Wizard is selected during installation (see *Install the Main Keyfactor Command Components on the Keyfactor Command Server(s): Service Tab* in the *Keyfactor Command Server Installation Guide*).

You will need to import templates if you add a new template or change the name or key size of a template after it has been imported into Keyfactor Command and don't want to wait for the automated import process or have not configured the automated process (see Importing Certificate Templates on the next page).

Certificate templates need to be configured to support PFX and CSR enrollment (see Configuring Template Options on page 360).

Note: When EJBCA templates are imported, they are named using a naming scheme of:

- Short Name: *<end entity profile name>_<certificate profile name>*
- Display Name: *<end entity profile name>* (*<certificate profile name>*)

Only certificate profiles configured as *available* in a given end entity profile will be imported as templates associated with the given end entity profile name.

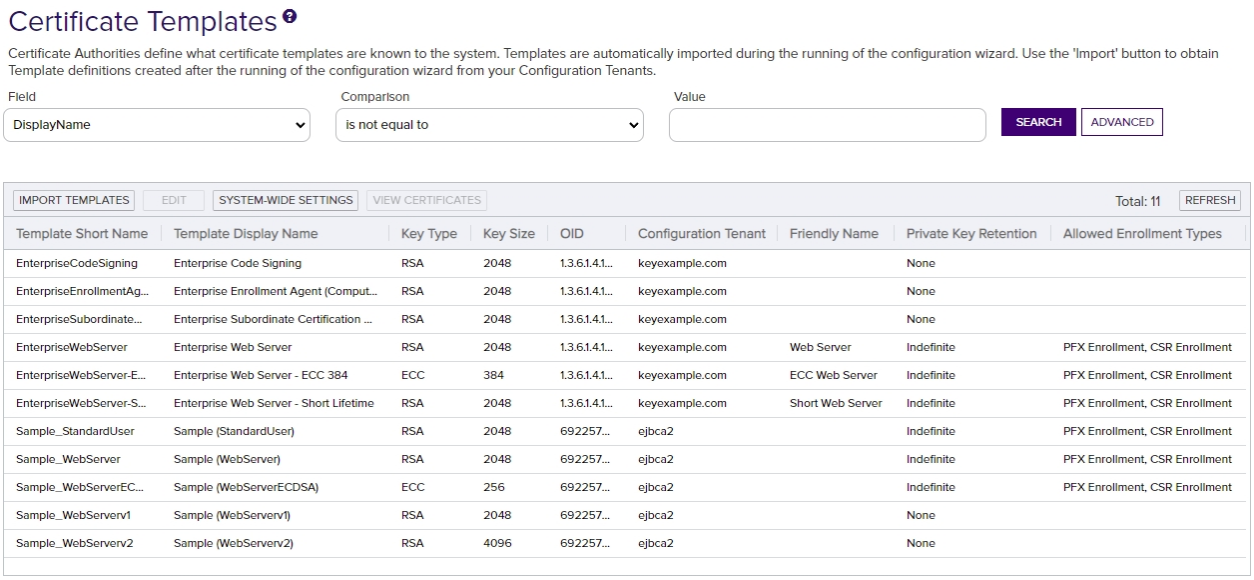


Figure 210: Certificate Templates

Tip: Click the help icon (?) next to the page title to open the embedded web copy of the *Keyfactor Command Documentation Suite* to this section.
You can also find the help icon at the top of the page next to the **Log Out** button. From here you can choose to open either the *Keyfactor Command Documentation Suite* at the home page or the *Keyfactor API Endpoint Utility*.

Certificate Template Operations

Certificate templates are imported from their source rather than created in Keyfactor Command, which means there are limited operations that need to be performed in Keyfactor Command in relation to them. Supported actions on the certificate template page include:

- **Import Templates**

  The certificate templates in the primary Active Directory forest (the forest in which Keyfactor Command is installed) will be imported automatically by the Keyfactor Command configuration wizard during the Keyfactor Command installation. The template import option is used for templates from other sources or for new templates created or edited after the Keyfactor Command installation.

- **Configure System-Wide Settings**

  The global settings option allows you to configure regular expressions, certificate subject defaults and policies that apply to all enrollments unless overridden by template-level settings.

- **Edit Template Options**

  Although templates are imported from their source, there are multiple Keyfactor Command-specific settings that can be configured on the templates to allow them to be used within the product.

- **View Certificates for a Template**

  The view certificates option takes you to the certificate search interface with the query field populated by the selected template.

Importing Certificate Templates

You only need to import templates if you have EJBCA CAs, Microsoft CAs in forests other than the forest in which Keyfactor Command was installed, or have added a new template or changed the name or key size of a template after it has been imported into Keyfactor Command and don't want to wait for the automated import process or have not configured the automated process (see Certificate Templates on page 352).

To import certificate templates:

1. In the Management Portal, browse to *Locations* > *Certificate Templates*.
2. On the Certificate Templates page, click **Import Templates**.
3. In the Select Configuration Tenant dialog, select a configuration tenant in the dropdown.

   Tip: Previous versions of Keyfactor Command referred to the **Configuration Tenant** as the **Template Forest**.

   If you have a forest in a two-way trusted relationship with the forest in which Keyfactor Command is installed or have configured a Microsoft CA with the *Use Explicit Credentials* option or an EJBCA CA, the configuration tenant for this CA will appear in the dropdown. Import once for each configuration tenant containing templates that you want to import. The import process may take several seconds.

Note: When EJBCA templates are imported, they are named using a naming scheme of:

- Short Name: *<end entity profile name>_<certificate profile name>*
- Display Name: *<end entity profile name>* (*<certificate profile name>*)

Only certificate profiles configured as *available* in a given end entity profile will be imported as templates associated with the given end entity profile name.

Tip: Out of the box, only templates for Microsoft CAs in the forest in which Keyfactor Command is installed and any Microsoft CAs in forests in a two-way trust with this forest can be imported using the template import. In order to import templates for other Microsoft CAs, you need to configure the *Use Explicit Credentials* option for each Microsoft CA for which you want to import templates and enter credentials valid for that CA with appropriate permissions to allow Keyfactor Command to query the remote CA for template records. For Microsoft CAs joined to a remote forest, only one CA in each forest needs to be configured to allow the template import to function.

Configuring System-Wide Settings

System-wide settings apply to all enrollments done through Keyfactor Command unless they are overridden by template-specific settings (see Enrollment Regexes Tab on page 368, Enrollment Defaults Tab on page 370, and Policies Tab on page 372). Although system-wide settings are configured on the templates page, they also apply to enrollments done without a template (e.g. standalone CAs).

Note: System-wide settings replaced and enhanced selected application settings for enrollment beginning in release 10.

To configure system-wide options:

1. In the Keyfactor Command Management Portal, browse to *Locations > Certificate Templates*.
2. On the Certificate Templates page, click **System-Wide Settings** at the top of the grid.
3. When you open the system-wide settings, you will see three tabs. Configure the system-wide setting information with the appropriate data using the following instructions.
4. Click **Save** to save the system-wide settings. Click **Back** to return to the certificate templates page.

Enrollment RegExes Tab

Regular expressions for enrollment are used to validate that the data entered in the certificate subject fields meets certain criteria.

Tip: To use a system-wide enrollment regular expression and allow a specific template to bypass that regular expression, you can configure a template-level regular expression for the desired subject part and set it to nothing.

To configure a system-wide regular expression:

1. On the Enrollment RegExes tab, double-click a subject part row in the grid, right-click the row and choose **Edit** from the right-click menu, or highlight the row in the grid and click **Edit** at the top of the grid.
2. On the Enrollment RegEx dialog, in the *RegEx* field, enter a regular expression against which to validate the subject part. See Regular Expressions on page 375 for examples.
3. In the *Error* field, enter an error message to be displayed to the user in the enrollment pages of the Keyfactor Command Management Portal or as a response to an enrollment API request when the subject part referenced in the CSR or entered for a PFX does not match the regular expression defined for the subject part field. Note that the error message already includes the subject part followed by a colon (e.g. *Organization:* or *Invalid O provided*: depending on the interface). Your custom message follows this.
4. Click **Save** to save the regular expression.

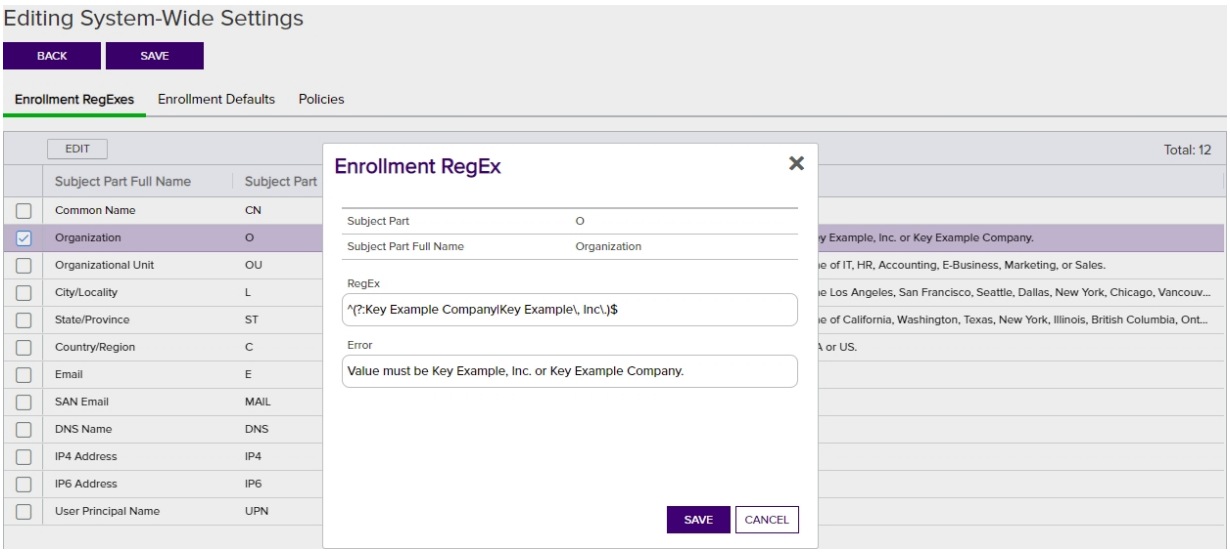


Figure 211: Configure System-Wide Enrollment Regular Expressions

Tip: To prevent users from adding a given SAN field to a certificate, create a regular expression on the field with the following value:

```
^$
```

This will disallow entry of any data in the SAN field and thus prevent users from submitting the certificate request with this SAN.

Enrollment Defaults Tab

Enrollment defaults allow you to define default values for select certificate subject parts that will auto-populate on the PFX enrollment and CSR generation pages in the Keyfactor Command Management Portal.

To configure a system-wide enrollment default:

1. On the Enrollment Defaults tab, double-click a subject part row in the enrollment defaults grid, right-click the row and choose **Edit** from the right-click menu, or highlight the row in the grid and click **Edit** at the top of the grid.

2. On the Enrollment Default dialog, in the *Value* field, enter a value to auto-populate in the PFX enrollment and CSR generation pages of the Keyfactor Command Management Portal. During PFX enrollment or CSR generation, the user can accept the value or modify it; it is not enforced.

3. Click **Save** to save the default.

Note: System-wide Enrollment defaults do not apply to requests made with CSR enrollment or the Keyfactor API.

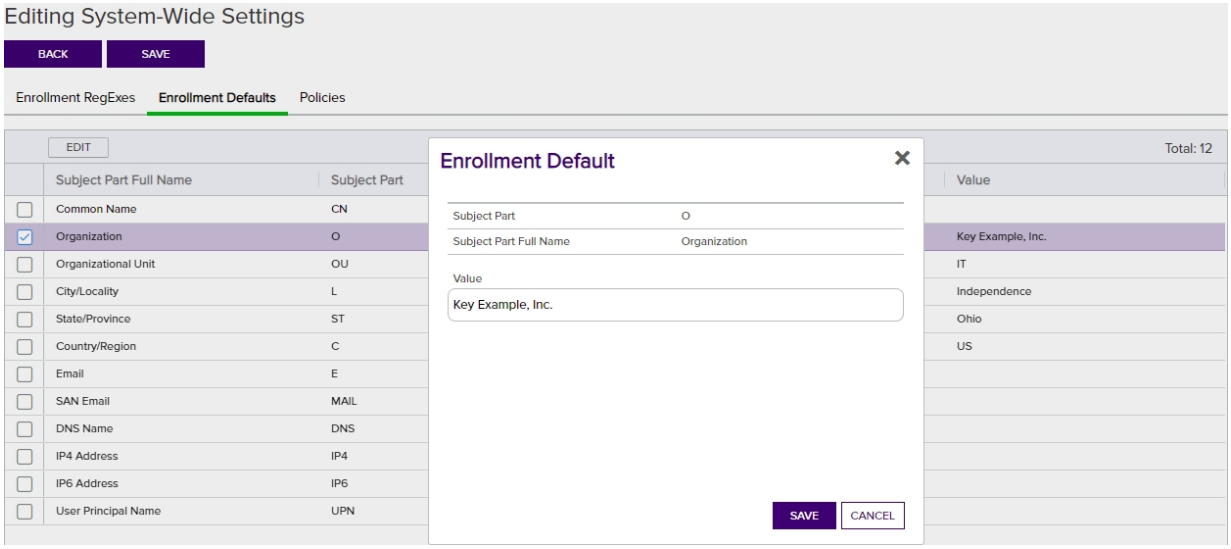


Figure 212: Configure System-Wide Enrollment Defaults

Tip: See also the *Subject Format* application setting, which takes precedence over enrollment defaults at both the system-wide and template level (see Application Settings: Enrollment Tab on page 591 in the *Keyfactor Command Reference Guide*).

Policies Tab

Policies for templates cover the following settings:

Enrollment Policies:

- Allow Wildcards

  Enable this option to allow certificates to be created containing wildcards (e.g. *.keyexample.com). The default is enabled.

- Allow Public Key Reuse

  Enable this option to allow public keys to be reused on certificate renewals. The default is enabled.

- Enforce RFC 2818 Compliance

  Enable this option to force certificate enrollments made through Keyfactor Command to include at least one DNS SAN. In the Keyfactor Command Management Portal, this causes the CN entered in PFX enrollment to automatically be replicated as a DNS Name SAN, which will be

set to *Read Only*. For CSR enrollment, if the CSR does not have a SAN that matches the CN, one will automatically be added to the certificate if this is set. The default is disabled.

> **Tip:** For CA gateways, some cloud providers will automatically include SANs without you needing to enable the **Enforce RFC 2818 Compliance** option. Some cloud providers won't support submission of a SAN that matches the CN (which is the default when you enable the RFC 2818 option). Keyfactor recommends disabling this option for CA gateways.

Supported Key Types:

- RSA Key Sizes

  A list of RSA key sizes that are valid for enrollment through Keyfactor Command. If a key size is not in this list, enrollment will not be supported for requests specifying that key size. To change the selected values, in the dropdown uncheck any values you do not wish to support. The default values are:

  ```
  1024, 2048, 4096
  ```

- ECC Curves

  A list of elliptic curve algorithms that are valid for enrollment through Keyfactor Command. To change the selected values, in the dropdown uncheck any values you do not wish to support. The default values are:

  ```
  P-256/prime256v1/secp256r1, P-384/secp384r1, P-521/secp521r1
  ```

- Allow Ed448 / Allow Ed25519

  Set global template values for allowing Ed448 and Ed25519 keys. Templates that utilize Ed448 or Ed25519 key types can be imported into Keyfactor Command. These key types are only available with EJBCA CAs. Default is disabled.

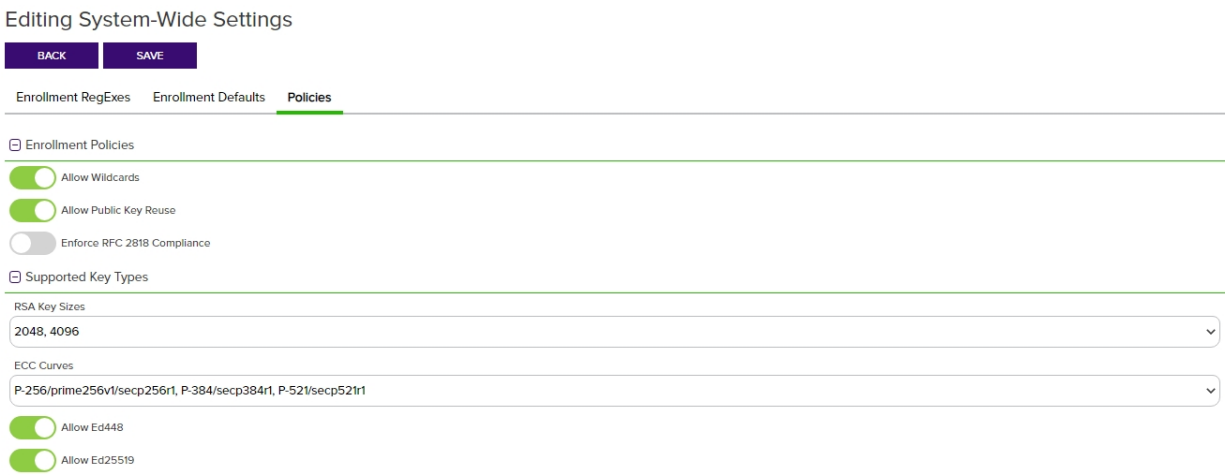


Figure 213: Configure System-Wide Policies

Configuring Template Options

The options configured in templates relate to how they appear and function for PFX and CSR enrollment in the Management Portal.

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:
Certificate Metadata Types: *Modify*
PKI Management: *Read*
PKI Management: *Modify*

To configure template options:

1. In the Keyfactor Command Management Portal, browse to *Locations* > *Certificate Templates*.
2. On the Certificate Templates page, double-click the template, right-click the template and choose **Edit** from the right-click menu, or highlight the row in the template grid and click **Edit** at the top of the grid.
3. When you open the certificate template for editing, you will see several tabs. Complete the template information with the appropriate data using the following instructions.
4. Click **Save** to save the changes to the template record. Click **Back** to return to the main certificate templates page without saving changes.

Details Tab

The information in the *Details* section is for reference and cannot be edited. This includes:

- **Template Short Name**—The common name of the template. This name typically does not contain spaces.
- **Template Display Name**—The display name of the template.

- **Key Size**—The minimum supported key size of the template.
- **OID**—For a Microsoft certificate template, the object ID of the template retrieved from Active Directory. For an EJBCA certificate template, this field is generated within Keyfactor Command as an object identifier, but does not follow official OID conventions.
- **Curve**—For ECC templates, the elliptic curve algorithm defined for the certificate template.

In the *Friendly Name* section, enter a **Friendly Name**, if desired. Template friendly names, if configured, appear in template selection dropdowns in place of the template short names. This can be useful in environments where the template short names are long or not very human readable. This setting is not required to enable enrollment or configure private key retention.

In the *Allowed Enrollment Types* section, click the toggle buttons to enable the options for **CSR Enrollment**, **PFX Enrollment** and/or **CSR Generation** as desired. Enabling these options causes the template to appear in dropdowns in the corresponding section of the Management Portal. In the case of CSR Enrollment and PFX Enrollment, the templates only appear in dropdowns on the enrollment pages if they are available for enrollment from a CA also configured for enrollment within Keyfactor Command (see Adding or Modifying a CA Record on page 330).

In the *Private Key Retention* section, click the toggle button to enable **Private Key Retention**, if desired, and select the retention type in the dropdown. Enter the number of days, weeks, months, or years to keep the encrypted private key stored in the Keyfactor Command database based on the type selected, then select the desired time frame (Day(s), Week(s), Month(s), or Year(s)). You will not have the option to choose a retention timeframe if you choose **Indefinite**.

Configuring private key retention allows the private keys for certificates enrolled through Keyfactor Command to be stored, encrypted, in the Keyfactor Command database for a user-definable period of time.

Important: Any templates that are configured on the Microsoft CA Issuance Requirements tab for CA certificate manager approval cannot be used for PFX enrollment and associated pending, issued, and denied alerting in Keyfactor Command without configuring private key retention. Edit the template in Keyfactor Command, and on the Details tab check the Private Key Retention box. Set the dropdown to some value other than blank and for retention options of *After Expiration* or *From Issuance*, enter a value for the number of days, weeks, months or years to retain the private key. Without this setting, the template will not display on the template dropdown during PFX enrollment.

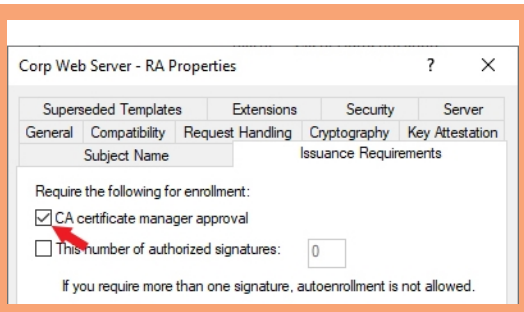


Figure 214: Microsoft Issuance Requirements on a Template for Manager Approval

Note: This does not apply to certificate requests requiring approval at a Keyfactor Command workflow level.

The private key retention configuration options are:

- Blank

  The private key will not be retained if the box is unchecked, or the *blank* option is selected.
- Indefinite

  The private key will be retained until it is explicitly deleted.
- After Expiration

  The private key will be retained until the specified number of days, weeks, months or years after the certificate expires, at which point it will be scheduled for deletion.
- From Issuance

  The private key will be retained until the specified number of days, weeks, months or years after the date on which the certificate was issued, at which point it will be scheduled for deletion.

Note: When the retention period is stored in the database, weeks are converted to 7 days, months are converted to 30 days, and years are converted to 365 days.

Tip: Setting the retention period to 0 will cause the private keys to be purged by the private key clean up job when it next runs, after the certificate expires or after the certificate is issued.

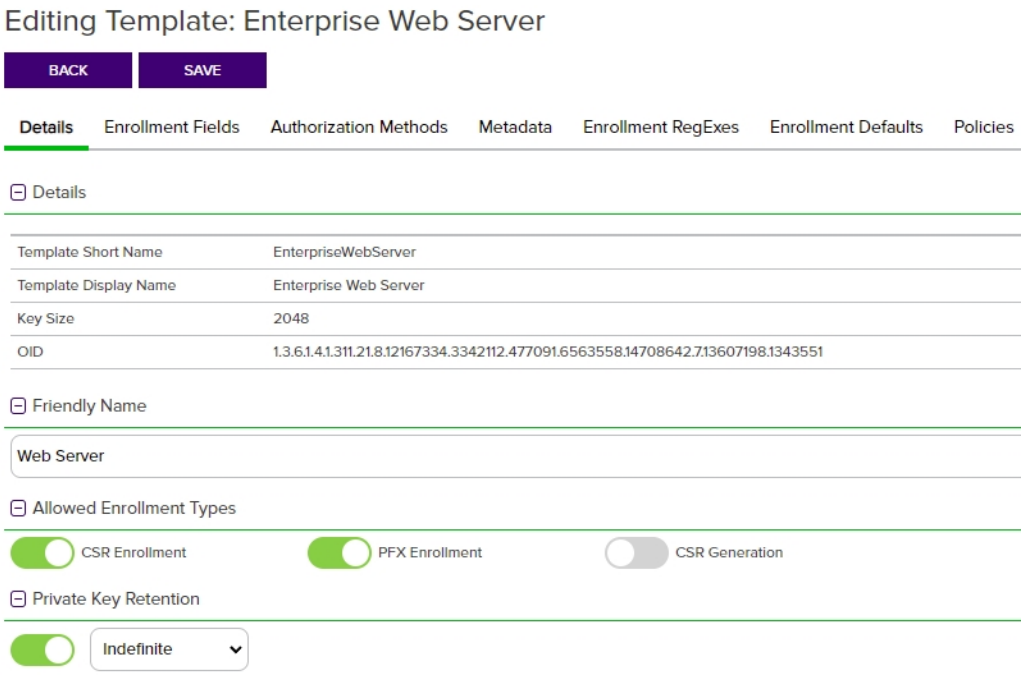


Figure 215: Certificate Template: Details Tab for a Microsoft Template

Enrollment Fields Tab

On the Enrollment Fields tab, you can add custom enrollment fields. These are configured on a per-template basis to allow you to submit custom fields with CSR enrollments and PFX enrollments to supply custom request attributes to the CA during the enrollment process. This functionality offers such benefits as:

- Preventing users from requesting invalid certificates, based on your specific certificate requirements per template.
- Providing additional information to the CA with the request.

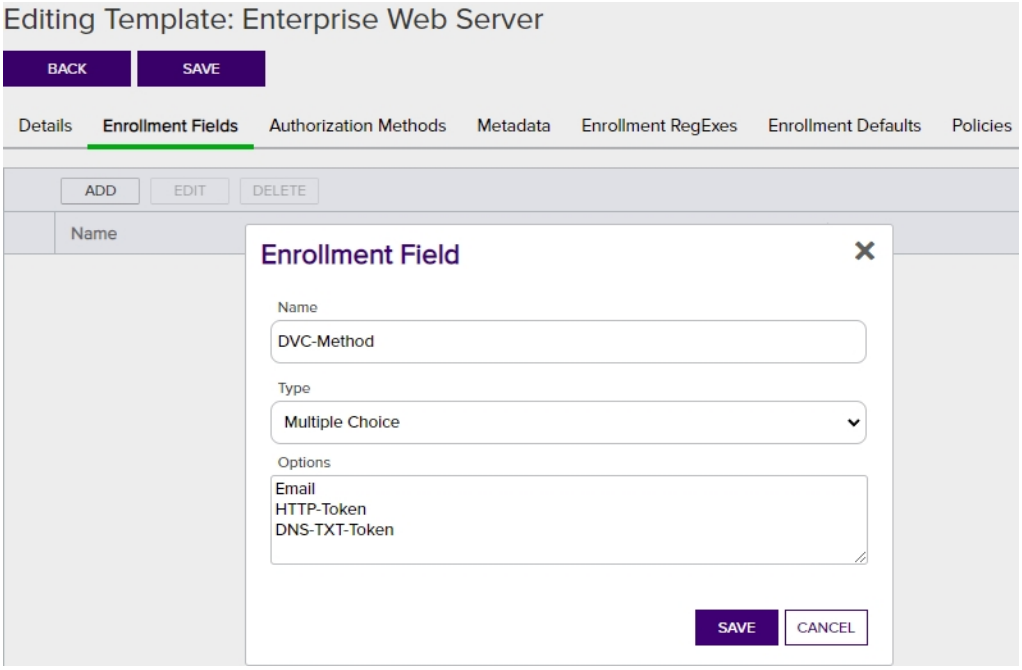


Figure 216: Configure Template: Enrollment Fields Tab

Once created on the template, these values are shown in Keyfactor Command on the PFX and CSR enrollment pages in the *Additional Enrollment Fields* section. The fields are mandatory during enrollment. The data will appear on the CA / Issued Certificates attribute tab for certificates enrolled with a template configured with Keyfactor Command enrollment fields.

Note: These are not metadata fields, so they are not stored in the Keyfactor Command database, but simply passed through to the CA. The CA in turn could, via a gateway or policy module, use this data to perform required actions.

On the Enrollment Fields tab you can add, edit and delete enrollment fields.

To add a new enrollment field:

1. On the **Enrollment Fields** tab of the selected template click **Add**. If there are existing fields configured they will appear in a list on this tab.
2. Enter a **Field Name** for the new custom field. This name will appear on the enrollment pages.
3. Select a **Parameter Type**. The options are:
    - **String**: A free-form data entry field.

- **Multiple Choice**: Provides a list of acceptable values for the field. A text box will open up below this choice for you to enter the list of acceptable values. Add each value on a separate line. Click **OK** to close the box.

4. Click **Save** to save and close the add window.

Authorization Methods Tab

The **Restrict Allowed Requesters** option is used to select Keyfactor Command security roles that a user must belong to in order to successfully enroll for certificates in Keyfactor Command using this template. This is typically used for EJBCA templates and Microsoft templates that are not in the local Active Directory forest, since in these cases, Keyfactor Command cannot make use of the access control model of the CA itself to determine which users can enroll for certificates; this setting replaces that functionality. This setting is similar to setting *request certificates* for the selected security roles at the template level on a Microsoft CA. For multi-forest environments, this setting should be used on any templates from forests other than the Keyfactor Command forest that will be used for enrollment regardless of the type of trust between the forests, including two-way trusts.

> **Tip:** In addition to granting permissions at the template level, you may need to enable the **Restrict Allowed Requesters** option to grant permissions at the CA level (see Adding or Modifying a CA Record on page 330). This is generally only required for untrusted CAs (including CAs in a forest with a one-way trust with the forest in which the Keyfactor Command server is located), but may be needed for CAs in a forest with a two-way trust with the Keyfactor Command forest depending on the security configuration in the environment.

On the Authorization Methods tab you can add, edit and delete allowed requesters.

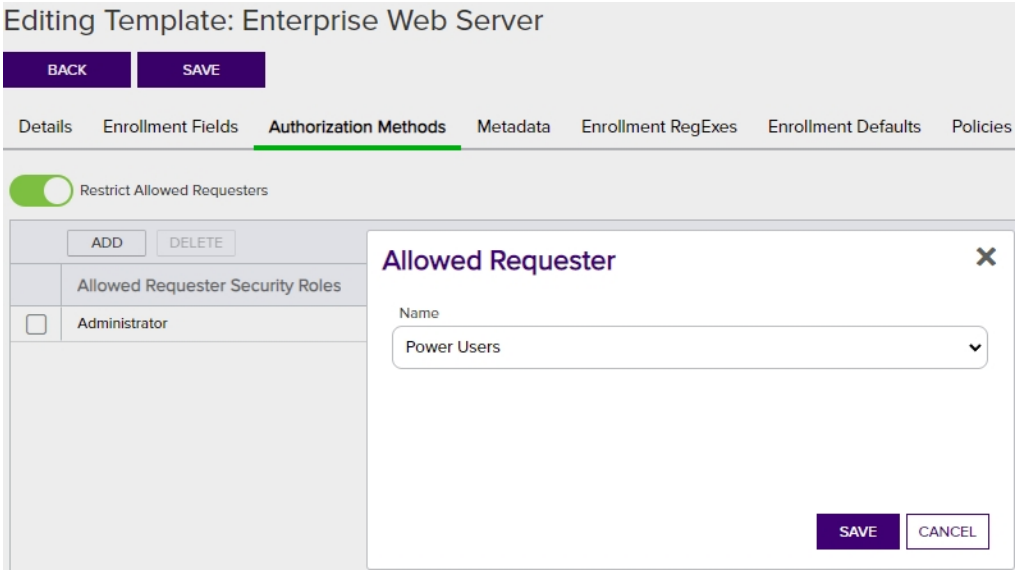


Figure 217: Certificate Template: Authorization Methods Tab

To add a new allowed requester, click to toggle the **Restrict Allowed Requesters** button and:

1. On the **Authorization Methods** tab of the selected template click **Add**. If there are existing requesters configured, they will appear in a list on this tab.
2. In the Security Role dropdown, select a Keyfactor Command security role (see Security Roles and Identities on page 609) to grant enrollment permissions on the template.
3. Click **Save** to save and close the add window.

Metadata Tab

From the **Metadata** tab you can:

- View the metadata field settings for that specific template.
- Configure how (or whether) the metadata fields will appear during enrollment for that specific template.

System-wide metadata fields are defined in System Settings (see Certificate Metadata on page 646). Once the system-wide metadata has been defined, the **Enrollment Handling** setting can be configured on a template-specific basis, potentially overriding a system-wide *required, hidden or optional* setting for *that metadata field* on *that template*, causing only the set of fields configured for the template to appear on the PFX and CSR enrollment pages when the template is selected, and determining if they are required or optional.

Tip: This allows an administrator to apply *required, hidden or optional* settings to a metadata field on a per-template basis so that only certain metadata fields appear on certain templates. For example, if metadata fields A and B are set to *required* or *optional*

and Metadata field C is set to *hidden* for the WebServer template, only A and B will appear during enrollment with that template.

A default value for a metadata field can also be configured that is different from, and overrides, the default value entered for the system-wide metadata field. For string metadata fields, a regular expression validation and error message can also be configured on a template-specific basis. The order in which the metadata fields appear can be changed globally (see Sorting Metadata Fields on page 651).

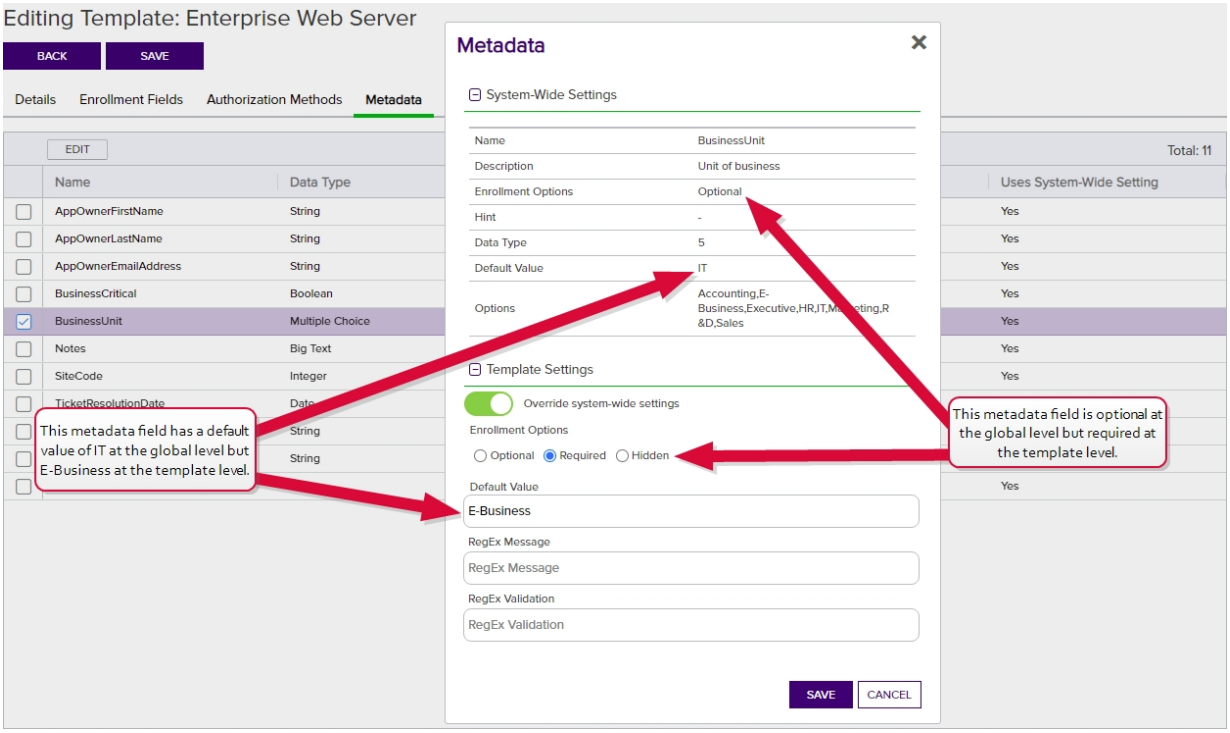


Figure 218: Certificate Template: Metadata Tab

The Metadata grid columns can be sorted by clicking the column heading (except Default Value). The columns are:

- **Name**: The name of the metadata field.
- **Data Type**: The metadata field type: *String, Integer, Date, Boolean, Multiple Choice, or Big Text*.
- **Enrollment Handling**: The handling of the metadata field during enrollment*: Optional, Required or Hidden*.
- **Default Value**: The default value during enrollment, if there is one, will be displayed.

- **Uses System-Wide Settings**: Displays *Yes* if system-wide settings are in effect for this template, or *No* if template-specifc settings are in effect.

To configure metadata fields for a template:

1. On the Metadata tab, double-click a row in the metadata grid, right-click the row and choose **Edit** from the right-click menu, or highlight the row in the grid and click **Edit** at the top of the grid.
2. In the Metadata dialog in the *System-Wide Settings* section, review the existing system-wide settings for the metadata field.
3. In the *Template Settings* section, click to toggle the **Override system-wide settings** button. Configure the template-level settings for the metadata field. The available fields will vary depending on the type of the metadata field and may include:
    - Choose the *Enrollment Options* for this template by selecting the appropriate radio button:
        a. **Optional**: The metadata field will appear during enrollment with this template, but it will not be required to complete enrollment.
        b. **Required**: This field will be required in order to complete enrollment with this template.
        c. **Hidden**: This field will not be displayed during enrollment with this template.
    - Set the *Default Value* if desired. If no default value is desired, the field may be left blank. For Multiple Choice type metadata fields, this field will appear as a dropdown where you can select from the existing values configured for the metadata field.
    - If desired, set a *RegEx Message* and *RegEx Validation* string specific to the template used to validate the value upon enrollment entry, and any error message to display if the entry does not match the regex definition. For more information, see Adding or Modifying a Metadata Field on page 646. This option is supported for string type metadata fields.
4. Click **Save** on the Metadata dialog to save changes for each metadata field.

Enrollment Regexes Tab

Enrollment Regexes can be applied at either the template-specifc level or system-wide level. Template-level regular expressions are used to validate that the certificate subject data entered on the CSR enrollment, CSR generation, and PFX enrollment pages meets certain criteria. Template-level regular expressions differ from system-wide regular expressions (see Configuring System-Wide Settings on page 355) as they apply on a per-template basis, rather than system-wide. In the case of a conflict in a regular expression between system-wide and template-level definitions, the template-level regular expression takes precedence.

Tip: To use a system-wide enrollment regular expression for a subject part and allow a specific template to bypass that regular expression, you can configure a template-level regular expression for the desired subject part and set it to no value.

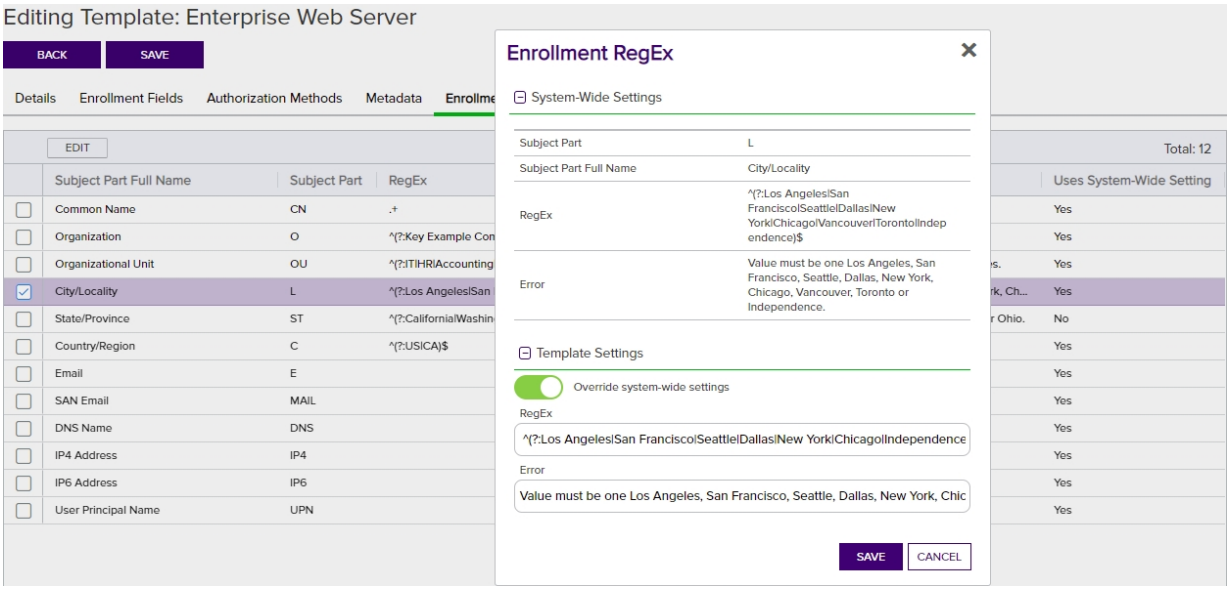


Figure 219: Certificate Template: Enrollment RegExesTab

The Enrollment Regexes grid columns can be sorted by clicking the column heading (except Regex and Error). The columns are:

- **Subject Part Full Name**: The descriptive name of the certificate subject part (e.g. Common Name).
- **Subject Part**: The code for the certificate subject information part. For instance, CN=Common Name.
- **RegEx**: The regular expression to apply to the subject part.
- **Error**: The error message to display (upon **Save** when enrolling), when the entry does not meet the specified criteria.
- **Uses System-Wide Settings**: Displays **Yes** if system-wide settings are in effect for this template, or *No* if template-specifc settings are in effect.

To configure template regular expression fields for a template:

1. On the Template Regexes tab, double-click a row in the regular expression grid, right-click the row and choose **Edit** from the right-click menu, or highlight the row in the grid and click **Edit** at the top of the grid.

2. In the Enrollment RegEx dialog in the *System-Wide Settings* section, review the existing system-wide settings for the subject part.
3. In the *Template Settings* section, click to toggle the **Override system-wide settings** button. Enter a regular expression in the **RegEx** field. See Regular Expressions on page 375 for examples.
4. In the **Error** field enter the error message to display during enrollment if the data entered for the subject part does not meet the validation rule.
5. Click **Save** on the Enrollment RegEx dialog to save each template-level regular expression.

The regular expressions will be applied at the time of enrollment. Entries which do not match the regular expression requirements will be flagged with an error message during enrollment entry when you click **Enroll** (or **Generate** for CSR generation).

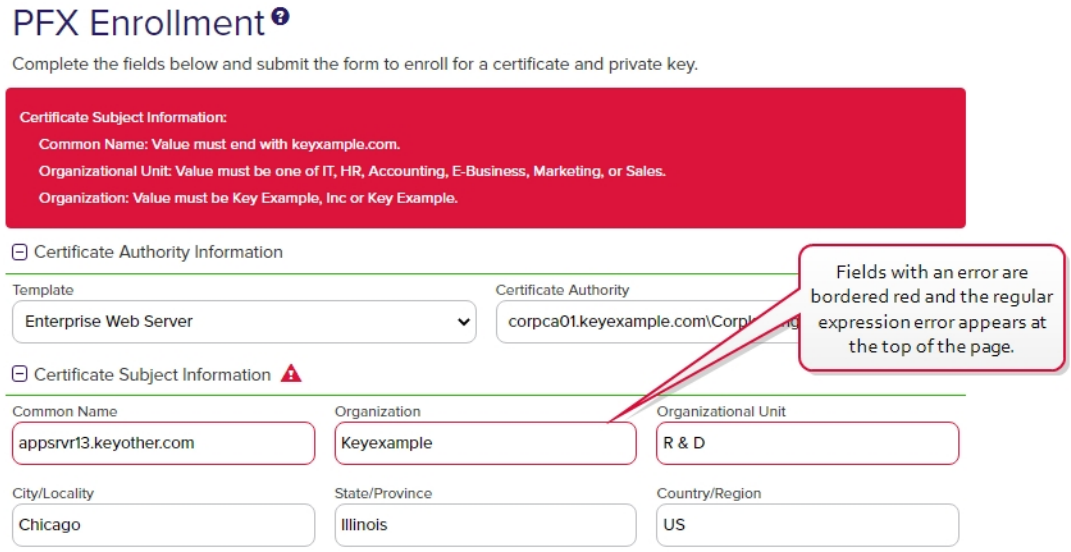


Figure 220: Certificate Template: Template Regular Expression Error on Enrollment

Tip: To prevent users from adding a given SAN field to a certificate, create a regular expression on the field with the following value:

```
^$
```

This will disallow entry of any data in the SAN field and thus prevent users from submitting the certificate request with this SAN.

Enrollment Defaults Tab

Template-level enrollment defaults allow you to define default values for certificate subject parts that will auto-populate on the PFX enrollment and CSR generation pages in the Keyfactor Command Management Portal. Template-level default values differ from system-wide default

values (see Configuring System-Wide Settings on page 355) as they apply on a per-template basis, rather than system-wide. In the case of a conflict in a default value between system-wide and template-level definitions, the template-level default values takes precedence.

Note: These default values will not be applied to the additional SANs fields in CSR Enrollment.

Tip: To use a system-wide enrollment default value in a subject part and allow a specific template to bypass that default value, you can configure a template-level default value for the desired subject part and set it to no value.

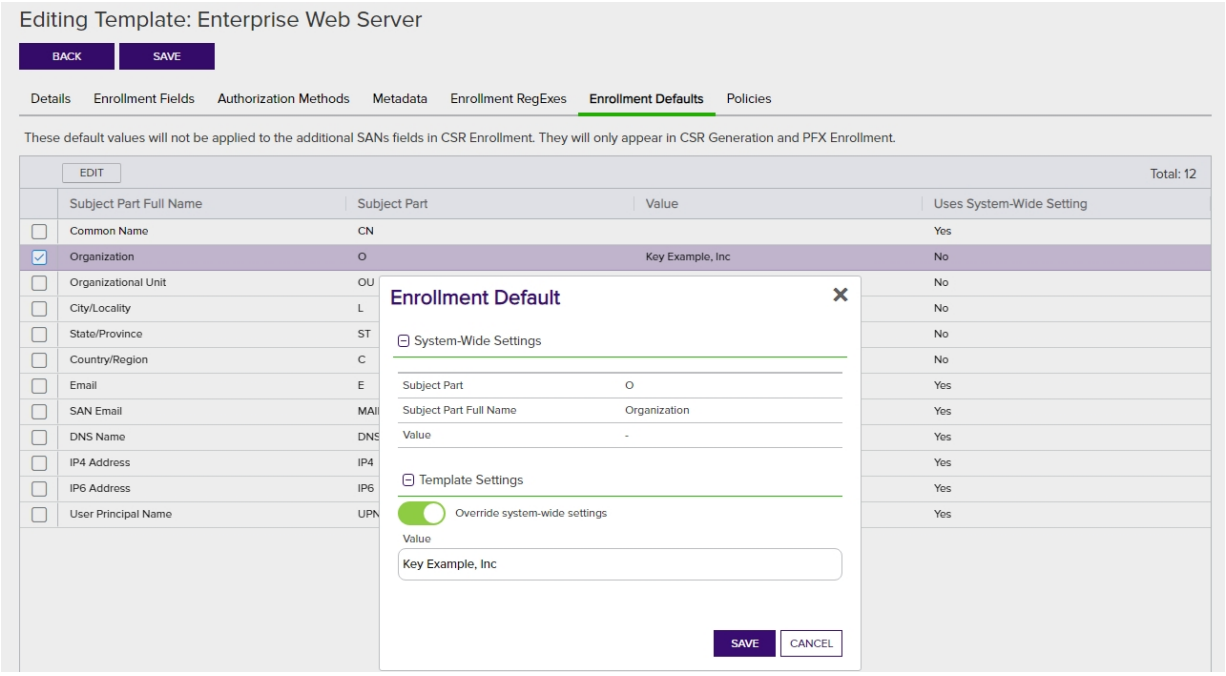


Figure 221: Certificate Template: Enrollment Defaults Tab

The Enrollment Defaults grid columns can be sorted by clicking the column heading (except Value). The columns are:

- **Subject Part Full Name**: The descriptive name of the certificate subject part (e.g. Common Name).
- **Subject Part**: The code for the certificate subject information part. For instance, CN=Common Name.
- **Value**: The default value to apply to the subject part.

- **Uses System-Wide Settings**: Displays **Yes** if system-wide settings are in effect for this template, or *No* if template-specific settings are in effect.

To configure template-level default values for a template:

1. On the Enrollment Defaults tab, double-click a row in the defaults grid, right-click the row and choose **Edit** from the right-click menu, or highlight the row in the grid and click **Edit** at the top of the grid.
2. In the Enrollment Default dialog in the *System-Wide Settings* section, review the existing system-wide default value for the subject part.
3. In the *Template Settings* section, click to toggle the **Override system-wide settings** button. Enter a template-level default value for the subject part in the **Value** field.
4. Click **Save** on the Enrollment Default dialog to save each template-level default.

Note: Enrollment defaults do not apply to requests made with CSR enrollment or the Keyfactor API.

Tip: See also the *Subject Format* application setting, which takes precedence over enrollment defaults at both the system-wide and template level (see Application Settings: Enrollment Tab on page 591 in the *Keyfactor Command Reference Guide*).

Policies Tab

The Policies Tab allows you to set template-level policy definitions which take precedence over system-wide settings (see Configuring System-Wide Settings on page 355).

The **Enrollment Policies** section displays the *System-Wide Setting* (*Yes* or *No*) for each of the template enrollment policies and allows you to **Override System-Wide Setting** for the specific template. Enabling **Override System-Wide Setting** will cause the system setting is to be disregarded and allow you to enable or disable the setting for that policy on the template. **Override System-Wide Setting** does not automatically set the policy to the opposite, the selection on the policy (enabled/disabled) will supersede any other settings.

- Allow Wildcards

  Enable this option to allow certificates to be created containing wildcards (e.g. *.keyexample.com) using this template.
- Allow Public Key Reuse

  Enable this option to allow private keys to be reused on certificate renewals made using this template.
- Enforce RFC 2818 Compliance

  Enable this option to force certificate enrollments made through Keyfactor Command for this template to include at least one DNS SAN. In the Keyfactor Command Management Portal, this

causes the CN entered in PFX enrollment to automatically be replicated as a SAN, which the user can either change or accept. For CSR enrollment, if the CSR does not have a SAN that matches the CN, one will automatically be added to the certificate if this is set.

Tip: For CA gateways, some cloud providers will automatically include SANs without you needing to enable the **Enforce RFC 2818 Compliance** option. Some cloud providers won't support submission of a SAN that matches the CN (which is the default when you enable the RFC 2818 option). Keyfactor recommends disabling this option for CA gateways.

The **Supported Key Types** section displays the *System-Wide Setting* (*value* or *Yes*/*No*) for the supported key type and allows you to Override System-Wide Setting for the specific template. Enabling **Override System-Wide Setting** will cause the system-wide setting is to be disregarded, enable the settings field, and allow you to select the setting for that policy on the template. **Override System-Wide Setting** does not automatically set the policy to the opposite, the selection on the policy (values or enabled/disabled) will supersede any other settings. Depending on the type of template selected, one of these settings will be available for configuration:

RSA Key Sizes

A list of RSA key sizes that are valid for enrollment through Keyfactor Command for this template. If a key size is not in this list, enrollment will not be supported for requests specifying that key size. To change the selected values, in the dropdown check any values you wish to support. The available values are: 1024, 2048, 4096

ECC Curves

A list of elliptic curve algorithms that are valid for enrollment through Keyfactor Command for this template. To change the selected values, in the dropdown check any values you wish to support. The available values are: P-256/prime256v1/secp256r1, P-384/secp384r1, P-521/secp521r1

Allow Ed448 for Template / Allow Ed25515 for Template

Enable or disable allowing Ed448 or Ed25519 keys on the template.

Note: When enrolling with the template, the key size of the request is validated against the template key size. This allows for a key size to be set on a template in Keyfactor Command for validation purposes that can be different than the CA template key size setting. Care should be taken to make sure any template policy settings take into consideration CA template key size settings so that errors do not occur at the CA level.

- If a CSR Enrollment request is made with a key size that is not valid, per the template policy settings, an error will be displayed when you click the **Enroll** button (for example, the CSR has a key size of 2048 but the template policy supports only 4096).
- For PFX Enrollment, the request will contain the minimum settings from the Keyfactor Command presiding template settings.

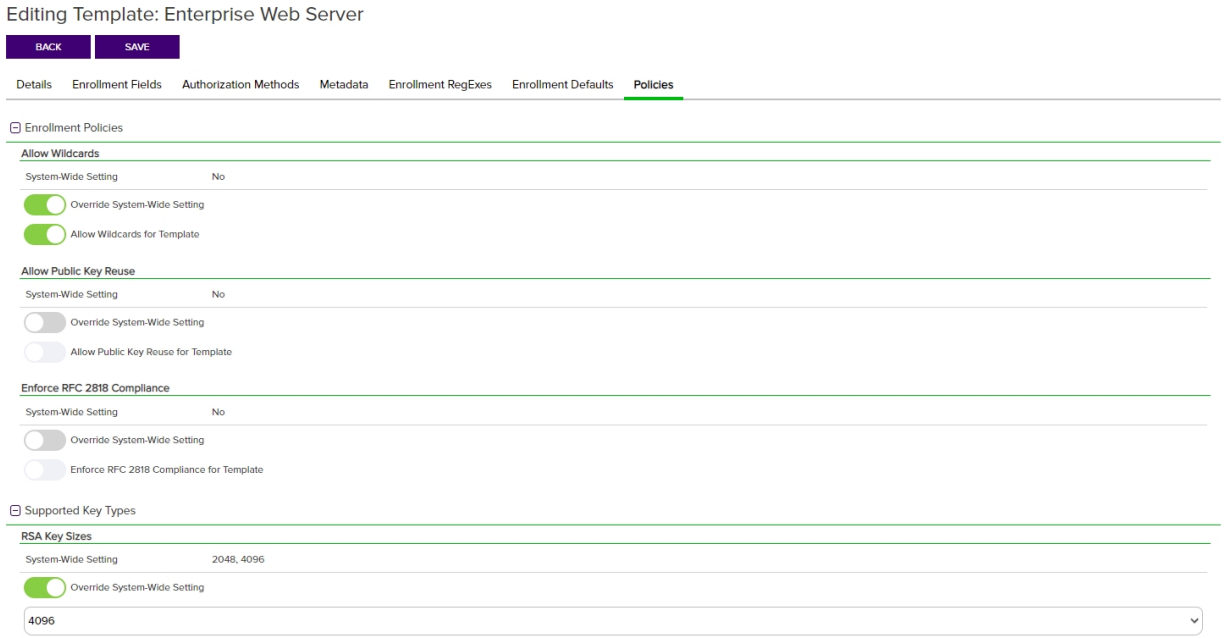


Figure 222: Certificate Template: Policies Tab

Tip: Templates that are configured for CA-level key archiving are not supported for enrollment done through Keyfactor Command. For a Microsoft CA, this is the "Archive subject's encryption private key" setting on the template. For an EJBCA CA, this is the "Key Recoverable" setting on the end entity profile, which only appears if key recovery has been enabled in system configuration. An error similar to the following on enrollment is an indication that a Microsoft template is configured to archive the private key:

```
The request is missing a required private key for archival by the server.
```

For enrollments done through Keyfactor Command for either Microsoft or EJBCA CAs, use Keyfactor Command private key retention (see Details Tab on page 360).

Viewing Template Certificates

To view the certificates in the Keyfactor Command database for a given template, highlight the template in the grid and click **View Certificates** at the top of the grid or right-click the template and choose **View Certificates** from the right-click menu. This will take you to the certificate search page with the query field populated by the selected template (see Certificate Search Page on page 32).

You can save the search as a certificate collection at that point if desired (see Saving Search Criteria as a Collection on page 40).

Regular Expressions

Several fields on the CSR enrollment, CSR generation, and PFX enrollment pages support using regular expressions to validate that the data entered in the fields meets certain criteria. Both certificate subject fields and metadata string fields can be configured with regular expressions. The certificate subject fields that support regular expressions are shown in Table 15: Supported Regular Expressions for Enrollment with Examples.

Regular expressions for enrollment can be defined at a global level to apply to all enrollments and at a template level to apply only to enrollments done with that template. Template-level definitions take precedence over global definitions.

Both the regular expressions that do the validation and the error message that the user receives when the validation fails are user definable. For example, for the common name field you could define a regular expression similar to the following:

```
^[a-zA-Z0-9'_\.\-]*\.keyexample\.com$
```

This regular expression specifies that the data entered in the field must consist of some number of characters in the first portion of the field made up only of lowercase letters, uppercase letters, numbers, apostrophes, underscores, periods, and/or hyphens followed by exactly *.keyexample.com*. Using this regular expression would prevent users from requesting certificates with common names such as myserver.contoso.com, forcing them to request certificates for domain names that are valid for your organization. Your error message to the user in this case might be something like:

```
Common names must end with keyexample.com.
```

The error message to the user appears immediately once the user leaves the field being validated after entering data that doesn't meet the regular expression requirements.

Table 15: Supported Regular Expressions for Enrollment with Examples

Subject Part	Example

CN (Common Name)	This regular expression specifies that the data entered in the field must consist of some number of characters in the first portion of the field made up only of lowercase letters, uppercase letters, numbers, apostrophes, underscores, periods, and/or hyphens followed by exactly *.keyexample.com*:
	`^[a-zA-Z0-9'_\.\-]*\.keyexample\.com$`
	The default value for the Common Name regular expression is:
	`.+`

Subject Part	Example
	This requires entry of at least one character in the Common Name field in the enrollment pages.
O (Organization)	This regular expression requires that the organization name entered in the field be one of “Key Example Inc”, “Key Example” or “Key Example Inc.”: `^(?:Key Example Inc|Key Example|Key Example, Inc\.)$` The period in the final company name (Key Example, Inc.) needs to be escaped in the regular expression with a slash (”\”) but the comma does not.
OU (Organization Unit)	This regular expression requires that the organizational unit entered in the field be one of these four departments: `^(?:IT|HR|Accounting|E-Commerce)$`
L (City/Locality)	This regular expression requires that the city entered in the field be one of these five cities: `^(?:Boston|Chicago|New York|London|Dallas)$`
ST (State/Province)	This regular expression requires that the state entered in the field be one of these eight states: `^(?:Massachusetts|Illinois|New York|Ontario|Texas)$`
C (Country)	This regular expression requires that the country entered in the field be either US or CA: `^(?:US|CA)$`
E (Email)	This regular expression specifies that the data entered in the field must consist of some number of characters prior to the “@” made up only of lowercase letters, uppercase letters, numbers, apostrophes, underscores, periods, and/or hyphens followed by exactly “@keyexample.com”: `^[a-zA-Z0-9'_\.\-]*@keyexample\.com$`
DNS (Subject Alternative Name: DNS Name)	This regular expression specifies that the data entered in the field must consist of some number of characters in the first portion of the field made up only of lowercase letters, uppercase letters, numbers, apostrophes, underscores, periods, and/or hyphens followed by exactly either “.keyexample1.com” or “.keyexample2.com”: `^[a-zA-Z0-9'_\.\-]*\.(?:keyexample1\.com|keyexample2\.com)$`

Subject Part	Example

IPv4 (Subject Alternative Name: IPv4 Address)	This regular expression specifies that the data entered in the field must be exactly "130.101." followed by anywhere between 1 and 3 numbers followed by exactly "." followed by anywhere between 1 and 3 numbers:
	`^130\.101\.(?:[0-9]{1,3})\.(?:[0-9]{1,3})$`
	This regular expression specifies only that the IPv4 address is made up of 4 sets of between 1 and 3 numbers separated by periods:
	`^(?:[0-9]{1,3}\.){3}[0-9]{1,3}$`

IPv6 (Subject Alternative Name: IPv6 Address)	This regular expression specifies that the data entered in the field must be made up of eight sets of between one and four numbers and/or uppercase letters separated by colons: `^(?:[A-F0-9]{1,4}:){7}[A-F0-9]{1,4}$`
MAIL (Subject Alternative Name: Email)	This regular expression specifies that the data entered in the field must consist of some number of characters prior to the "@" made up only of lowercase letters, uppercase letters, numbers, apostrophes, underscores, periods, and/or hyphens followed by exactly "@keyexample.com": `^[a-zA-Z0-9'_\.\-]*@keyexample\.com$`
UPN (Subject Alternative Name: User Principal Name)	This regular expression specifies that the data entered in the field must consist of some number of characters prior to the "@" made up only of lowercase letters, uppercase letters, numbers, apostrophes, underscores, periods, and/or hyphens followed by exactly "@keyexample.com": `^[a-zA-Z0-9'_\.\-]*@keyexample\.com$`

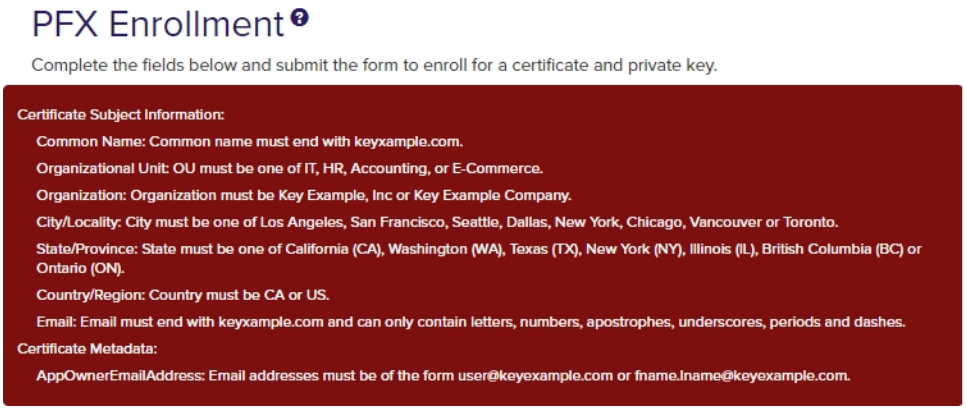


Figure 223: PFX Enrollment Regular Expression Validation Error

For more information about configuring regular expressions on metadata fields, see Certificate Metadata on page 646.

Using the Template Search Feature

The search function allows you to query the database for information. The same query structure is used in multiple locations within the Keyfactor Command Management Portal.

When you first open the page, you will see the simple search option. To execute a search, select the field and comparison operators in the dropdowns and type something on which to search in the value field (if applicable). If you select an *is null* or *is not null* comparison operator, the value field will be grayed out. Click the **Search** button to execute the query.

Each query consists of three parts:

Query Field

The available fields for querying vary depending on the area of the Management Portal in which the search is used. On this page, the queries can be done on the following built-in fields:

DisplayName

Complete or partial matches with the name of the template Display Name.

AllowedEnrollmentType

Complete or partial matches with allowed enrollment types on the template.

IsDefaultTemplate

The template is one of the Microsoft default templates (true/false). This is helpful to filter out the templates that you did/didn't create.

ConfigurationTenant

Complete or partial matches with the Configuration Tenant name.

FriendlyName

Complete or partial matches with the Keyfactor Command friendly name of the template.

ShortName

Complete or partial matches with the template Short Name.

HasPrivateKeyRetention

Private Key Retention is selected for this template (true/false).

KeyType

Complete or partial matches with the key type signing algorithm.

ForestRoot

Complete or partial matches with the forest location. NOTE: This will be deprecated in a future release and replaced with ConfigurationTenant.

Comparison Operator

The query comparison operators vary depending on the type of field selected and the specific properties of the field. The list below shows the dropdown list comparison operators, as well as the equivalent query language syntax (in parentheses).

Most string fields (the vast majority of the built-in fields) support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Contains (-contains)
- Does not contain (-notcontains)
- Starts with (-startswith)
- Ends with (-endswith)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Most date and integer fields support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Is less than (-lt)
- Is less than or equal to (-le)
- Is greater than (-gt)
- Is greater than or equal to (-ge)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Most Boolean (true/false) fields support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Comparison Value

The value you enter for comparison must match the field type. For example, integer fields only support numerical values. String fields support all alphanumeric characters. Boolean fields only support True or False. The value field is not case sensitive. Date fields support only properly formatted dates and will initially display as mm/dd/yyyy. You can choose to populate the date field by:

- Clicking in a date Value field to open a pop-up calendar to select a date that will populate the field.
- Clicking in a segment of the date format (i.e., mm/dd/yyyy) and entering a value. As you continue to type in any one segment, the cursor will keep moving onto the next segment.

The results that match your search criteria will be displayed in the results grid below the search selection options.

Advanced Searches

On any search page you can click **Advanced** to the right of the Search button to display the advanced search options. Click **Simple** to close the advanced search options again.

Multiple Criteria

Using the advanced search options, you can build a query based on multiple criteria using AND/OR logic. As with a simple search, you select a field and comparison operator in the drop-downs and

then enter a comparison value, if applicable. Click **Insert** to add the search criteria to the query field below the selection fields. Use the selection fields to build multiple search criteria. Each time you click the insert button, an AND is added between the previous search criteria and the newly added one. You can change the AND to an OR if desired. You can use parentheses around portions of the query along with AND/OR to change the query meaning.

For example, for certificate searches:

```
(CN -contains "appsrvr" AND IssuedDate -ge "01/01/2022") OR (CN -contains "appsrvr" AND
TemplateShortName -contains "web")
```

This query will return all the certificates issued on or after January 1, 2022 with the string appsrvr in the CN and also all certificates issued at any time with the string appsrvr in the CN using a template referencing web. When you have entered all the desired search criteria, click **Search** to execute the query. If you wish to clear the query field and start over, click the **Clear** button.

2.1.8.3 Certificate Stores

The certificate store feature in Keyfactor Command allows you to search for and inventory certificates from multiple types of certificate stores, import the certificates found in them into the Keyfactor Command database, add new certificates to the stores, and remove certificates from them. This feature uses Keyfactor orchestrators to communicate with the Keyfactor Command server. This section of the documentation describes the management tasks that can be done through the Management Portal. For information about installing and configuring orchestrators, see the *Keyfactor Orchestrators Installation and Configuration Guide*.

Certificate stores are managed by configuring the store locations through the Management Portal, assigning an inventory schedule, and optionally assigning stores to containers (groups) for ease of management. You can create records for stores in the Management Portal manually or by using the discovery feature (Java keystore, PEM, and F5 REST only among the built-in stores—custom modules used by the AnyAgent framework may support discovery).

Managing certificate store requires that an appropriate instance of a Keyfactor orchestrator is running in the environment and has been approved in the Management Portal (see Orchestrator Management on page 481). Java and PEM certificate stores can be managed with an instance of the Keyfactor Java Agent running on the machine where the Java and PEM certificate stores are located. Amazon Web Services (AWS), F5, File Transfer Protocol (FTP), and NetScaler certificate store can be management with the Keyfactor Universal Orchestrator[1] or Windows Orchestrator running in a network location that has access to both the Keyfactor Command server and the internet (AWS) or the FTP, F5 or NetScaler machine(s) or device(s). Managing IIS certificate stores requires an instance of the Keyfactor Universal Orchestrator or Windows Orchestrator running on a domain-joined server in the same AD forest as the IIS server(s) and the Keyfactor Command server.

Once your certificate stores have been inventoried and their certificates imported into Keyfactor Command, you can use the standard Management Portal features for managing certificates—such as

[1]Support for some of this functionality on the Keyfactor Universal Orchestrator requires the addition of a custom extension. Contact your Keyfactor representative for more information.

Expiration Alerts (see Expiration Alerts on page 161)—to manage the certificates from the certificate store locations even if the certificates were not generated by your Keyfactor Command configured CAs.

Most certificate store types can use **Privileged Access Management (PAM)** or **Keyfactor Secrets** to manage passwords on the certificate stores. Certificate store types not supported for this include PEM, IIS Personal, IIS Revoked, and IIS Trusted Roots (because these stores do not require storage of a password).

F5 and IIS Certificate Store Terminology

This section uses the following terminology for F5 and IIS certificate stores:

F5 CA Bundles REST

Certificates and keys for the *F5 CA Bundles REST* are those found within F5 *Bundles*. Note that the *ca-bundle* cannot be managed with Keyfactor Command, as it is protected and managed directly by F5. Only the *Include Bundles* may be managed with this option. This option uses the F5 iControl REST API. It is intended to be used with BIG-IP versions 13 and later. The F5 CA Bundles REST option supports certificate discovery on the F5 device and F5 high availability.

F5 SSL Profiles

Certificates and keys for the *F5 SSL Profiles* are those used by any applications configured for use by the F5 device. These are certificates that are available in the F5 interface as the SSL certificate list. This option uses the F5 SOAP API. It is intended to be used with BIG-IP version 12.

F5 SSL Profiles REST

Certificates and keys for the *F5 SSL Profiles REST* are those used by any applications configured for use by the F5 device. These are certificates that are available in the F5 interface as the SSL certificate list. This option uses the F5 iControl REST API. It is intended to be used with BIG-IP versions 13 and later. The REST version of F5 SSL Profiles supports certificate discovery on the F5 device and F5 high availability.

F5 Web Server

F5 Web Server REST

Certificates and keys for the *F5 Web Server REST* are those used by the device itself for the F5 portal and the API. This certificate is referred to as the *device certificate* within the F5 interface. This option uses the F5 iControl REST API. It is intended to be used with BIG-IP versions 13 and later. The F5 Web Server REST option supports F5 high availability.

IIS Revoked

The Untrusted Certificates store of the local computer.

IIS Trusted Roots

The Trusted Root Certification Authorities store of the local computer.

IIS Personal

The Personal store of the local computer.

Certificates and keys for the *F5 Web Server* are those used by the device itself for the F5 portal and the SOAP API. This certificate is referred to as the *device certificate* within the F5 interface. This option uses the F5 SOAP API. It is intended to be used with BIG-IP version 12.

Tip: Click the help icon (?) next to the page title to open the embedded web copy of the *Keyfactor Command Documentation Suite* to this section.
You can also find the help icon at the top of the page next to the **Log Out** button. From here you can choose to open either the *Keyfactor Command Documentation Suite* at the home page or the *Keyfactor API Endpoint Utility*.

Using the Certificate Store Search Feature

The search function allows you to query the database for information. The same query structure is used in multiple locations within the Keyfactor Command Management Portal.

When you first open the page, you will see the simple search option. To execute a search, select the field and comparison operators in the dropdowns and type something on which to search in the value field (if applicable). If you select an *is null* or *is not null* comparison operator, the value field will be grayed out. Click the **Search** button to execute the query.

Each query consists of three parts:

Query Field

The available fields for querying vary depending on the area of the Management Portal in which the search is used. On this page, the queries can be done on the following built-in fields:

Agent Available

Orchestrator has been approved and made available to manage certificate store jobs (true/false).

Agent ID

Orchestrator Id matches or doesn't match the entered GUID (primarily used for internally generated searches when the user is redirected here from another page).

Category

Certificate store matches or doesn't match the selected category—Amazon Web Services, F5 CA Bundles REST, F5 SSL Profiles, F5 SSL Profiles REST, F5 Web Server, F5 Web Server

Container

Complete or partial matches with one or more certificate store containers.

Has Inventory Scheduled

Certificate store has an inventory job scheduled (true/false).

Store Path

Complete or partial matches with the full path to a certificate store—e.g. /opt/application/mystore.crt or c:\program files\application\mystore.jks.

REST, File Transfer Protocol, IIS Personal, IIS Revoked, Java Keystore, NetScaler, or PEM File.

Client Machine

Complete or partial matches with the client machine(s) on which a store or stores may be found.

Comparison Operator

The query comparison operators vary depending on the type of field selected and the specific properties of the field. The list below shows the dropdown list comparison operators, as well as the equivalent query language syntax (in parentheses).

Most string fields (the vast majority of the built-in fields) support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Contains (-contains)
- Does not contain (-notcontains)
- Starts with (-startswith)
- Ends with (-endswith)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Most date and integer fields support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Is less than (-lt)
- Is less than or equal to (-le)
- Is greater than (-gt)
- Is greater than or equal to (-ge)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Most Boolean (true/false) fields support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Comparison Value

The value you enter for comparison must match the field type. For example, integer fields only support numerical values. String fields support all alphanumeric characters. Boolean fields only support True or False. The value field is not case sensitive. Date fields support only properly formatted dates and will initially display as mm/dd/yyyy. You can choose to populate the date field by:

- Clicking in a date Value field to open a pop-up calendar to select a date that will populate the field.
- Clicking in a segment of the date format (i.e., mm/dd/yyyy) and entering a value. As you continue to type in any one segment, the cursor will keep moving onto the next segment.

The results that match your search criteria will be displayed in the results grid below the search selection options.

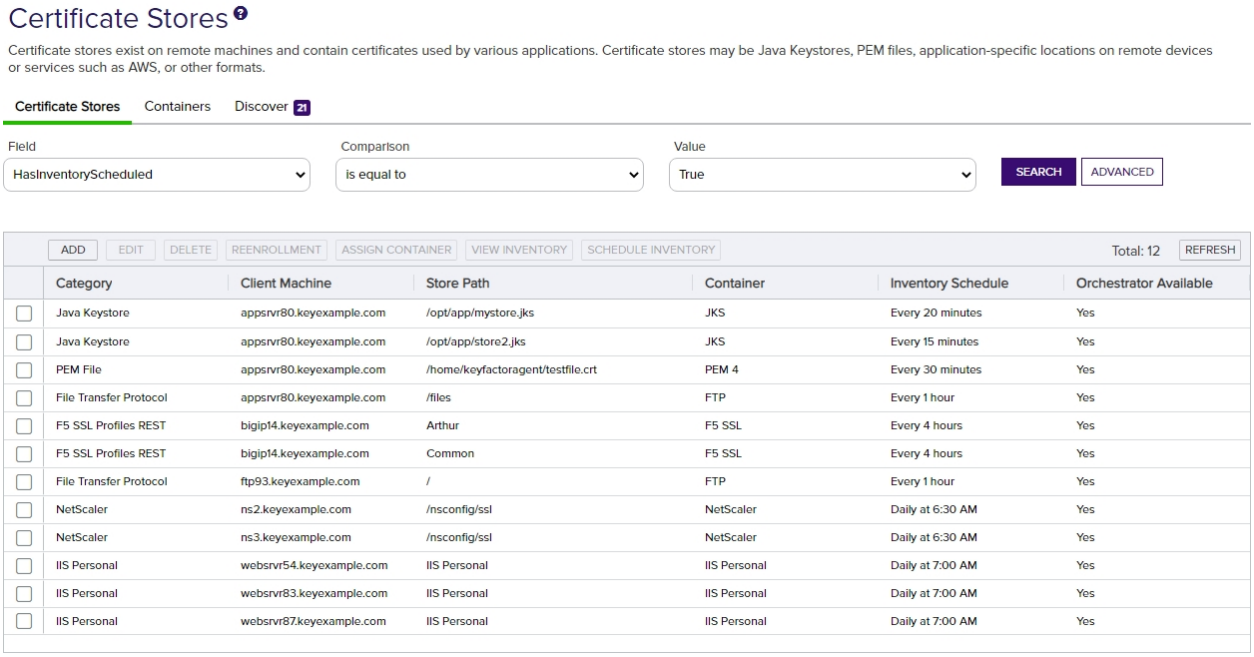


Figure 224: Simple Certificate Store Search

The search results can be sorted by clicking on a column header in the results grid for every column except Inventory Schedule and Orchestrator Available. Click the column header again to reverse the sort order. The grid columns can be arranged in any order desired by click-holding and dragging the header of the column you wish to move. The column widths may be adjusted by click-holding and dragging the line separating two column headers.

Advanced Searches

On any search page you can click **Advanced** to the right of the Search button to display the advanced search options. Click **Simple** to close the advanced search options again.

Multiple Criteria

Using the advanced search options, you can build a query based on multiple criteria using AND/OR logic. As with a simple search, you select a field and comparison operator in the drop-downs and then enter a comparison value, if applicable. Click **Insert** to add the search criteria to the query field below the selection fields. Use the selection fields to build multiple search criteria. Each time you click the insert button, an AND is added between the previous search criteria and the newly added one. You can change the AND to an OR if desired. You can use parentheses around portions of the query along with AND/OR to change the query meaning.

For example, for certificate searches:

```
(CN -contains "appsrvr" AND IssuedDate -ge "01/01/2022") OR (CN -contains "appsrvr" AND
TemplateShortName -contains "web")
```

This query will return all the certificates issued on or after January 1, 2022 with the string appsrvr in the CN and also all certificates issued at any time with the string appsrvr in the CN using a template referencing web. When you have entered all the desired search criteria, click **Search** to execute the query. If you wish to clear the query field and start over, click the **Clear** button.

Certificate Store Operations

To select a single row in the certificate store grid, click to highlight it and then select an operation from either the top of the grid or the right-click menu. The delete, schedule inventory and assign container operations can be done on multiple certificate stores at once. To select multiple rows, click the checkbox for each row on which you would like to perform an operation. Then select an operation from the top of the grid. The selected stores must all be of the same category (e.g. PEM or Java) to perform the assign container operation. The right-click menu supports operations on only one store at a time.

Adding or Modifying a Certificate Store

Before creating a certificate store in Keyfactor Command, you must approve an orchestrator to handle the store. Some orchestrators can be configured for auto-approval. See Orchestrator Auto-Registration on page 474 and Orchestrator Management on page 481.

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:
Agent Management: *Read*
Certificate Store Management: *Read*
Certificate Store Management: *Modify*

Permissions for certificate stores can be set at either the global or certificate store container level. See *Container Permissions* in the *Keyfactor Command Reference Guide* for more information about global vs container permissions.

Certificate stores can be added manually or, for some types of stores, automatically using a discover process (see Certificate Store Discovery on page 424).

Note: A user with the appropriate permissions may create more than one certificate store on a given location provided the stores are of different categories/types.

Stores of the same type should still fail to be saved using the same target

To define a new certificate store location manually or edit an existing one:

1. In the Management Portal, browse to *Locations* > *Certificate Stores*.
2. On the Certificate Stores page, select the Certificate Stores tab (the default when you first visit the page).
3. On the Certificate Stores tab, click **Add** to create a new store location, or click **Edit** from either the top or right-click menu to modify an existing one.
4. In the Certificate Stores dialog, select the type of certificate store in the **Category** dropdown. This field cannot be modified on an edit.
5. In the **Container** field, select a container into which to place the store for organization from your previously defined list, if desired. This field is optional. If no container matching the type of certificate store you are adding exists, no containers will be available in the dropdown (see Certificate Store Container Operations on page 421). Leave blank if you do not wish the certificate store to be associated with a specific store container. If you are using PAM and choose not to select a container, you will need to have created a PAM provider (see PAM Provider Configuration in Keyfactor Command on page 691) with no certificate store container in order for it to be available for selection when setting a user or password.

For an Amazon Web Services Certificate Store

- Enter the fully qualified domain name of the Keyfactor Universal Orchestrator[1] or Windows Orchestrator machine that will manage the store in the **Client Machine** field. This field cannot be modified on an edit.
- In the **Store Path** dropdown, select the region for your Amazon Web Service. This field cannot be modified on an edit.
- Click the **Set Access Key** field to enter the API access key for your web service. In the Access Key dialog, the options are Load From Keyfactor Secrets or Load From PAM Provider.
- Click the **Set Secret Key** field to enter the API secret key for your web service. In the Secret Key dialog, the options are Load From Keyfactor Secrets or Load From PAM Provider.

  A Keyfactor secret is a user-defined password or other information that is encrypted and stored securely in the Keyfactor Command database. Although Keyfactor recommends using Privileged Access Management (see Privileged Access Management (PAM) on page 677) as a more secure solution to secure information, Keyfactor Secret is an option for customers that do not already have a relationship with a PAM provider such as CyberArk or Delinea (formerly Thycotic).

[1]Support for this functionality on the Keyfactor Universal Orchestrator requires the addition of a custom extension. Contact your Keyfactor representative for more information.

Select the **Load From Keyfactor Secrets** radio button as the *Secret Source* if you want Keyfactor Command to encrypt and store the password in the Keyfactor Command database. Enter and confirm a password.

Select the **Load from PAM Provider** radio button as the *Secret Source* if you want to store the password in a supported third-party PAM solution (see Privileged Access Management (PAM) on page 677). The remaining fields on the dialog will vary depending on the PAM provider.

CyberArk

Select CyberArk in the **Providers** dropdown if your PAM provider is CyberArk. The remaining fields in the dialog will then be:

- PrivateArk Protected Password Name—The name of the username or password in the safe (see Create a CyberArk Password on page 683).
- PrivateArk Folder Name—The path and name of the folder that stores the CyberArk Password (e.g. Root or Root\MyDir).

Delinea (formerly Thycotic)

Select Delinea in the **Providers** dropdown if your PAM provider is Delinea. The remaining field in the dialog will then be:

- Delinea Secret ID—The numeric ID of the secret to retrieve from Secret Server (see Create a Delinea Secret Server Secret on page 687).

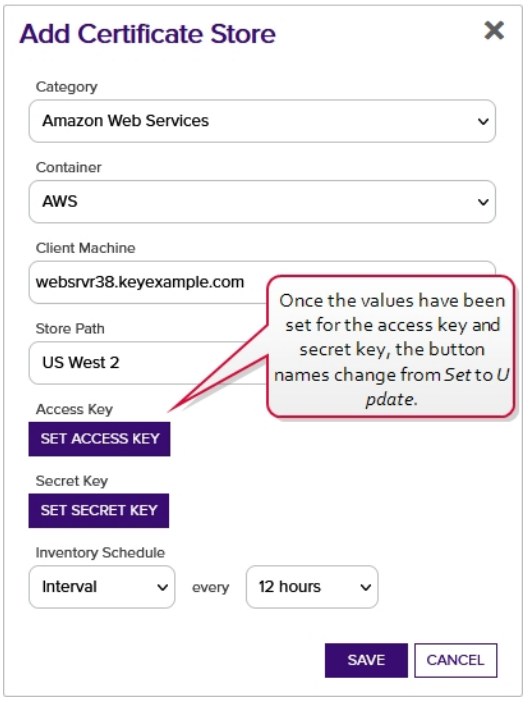


Figure 225: Add New Amazon Web Services Certificate Store

For an F5 CA Bundles REST Certificate Store

Tip: F5 CA bundle stores can be added using the certificate store discovery option rather than manually, if desired (see Certificate Store Discovery on page 424).

- Enter the fully qualified domain name of the F5 device (or F5 cluster for a high availability deployment) on which the certificate store is located in the **Client Machine** field. This field cannot be modified on an edit.
- In the **Store Path** field, enter the path to the CA bundle on the F5 device into which you want to install the certificate (e.g. /Common/myca-bundle). The Store Path name is case sensitive, so, for example, if the partition name on the F5 is *Common* it must be entered in the Store Path field as *Common* rather than *common*. This field cannot be modified on an edit.
- Select the name of the Keyfactor Universal Orchestrator[1] or Windows Orchestrator machine that will manage the stores in the **Orchestrator** dropdown. The orchestrator must be approved in order to appear here. Some orchestrators can be configured for auto-approval. See Orchestrator Auto-Registration on page 474 and Orchestrator Management on page 481.

- In the **Primary Node** field, enter the fully qualified domain name of the F5 device that acts as the primary node in a highly available F5 implementation. If you're using a single F5 device, this will often be the same value you entered in the Client Machine field.

  Tip: Configuration of the primary node is necessary to allow management jobs that update certificates on the F5 device to wait until the primary node is available before making their update. Inventory jobs are carried out against any available node.

- In the **Primary Node Check Retry Wait Seconds** field, either accept the default value of 120 seconds or enter a new value. This value represents the number of seconds the orchestrator will wait after a pending management job cannot be completed because the primary node cannot be contacted before trying to contact the primary node again to retry the job.
- In the **Primary Node Check Retry Maximum** field, either accept the default value of 3 retry attempts or enter a new value. This value represents the number of times the orchestrator will retry a pending management job that is failing because the primary node cannot be contacted before declaring the job failed.
- In the **Version of F5** dropdown, select the version of F5 this server is running. The F5 REST API is supported on version 13 and up.

  Tip: Select v15 for version 15 and above.

- Click **Set Server Username** to choose the source from which to load a user valid on the F5 device with *Administrator* permissions. In the Server Username dialog, the options are Load From Keyfactor Secrets or Load From PAM Provider. The *No Value* option is typically not supported for F5 stores.

  Note: Although a user with Resource Administrator permissions is sufficient when using the F5 methods that use the SOAP API, the F5 methods that use the REST API require full Administrator permissions.

- Click **Set Server Password** to choose the source to load a valid password for the server. In the Server Password dialog, the options are Load From Keyfactor Secrets or Load From PAM Provider. The *No Value* option is typically not supported for F5 stores.

  A Keyfactor secret is a user-defined password or other information that is encrypted and stored securely in the Keyfactor Command database. Although Keyfactor recommends using Privileged Access Management (see Privileged Access Management (PAM) on page 677) as a more secure solution to secure information, Keyfactor Secret is an option

for customers that do not already have a relationship with a PAM provider such as CyberArk or Delinea (formerly Thycotic).

Select the **Load From Keyfactor Secrets** radio button as the *Secret Source* if you want Keyfactor Command to encrypt and store the password in the Keyfactor Command database. Enter and confirm a password.

Select the **Load from PAM Provider** radio button as the *Secret Source* if you want to store the password in a supported third-party PAM solution (see Privileged Access Management (PAM) on page 677). The remaining fields on the dialog will vary depending on the PAM provider.

CyberArk

Select CyberArk in the **Providers** dropdown if your PAM provider is CyberArk. The remaining fields in the dialog will then be:

- PrivateArk Protected Password Name—The name of the username or password in the safe (see Create a CyberArk Password on page 683).
- PrivateArk Folder Name—The path and name of the folder that stores the CyberArk Password (e.g. Root or Root\MyDir).

Delinea (formerly Thycotic)

Select Delinea in the **Providers** dropdown if your PAM provider is Delinea. The remaining field in the dialog will then be:

- Delinea Secret ID—The numeric ID of the secret to retrieve from Secret Server (see Create a Delinea Secret Server Secret on page 687).

- In the **Use SSL** section, select *True* to use SSL to communicate with the F5 device or cluster, if desired. The F5 device must trust the CA that issued the certificate used to protect the Keyfactor Command server if you select this option or you must set the *Ignore Server SSL Warnings* application setting to *True* (see Application Settings on page 583).

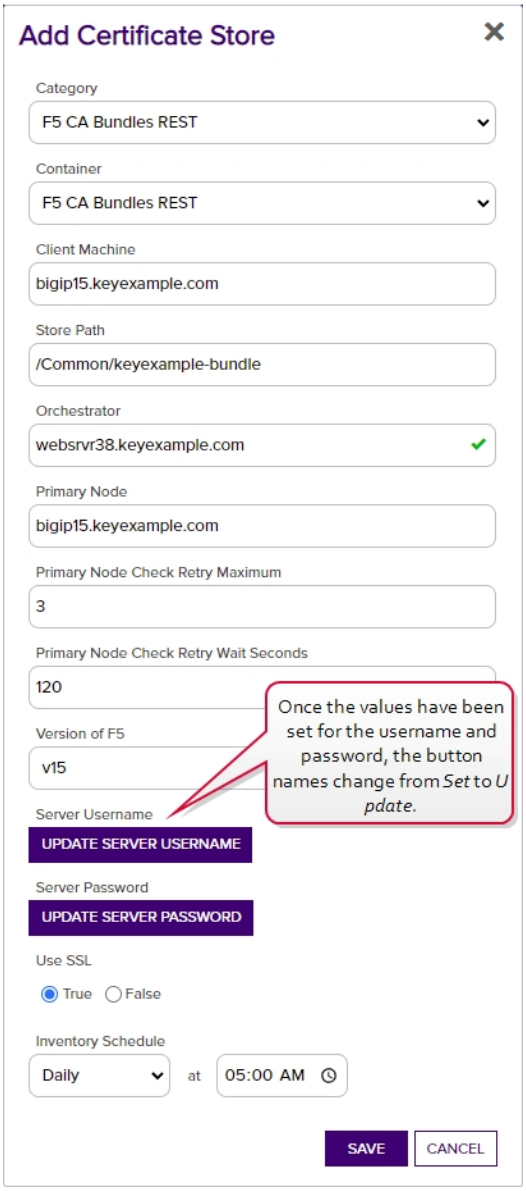


Figure 226: Add New F5 CA Bundles REST Certificate Store Location

For an F5 SSL Profile Certificate Store (SOAP)

- Enter the fully qualified domain name of the F5 device on which the certificate store is located in the **Client Machine** field. This field cannot be modified on an edit.
- In the **Store Path** field, enter the name of the partition on the F5 device into which you want to install the certificate. The Store Path name is case sensitive, so if the partition

name on the F5 is *Common* it must be entered in the Store Path field as *Common* rather than *common*. This field cannot be modified on an edit.

- Select the name of the Windows Orchestrator machine that will manage the stores in the**Orchestrator** dropdown. The orchestrator must be approved in order to appear here. Orchestrators can be configured for auto-approval. See Orchestrator Auto-Registration on page 474 and Orchestrator Management on page 481.
- Click **Set Server Username** to choose the source from which to load a user valid on the F5 device with Administrator or Resource Administrator permissions. In the Server Username dialog, the options are Load From Keyfactor Secrets or Load From PAM Provider. The *No Value* option is typically not supported for F5 stores.
- Click **Set Server Password** to choose the source to load a valid password for the server. In the Server Password dialog, the options are Load From Keyfactor Secrets or Load From PAM Provider. The *No Value* option is typically not supported for F5 stores.

  A Keyfactor secret is a user-defined password or other information that is encrypted and stored securely in the Keyfactor Command database. Although Keyfactor recommends using Privileged Access Management (see Privileged Access Management (PAM) on page 677) as a more secure solution to secure information, Keyfactor Secret is an option for customers that do not already have a relationship with a PAM provider such as CyberArk or Delinea (formerly Thycotic).

  Select the **Load From Keyfactor Secrets** radio button as the *Secret Source* if you want Keyfactor Command to encrypt and store the password in the Keyfactor Command database. Enter and confirm a password.

  Select the **Load from PAM Provider** radio button as the *Secret Source* if you want to store the password in a supported third-party PAM solution (see Privileged Access Management (PAM) on page 677). The remaining fields on the dialog will vary depending on the PAM provider.

CyberArk

Select CyberArk in the **Providers** dropdown if your PAM provider is CyberArk. The remaining fields in the dialog will then be:

- PrivateArk Protected Password Name—The name of the username or password in the safe (see Create a CyberArk Password on page 683).
- PrivateArk Folder Name—The path and name of the folder that stores the CyberArk Password (e.g. Root or Root\MyDir).

Delinea (formerly Thycotic)

Select Delinea in the **Providers** dropdown if your PAM provider is Delinea. The remaining field in the dialog will then be:

- Delinea Secret ID—The numeric ID of the secret to retrieve from Secret Server (see Create a Delinea Secret Server Secret on page 687).

- In the **Use SSL** section, select *True* to use SSL to communicate with the F5 device or cluster, if desired. The F5 device must trust the CA that issued the certificate used to protect the Keyfactor Command server if you select this option or you must set the *Ignore Server SSL Warnings* application setting to *True* (see Application Settings on page 583).

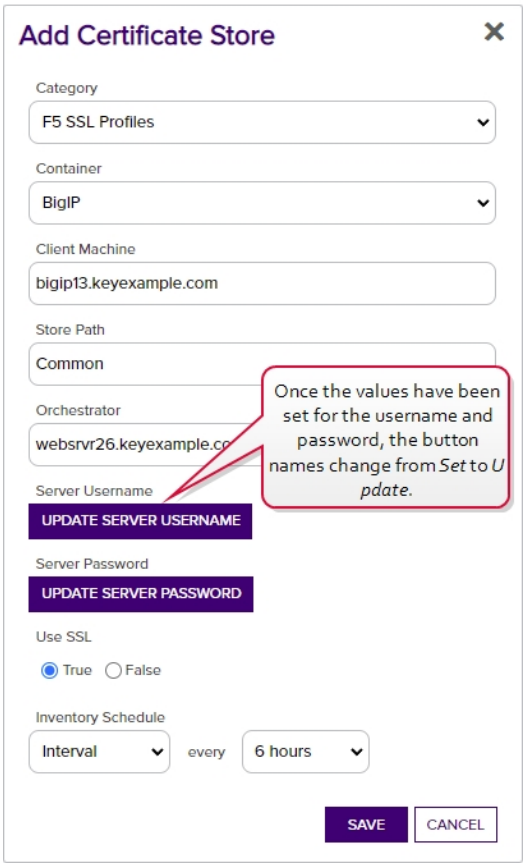


Figure 227: Add New F5 SSL Profile Certificate Store Location

For an F5 SSL Profile REST Certificate Store

Tip: F5 SSL profile stores can be added using the certificate store discovery option rather than manually, if desired, if you opt to select the REST connection method (see Certificate Store Discovery on page 424).

- Enter the fully qualified domain name of the F5 device (or F5 cluster for a high availability deployment) on which the certificate store is located in the **Client Machine** field. This field cannot be modified on an edit.

- In the **Store Path** field, enter the name of the partition on the F5 device into which you want to install the certificate. The Store Path name is case sensitive, so if the partition name on the F5 is *Common* it must be entered in the Store Path field as *Common* rather than *common*. This field cannot be modified on an edit.
- Select the name of the Keyfactor Universal Orchestrator[1] or Windows Orchestrator machine that will manage the stores in the**Orchestrator** dropdown. The orchestrator must be approved in order to appear here. Some orchestrators can be configured for auto-approval. See Orchestrator Auto-Registration on page 474 and Orchestrator Management on page 481.
- In the **Primary Node** field, enter the fully qualified domain name of the F5 device that acts as the primary node in a highly available F5 implementation. If you're using a single F5 device, this will often be the same value you entered in the Client Machine field.

  Tip: Configuration of the primary node is necessary to allow management jobs that update certificates on the F5 device to wait until the primary node is available before making their update. Inventory jobs are carried out against any available node.

- In the **Primary Node Check Retry Wait Seconds** field, either accept the default value of 120 seconds or enter a new value. This value represents the number of seconds the orchestrator will wait after a pending management job cannot be completed because the primary node cannot be contacted before trying to contact the primary node again to retry the job.
- In the **Primary Node Check Retry Maximum** field, either accept the default value of 3 retry attempts or enter a new value. This value represents the number of times the orchestrator will retry a pending management job that is failing because the primary node cannot be contacted before declaring the job failed.
- In the **Version of F5** dropdown, select the version of F5 this server is running. The F5 REST API is supported on version 13 and up.

  Tip: Select v15 for version 15 and above.

- Click **Update Server Username** to choose the source from which to load a user valid on the F5 device with *Administrator* permissions. In the Server Username dialog, the options are Load From Keyfactor Secrets or Load From PAM Provider. The *No Value* option is typically not supported for F5 stores.

> **Note:** Although a user with Resource Administrator permissions is sufficient when using the F5 methods that use the SOAP API, the F5 methods that use the REST API require full Administrator permissions.

- Click **Update Server Password** to choose the source to load a valid password for the server. In the Server Password dialog, the options are Load From Keyfactor Secrets or Load From PAM Provider. The *No Value* option is typically not supported for F5 stores.

  A Keyfactor secret is a user-defined password or other information that is encrypted and stored securely in the Keyfactor Command database. Although Keyfactor recommends using Privileged Access Management (see Privileged Access Management (PAM) on page 677) as a more secure solution to secure information, Keyfactor Secret is an option for customers that do not already have a relationship with a PAM provider such as CyberArk or Delinea (formerly Thycotic).

  Select the **Load From Keyfactor Secrets** radio button as the *Secret Source* if you want Keyfactor Command to encrypt and store the password in the Keyfactor Command database. Enter and confirm a password.

  Select the **Load from PAM Provider** radio button as the *Secret Source* if you want to store the password in a supported third-party PAM solution (see Privileged Access Management (PAM) on page 677). The remaining fields on the dialog will vary depending on the PAM provider.

  ### CyberArk

  Select CyberArk in the **Providers** dropdown if your PAM provider is CyberArk. The remaining fields in the dialog will then be:

  - PrivateArk Protected Password Name—The name of the username or password in the safe (see Create a CyberArk Password on page 683).
  - PrivateArk Folder Name—The path and name of the folder that stores the CyberArk Password (e.g. Root or Root\MyDir).

  ### Delinea (formerly Thycotic)

  Select Delinea in the **Providers** dropdown if your PAM provider is Delinea. The remaining field in the dialog will then be:

  - Delinea Secret ID—The numeric ID of the secret to retrieve from Secret Server (see Create a Delinea Secret Server Secret on page 687).

- In the **Use SSL** section, select *True* to use SSL to communicate with the F5 device or cluster, if desired. The F5 device must trust the CA that issued the certificate used to protect the Keyfactor Command server if you select this option or you must set the *Ignore Server SSL Warnings* application setting to *True* (see Application Settings on page 583).

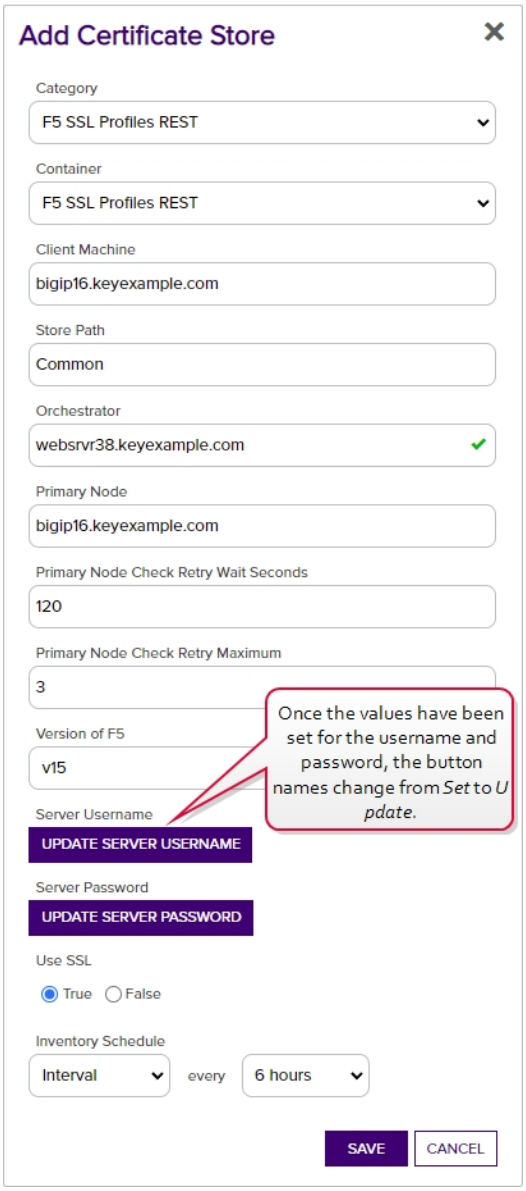


Figure 228: Add New F5 SSL Profile REST Certificate Store Location

For an F5 Web Server Certificate Store (SOAP)

- Enter the fully qualified domain name of the F5 device on which the certificate store is located in the **Client Machine** field. This field cannot be modified on an edit.
- The **Store Path** is configured to a fixed value for this type of store and cannot be changed.

- Select the name of the Windows Orchestrator machine that will manage the stores in the**Orchestrator** dropdown. The orchestrator must be approved in order to appear here. Orchestrators can be configured for auto-approval. See Orchestrator Auto-Registration on page 474 and Orchestrator Management on page 481.
- Click **Set Server Username** to choose the source from which to load a user valid on the F5 device with Administrator or Resource Administrator permissions. In the Server Username dialog, the options are Load From Keyfactor Secrets or Load From PAM Provider. The *No Value* option is typically not supported for F5 stores.
- Click **Set Server Password** to choose the source to load a valid password for the server. In the Server Password dialog, the options are Load From Keyfactor Secrets or Load From PAM Provider. The *No Value* option is typically not supported for F5 stores.

  A Keyfactor secret is a user-defined password or other information that is encrypted and stored securely in the Keyfactor Command database. Although Keyfactor recommends using Privileged Access Management (see Privileged Access Management (PAM) on page 677) as a more secure solution to secure information, Keyfactor Secret is an option for customers that do not already have a relationship with a PAM provider such as CyberArk or Delinea (formerly Thycotic).

  Select the **Load From Keyfactor Secrets** radio button as the *Secret Source* if you want Keyfactor Command to encrypt and store the password in the Keyfactor Command database. Enter and confirm a password.

  Select the **Load from PAM Provider** radio button as the *Secret Source* if you want to store the password in a supported third-party PAM solution (see Privileged Access Management (PAM) on page 677). The remaining fields on the dialog will vary depending on the PAM provider.

  ### CyberArk

  Select CyberArk in the **Providers** dropdown if your PAM provider is CyberArk. The remaining fields in the dialog will then be:

  - PrivateArk Protected Password Name—The name of the username or password in the safe (see Create a CyberArk Password on page 683).
  - PrivateArk Folder Name—The path and name of the folder that stores the CyberArk Password (e.g. Root or Root\MyDir).

  ### Delinea (formerly Thycotic)

  Select Delinea in the **Providers** dropdown if your PAM provider is Delinea. The remaining field in the dialog will then be:

  - Delinea Secret ID—The numeric ID of the secret to retrieve from Secret Server (see Create a Delinea Secret Server Secret on page 687).

- In the **Use SSL** section, select *True* to use SSL to communicate with the F5 device or cluster, if desired. The F5 device must trust the CA that issued the certificate used to protect the Keyfactor Command server if you select this option or you must set the *Ignore Server SSL Warnings* application setting to *True* (see Application Settings on page 583).

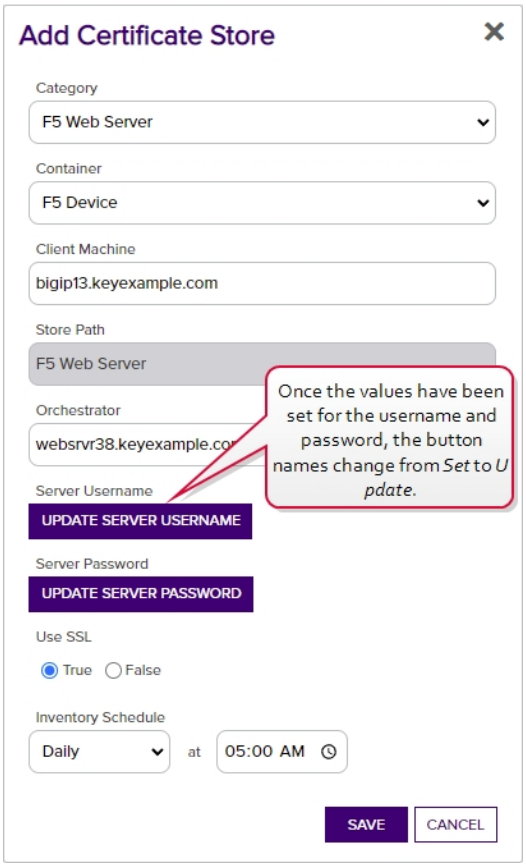


Figure 229: Add New F5 Web Server Certificate Store Location

For an F5 Web Server REST Certificate Store

- Enter the fully qualified domain name of the F5 device (or F5 cluster for a high availability deployment) on which the certificate store is located in the **Client Machine** field. This field cannot be modified on an edit.
- The **Store Path** is configured to a fixed value for this type of store and cannot be changed.
- Select the name of the Keyfactor Universal Orchestrator[1] or Windows Orchestrator machine that will manage the stores in the**Orchestrator** dropdown. The orchestrator must be approved in order to appear here. Some orchestrators can be configured for auto-

approval. See Orchestrator Auto-Registration on page 474 and Orchestrator Management on page 481.

- In the **Primary Node** field, enter the fully qualified domain name of the F5 device that acts as the primary node in a highly available F5 implementation. If you're using a single F5 device, this will typically be the same value you entered in the Client Machine field.

  Tip: Configuration of the primary node is necessary to allow management jobs that update certificates on the F5 device to wait until the primary node is available before making their update. Inventory jobs are carried out against any available node.

- In the **Primary Node Check Retry Wait Seconds** field, either accept the default value of 120 seconds or enter a new value. This value represents the number of seconds the orchestrator will wait after a pending management job cannot be completed because the primary node cannot be contacted before trying to contact the primary node again to retry the job.
- In the **Primary Node Check Retry Maximum** field, either accept the default value of 3 retry attempts or enter a new value. This value represents the number of times the orchestrator will retry a pending management job that is failing because the primary node cannot be contacted before declaring the job failed.
- In the **Version of F5** dropdown, select the version of F5 this server is running. The F5 REST API is supported on version 13 and up.

  Tip: Select v15 for version 15 and above.

- Click **Update Server Username** to choose the source from which to load a user valid on the F5 device with *Administrator* permissions. In the Server Username dialog, the options are Load From Keyfactor Secrets or Load From PAM Provider. The *No Value* option is typically not supported for F5 stores.

  Note: Although a user with Resource Administrator permissions is sufficient when using the F5 methods that use the SOAP API, the F5 methods that use the REST API require full Administrator permissions.

- Click **Update Server Password** to choose the source to load a valid password for the server. In the Server Password dialog, the options are Load From Keyfactor Secrets or Load From PAM Provider. The *No Value* option is typically not supported for F5 stores.

  A Keyfactor secret is a user-defined password or other information that is encrypted and stored securely in the Keyfactor Command database. Although Keyfactor recommends using Privileged Access Management (see Privileged Access Management (PAM) on

page 677) as a more secure solution to secure information, Keyfactor Secret is an option for customers that do not already have a relationship with a PAM provider such as CyberArk or Delinea (formerly Thycotic).

Select the **Load From Keyfactor Secrets** radio button as the *Secret Source* if you want Keyfactor Command to encrypt and store the password in the Keyfactor Command database. Enter and confirm a password.

Select the **Load from PAM Provider** radio button as the *Secret Source* if you want to store the password in a supported third-party PAM solution (see Privileged Access Management (PAM) on page 677). The remaining fields on the dialog will vary depending on the PAM provider.

CyberArk

Select CyberArk in the **Providers** dropdown if your PAM provider is CyberArk. The remaining fields in the dialog will then be:

- PrivateArk Protected Password Name—The name of the username or password in the safe (see Create a CyberArk Password on page 683).
- PrivateArk Folder Name—The path and name of the folder that stores the CyberArk Password (e.g. Root or Root\MyDir).

Delinea (formerly Thycotic)

Select Delinea in the **Providers** dropdown if your PAM provider is Delinea. The remaining field in the dialog will then be:

- Delinea Secret ID—The numeric ID of the secret to retrieve from Secret Server (see Create a Delinea Secret Server Secret on page 687).

- In the **Use SSL** section, select *True* to use SSL to communicate with the F5 device or cluster, if desired. The F5 device must trust the CA that issued the certificate used to protect the Keyfactor Command server if you select this option or you must set the *Ignore Server SSL Warnings* application setting to *True* (see Application Settings on page 583).

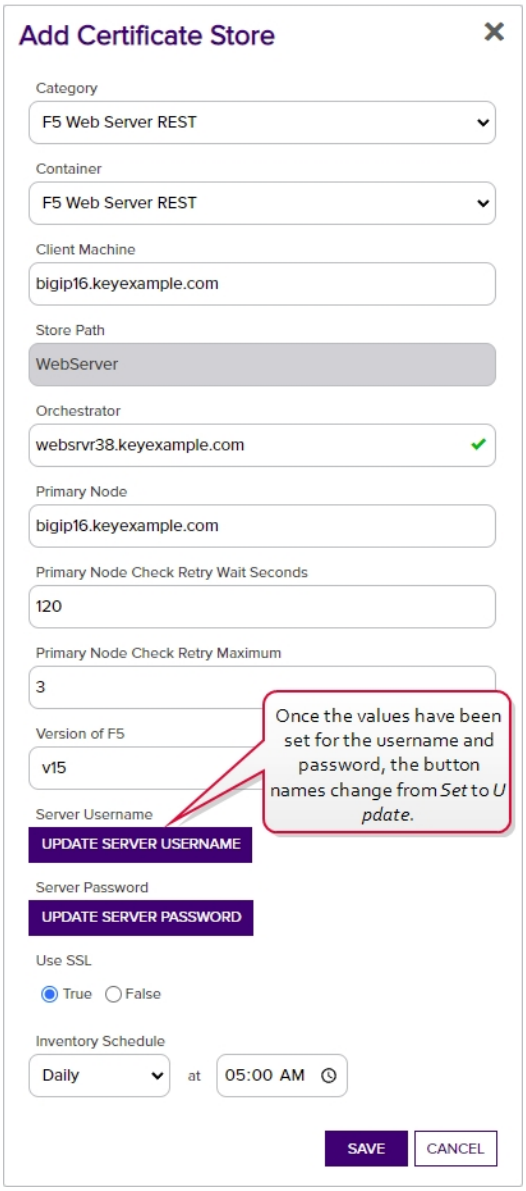


Figure 230: Add New F5 Web Server REST Certificate Store Location

For a File Transfer Protocol Certificate Store

- Enter the fully qualified domain name of the machine on which the certificate store is located in the **Client Machine** field. This field cannot be modified on an edit.
- In the **Store Path** field, enter the name of the directory containing the PEM certificate store(s) you wish to manage via FTP. The directory name is given relative to the FTP root

and should include a leading forward slash (/) for both Windows and Linux FTP servers. Enter just a forward slash to manage the FTP root. This field cannot be modified on an edit.

- Select the name of the Keyfactor Universal Orchestrator or Windows Orchestrator machine that will manage the stores in the **Orchestrator** dropdown. The orchestrator must be approved in order to appear here. Some orchestrators can be configured for auto-approval. See Orchestrator Auto-Registration on page 474 and Orchestrator Management on page 481.
- Click **Update Server Username** to choose the source from which to load a user valid on the FTP server with sufficient permissions to read and/or write to the file storage location as needed. In the Server Username dialog, the options are No Value, Load From Keyfactor Secrets, and Load From PAM Provider.
- Click **Update Server Password** to choose the source to load a valid password for the server. In the Server Password dialog, the options are No Value, Load From Keyfactor Secrets, and Load From PAM Provider.

  Select **No Value** if your FTP server supports anonymous and you wish to connect using this.

  A Keyfactor secret is a user-defined password or other information that is encrypted and stored securely in the Keyfactor Command database. Although Keyfactor recommends using Privileged Access Management (see Privileged Access Management (PAM) on page 677) as a more secure solution to secure information, Keyfactor Secret is an option for customers that do not already have a relationship with a PAM provider such as CyberArk or Delinea (formerly Thycotic).

  Select the **Load From Keyfactor Secrets** radio button as the *Secret Source* if you want Keyfactor Command to encrypt and store the password in the Keyfactor Command database. Enter and confirm a password.

  Select the **Load from PAM Provider** radio button as the *Secret Source* if you want to store the password in a supported third-party PAM solution (see Privileged Access Management (PAM) on page 677). The remaining fields on the dialog will vary depending on the PAM provider.

CyberArk

Select CyberArk in the **Providers** dropdown if your PAM provider is CyberArk. The remaining fields in the dialog will then be:

- PrivateArk Protected Password Name—The name of the username or password in the safe (see Create a CyberArk Password on page 683).
- PrivateArk Folder Name—The path and name of the folder that stores the CyberArk Password (e.g. Root or Root\MyDir).

Delinea (formerly Thycotic)

Select Delinea in the **Providers** dropdown if your PAM provider is Delinea. The remaining field in the dialog will then be:

- Delinea Secret ID—The numeric ID of the secret to retrieve from Secret Server (see Create a Delinea Secret Server Secret on page 687).

- In the **Use SSL** section, select *True* to use SSL to communicate with the FTP server, if desired.

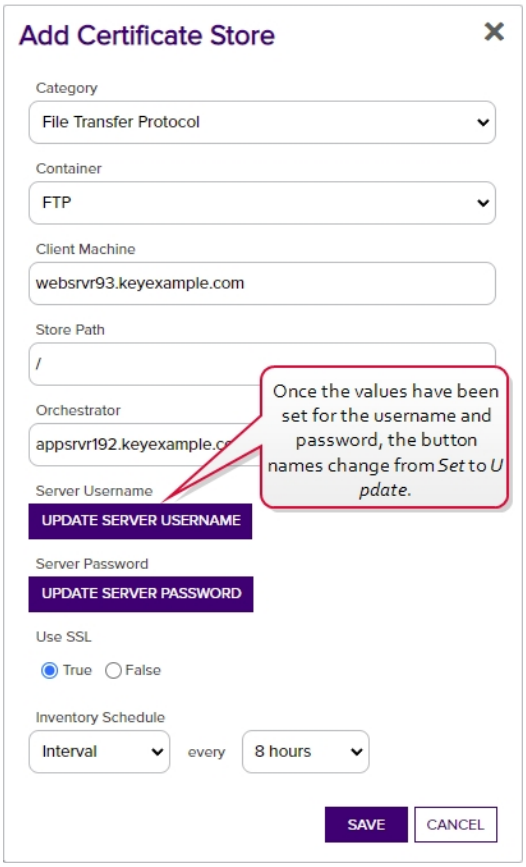


Figure 231: Add New FTP Certificate Store Location

For an IIS Certificate Store

The options are the same for all three types of IIS certificate stores (IIS Personal, IIS Revoked and IIS Trusted Roots).

- Enter the fully qualified domain name of the server on which the certificate store is located in the **Client Machine** field. This field cannot be modified on an edit.

> **Important:** Use the actual hostname of the IIS server in the **Client Machine** field rather than a DNS alias (either "A" or CNAME records). This is necessary because the orchestrator uses PowerShell remoting for some of the machine certificate store functions, which relies on Kerberos authentication. Kerberos authentication requires that the target machine has a service principal name (SPN) in the HTTP/ format assigned to the target's machine account. This will be present by default (as part of the HOST/ format record) as long as the HTTP/ format SPN has not been manually assigned elsewhere. Using an alias gets into complexities of setting up appropriate SPNs and assuring that there are not duplicate SPNs in the environment. If you wish to manage the IIS server hosting Keyfactor Command, you will need to use a DNS alias for either your Keyfactor Command server or the IIS store access. Contact Keyfactor for design assistance.

- The **Store Path** is configured to a fixed value for this type of store and cannot be changed.
- Select the name of the Keyfactor Universal Orchestrator or Windows Orchestrator machine that will manage the stores in the**Orchestrator** dropdown. The orchestrators must be approved in order to appear here. Some orchestrator can be configured for auto-approval. See Orchestrator Auto-Registration on page 474 and Orchestrator Management on page 481.

  > **Tip:** When managing IIS stores, the orchestrator does so with the account it's running as (its own service account credentials). The orchestrator service account needs sufficient permissions to be able to install, delete, and update certificates. Typically, this would be a domain account that has local administrator permission on the IIS machines it needs to manage.

- In the **Use SSL** section, select *True* to cause the orchestrator to use SSL when communicating with IIS targets. For more information, see *Configure the Targets for IIS Management* in the *Keyfactor Orchestrators Installation and Configuration Guide*.

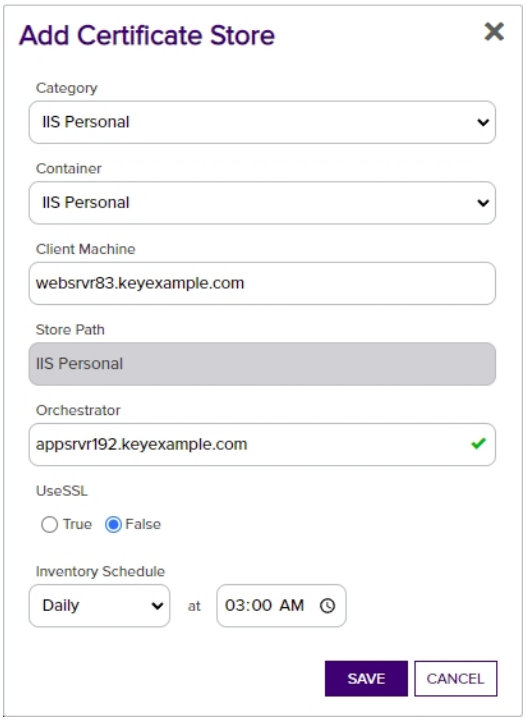


Figure 232: Add New IIS Personal Certificate Store Location

For a Java Keystore

Tip: Java keystores can be added using the certificate store discovery option rather than manually, if desired (see Certificate Store Discovery on page 424).

- Enter the fully qualified domain name of the machine on which the keystore is or will be located in the **Client Machine** field. This field cannot be modified on an edit.
- In the **Store Path** field, enter the full path to the keystore on that machine, including the file name. Paths and filenames entered for Linux/UNIX machines are case sensitive. This field cannot be modified on an edit.
- Select the **Type** from the dropdown. The available types are:
    - JKS
      Standard Java keystore.
    - PKCS12
      PKCS12 type files (e.g. P12 or PFX), which are discoverable with the Java Agent using compatibility mode introduced in Java version 1.8.
    - Windows-My
      Windows local machine personal certificate store. This option is only supported

with a custom extension based on the AnyAgent framework. The Keyfactor Java Agent does not include functionality to manage this type of store.

- Click **Set Store Password**. The Store Password dialog will open. In the Store Password dialog, the options are No Value, Load From Keyfactor Secrets, and Load From PAM Provider.

  Select **No Value** if your keystore does not have a password configured.

  A Keyfactor secret is a user-defined password or other information that is encrypted and stored securely in the Keyfactor Command database. Although Keyfactor recommends using Privileged Access Management (see Privileged Access Management (PAM) on page 677) as a more secure solution to secure information, Keyfactor Secret is an option for customers that do not already have a relationship with a PAM provider such as CyberArk or Delinea (formerly Thycotic).

  Select the **Load From Keyfactor Secrets** radio button as the *Secret Source* if you want Keyfactor Command to encrypt and store the password in the Keyfactor Command database. Enter and confirm a password.

  Select the **Load from PAM Provider** radio button as the *Secret Source* if you want to store the password in a supported third-party PAM solution (see Privileged Access Management (PAM) on page 677). The remaining fields on the dialog will vary depending on the PAM provider.

  ### CyberArk

  Select CyberArk in the **Providers** dropdown if your PAM provider is CyberArk. The remaining fields in the dialog will then be:

  - PrivateArk Protected Password Name—The name of the username or password in the safe (see Create a CyberArk Password on page 683).
  - PrivateArk Folder Name—The path and name of the folder that stores the CyberArk Password (e.g. Root or Root\MyDir).

  ### Delinea (formerly Thycotic)

  Select Delinea in the **Providers** dropdown if your PAM provider is Delinea. The remaining field in the dialog will then be:

  - Delinea Secret ID—The numeric ID of the secret to retrieve from Secret Server (see Create a Delinea Secret Server Secret on page 687).

- If the keystore does not already exist and you would like to create it, check the **Create Certificate Store** box. This will cause the file to be created on the target.

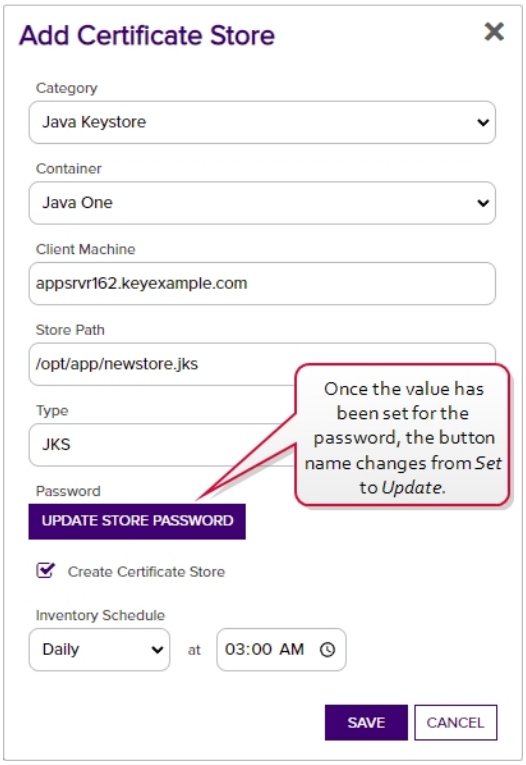


Figure 233: Add New Java Keystore Location

For a NetScaler Certificate Store

- Enter the fully qualified domain name of the Citrix ADC (a.k.a. NetScaler) device on which the certificate store is located in the **Client Machine** field. This field cannot be modified on an edit.
- In the **Store Path** field, enter the name of the directory on the Citrix ADC device containing the certificate store(s) you wish to manage. The Store Path name is case sensitive. This field cannot be modified on an edit.
- Select the name of the Keyfactor Universal Orchestrator[1] or Windows Orchestrator machine that will manage the stores in the **Orchestrator** dropdown. The orchestrator must be approved in order to appear here. Some orchestrators can be configured for auto-approval. See Orchestrator Auto-Registration on page 474 and Orchestrator Management on page 481.
- Click **Set Server Username** to choose the source from which to load a user valid on the Citrix ADC device with partition-admin permissions. In the Server Username dialog, the options are Load From Keyfactor Secrets or Load From PAM Provider.
- Click **Set Server Password** to choose the source to load a valid password for the server. In the Server Password dialog, the options are Load From Keyfactor Secrets or Load

From PAM Provider.

A Keyfactor secret is a user-defined password or other information that is encrypted and stored securely in the Keyfactor Command database. Although Keyfactor recommends using Privileged Access Management (see Privileged Access Management (PAM) on page 677) as a more secure solution to secure information, Keyfactor Secret is an option for customers that do not already have a relationship with a PAM provider such as CyberArk or Delinea (formerly Thycotic).

Select the **Load From Keyfactor Secrets** radio button as the *Secret Source* if you want Keyfactor Command to encrypt and store the password in the Keyfactor Command database. Enter and confirm a password.

Select the **Load from PAM Provider** radio button as the *Secret Source* if you want to store the password in a supported third-party PAM solution (see Privileged Access Management (PAM) on page 677). The remaining fields on the dialog will vary depending on the PAM provider.

CyberArk

Select CyberArk in the **Providers** dropdown if your PAM provider is CyberArk. The remaining fields in the dialog will then be:

- PrivateArk Protected Password Name—The name of the username or password in the safe (see Create a CyberArk Password on page 683).
- PrivateArk Folder Name—The path and name of the folder that stores the CyberArk Password (e.g. Root or Root\MyDir).

Delinea (formerly Thycotic)

Select Delinea in the **Providers** dropdown if your PAM provider is Delinea. The remaining field in the dialog will then be:

- Delinea Secret ID—The numeric ID of the secret to retrieve from Secret Server (see Create a Delinea Secret Server Secret on page 687).

- In the **Use SSL** section, select *True* to use SSL to communicate with the Citrix ADC device or cluster, if desired.

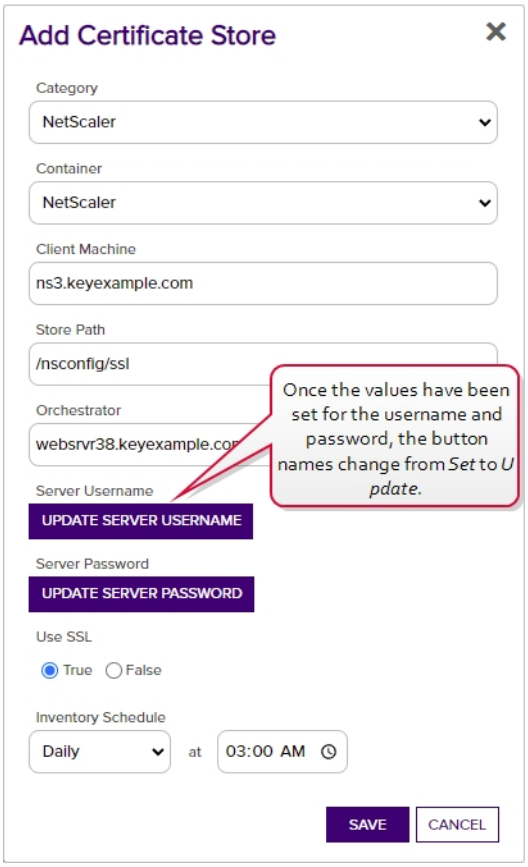


Figure 234: Add New NetScaler Certificate Store Location

For a PEM Certificate Store

Tip: PEM stores can be added using the certificate store discovery option rather than manually, if desired (see Certificate Store Discovery on page 424).

- Enter the fully qualified domain name of the machine on which the certificate store is located in the **Client Machine** field. This field cannot be modified on an edit.
- In the **Store Path** field, enter the full path to the store on that machine, including the file name. Paths and filenames entered for Linux/UNIX machines are case sensitive. This field cannot be modified on an edit.
- In the **Separate Private Key** section, select *True* if the private key for the certificate is stored in a separate file from the certificate.

- If you selected *True* in the Separate Private Key section, enter the full path to the private key on the machine, including the file name, in the **Path to Private Key File** field. Paths and filenames entered for Linux/UNIX machines are case sensitive.

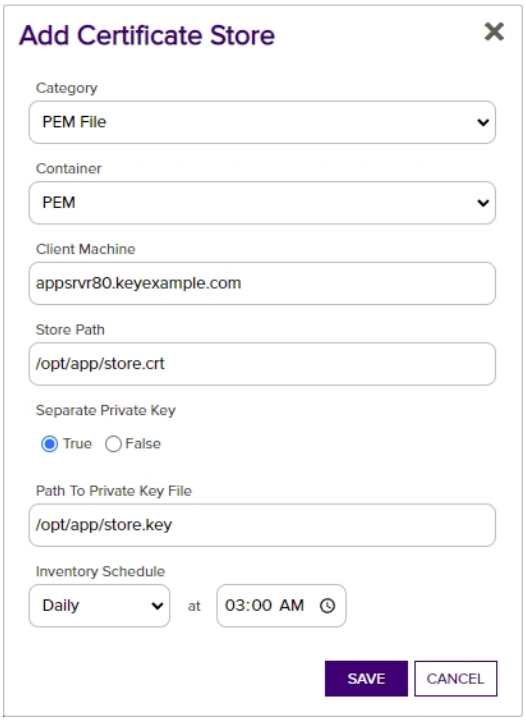


Figure 235: Add New PEM Certificate Store Location

6. In the Inventory Schedule fields, select an inventory schedule for the store, if desired. You can choose to run the inventory *Daily*, on an *Interval*, *Immediately*, *Exactly Once*, or set inventorying to *Off*.
    - If you select **Daily**, you can set the time of day when the inventory should begin every day.
    - If you select **Interval**, you can select a scan frequency of anywhere from every 1 minute to every 12 hours.
    - If you select **Immediate**, the inventory will run within a few minutes of saving the record and will run only once. After this, the inventory schedule will be cleared.
    - If you select **Exactly Once**, you can select a date and time at which to run the inventory job. After the job has run, the inventory schedule will be cleared.
    - Select **Off** to disable the inventory job.

    If you are using Certificate Store Containers (see Certificate Store Containers on page 418) to manage your stores and their schedules you do not need to set an inventory schedule here.
7. Click **Save** to save the new or edited certificate store location.

Deleting a Certificate Store

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:
Certificate Store Management: *Read*
Certificate Store Management: *Modify*

Permissions for certificate stores can be set at either the global or certificate store container level. See *Container Permissions* in the *Keyfactor Command Reference Guide* for more information about global vs container permissions.

To delete a certificate store:

1. In the Management Portal, browse to *Locations > Certificate Stores*.
2. On the Certificate Stores page, select the Certificate Stores tab (the default when you first visit the page).
3. On the Certificate Stores tab, highlight the row(s) in the certificate store grid of the store(s) to delete and click **Delete** at the top of the grid or right-click the store location in the grid and choose **Delete** from the right-click menu. The right-click menu supports operations on only one store at a time.
4. On the Confirm Operation alert, click **OK** to confirm or **Cancel** to cancel the operation.

Note: This doesn't delete the actual certificate store on the target server, just the Keyfactor Command definition of it.

Viewing a Certificate Store

Users without modify permissions to certificate stores will see a *View* option instead of an *Edit* option on the Certificate Stores page to allow them to see a read-only view of the certificate store configuration details.

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:
Agent Management: *Read*
Certificate Store Management: *Read*

Permissions for certificate stores can be set at either the global or certificate store container level. See *Container Permissions* in the *Keyfactor Command Reference Guide* for more information about global vs container permissions.

To view the details of a certificate store:

1. In the Management Portal, browse to *Locations* > *Certificate Stores*.
2. On the Certificate Stores page, select the Certificate Stores tab (the default when you first visit the page).
3. On the Certificate Stores tab, highlight the row in the certificate store grid of the store for which to view certificate store details and click **View** at the top of the grid or right-click the store location in the grid and choose **View** from the right-click menu.

The fields are the same as those described for adding or editing a certificate store (see Adding or Modifying a Certificate Store on page 385), but none of the fields are editable when using the *View* option.

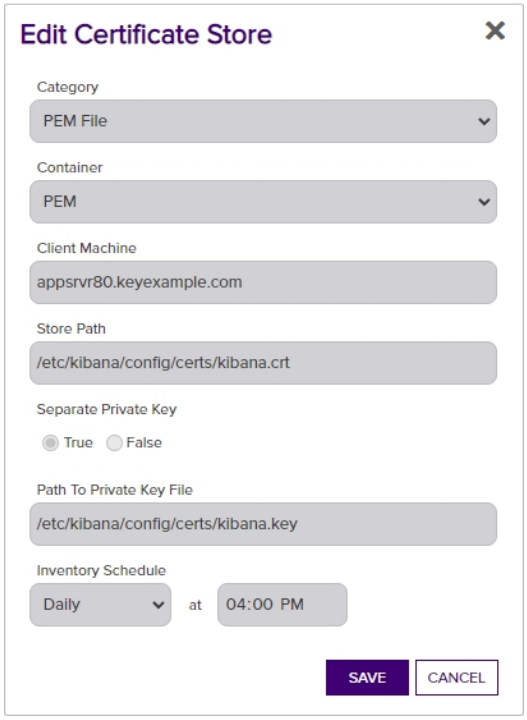


Figure 236: View Details for a Certificate Store

Certificate Store Reenrollment

The Reenrollment option is available for:

- PEM certificate stores managed by the Native Agent.
- PEM and Java certificate stores managed by the Java and Android Agents.
- Any custom certificate store types created with the AnyAgent Framework to support this functionality.

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:
Certificate Enrollment: *Enroll CSR*
Certificate Store Management: *Read*
Certificate Store Management: *Modify*

Permissions for certificate stores can be set at either the global or certificate store container level. See *Container Permissions* in the *Keyfactor Command Reference Guide* for more information about global vs container permissions.

In addition, the either the user scheduling the reenrollment job or the user configured to provide authentication to the CA (see Authorization Methods Tab on page 341) must have enrollment permissions configured on the CA and template.

To begin a reenrollment:

1. In the Management Portal, browse to *Locations* > *Certificate Stores*.
2. On the Certificate Stores page, select the Certificate Stores tab (the default when you first visit the page).
3. On the Certificate Stores tab, highlight the row in the certificate store grid of the store to reenroll and click **Reenrollment** at the top of the grid or right-click the store location in the grid and choose **Reenrollment** from the right-click menu.
4. On the Reenrollment dialog, enter a **Subject Name** for the new certificate using X.500 format and add an **Alias** for Java stores. PEM store reenrollments do not display the Alias field.
5. If desired, select a **Certificate Authority** to direct the enrollment request to and/or **Template** for the request.

   Note: If you don't select a template or CA for reenrollment, the values configured for the *Template For Submitted CSRs* and/or *Certificate Authority For Submitted CSRs* application setting(s) (see Application Settings on page 583) will be used.
6. Click Done to submit the request.

The reenrollment job will be scheduled to run immediately. Visit the Orchestrator Jobs page to check on the progress of the job (see Orchestrator Job Status on page 493).

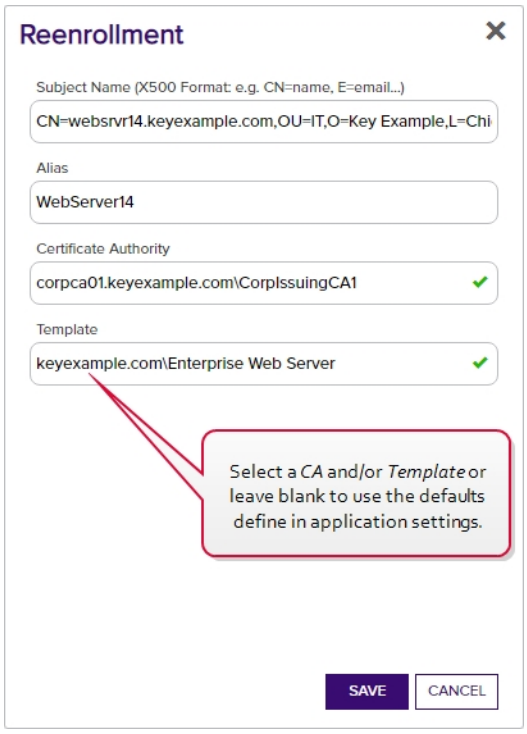


Figure 237: Enter a Information for Java Keystore Reenrollment

Setting a New Password on a Certificate Store

The option to reset the password on a certificate store updates the data for the certificate store as stored in the Keyfactor Command database but does not make any modifications to the certificate store itself. This option is available from the right-click menu only.

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:
Certificate Store Management: *Read*
Certificate Store Management: *Modify*

Permissions for certificate stores can be set at either the global or certificate store container level. See *Container Permissions* in the *Keyfactor Command Reference Guide* for more information about global vs container permissions.

To reset the password for a certificate store:

1. In the Management Portal, browse to *Locations* > *Certificate Stores*.
2. On the Certificate Stores page, select the Certificate Stores tab (the default when you first visit the page).
3. On the Certificate Stores tab, highlight the row in the certificate store grid of the store to

update and choose **Set New Password** from the right-click menu.

4. Enter and confirm the new password and click **Save**.

Assigning a Certificate Store to a Container

Before assigning a certificate store to a container, you need to create the container (see Certificate Store Containers on page 418). If you select multiple certificate stores to assign to a container at once, they must all be stores of the same type (e.g. PEM).

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:
Certificate Store Management: *Read*
Certificate Store Management: *Modify*

Permissions for certificate stores can be set at either the global or certificate store container level. See *Container Permissions* in the *Keyfactor Command Reference Guide* for more information about global vs container permissions.

To assign a certificate store to a container:

1. In the Management Portal, browse to *Locations* > *Certificate Stores*.
2. On the Certificate Stores page, select the Certificate Stores tab (the default when you first visit the page).
3. On the Certificate Stores tab, highlight the row(s) in the certificate store grid of the store(s) to be assigned to the container and click **Assign Container** at the top of the grid or right-click the store location in the grid and choose **Assign Container** from the right-click menu. The right-click menu supports operations on only one store at a time.
4. Select a certificate store container in the Container Name field and click **Save**.

Viewing Inventory for a Certificate Store

Once at least one inventory job has been completed for a given certificate store, you can view the certificates imported from the store.

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:
Certificate Store Management: *Read*
Privileged Access Management: *Read*

Permissions for certificate stores can be set at either the global or certificate store container level. See *Container Permissions* in the *Keyfactor Command Reference Guide* for more information about global vs container permissions.

To view the inventoried certificates for a store:

1. In the Management Portal, browse to *Locations > Certificate Stores*.
2. On the Certificate Stores page, select the Certificate Stores tab (the default when you first visit the page).
3. On the Certificate Stores tab, highlight the row in the certificate store grid of the store for which to view inventory and click **View Inventory** at the top of the grid or right-click the store location in the grid and choose **View Inventory** from the right-click menu.

On the left of the inventory viewing dialog you can select a certificate from the store to view. On the right of the dialog you can see details about that certificate, including the metadata associated with the certificate. In the Certificate Selection area of the screen, you can select between the chain certificates for the selected certificate and the end entity certificate, for certificates stored with a chain.

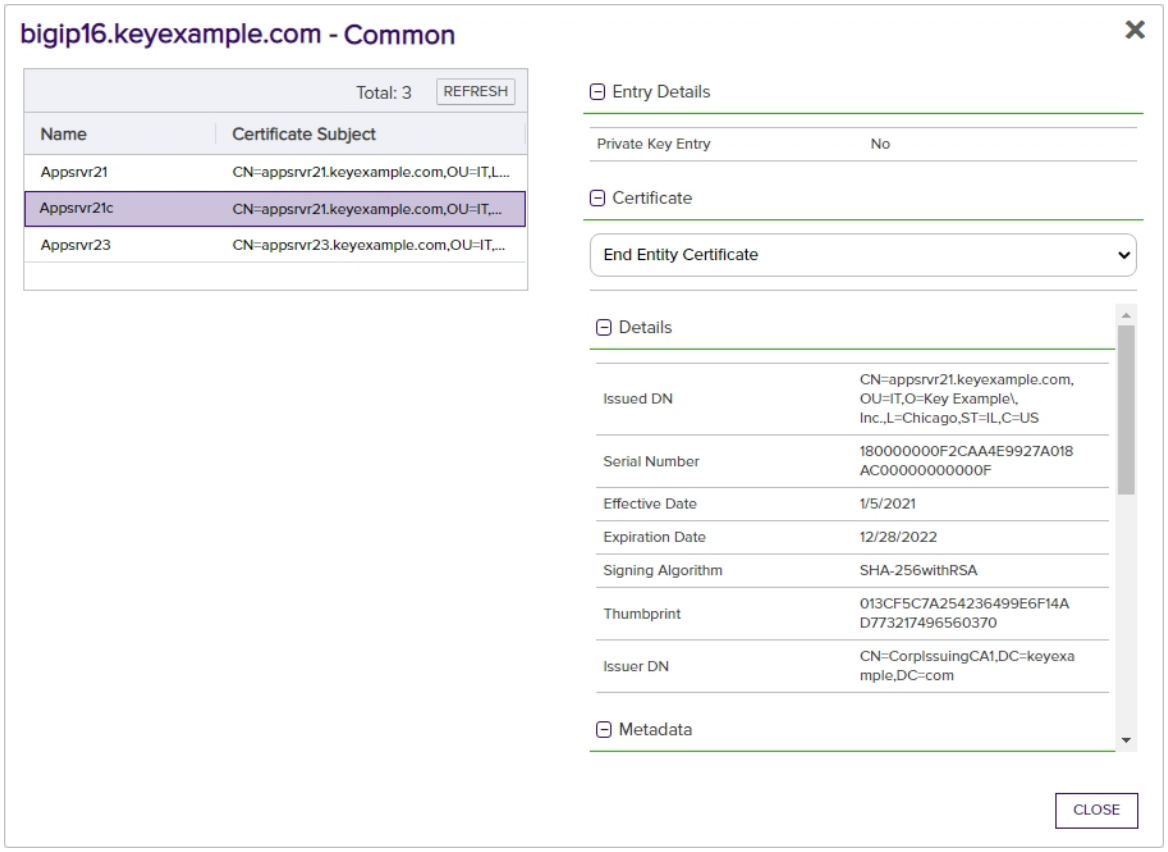


Figure 238: View Inventoried Certificates for a Certificate Store

Scheduling Inventory for a Certificate Store

Scheduling inventory for a certificate store allows Keyfactor Command to inspect the certificates inside a given store and add them to the Keyfactor Command database.

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:
Certificate Store Management: *Read*
Certificate Store Management: *Schedule*

Permissions for certificate stores can be set at either the global or certificate store container level. See *Container Permissions* in the *Keyfactor Command Reference Guide* for more information about global vs container permissions.

To schedule inventory:

1. In the Management Portal, browse to *Locations* > *Certificate Stores*.
2. On the Certificate Stores page, select the Certificate Stores tab (the default when you first visit the page).
3. On the Certificate Stores tab, highlight the row(s) in the certificate store grid of the store(s) for which you want to schedule inventory and click **Schedule Inventory** at the top of the grid, or choose **Schedule Inventory** from the right-click menu. The right-click menu supports operations on only one store at a time.
4. In the Certificate Store Inventory Schedule dialog, select a schedule for the store(s). You can choose to run the inventory *Daily*, on an *Interval*, *Immediately*, *Exactly Once*, or set inventorying to *Off*.
    - If you select **Daily**, you can set the time of day when the inventory should begin every day.
    - If you select **Interval**, you can select a scan frequency of anywhere from every 1 minute to every 12 hours.
    - If you select **Immediate**, the inventory will run within a few minutes of saving the record and will run only once. After this, the inventory schedule will be cleared.
    - If you select **Exactly Once**, you can select a date and time at which to run the inventory job. After the job has run, the inventory schedule will be cleared.
    - Select **Off** to disable the inventory job.

You have the option to not schedule inventory on a store-by-store basis and instead create containers and set inventory schedules that will apply to all the stores added to each container. See Certificate Store Containers on the next page for information on creating containers.

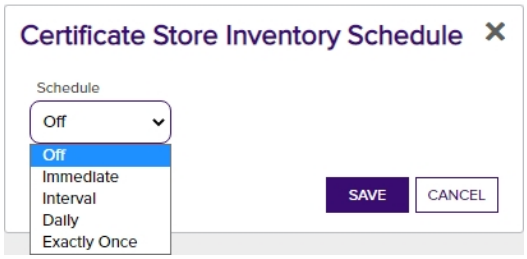


Figure 239: Schedule Inventory for a Certificate Store Location

Certificate Store Containers

Certificate store containers allow you to collect similar stores together to provide organization, allow for simplified bulk operations and control access.

Using the Containers Search Feature

The search function allows you to query the database for information. The same query structure is used in multiple locations within the Keyfactor Command Management Portal.

When you first open the page, you will see the simple search option. To execute a search, select the field and comparison operators in the dropdowns and type something on which to search in the value field (if applicable). If you select an *is null* or *is not null* comparison operator, the value field will be grayed out. Click the **Search** button to execute the query.

Each query consists of three parts:

Query Field

The available fields for querying vary depending on the area of the Management Portal in which the search is used. On this page, the queries can be done on the following built-in fields:

Name	CertStoreType
Complete or partial matches with the name of the container.	The certificate store type of the container.
Schedule	
Whether the container has a schedule defined, true/false.	

Comparison Operator

The query comparison operators vary depending on the type of field selected and the specific properties of the field. The list below shows the dropdown list comparison operators, as well as the equivalent query language syntax (in parentheses).

Most string fields (the vast majority of the built-in fields) support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Contains (-contains)
- Does not contain (-notcontains)
- Starts with (-startswith)
- Ends with (-endswith)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Most date and integer fields support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Is less than (-lt)
- Is less than or equal to (-le)
- Is greater than (-gt)
- Is greater than or equal to (-ge)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Most Boolean (true/false) fields support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Comparison Value

The value you enter for comparison must match the field type. For example, integer fields only support numerical values. String fields support all alphanumeric characters. Boolean fields only support True or False. The value field is not case sensitive. Date fields support only properly formatted dates and will initially display as mm/dd/yyyy. You can choose to populate the date field by:

- Clicking in a date Value field to open a pop-up calendar to select a date that will populate the field.
- Clicking in a segment of the date format (i.e., mm/dd/yyyy) and entering a value. As you continue to type in any one segment, the cursor will keep moving onto the next segment.

The results that match your search criteria will be displayed in the results grid below the search selection options.

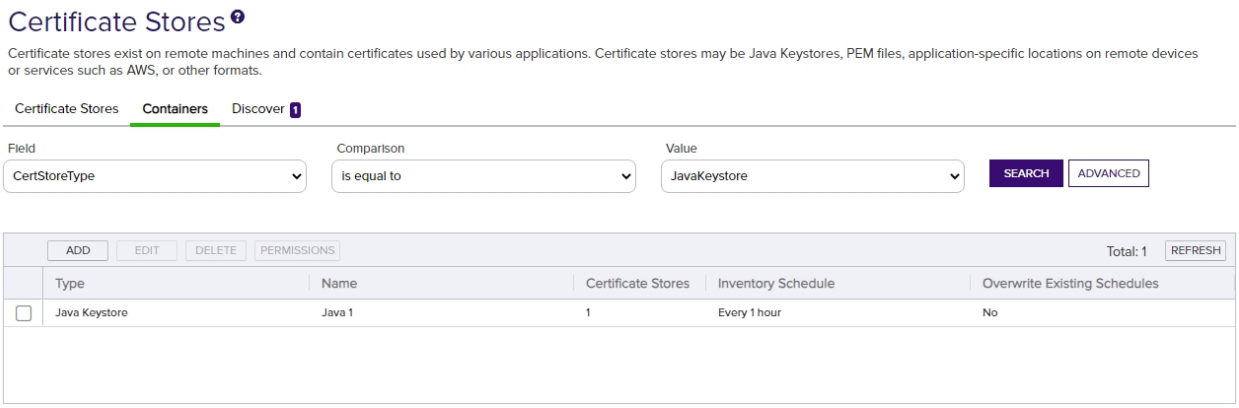


Figure 240: Certificate Store Container Search

The search results can be sorted by clicking on a column header in the results grid for most columns. Click the column header again to reverse the sort order. The grid columns can be arranged in any order desired by click-holding and dragging the header of the column you wish to move. The column widths may be adjusted by click-holding and dragging the line separating two column headers.

Advanced Searches

On any search page you can click **Advanced** to the right of the Search button to display the advanced search options. Click **Simple** to close the advanced search options again.

Multiple Criteria

Using the advanced search options, you can build a query based on multiple criteria using AND/OR logic. As with a simple search, you select a field and comparison operator in the drop-downs and then enter a comparison value, if applicable. Click **Insert** to add the search criteria to the query field below the selection fields. Use the selection fields to build multiple search criteria. Each time you click the insert button, an AND is added between the previous search criteria and the newly added one. You can change the AND to an OR if desired. You can use parentheses around portions of the query along with AND/OR to change the query meaning.

For example, for certificate searches:

```
(CN -contains "appsrvr" AND IssuedDate -ge "01/01/2022") OR (CN -contains "appsrvr" AND
TemplateShortName -contains "web")
```

This query will return all the certificates issued on or after January 1, 2022 with the string appsrvr in the CN and also all certificates issued at any time with the string appsrvr in the CN using a template referencing web. When you have entered all the desired search criteria, click **Search** to execute the query. If you wish to clear the query field and start over, click the **Clear** button.

Certificate Store Container Operations

Certificate store container operations include creating or editing containers—including scheduling inventory for the container—and deleting containers.

Adding or Modifying a Certificate Store Container

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:
Certificate Store Management: *Read*
Certificate Store Management: *Modify*

To add or edit a certificate store container:

1. In the Management Portal, browse to *Locations* > *Certificate Stores*.
2. On the Certificate Stores page, select the Containers tab.

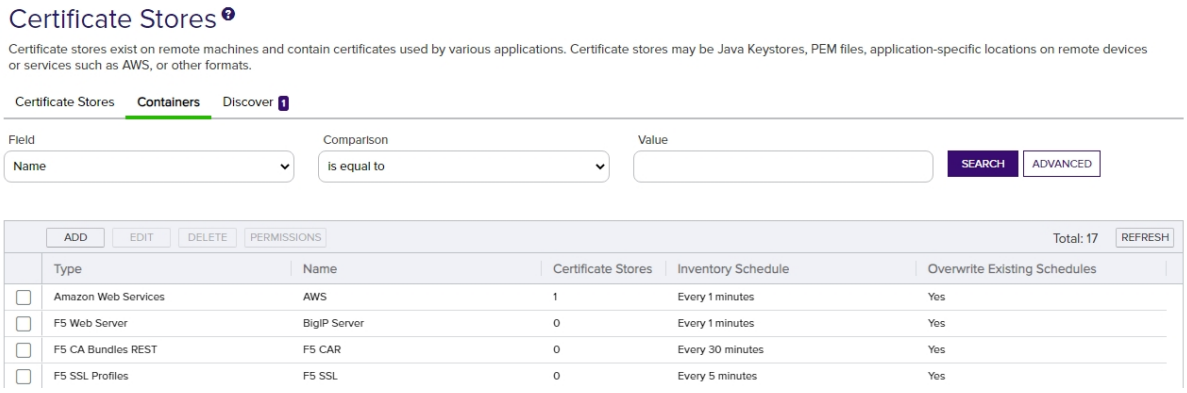


Figure 241: Certificate Store Containers

3. On the Containers tab, click **Add** to create a new container, or click **Edit** from either the top or right-click menu to modify an existing one.
4. In the Schedule Container dialog, select the appropriate **Type** for the container from the drop-down. This field cannot be modified on an edit.

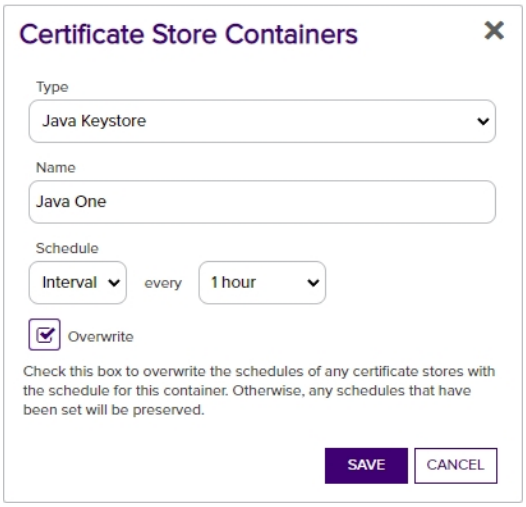


Figure 242: Define a Certificate Store Container

5. Enter a name for the container in the **Name** field.
6. In the **Inventory Schedule** fields, select an inventory frequency to apply as a default to certificate stores added to the container. The choices are:
    - Daily at a selected time
    - At intervals of anywhere from every one minute to every 12 hours
    - Off
7. If desired, check the **Overwrite Existing Schedules** box. This option will apply the schedule from the container to any stores in the container, including those that already have a schedule, whenever the container schedule is updated.
8. Click **Save** to save the container.

Deleting a Container

Deleting a container that contains certificate stores does not delete the associated certificate stores. The certificate stores will remain and be disassociated from the container.

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:
Certificate Store Management: *Read*
Certificate Store Management: *Modify*

To delete a certificate store container:

1. In the Management Portal, browse to *Locations > Certificate Stores*.
2. On the Certificate Stores page, select the Containers tab.

3. On the Containers tab, highlight the row in the certificate store containers grid of the container to delete and click **Delete** at the top of the grid or right-click the container in the grid and choose **Delete** from the right-click menu. Only one container may be deleted at a time.

4. On the Confirm Operation alert, click **OK** to confirm or **Cancel** to cancel the operation.

Container Permissions

Permissions for a container can be viewed or modified using the permission option on the certificate store containers tab. Container permissions can also be configured as part of the overall permission configuration on the security roles page. For more information, see Container Permissions on page 624 and Security Roles and Identities on page 609.

To view or modify permissions for a certificate store container:

1. In the Management Portal, browse to *Locations* > *Certificate Stores*.

2. On the Certificate Stores page, select the Containers tab.

3. On the Containers tab, highlight the row in the certificate store containers grid of the container for which to view permissions and click **Permissions** at the top of the grid or right-click the container in the grid and choose **Permissions** from the right-click menu.

4. In the Container Permissions dialog, review the permissions (Read, Schedule, and Modify) configured for each defined security role. To limit the security roles shown in the container permissions dialog, type a string in the filter box at the top of the dialog. For example, using a filter of *er* in the below-shown dialog will limit the results to Power Users, Renewal Handler API, and Revokers.

   Active checks indicate the top level permission that has been granted. Grayed out checks indicate permissions that have been inherited.

   To modify permissions, check or uncheck the desired permissions box.

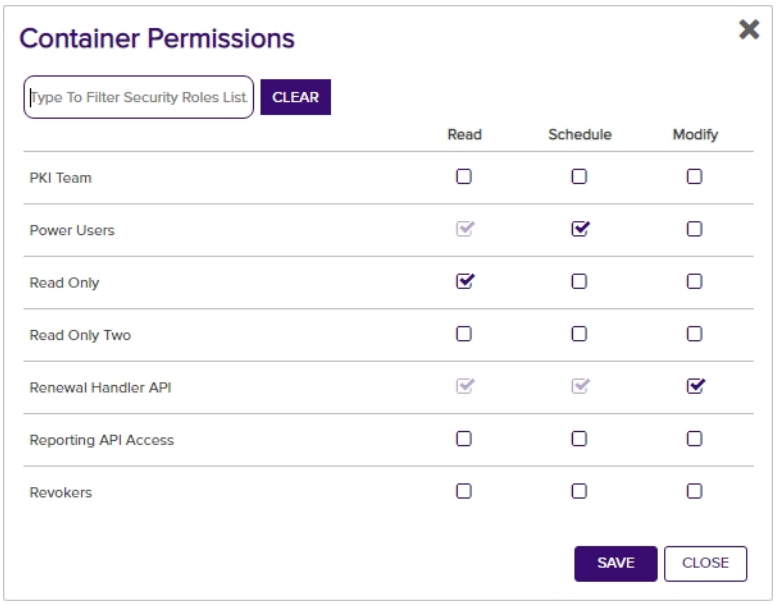


Figure 243: View or Modify Permissions on a Certificate Store Container

5. Click **Save** if you've made any changes, or just **Close** to close the dialog.

Certificate Store Discovery

The certificate store discovery feature is used to scan machines and devices for existing certificates and certificate stores, which can then be configured for management in Keyfactor Command. Certificate store discovery is supported for the following built-in features:

- PEM and Java certificate stores discovered by the Keyfactor Java Agent. Only stores to which the service account running the Keyfactor Command Java Agent has at least read permissions will be returned on a discover job.
- F5 bundle and SSL certificates discovered by the Keyfactor Windows Orchestrator on F5 devices using the F5 REST API (v13+).

The small number that appears on the tab to the right of the word Discover indicates how many discovered stores there are, if any. This acts as a reminder to check the discover tab for stores after a discovery job is complete.

Scheduling a Certificate Store Discovery Job

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:
Certificate Store Management: *Read*
Certificate Store Management: *Schedule*
Certificate Store Management: *Modify*
Privileged Access Management: *Read*

To use the certificate store discovery feature:

1. On the Certificate Store page, select the Discover tab.
2. On the Discover tab, click **Schedule**.
3. In the Schedule Discovery dialog, select Java Keystore, PEM File, F5 CA Bundles REST, or F5 SSL Profiles REST in the **Category** field dropdown. The remaining fields in the dialog will vary slightly depending on the category you selected.

Java Keystores

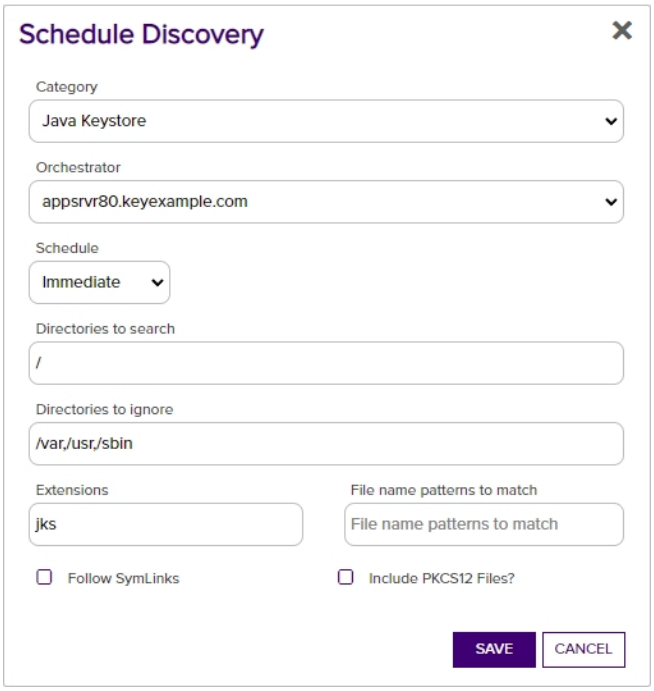


Figure 244: Schedule Java Keystore Discover Job

PEM Stores

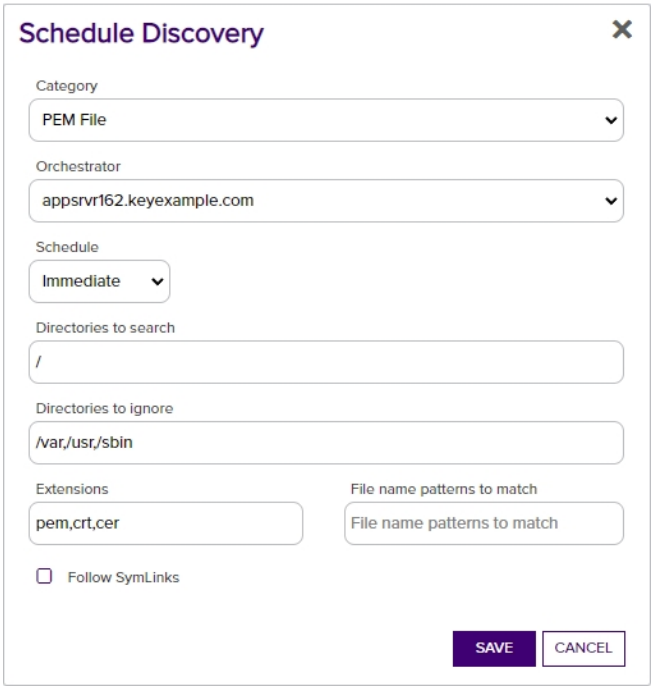


Figure 245: Schedule PEM Certificate Store Discover Job

F5 CA Bundle REST Stores

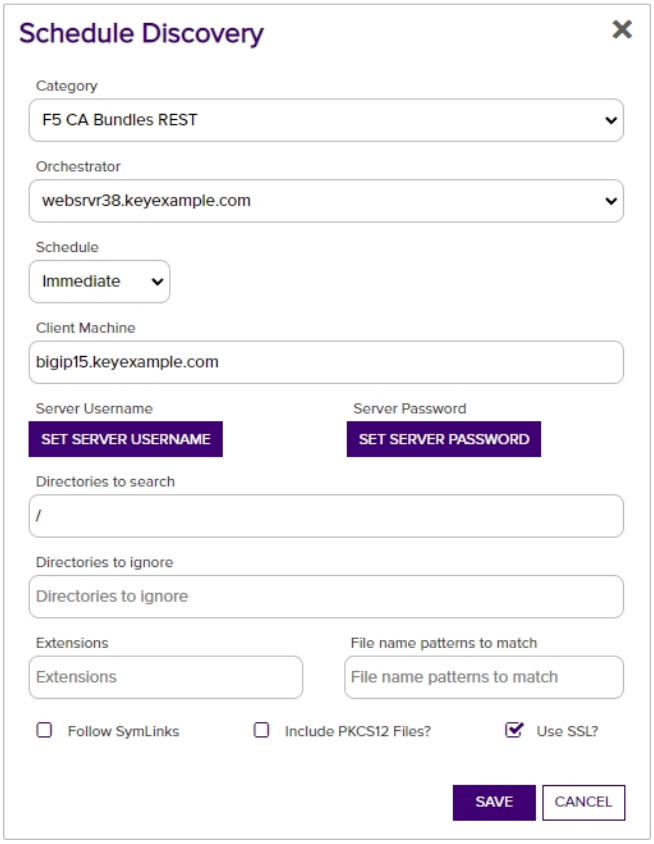


Figure 246: Schedule F5 CA Bundle Certificate Discover Job

F5 SSL Profile REST Stores

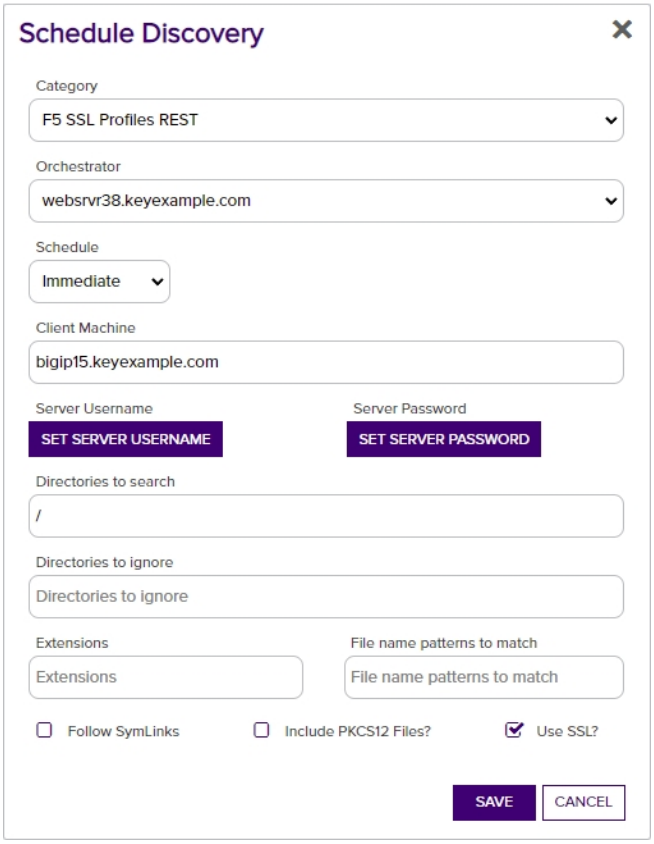


Figure 247: Schedule F5 SSL Profile Certificate Discover Job

4. In the Schedule Discovery dialog, select Java Keystore, PEM File, F5 CA Bundles REST, or F5 SSL Profiles REST in the **Category** field dropdown. The remaining fields in the dialog will vary slightly depending on the category you selected.

5. In the **Orchestrator** field, select the fully qualified domain name of the Keyfactor Universal Orchestrator[1], Windows Orchestrator, or Java Agent machine managing the scanning. In the case of Java Agents, this is also the machine you wish to scan for stores. This field is required.

6. In the **Schedule** dropdown, select either *Immediate*, to run the discover job within a few minutes of saving it, or *Exactly Once*, to select a date and time for the job. The default is Immediate.

7. For F5 discovery jobs, in the **Client Machine** field enter the fully qualified domain name or IP address of the F5 device to be scanned.

[1]Support for this functionality on the Keyfactor Universal Orchestrator requires the addition of a custom extension. Contact your Keyfactor representative for more information.

8. For F5 discovery jobs, click **Set Server Username** and, in the Server Username dialog, choose the source from which to load a user valid on the F5 device with Administrator permissions. In the Server Username dialog, the options are Load From Keyfactor Secrets or Load From PAM Provider. The *No Value* option is typically not supported for F5 stores.

   Note: Although a user with Resource Administrator permissions is sufficient when using the F5 methods that use the SOAP API, the F5 methods that use the REST API require full Administrator permissions.

   A Keyfactor secret is a user-defined password or other information that is encrypted and stored securely in the Keyfactor Command database. Although Keyfactor recommends using Privileged Access Management (see Privileged Access Management (PAM) on page 677) as a more secure solution to secure information, Keyfactor Secret is an option for customers that do not already have a relationship with a PAM provider such as CyberArk or Delinea (formerly Thycotic).

   Select the **Load From Keyfactor Secrets** radio button as the *Secret Source* if you want Keyfactor Command to encrypt and store the password in the Keyfactor Command database. Enter and confirm a password.

   Select the **Load from PAM Provider** radio button as the *Secret Source* if you want to store the password in a supported third-party PAM solution (see Privileged Access Management (PAM) on page 677). The remaining fields on the dialog will vary depending on the PAM provider.

   ### CyberArk

   Select CyberArk in the **Providers** dropdown if your PAM provider is CyberArk. The remaining fields in the dialog will then be:

   - PrivateArk Protected Password Name—The name of the username or password in the safe (see Create a CyberArk Password on page 683).
   - PrivateArk Folder Name—The path and name of the folder that stores the CyberArk Password (e.g. Root or Root\MyDir).

   ### Delinea (formerly Thycotic)

   Select Delinea in the **Providers** dropdown if your PAM provider is Delinea. The remaining field in the dialog will then be:

   - Delinea Secret ID—The numeric ID of the secret to retrieve from Secret Server (see Create a Delinea Secret Server Secret on page 687).

9. For F5 discovery jobs, click **Set Server Password** and, in the Server Password dialog, choose the source from which to load the password for the user specified with Set Server Username. In the Server Password dialog, the options are Load From Keyfactor Secrets or Load From PAM Provider. The *No Value* option is typically not supported for F5 stores.

A Keyfactor secret is a user-defined password or other information that is encrypted and stored securely in the Keyfactor Command database. Although Keyfactor recommends using Privileged Access Management (see Privileged Access Management (PAM) on page 677) as a more secure solution to secure information, Keyfactor Secret is an option for customers that do not already have a relationship with a PAM provider such as CyberArk or Delinea (formerly Thycotic).

Select the **Load From Keyfactor Secrets** radio button as the *Secret Source* if you want Keyfactor Command to encrypt and store the password in the Keyfactor Command database. Enter and confirm a password.

Select the **Load from PAM Provider** radio button as the *Secret Source* if you want to store the password in a supported third-party PAM solution (see Privileged Access Management (PAM) on page 677). The remaining fields on the dialog will vary depending on the PAM provider.

CyberArk

Select CyberArk in the **Providers** dropdown if your PAM provider is CyberArk. The remaining fields in the dialog will then be:

- PrivateArk Protected Password Name—The name of the username or password in the safe (see Create a CyberArk Password on page 683).
- PrivateArk Folder Name—The path and name of the folder that stores the CyberArk Password (e.g. Root or Root\MyDir).

Delinea (formerly Thycotic)

Select Delinea in the **Providers** dropdown if your PAM provider is Delinea. The remaining field in the dialog will then be:

- Delinea Secret ID—The numeric ID of the secret to retrieve from Secret Server (see Create a Delinea Secret Server Secret on page 687).

10. In the **Directories to search** field, specify the directory or directories to search. Multiple directories should be separated by commas. This field is required.

Java

For Java discovery, enter at a minimum either "/" for a Linux server or "c:\" for a Windows server (without the quotation marks).

PEM

For PEM discovery, enter at a minimum either "/" for a Linux server or "c:\" for a Windows server (without the quotation marks).

F5

For F5 discovery, enter "/" (without the quotation marks).

11. For F5 discovery jobs, check the **Use SSL** box to use SSL to communicate with the F5 device or cluster. The F5 device must trust the CA that issued the certificate used to protect the Keyfactor Command server if you select this option or you must set the *Ignore Server SSL Warnings* application setting to True (see Application Settings on page 583).
12. Populate the remaining optional fields as needed. See Table 16: Discovery Options.
13. Click **Save** to schedule the discovery task. Once the scan begins, it may take several minutes to complete.
14. Return to the Discover tab for the results of the scan. Check the Orchestrator Jobs page (see Orchestrator Job Status on page 493) to review jobs in progress.

Table 16: Discovery Options

Option	Description
Category	Select the type of certificate store to scan.
Orchestrator	Select the fully qualified domain name of the Keyfactor Universal Orchestrator, Windows Orchestrator, or Java Agent machine managing the scanning. In the case of Java Agents, this is also the machine to be scanned for certificate stores. This field is required.
Schedule	Specify the schedule for the scan—Immediate or Exactly Once. If you select Exactly Once, select a date and time for the scan. The default is Immediate.
Client Machine	For F5 devices, enter the fully qualified domain name or IP address of the F5 device or cluster to be scanned for certificates. This option applies only to F5 CA bundle and F5 SSL profile discover jobs. This field is required.
Server Username	For F5 devices, set the username used to authenticated to the device or cluster.
Server Password	For F5 devices, set the password used to authenticated to the device or cluster.
Directories to search	Specify the directory or directories to be searched. Multiple directories should be separated by commas. All directories specified to which the service account user (the user account that the Java agent is operating as or the user configured for the F5 device using the Change Credentials option) has read rights will be searched other than the excluded directories specified using the *Directories to ignore* option. It is not necessary to use quotation marks around directory paths containing spaces. For F5, the path should be specified as "/" (without the quotation marks). This field is required.

Option	Description
Directories to ignore	Specify any directories that should not be included in the search. Multiple directories should be separated by commas. It is not necessary to use quotation marks around directory paths containing spaces.
Extensions	Specify file extensions for which to search. For example, search for files with the extension *jks* but not *txt*. The dot should not be included when specifying extensions.
File name patterns to match	Specify all or part of a string against which to compare the file names of certificate store files and return only those that contain the specified string. It is not necessary to use quotation marks around strings containing spaces.
Follow SymLinks	If this option is specified, the tool will follow symbolic links on Linux and UNIX operating systems and report both the actual location of a found certificate store file in addition to the symbolic link pointing to the file. This option is ignored for searches of Windows-based Java Agents.
Include PKCS12 Files	If this option is specified, the tool will use the compatibility mode introduced in Java version 1.8 to locate both JKS and PKCS12 type files. This option applies only to Java keystore discover jobs.
Use SSL	For F5 devices, use SSL to communicate to the device or cluster.

Managing Discovered Certificate Stores

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:
Certificate Store Management: *Read*
Certificate Store Management: *Modify*
Privileged Access Management: *Read*

To manage discovered certificate stores:

1. In the Management Portal, browse to *Locations* > *Certificate Stores*.
2. On the Certificate Stores page, select the Discover tab.
3. On the Discover tab, highlight one or more store row(s) in the grid and click **Manage** at the top of the grid or right-click the store in the grid and choose **Manage** from the right-click menu. Java keystores require entry of the store password or PAM credential access information during the approval process. If you select more than one Java keystore for approval at the same time, they must all share the same password or PAM information. The right-click menu supports operations on only one store at a time.

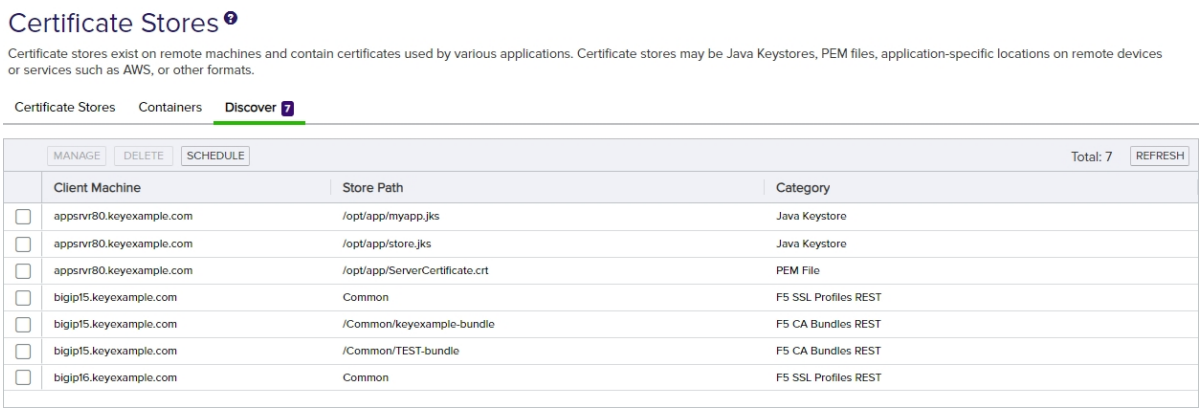


Figure 248: Discovered Certificate Stores

For a Java Keystore

In the Approve Certificate Stores dialog configure the following fields:

- If desired, select a **Container** from the dropdown.
- Click the **Set Password** button to enter the password for the keystore. In the Password dialog, the options are No Value, Load From Keyfactor Secrets, and Load From PAM Provider.

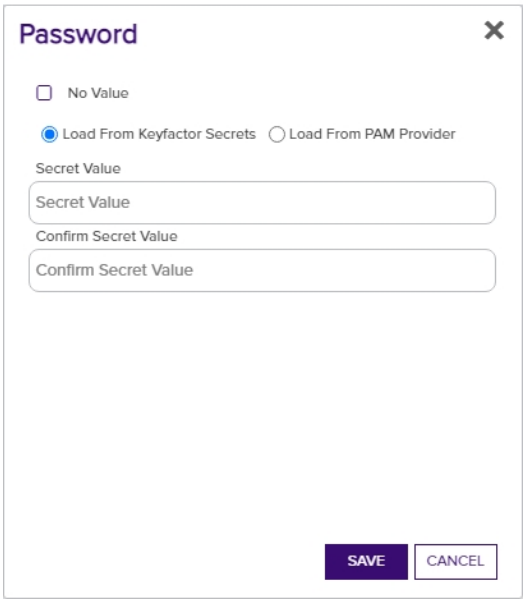


Figure 249: Java Keystore Set Password

Select **No Value** if your keystore does not have a password configured.

A Keyfactor secret is a user-defined password or other information that is encrypted and stored securely in the Keyfactor Command database. Although Keyfactor recommends using Privileged Access Management (see Privileged Access Management (PAM) on page 677) as a more secure solution to secure information, Keyfactor Secret is an option for customers that do not already have a relationship with a PAM provider such as CyberArk or Delinea (formerly Thycotic).

Select the **Load From Keyfactor Secrets** radio button as the *Secret Source* if you want Keyfactor Command to encrypt and store the password in the Keyfactor Command database. Enter and confirm a password.

Select the **Load from PAM Provider** radio button as the *Secret Source* if you want to store the password in a supported third-party PAM solution (see Privileged Access Management (PAM) on page 677). The remaining fields on the dialog will vary depending on the PAM provider.

CyberArk

Select CyberArk in the **Providers** dropdown if your PAM provider is CyberArk. The remaining fields in the dialog will then be:

- PrivateArk Protected Password Name—The name of the username or password in the safe (see Create a CyberArk Password on page 683).
- PrivateArk Folder Name—The path and name of the folder that stores the CyberArk Password (e.g. Root or Root\MyDir).

Delinea (formerly Thycotic)

Select Delinea in the **Providers** dropdown if your PAM provider is Delinea. The remaining field in the dialog will then be:

- Delinea Secret ID—The numeric ID of the secret to retrieve from Secret Server (see Create a Delinea Secret Server Secret on page 687).

- Select a **Type** from the dropdown. The default is JKS.

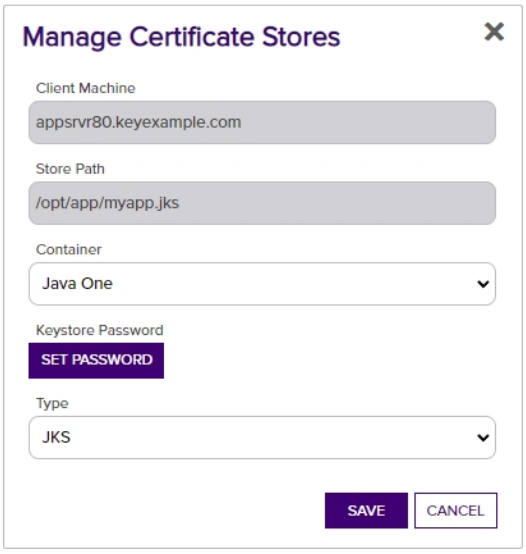


Figure 250: Manage a Discovered Java Certificate Store

For a PEM certificate store

In the Approve Certificate Stores dialog configure the following fields:

- If desired, select a **Container** from the dropdown.
- If the certificate store has a **Separate Private Key** file, select the *True* radio button.
- If the certificate store has a separate private key, enter the path and filename for the key file in the **Path to Private Key File** field.

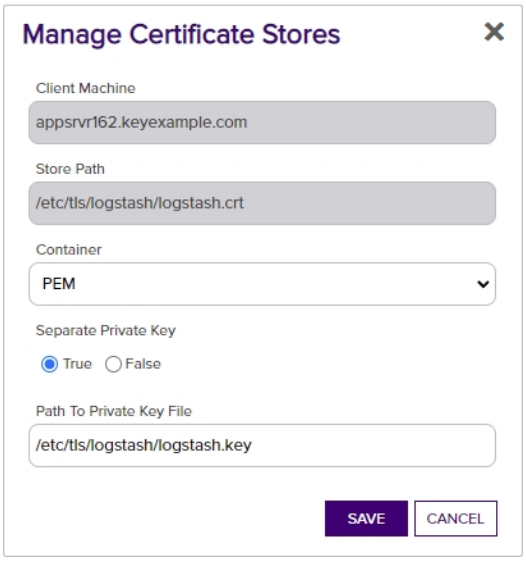


Figure 251: Manage a Discovered PEM Certificate Store

For an F5 CA Bundle certificate

In the Approve Certificate Store dialog configure the following fields:

- If desired, select a **Container** from the dropdown.
- In the **Primary Node** field, enter the fully qualified domain name of the F5 device that acts as the primary node in a highly available F5 implementation. If you're using a single F5 device, this will often be the same value you entered in the Client Machine field.

  Tip: Configuration of the primary node is necessary to allow management jobs that update certificates on the F5 device to wait until the primary node is available before making their update. Inventory jobs are carried out against any available node.

- In the **Primary Node Check Retry Wait Seconds** field, either accept the default value of 120 seconds or enter a new value. This value represents the number of seconds the orchestrator will wait after a pending management job cannot be completed because the primary node cannot be contacted before trying to contact the primary node again to retry the job.
- In the **Primary Node Check Retry Maximum** field, either accept the default value of 3 retry attempts or enter a new value. This value represents the number of times the orchestrator will retry a pending management job that is failing because the primary node cannot be contacted before declaring the job failed.

- In the **Version of F5** dropdown, select the version of F5 this server is running. The F5 REST API is supported on version 13 and up.

  Tip: Select v15 for version 15 and above.

- Click **Set Server Username** to choose the source from which to load a user valid on the F5 device with *Administrator* permissions. In the Server Username dialog, the options are Load From Keyfactor Secrets or Load From PAM Provider. The *No Value* option is typically not supported for F5 stores.

  Note: Although a user with Resource Administrator permissions is sufficient when using the F5 methods that use the SOAP API, the F5 methods that use the REST API require full Administrator permissions.

- Click **Set Server Password** to choose the source to load a valid password for the server. In the Server Password dialog, the options are Load From Keyfactor Secrets or Load From PAM Provider. The *No Value* option is typically not supported for F5 stores.

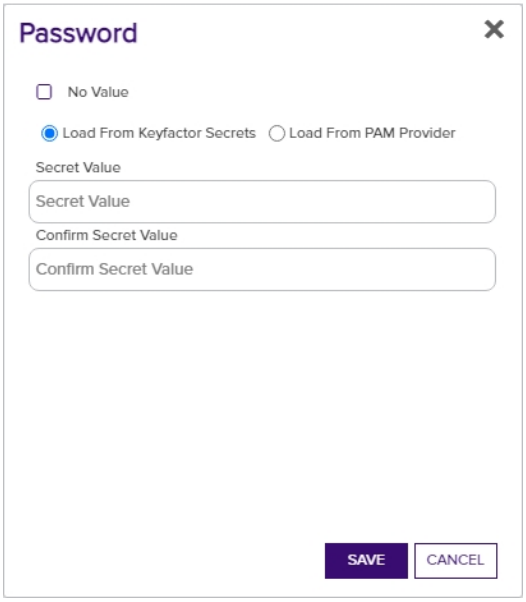


Figure 252: F5 CA Bundle Set Password

A Keyfactor secret is a user-defined password or other information that is encrypted and stored securely in the Keyfactor Command database. Although Keyfactor recommends using Privileged Access Management (see Privileged Access Management (PAM) on page 677) as a more secure solution to secure information, Keyfactor Secret is an option

for customers that do not already have a relationship with a PAM provider such as CyberArk or Delinea (formerly Thycotic).

Select the **Load From Keyfactor Secrets** radio button as the *Secret Source* if you want Keyfactor Command to encrypt and store the password in the Keyfactor Command database. Enter and confirm a password.

Select the **Load from PAM Provider** radio button as the *Secret Source* if you want to store the password in a supported third-party PAM solution (see Privileged Access Management (PAM) on page 677). The remaining fields on the dialog will vary depending on the PAM provider.

CyberArk

Select CyberArk in the **Providers** dropdown if your PAM provider is CyberArk. The remaining fields in the dialog will then be:

- PrivateArk Protected Password Name—The name of the username or password in the safe (see Create a CyberArk Password on page 683).
- PrivateArk Folder Name—The path and name of the folder that stores the CyberArk Password (e.g. Root or Root\MyDir).

Delinea (formerly Thycotic)

Select Delinea in the **Providers** dropdown if your PAM provider is Delinea. The remaining field in the dialog will then be:

- Delinea Secret ID—The numeric ID of the secret to retrieve from Secret Server (see Create a Delinea Secret Server Secret on page 687).

- In the **Use SSL** section, select *True* to use SSL to communicate with the F5 device or cluster, if desired. The F5 device must trust the CA that issued the certificate used to protect the Keyfactor Command server if you select this option or you must set the *Ignore Server SSL Warnings* application setting to *True* (see Application Settings on page 583).

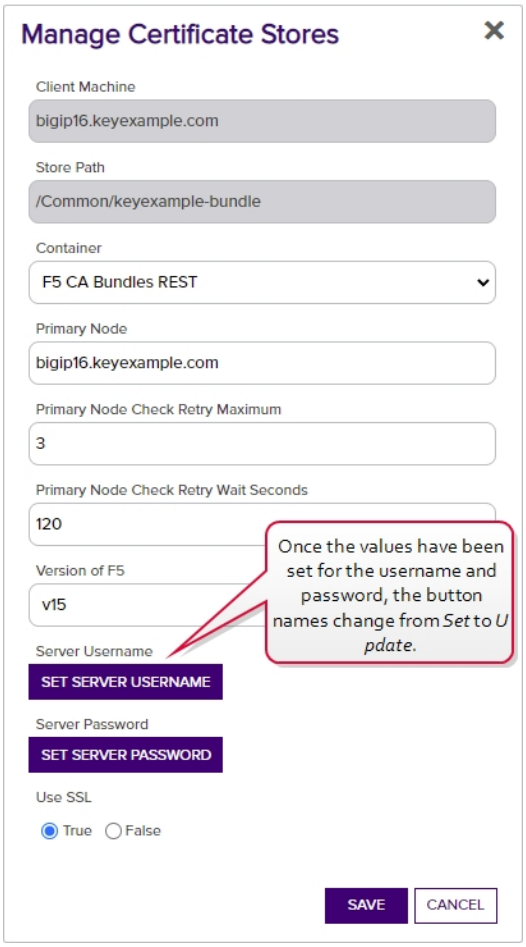


Figure 253: Manage a Discovered F5 CA Bundle Certificate

For an F5 SSL Profile certificate

In the Approve Certificate Store dialog configure the following fields:

- If desired, select a **Container** from the dropdown.
- In the **Primary Node** field, enter the fully qualified domain name of the F5 device that acts as the primary node in a highly available F5 implementation. If you're using a single F5 device, this will often be the same value you entered in the Client Machine field.

> **Tip:** Configuration of the primary node is necessary to allow management jobs that update certificates on the F5 device to wait until the primary node is available before making their update. Inventory jobs are carried out against any available node.

- In the **Primary Node Check Retry Wait Seconds** field, either accept the default value of 120 seconds or enter a new value. This value represents the number of seconds the orchestrator will wait after a pending management job cannot be completed because the primary node cannot be contacted before trying to contact the primary node again to retry the job.
- In the **Primary Node Check Retry Maximum** field, either accept the default value of 3 retry attempts or enter a new value. This value represents the number of times the orchestrator will retry a pending management job that is failing because the primary node cannot be contacted before declaring the job failed.
- In the **Version of F5** dropdown, select the version of F5 this server is running. The F5 REST API is supported on version 13 and up.

  Tip: Select v15 for version 15 and above.

- Click **Set Server Username** to choose the source from which to load a user valid on the F5 device with *Administrator* permissions. In the Server Username dialog, the options are Load From Keyfactor Secrets or Load From PAM Provider. The *No Value* option is typically not supported for F5 stores.

  Note: Although a user with Resource Administrator permissions is sufficient when using the F5 methods that use the SOAP API, the F5 methods that use the REST API require full Administrator permissions.

- Click **Set Server Password** to choose the source to load a valid password for the server. In the Server Password dialog, the options are Load From Keyfactor Secrets or Load From PAM Provider. The *No Value* option is typically not supported for F5 stores.

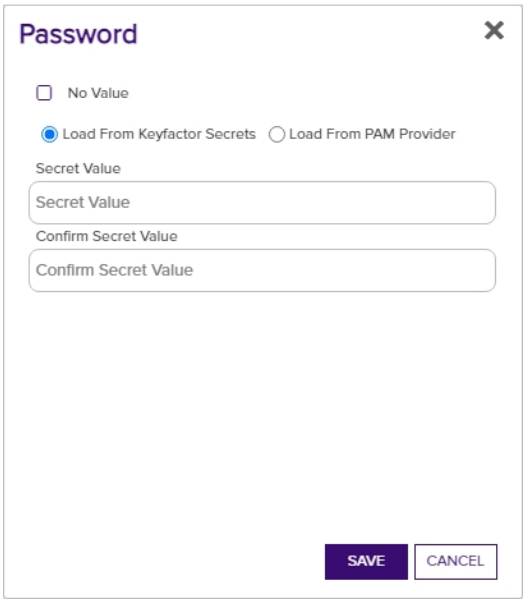


Figure 254: F5 SSL Profiles Set Password

A Keyfactor secret is a user-defined password or other information that is encrypted and stored securely in the Keyfactor Command database. Although Keyfactor recommends using Privileged Access Management (see Privileged Access Management (PAM) on page 677) as a more secure solution to secure information, Keyfactor Secret is an option for customers that do not already have a relationship with a PAM provider such as CyberArk or Delinea (formerly Thycotic).

Select the **Load From Keyfactor Secrets** radio button as the *Secret Source* if you want Keyfactor Command to encrypt and store the password in the Keyfactor Command database. Enter and confirm a password.

Select the **Load from PAM Provider** radio button as the *Secret Source* if you want to store the password in a supported third-party PAM solution (see Privileged Access Management (PAM) on page 677). The remaining fields on the dialog will vary depending on the PAM provider.

CyberArk

Select CyberArk in the **Providers** dropdown if your PAM provider is CyberArk. The remaining fields in the dialog will then be:

- PrivateArk Protected Password Name—The name of the username or password in the safe (see Create a CyberArk Password on page 683).
- PrivateArk Folder Name—The path and name of the folder that stores the CyberArk Password (e.g. Root or Root\MyDir).

Delinea (formerly Thycotic)

Select Delinea in the **Providers** dropdown if your PAM provider is Delinea. The remaining field in the dialog will then be:

- Delinea Secret ID—The numeric ID of the secret to retrieve from Secret Server (see Create a Delinea Secret Server Secret on page 687).

- In the **Use SSL** section, select *True* to use SSL to communicate with the F5 device or cluster, if desired. The F5 device must trust the CA that issued the certificate used to protect the Keyfactor Command server if you select this option or you must set the *Ignore Server SSL Warnings* application setting to *True* (see Application Settings on page 583).

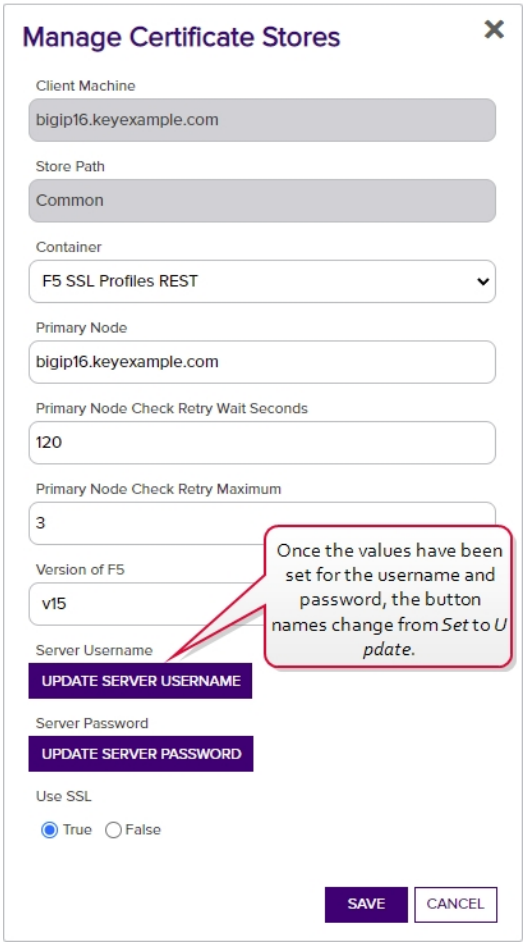


Figure 255: Manage a Discovered F5 SSL Profile Certificate

Deleting a Discovered Certificate Store

Discovered certificate stores can be deleted one at a time or in multiples.

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:
Certificate Store Management: *Read*
Certificate Store Management: *Modify*

To delete a discovered certificate store:

1. In the Management Portal, browse to *Locations* > *Certificate Stores*.
2. On the Certificate Stores page, select the Discover tab.
3. On the Discover tab, highlight the row(s) in the discover grid of the store(s) to delete and click **Delete** at the top of the grid or right-click the store location in the grid and choose **Delete** from the right-click menu. The right-click menu supports operations on only one store at a time.
4. On the Confirm Operation alert, click **OK** to confirm or **Cancel** to cancel the operation.

2.1.8.4 SSL Discovery

SSL network discovery and monitoring is used to survey designated internet-facing or internal IP addresses and ports to locate and import certificates, as well as alert certificate owners when the certificates are nearing expiration or are not found. Discovery jobs scan network segments to locate certificates at TLS endpoints; whereas, monitoring jobs inspect certificates for health and expiration and notify recipients regarding the status of the certificates. With the introduction of the Keyfactor Universal Orchestrator, SSL discovery can scan TLS 1.3 endpoints using any of the 5 ciphersuites referenced in appendix B.4 of RFC 8446.

SSL network discovery and monitoring scanning is performed by orchestrators that are assigned to orchestrator pools. An orchestrator pool contains orchestrators that support SSL discovery and monitoring capabilities for its networks. Orchestrator architecture allows for a pool of orchestrators to work in parallel to execute scan jobs. Based on defined schedules, Keyfactor Command creates discovery or monitoring scan jobs. Several scan jobs may be created from one large request. Orchestrators poll the Keyfactor Command Service to determine if scan jobs are available. Scan jobs are then executed by available orchestrators. Keyfactor Command automatically distributes the scanning load across the orchestrators in the pool by generating and managing individual scan jobs. Additionally, the orchestrator that discovers the certificate can be different than the orchestrator that monitors the certificate.

The orchestrator SSL scanning process will attempt to scan with and without server name indication (SNI) for endpoints specified by host name during discovery scans and only use SNI during a monitoring scan if the endpoint has an SNI name from the discovery scan. Whenever an endpoint is defined to scan by its host name, the orchestrator will try to scan that endpoint twice, one normal scan against the endpoint and one using the supplied host name as the SNI extension.

Keyfactor Command is installed with a *Default Orchestrator Pool* that holds all the orchestrators that have been configured for SSL network discovery and monitoring. Custom orchestrator pools can be created as needed.

Note: The orchestrators in the network's orchestrator pool must have access to the network the pool is assigned to scan. Ideally, orchestrators are placed in close network proximity to the addresses they are configured to scan. Scanning across WAN or slow network links can impact performance and potentially miss certificates due to timeouts or network congestion. Additionally, firewalls between the orchestrators and their target networks need to be configured to allow connections to the scanned addresses and ports.

SSL network discovery and monitoring is divided into three areas:

- **Network Definitions**

  Network definitions are used to define a collection of networks that will be scanned by the designated orchestrator pool. Networks are defined using IP addresses, ports and hostnames. Within this option, you can schedule discovery and/or monitoring tasks. You can also configure networks to automatically tag a discovered endpoint with a certificate for monitoring.

- **Orchestrator Pools Definition**

  On the orchestrator pools definition tab you define a group of available orchestrators that support the SSL discovery and monitoring capabilities. For each orchestrator added to the orchestrator pool, you can select discover and/or monitor option(s).

- **Results**

  The results tab shows the results of endpoints that have been scanned, including both positive (true, a certificate was found) or negative (false, a certificate was not found) results. If a response was received from an endpoint during a scan, it is included in the results; negative results are hidden by default. The *Monitor Status* (True/False) and *Reviewed Status* (True/False) of an endpoint are included in the results tab.

The SSL network discovery and monitoring features can only be used if at least one compatible (see the *Compatibility Matrix* in the *Keyfactor Command Documentation Suite*) instance of the Keyfactor Universal Orchestrator or Windows Orchestrator is running in the environment and the orchestrator has been approved in the Management Portal. Keyfactor recommends that the orchestrator(s) used for SSL network discovery and monitoring be installed on a server other than the primary Keyfactor Command server(s) due to the resource requirements of the scanning process when scanning large network segments.

Tip: Click the help icon (?) next to the page title to open the embedded web copy of the *Keyfactor Command Documentation Suite* to this section.
You can also find the help icon at the top of the page next to the **Log Out** button. From here you can choose to open either the *Keyfactor Command Documentation Suite* at the home page or the *Keyfactor API Endpoint Utility*.

Network Definitions

On the Network Definitions tab you can create, edit and delete networks, and run and view scans. This section is also used to view the results of the discovery and monitoring jobs by linking directly to the Results tab for a selected network.

Discovery jobs attempt to initiate TLS connections to specified IP addresses and ports or ranges of IP addresses and ports. If a TLS connection is successful, the certificates provided by the target server as part of the TLS handshake are downloaded for further inspection and importation into the Keyfactor Command database. Locations that provide any level of response during the connection attempt (don't time out) are shown in the results grid when the discovery scan finishes regardless of whether a certificate was successfully downloaded. If a TCP connection is established, but a TLS connection is not, an SSL connection will be attempted. Any certificate obtained via SSL connection will be imported into the Keyfactor Command database. If a TLS connection is successful, an SSL connection will not be attempted.

Monitoring jobs scan a chosen set of locations that have already been discovered by a discovery job scan. Like discovery jobs, monitoring jobs attempt to initiate TLS connections with the locations specified. In the case of monitoring jobs, however, a certificate is expected at the endpoint since endpoints are generally identified for monitoring if they have certificates that need monitoring. As a result, monitoring jobs report on timeouts as well as connection failures and successes.

The network definitions grid includes these fields:

Name

The name of the network.

Orchestrator Pool

The name of the orchestrator pool (see Orchestrator Pools Definition on page 459).

Discovery Status

The current status of the discovery job for the network, if configured. The possible statuses are:

- *Scheduled* indicates a job has been scheduled but has never run.
- *Last Scanned* indicates a job has run to completion. The date indicates when the job finished.
- *Running* indicates a job is currently in progress. The percentage complete shown will be zero for small jobs for the entire duration of the job because this value is updated upon completion of each segment of a scan job (and small jobs generally consist of only one segment).
- *In Quiet Hours* indicates that a quiet hours time window for the job is currently in effect and no jobs can be run (see SSL Network Operations on the next page).
- *Disabled* indicates that the *Scanning Enabled* box has been unchecked in the network definition

Monitor Status

The current status of the monitoring job for the network, if configured. The possible statuses are the same as those for discovery.

Description

The description entered in the network definition.

(see SSL Network Operations below). No scanning jobs will be run when the network is in this state.

SSL Network Operations

SSL Network Operations include adding, editing and deleting SSL network definitions, initiating a manual scan and monitoring scheduled network scan jobs.

Tip: SSL scan jobs use priority rules to determine which job segments run first if there are multiple job segments to be run (large jobs are divided into multiple job segments—see Monitoring Network Scan Jobs with View Scan Details on page 454). Job segments are run with the following priority rules:

- Job segments for Scan Now jobs (see Initiating a Manual Scan on page 455) are run ahead of those for scheduled jobs.
- New job segments for in-progress jobs with multiple segments are prioritized based on job age—segments for jobs that have been running the longest move to the front of the line.
- New job segments for in progress jobs with multiple segments start ahead of job segments for jobs that have not yet started.

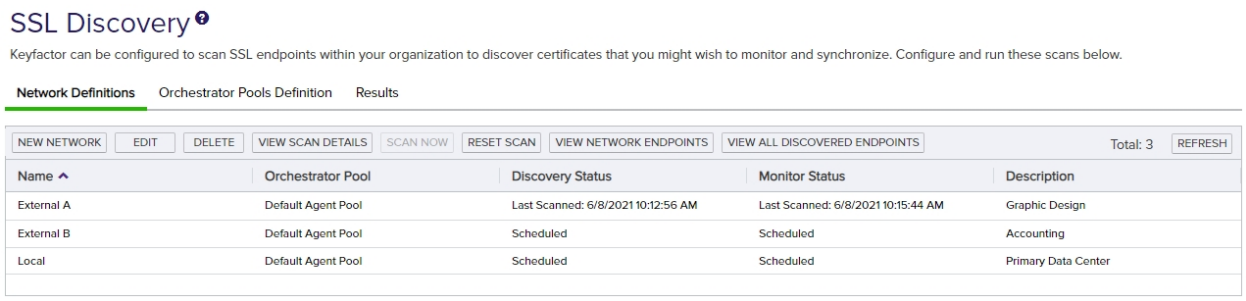


Figure 256: SSL Network Discovery

Adding or Modifying an SSL Network

To define a new network or edit an existing one:

1. In the Management Portal, browse to *Locations > SSL Discovery.*
2. On the SSL Network Discovery page, select the Network Definitions tab (the default when you first visit the page).
3. On the Network Definitions tab, click **New Network** to setup a network to scan, or select an existing network from the grid and click **Edit.**
4. The SSL Network Definition dialog is divided into four tabs: Basic, Advanced, Network Ranges, and Quiet Hours. Enter the network information for each tab, as required. Each tab is described

in detail below.

Basic Tab

In the SSL Network Definition dialog on the Basic tab, enter the following information:

- **Name**: Enter a name for the network. The network name can be anything; however, it is recommended that the name reflect the subnet or location that you will be discovering with the network.

  Tip: The SSL network name is searchable with certificate search and also appears in the location details grid of the certificate details, if the certificate was found during an SSL scan.

- **Description**: Enter a description for the network.
- **Orchestrator Pool**: From the dropdown, select an orchestrator pool that contains orchestrators with SSL discovery and monitoring capabilities.

  Note: Keyfactor Command is installed with a Default Orchestrator Pool and orchestrators with SSL discovery and monitoring capabilities created in Keyfactor Command are automatically assigned to that pool.

- **Discovery/Monitoring Schedule**: Select the discovery and monitoring job frequency. Possible options are:
  - Off—No jobs will run.
  - Daily—Enter selected time.
  - Interval—Enter an interval from every 10 minutes to every 12 hours.
  - Weekly—Enter a selected day or days of the week at a selected time.
  - Monthly—Enter a selected day of the month (1st through 27th) at a selected time.

  Note: The configured schedule determines when the scan is requested to start. The actual start of the scan is dependent on the orchestrator heartbeat Interval, which is defined by the *Heartbeat Interval (minutes)* application setting (see Application Settings on page 583). The default is 5 minutes.

- **Notification Recipients**: Enter one or more email address(es) of the recipients who should receive monitoring results (newline separated).

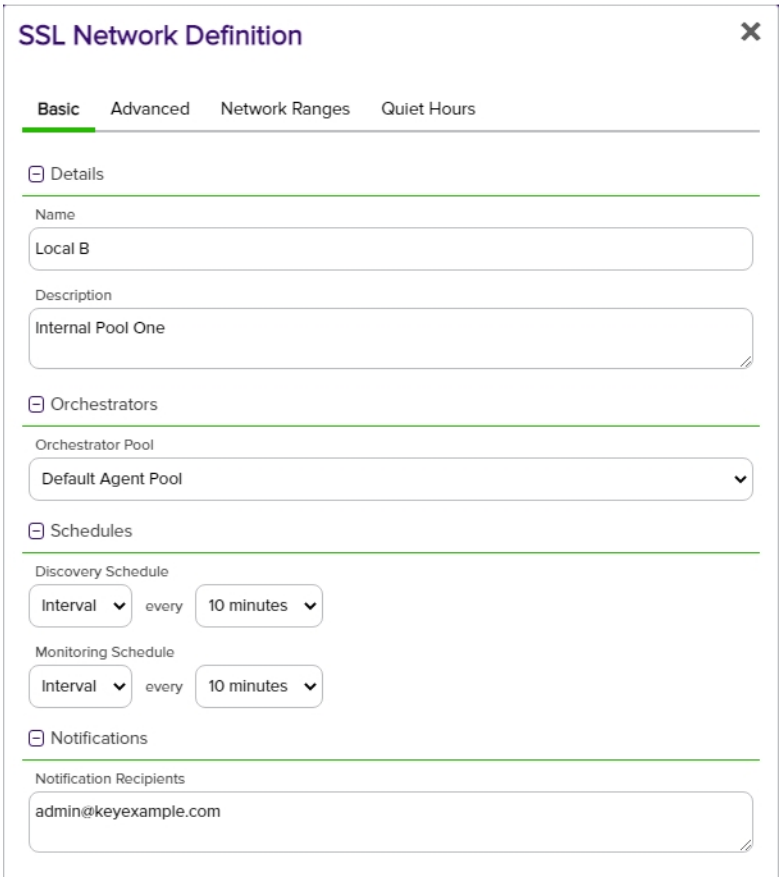


Figure 257: Define a New Network—Basic Tab

Advanced Tab

In the SSL Network Definition dialog on the Advanced tab, enter the following information:

- **Scanning Enabled** : Click to enable scanning for the network. If unchecked, no new network scans will be scheduled, but the current scan will finish, if this setting is changed during a scan also, the network will appear as *Disabled* on the SSL Network Discovery page.
- **Automatically monitor network endpoints during discovery**: Enable this option to instruct the orchestrator to tag endpoint certificates, found during discovery scanning, for monitoring. It is recommended to enable this option.
- **Request robots.txt**: Each network definition contains an option to do a GET on robots.txt on endpoints. Orchestrators perform a GET /robots.txt request to behave like a webcrawler and provide an explanation of network activity.

- **Discover Timeout (in ms)**: Enter the amount of time (in milliseconds) the scan will wait (before timing out) to discover the endpoint. Shorter timeout periods will increase the overall scanning throughput, however will also increase the chance of missing a certificate on a slow or congested network
- **Monitor Timeout (in ms)**: Enter the amount of time (in milliseconds) the scan will wait (before timing out) to receive the discovered endpoint certificate expiration details.
- **Expiration Alert (in days)**: Enter the number of days within which to begin warning regarding upcoming expiration in notification email messages.

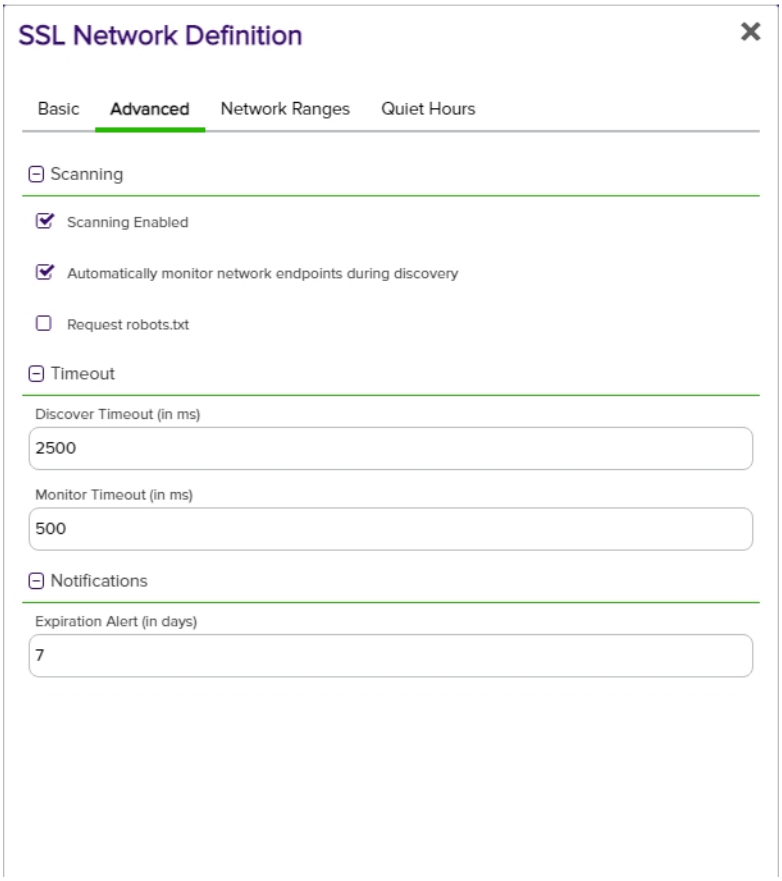


Figure 258: Define a New Network—Advanced Tab

Network Ranges Tab

There are two sections to the Network Ranges Tab: **Add Range** and **Ranges**. For each named network defined, multiple ranges are allowed. New networks can be added by using either the *add range tool*, or pasting the IP address, hostname, or network notation into the Network Ranges box.

The Add Range section

The **Add Range** section is for adding new networks via the *add range tool.* When you open the Network Ranges tab, the **Add Range** section shows default values of:

- **Type**: Network Notation
- **CIDR Block**: 0.0.0.0/24:443

Notice that the details grid reflects the default value and the default type—*network notation*. As you begin entry of a new network range of the type *network notation*, the details section will reflect your entries as you type, allowing you to verify your entry. The details grid will not show if you chose another type of notation.

Define new network locations, using the add range tool, as follows:

a. In the **Add Range** section of the page, select your desired method for adding a location in the **Type** dropdown. The available options are:

   - **Network Notation**: Enter an IP address range using CIDR notation by populating the **CIDR Block** field and selecting the desired subnet in the dropdown. The default subnet is /24, which is one full octet of variability, or 254 locations.
   - **IP Address**: Enter a single IP address by populating the **IP Address** field and adding one port.
   - **Host Name**: Add a single location using a host machine name by filling in the **Host Name** field in the host name section and adding one port. During scans, host names are converted to IP addresses and scans are conducted via IP address. Keyfactor Command will do two scans against that address, one using the hostname as the SNI (server name indication) and one not using SNI. This is because different servers can be hosted on the same IP address but are accessed via different SNIs (or without one at all).

     Note: All methods support adding multiple ports, either comma separated (433,450), or as a range (433-450).

b. Enter the desired network notation, IP address, or host name, and click the **Add** action button.

c. Repeat this step for multiple IP addresses or host names. Each entry will be added as a newline in the Network Ranges box at the bottom of the dialog.

d. Click **Save**.

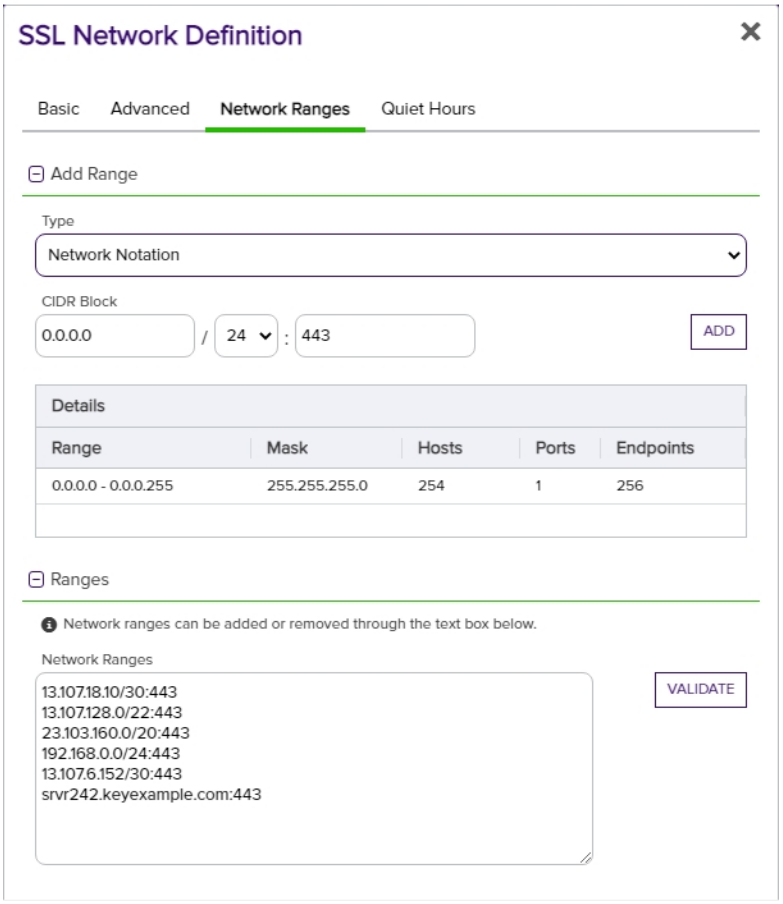


Figure 259: Define a New Network—Network Ranges Tab

The details grid displays only for the type *network notation* and will only display the value being typed in the CIDR block, or the last value entered. The fields in the details grid are defined as follows:

- **Range**: This is the range of addresses reflected by the CIDR notation entered.
- **Mask**: Defined by the bitmask (between 1 -30) applied to the address in the CIDR block to identify the IP addresses included. The bigger the mask the fewer IP addresses will fall under the defined range. For example, with a "/24", the first 3 sections of the IP address must match exactly, while the last section can be any value from 0 to 255.
- **Hosts**: This is the number of useable IP addresses in a given CIDR. (This is always two less than the number of endpoints. This is because the smallest address is reserved as

the address of the overall network the CIDR represents, while the largest is used as the broadcast address).

- **Ports**: This is the number of ports the given CIDR will have.
- **Endpoints**: The endpoints number reflects the number of endpoints based on the network size (/24, /25, etc) times the number of ports defined. Each time you go up in network size the network number will double (”/24” has 256, ”/23” has 512, ”/22” has 1,024 etc). So if you have just one port defined, the number of endpoints will be 256 for a ”/24” network, but if you had 3 ports (like say 443-445) that number would jump to 768. The same scenario for a ”/23” network would be 512 for one port and 1,536 for three ports.

The Ranges section

You can see any existing network definitions in the Network Ranges box in the **Ranges** section of the dialog. The **Ranges** section:

- Displays existing defined network ranges.
- Allows you to edit or delete existing network ranges. To delete a network range, highlight the selected range and click **Delete** on your keyboard. To edit a network range, highlight the selection to change and type over with the desired value(s).
- Accepts typed or pasted ranges, bypassing the *add range tool*. To add a network range, click inside the network ranges text box and type the desired value(s) or paste from your local clipboard. Ranges added this way must also contain the ports notation (e.g, :443).
- Validates network ranges as defined. To validate the list of ranges defined for the network, click the **Validate** action button. Based on the result, either a green *Network ranges are valid* message will display, or an alert will pop up with the list of invalid ranges.

Quiet Hours Tab

Quiet hours are ranges of hours or days during which scanning will not take place. Any scans in progress when the quiet hour window is reached will pause for the duration of the window and resume when the window is complete. SSL scans will show a status of **In Quiet Hours** if scanning is currently in that status.

In the SSL Network Definition dialog on the Quiet Hours tab, define quiet hour periods as follows:

a. In the Add Quiet Hours section of the page, select a day and time to begin a quiet hour period in the *Start* section.

b. Select a day of the week and time to end the quiet hour period in the *End* section.

c. Click **Add** to add the quiet hour period to the Quiet Hours section of the page.

d. Repeat the above steps for any additional quiet hour periods.

Note: Quiet hours replace and expand upon the blackout period option that existed in previous versions of Keyfactor Command.

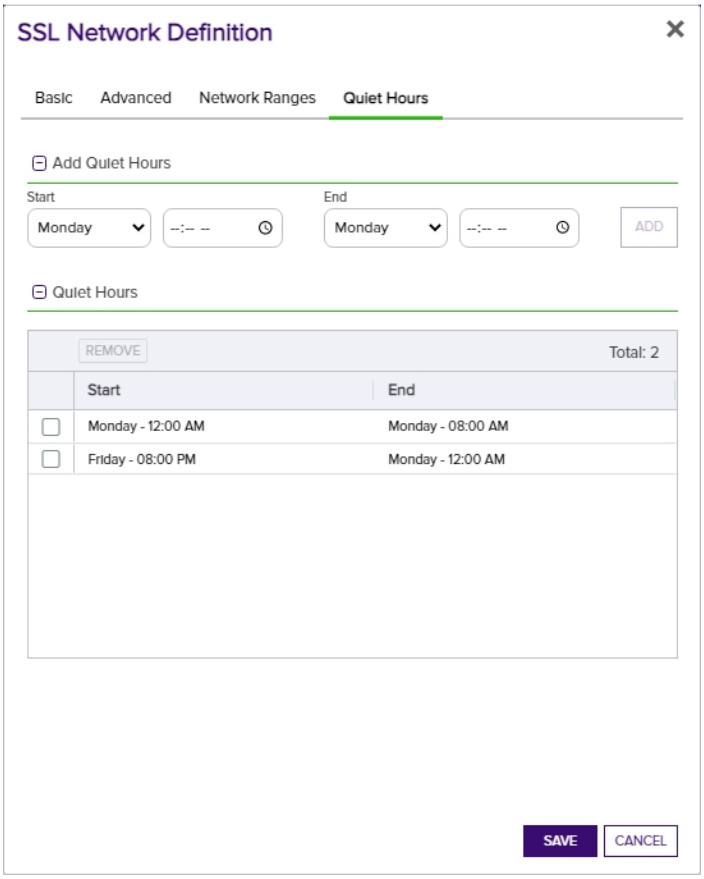


Figure 260: Define a New Network—Quiet Hours Tab

5. Click Save to save the new network definition or changes.

Deleting an SSL Network

1. In the Management Portal, browse to *Locations > SSL Discovery*.
2. On the SSL Network Discovery page, select the Network Definitions tab (the default when you first visit the page).

3. On the Network Definitions tab, highlight the row in the SSL network grid of the network to delete and click **Delete** at the top of the grid or right-click the network in the grid and choose **Delete** from the right-click menu.

4. On the Confirm Operation alert, click **OK** to confirm or **Cancel** to cancel the operation.

Monitoring Network Scan Jobs with View Scan Details

At any time, you can view the status of the latest scan jobs by viewing scan details from the *SSL Discovery* page. Right-click the network location in the grid and choose **View Scan Details** from the right-click menu or highlight the row in the network grid and click **View Scan Details** at the top of the grid.

This takes you to a separate page with separate tabs for Discovery and Monitoring jobs (see Figure 261: SSL Network Scan Details Page). Details for the last scanned job display above the grid in each tab and the scanned segments for the latest scan populate the grid. You will only see more than one row in the grid if the SSL management job was broken into segments due to having a large number of endpoints. The number of endpoints per segment is configurable (see the *SSL Maximum Scan Job Size* setting in Application Settings: Agents Tab on page 596). The grid will display the latest completed job and will be refreshed with new scan details when the next scan begins.

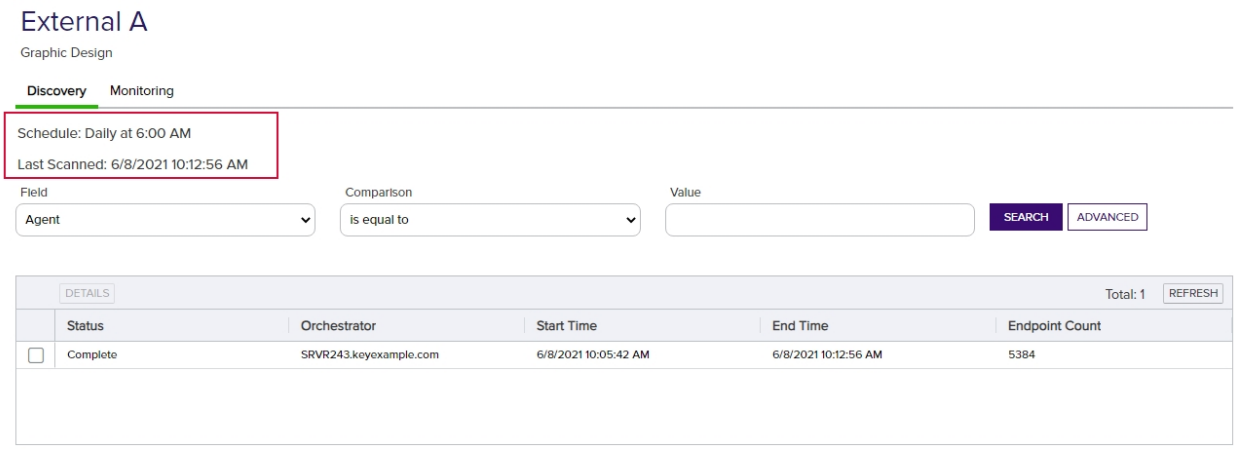


Figure 261: SSL Network Scan Details Page

To view details for a segment, double-click the segment, right-click the segment and choose **Details** from the right-click menu, or highlight the row in the scan details grid and click **Details** at the top of the grid (see SSL Network Scan Detail Segment Details on the next page).

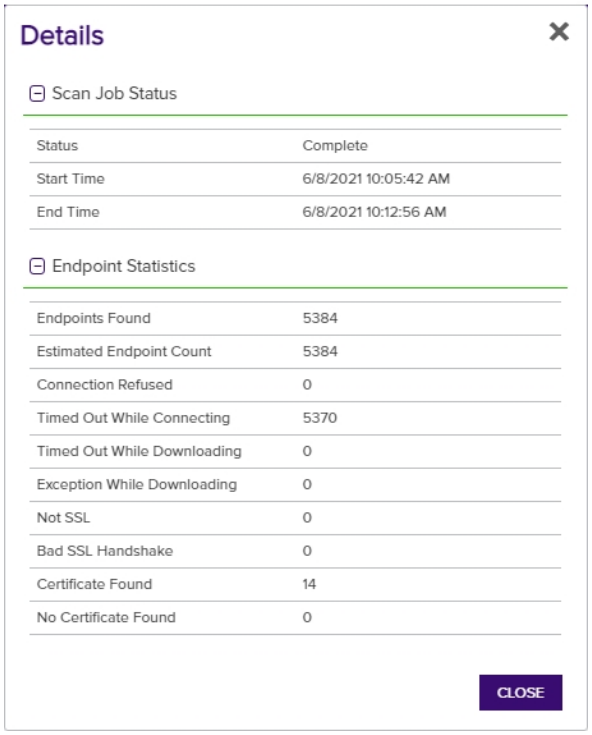


Figure 262: SSL Network Scan Detail Segment Details

Tip: If jobs are taking longer to complete than expected, see Slow SSL Jobs on page 752.

Initiating a Manual Scan

In addition to SSL scanning jobs that can be run as scheduled, the Network Definitions tab includes a feature that allows you to manually initiate a scan for a configured network at any time that a scan is not already running for the network or the network is not in quiet hours. When you initiate a scan using the scan now feature, you can choose whether to run a discovery scan, a monitoring scan, or both.

To initiate a manual scan for a network:

1. In the Management Portal, browse to *Locations > SSL Discovery*.
2. On the SSL Network Discovery page, select the Network Definitions tab (the default when you first visit the page).
3. On the Network Definitions tab, highlight the row in the SSL network grid of the network to scan and click **Scan Now** at the top of the grid or right-click the network in the grid and choose **Scan Now** from the right-click menu. The scan will begin immediately.

Tip: If a scan is already in progress for the network, the option to start a scan of that type will be grayed out and cannot be selected.

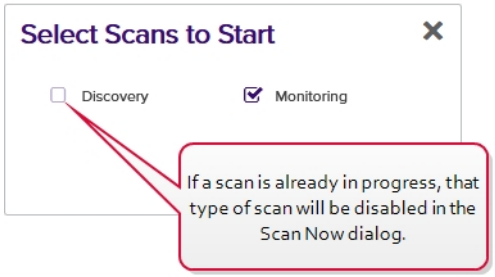


Figure 263: SSL Network ScanNow

Reset Scan

Resetting an SSL scan deletes all scan jobs, scan job parts, logical scan jobs, and current schedules associated with the selected network. The agent job status relating to the SSL scans is set to failed and completed, and the agent is forced to register for a new session. Afterward, *Scan Now* is enabled to allow you to initiate a manual scan. When you select *Reset Scan*, you will receive a **Confirm Operation** message. Click **OK** to proceed or **Cancel** to quit.

Tip: If you have an SSL scan job that appears stuck or crashed without a failure result, you can use the reset scan option to cancel the dysfunctional scan job.

View Network Endpoints and View Discovered Endpoints

See the Results on page 461 documentation for more information on these action buttons.

Using the Network Scan Details Search

The search function allows you to query the database for information. The same query structure is used in multiple locations within the Keyfactor Command Management Portal.

When you first open the page, you will see the simple search option. To execute a search, select the field and comparison operators in the dropdowns and type something on which to search in the value field (if applicable). If you select an *is null* or *is not null* comparison operator, the value field will be grayed out. Click the **Search** button to execute the query.

Each query consists of three parts:

Query Field

The available fields for querying vary depending on the area of the Management Portal in which the search is used. On this page, the queries can be done on the following built-in fields:

Agent

Complete or partial matches with the orchestrator name as listed in the Orchestrator field.

Status

Status matches or doesn't match the selected category—Not Started, In Progress, Complete

The SSL scan will show a status of *In Quiet Hours* if scanning is currently in that status. See SSL Network Operations on page 446.

Start Time

The time at which scanning of the segment began. Supports the %TODAY% token (see Advanced Searches on the next page).

End Time

The time at which scanning of the segment began. Supports the %TODAY% token (see Advanced Searches on the next page).

Endpoint Count

The number of endpoints scanned in the segment. The maximum number of endpoints per segment is configurable (see the SSL Maximum Scan Job Size setting in Application Settings: Agents Tab on page 596).

Comparison Operator

The query comparison operators vary depending on the type of field selected and the specific properties of the field. The list below shows the dropdown list comparison operators, as well as the equivalent query language syntax (in parentheses).

Most string fields (the vast majority of the built-in fields) support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Contains (-contains)
- Does not contain (-notcontains)
- Starts with (-startswith)
- Ends with (-endswith)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Most date and integer fields support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Is less than (-lt)
- Is less than or equal to (-le)
- Is greater than (-gt)
- Is greater than or equal to (-ge)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Most Boolean (true/false) fields support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Comparison Value

The value you enter for comparison must match the field type. For example, integer fields only support numerical values. String fields support all alphanumeric characters. Boolean fields only support True or False. The value field is not case sensitive. Date fields support only properly formatted dates and will initially display as mm/dd/yyyy. You can choose to populate the date field by:

- Clicking in a date Value field to open a pop-up calendar to select a date that will populate the field.
- Clicking in a segment of the date format (i.e., mm/dd/yyyy) and entering a value. As you continue to type in any one segment, the cursor will keep moving onto the next segment.

The results that match your search criteria will be displayed in the results grid below the search selection options.

Advanced Searches

On any search page you can click **Advanced** to the right of the Search button to display the advanced search options. Click **Simple** to close the advanced search options again.

Multiple Criteria

Using the advanced search options, you can build a query based on multiple criteria using AND/OR logic. As with a simple search, you select a field and comparison operator in the drop-downs and then enter a comparison value, if applicable. Click **Insert** to add the search criteria to the query field below the selection fields. Use the selection fields to build multiple search criteria. Each time you click the insert button, an AND is added between the previous search criteria and the newly added one. You can change the AND to an OR if desired. You can use parentheses around portions of the query along with AND/OR to change the query meaning.

For example, for certificate searches:

```
(CN -contains "appsrvr" AND IssuedDate -ge "01/01/2022") OR (CN -contains "appsrvr" AND
TemplateShortName -contains "web")
```

This query will return all the certificates issued on or after January 1, 2022 with the string appsrvr in the CN and also all certificates issued at any time with the string appsrvr in the CN using a template referencing web. When you have entered all the desired search criteria, click **Search** to execute the query. If you wish to clear the query field and start over, click the **Clear** button.

In addition to the options available in the query builder, three special values can be used in selected searches by typing them in directly:

- %TODAY%
  Use the TODAY special value in place of a specific date in date queries. This option supports math operations, so you can use TODAY-10 or TODAY+30. The built-in *Certificates Expiring in 7 Days* collection uses this special value (see Certificate Collection Manager on page 80).
- %ME%
  Use the ME special value in place of a specific domain\user name in queries that match a

domain\user name. The built-in *My Certificates* collection uses this special value (see Certificate Collection Manager on page 80).

- %ME-AN%
  Use the ME-AN special value in place of a specific user name excluding the domain. This is beneficial in environments with multiple domains where there is a desire to query for a user's certificates even if they were requested across multiple domains.

Important: The special query options of %TODAY%, %ME%, and %ME-AN% are only supported in uppercase. Lowercase equivalents (e.g. %me%) cannot be substituted.

Orchestrator Pools Definition

SSL network discovery and monitoring scanning is performed by assigning an orchestrator pool, containing orchestrators with discovery and monitoring capabilities, to a network. An orchestrator pool contains one to many orchestrators that support the SSL discovery and monitoring capabilities. Network scanning using orchestrator pools allows the work to be dispersed among the orchestrators in the pool.

Out of the box, all approved Windows orchestrators and Keyfactor Universal Orchestrators with the SSL capability are assigned to a default orchestrator pool. For scanning of larger and more complicated networks, orchestrator pools can be configured with multiple orchestrators running concurrently to perform the scanning operation.

Note: Approved orchestrators assigned to a custom pool will be removed from the default orchestrator pool. If a custom pool is removed, the orchestrator will be re-assigned to the default orchestrator pool.

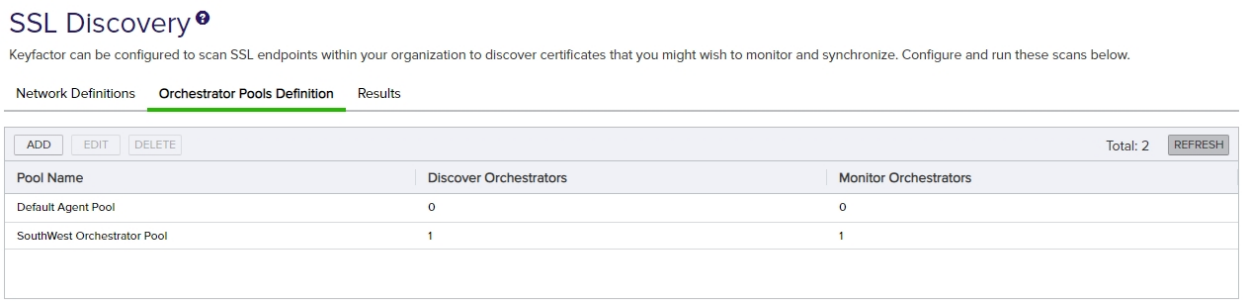


Figure 264: SSL Orchestrator Pools

Orchestrator Pool Operations

Orchestrator pool operations include: creating, editing or deleting pools.

Adding or Modifying an Orchestrator Pool

1. In the Management Portal, browse to *Locations > SSL Discovery*.
2. On the SSL Network Discovery page, select the **Orchestrator Pools Definition** tab.
3. On the Orchestrator Pools Definition tab, click **Add** from the top menu to create a new pool, or **Edit** from either the top or right click menu, to modify an existing one.

   Note: The available edit options include edit the name of the pool or select/de-select the discover/monitor options.

4. In the SSL Orchestrator Pool Definition dialog, enter a unique Orchestrator Pool name in the **Name** field.

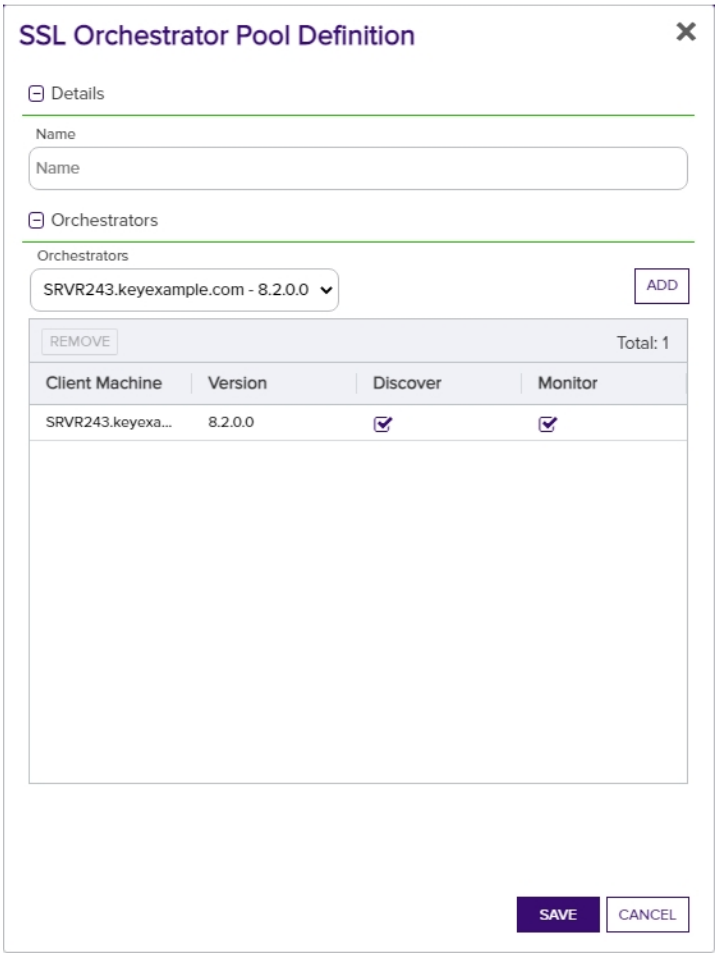


Figure 265: Add an Orchestrator Pool

5. From the **Orchestrators** dropdown, select eligible orchestrators—those orchestrators that support monitor and discovery capabilities—to add to the orchestrator pool and click **Add**.

   Tip: Orchestrators are added with discover and monitor responsibilities. You can de-select one of these options, if needed.

6. Highlight a row and click **Remove** to remove the orchestrator from the orchestrator pool. The orchestrator will be returned to the default orchestrator pool.

   Note: You are not able to remove orchestrators from the default orchestrator pool; they are automatically removed if assigned to a custom orchestrator pool.

7. Click **Save** to save the orchestrator pool.

Deleting an Orchestrator Pool

You may delete one expiration record at a time.

1. In the Management Portal, browse to *Locations > SSL Discovery*.
2. On the SSL Network Discovery page, select the **Orchestrator Pools Definition** tab and select the row you wish to delete.
3. Click **Delete** at the top of the grid, or from the right click menu.
4. On the Confirm Operation alert, click **OK** to confirm or **Cancel** to cancel the operation.

   Note: You are not able to remove the default orchestrator pool.

Results

The SSL network discovery and monitoring results include endpoints that returned certificates as well as endpoints that resulted in some level of response (did not time out) but did not return certificates.

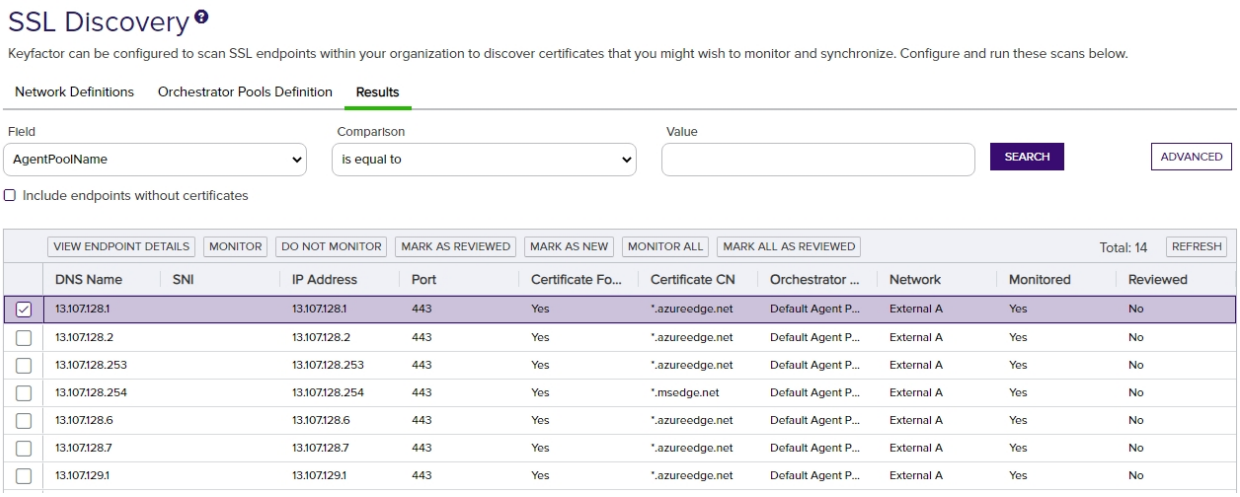


Figure 266: SSL Discovery Results

For each endpoint discovered during the scan, the results grid includes the following:

DNS Name

The host name converted to an IP address, or the IP address scanned. The DNS name is resolved by the orchestrator performing the scan, based on the DNS settings of the server running the orchestrator.

SNI

The server name indication (SNI), if one is found.

IP Address

The IP address scanned.

Port

The port scanned.

Certificate Found

Whether a certificate was found at the endpoint on the most recent scan (true/false).

Certificate CN

Common name discovered on the certificate.

Orchestrator Pool

The orchestrator pool name that contains the orchestrator that discovered and/or monitored the endpoint.

Network

The name of the network.

Monitored

Whether the discovered endpoint is configured for monitoring (true/false). If the *Automatically monitor endpoints found during discovery* option is enabled in the network definition, the orchestrator will, upon initial discovery, monitor the discovered certificate. You can change the monitoring status of a discovered endpoint in the results grid.

Reviewed

The discovered endpoint has been reviewed (true/false). To denote an endpoint as reviewed, highlight the row in the results grid and click **Mark as Reviewed** at the top of the grid or right-click the endpoint and choose **Mark as Reviewed**.

Using the Discovery Results Search Feature

The search function allows you to query the database for information. The same query structure is used in multiple locations within the Keyfactor Command Management Portal.

When you first open the page, you will see the simple search option. To execute a search, select the field and comparison operators in the dropdowns and type something on which to search in the value field (if applicable). If you select an *is null* or *is not null* comparison operator, the value field will be grayed out. Click the **Search** button to execute the query.

Each query consists of three parts:

Query Field

The available fields for querying vary depending on the area of the Management Portal in which the search is used. On this page, the queries can be done on the following built-in fields:

Agent Pool Name

Complete or partial matches with the orchestrator pool that contains orchestrators used to discover and monitor the results.

Certificate CN

Complete or partial matches with the certificate common name.

Network Name

Complete or partial matches with the network name.

Port

Numeric matches with the port number for the discovered endpoint.

Certificate Found

Certificate was found at the endpoint on the most recent scan (true/false).

Reverse DNS

Complete or partial matches with the DNS name resolved based on the discovered IP address. If a host name could not be resolved, this will be the IP address.

IP Address

Complete or partial matches with the IP address.

Is Monitored

Endpoint has been marked as monitored (true/-false). By default, only endpoints that are marked as monitored equals true are displayed.

Issuer DN

Complete or partial matches with the issuer distinguished name.

Reviewed

Whether it is true or false that the scan has been reviewed.

Self Signed

Certificate is self-signed (true/false).

SNI Name

The server name indication (SNI) of the endpoint.

Status

The status of the scan. Options include: Certificate Found, Timed Out Connecting, Exception Connecting, Timed Out Downloading, Exception Downloading, Not SSL, Exception in Sql, Invalid or Unreachable Host, Connection Refused, Bad SSL Handshake, Client Authentication Failed, No Certificate, SSL Refused, Not Probed, Unknown.

Comparison Operator

The query comparison operators vary depending on the type of field selected and the specific properties of the field. The list below shows the dropdown list comparison operators, as well as the equivalent query language syntax (in parentheses).

Most string fields (the vast majority of the built-in fields) support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Contains (-contains)
- Does not contain (-notcontains)
- Starts with (-startswith)
- Ends with (-endswith)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Most date and integer fields support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Is less than (-lt)
- Is less than or equal to (-le)
- Is greater than (-gt)
- Is greater than or equal to (-ge)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Most Boolean (true/false) fields support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Comparison Value

The value you enter for comparison must match the field type. For example, integer fields only support numerical values. String fields support all alphanumeric characters. Boolean fields only support True or False. The value field is not case sensitive. Date fields support only properly formatted dates and will initially display as mm/dd/yyyy. You can choose to populate the date field by:

- Clicking in a date Value field to open a pop-up calendar to select a date that will populate the field.
- Clicking in a segment of the date format (i.e., mm/dd/yyyy) and entering a value. As you continue to type in any one segment, the cursor will keep moving onto the next segment.

The results that match your search criteria will be displayed in the results grid below the search selection options.

Advanced Searches

On any search page you can click **Advanced** to the right of the Search button to display the advanced search options. Click **Simple** to close the advanced search options again.

Multiple Criteria

Using the advanced search options, you can build a query based on multiple criteria using AND/OR logic. As with a simple search, you select a field and comparison operator in the drop-downs and then enter a comparison value, if applicable. Click **Insert** to add the search criteria to the query field below the selection fields. Use the selection fields to build multiple search criteria. Each time you click the insert button, an AND is added between the previous search criteria and the newly added one. You can change the AND to an OR if desired. You can use parentheses around portions of the query along with AND/OR to change the query meaning.

For example, for certificate searches:

```
(CN -contains "appsrvr" AND IssuedDate -ge "01/01/2022") OR (CN -contains "appsrvr" AND
TemplateShortName -contains "web")
```

This query will return all the certificates issued on or after January 1, 2022 with the string appsrvr in the CN and also all certificates issued at any time with the string appsrvr in the CN using a template referencing web. When you have entered all the desired search criteria, click **Search** to execute the query. If you wish to clear the query field and start over, click the **Clear** button.

SSL Results Action Options

The following options are available on the results tab:

- To view the details for a discovered endpoint, double-click the result, right-click the result and choose **View Endpoint Details** from the right-click menu, or highlight the row in the results grid and click **View Endpoint Details** at the top of the grid (see Viewing Endpoint Details below).
- To add a discovered endpoint to a monitoring job, right-click the result and choose **Monitor** from the right-click menu, or highlight the row in the results grid and click **Monitor** at the top of the grid.
- To remove an endpoint from a monitoring job, right-click a result that has a Monitor Status of *true* and choose **Do Not Monitor** from the right-click menu, or highlight the row in the results grid and click **Do Not Monitor** at the top of the grid.
- To change endpoints to reviewed, right-click the result and choose **Mark as Reviewed** from the right-click menu, or highlight the row in the results grid and click **Mark as Reviewed** at the top of the grid. Newly found endpoints default to a reviewed state of *false*.
- To change reviewed endpoints to not reviewed, right-click the result and choose **Mark as New** from the right-click menu, or highlight the row in the results grid and click **Mark as New** at the top of the grid.
- To add all discovered endpoints to a monitoring job, click **Monitor All** at the top of the grid.
- To change all endpoints to reviewed, click **Mark All as Reviewed** at the top of the grid.
- You can click the **Include Endpoints without Certificates** button at the top of the results grid to toggle inclusion of endpoints without certificates in the results. By default they are excluded.

To select a single row in the grid, click to highlight it and then select an operation from either the top of the grid or the right-click menu. Some of the operations support action on multiple results at once. To select multiple rows, hold down the CTRL key and click each row on which you would like to perform an operation. Then select an operation from the top of the grid. The right-click menu supports operations on only one certificate at a time.

Viewing Endpoint Details

To view details of the scan history and certificates found for an SSL job, in the SSL discovery results grid, double-click the result, right-click the result and choose **View Endpoint Details** from the right-click menu, or highlight the row in the results grid and click **View Endpoint Details** at the top of the grid. The endpoint history dialog includes this information:

- The **SSL/TLS Endpoint Details** section of the dialog includes details of the selected certificate including the IP address, port, DNS name, SNI (if available), endpoint network name, orchestrator pool name that contained the orchestrator which performed the scan, and monitoring status of the certificate (true/false).
- The **Chain Level** dropdown allows you to view details of certificates chained to the selected certificate. The default is the end entity certificate.
- The **Certificate Details** section provides details of the certificate selected in the chain level dropdown.
- The **Endpoint History** section on the right side of the endpoint history dialog details each individual scan including the date of the scan, source (monitoring or discovery), the IP address and the certificate status.

The details menu can also provide information on why a certificate was not found if one was expected.

Endpoint history records on the endpoint details page older than 30 days, by default, are automatically purged daily. You can change the length of time for which records are retained by updating the *Retain SSL Endpoint History (days)* in the application settings.

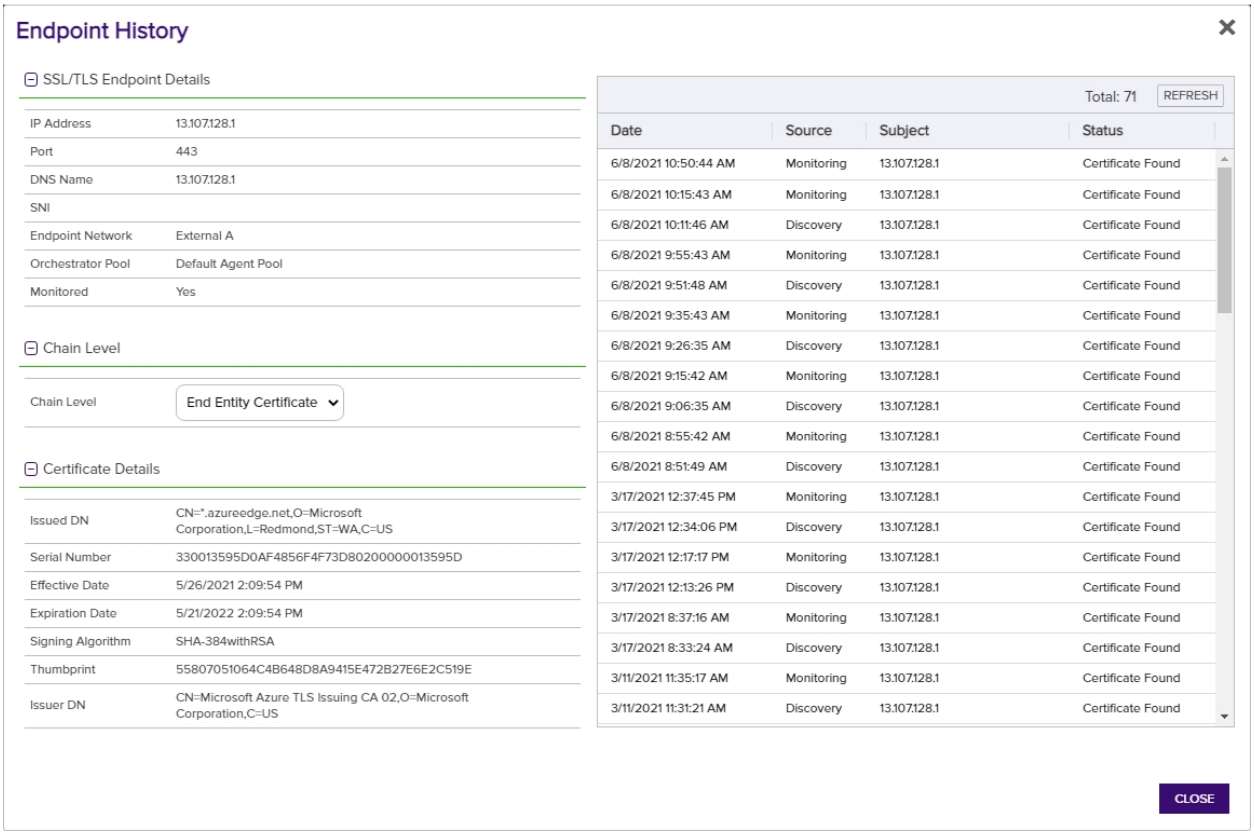


Figure 267: SSL Discovery and Monitoring Result Details

Tracking the Expiration on SSL Certificates

At the conclusion of a of a network monitoring scan, an email is sent to the configured recipients indicating which, if any, certificates associated with that network are nearing expiration. *Near* expiration is determined based on the *Expiration Alert (in days)* setting in the network definition, which defaults to 7 days (see SSL Network Operations on page 446).

This is one method of tracking expiration on SSL certificates, but since the certificates are synchronized to the Keyfactor Command database, you can also use regular expiration alerts (see Expiration Alerts on page 161) and reports (see Reports on page 86) to track expiration for these certificates as you would for certificates issued from internal CAs.

Understanding Notification Emails

The discovery and monitoring notification emails that are delivered at the conclusion of discovery and monitoring scans both include information about the status of the endpoints scanned, but they present this information slightly differently. The discovery email breaks down what happened when the job attempted to find a certificate at each of the endpoints it attempted to communicate with. The monitoring email, on the other hand, focuses on monitoring the status of the certificate that is expected to be at the endpoint. Although the monitoring email can be used for identifying certificates that are coming up for expiration, other solutions, such as expiration alerts (see Expiration Alerts on page 161), may be more useful for this. What the expiration alerts can't do for you, however, and the monitoring email can, is identify servers that may have gone offline or whose certificate may have disappeared. In other words, expiration alerts monitor certificate status and monitoring alerts monitor endpoint status. See the example in Figure 269: SSL Monitoring Email. This shows three servers that previously had been discovered to have a certificate now being unresponsive. In some cases, the servers or certificates may still be there and the requests for them have just timed out due to slow network connections or other issues, but this provides you with an opportunity to investigate these servers to determine what the problem might be.

The various numbers that are reported in the Discovery and Monitoring emails are:

- **The number in the subject:** The total number of endpoints that have expired/expiring certificates plus the total number of endpoints that did not return a certificate.
- **Expired/Expiring certificates number:** The total number of certificates that are expired or will expire within the next X number of days. The value of X is a configurable setting in Keyfactor Command and is set in the network definition for each network (see the *Expiration Alert* setting in SSL Network Operations on page 446).
- **Number of endpoints that did not return a certificate**: The total number of endpoints that did not return a certificate.
- **Number of rows in each grid:** A configurable setting in Keyfactor Command (see the *SSL Maximum Email Results* application setting in Application Settings: Agents Tab on page 596). The number of rows in the grids is not reflected in the total counts.

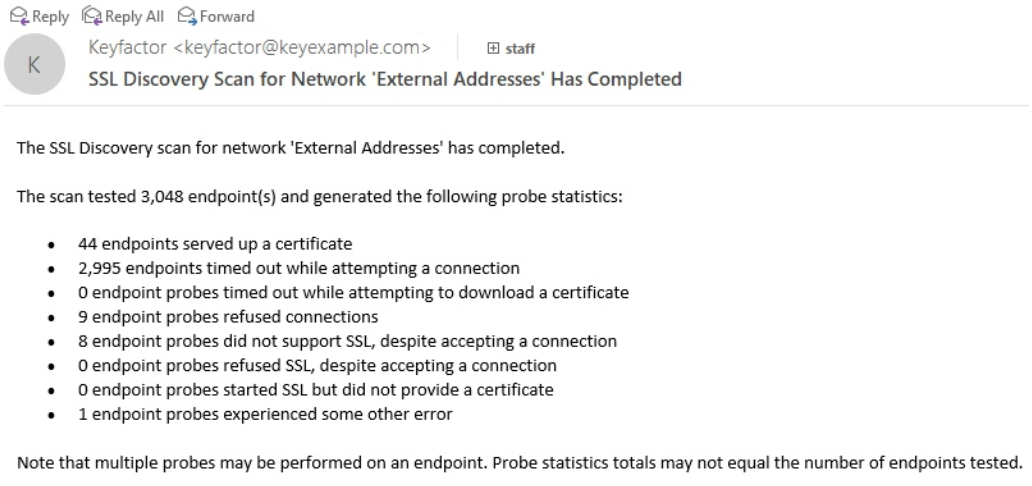
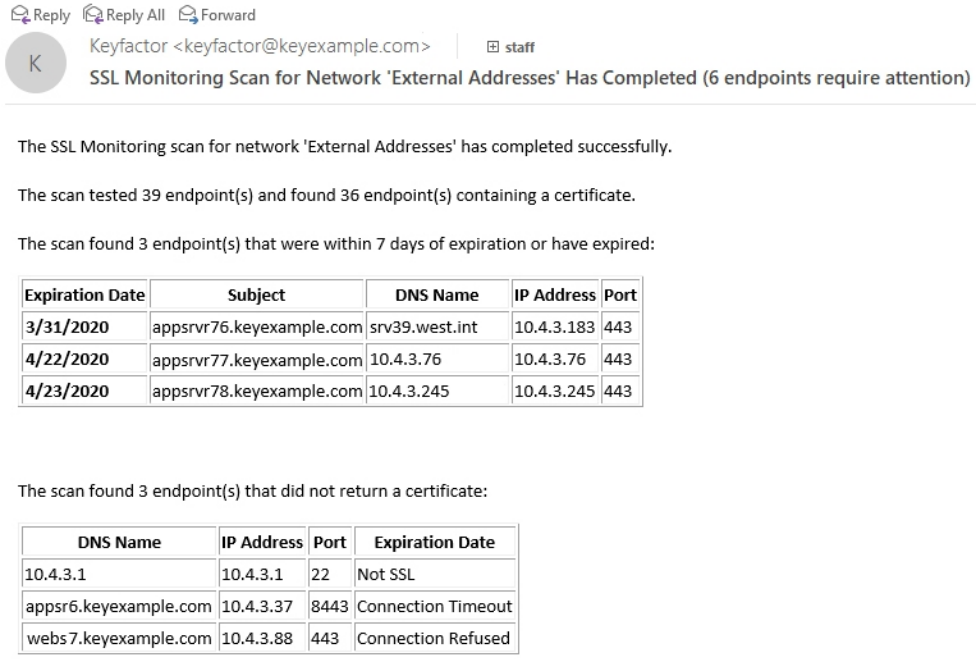


Figure 268: SSL Discovery Email



Reply Reply All Forward

K Keyfactor <keyfactor@keyexample.com> staff

SSL Monitoring Scan for Network 'External Addresses' Has Completed (6 endpoints require attention)

The SSL Monitoring scan for network 'External Addresses' has completed successfully.

The scan tested 39 endpoint(s) and found 36 endpoint(s) containing a certificate.

The scan found 3 endpoint(s) that were within 7 days of expiration or have expired:

Expiration Date	Subject	DNS Name	IP Address	Port
3/31/2020	appsrvr76.keyexample.com	srv39.west.int	10.4.3.183	443
4/22/2020	appsrvr77.keyexample.com	10.4.3.76	10.4.3.76	443
4/23/2020	appsrvr78.keyexample.com	10.4.3.245	10.4.3.245	443

The scan found 3 endpoint(s) that did not return a certificate:

DNS Name	IP Address	Port	Expiration Date
10.4.3.1	10.4.3.1	22	Not SSL
appsr6.keyexample.com	10.4.3.37	8443	Connection Timeout
webs7.keyexample.com	10.4.3.88	443	Connection Refused

Figure 269: SSL Monitoring Email

Table 17: SSL Email Notification Values Defined

Value	Meaning
Timed out while connecting	A timeout occurred when attempting to establish a TCP connection. The timeout interval is defined on the Advanced tab of the SSL network definition page, see SSL Network Operations on page 446. The shorter the timeout, the faster the scan goes, but the higher chance that if there is actually something listening at the port, a connection won't be established causing a timeout. If the orchestrator is overloaded (too many parallel tasks), it can add to the time needed to make a connection and increase the chance of a timeout. Network transit time affects timeouts as does the load and speed of the target system in the ability to establish a TCP handshake.
Timed out while downloading	A TCP connection was made and a TLS connection was started, but it took too long to actually receive the certificate. This is a rare condition. This is a parameter that is locally configurable on the orchestrator and defaults to 15 seconds. This value is displayed in the debug trace.
Connection refused	The target IP and Port are listening, but the TCP connection was actively refused.
Not SSL	A TCP connection was established, but when the first packet of the TLS handshake

Value	Meaning
	was sent, it did not get a TLS response, implying that some protocol other than TLS is listening on the target.
Bad SSL handshake	A TCP connection was established and a proper response to the first TLS packet was returned, but something failed in the rest of the TLS handshake. Several of the internal reasons for why a TLS handshake may have failed have been combined along with other counters in the email response.
Certificate found	A TCP connection and a TLS handshake were completed and the TLS handshake returned a certificate (all within the connection and download timeout periods)

2.1.9 Orchestrators

Keyfactor Command uses orchestrators (a.k.a. agents) to manage a wide variety of certificate store types. As of this writing, Keyfactor offers these orchestrators:

Keyfactor Universal Orchestrator

This orchestrator runs on Windows servers or Linux servers and is used to run jobs at the request of the Keyfactor Command server. Jobs primarily perform certificate management tasks, but other types of operations are also supported. Jobs are provided to the orchestrator as extensions; both built-in and custom extensions are supported. The orchestrator includes built-in extensions to run SSL discovery and management tasks, interact with Windows servers for certificate management (IIS certificate stores), interact with File Transfer Protocol (FTP) capable devices for certificate management, manage synchronization of certificate authorities in remote forests, and retrieve the orchestrator logs for analysis with the Keyfactor API.

Keyfactor Windows Orchestrator

This orchestrator runs on Windows servers and is used to manage synchronization of certificate authorities in remote forests, run SSL discovery and management tasks, and interact with Windows servers as well as F5 devices, NetScaler devices, Amazon Web Services (AWS) resources, and File Transfer Protocol (FTP) capable devices, for certificate management. In addition, the AnyAgent capability of the Keyfactor Windows Orchestrator allows it to be extended to create custom Certificate Store Types and management capabilities regardless of source platform or location.

The Keyfactor Windows Orchestrator is no longer being developed; its last release was version 8.5. The functionality of this orchestrator is being replaced by the Keyfactor Universal Orchestrator, which offers built-in extensions to cover some functionality plus the ease of plug-and-play extensions to add further functionality. Keyfactor intends to make some further extensions available as open source downloads in the future. Until such time as these are available to replace all the functions of the Keyfactor Windows Orchestrator, Keyfactor recommends customers continue to use the Keyfactor Windows Orchestrator version 8.5, which is fully compatible with version 9 of Keyfactor Command.

Keyfactor Java Agent

This orchestrator runs on Windows or Linux servers and is used to perform discovery of Java keystores and PEM certificate stores, to inventory discovered stores, and to push certificates out to stores as needed.

> ⚠ **Important:** The Keyfactor Java Agent will be deprecated in version 11.0 of Keyfactor Command. Customers are encouraged to begin planning a migration to the Keyfactor Universal Orchestrator with the Remote File custom extension publicly available at:
>
> https://github.com/Keyfactor/remote-file-orchestrator

Keyfactor Mac Auto-Enrollment Agent

This orchestrator runs on Apple Macintosh computers and allows users to auto-enroll for certificates.

Keyfactor Android Agent

This orchestrator runs on Android OS Devices and is used to manage PEM and Java keystores. The orchestrator is distributed as part of the Keyfactor Integration SDK (software development kit). Contact Keyfactor for more information.

Keyfactor Native Agent

This orchestrator is a reference implementation intended for customers wanting to include Keyfactor Command certificate store management functionality in embedded or other platforms. The orchestrator is distributed as part of the Keyfactor Integration SDK (software development kit). Contact Keyfactor for more information.

Keyfactor AnyAgent

The Keyfactor AnyAgent runs on Windows or Linux servers and is used to allow management of certificates regardless of source or location by allowing customers to implement custom agent functionality. Custom store types and/or job capabilities, on which agents operate, are created by adding commands and leveraging extendable code to communicate through an API with Keyfactor Command. Because of the custom nature of the functionality of the AnyAgent, it is not included in the table below, as it could be designed to do one or more of the capacities below, or additional capacities not included below. Contact Keyfactor for more information.

Keyfactor Bash Orchestrator

This orchestrator runs on Linux servers and is used to perform discovery of SSH keys, generation of SSH keys, and management of SSH keys and Linux logons.

Table 18: Orchestrator Capabilities

	Universal	Windows	Java	Android	Native	Mac	Bash
Amazon Web Services Add/Remove	✓[1]	✓					
Amazon Web Services Inventory	✓[1]	✓					
Certificate Auto-enroll-ment						✓	
Certificate Reenrollment			✓	✓	✓		
Certificate Renewal	✓	✓	✓	✓	✓		
F5 (Web Server, SSL Profiles, CA Bundles) Add/Remove	✓[1]	✓					
F5 (Web Server & SSL Profiles, CA Bundles) Inventory	✓[1]	✓					
F5 (SSL Profiles & CA Bundles) Discovery	✓[1]	✓					
File Transfer Protocol Add/Remove	✓	✓					
File Transfer Protocol Inventory	✓	✓					

[1]Support for this functionality on the Keyfactor Universal Orchestrator requires the addition of a custom extension. Contact your Keyfactor representative for more information.

	Universal	Windows	Java	Android	Native	Mac	Bash
IIS (Personal, Revoked, Trusted) Add/Remove	✓	✓					
IIS (Personal, Revoked, Trusted) Inventory	✓	✓					
Java Keystore Add/Remove	✓[1]		✓	✓			
Java Keystore Create	✓[1]		✓	✓			
Java Keystore Discovery	✓[1]		✓				
Java Keystore Inventory	✓[1]		✓	✓			
Linux Logon Management							✓
Log Fetching	✓				✓		
NetScaler Add/Remove	✓[1]	✓					
NetScaler Inventory	✓[1]	✓					
PEM Add/Remove	✓[1]		✓	✓	✓		
PEM Discovery	✓[1]		✓				
PEM Inventory	✓[1]		✓	✓	✓		
Remote CA & Template Synchronization	✓	✓					

	Universal	Windows	Java	Android	Native	Mac	Bash
SSL Discovery & Monitoring	✓	✓					
SSH Key Discovery							✓
SSH Key Generation							✓
SSH Key Management							✓

The options available in the Orchestrator Management section of the Management Portal are:

Auto-Registration

Configure Keyfactor Command to allow orchestrators to auto-register.

Management

View and configure orchestrators.

Jobs

View active orchestrator jobs and review job errors.

Blueprints

Snapshot the certificate stores and scheduled jobs of one machine and apply them to multiple other similar machines.

Mac Auto-Enrollment

Configure settings for Mac auto-enrollment.

2.1.9.1 Orchestrator Auto-Registration

Orchestrator auto-registration allows you to automatically approve or deny new orchestrators without administrator input, if desired. This is useful in environments hosting a large number of orchestrators. On the Orchestrator Auto-Registration Settings page you define the conditions under which an orchestrator (e.g. Keyfactor Windows Orchestrator, Keyfactor Java Agent, or Keyfactor Mac Auto-Enroll Agent) can automatically be approved using the built-in auto-registration system. This is one of two ways that Keyfactor Command supports orchestrator auto-registration. Keyfactor Command also offers an enhanced orchestrator auto-registration system that allows the construction of custom orchestrator auto-approval handler modules. Any custom auto-registration

handlers are processed first before the built-in auto-registration system runs. For more information about custom auto-registration handlers, see Custom Auto-Registration Handlers on page 479.

The configurable settings for the built-in auto-registration system are:

- Auto-Register

  Should orchestrators be allowed to auto register? If the *Auto-Register* box is checked but the *Validate Users* setting is not checked, any orchestrator that appears in your environment will automatically be approved regardless of origin.

- Validate Users

  Do the user accounts under which the orchestrators are running need to be a member of a specific group in order to auto-register (aka validation)?

  - User Groups

    If the user accounts must be a member of a group to auto-register (*Validate Users* is checked), which group or groups is that (or which user account if all orchestrators will be registering as the same user)? If the *Auto-Register* setting and the *Validate Users* settings are both enabled, then this field will be considered. If *Validate Users* is not checked, this setting will not be displayed.

The default auto-registration settings are to allow no orchestrators to auto-register.

Note: The built-in auto-registration system does not support the Keyfactor Universal Orchestrator. If you need auto-registration with the Keyfactor Universal Orchestrator, see Custom Auto-Registration Handlers on page 479.

Tip: Click the help icon (?) next to the page title to open the embedded web copy of the *Keyfactor Command Documentation Suite* to this section.
You can also find the help icon at the top of the page next to the **Log Out** button. From here you can choose to open either the *Keyfactor Command Documentation Suite* at the home page or the *Keyfactor API Endpoint Utility*.

Orchestrator Auto-Registration Settings

The Orchestrator Auto-Registration Settings grid shows the current settings for the following defined job types:

Amazon Web Services Inventory

Auto-register the Keyfactor Windows Orchestrator to allow it to synchronize certificates from AWS locations.

Amazon Web Services Management

Auto-register the Keyfactor Windows Orchestrator

Java Keystore Discovery

Auto-register the Java Agent to allow it to run discovery tasks to locate Java keystores.

Java Keystore Inventory

Auto-register the Java Agent to allow it to inventory certificates in Java keystores.

to allow it to manage certificates on and deliver certificates to AWS locations.

F5 CA Bundles REST Discovery

Auto-register the Keyfactor Windows Orchestrator to allow it to run discovery tasks to locate CA bundles on the F5 device(s).

F5 CA Bundles REST Inventory

Auto-register the Keyfactor Windows Orchestrator to allow it to synchronize CA bundles from the F5 device(s).

F5 CA Bundles REST Management

Auto-register the Keyfactor Windows Orchestrator to allow it to manage CA bundles on and deliver certificates to CA bundles on the F5 device(s).

F5 Certificate Store Inventory

Auto-register the Keyfactor Windows Orchestrator to allow it to synchronize certificates from the F5 device(s).

F5 Certificate Store Management

Auto-register the Keyfactor Windows Orchestrator to allow it to manage certificates on and deliver certificates to the F5 device(s).

F5 Keygen/re-enrollment

Setting reserved for future use.

F5 SSL Profiles REST Discovery

Auto-register the Keyfactor Windows Orchestrator to allow it to run discovery tasks to locate SSL certificates on the F5 device(s).

F5 SSL Profiles REST Inventory

Auto-register the Keyfactor Windows Orchestrator to allow it to synchronize SSL certificates from the F5 device(s).

Java Keystore Keygen/re-enrollment

Setting reserved for future use.

Java Keystore Management

Auto-register the Java Agent to allow it to manage (add/remove) certificates in Java keystores.

Mac Auto-Enrollment

Auto-register users on Apple Macintosh computers running the Keyfactor Mac Auto-Enrollment Agent for auto-enrollment for certificates.

NetScaler Certificate Store Inventory

Auto-register the Keyfactor Windows Orchestrator to allow it to synchronize certificates from NetScaler devices.

NetScaler Certificate Store Management

Auto-register the Keyfactor Windows Orchestrator to allow it to manage certificates on and deliver certificates to NetScaler devices.

NetScaler Keygen/re-enrollment

Setting reserved for future use.

Orchestrator Log Retrieval

Auto-register the Native Agent to allow it to perform the fetch logs function.

PEM Certificate Store Discovery

Auto-register the Java Agent to allow it to run discovery tasks to locate PEM certificate stores. Apache servers typically use PEM certificate stores.

PEM Certificate Store Inventory

Auto-register the Java Agent to allow it to inventory certificates in PEM certificate stores.

F5 SSL Profiles REST Management

Auto-register the Keyfactor Windows Orchestrator to allow it to manage SSL certificates on and deliver certificates to the F5 device(s).

F5 Web Server REST Inventory

Auto-register the Keyfactor Windows Orchestrator to allow it to synchronize device certificates from the F5 device(s).

F5 Web Server REST Management

Auto-register the Keyfactor Windows Orchestrator to allow it to manage device certificates on and deliver certificates to the F5 device(s).

File Transfer Protocol Inventory

Auto-register the Keyfactor Windows Orchestrator to allow it to synchronize certificates from PEM certificate stores on FTP capable devices.

File Transfer Protocol Management

Auto-register the Keyfactor Windows Orchestrator to allow it to manage certificates on and deliver certificates to PEM certificate stores on FTP capable devices.

IIS Certificate Store Inventory

Auto-register the Keyfactor Windows Orchestrator to allow it to synchronize certificates from the machine certificate stores of Windows servers.

IIS Certificate Store Management

Auto-register the Keyfactor Windows Orchestrator to allow it to manage certificates in and deliver certificates to the machine certificate stores of Windows servers and optionally bind the certificates to Internet Information Services (IIS) web sites.

IIS Keygen/re-enrollment

Setting reserved for future use.

PEM Certificate Store Management

Auto-register the Java Agent to allow it to manage (add/remove) certificates in PEM certificate stores.

PEM Keygen/re-enrollment

Setting reserved for future use.

Remote Certificate Authority

Auto-register the Keyfactor Windows Orchestrator to allow it to synchronize certificates from the remote CA(s) to the Keyfactor Command database.

Remote Template Sync

Auto-register the Keyfactor Windows Orchestrator to allow it to synchronize templates from the remote CA(s) to the Keyfactor Command database.

Secure Shell Management

Auto-register the Keyfactor Bash Orchestrator to allow it to run SSH tasks.

SSL Endpoint Compliance

Auto-register the Windows Orchestrator to allow it to run SSL compliance tasks.

SSL Endpoint Discovery

Auto-register the Windows Orchestrator to allow it to run SSL discovery tasks.

SSL Endpoint Monitoring

Auto-register the Windows Orchestrator to allow it to run SSL monitoring tasks.

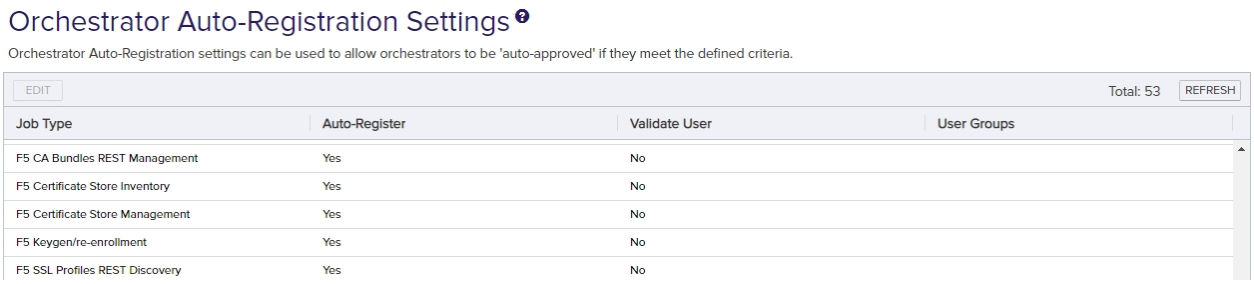


Figure 270: Orchestrator Auto-Registration Settings Page

Note: The built-in auto-registration system does not support the Keyfactor Universal Orchestrator. If you need auto-registration with the Keyfactor Universal Orchestrator, see Custom Auto-Registration Handlers on the next page.

Editing Orchestrator Auto-Registration Jobs

To edit one of the orchestrator job types:

1. In the Management Portal, browse to *Orchestrators > Auto-Registration*.
2. On the Orchestrator Auto-Registration Settings page, highlight the row in the grid of the job you want to edit and click **Edit** at the top of the grid or right-click the job in the grid and choose **Edit** from the right-click menu.

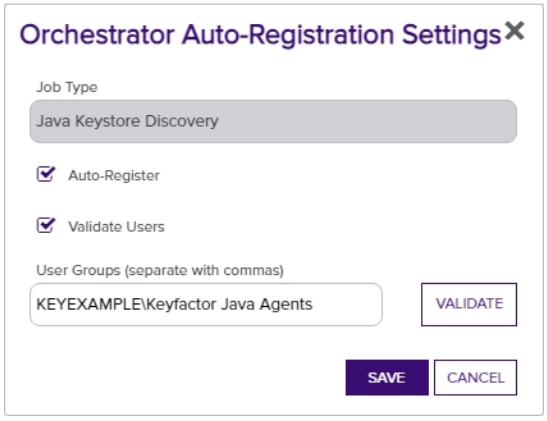


Figure 271: Orchestrator Auto-Registration Edit

3. In the Orchestrator Auto-Registration Settings dialog, check the **Auto-Register** box if you want orchestrators to be able to auto-register. If you do not enable this, an administrator will need to visit the Orchestrator Management page in the Management Portal and manually approve each orchestrator.

4. Check the **Validate Users** box if you want the users under which the orchestrators are running to be a member of a specific AD group in order to auto-register. If you do not enable this but you do enable auto-registration, all orchestrators will auto-register.

    a. In the **User Groups** field, enter the AD group or groups against which to validate the user accounts in *DOMAIN\group name* format. Multiple groups should be separated by a comma and no space. User accounts may be used if desired.

    b. Click the **Validate** button to validate the entered group(s).

1. Click **Save**.

> **Important:** The same Active Directory group or groups in the primary Keyfactor Command forest must be used for all roles serviced by a given orchestrator type (e.g. Keyfactor Java Agent or Keyfactor Windows Orchestrator). All auto-registration settings must be populated if any are to be used even if all features are not planned for use. For example, if you plan to use SSL management but not AWS, F5, FTP, IIS, NetScaler or remote CA functionality, you still need to populate the AWS, F5, FTP, IIS, NetScaler and remote CA auto-registration settings to enable auto-registration for the Keyfactor Windows Orchestrator to function correctly. Similarly, if you plan to use, for example, Java keystores but not PEM certificate stores, you still need to populate both the Java keystore and the PEM auto-registration settings to enable auto-registration for the Java Agent to function correctly. Settings reserved for future use do not need to be populated, though doing so will not hurt anything.

Custom Auto-Registration Handlers

With the custom handler system of auto-registration, a handler module is written and compiled into a DLL, which is then registered in the Keyfactor Command configuration and called whenever a new orchestrator performs an initial registration request, provided there are sufficient licenses available to support the orchestrator. The handler then has the flexibility to call out to an external system such as a database or web service or use any other means to determine whether the orchestrator should be approved and what values should be applied for the blueprint, metadata, and orchestrator ClientID.

When an orchestrator first connects to Keyfactor Command, available registration handlers run in sequence to determine if the orchestrator can be automatically approved. A handler will return one of three results: Allow, Deny, and Defer. Handlers are executed in order of registration until one returns Allow or Deny or until all handlers have been executed. Whenever an executed handler returns a response of Defer, the next registered handler will be executed. If any executed handler returns a response of Deny, further processing will cease and the orchestrator will be moved into a Disapproved state. In both of these cases, values returned by the output parameters will be ignored by Keyfactor Command.

In the event of an Allow response, the following actions will occur:

- The orchestrator will be set to an Approved state.

- If the value for blueprintName corresponds to a valid orchestrator blueprint that can be applied to this orchestrator, it is applied. Otherwise, the response is rejected, the orchestrator is left with a state of New, and an error is logged.
- If the value for ClientID is non-null, it will be permanently associated with this orchestrator approval. The orchestrator will be expected to provide this value for the ClientMachine field on all future calls.
- If the CSR attribute was provided to the handler, it will be submitted for issuance and the resulting certificate will be returned to the orchestrator.
- If the request results in an issued certificate and the metadata output parameter has values, the valid metadata field values will be associated with the issued certificate.
- If ClientParameters has a value, the parameters will be returned to the orchestrator (but will not be used by Keyfactor Command).

If no handler returns a response aside from Defer, the process will continue to the built-in auto-registration system, and if the orchestrator is not approved at the conclusion of that, the orchestrator will be left in the New state for manual approval.

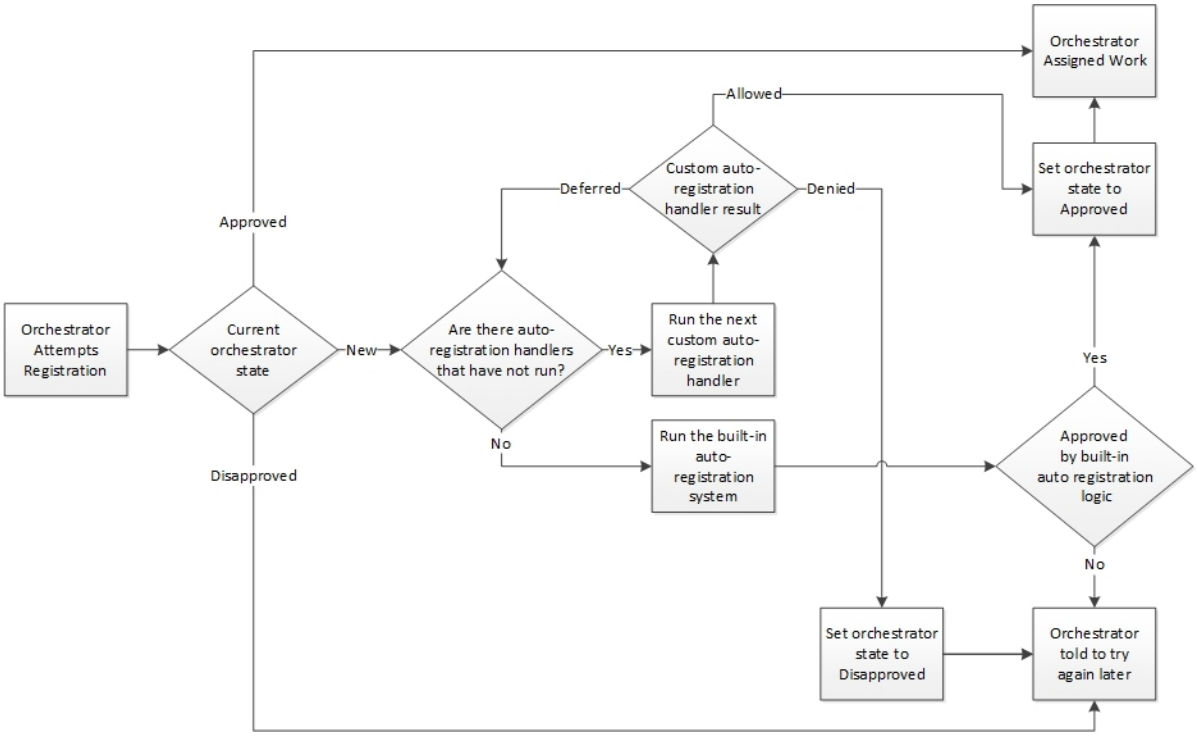


Figure 272: Orchestrator Auto-Registration Flow

Tip: Sample handler source is available as a starting point for creating a custom auto-registration handler. Contact Keyfactor support for assistance.

2.1.9.2 Orchestrator Management

Orchestrators (e.g. Keyfactor Universal Orchestrator, Keyfactor Java Agent, and Keyfactor Bash Orchestrator) are managed through the Orchestrator Management page. The orchestrator management grid shows every orchestrator that is actively or has historically been in communication with the Keyfactor Command server.

The orchestrator management grid can be sorted in ascending order by clicking on a column header, with the exception of the *Capabilities* column. Click the column header again to reverse the sort order. The grid columns can be arranged in any order desired by click-holding and dragging the header of the column you wish to move. The column widths may also be adjusted by click-holding and dragging the line separating two column headers. By default, disapproved orchestrators are not included in the display. To include them, click the **Include Disapproved** box.

For a description of the columns shown in the orchestrator management grid, see Viewing Orchestrator Details on page 484.

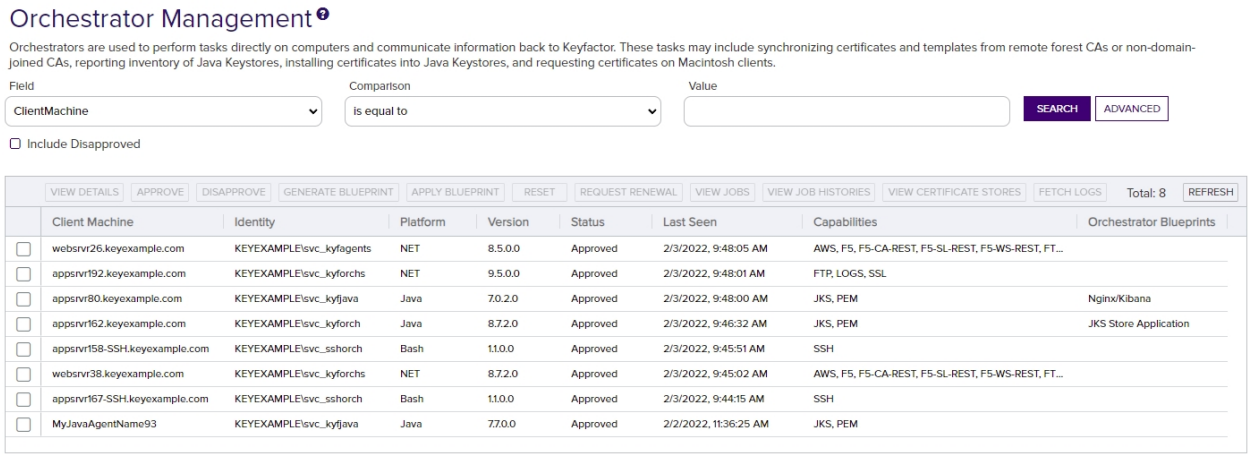


Figure 273: Keyfactor Orchestrators

Tip: Click the help icon (?) next to the page title to open the embedded web copy of the *Keyfactor Command Documentation Suite* to this section.
You can also find the help icon at the top of the page next to the **Log Out** button. From here you can choose to open either the *Keyfactor Command Documentation Suite* at the home page or the *Keyfactor API Endpoint Utility*.

Using the Orchestrator Management Search Feature

The search function allows you to query the database for information. The same query structure is used in multiple locations within the Keyfactor Command Management Portal.

When you first open the page, you will see the simple search option. To execute a search, select the field and comparison operators in the dropdowns and type something on which to search in the value

field (if applicable). If you select an *is null* or *is not null* comparison operator, the value field will be grayed out. Click the **Search** button to execute the query.

Each query consists of three parts:

Query Field

The available fields for querying vary depending on the area of the Management Portal in which the search is used. On this page, the queries can be done on the following built-in fields:

Client Machine

Complete or partial matches with the orchestrator name as listed in the Client Machine field.

Last Seen

Orchestrator last contacted the Keyfactor Command server before, after or on a specified date.

Platform

Platform matches or doesn't match the selected category—.NET, Java, Mac, Android, Native, Unknown.

Status

Status matches the selected category—New, Approved or Disapproved.

Identity

Complete or partial matches with the Active Directory account the orchestrator used when registering with the Keyfactor Command server.

Capabilities

Capability matches the selected category—AWS, CA, F5, FTP, IIS, JKS, NS, PEM, SSL, LOGS and any custom types you've created.

Version

Complete or partial matches with the version the orchestrator reported when registering with the Keyfactor Command server.

Comparison Operator

The query comparison operators vary depending on the type of field selected and the specific properties of the field. The list below shows the dropdown list comparison operators, as well as the equivalent query language syntax (in parentheses).

Most string fields (the vast majority of the built-in fields) support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Contains (-contains)
- Does not contain (-notcontains)
- Starts with (-startswith)
- Ends with (-endswith)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Most date and integer fields support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Is greater than (-gt)
- Is greater than or equal to (-ge)

- Is less than (-lt)
- Is less than or equal to (-le)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Most Boolean (true/false) fields support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Comparison Value

The value you enter for comparison must match the field type. For example, integer fields only support numerical values. String fields support all alphanumeric characters. Boolean fields only support True or False. The value field is not case sensitive. Date fields support only properly formatted dates and will initially display as mm/dd/yyyy. You can choose to populate the date field by:

- Clicking in a date Value field to open a pop-up calendar to select a date that will populate the field.
- Clicking in a segment of the date format (i.e., mm/dd/yyyy) and entering a value. As you continue to type in any one segment, the cursor will keep moving onto the next segment.

The results that match your search criteria will be displayed in the results grid below the search selection options.

Advanced Searches

On any search page you can click **Advanced** to the right of the Search button to display the advanced search options. Click **Simple** to close the advanced search options again.

Multiple Criteria

Using the advanced search options, you can build a query based on multiple criteria using AND/OR logic. As with a simple search, you select a field and comparison operator in the drop-downs and then enter a comparison value, if applicable. Click **Insert** to add the search criteria to the query field below the selection fields. Use the selection fields to build multiple search criteria. Each time you click the insert button, an AND is added between the previous search criteria and the newly added one. You can change the AND to an OR if desired. You can use parentheses around portions of the query along with AND/OR to change the query meaning.

For example, for certificate searches:

```
(CN -contains "appsrvr" AND IssuedDate -ge "01/01/2022") OR (CN -contains "appsrvr" AND
TemplateShortName -contains "web")
```

This query will return all the certificates issued on or after January 1, 2022 with the string appsrvr in the CN and also all certificates issued at any time with the string appsrvr in the CN using a template referencing web. When you have entered all the desired search criteria, click **Search** to execute the query. If you wish to clear the query field and start over, click the **Clear** button.

- %TODAY%
  Use the TODAY special value in place of a specific date in date queries. This option supports math operations, so you can use TODAY-10 or TODAY+30. The built-in *Certificates Expiring in 7 Days* collection uses this special value (see Certificate Collection Manager on page 80).
- %ME%
  Use the ME special value in place of a specific domain\user name in queries that match a domain\user name. The built-in *My Certificates* collection uses this special value (see Certificate Collection Manager on page 80).
- %ME-AN%
  Use the ME-AN special value in place of a specific user name excluding the domain. This is beneficial in environments with multiple domains where there is a desire to query for a user's certificates even if they were requested across multiple domains.

Important: The special query options of %TODAY%, %ME%, and %ME-AN% are only supported in uppercase. Lowercase equivalents (e.g. %me%) cannot be substituted.

Viewing Orchestrator Details

To view details of an orchestrator, double-click the orchestrator, right-click the orchestrator and choose **View Details** from the right-click menu, or highlight the row in the grid and click **View Details** at the top of the grid. The orchestrator details dialog includes this information:

Id

The GUID of the orchestrator.

Client Machine

The host name of the orchestrator machine, either short or fully qualified depending upon how the machine reports itself.

Identity

The Active Directory user account the orchestrator is using to authenticate to Keyfactor Command, which may or may not be the same as the user account under which the orchestrator is running. For example, the Keyfactor Windows Orchestrator service runs as a service account on the orchestrator machine but its identity on the Keyfactor Command server will be a service account in the Keyfactor Command forest. This identity may be different from that of the service account on the orchestrator machine, which may be in a remote forest.

Capabilities

The target types that are supported by that orchestrator—e.g. AWS, F5, FTP, IIS, JKS, NS (NetScaler), PEM, SSH, SSL, Windows—as appropriate for the type of orchestrator. This includes custom AnyAgent capabilities. Keyfactor Command also has LOGS capabilities for Keyfactor Universal Orchestrators, Native Agents, and any orchestrators built on the AnyAgent platform.

Orchestrator Blueprints

The last blueprint applied to the orchestrator, if any (see Orchestrator Blueprints on page 503).

Legacy Thumbprint

The thumbprint of the certificate previously used by the orchestrator for client certificate authentication before a certificate renewal operation took place (rotating the current thumbprint into the legacy thumbprint). The legacy thumbprint is cleared once the orchestrator successfully registers with a new thumbprint.

Platform

The platform of the orchestrator—Java for the Java Agent, .NET Core for the Keyfactor Universal Orchestrator, .NET for the Keyfactor Windows Orchestrator, Bash for the Keyfactor Bash Orchestrator, and ObjectiveC for the Mac agent, for example.

Version

The version number that the orchestrator has reported.

Status

Whether the orchestrator has been approved for operations with the Keyfactor Command server. Newly registered orchestrators show New in this column. Disapproved orchestrators show Disapproved.

Last Seen

The date and time when the orchestrator last contacted the Keyfactor Command server.

Current Thumbprint

The thumbprint of the certificate that Keyfactor Command is expecting the orchestrator to use for client certificate authentication.

Authentication Certificate Renewal Request Status

The last error code, if any, reported from the orchestrator when trying to register a session. This code is cleared on successful session registration.

Last Thumbprint Used

The thumbprint of the certificate that the orchestrator most recently used for client certificate authentication. In most cases, this will match the *Current Thumbprint*.

Last Error Code

The last error code, if any, reported from the orchestrator when trying to register a session. This code is cleared on successful session registration.

Last Error Message

The last error code, if any, reported from the orchestrator when trying to register a session. This message is cleared on successful session registration.

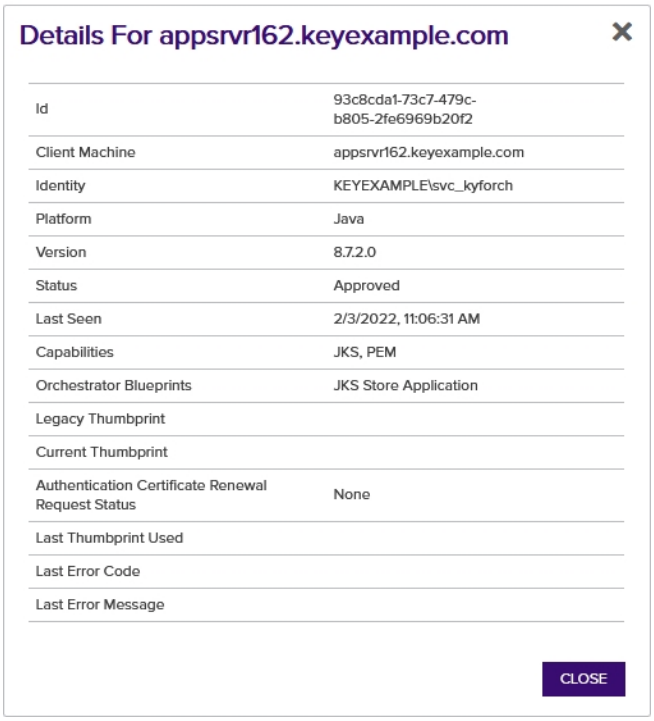


Figure 274: View Details for an Orchestrator

Approving or Disapproving Orchestrators

When orchestrators first appear in Keyfactor Command, they have a status of New. The orchestrator cannot perform any jobs while it has this status. To approve an orchestrator, highlight the row in the orchestrator management grid and click **Approve** at the top of the grid or right-click the orchestrator in the grid and choose **Approve** from the right-click menu. Once you have approved a Keyfactor Universal Orchestrator, Windows Orchestrator or Java Agent, you can schedule jobs for the orchestrator. Once you have approved an SSH Orchestrator, you can configure server groups and servers for that orchestrator and begin scanning servers. Once you have approved a Mac enroll agent, users can enroll for certificates from that Mac. Some orchestrators may be configured for auto-approval via auto-registration (see Orchestrator Auto-Registration on page 474).

To disapprove an orchestrator, highlight the row in the orchestrator management grid and click **Disapprove** at the top of the grid or right-click the orchestrator in the grid and choose **Disapprove** from the right-click menu. When an orchestrator is disapproved, operations with Keyfactor Command can no longer be carried out by this orchestrator.

Generating and Applying Blueprints

To generate a blueprint from an orchestrator, highlight the row in the orchestrator management grid and click **Generate Blueprint** at the top of the grid or right-click the orchestrator in the grid and

choose **Generate Blueprint** from the right-click menu. For more information about blueprints, see Orchestrator Blueprints on page 503.

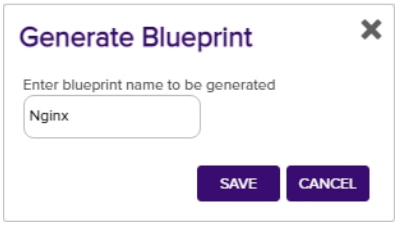


Figure 275: Generate a Blueprint from an Existing Orchestrator

To apply a blueprint to an orchestrator, highlight the row in the orchestrator management grid and click **Apply Blueprint** at the top of the grid or right-click the orchestrator in the grid and choose **Apply Blueprint** from the right-click menu. For more information about blueprints, see Orchestrator Blueprints on page 503.

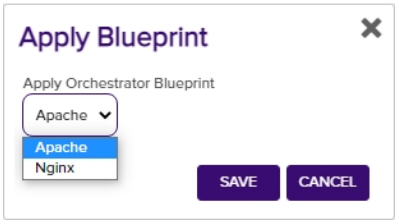


Figure 276: Apply a Blueprint from a New Orchestrator

Resetting or Renewing an Orchestrator

The orchestrator reset and renewal functions are both useful for orchestrator maintenance. The reset function can be used when an orchestrator that is in an error state or if you've made some changes on the orchestrator side that necessitate a refresh. The renewal function is used for orchestrators that are authenticating via client certificate to initiate a client certificate renewal before this would occur automatically based on approaching certificate expiration.

Orchestrator Reset

The orchestrator reset function:

- Removes all current orchestrator jobs for the selected orchestrator.
- Deletes all associated certificate stores.
- Sets the orchestrator status to new.
- For orchestrators configured to use client certificate authentication, clears the certificate thumbprints stored for the orchestrator to allow it to be reconfigured with a new certificate.

To reset an orchestrator, highlight the row in the orchestrator management grid and click **Reset** at the top of the grid or right-click the agent in the grid and choose **Reset** from the right-click menu.

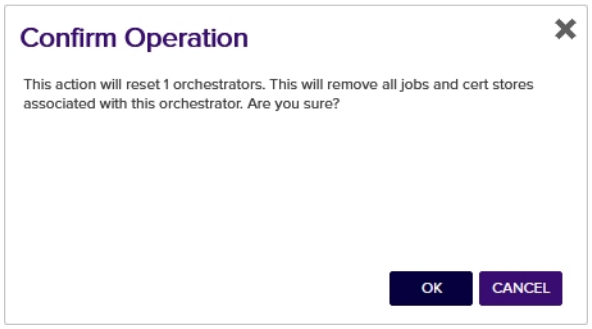


Figure 277: Reset an Orchestrator

Orchestrator Renewal

The orchestrator renewal function is used to request or require that the orchestrator enroll for a new client authentication certificate on the orchestrator's next session registration. It is used in conjunction with a custom renewal extension on the orchestrator to force the orchestrator to enroll for a new certificate before it would normally do so based on the warning and expiry windows. See *Register a Client Certificate Renewal Extension* in the *Keyfactor Orchestrators Installation and Configuration Guide* for more information and custom renewal extensions on the renewal process.

To request certificate renewal for an orchestrator, highlight the row in the orchestrator management grid and click **Request Renewal** at the top of the grid or right-click the agent in the grid and choose **Request Renewal** from the right-click menu. In the Renewal Status dropdown, select one of the available options:

- None
  Unset the value so that the orchestrator will not request a new client authentication certificate (based on this value).
- Request
  The orchestrator will request a new client authentication certificate when it next registers for a session. Orchestrator activity will be allowed to continue as usual.
- Require
  The orchestrator will request a new client authentication certificate when it next registers for a session. A new session will not be granted and orchestrator activity will not be allowed to continue until the orchestrator acquires a new certificate.

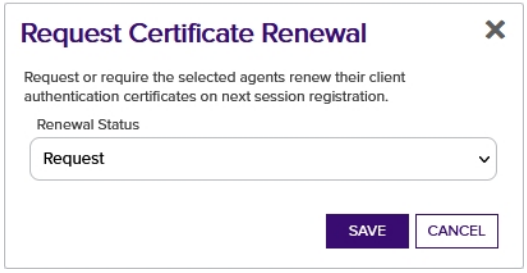


Figure 278: Request Renewal for an Orchestrator

Viewing Active Jobs for an Orchestrator

To view all the active jobs for an orchestrator, highlight the row in the orchestrator management grid and click **View Jobs** at the top of the grid or right-click the orchestrator in the grid and choose **View Jobs** from the right-click menu. This will take you to the scheduled jobs tab of the orchestrator job status page with the query field populated by the selected orchestrator.

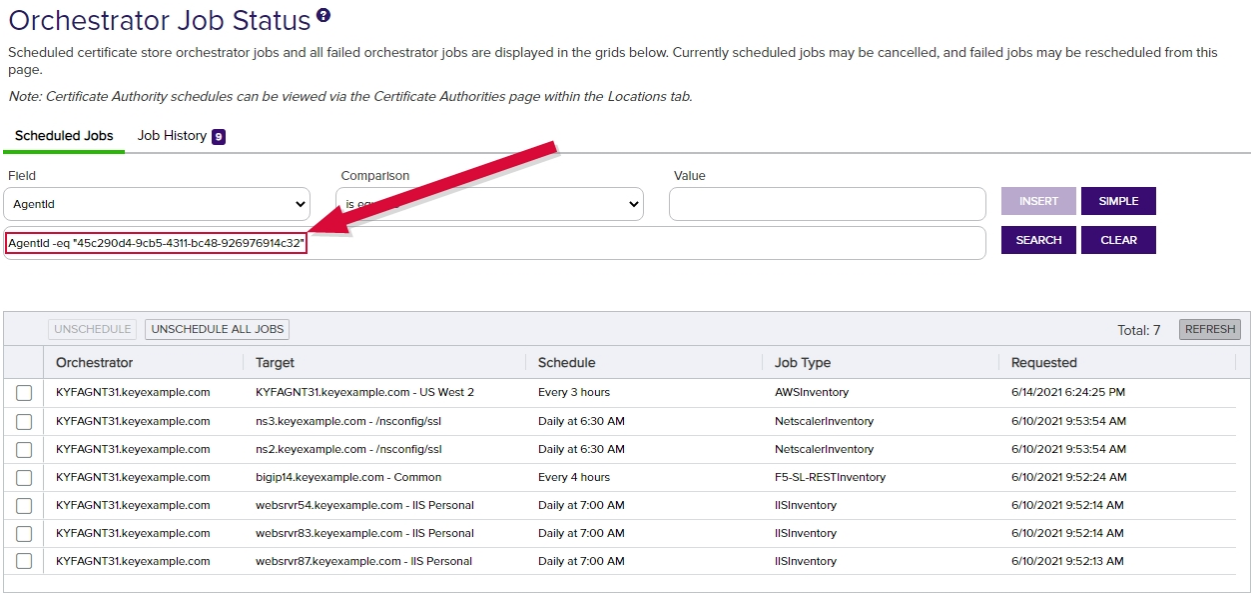


Figure 279: View Active Jobs for an Orchestrator

Viewing the Job History for an Orchestrator

To view job history for an orchestrator, highlight the row in the orchestrator management grid and click **View Job Histories** at the top of the grid or right-click the orchestrator in the grid and choose **View Job Histories** from the right-click menu. This will take you to the job history tab of the orchestrator job status page with the query field populated by the selected orchestrator.

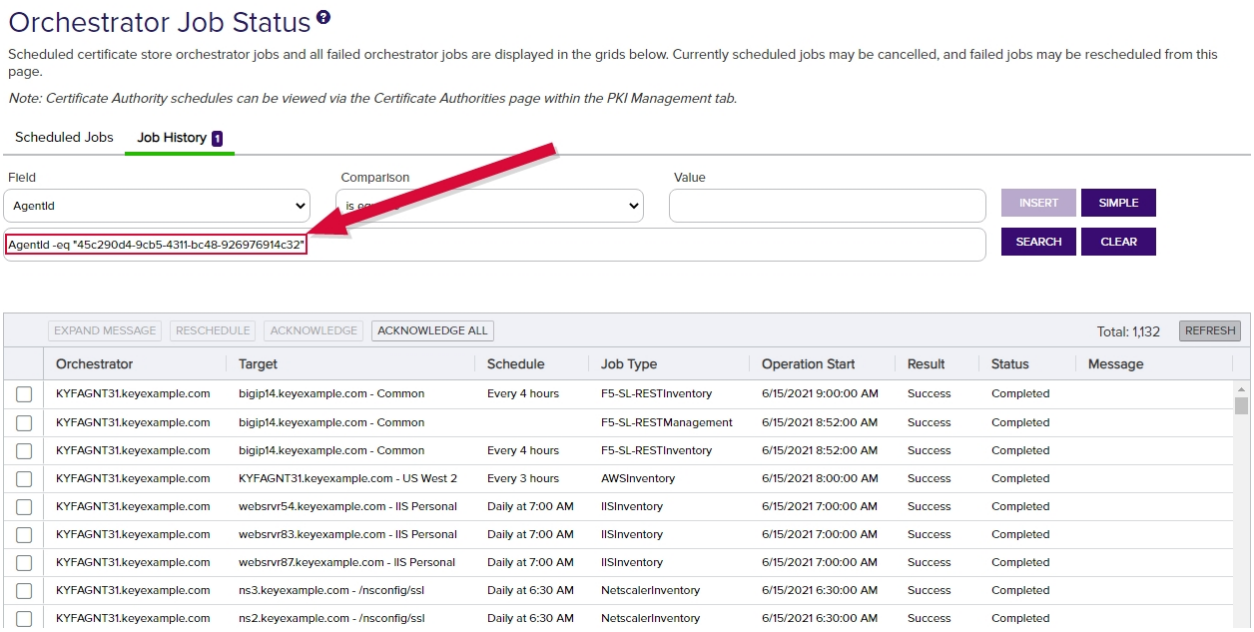


Figure 280: View Job History for an Orchestrator

Viewing Certificate Stores Associated with an Orchestrator

To view the certificate stores associated with an orchestrator, highlight the row in the orchestrator management grid and click **View Certificate Stores** at the top of the grid or right-click the orchestrator in the grid and choose **View Certificate Stores** from the right-click menu. This will take you to the certificate stores page with the query field populated by the selected orchestrator.

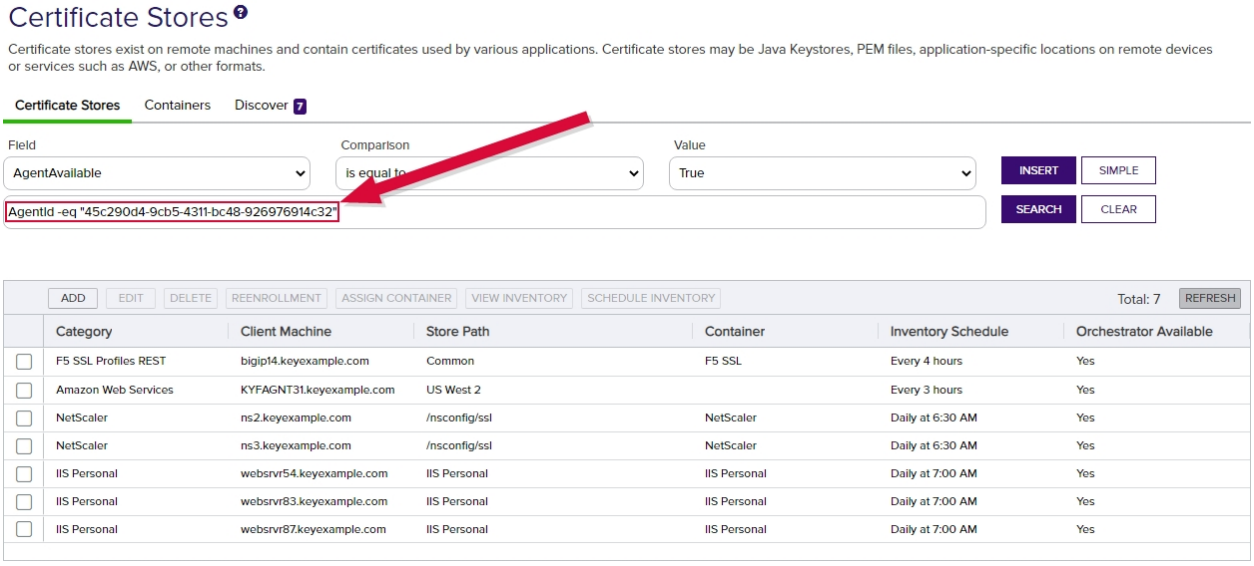


Figure 281: View Certificate Stores for an Orchestrator

Tip: This option is only useful for orchestrators that have a capability that makes use of certificate stores (e.g. JKS, PEM, IIS, etc. not SSL or SSH).

Fetch Logs

The fetch logs function is designed to retrieve a portion of the tail end of the orchestrator log for easy review. It is supported for both the Keyfactor Universal Orchestrator and the Native Agent.

To schedule a job to fetch the logs, click **Fetch Logs** from the actions buttons at the top of the Orchestrator Management grid or from the right-click menu. The job will be scheduled to run immediately, which means it should complete within a few minutes depending on other activity occurring at the same time. The fetch logs job will appear in Scheduled Jobs under Orchestrator Job Status with a job type of *Fetch Logs* and when complete will appear in Job History (see Job History on page 498).

For Native Agent fetch log jobs, when the job is complete, locate the completed job on the Job History tab and double-click or click **Expand Message** from the right-click menu or at the top of the grid. The job status message details show 4000 characters of the tail end of the log.

To review the log data for logs fetched from a Keyfactor Universal Orchestrator, use the *GET /OrchestratorJobs/JobStatus/Data* Keyfactor API method. See *Get Orchestrator Jobs Job Status Data* in the *Keyfactor Web APIs Reference Guide* for more information.

Tip: The orchestrator must be approved and have the LOGS capability in order for the *Fetch Logs* function to be enabled.

Note: The orchestrator must be configured to write log entries to a file in order for the *Fetch Logs* function to be able to retrieve logs. The Keyfactor Universal Orchestrator does this by default, but the Native Agent needs to be configured appropriately to write to a file in order to support this feature.
To set up logging on the Native Agent, see the Native Agent configuration instructions to configure logging and start the orchestrator with the appropriate logging level to allow for the use of the **Fetch Logs** feature:

https://github.com/Keyfactor/Keyfactor-CAgent

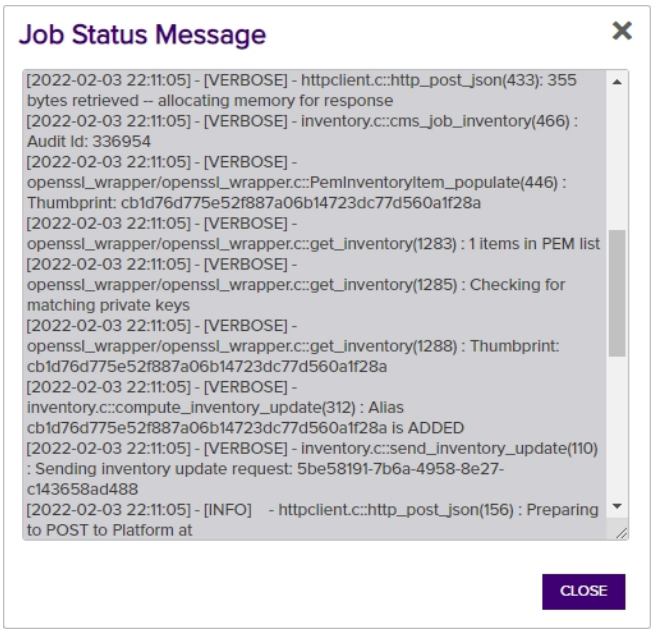


Figure 282: Sample Native Agent Fetch Log Results

Tip: If jobs for the Keyfactor Universal Orchestrator fail with messages similar to the following:

```
2021-08-05 10:47:23.1940
Keyfactor.Orchestrators.JobExecutors.OrchestratorJobExecutor [Debug] - Response
status code does not indicate success: 413 (Request Entity Too Large).

at System.Net.Http.HttpResponseMessage.EnsureSuccessStatusCode() in /_
/src/System.Net.Http/src/System/Net/Http/HttpResponseMessage.cs:line 172

at Keyfactor.Orchestrators.Services.HttpService.SendPostAsync[T](String uri,
Object requestData, Dictionary`2 headers) in F:\BuildAgents\Default1\_
work\24\s\src\OrchestratorServices\HttpService.cs:line 38
```

This indicates that the amount of data being returned on the job is greater than IIS on the Keyfactor Command server is configured to accept. You will need to make modifications to the IIS settings on your Keyfactor Command server to allow it to accept larger incoming pieces of content. You can do this using the configuration editor built into the IIS management console. Make the setting changes at the Default Web Site level (or other web site, if you installed your Keyfactor Command in an alternate web site). There are three settings that may need modification:

- system.webServer/security/requestFiltering/requestLimits/maxAllowedContentLength
- system.webServer/serverRuntime/uploadReadAheadSize
- system.web/httpRuntime/maxRequestLength

The most important of these is *maxAllowedContentLength*. Set this value to at least 2,500,000 bytes to support the maximum returned data size for the Keyfactor Universal Orchestrator. The default values of 4096 KB for the *maxRequestLength* and 49,152 for *uploadReadAheadSize* will probably be sufficient in most environments, unless you are also using SSL scanning (see Monitoring Network Scan Jobs with View Scan Details on page 454). (The system.webServer values are set in bytes while the system.web values are set in kilobytes.)

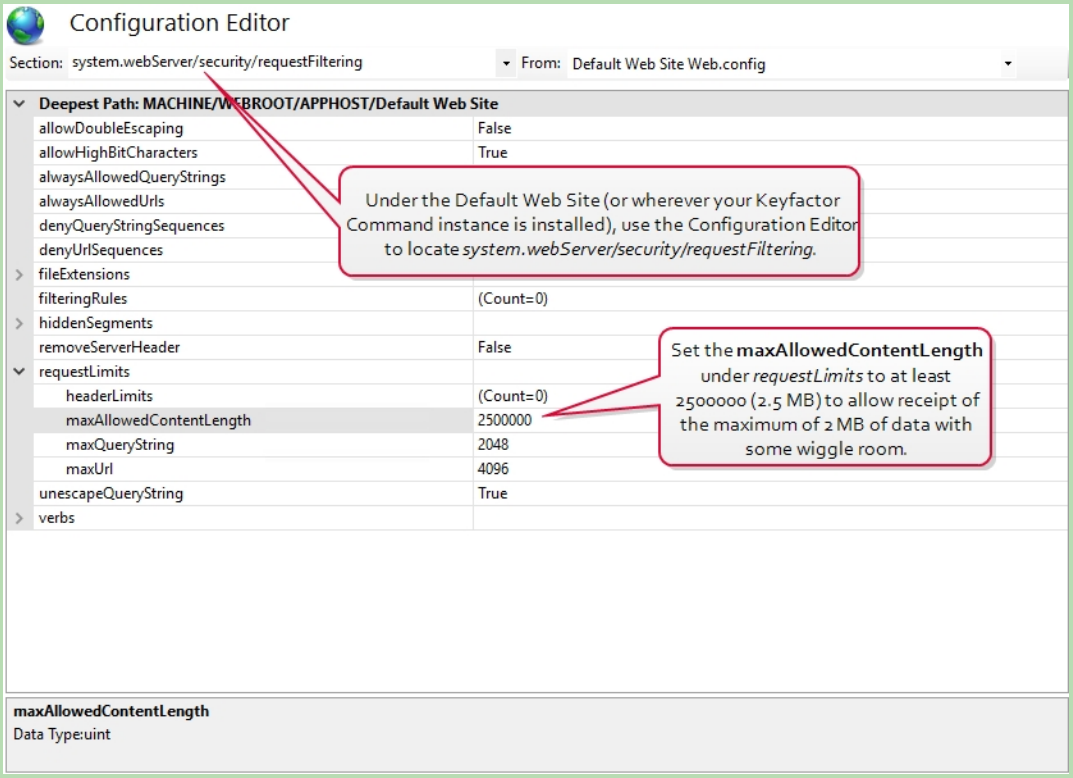


Figure 283: Modify IIS Settings for Keyfactor Universal Orchestrator Custom Jobs: maxAllowedContentLength

2.1.9.3 Orchestrator Job Status

The Orchestrator Job Status page provides information on currently scheduled certificate store, SSH, and SSL jobs as well as an audit log of job history.

Tip: Click the help icon (?) next to the page title to open the embedded web copy of the *Keyfactor Command Documentation Suite* to this section.
You can also find the help icon at the top of the page next to the **Log Out** button. From here you can choose to open either the *Keyfactor Command Documentation Suite* at the home page or the *Keyfactor API Endpoint Utility*.

Scheduled Jobs

The Scheduled Jobs tab on the Orchestrator Job Status page shows all of the currently scheduled jobs for any approved Android, Java, Native, and SSH Orchestrators and jobs other than remote CA sync for approved Keyfactor Universal Orchestrators and Windows Orchestrators (SSL jobs only appear while they are in progress). At a glance, you can see what discovery, inventory, management, and synchronization jobs are scheduled for all the active orchestrators that can communicate with Keyfactor Command.

The Orchestrator Job Status grid includes these fields:

Orchestrator

The host on which the orchestrator is running.

Target

The target machine name followed by the path and file name to the certificate store on the target machine for many types of jobs. This field may be blank for some types of jobs.

Schedule

The time at which or frequency with which a job will run. Add and remove certificate jobs will show *Immediately* unless they have been scheduled for a later time. Renewals and reenrollments will always show *Immediately* since these can't be scheduled for a later time. SSL jobs will always show *Immediately* since they only appear in the grid while they are in progress.

Job Type

The type of job—e.g. inventory, discovery, management (add and remove certificate), synchronization.

Requested

The date and time when the job was configured or updated.

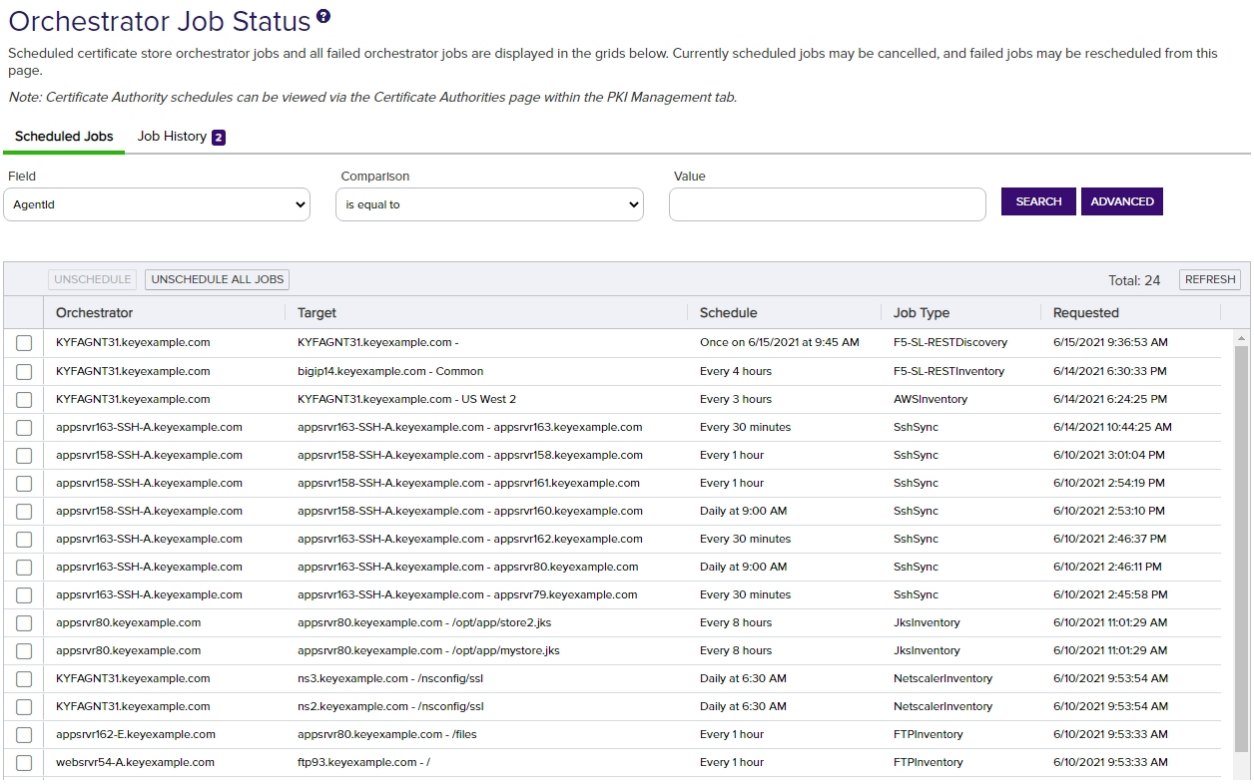


Figure 284: Orchestrator Job Status Scheduled Jobs

Orchestrator Scheduled Job Search Feature

The search function allows you to query the database for information. The same query structure is used in multiple locations within the Keyfactor Command Management Portal.

When you first open the page, you will see the simple search option. To execute a search, select the field and comparison operators in the dropdowns and type something on which to search in the value field (if applicable). If you select an *is null* or *is not null* comparison operator, the value field will be grayed out. Click the **Search** button to execute the query.

Each query consists of three parts:

Query Field

The available fields for querying vary depending on the area of the Management Portal in which the search is used. On this page, the queries can be done on the following built-in fields:

Agent Machine

Complete or partial matches with the orchestrator name as listed in the Orchestrator Machine field.

Job Type

Job Type contains or doesn't contain the selected keywords—Management (including add and remove certificates), Inventory, Certstore Discovery, SSL

Target Path

Complete or partial matches with the contents of the Target field, including the target machine name and the certificate store path and file name.

Schedule Type

Schedule Type matches the selected category—Immediate, Interval, Daily, Weekly, Monthly, Once.

Requested

Job was requested or updated before, after or on a specified date. Supports the %TODAY% token (see Advanced Searches on the next page).

Discovery, Reenrollment, SSL Monitoring, Sync, Enrollment.

Agent Type

Orchestrator Type matches the selected category—AWS, CA, F5, F5-WS-REST, F5-SL-REST, F5-CA-REST, FTP, IIS, JKS, NS, PEM, SSL, and any custom types you've created.

Agent Platform

Orchestrator Platform matches or doesn't match the selected category—Java (JKS and PEM), .NET (AWS, F5, FTP, IIS, NetScaler, and SSL), Mac, Android, Native, Bash (SSH), Unknown.

Agent ID

Orchestrator ID matches or doesn't match the entered GUID (primarily used for internally generated searches when the user is redirected here from another page).

Comparison Operator

The query comparison operators vary depending on the type of field selected and the specific properties of the field. The list below shows the dropdown list comparison operators, as well as the equivalent query language syntax (in parentheses).

Most string fields (the vast majority of the built-in fields) support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Contains (-contains)
- Does not contain (-notcontains)
- Starts with (-startswith)
- Ends with (-endswith)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Most date and integer fields support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Is less than (-lt)
- Is less than or equal to (-le)
- Is greater than (-gt)
- Is greater than or equal to (-ge)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Most Boolean (true/false) fields support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Comparison Value

The value you enter for comparison must match the field type. For example, integer fields only support numerical values. String fields support all alphanumeric characters. Boolean fields only support True or False. The value field is not case sensitive. Date fields support only properly formatted dates and will initially display as mm/dd/yyyy. You can choose to populate the date field by:

- Clicking in a date Value field to open a pop-up calendar to select a date that will populate the field.
- Clicking in a segment of the date format (i.e., mm/dd/yyyy) and entering a value. As you continue to type in any one segment, the cursor will keep moving onto the next segment.

The results that match your search criteria will be displayed in the results grid below the search selection options.

Advanced Searches

On any search page you can click **Advanced** to the right of the Search button to display the advanced search options. Click **Simple** to close the advanced search options again.

Multiple Criteria

Using the advanced search options, you can build a query based on multiple criteria using AND/OR logic. As with a simple search, you select a field and comparison operator in the drop-downs and then enter a comparison value, if applicable. Click **Insert** to add the search criteria to the query field below the selection fields. Use the selection fields to build multiple search criteria. Each time you click the insert button, an AND is added between the previous search criteria and the newly added one. You can change the AND to an OR if desired. You can use parentheses around portions of the query along with AND/OR to change the query meaning.

For example, for certificate searches:

```
(CN -contains "appsrvr" AND IssuedDate -ge "01/01/2022") OR (CN -contains "appsrvr" AND
TemplateShortName -contains "web")
```

This query will return all the certificates issued on or after January 1, 2022 with the string appsrvr in the CN and also all certificates issued at any time with the string appsrvr in the CN using a template referencing web. When you have entered all the desired search criteria, click **Search** to execute the query. If you wish to clear the query field and start over, click the **Clear** button.

In addition to the options available in the query builder, three special values can be used in selected searches by typing them in directly:

- %TODAY%
  Use the TODAY special value in place of a specific date in date queries. This option supports math operations, so you can use TODAY-10 or TODAY+30. The built-in *Certificates Expiring in 7 Days* collection uses this special value (see Certificate Collection Manager on page 80).
- %ME%
  Use the ME special value in place of a specific domain\user name in queries that match a

domain\user name. The built-in *My Certificates* collection uses this special value (see Certificate Collection Manager on page 80).

- %ME-AN%
  Use the ME-AN special value in place of a specific user name excluding the domain. This is beneficial in environments with multiple domains where there is a desire to query for a user's certificates even if they were requested across multiple domains.

> **Important:** The special query options of %TODAY%, %ME%, and %ME-AN% are only supported in uppercase. Lowercase equivalents (e.g. %me%) cannot be substituted.

Unschedule a Job

To unschedule a job, highlight the row for the job in the orchestrator job status grid and click **Unschedule** at the top of the grid or right-click the job in the grid and choose **Unschedule** from the right-click menu.

To unschedule multiple jobs, do a search for the jobs you wish to unschedule (e.g. JobType -contains "Discovery") and click **Unschedule All Jobs** at the top of the grid.

If an inventory job for a certificate store is unscheduled, all instances of that job will be removed (as opposed to just the next inventory job) and that store will not be inventoried again until another inventory job is scheduled for it on the Certificate Stores page.

> **Tip:** SSL discovery and monitoring jobs and SSH synchronization jobs cannot be unscheduled from this page—this should be done in SSL and SSH management instead (see SSL Discovery on page 443 and SSH Server Groups on page 542).

Job History

The Job History tab on the Orchestrator Jobs page shows a record of discovery, inventory and management jobs for certificate stores, SSH servers, SSL endpoints and remote CAs. It keeps the three most recent inventory jobs, whether they have warnings, failed, or succeeded. Information on potential causes of the problem to allow for troubleshooting is provided for failed jobs. The small number that appears on the tab to the right of the title indicates how many failures and warnings there have been, if any, within the last seven days, by default, unless the job has been marked as acknowledged (see Handling Job History Error or Warning Messages on page 502). This acts as a reminder to check for failures and warnings. This number of days for reporting is configurable using the *Job Failures and Warnings Age Out (days)* application setting (see Application Settings: Agents Tab on page 596).

The Job History grid includes these fields:

Orchestrator

The host on which the orchestrator was running.

Operation Start

The time at which the job was run.

Target

The target machine name followed by the path and file name to the certificate store on the target machine for many types of jobs, the endpoint group name for SSL jobs, or the CA name for remote CA jobs. This field may be blank for some types of jobs.

Schedule

The time at which or frequency with which a job was scheduled to run. Add and remove certificate jobs, will show *Immediately* unless they were scheduled for a later time. Renewal and reenrollment jobs will always show *Immediately* since they don't support later scheduling, as will fetch logs jobs.

Job Type

The type of job that was run and in some cases the orchestrator type associated with the job (e.g. F5 SSL Profiles Management, PEM File Discovery, Java Keystore Inventory or CA Synchronization).

Operation End

The time at which the job was completed.

Result

The outcome of the job—e.g. Success, Failure, or Warning. Under some circumstances—for example, jobs that are still actively running—Unknown may appear here.

Status

The status of the job—e.g. Acknowledged, Completed, CompletedWillRetry, or InProcess. If a job shows as CompletedWillRetry, it has failed at least once, is automatically retrying five times, by default (see the *Number of times a job will retry before reporting failure* in Application Settings: Agents Tab on page 596) and cannot be rescheduled because it is still attempting to run.

Message

The message indicating the reason for the failure or warning, if applicable. Double-click the grid row or right-click and choose **Expand Message** from the right-click menu to read the error message in full.

Note: Currently, any jobs initiated with the **Fetch Logs** function will not be included in any **Job Type** search results, but will be included in any other query search field. See Fetch Logs on page 491 for more information.

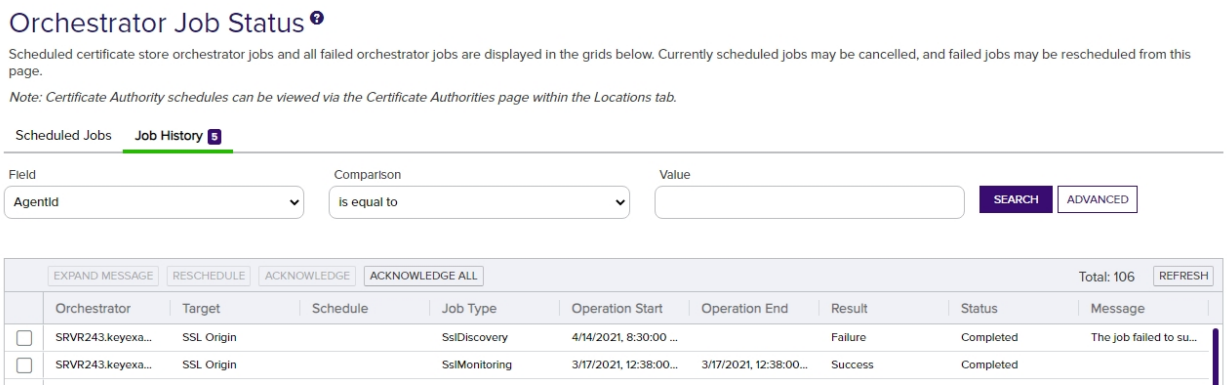


Figure 285: Orchestrator Job History

Note: For Bash Orchestrator message resolution see SSH-Bash Orchestrator Job History Warning Resolution on page 699.

Job History Search Feature

The search function allows you to query the database for information. The same query structure is used in multiple locations within the Keyfactor Command Management Portal.

When you first open the page, you will see the simple search option. To execute a search, select the field and comparison operators in the dropdowns and type something on which to search in the value field (if applicable). If you select an *is null* or *is not null* comparison operator, the value field will be grayed out. Click the **Search** button to execute the query.

Each query consists of three parts:

Query Field

The available fields for querying vary depending on the area of the Management Portal in which the search is used. On this page, the queries can be done on the following built-in fields:

Status

Status matches or doesn't match the selected category—Acknowledged, Completed, InProcess, Waiting, Unknown.

Result

Result matches or doesn't match the selected category—Failure, Warning, Success, Unknown.

Agent

Complete or partial matches with the orchestrator name as listed in the orchestrator field.

Target Path

Complete or partial matches with the contents of the Target field, including the target machine name and the certificate store path and file name for types of jobs listing those, or for SSL jobs, the endpoint group name, or for remote CA synchronization jobs, the CA name.

Schedule Type

Schedule Type matches or does not match the

Job Type

Job Type matches or does not match the selected category—Management, Inventory, Certstore Discovery, SSL Discovery, Reenrollment, SSL Monitoring, CA Synchronization.

Operation Start

Operation Start before or after a specified date and time. Supports the %TODAY% token (see Advanced Searches on the next page).

Message

Partial matches with the error or warning message listed in the Message field.

Agent ID

Agent ID matches or doesn't match the entered GUID (primarily used for internally generated searches when the user is redirected here from another page).

selected category—Immediate, Interval, Daily, Weekly, Monthly, Once.

Comparison Operator

The query comparison operators vary depending on the type of field selected and the specific properties of the field. The list below shows the dropdown list comparison operators, as well as the equivalent query language syntax (in parentheses).

Most string fields (the vast majority of the built-in fields) support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Contains (-contains)
- Does not contain (-notcontains)
- Starts with (-startswith)
- Ends with (-endswith)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Most date and integer fields support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Is less than (-lt)
- Is less than or equal to (-le)
- Is greater than (-gt)
- Is greater than or equal to (-ge)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Most Boolean (true/false) fields support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Comparison Value

The value you enter for comparison must match the field type. For example, integer fields only support numerical values. String fields support all alphanumeric characters. Boolean fields only support True or False. The value field is not case sensitive. Date fields support only properly formatted dates and will initially display as mm/dd/yyyy. You can choose to populate the date field by:

- Clicking in a date Value field to open a pop-up calendar to select a date that will populate the field.
- Clicking in a segment of the date format (i.e., mm/dd/yyyy) and entering a value. As you continue to type in any one segment, the cursor will keep moving onto the next segment.

The results that match your search criteria will be displayed in the results grid below the search selection options.

Advanced Searches

On any search page you can click **Advanced** to the right of the Search button to display the advanced search options. Click **Simple** to close the advanced search options again.

Multiple Criteria

Using the advanced search options, you can build a query based on multiple criteria using AND/OR logic. As with a simple search, you select a field and comparison operator in the drop-downs and then enter a comparison value, if applicable. Click **Insert** to add the search criteria to the query field below the selection fields. Use the selection fields to build multiple search criteria. Each time you click the insert button, an AND is added between the previous search criteria and the newly added one. You can change the AND to an OR if desired. You can use parentheses around portions of the query along with AND/OR to change the query meaning.

For example, for certificate searches:

```
(CN -contains "appsrvr" AND IssuedDate -ge "01/01/2022") OR (CN -contains "appsrvr" AND
TemplateShortName -contains "web")
```

This query will return all the certificates issued on or after January 1, 2022 with the string appsrvr in the CN and also all certificates issued at any time with the string appsrvr in the CN using a template referencing web. When you have entered all the desired search criteria, click **Search** to execute the query. If you wish to clear the query field and start over, click the **Clear** button.

In addition to the options available in the query builder, three special values can be used in selected searches by typing them in directly:

- %TODAY%
  Use the TODAY special value in place of a specific date in date queries. This option supports math operations, so you can use TODAY-10 or TODAY+30. The built-in *Certificates Expiring in 7 Days* collection uses this special value (see Certificate Collection Manager on page 80).
- %ME%
  Use the ME special value in place of a specific domain\user name in queries that match a domain\user name. The built-in *My Certificates* collection uses this special value (see Certificate Collection Manager on page 80).
- %ME-AN%
  Use the ME-AN special value in place of a specific user name excluding the domain. This is beneficial in environments with multiple domains where there is a desire to query for a user's certificates even if they were requested across multiple domains.

> **Important:** The special query options of %TODAY%, %ME%, and %ME-AN% are only supported in uppercase. Lowercase equivalents (e.g. %me%) cannot be substituted.

Handling Job History Error or Warning Messages

To view the details of an error or warning message, double-click the row for the job in the orchestrator job history grid, right-click the job and choose **Expand Message** from the right-click menu, or highlight the row in the grid and click **Expand Message** at the top of the grid.

To reschedule a job, correct the error that caused the problem, then highlight the row for the job in the orchestrator job history grid and click **Reschedule** at the top of the grid or right-click the job in the grid and choose **Reschedule** from the right-click menu.

To mark an error or warning grid entry as acknowledged, highlight the row for the job in the orchestrator job history grid and click **Acknowledge** at the top of the grid or right-click the job in the grid and choose **Acknowledge** from the right-click menu. Jobs that are in process or that have completed successfully cannot be marked as acknowledged. Marking a job as acknowledged removes it from the count on the job history tab (if the job falls within the count period defined by the *Job Failures and Warnings Age Out (days)* application setting—see Application Settings: Agents Tab on page 596).

2.1.9.4 Orchestrator Blueprints

The orchestrator blueprint system allows a large number of similar orchestrators to be configured with minimal effort on the part of the user. By taking a snapshot of the certificate stores and scheduled jobs on one orchestrator, matching certificate stores and jobs can be defined on another orchestrator with just a few clicks. With an orchestrator auto-registration handler, blueprint application can even be completely automated, so that a large number of machines or devices can be configured and obtain certificates with no user input after initial configuration of the blueprint and handler. This can greatly improve security by ensuring that each device is provisioned from day one with a unique certificate using a private key generated on the device as well as an up-to-date list of trusted roots, and it allows for continuous monitoring and reporting of all certificates across all configured devices.

Orchestrator blueprints are generated from the Orchestrator Management page (see Orchestrator Management on page 481) and applied to new orchestrators manually via the Orchestrator Management page. On the Orchestrator Blueprints page, you can review the existing blueprints, view details of a blueprint (what certificate stores and scheduled jobs are included in the blueprint), and delete blueprints.

Blueprint Operations

Some blueprint operations are carried out on the Orchestrator Management page (generating and applying blueprints) while others are done on the Orchestrator Blueprints page (viewing and deleting blueprints).

Applying Blueprints

When you apply a blueprint to an orchestrator, you are defining a set of certificate stores and scheduled jobs for that orchestrator as determined by the blueprint at the time that the blueprint is applied. There is no ongoing effect to having a blueprint applied. If the blueprint is deleted, this does not affect the orchestrators to which the blueprint was applied. Likewise, changing the orchestrator from which the blueprint was created after creation of the blueprint does not affect the blueprint. The blueprint continues to contain the certificate stores and scheduled jobs that were associated with the orchestrator at the time the blueprint was taken.

Orchestrator blueprints work with Java and PEM certificate stores and can be used with the Java, Native, and Android agents.

Blueprints are applied to an orchestrator from the Orchestrator Management page (see Generating and Applying Blueprints on page 486).

Modifying Blueprints

Blueprints can't be edited. To modify a blueprint, modify the certificate stores and scheduled jobs on the orchestrator from which the blueprint was taken and capture a new blueprint (see Generating and Applying Blueprints on page 486). This will replace the existing blueprint. An orchestrator can only have one blueprint at a time.

Figure 286: Orchestrator Blueprints

Deleting Blueprints

To delete a blueprint:

1. In the Management Portal, browse to *Orchestrators > Orchestrator Blueprints*.
2. On the Orchestrator Blueprints page, select an orchestrator blueprint and click **Delete** from either the top or right-click menu.
3. On the Confirm Operation alert, click **OK** to confirm or **Cancel** to cancel the operation.

Viewing Blueprint Details

To view the details of a blueprint:

1. In the Management Portal, browse to *Orchestrators > Orchestrator Blueprints*.
2. On the Orchestrator Blueprints page, select an orchestrator blueprint and double-click or click **View** from either the top or right-click menu.
3. On the Confirm Operation alert, click **OK** to confirm or **Cancel** to cancel the operation.

On the Certificate Stores tab you can see the certificate store paths and types that have been associated with the blueprint. On the Scheduled Jobs tab you can see the scheduled jobs for these certificate stores. These would generally be inventory jobs, though it is possible to blueprint an orchestrator with other types of active jobs (e.g. discovery).

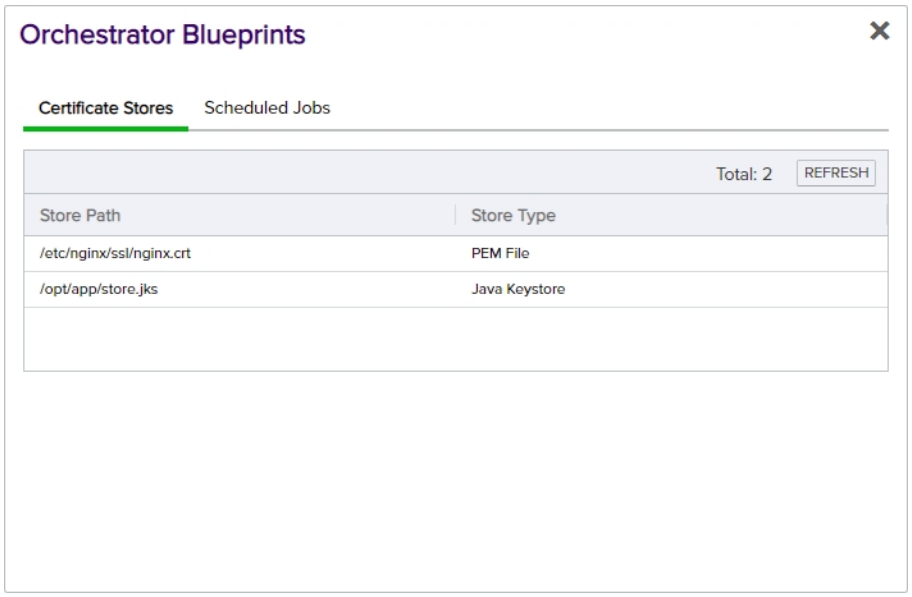


Figure 287: Orchestrator Blueprint Details: Certificate Stores Tab

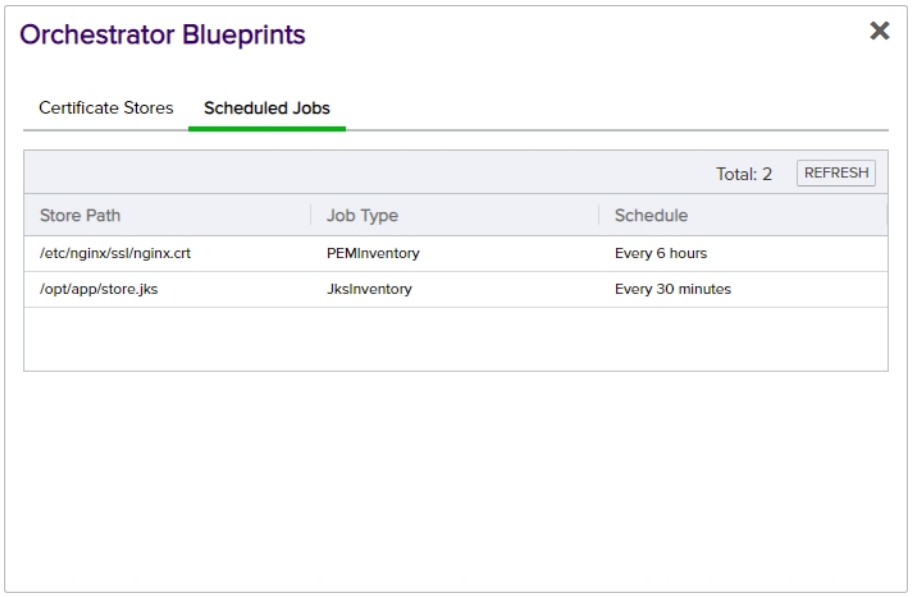


Figure 288: Orchestrator Blueprint Details: Scheduled Jobs Tab

2.1.9.5 Mac Auto-Enrollment

The settings on the Mac Auto-Enrollment page control how Mac auto-enrollment agents in your environment auto-enroll for certificates through Keyfactor Command. The available settings are:

Enabled **Metadata Field Name**

Controls whether Mac auto-enrollment is allowed in the environment.

Interval

Defines, in minutes, how frequently the agent should check to see if there are new certificates for which to enroll.

Use Metadata

If enabled, allows you to automatically associate data in a custom metadata field with an auto-enrolled Mac certificate. See Certificate Metadata on page 646 for more information about metadata fields.

Choose an existing metadata string or Boolean field in the dropdown to populate for the certificate, if *Use Metadata* is enabled.

Metadata Value Type

Determines whether the data inserted in the metadata field will be based on the machine from which the certificate is requested or will be set to the same value for all certificates. Choose *Special Text* to pick from machine-specific values in the Metadata Value dropdown. Choose *Static Value* to enter text that will be populated in every Mac auto-enrollment certificate that is issued.

Metadata Value

If you select Special Text for the Metadata Value Type, this field will be a dropdown including values that are available from the Mac client. In the current version of the agent, only the Mac serial number is available. If you select Static Value for the Metadata Value Type, this will be a free-form field in which you can type any text you want to appear in the selected metadata field for all Mac auto-enrolled certificates. If you've selected a Boolean metadata field, you'll have the choice of *True* or *False* for the value.

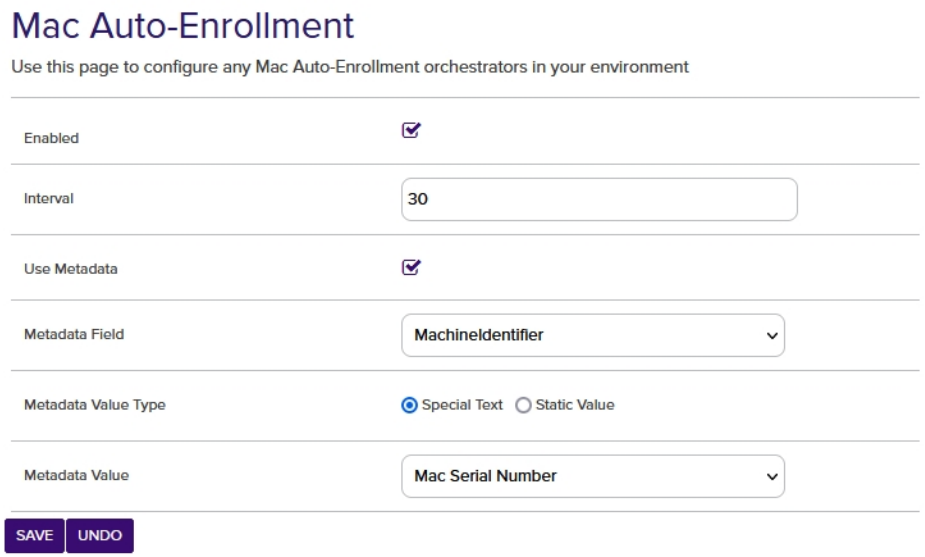


Figure 289: Mac Auto-Enrollment Configuration

To save your changes, click **Save** at the bottom of the page, or to revert to the previous settings without saving, click Undo.

Tip: For more information about the Mac Auto-Enrollment Agent, see the separate Mac Auto-Enrollment Guide.

2.1.10 SSH

Keyfactor SSH Management is designed to allow organizations to inventory and manage secure shell (SSH) keys across the enterprise. The solution consists of two elements; the SSH functionality on the Keyfactor Command Management Portal and the Keyfactor Bash Orchestrator.

The Keyfactor Bash Orchestrator runs on Linux servers and can be operated in two possible modes:

- The orchestrator is used in *inventory only* mode to perform discovery of SSH public keys and associated Linux user accounts across multiple configured targets.

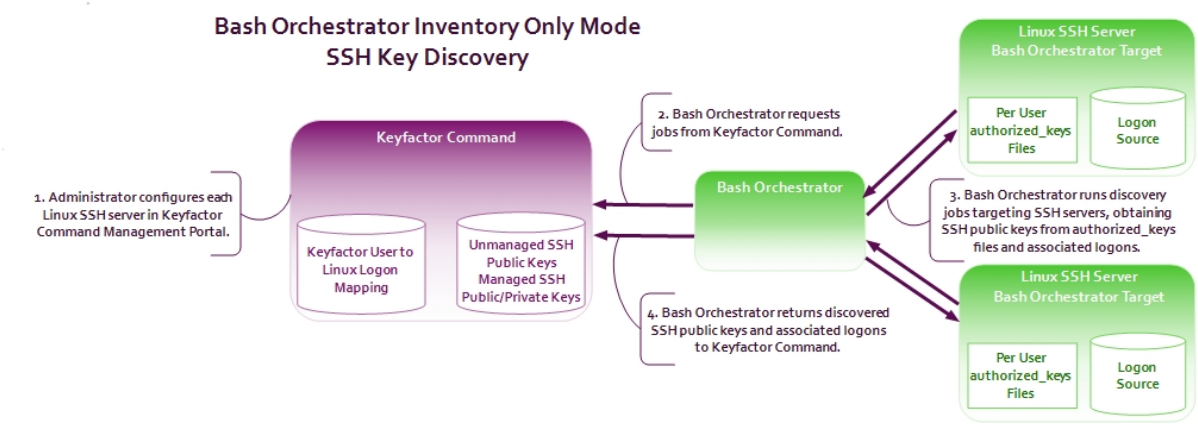


Figure 290: SSH Key Discovery Flow

- When operated in *inventory and publish policy* mode, the orchestrator can be used to add SSH public keys and Linux user accounts on targets and remove rogue keys that appear without authorization.

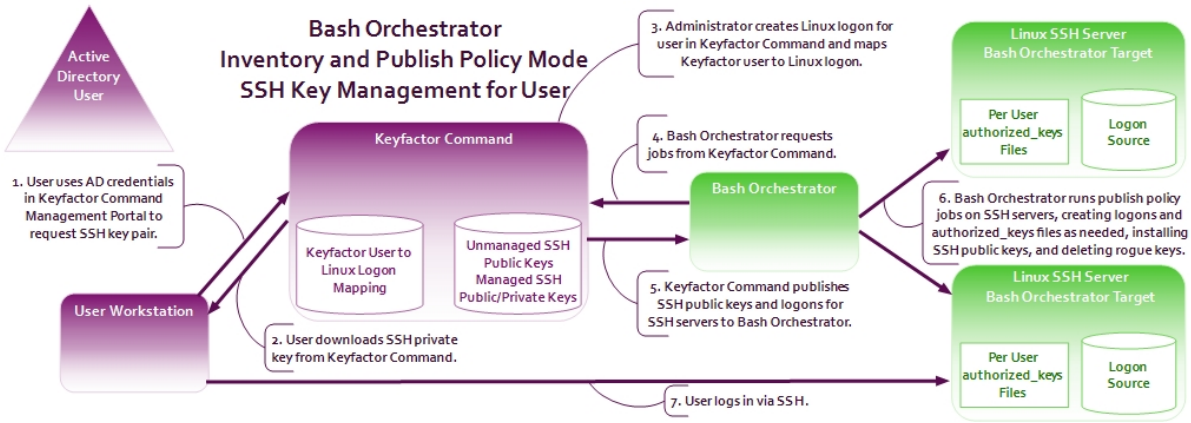


Figure 291: SSH User Key Management Flow

As you work with SSH keys in Keyfactor Command, you will need to understand the difference between *users*, *service accounts*, and *logons*:

- A *user* is an account in Keyfactor Command—based on an Active Directory user account—which has been granted the Keyfactor Command SSH User role permission (see SSH Permissions on page 579).

  A *user* can use the My SSH Key tool (see My SSH Key on page 512) to generate an SSH key pair for himself or herself. This stores the user's SSH public and private key in the Keyfactor Command database. An administrator can then use one of the options in the SSH section of the Management Portal (see Editing Access to an SSH Server on page 561, Editing Access to an SSH Server Group on page 545, or Adding Logons on page 567) to map the *user* record and its associated public key to one or more *logons*, creating new *logons* if needed. For servers operating in *inventory and publish policy* mode, this will cause the *user*'s public key to be published to the authorized_keys file(s) for each mapped *logon* on the associated SSH server(s) during the next synchronization job. The *user* downloads the private key of the key pair to his or her machine in the My SSH Key tool and retains it there to allow for SSH connections to the target servers the administrator distributes the matching public key to.

  Note: If an administrator maps a *user*'s public key to a *logon* for a server that is in *inventory only* mode, nothing will happen. The key will not be published to the server.

  Note: OpenSSH maintains a file for each user that contains the public keys authorized to connect via SSH. By default, this file is named authorized_keys. In this document, we refer to this file as *authorized_keys*, however in your environment, this file may have a different name. The file name used in a given environment is defined in the AuthorizedKeysFile setting in the OpenSSH sshd_config file.

- A *service account* is a string representing a service for which an SSH key has been requested through the Service Account Keys page (see Service Account Keys on page 524). It is made up of the *Username* and *Client Hostname* entered during service account key creation in the form

servicename@hostname (e.g. myservice@appsrvr12).

> **Tip:** The client hostname that makes up part of the service account name is not necessarily an actual server hostname. It is a user-defined reference that can contain any string.

An administrator can use the Service Account Keys page (see Service Account Keys on page 524) to generate an SSH key pair for an application—referenced by a *service account* name—that makes use of SSH for communication, storing the application's SSH public and private key in the Keyfactor Command database. The administrator needs to store the private key securely on the Linux server where the service account for the application can access it and follow the same procedure as for users to distribute the public key to the appropriate SSH server(s) operating in *inventory and publish policy* mode.

> **Note:** If an administrator maps a *service account*'s public key to a *logon* for a server that is in *inventory only* mode, nothing will happen. The key will not be published to the server.

- A *logon* is a Linux user account. In most cases for the purposes of SSH management, these are Linux user accounts that have or are intended to have SSH public keys associated with them on managed SSH servers, stored in an authorized_keys files. However, Linux *logons* without keys (and which should likely never have keys like "root" or OS-specific accounts like "halt") also appear in Keyfactor CommandSSH management.

Typically, you would initially configure your servers in *inventory only* mode and scan the servers for any existing authorized_keys files containing SSH public keys. This is the discovery phase. Once the discovery phase is complete for a server or server group, you would then switch it to *inventory and publish policy* mode.

When a server is in *inventory and publish policy* mode, any new keys that appear in its authorized_keys files in a manner other than by distribution from Keyfactor Command are automatically deleted. This allows administrators to closely control who has access to the servers via SSH. Any keys and authorized_keys files that were in place before the switch to managed mode are synchronized to Keyfactor Command (see Unmanaged SSH Keys on page 538) but not removed from the Linux server. The administrator can choose to remove them through Keyfactor CommandSSH management once the switch to *inventory and publish policy* mode is made, if desired. Any keys placed on the Linux server via Keyfactor Command once the servers are in *inventory and publish policy* mode are considered managed keys and do not appear on the Unmanaged Keys page.

As SSH servers are scanned for SSH keys during the initial discovery phase, the Linux user accounts associated with these keys are synchronized to Keyfactor Command. These user accounts—logons—can be viewed on the Logons tab under Server Manager. Once each server is switched to *inventory and publish policy* mode, these logons can be managed and additional logons can be added to the Linux servers via Keyfactor CommandSSH management.

> **Example:** A large organization has dozens of Linux servers that have historically been accessed using SSH public key authentication. They don't know who has access to which servers using this method or what public keys are out on the servers. To get the keys under

control, they first do discovery:

1. Install the Keyfactor Bash Orchestrator on one Linux server in the environment.
2. Copy the remoteinstall.sh script, containing the public key of the orchestrator service account, from the orchestrator to the first ten Linux targets they want to bring under control.
3. On each of the control targets, run the remoteinstall.sh script. This creates a local user account and installs the orchestrator's SSH public key to allow the orchestrator to use SSH to remote into the control target to run inventory and publish policy.
4. In the Keyfactor Command Management Portal, approve the new orchestrator (see Approving or Disapproving Orchestrators on page 486).
5. In the Management Portal, create at least one server group, setting a scanning schedule of every hour (Interval = 1 hour) for the initial discovery phase and leaving the **Enforce Publish Policy** box unchecked (see Adding Server Groups on page 543).

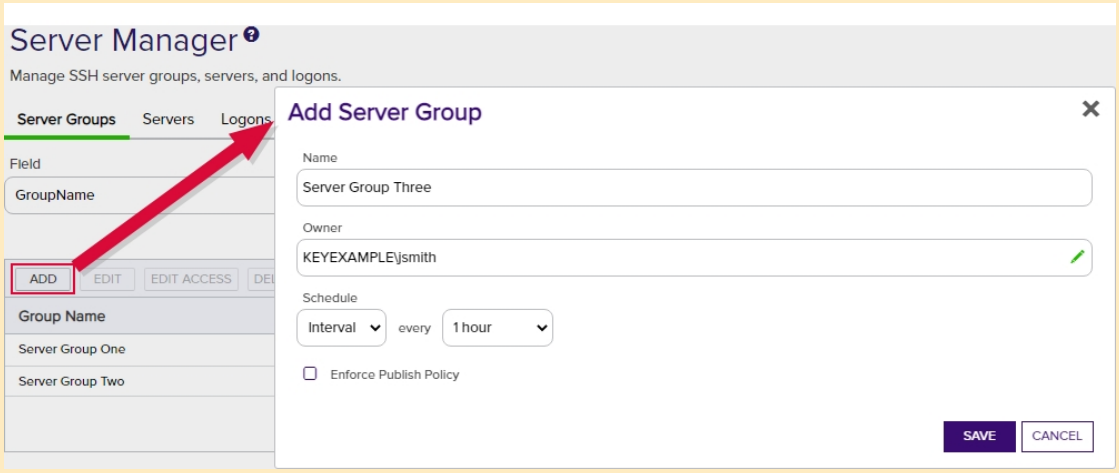


Figure 292: Add SSH Server Group for Discovery

6. In the Management Portal, add one server record for the orchestrator and one for each control target (a total of 11 records added), making them members of the group created in the previous step and selecting the **Inventory Only** radio button on the Basic tab (see Adding SSH Servers on page 559).

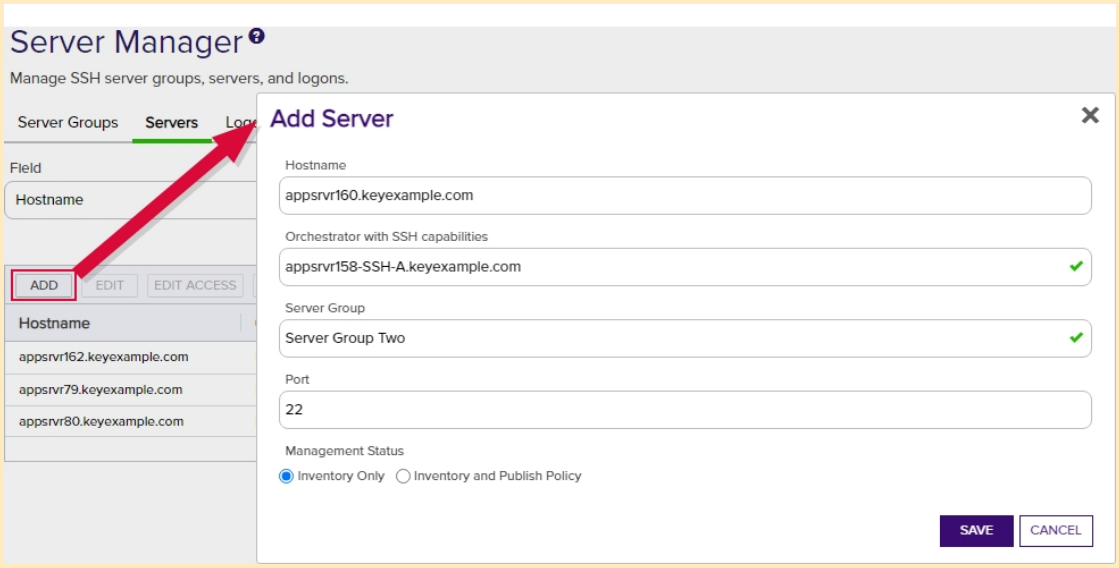


Figure 293: Add SSH Server for Discovery

7. After allowing the discovery scans to run, review the logons (see Logons on page 567) and the keys discovered (see Unmanaged SSH Keys on page 538) to see what keys are out on the servers and who they belong to.

Now having a handle on what keys are on these ten target servers plus the orchestrator itself, they are now ready to bring these servers under management. To bring the servers under management, they:

1. In the Management Portal, edit the record for the server group and check the **Enforce Publish Policy** box (see Editing or Deleting an SSH Server on page 561). This change will replicate to all servers in the group.
2. In the Management Portal, use the Logons page to remove any Linux user accounts that should not be on the target servers (see Editing or Deleting a Logon on page 570).
3. In the Management Portal, use the Unmanaged SSH Keys page to remove any public keys that are no longer needed from the target servers (see Deleting an Unmanaged Key on page 539).

These servers are now ready for ongoing management. The administrator is now ready to do discovery on the next group of servers, for which a second server group should be created.

See further examples in My SSH Key on the next page and Service Account Keys on page 524.

For more information about the orchestrator, see *Bash Orchestrator* in the *Keyfactor Orchestrators Installation and Configuration Guide*.

The options available in the SSH section of the Management Portal are:

My SSH Key

Generate an SSH key pair for the logged on user and download the private key to the local machine. The public key is stored in Keyfactor Command and can be pushed out to Linux client controlled by the Keyfactor Bash Orchestrator to allow the user access to the servers.

Service Account Keys

Generate an SSH key pair for a service using SSH and download the private key to the local machine. The public key is stored in Keyfactor Command and can be pushed out to Linux servers controlled by the Keyfactor Bash Orchestrator to allow the user access to the servers.

Unmanaged Keys

Review public SSH keys found during discovery on servers configured to be inventoried by the Keyfactor Bash Orchestrator in *inventory only* mode.

Server Manager

Manage servers, server groups, server logons for Linux clients, and SSH users controlled by the Keyfactor Bash Orchestrator.

2.1.10.1 My SSH Key

On the My SSH Key page, any user with the *SSH User* Keyfactor Command role permission (see SSH Permissions on page 579) can generate an SSH key pair for himself or herself. If the user has previously generated a key pair through Keyfactor Command, it will be displayed here. In this interface a user can view only his or her own key pair; keys for any other Keyfactor Command users are not accessible.

Example: An administrator wants to provision new user Zed Adams and grant him access to login via secured SSH using PuTTY to three Linux servers controlled by the Keyfactor Bash Orchestrator. The servers are set to both inventory and publish policy. To accomplish this, the administrator:

1. Adds Zed's AD account to the AD group that grants him the SSH User role permission in Keyfactor Command and allows him to login to the Management Portal.
2. Directs Zed to login to the Management Portal, go to the My SSH Key page and generate a new key pair (see Generating a New Key on page 518). She instructs him to enter the following information in the form:
    - **Key Type**: Ed25519
    - **Key Length**: 256
    - **Username**: Accept the default (his AD username)
    - **Email**: zed.adams@keyexample.com

- **Passphrase**: A password of Zed's choosing used to secure the private key on download.
- **Comment**: Zed B. Adams

3. Instructs Zed to download the SSH private key and use the PuTTY Key Generator tool to open the key and convert it to the PuTTY format:

    a. Click **Load** and browse to locate the downloaded private key. This key is named something like *SSH-Key-KEYEXAMPLE-zadams.identity*.

    b. In the Parameters section of the page, select **Ed25519** as the type of key to generate.

    c. Click **Save private key** and save the private key in the PuTTY format (*.ppk) in a safe location on the local machine.

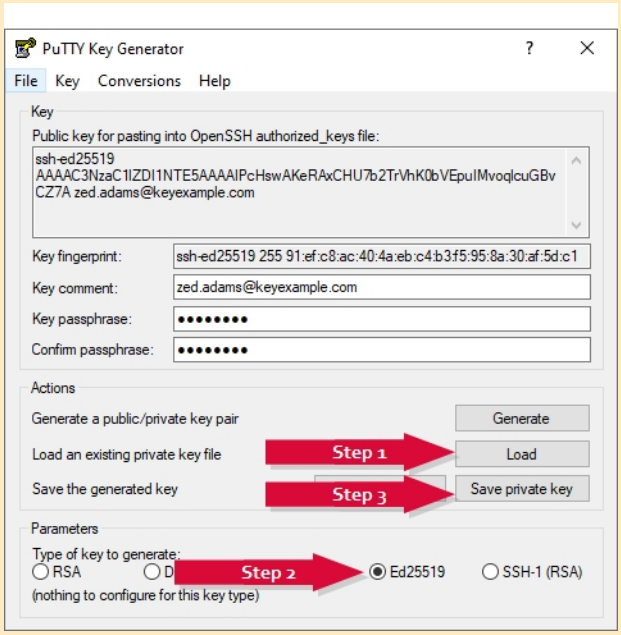


Figure 294: Use PuTTY Key Generator to Convert Zed's Private Key

4. Uses the Keyfactor Command Management Portal to create Linux logons for Zed on each of the three servers that Zed should have access to and map Zed's new public key to these three logons (see Editing Access to an SSH Server Group on page 545).

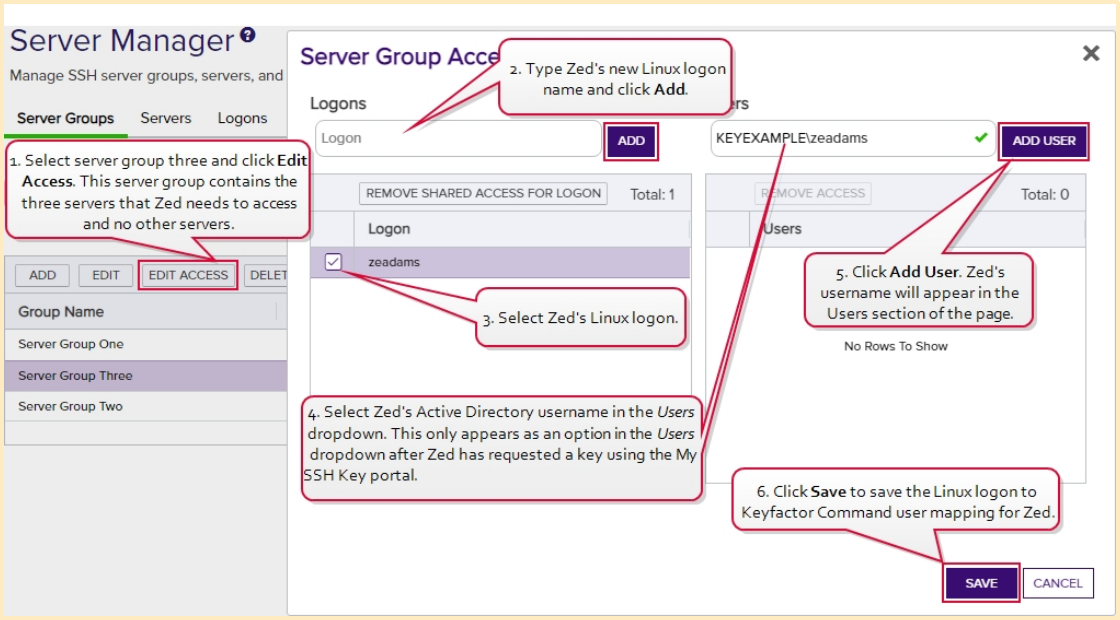


Figure 295: Create Logons and Mappings for Zed

Note: The three servers that Zed needs access to are in a server group so the administrator can create Zed's logons and map his key using the Access Management option on the Server Group page. If the servers were in different server groups or the server group contained servers to which Zed should not have access, the administrator would need to create the logons and mappings separately for each server using the Access Management option on the Servers page (see Editing Access to an SSH Server on page 561).

5. Waits for the logons to be created on the three servers and the public key to be published to them. The time that this takes depends on the frequency of the server group synchronization schedule (see Adding Server Groups on page 543).

6. Instructs Zed to configure PuTTY to use the private key for authentication, providing also connection information for the three Linux servers to which he will be connecting.

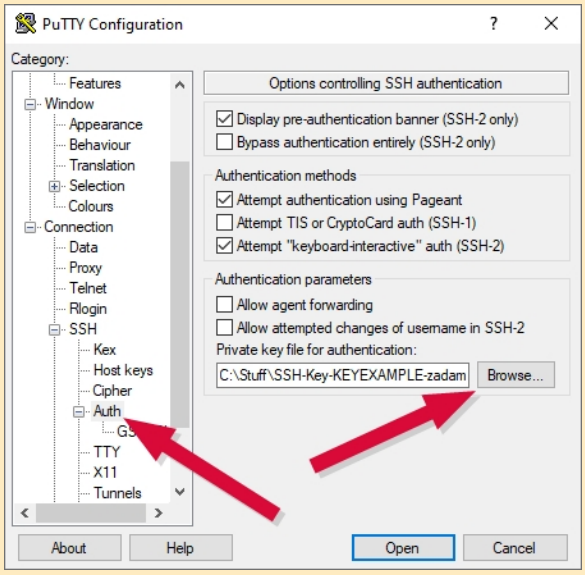


Figure 296: Configure PuTTY to Use Zed's Private Key

7. Confirms that Zed is able to successfully connect using secured SSH to each of the three servers.

This information is included for a key:

Creation Date

The date on which the SSH key pair was generated.

Stale Date

The date on which the SSH key pair is considered to have reached the end of its lifetime. By default, the lifetime of an SSH key pair is 365 days (see Application Settings: SSH Tab on page 604).

Key Type

A number of cryptographic algorithms can be used to generate SSH keys. Keyfactor Command supports RSA, Ed25519, and ECDSA. RSA keys are more universally supported, and this is the default key type when generating a new key.

Key Length

The key length available when generating a new key depends on the key type selected. Keyfactor Command supports 256 bits for Ed25519 and ECDSA and 2048 or 4096 bits for RSA. The default key length is 2048.

Email

The email address of the user requesting the key. This email address is used to alert the user when the key pair is approaching the end of its lifetime (see Key Rotation Alerts on page 193).

Comment

The user-defined descriptive comment, if any, on the key. Although entry of an email address in the comment field of an SSH key is traditional, this is not a required format. The comment may can contain any characters supported for string fields, including spaces and most punctuation marks.

SHA256 Fingerprint

The fingerprint of the public key. Each SSH public key has a single cryptographic fingerprint that can be used to uniquely identify the key.

Public Key

The public key of the key pair.

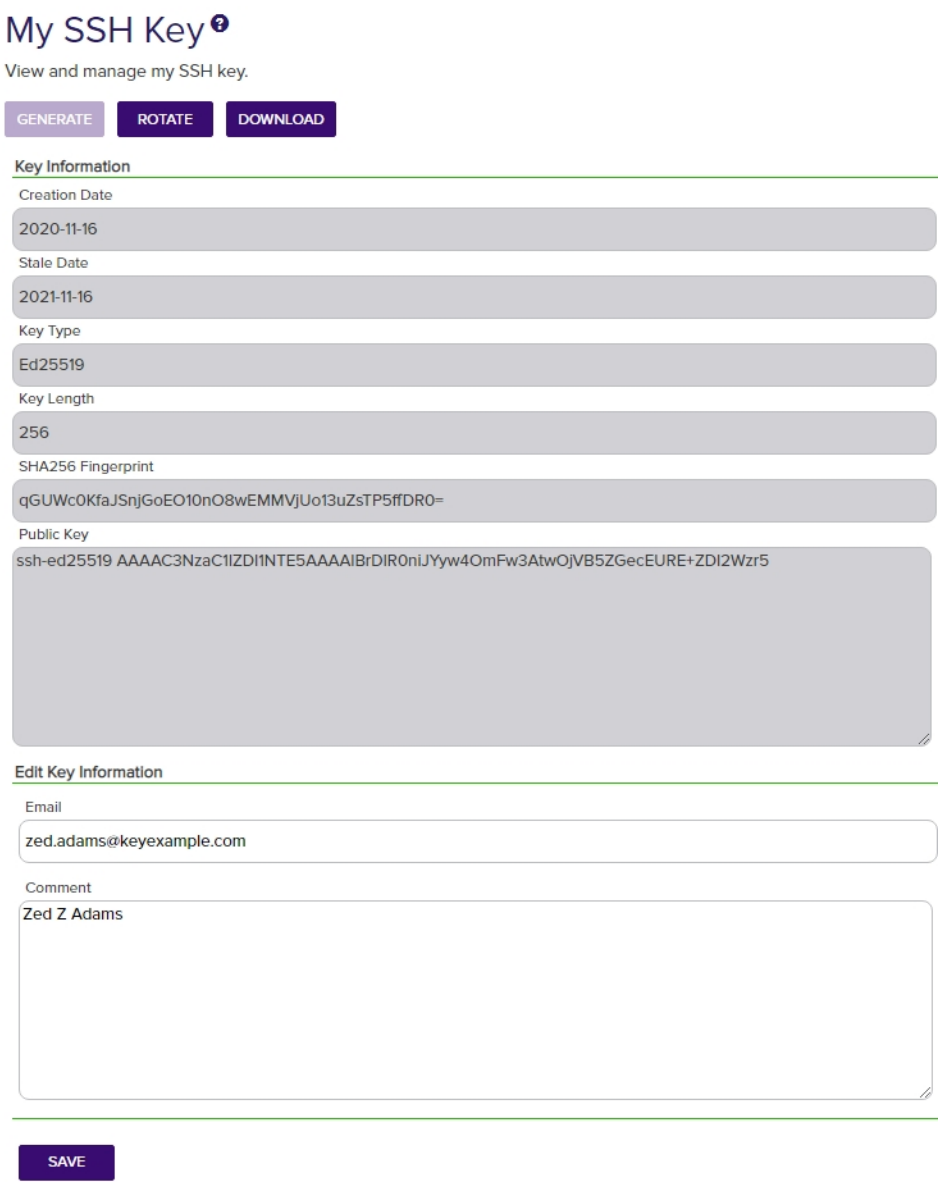


Figure 297: Key Information for an SSH User Key

Tip: Click the help icon (?) next to the page title to open the embedded web copy of the *Keyfactor Command Documentation Suite* to this section.
You can also find the help icon at the top of the page next to the **Log Out** button. From here you can choose to open either the *Keyfactor Command Documentation Suite* at the home page or the *Keyfactor API Endpoint Utility*.

Generating a New Key

> **Important:** A given user can only have one SSH key pair in Keyfactor Command. Generating a new key pair removes the existing key pair from Keyfactor Command, if one exists. This means any mappings between the Keyfactor user and Linux logon accounts will be updated with the public key from the new key pair. This essentially invalidates the user's previous private key for servers managed with the Keyfactor Bash Orchestrator. Although the Generate button is not active for users who already have a key pair, the Rotate button will also remove the existing key pair.

To generate a new SSH key pair:

1. In the Management Portal, browse to *SSH > My SSH Key*.
2. On the My SSH Key page, click **Generate**.

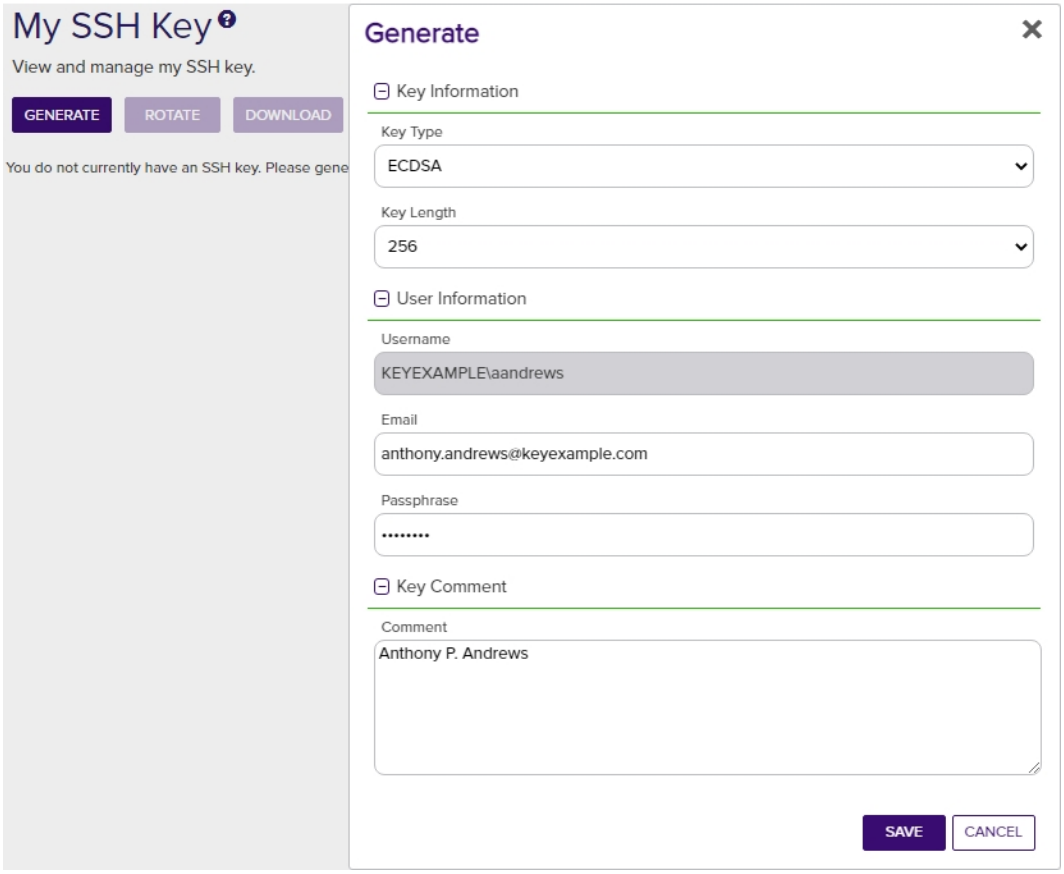


Figure 298: Generate an SSH Key Pair

3. In the Key Information section of the Generate dialog, select a **Key Type** in the dropdown (see Key Type on page 515).

4. In the Key Information section, select a **Key Length** in the dropdown (see Key Length on page 515). The available key lengths will vary depending upon the option selected in the Key Type dropdown.

5. In the User Information section, confirm that the displayed **Username** matches the Active Directory user name you wish to associate with your key. This field defaults to your logged in username and cannot be edited.

6. In the User Information section, enter an **Email** address. This address is used for key rotation alerts (see Key Rotation Alerts on page 193). This field is required.

7. In the User Information section, enter a **Passphrase** to encrypt the downloaded copy of the private key of the key pair. You will need to provide this passphrase again when you use the private key to connect via SSH. By default, the minimum password length is 12 characters (see the *SSH Key Password* setting in Application Settings: SSH Tab on page 604). This field is required.

   Tip: Your private key downloads immediately at the conclusion of the generation process, encrypted with this passphrase. You may later download the private key again from this same page and encrypt it with a different passphrase, if desired.

8. In the Key Comment section, enter a **Comment** to include with the key. This field is optional.

   Tip: Although entry of an email address in the comment field of an SSH key is traditional, this is not a required format. The comment may contain any characters supported for string fields, including spaces and most punctuation marks.

9. Click **Save** to create the key pair.

Tip: Once the key pair is generated, the user needs to download the private key as an encrypted file and store it locally and an administrator needs to use Keyfactor Command to associate the user's Keyfactor user account with his or her Linux logon account on the target server that the user wishes to access via SSH. After this is complete and the orchestrator has published the user's public key to the target server, the user may connect via SSH to the target server using the new private key for authentication. For more information, see SSH on page 507.

Rotating a Key

The rotate key option is used to replace an existing key that is approaching the end of its life or has been compromised. If key rotation alerts have been configured in the environment (see Key Rotation Alerts on page 193), the user will receive an email when the key is approaching the end if its lifetime to instruct the user to rotate his or her keys.

Important: A given user can only have one SSH key pair in Keyfactor Command. Generating a new key pair with the rotate option removes the existing key pair from Keyfactor Command. This means any mappings between the Keyfactor user and Linux logon accounts will be updated with the public key from the new key pair. This essentially invalidates the user's previous private key for servers managed with the Keyfactor Bash Orchestrator.

The rotate dialog defaults to all the existing settings of the user's current key. At its simplest, users may choose to accept all the defaults, enter a passphrase to encrypt the downloaded private key and click save to generate the new key pair.

To rotate an SSH key pair:

1. In the Management Portal, browse to *SSH > My SSH Key*.
2. On the My SSH Key page, click **Rotate**.

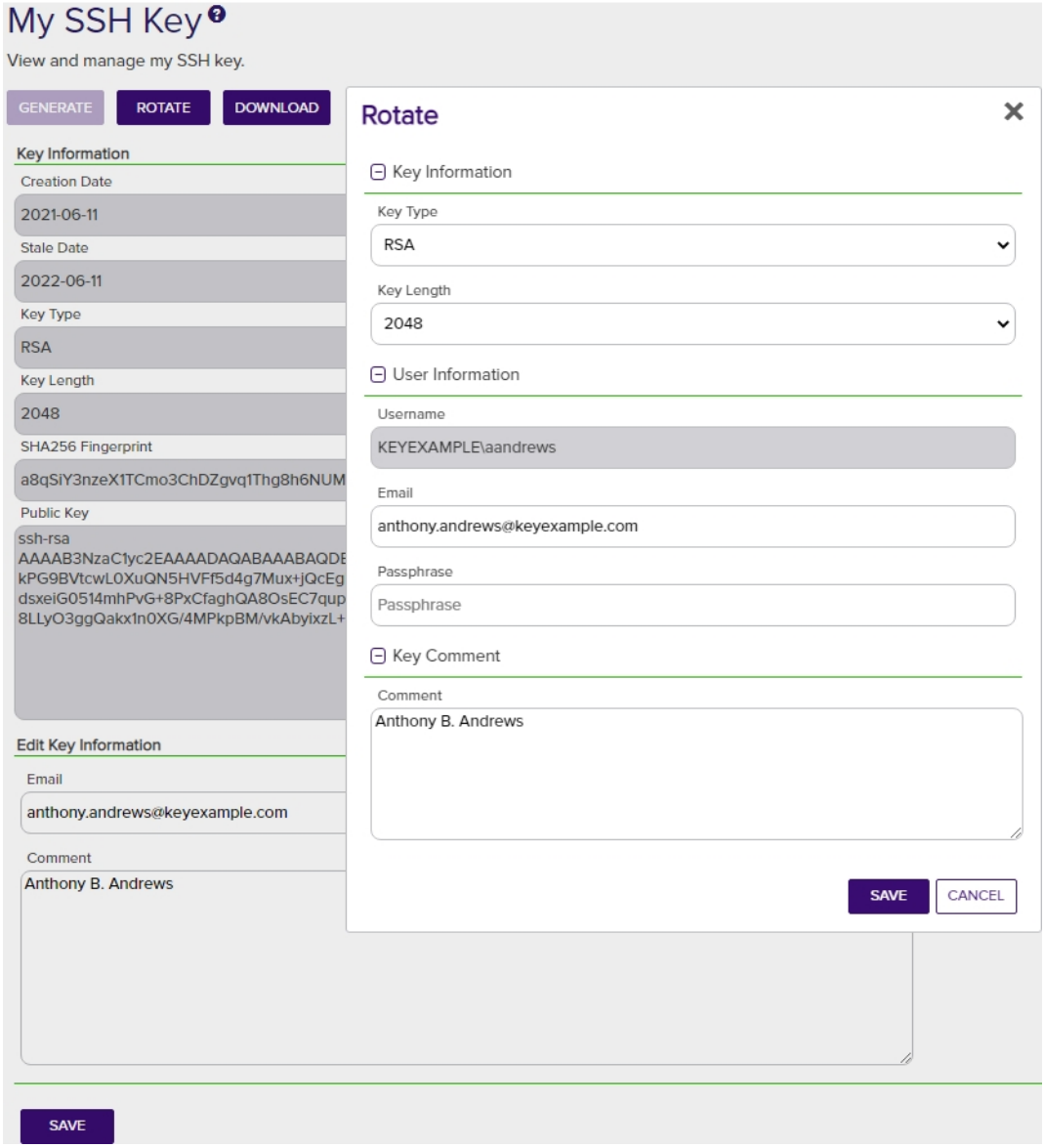


Figure 299: Rotate an SSH Key Pair

3. In the Key Information section of the Rotate dialog, modify the existing **Key Type** in the drop-down, if desired (see Key Type on page 515).

4. In the Key Information section, modify the existing **Key Length** in the dropdown, if desired (see Key Length on page 515). The available key lengths will vary depending upon the option select in the Key Type dropdown.

5. In the User Information section, confirm that the displayed **Username** matches the Active Directory user name you wish to associate with your key. This field defaults to your logged in username and cannot be edited.

6. In the User Information section, modify the existing **Email** address, if desired. This address is used for key rotation alerts (see Key Rotation Alerts on page 193). This field is required.

7. In the User Information section, enter a **Passphrase** to encrypt the downloaded copy of the private key of the key pair. You will need to provide this passphrase again when you use the private key to connect via SSH. By default, the minimum password length is 12 characters (see the *SSH Key Password* setting in Application Settings: SSH Tab on page 604). This field is required.

8. In the Key Comment section, modify the existing **Comment** to include with the key, if desired. This field is optional.

   Tip: Although entry of an email address in the comment field of an SSH key is traditional, this is not a required format. The comment may can contain any characters supported for string fields, including spaces and most punctuation marks.

9. Click **Save** to create the new key pair.

Tip: Once the key pair is generated, the user needs to download the private key as an encrypted file and store it locally and an administrator needs to use Keyfactor Command to associate the user's Keyfactor user account with his or her Linux logon account on the target server that the user wishes to access via SSH. After this is complete and the orchestrator has published the user's public key to the target server, the user may connect via SSH to the target server using the new private key for authentication. For more information, see SSH on page 507.

Downloading a Key

After generating a key pair, you need to download the private key on the machine from which you will be making SSH connections. Although the private key is encrypted, for best security practice it should not be moved around from machine to machine.

The key downloads in the proprietary OpenSSH private key format, encrypted by a user-defined password.

Only the private key can be downloaded with the download option, though the public key is displayed on the screen and may be copied and pasted to a file, if desired.

To download the private key:

1. In the Management Portal, browse to *SSH > My SSH Key*.

2. On the My SSH Key page, confirm that you have been issued a key pair and click **Download**.

3. In the Download dialog, enter a passphrase that will be used to encrypt the private key. By default, the minimum password length is 12 characters (see the *SSH Key Password* setting in Application Settings: SSH Tab on page 604). This field is required.

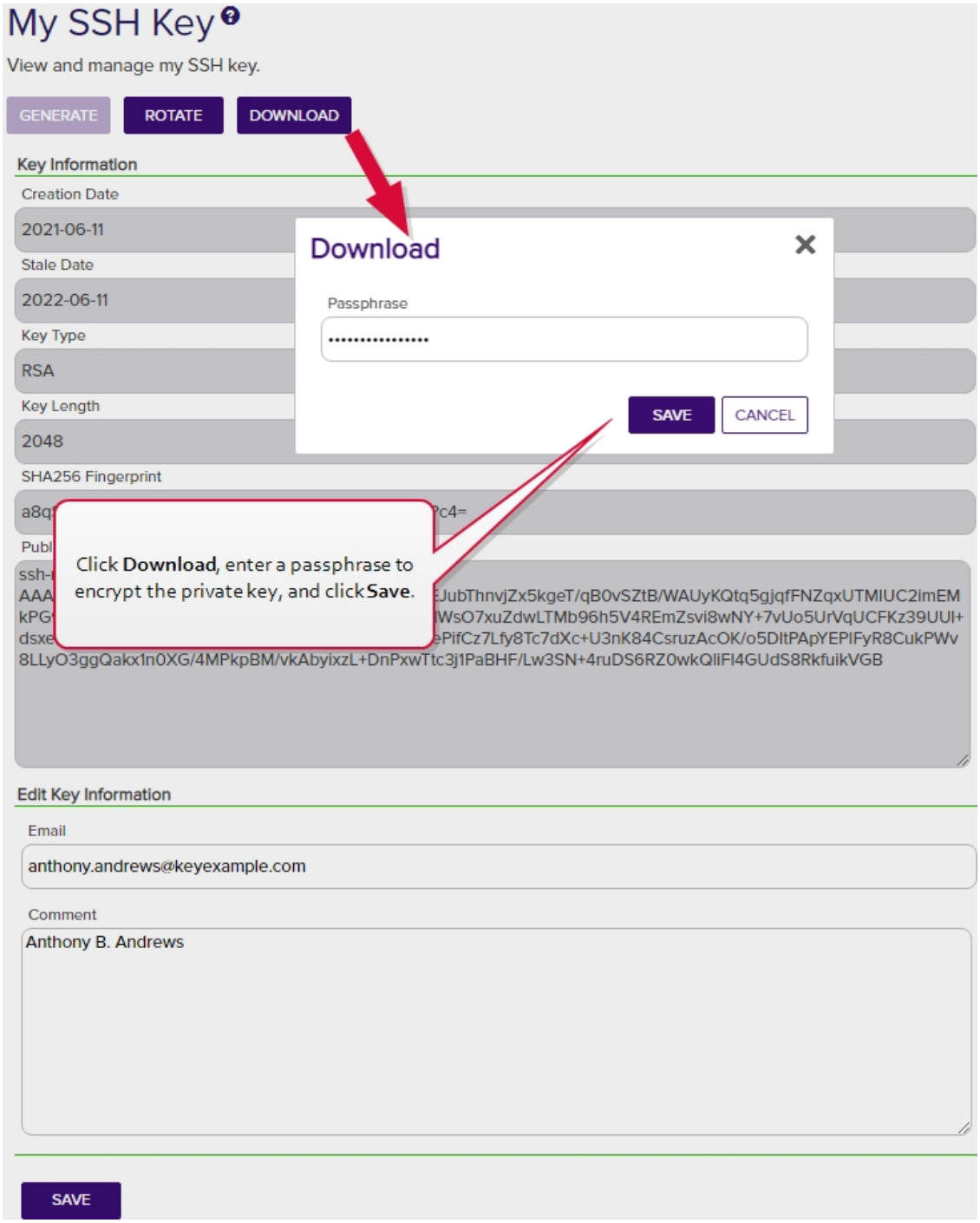


Figure 300: Add a Password to Encrypt the Downloaded Private Key

4. Click **Download** to save the file to your local machine.

By default, the file has the following name, where *DOMAIN* is your Active Directory domain name and *username* is the Active Directory user name of the user logged into the Keyfactor Command Management Portal:

SSH-Key-*DOMAIN*-*username*.identity

Editing Key Information

Once you have generated an SSH key pair, most things about the key pair are fixed and cannot be changed. However, two pieces of key information can be changed for an existing key pair—the email address to which alerts about the key should be directed and the comment associated with the public key.

To modify the email address or key comment:

1. In the Management Portal, browse to *SSH > My SSH Key*.
2. On the My SSH Key page, update the fields in the Edit Key Information section as needed and click **Save**.

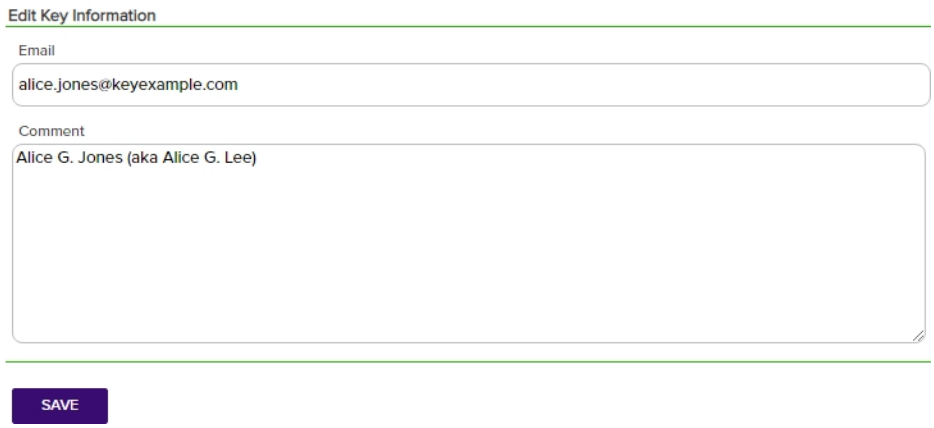


Figure 301: Edit SSH User Key Information

Changes made to the key comment will be published to any associated servers during the next synchronization cycle.

2.1.10.2 Service Account Keys

On the Service Account Keys page, an administrator can view and download existing keys issued for service accounts and generate new key pairs.

Example: An administrator wants to generate a new SSH key pair for the green chicken application, which is a Linux-based log aggregation application. The application uses secure

SSH to communicate internally between the server collecting the logs and the servers from which the logs are being collected. All the servers are controlled by the Keyfactor Bash Orchestrator. The servers are set to both inventory and publish policy. To accomplish this, the administrator:

1. Uses the Keyfactor Command Management Portal to create a new key pair (see Creating a Service Account Key on page 527). She enters the following information in the form:
    - **Key Type**: Ed25519
    - **Key Length**: 256
    - **Server Group**: Server Group One

      The server group to which the Linux servers belong that the public key will be distributed to.
    - **Client Hostname**: appsrvr75

      The Linux server on which the private key of the SSH key pair will be download. This does not need to be a server added for management in Keyfactor Command and is a field for reference only.
    - **Username**: svc_greenchicken

      The service account name the application uses. This does not need to match the Linux logon name the application uses. This username together with the client hostname make the full user name for the service account key within Keyfactor Command svc_greenchicken@appsrvr75.
    - **Email**: pkiadmins@keyexample.com

      The group responsible for rotating the key when it reaches the end of its lifetime. This group will receive email alerts when the key is becoming stale.
    - **Passphrase**: A complex password used to secure the private key.

      She needs to record the passphrase because this will be needed by application to access the private key.
    - **Comment**: Green Chicken Service

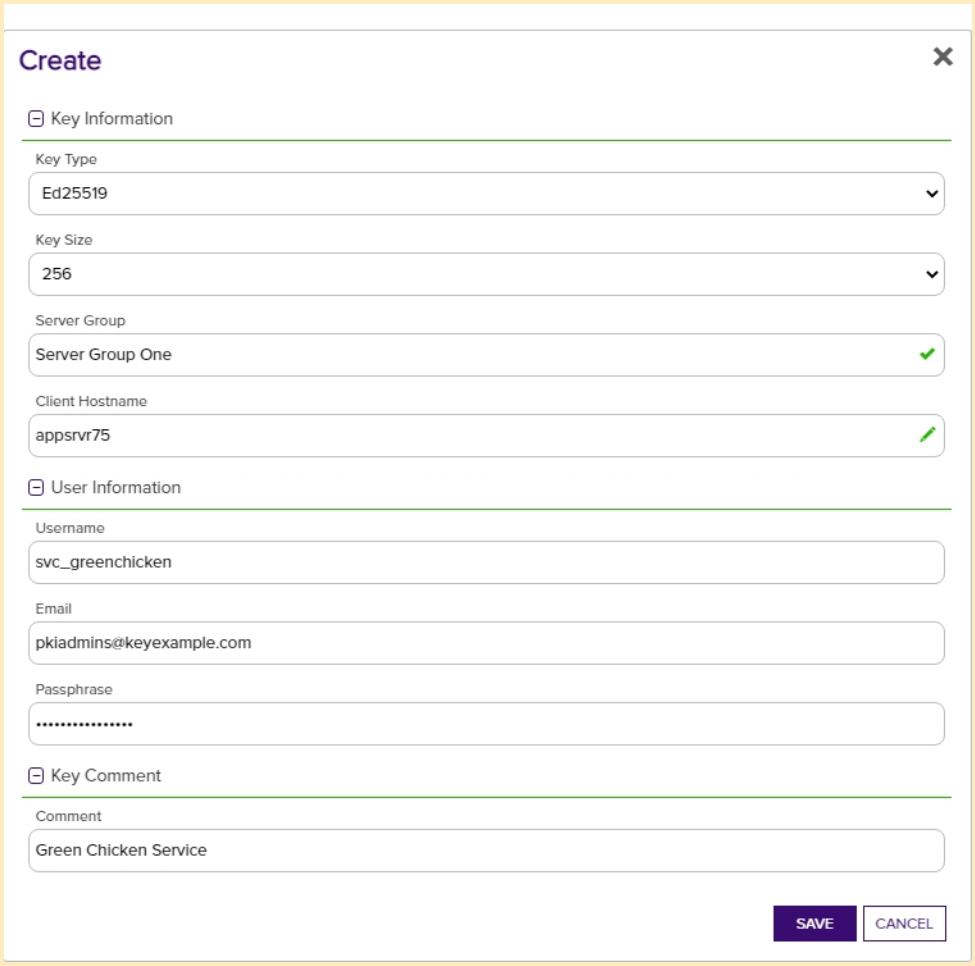


Figure 302: Acquire a New Service Account Key

2. Downloads the SSH private key on the server doing the log collection, from which the SSH connections will be made to collect logs.

3. Uses the Management Portal to map the new public key for the full service account user name (svc_greenchicken@appsrvr75) to the Linux logons for the service on the servers from which the logs will be collected (see Editing Access to an SSH Server Group on page 545).

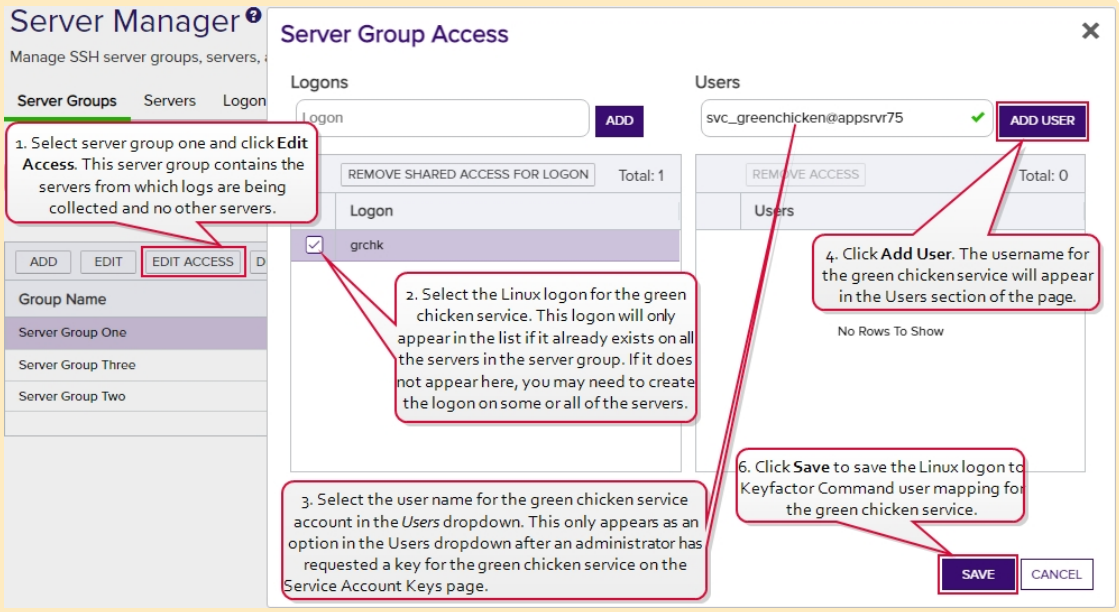


Figure 303: Map Service Account Public Key to Logon

Note: The servers that the logs will be collected from are organized into a server group so the administrator can create logons and map the service account key using the Access Management option on the Server Group page. If the servers were in different server groups or the server group contained servers which should not be updated with logons and keys for the green chicken service, the administrator would need to create the logons and mappings separately for each server using the Access Management option on the Servers page (see Editing Access to an SSH Server on page 561).

4. Waits for the public key to be published to the servers. The time that this takes depends on the frequency of the server group synchronization schedule (see Adding Server Groups on page 543).
5. Confirms that the service is able to successfully connect using secured SSH.

Tip: Click the help icon (?) next to the page title to open the embedded web copy of the *Keyfactor Command Documentation Suite* to this section.
You can also find the help icon at the top of the page next to the **Log Out** button. From here you can choose to open either the *Keyfactor Command Documentation Suite* at the home page or the *Keyfactor API Endpoint Utility*.

Creating a Service Account Key

To create a new service account key:

1. In the Management Portal, browse to *SSH > Service Account Keys*.
2. On the Service Account Keys page, click **Create**.

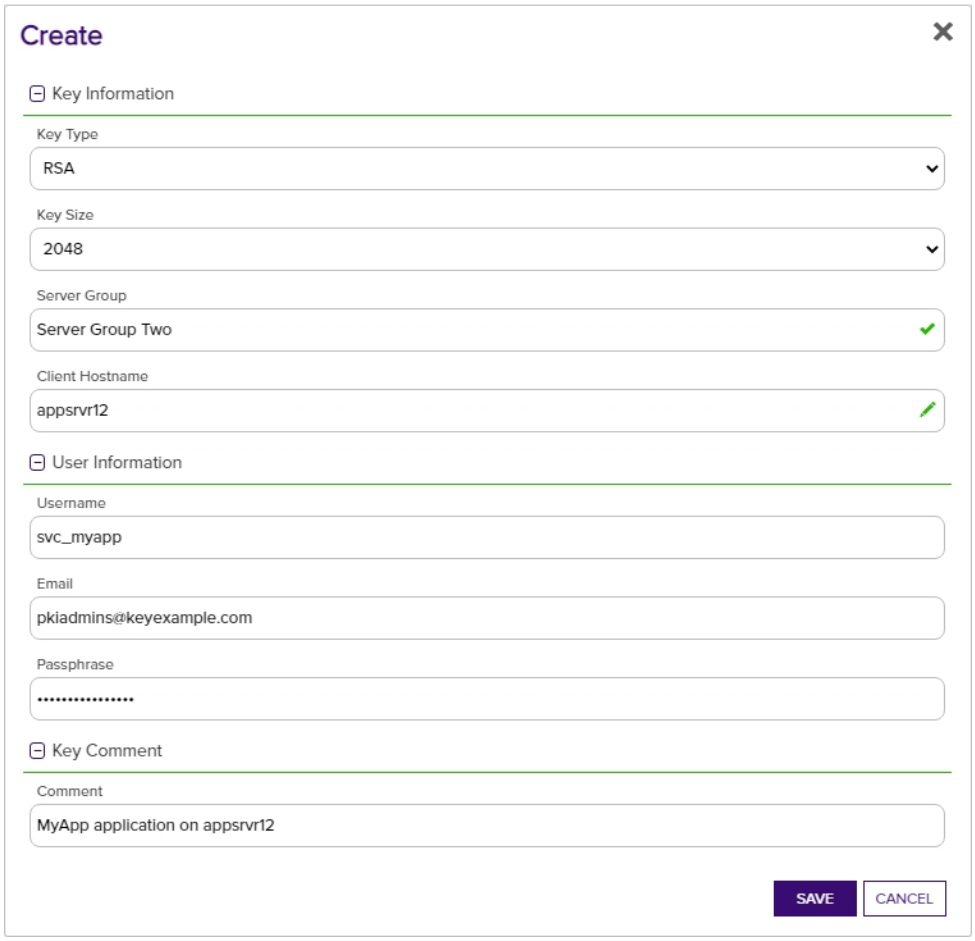


Figure 304: Add a Service Account Key

3. In the Key Information section of the Create dialog, select a **Key Type** in the dropdown (see Key Type on page 515).
4. In the Key Information section, select a **Key Length** in the dropdown (see Key Length on page 515). The available key lengths will vary depending upon the option select in the Key Type dropdown.
5. In the Key Information section, select a **Server Group** in the dropdown (see SSH Server Groups on page 542). The server group is used to control who has access in the Management Portal to the service account key. It does not limit where the key can be published. This field is required.
6. In the Key Information section, enter a **Client Hostname** reference for the service account key. This field is used for reference only and does not need to match an actual client hostname. It is

used when building the full user name of the service account key for mapping to Linux logons for publishing to Linux servers (e.g. username@client_hostname). The naming convention is to enter the hostname of the server on which the application that will use the private key resides (e.g. appsrvr12), but you can put anything you like in this field (e.g. cheesetoast). This field is required.

7. In the User Information section of the page, enter the **Username** of the service account that will be using the key to connect to the target server (e.g. svc_myapp). This username will be combined with the Client Hostname to build the full user name of the service account key for mapping to Linux logons (e.g. svc_myapp@appsrvr12). You will need to know this full user name when creating the mappings to publish the public key to the target servers (see Editing Access to an SSH Server Group on page 545, Editing Access to an SSH Server on page 561, Adding Logons on page 567, or Editing or Deleting a Logon on page 570). This field is required.

8. In the User Information section of the page, enter the **Email** address of the administrator or group of administrators responsible for managing the key. This is the address to which key rotation alerts for this key will be directed (see Key Rotation Alerts on page 193). This field is required.

9. In the User Information section, enter a **Passphrase** to encrypt the downloaded copy of the private key of the key pair. The service that uses the private key will need to be able to provide it when connecting via SSH. By default, the minimum password length is 12 characters (see the *SSH Key Password* setting in Application Settings: SSH Tab on page 604). This field is required.

   Tip: The private key downloads immediately at the conclusion of the creation process, encrypted with this passphrase. You may later download the private key again from this same page and encrypt it with a different passphrase, if desired.

10. In the Key Comment section, enter a **Comment** to include with the key. This field is optional.

    Tip: Although entry of an email address in the comment field of an SSH key is traditional, this is not a required format. The comment may contain any characters supported for string fields, including spaces and most punctuation marks.

11. Click **Save** to save the new service account key.

    Tip: Once the key pair is generated, an administrator needs to download the private key as an encrypted file and store it locally on the machine from which the service will make SSH connections using the private key. Additionally, an administrator needs to use Keyfactor Command to map the full user name built from the username and client hostname entered when generating the service account key pair (e.g. svc_myapp@appsrvr12) to the Linux logon account that the service account will operate as when logging in via SSH on the target server(s) where the public key needs to reside (see Editing Access to an SSH Server Group on page 545, Editing Access to an SSH Server on page 561, Adding Logons on page 567, or Editing or Deleting a Logon on page 570). After this is complete and the orchestrator has published the public key to the target

server(s), the service may connect via SSH to the target server(s) using the new private key for authentication. For more information, see SSH on page 507.

Editing Service Account Key Information

Once you have generated an SSH key pair, most things about the key pair are fixed and cannot be changed. However, two pieces of key information can be changed for an existing key pair—the email address to which alerts about the key should be directed and the comment associated with the public key.

Tip: Only service account keys belonging to server groups that the current user is the owner on appear in the grid unless the user holds the *SSH Enterprise Admin* role.

To modify the email address or key comment:

1. In the Management Portal, browse to *SSH* > *Service Account Keys*.
2. On the Service Account Keys page, double-click the key for the desired service account in the grid, highlight the row in the grid and click **Edit** at the top of the grid, or right-click the key in the grid and choose **Edit** from the right-click menu.
3. In the Edit Key dialog, update the **Email** and **Comment** fields as needed and click **Save**.

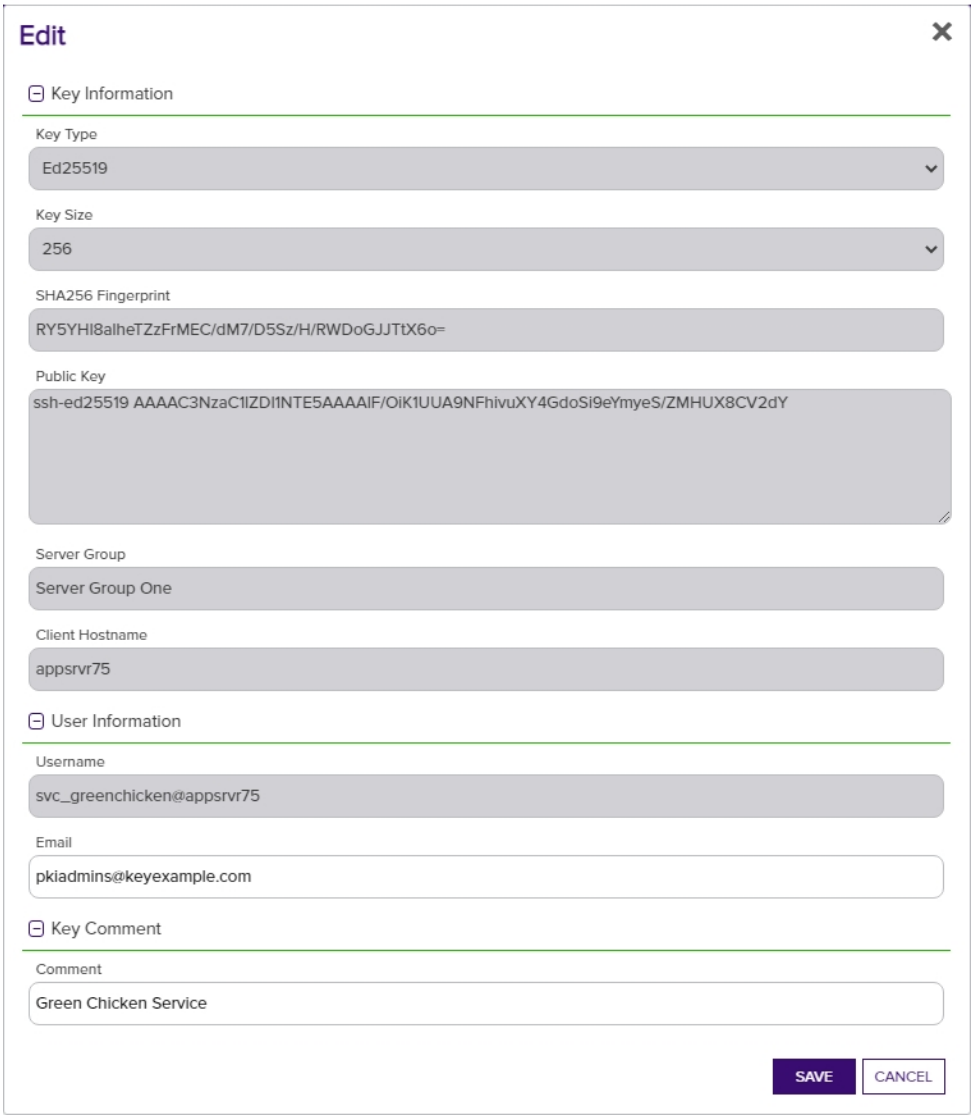


Figure 305: Edit SSH Service Account Key Information

Changes made to the key comment will be published to any mapped logons on associated servers during the next synchronization cycle.

Rotating a Service Account Key

The rotate key option is used to replace an existing key that is approaching the end of its life or has been compromised. If key rotation alerts have been configured in the environment (see Key Rotation Alerts on page 193), the administrator responsible for managing the service account key will receive an email when the key is approaching the end if its lifetime to instruct the him or her to rotate the service account key.

Important: A given service account can only have one SSH key pair in Keyfactor Command. Generating a new key pair with the rotate option removes the existing key pair from Keyfactor Command. This means any mappings between the Keyfactor service account and Linux logon accounts will be updated with the public key from the new key pair. This essentially invalidates the service account's previous private key for servers managed with the Keyfactor Bash Orchestrator.

The rotate dialog defaults to all the existing settings of the service account's current key. At its simplest, the administrator may choose to accept all the defaults, enter a passphrase to encrypt the downloaded private key and click save to generate the new key pair.

To rotate a service account key pair:

1. In the Management Portal, browse to *SSH > Service Account Keys*.
2. On the Service Account Keys page, click **Rotate**.

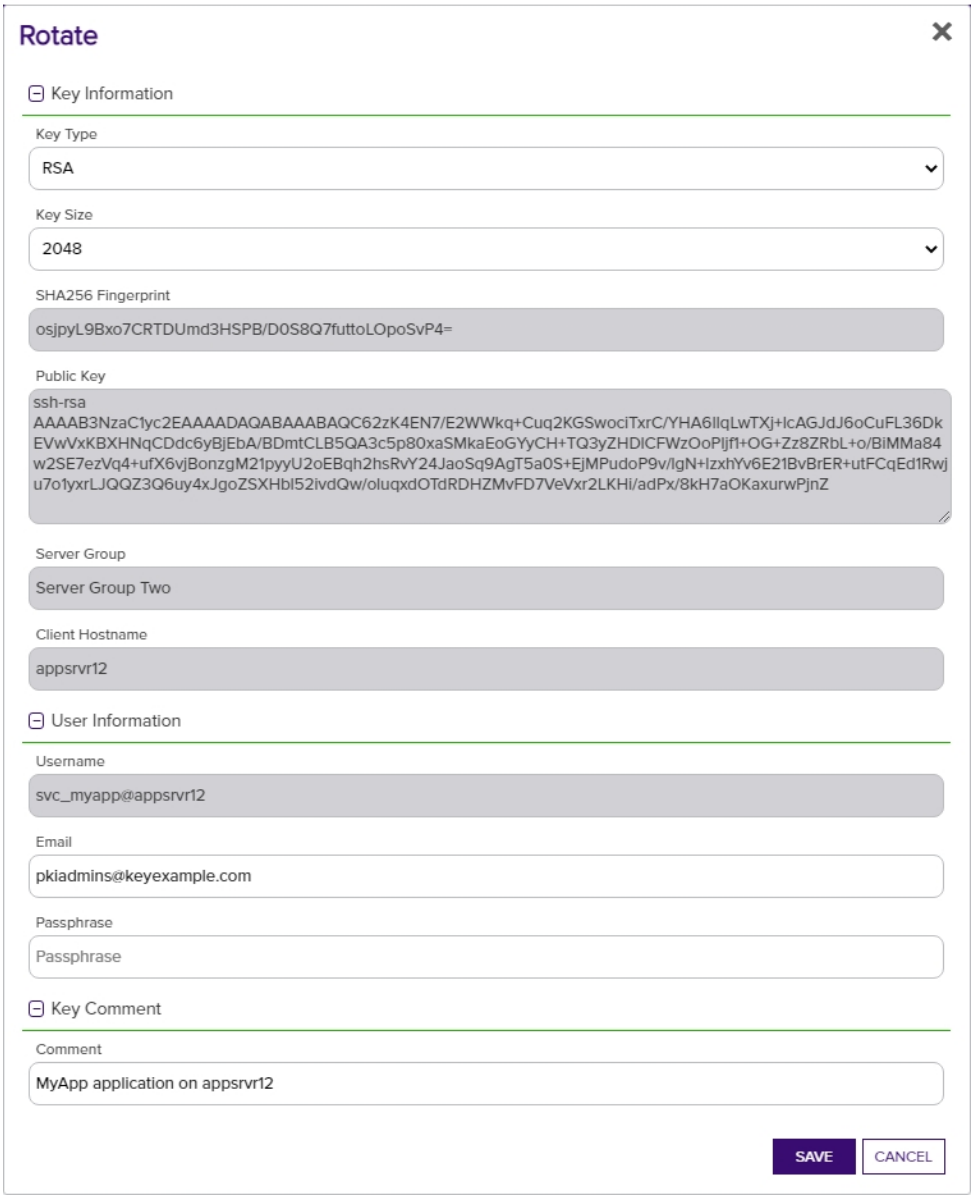


Figure 306: Rotate an SSH Key Pair

3. In the Key Information section of the Rotate dialog, modify the existing **Key Type** in the dropdown, if desired (see Key Type on page 515).

4. In the Key Information section, modify the existing **Key Length** in the dropdown, if desired (see Key Length on page 515). The available key lengths will vary depending upon the option select in the Key Type dropdown.

5. In the User Information section, modify the existing **Email** address, if desired. This address is used for key rotation alerts (see Key Rotation Alerts on page 193). This field is required.

6. In the User Information section, enter a **Passphrase** to encrypt the downloaded copy of the private key of the key pair. You will need to provide this passphrase again when you use the private key to connect via SSH. By default, the minimum password length is 12 characters (see the *SSH Key Password* setting in Application Settings: SSH Tab on page 604). This field is required.

7. In the Key Comment section, modify the existing **Comment** to include with the key, if desired. This field is optional.

   Tip: Although entry of an email address in the comment field of an SSH key is traditional, this is not a required format. The comment may can contain any characters supported for string fields, including spaces and most punctuation marks.

8. Click **Save** to create the new key pair.

Tip: Once the key pair is generated, an administrator needs to download the private key as an encrypted file and store it locally on the machine from which the service will make SSH connections using the private key. Additionally, an administrator needs to use Keyfactor Command to map the full user name built from the username and client hostname entered when generating the service account key pair (e.g. svc_myapp@appsrvr12) to the Linux logon account that the service account will operate as when logging in via SSH on the target server(s) where the public key needs to reside (see Editing Access to an SSH Server Group on page 545, Editing Access to an SSH Server on page 561, Adding Logons on page 567, or Editing or Deleting a Logon on page 570). After this is complete and the orchestrator has published the public key to the target server(s), the service may connect via SSH to the target server(s) using the new private key for authentication. For more information, see SSH on page 507.

Deleting a Service Account Key

To delete a service account key, highlight the row in the service account keys grid and click **Delete** at the top of the grid or right-click the key in the grid and choose **Delete** from the right-click menu.

Tip: Only service account keys belonging to server groups that the current user is the owner on appear in the grid unless the user holds the *SSH Enterprise Admin* role.

Downloading a Service Account Key

After generating a key pair, you need to download the private key on the machine from which you will be making SSH connections. Although the private key is encrypted, for best security practice it should not be moved around from machine to machine.

The key downloads in the proprietary OpenSSH private key format, encrypted by a user-defined password.

Only the private key can be downloaded with the download option, though the public key is displayed in the edit dialog and may be copied and pasted to a file, if desired.

Tip: Only service account keys belonging to server groups that the current user is the owner on appear in the grid unless the user holds the *SSH Enterprise Admin* role.

To download the private key:

1. In the Management Portal, browse to *SSH > Service Account Keys*.
2. On the Service Account Keys page, locate the key for the desired service account and click **Download**.

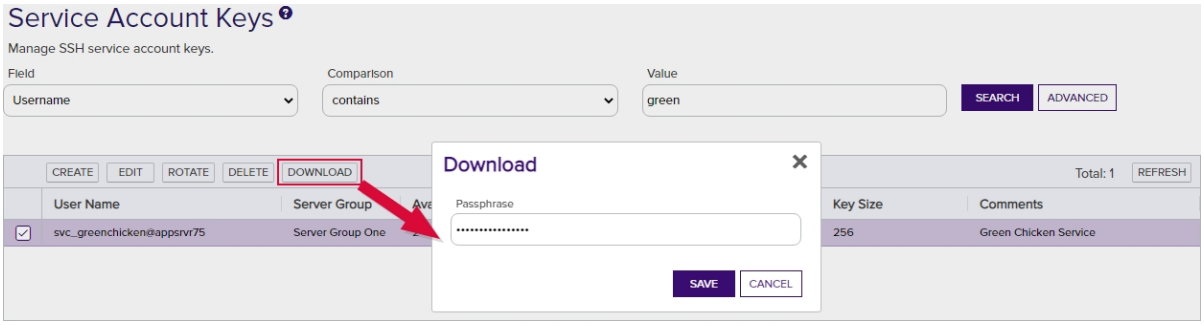


Figure 307: Download a Service Account Private Key

3. In the Download dialog, enter a passphrase that will be used to encrypt the private key. By default, the minimum password length is 12 characters (see the *SSH Key Password* setting in Application Settings: SSH Tab on page 604). This field is required.
4. Click **Download** to save the file to the local machine.

   By default, the file has the following name:

   SSH-Key-Service-Account.identity

Using the Service Account Key Search

The search function allows you to query the database for information. The same query structure is used in multiple locations within the Keyfactor Command Management Portal.

When you first open the page, you will see the simple search option. To execute a search, select the field and comparison operators in the dropdowns and type something on which to search in the value field (if applicable). If you select an *is null* or *is not null* comparison operator, the value field will be grayed out. Click the **Search** button to execute the query.

Tip: Only service account keys belonging to server groups that the current user is the owner on appear in the grid unless the user holds the *SSH Enterprise Admin* role.

Each query consists of three parts:

Query Field

The available fields for querying vary depending on the area of the Management Portal in which the search is used. On this page, the queries can be done on the following built-in fields:

Server Group Name

Complete or partial matches with the name of the server group that the service account key is associated with.

Username

Complete or partial matches with the username of the service account key. The username is made up of the username and client hostname entered when the service account key was created (e.g. myapp@appsrvr75).

Creation Date

The date on which the key was created.

Key Type

Whether the key is RSA, ECC, or Ed25519

Key Length

The key size of the key.

Comments

Complete or partial matches with the user-defined comments on the key.

Comparison Operator

The query comparison operators vary depending on the type of field selected and the specific properties of the field. The list below shows the dropdown list comparison operators, as well as the equivalent query language syntax (in parentheses).

Most string fields (the vast majority of the built-in fields) support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Contains (-contains)
- Does not contain (-notcontains)
- Starts with (-startswith)
- Ends with (-endswith)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Most date and integer fields support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Is less than (-lt)
- Is less than or equal to (-le)
- Is greater than (-gt)
- Is greater than or equal to (-ge)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Most Boolean (true/false) fields support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Comparison Value

The value you enter for comparison must match the field type. For example, integer fields only support numerical values. String fields support all alphanumeric characters. Boolean fields only support True or False. The value field is not case sensitive. Date fields support only properly formatted dates and will initially display as mm/dd/yyyy. You can choose to populate the date field by:

- Clicking in a date Value field to open a pop-up calendar to select a date that will populate the field.
- Clicking in a segment of the date format (i.e., mm/dd/yyyy) and entering a value. As you continue to type in any one segment, the cursor will keep moving onto the next segment.

The results that match your search criteria will be displayed in the results grid below the search selection options.

Advanced Searches

On any search page you can click **Advanced** to the right of the Search button to display the advanced search options. Click **Simple** to close the advanced search options again.

Multiple Criteria

Using the advanced search options, you can build a query based on multiple criteria using AND/OR logic. As with a simple search, you select a field and comparison operator in the drop-downs and then enter a comparison value, if applicable. Click **Insert** to add the search criteria to the query field below the selection fields. Use the selection fields to build multiple search criteria. Each time you click the insert button, an AND is added between the previous search criteria and the newly added one. You can change the AND to an OR if desired. You can use parentheses around portions of the query along with AND/OR to change the query meaning.

For example, for certificate searches:

```
(CN -contains "appsrvr" AND IssuedDate -ge "01/01/2022") OR (CN -contains "appsrvr" AND
TemplateShortName -contains "web")
```

This query will return all the certificates issued on or after January 1, 2022 with the string appsrvr in the CN and also all certificates issued at any time with the string appsrvr in the CN using a template referencing web. When you have entered all the desired search criteria, click **Search** to execute the query. If you wish to clear the query field and start over, click the **Clear** button.

2.1.10.3 Unmanaged SSH Keys

When your SSH servers are configured in inventory only mode doing discovery, keys discovered on the servers are considered unmanaged and are displayed on the Unmanaged Keys page.

On this page you can review the discovered keys to get a sense of what's out there. You can view the keys, key comments, fingerprint, type and length. Once you switch your servers to inventory and publish policy mode, deleting a key from the unmanaged keys page will also delete the key from the server(s) in this mode on which it is found.

Note: Deleting a key on this page when the associated server is still in inventory only mode will *not* delete the key on the target server. The next time the server is scanned, the key will re-appear in Keyfactor Command.

As you bring your servers under management, clean up old keys, and control installation of new keys, the number of keys appearing on the unmanaged keys page should begin to diminish. Eventually, the page should be empty when all your servers have been brought under management and all old keys have been replaced with new, managed, keys.

Tip: Click the help icon (?) next to the page title to open the embedded web copy of the *Keyfactor Command Documentation Suite* to this section.
You can also find the help icon at the top of the page next to the **Log Out** button. From here you can choose to open either the *Keyfactor Command Documentation Suite* at the home page or the *Keyfactor API Endpoint Utility*.

Viewing Unmanaged SSH Keys

To view details for an unmanaged public key, double-click the key, right-click the key and choose **View** from the right-click menu, or highlight the row in the unmanaged keys grid and click **View** at the top of the grid.

The view dialog includes two tabs:

- On the Basic tab, you can see information about the key itself, including the key length, fingerprint, comments associated with the key, and the public key itself.

Figure 308: View Basic Tab of an Unmanaged SSH Key

- On the Logon tab, you can view Linux logon names and servers mapped to the public key.

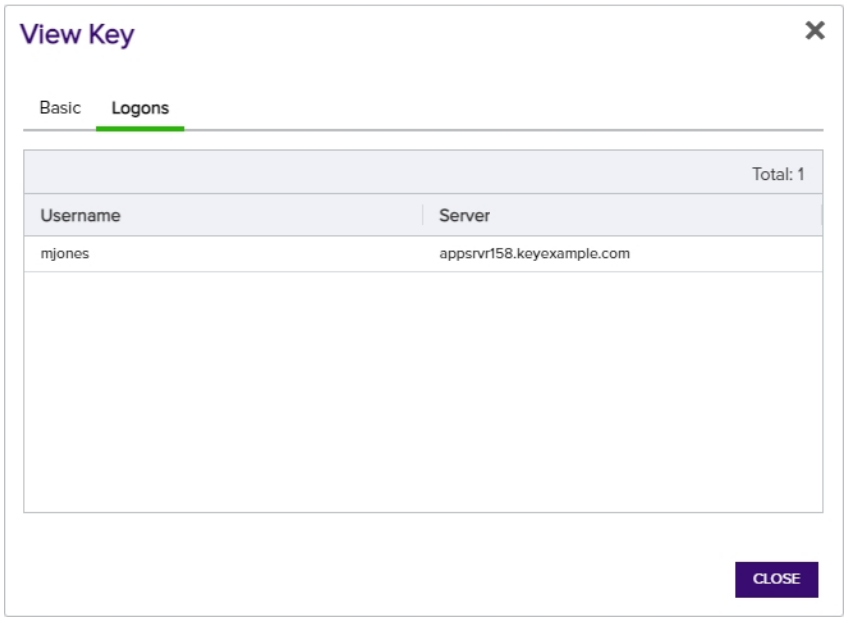


Figure 309: View Logon Tab of an Unmanaged SSH Key

Deleting an Unmanaged Key

To delete an unmanaged key, highlight the row in the unmanaged keys grid and click **Delete** at the top of the grid or right-click the key in the grid and choose **Delete** from the right-click menu.

Note: When you delete an unmanaged key that's found on any servers operating in inventory and publish policy mode (see SSH on page 507), the key will be removed from the target servers as well as from Keyfactor Command.

Using the Unmanaged Keys Search

The search function allows you to query the database for information. The same query structure is used in multiple locations within the Keyfactor Command Management Portal.

When you first open the page, you will see the simple search option. To execute a search, select the field and comparison operators in the dropdowns and type something on which to search in the value field (if applicable). If you select an *is null* or *is not null* comparison operator, the value field will be grayed out. Click the **Search** button to execute the query.

Each query consists of three parts:

Query Field

The available fields for querying vary depending on the area of the Management Portal in which the search is used. On this page, the queries can be done on the following built-in fields:

Discovered Date The date on which the key was discovered.	**Key Length** The key size of the key.
Key Comments Complete or partial matches with the user-defined comments on the key.	**Key Type** Whether the key is RSA, ECC, or Ed25519

Comparison Operator

The query comparison operators vary depending on the type of field selected and the specific properties of the field. The list below shows the dropdown list comparison operators, as well as the equivalent query language syntax (in parentheses).

Most string fields (the vast majority of the built-in fields) support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Contains (-contains)
- Does not contain (-notcontains)
- Starts with (-startswith)
- Ends with (-endswith)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Most date and integer fields support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Is less than (-lt)
- Is less than or equal to (-le)
- Is greater than (-gt)
- Is greater than or equal to (-ge)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Most Boolean (true/false) fields support:

- Is equal to (-eq)
- Is null (-eq NULL)

- Is not equal to (-ne)
- Is not null (-ne NULL)

Comparison Value

The value you enter for comparison must match the field type. For example, integer fields only support numerical values. String fields support all alphanumeric characters. Boolean fields only support True or False. The value field is not case sensitive. Date fields support only properly formatted dates and will initially display as mm/dd/yyyy. You can choose to populate the date field by:

- Clicking in a date Value field to open a pop-up calendar to select a date that will populate the field.
- Clicking in a segment of the date format (i.e., mm/dd/yyyy) and entering a value. As you continue to type in any one segment, the cursor will keep moving onto the next segment.

The results that match your search criteria will be displayed in the results grid below the search selection options.

Advanced Searches

On any search page you can click **Advanced** to the right of the Search button to display the advanced search options. Click **Simple** to close the advanced search options again.

Multiple Criteria

Using the advanced search options, you can build a query based on multiple criteria using AND/OR logic. As with a simple search, you select a field and comparison operator in the drop-downs and then enter a comparison value, if applicable. Click **Insert** to add the search criteria to the query field below the selection fields. Use the selection fields to build multiple search criteria. Each time you click the insert button, an AND is added between the previous search criteria and the newly added one. You can change the AND to an OR if desired. You can use parentheses around portions of the query along with AND/OR to change the query meaning.

For example, for certificate searches:

```
(CN -contains "appsrvr" AND IssuedDate -ge "01/01/2022") OR (CN -contains "appsrvr" AND
TemplateShortName -contains "web")
```

This query will return all the certificates issued on or after January 1, 2022 with the string appsrvr in the CN and also all certificates issued at any time with the string appsrvr in the CN using a template referencing web. When you have entered all the desired search criteria, click **Search** to execute the query. If you wish to clear the query field and start over, click the **Clear** button.

In addition to the options available in the query builder, three special values can be used in selected searches by typing them in directly:

- %TODAY%
  Use the TODAY special value in place of a specific date in date queries. This option supports math operations, so you can use TODAY-10 or TODAY+30. The built-in *Certificates Expiring in 7 Days* collection uses this special value (see Certificate Collection Manager on page 80).

- %ME%
  Use the ME special value in place of a specific domain\user name in queries that match a domain\user name. The built-in *My Certificates* collection uses this special value (see Certificate Collection Manager on page 80).
- %ME-AN%
  Use the ME-AN special value in place of a specific user name excluding the domain. This is beneficial in environments with multiple domains where there is a desire to query for a user's certificates even if they were requested across multiple domains.

Important: The special query options of %TODAY%, %ME%, and %ME-AN% are only supported in uppercase. Lowercase equivalents (e.g. %me%) cannot be substituted.

2.1.10.4 Server Manager

SSH key management is performed by one or more Keyfactor Bash Orchestrators controlling multiple targets. These are referred to collectively in the Management Portal as SSH servers. The SSH servers are collected together into one or more server groups. On the Server Manager page you first create one or more server groups to organize and set policies for your Linux SSH servers and then add an SSH server entry for each server you want to control with the orchestrator.

Scanning jobs are configured at the server group level. You can toggle between *inventory only* mode and *inventory and publish policy* mode at either the server group level or on an individual server basis, though if a server group is in *inventory and publish policy* mode (configured to *Enforce Publish Policy*), servers in this group cannot be in *inventory only* mode.

Scanning of targets cannot take place until they have been set up for control by the orchestrator (see *Install Remote Control Targets* in the *Keyfactor Orchestrators Installation and Configuration Guide*).

Tip: If you plan to scan and manage your orchestrator machine(s) in addition to any targets, you will need to add SSH server entries for these as though they were targets.

Once the scanning has begun, you can look at the Logons tab to see discovered logons from the targets and associated SSH public keys.

Tip: Click the help icon (?) next to the page title to open the embedded web copy of the *Keyfactor Command Documentation Suite* to this section.
You can also find the help icon at the top of the page next to the **Log Out** button. From here you can choose to open either the *Keyfactor Command Documentation Suite* at the home page or the *Keyfactor API Endpoint Utility*.

SSH Server Groups

On the Server Groups tab of the Server Manger page you create server groups that allow you to organize SSH servers and set synchronization schedules and management policies on a group level.

You must create at least one server group before you can add SSH servers into the Keyfactor Command Management Portal.

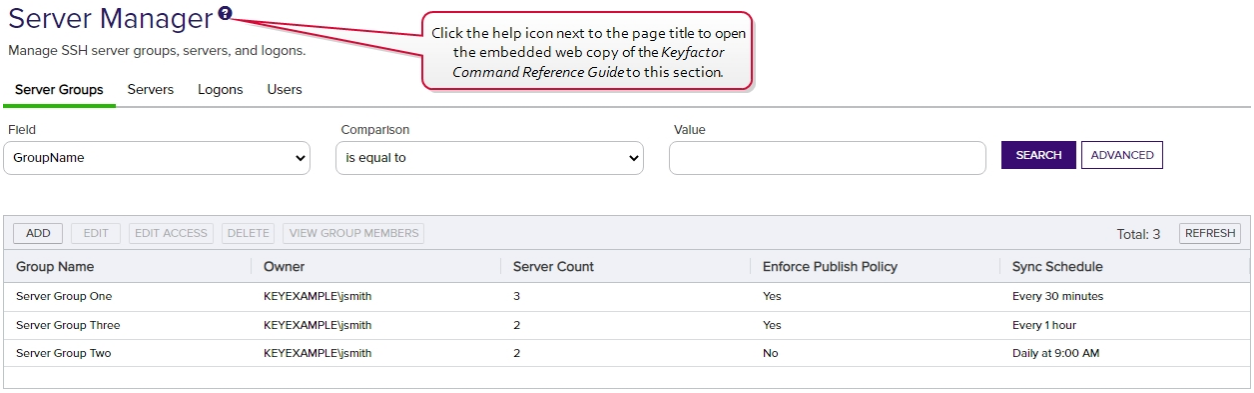


Figure 310: SSH Server Groups Grid

Tip: Click the help icon (?) next to the page title to open the embedded web copy of the *Keyfactor Command Reference Guide* to this section.
You can also find the help icon at the top of the page next to the **Log Out** button. From here you can choose to open either the *Keyfactor Command Documentation Suite* at the home page or the *Keyfactor API Endpoint Utility*.

Adding Server Groups

To add a new server group:

1. In the Management Portal, browse to *SSH > Server Manager*.
2. On the Server Manager page, select the Server Groups tab (the default when you first visit the page).
3. On the Server Groups tab, click **Add**.

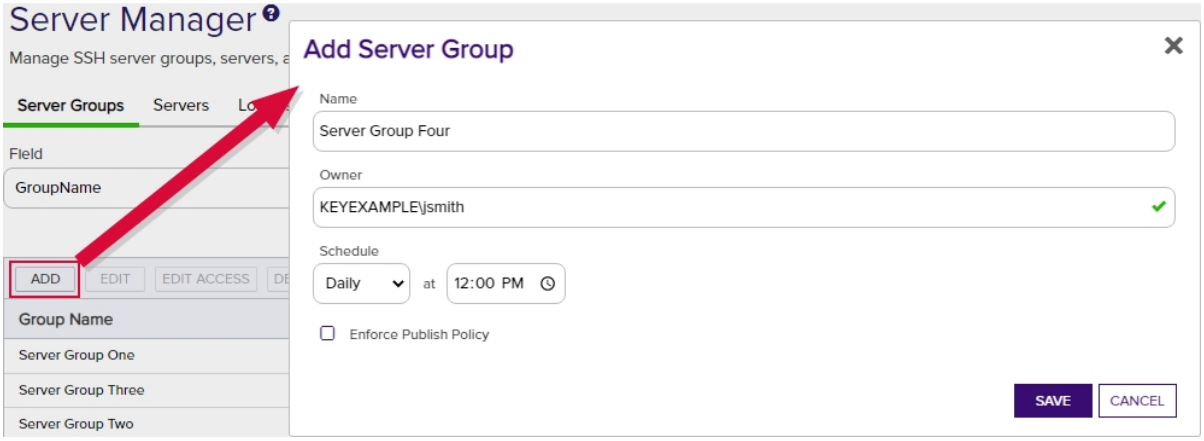


Figure 311: Add a Server Group

4. In the Add Server Group dialog, enter a name for the group in the **Name** field.
5. In the **Owner** dropdown, enter or select an Active Directory user with access to the Keyfactor Command Management Portal holding either the SSH Server Admin or SSH Enterprise Admin role (see SSH Permissions on page 579). Any users with one of these roles who have previously been made an owner on a server group or enrolled for an SSH key (see My SSH Key on page 512) will appear in the Owner dropdown.
6. In the **Schedule** dropdown, select a frequency for the server synchronization job. Possible options are:
    - Interval—Enter an interval from every 1 minute to every 12 hours
    - Daily—Enter selected time
    - Weekly—Enter a selected day or days of the week at a selected time
    - Monthly—Enter a selected day of the month (1st through 27th) at a selected time

    Tip: During initial configuration, you may want to set a short timeframe for job frequency and then extend it as the servers settle into a management routine.
7. If desired, check the **Enforce Publish Policy** box to set the server group to *inventory and publish policy* mode (see SSH on page 507).
8. Click **Save** to save the new server group.

Editing or Deleting a Server Group

To edit a server group, double-click the group, right-click the group and choose **Edit** from the right-click menu, or highlight the row in the server groups grid and click **Edit** at the top of the grid.

Tip: The owner can only be changed by a Keyfactor Command user who holds the *SSH Enterprise Admin* role (see SSH Permissions on page 579).

To delete a server group, highlight the row in the server groups grid and click **Delete** at the top of the grid or right-click the group in the grid and choose **Delete** from the right-click menu.

Editing Access to an SSH Server Group

Using the Edit Access function you create mappings between Keyfactor Command user accounts associated with SSH keys and Linux logons in order to publish the SSH public keys to all the Linux servers that belong to the selected server group (see SSH on page 507). You can also remove the mappings from here, which causes the SSH public keys to be removed from the Linux servers belonging to the selected server group.

Before adding a logon to user mapping, be sure that you have switched either the server group or all servers in the group to which you will add your mapping to *inventory and publish policy* mode (see Server Manager on page 542) so that the key for the user will be published to the servers in the group. If the servers in the server group are in *inventory only* mode and you add a mapping for it in Keyfactor Command, the mapping will appear in Keyfactor Command only and the key for the user will not be published out to the servers in the server group. If only some servers in the server group are in *inventory and publish policy* mode, the key for the user will only be published to those servers.

Tip: The time it will take for changes to access mappings to appear on your Linux servers will depend on the frequency of the server synchronization configured for the server group (see Adding Server Groups on page 543).

To edit the access for a server group, create a mapping between a Linux logon and a Keyfactor Command user, and publish the user's key to all the SSH servers belonging to that server group:

1. In the Management Portal, browse to *SSH > Server Manager*.
2. On the Server Manager page, select the Server groups tab.
3. In the Server groups grid, locate the server group that contains the servers you wish to publish an SSH key to by mapping a Keyfactor Command user to a Linux logon on that server group.
4. Right-click the server group and choose **Edit Access** from the right-click menu or highlight the row in the server groups grid and click **Edit Access** at the top of the grid.

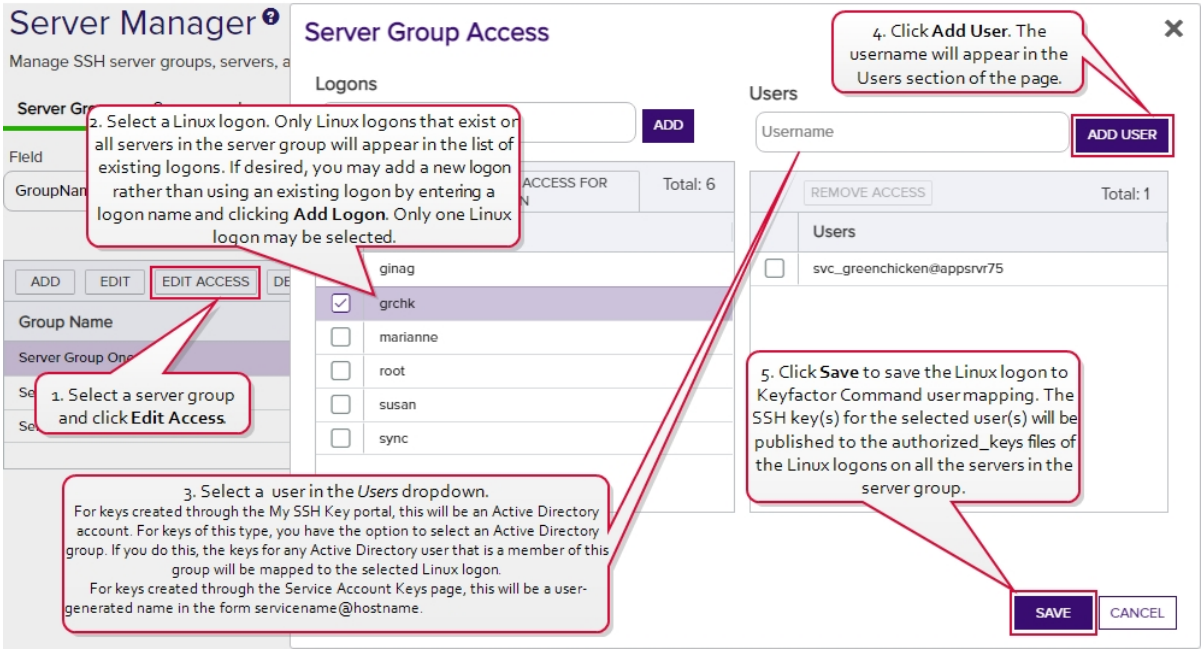


Figure 312: Edit Access for an SSH Server Group

5. On the Access Management page, select an existing Logon on the left side of the page. Logons only appear here if they exist with the same spelling on all servers in the server group. If you wish to add a new logon, enter the new logon name in the Logon field at the top of the left side of the page and click **Add Logon**. The new logon appears at the bottom of the Logon list. Click the **Logon** list title to sort the list, if desired. Select the new logon. Only one logon may be selected.

   Tip: If you have enabled SSSD support for your Keyfactor Bash Orchestrator and are adding a domain user, specify the user in username@domain format. For example bbrown@keyexample.com (or, depending on SSSD configuration, such as the case-sensitivity setting; BBROWN@keyexample.com). Note that the logon may be modified by the SSSD configuration file in ways in which Keyfactor Command cannot know about. Refer to SSH-SSSD Case Sensitivity Flag on page 700 for guidance on what to enter based on how the SSSD case sensitivity flag is configured.

6. In the Users dropdown at the top of the right side of the page, select a *user* or *service account* to associate the logon with. Only Keyfactor users that have keys stored in Keyfactor Command, that have been designated as server group owners, or AD users or groups that have been previously entered for association with a logon will appear in the dropdown. If desired, you may enter an Active Directory user or group name in this field. Using an Active Directory group to create Linux logon to Keyfactor user mappings will cause the keys stored in Keyfactor Command for any Active Directory users that are members of this group to be mapped to the selected Linux logon and published to the servers on which the Linux logon exists. Any Active Directory users that are members of this group but who do not have keys stored in Keyfactor Command will not be

mapped to the selected Linux logon. Click **Add User**.

> **Tip:** For keys created through the My SSH Key portal (see My SSH Key on page 512), a Keyfactor user is an Active Directory user account. For keys created through the Service Account Keys page (see Service Account Keys on page 524), a Keyfactor user is a user-generated service account name of the form servicename@hostname.

7. Repeat step 6 for any other user or service accounts that you wish to map to this logon on the servers in this server group.
8. Click **Save**.

To remove a mapping of a Linux logon to a Keyfactor Command user for all the servers in a server group, remove the public key from the Linux logon's authorized_keys files:

1. In the Management Portal, browse to *SSH > Server Manager*.
2. On the Server Manager page, select the Server Groups tab.
3. In the Server Groups grid, locate the server group that contains the servers you wish to remove an SSH key from by unmapping a Keyfactor Command user from a Linux logon on that server group.
4. Right-click the server group and choose **Edit Access** from the right-click menu or highlight the row in the server groups grid and click **Edit Access** at the top of the grid.

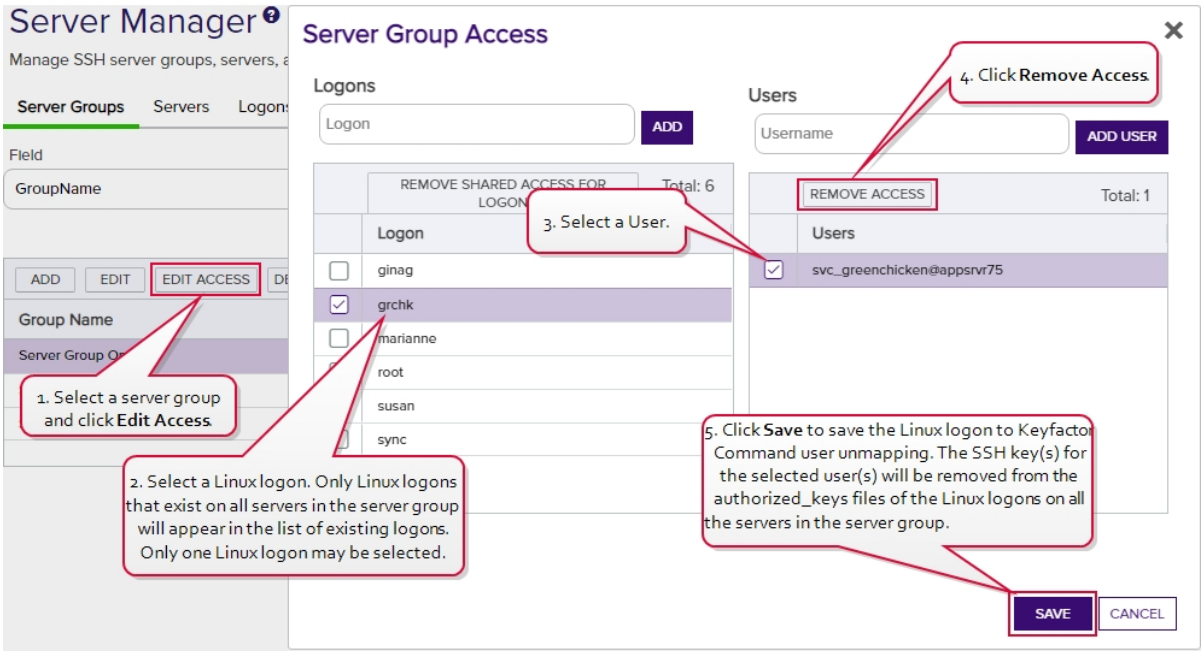


Figure 313: Edit Access for an SSH Server

5. On the Access Management page, select a Logon on the left side of the page. Only one logon may be selected.

6. In the Users section on the right side of the page, select a *user* or *service account* to unmap from the logon. Click **Remove Access** under *Users*. The Linux logon to Keyfactor user mapping for the *selected user* will be removed and the user's SSH key will be removed from the authorized_keys files of the Linux logons on all the servers in the server group.

   Tip: Clicking **Remove Shared Access for Logon** on the *Logons* side of the page removes *all* Linux logon to Keyfactor user mappings for the selected logon with one click without the need to select the users on the *Users* side of the page.
   If a logon has user mappings on some servers and not others in the group (see the example, below), these will not appear in the Server Group Edit dialog, and none of these user mappings will be removed. The *Remove Shared Access for Logon* option only removes user mappings that are visible in the Server Group Access dialog.

   This option does not delete the logon from any servers (see Editing or Deleting a Logon on page 570).

7. Repeat step 6 for any other user or service accounts that you wish to unmap from this logon on the servers in this server group.

8. Click **Save**.

Example: *Server Group One* contains three Linux servers—A, B and C. Linux logons for *Anne*, *Betty* and *Dave* exist on all three servers. A Linux logon for *Chuck* exists on servers A and B but not C. In Keyfactor Command:

- Anne has acquired an SSH key using My SSH Key (see My SSH Key on page 512) and an administrator has mapped it to her Linux logon for all three servers in *Server Group One*.
- Betty has acquired an SSH key using My SSH Key and an administrator has mapped it to her Linux logon account for servers A and B but not server C.
- Chuck has acquired an SSH key using My SSH Key and an administrator has mapped it to his Linux logon account for servers A and B. No Linux account exists for Chuck on server C and no user mapping has been done for Chuck for this server.
- Dave has acquired an SSH key using My SSH Key but it has not yet been mapped to his Linux logon account for any servers.

You can see these Linux logon to Keyfactor user mappings in Figure 314: Linux Logon to Keyfactor User Mappings for Anne, Betty, Chuck and Dave.

Figure 314: Linux Logon to Keyfactor User Mappings for Anne, Betty, Chuck and Dave

As a result of this logon setup and mapping configuration, when you open the Server Group Access dialog for *Server Group One* (see Figure 315: Server Group Access Editing Example), in the Logon column you will see *anne*, *betty* and *dave* but not *chuck*.

- *Chuck* is missing because he does not have a Linux logon account on server C.
- As you click on each of the users *anne*, *betty* and *dave* in the Logon column, on the right in the Users column, you will see that:
  - *Anne's* mapped user appears, but a mapped user does not appear for either *Betty* or *Dave*.
  - In *Betty's* case, this is because her Keyfactor user to Linux logon mapping does not exist for server C. Mapped users only appear if they are consistent across all Linux logons for a user.
  - In *Dave's* case, this is because he does not have a Keyfactor user to Linux logon mapping for any of the servers.
- Other shared Linux logons exist on the servers—such as root—that are not referenced in this example but are shown in Figure 315: Server Group Access Editing Example.

Tip: Logons only appear in the Linux logon column if they exist with the same spelling on all servers in the server group—*dave* does not equal *david* and will not be recognized as a Linux logon match.

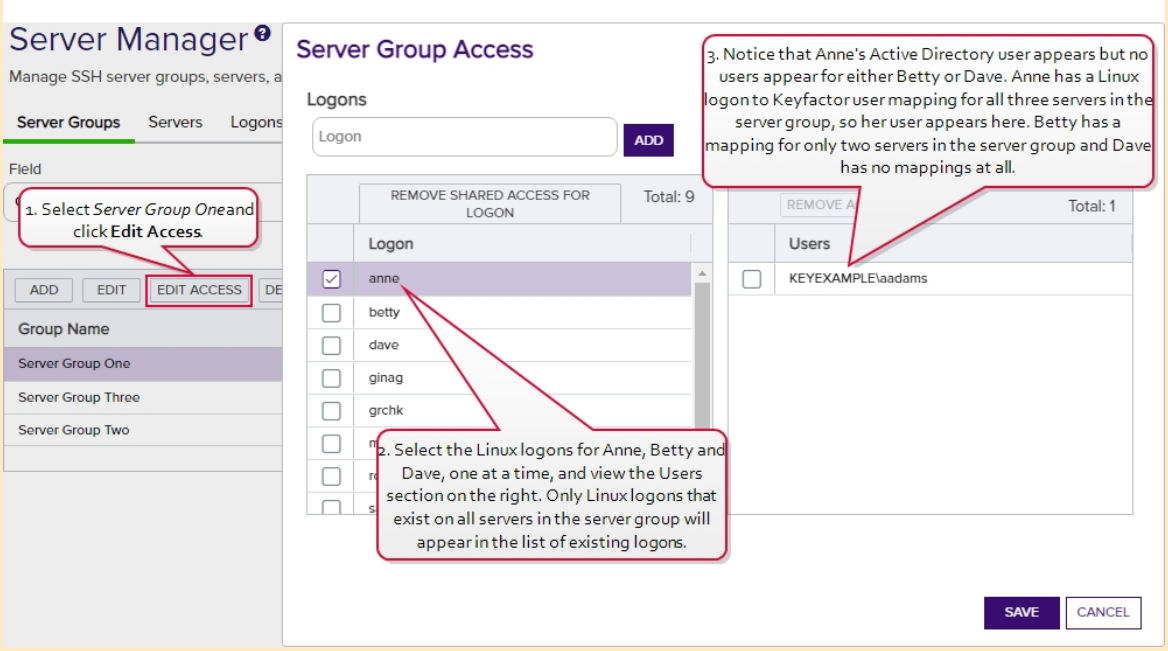


Figure 315: Server Group Access Editing Example

The administrator decides to do the following:

- On the Server Groups tab, she selects *Server Group One* and clicks **Edit Access** at the top of the grid.

- In the Server Group Access for *Server Group One*, she adds a Linux logon for *chuck* on the left and clicks **Save** without adding any user mappings on the right.
- Since *Chuck* already had Linux logon accounts on servers A and B, no changes are made on those servers. A Linux logon account is added on server C for *Chuck*.
- When the administrator opens the Server Group Access for *Server Group One* again, she sees *Chuck's* Linux logon on the left. When she clicks on *chuck*, no Users are shown on the right because *Chuck* only has Linux logon to Keyfactor user mappings for servers A and B, not for server C.

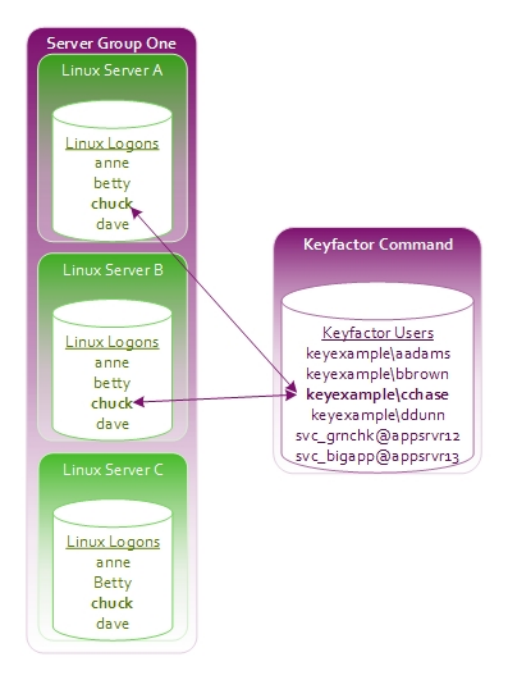


Figure 316: Concept: Add Linux Logon for Chuck on Server C

- In the Server Group Access for *Server Group One*, she selects *chuck* on the left and creates a mapping to *Chuck's* SSH key acquired through My SSH Key. This adds the key to the authorized_keys file for *Chuck* on any servers in the server group that lack the key—in this case, server C. This then completes the mappings for Linux logon the Keyfactor user for *Chuck* for the servers in this server group. *Chuck's* user will then appear in the Server Group Access dialog when *Chuck's* Logon is selected.

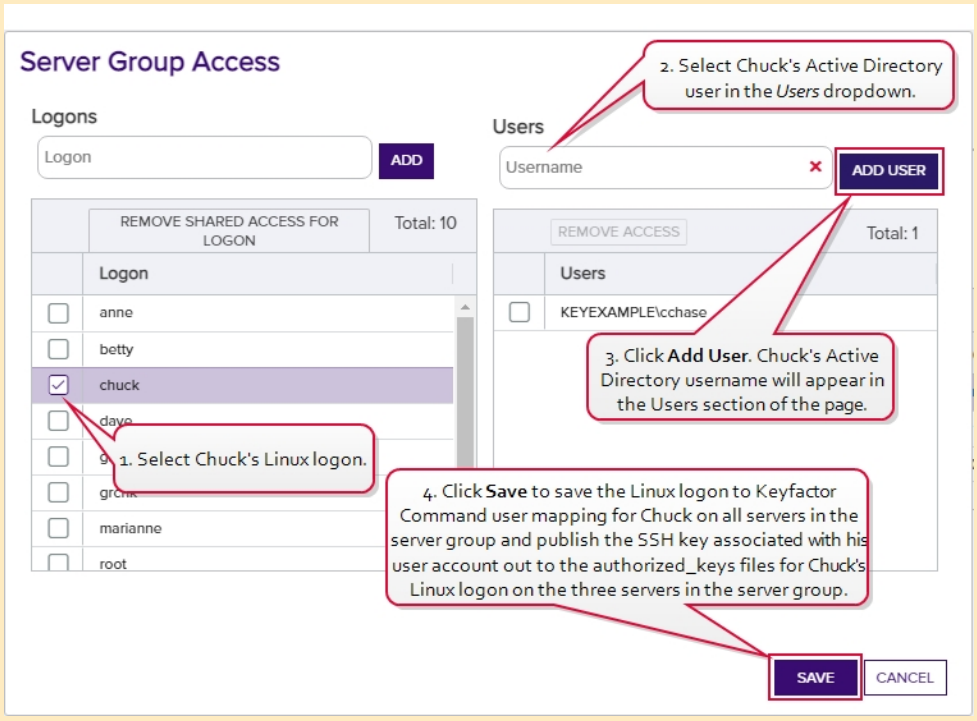


Figure 317: Server Group Access: Add Linux Logon for Chuck on Server C

- In the Server Group Access for *Server Group One*, she selects *betty* on the left and creates a mapping to *Betty's* Active Directory account, which is associated with the SSH key acquired through My SSH Key, and to a service account key for *Betty—svc_grnch-k@appsrvr12* and clicks **Save**. Since *Betty* already had Linux logon to Keyfactor user mappings for servers A and B and her SSH key was already on these servers, no changes are made to these servers. Her key acquired through My SSH Key is published out to server C and added to her authorized_keys file on that server. *Betty* had no previous mappings for the SSH service key *svc_grnchk@appsrvr12*, so this key is published out to all three servers in the server group and added to her authorized_keys files on those servers.

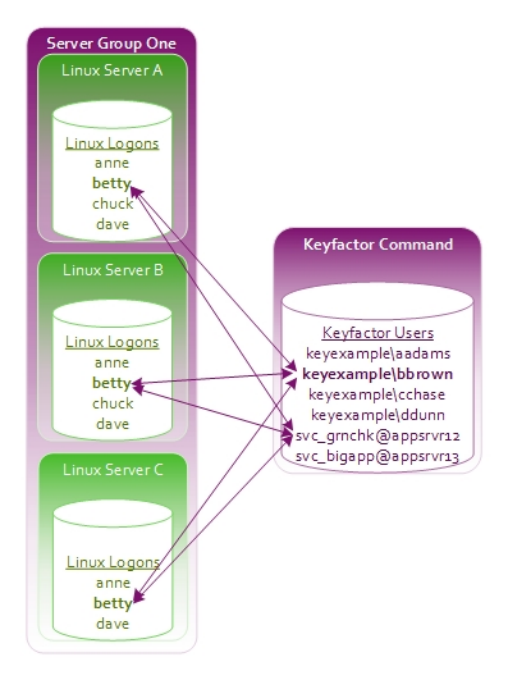


Figure 318: Add Logon to User Mapping for Betty

- At a later date, the administrator decides to remove Betty's access to the service account key. In the Server Group Access for *Server Group One*, she selects *betty* on the left and selects the service account key *svc_grnchk@appsrvr12* on the right. She clicks **Remove Access** and then **Save**. The SSH key for the *svc_grnchk@appsrvr12* service is removed from Betty's authorized_keys file on servers A, B and C. When she opens the Server Group Access dialog again and selects Betty, she sees Betty's Active Directory account, associated with the SSH key acquired through My SSH Key, but not the svc_grnchk@appsrvr12 service account.

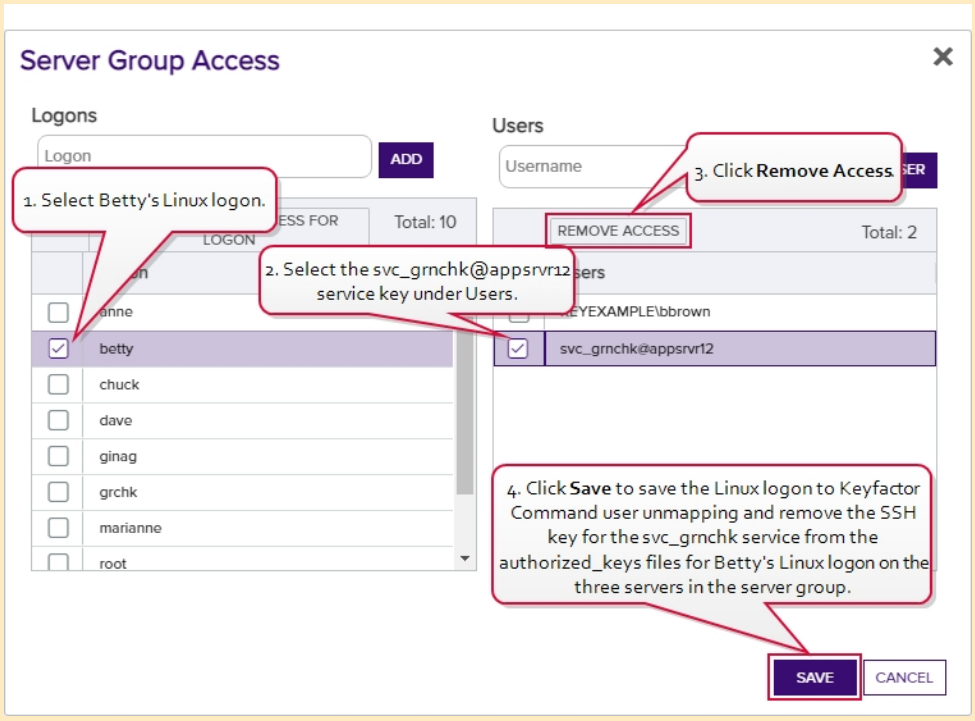


Figure 319: Remove Logon to User Mapping for Betty

- She decides to add Dave's key to the servers. On the Logons tab, she selects one of *Dave's* Linux logons on one of the servers in *Server Group One* and clicks **Edit** at the top of the grid. In the Edit Logon dialog, she changes to the Access Management tab, selects *Dave's* Active Directory account in the Users dropdown, and clicks **Add User** and **Save**. She repeats these steps for all the servers in *Server Group One* (servers A, B and C). *Dave's* SSH key acquired through My SSH Key is published out to all three servers in *Server Group One* and added to his authorized_keys files on those servers.

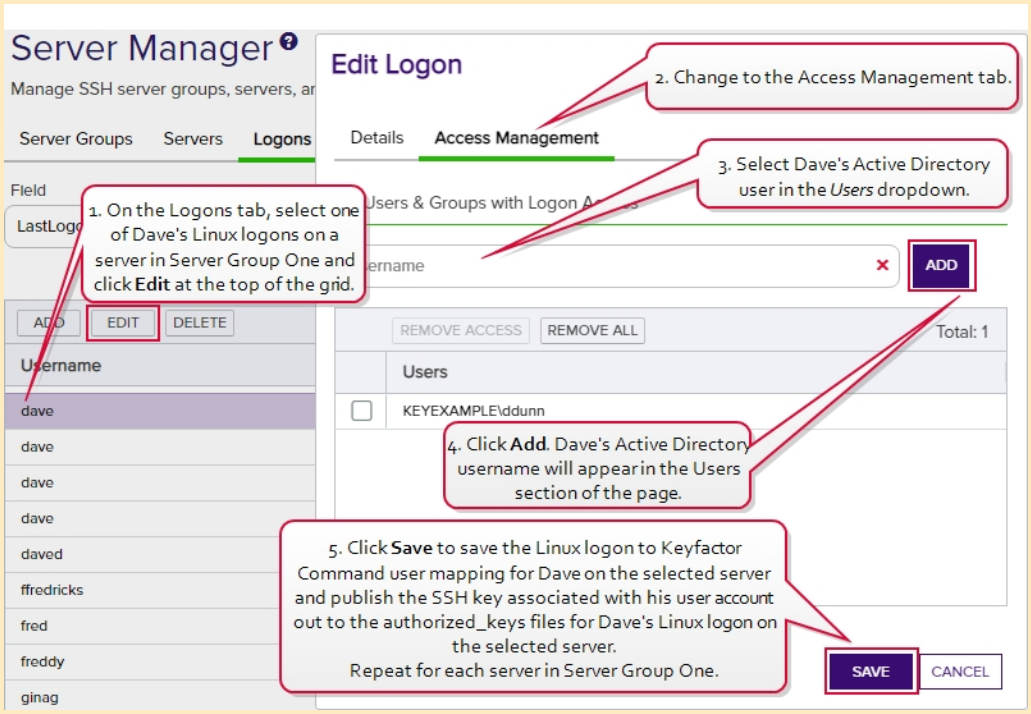


Figure 320: Add Individual Logon to User Mappings for Dave

- On the Server Groups tab, she selects *Server Group One* and clicks **Edit Access** at the top of the grid. In the Server Group Access for *Server Group One*, she selects *Dave's* Linux logon and sees that *Dave's* Active Directory account appears in the Users section on the right when it did not previously. This is because she created Linux logon to Keyfactor user mappings for *Dave* individually on the Logons tab for all the servers in *Server Group One*. If she had only done this for some of the servers in *Server Group One*, *Dave's* Active Directory user would not appear on the Server Group Access dialog.

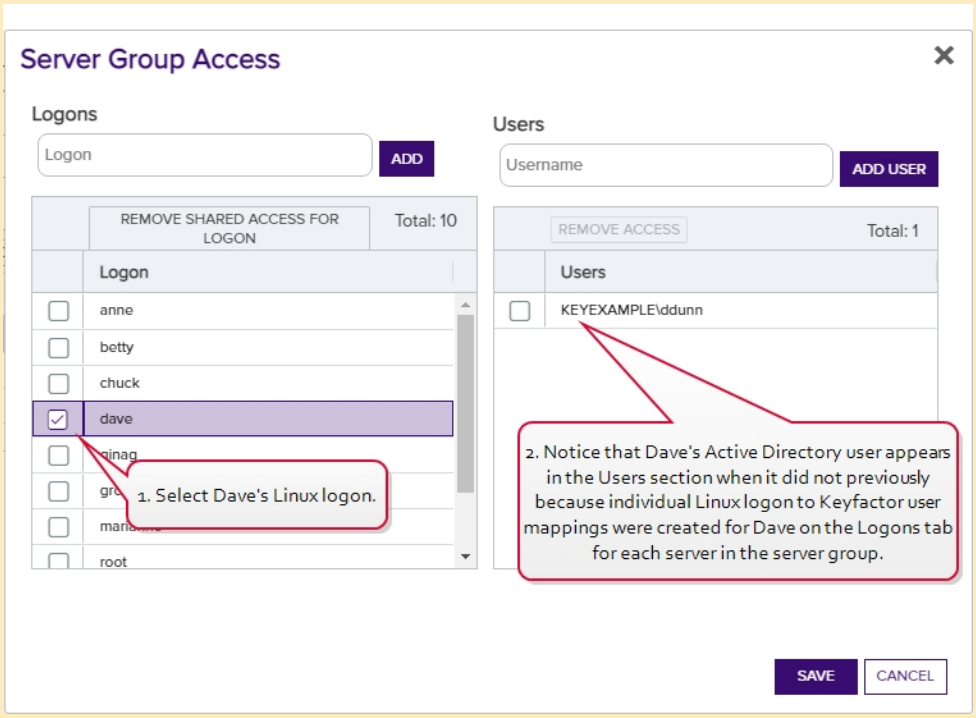


Figure 321: View Server Group Logon to User Mappings for Dave

Viewing Server Group Members

To view the servers belonging to a server group, highlight the row in the server groups grid and click **View Group Members** at the top of the grid or right-click the group in the grid and choose **View Group Members** from the right-click menu. This will take you to the Servers tab with the advanced search populated by a query for the selected server group name.

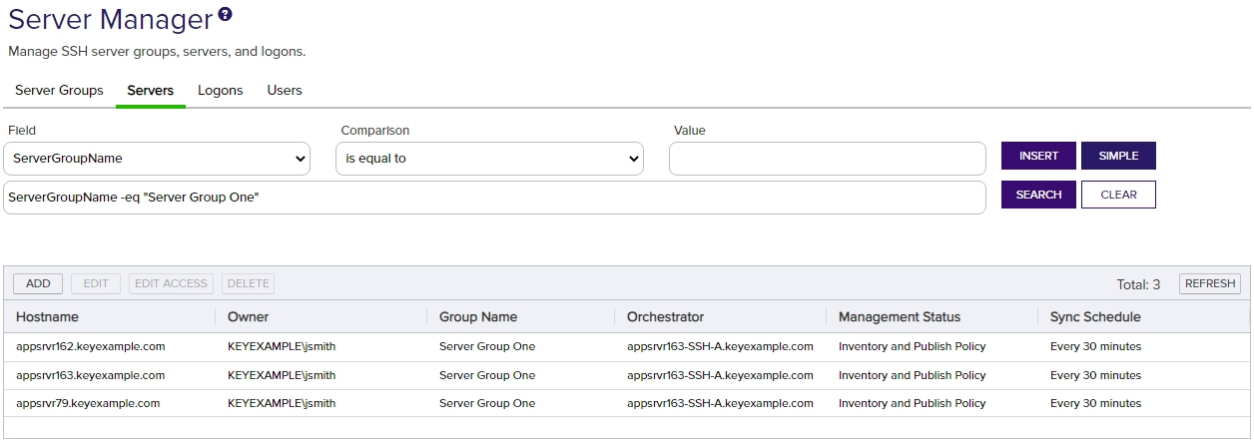


Figure 322: View Members of an SSH Server Group

Using the Server Group Search

The search function allows you to query the database for information. The same query structure is used in multiple locations within the Keyfactor Command Management Portal.

When you first open the page, you will see the simple search option. To execute a search, select the field and comparison operators in the dropdowns and type something on which to search in the value field (if applicable). If you select an *is null* or *is not null* comparison operator, the value field will be grayed out. Click the **Search** button to execute the query.

Each query consists of three parts:

Query Field

The available fields for querying vary depending on the area of the Management Portal in which the search is used. On this page, the queries can be done on the following built-in fields:

Group Name

Complete or partial matches with the server group name.

Owner Name

Complete or partial matches with the Active Directory username of the user who owns the server group. The owner can only be set by a Keyfactor Command user with the SSH Enterprise Admin role.

Enforce Publish Policy

Server group is set to *enforce publish policy* yes/no.

Tip: If a specific server in a server group is not operating as expected from an inventory and policy publishing mode perspective, check the inventory and publish policy state of the individual server. The setting on the server overrides the setting on the server's group.

Comparison Operator

The query comparison operators vary depending on the type of field selected and the specific properties of the field. The list below shows the dropdown list comparison operators, as well as the equivalent query language syntax (in parentheses).

Most string fields (the vast majority of the built-in fields) support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Contains (-contains)
- Does not contain (-notcontains)
- Starts with (-startswith)
- Ends with (-endswith)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Most date and integer fields support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Is greater than (-gt)
- Is greater than or equal to (-ge)

- Is less than (-lt)
- Is less than or equal to (-le)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Most Boolean (true/false) fields support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Comparison Value

The value you enter for comparison must match the field type. For example, integer fields only support numerical values. String fields support all alphanumeric characters. Boolean fields only support True or False. The value field is not case sensitive. Date fields support only properly formatted dates and will initially display as mm/dd/yyyy. You can choose to populate the date field by:

- Clicking in a date Value field to open a pop-up calendar to select a date that will populate the field.
- Clicking in a segment of the date format (i.e., mm/dd/yyyy) and entering a value. As you continue to type in any one segment, the cursor will keep moving onto the next segment.

The results that match your search criteria will be displayed in the results grid below the search selection options.

Advanced Searches

On any search page you can click **Advanced** to the right of the Search button to display the advanced search options. Click **Simple** to close the advanced search options again.

Multiple Criteria

Using the advanced search options, you can build a query based on multiple criteria using AND/OR logic. As with a simple search, you select a field and comparison operator in the drop-downs and then enter a comparison value, if applicable. Click **Insert** to add the search criteria to the query field below the selection fields. Use the selection fields to build multiple search criteria. Each time you click the insert button, an AND is added between the previous search criteria and the newly added one. You can change the AND to an OR if desired. You can use parentheses around portions of the query along with AND/OR to change the query meaning.

For example, for certificate searches:

```
(CN -contains "appsrvr" AND IssuedDate -ge "01/01/2022") OR (CN -contains "appsrvr" AND
TemplateShortName -contains "web")
```

This query will return all the certificates issued on or after January 1, 2022 with the string appsrvr in the CN and also all certificates issued at any time with the string appsrvr in the CN using a template referencing web. When you have entered all the desired search criteria, click **Search** to execute the query. If you wish to clear the query field and start over, click the **Clear** button.

In addition to the options available in the query builder, three special values can be used in selected searches by typing them in directly:

SSH Servers

On the Servers tab of the Server Manager page you enter records for all the SSH servers in the environment that will be inventoried or managed with the Keyfactor Bash Orchestrator. Each SSH server added here must have either the orchestrator installed on it or have had the remote install script for the orchestrator run on it, which sets up the machine for remote control by the orchestrator. For more information about the orchestrator, see *Bash Orchestrator* in the *Keyfactor Orchestrators Installation and Configuration Guide*.

You must create at least one server group before you can add SSH servers into the Keyfactor Command Management Portal (see SSH Server Groups on page 542).

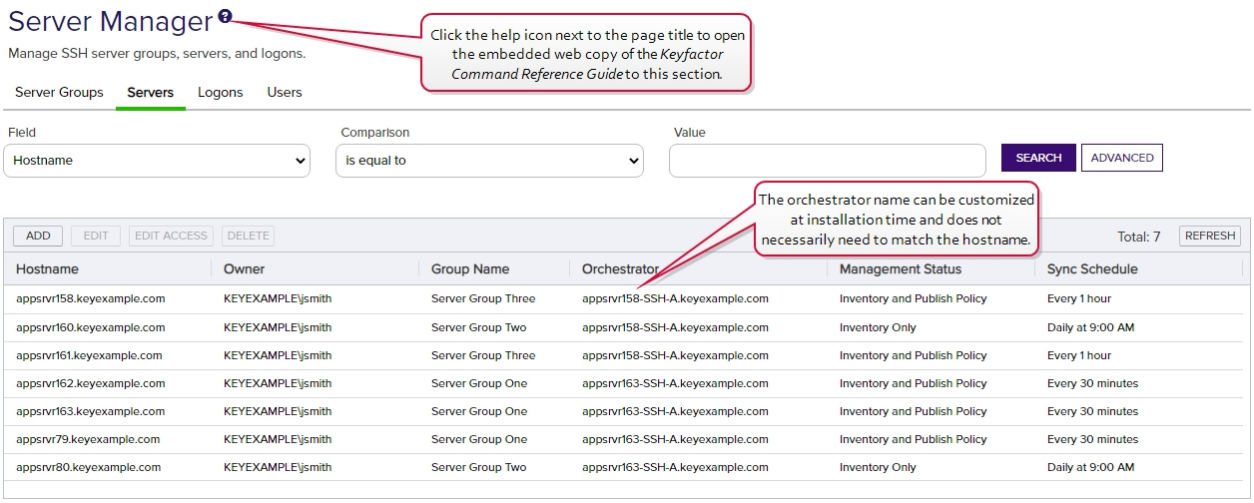


Figure 323: SSH Servers Grid

Tip: Click the help icon (?) next to the page title to open the embedded web copy of the *Keyfactor Command Reference Guide* to this section.
You can also find the help icon at the top of the page next to the **Log Out** button. From here you can choose to open either the *Keyfactor Command Documentation Suite* at the home page or the *Keyfactor API Endpoint Utility*.

Adding SSH Servers

Before adding a new SSH server, be sure that you have added at least one server group (see Adding Server Groups on page 543) and that your Keyfactor Bash Orchestrator has been registered and approved in Keyfactor Command (see Orchestrator Management on page 481).

To add a new SSH server:

1. In the Management Portal, browse to *SSH > Server Manager*.
2. On the Server Manager page, select the Servers tab.
3. On the Servers tab, click **Add**.

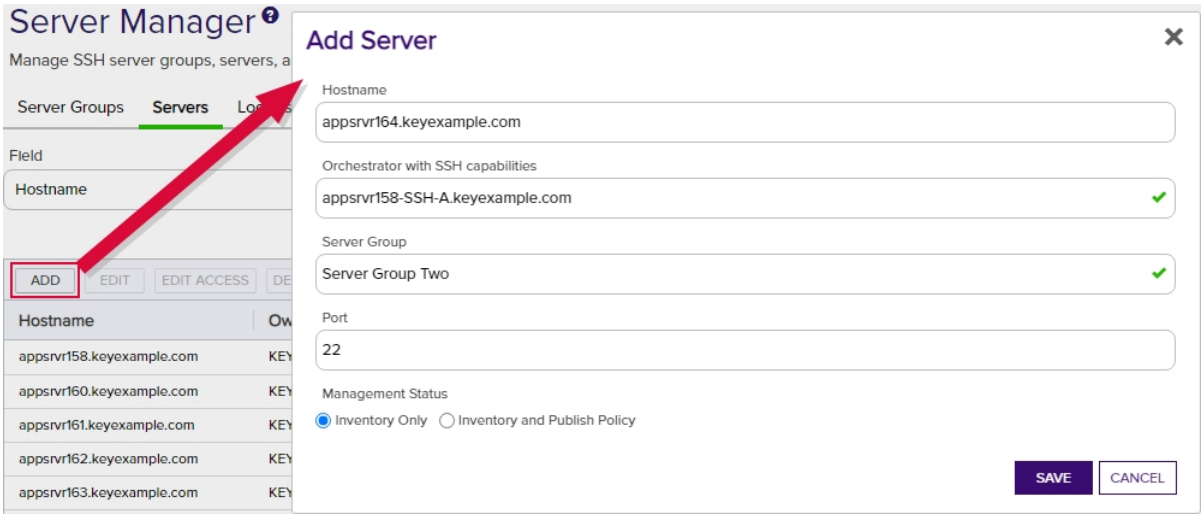


Figure 324: Add an SSH Server

4. In the Add Server dialog on the Basic tab, enter the DNS hostname for the server in the **Hostname** field. This can be either the FQDN or a short name. An IP address may be used if desired. This field is required.

   Note: The following values are **not** supported in the Hostname field:
   - 127.0.0.1
   - localhost
   - ::1

5. In the **Orchestrator** dropdown, select an approved orchestrator. This field is required.
6. In the **Server Group** dropdown, select an existing server group. This field is required.
7. In the **Port** field, either select the default SSH port of 22 or enter a custom port if an alternative port is used for SSH in your environment.
8. Select either the **Inventory Only** radio button or the **Inventory and Publish Policy** radio button (see SSH on page 507).

> **Tip:** If the server group you selected above is configured in *inventory and publish policy* mode (with the *Enforce Publish Policy* box checked), you will not be able to save the server in *inventory only* mode.

9. Click **Save** to save the new server.

> **Tip:** When you are first creating server records, you probably won't need to visit the Access Management tab of the server record. On this tab, you create mappings between Keyfactor Command user accounts associated with SSH keys and Linux logons in order to publish the SSH keys to the Linux servers (see SSH on page 507 and Editing or Deleting an SSH Server below).

Editing or Deleting an SSH Server

To edit a server, double-click the server, right-click the server and choose **Edit** from the right-click menu, or highlight the row in the servers grid and click **Edit** at the top of the grid.

Only two of the fields are available for editing:

- Port

  Change the SSH port set for the server, if desired.
- Management Status

  Select either the **Inventory Only** radio button or the **Inventory and Publish Policy** radio button.

  > **Tip:** If the server group for the server is configured in *inventory and publish policy* mode (with the *Enforce Publish Policy* box checked), you will not be able to save the server in *inventory only* mode.

To delete a server, highlight the row in the servers grid and click **Delete** at the top of the grid or right-click the server in the grid and choose **Delete** from the right-click menu.

> **Tip:** The hostname, orchestrator, and server group for a server are not editable. If you wish to change one of these, delete the record and add a fresh record for the server.

Editing Access to an SSH Server

Using the Edit Access function you create mappings between Keyfactor Command user accounts associated with SSH keys and Linux logons in order to publish the SSH public keys to the Linux servers (see SSH on page 507). You can also remove the mappings from here, which causes the SSH public keys to be removed from the Linux servers.

Before adding a logon to user mapping, be sure that you have switched the server to which you will add your mapping (or its server group) to *inventory and publish policy* mode (see Server Manager on

page 542) so that the key for the user will be published to the server. If the server is in *inventory only* mode and you add a mapping for it in Keyfactor Command, the mapping will appear in Keyfactor Command only and the key for the user will not be published out to the server.

To edit the access for a server, create a mapping between a Linux logon and a Keyfactor Command user, and publish the user's key to the SSH server:

1. In the Management Portal, browse to *SSH > Server Manager*.
2. On the Server Manager page, select the Servers tab.
3. In the Servers grid, locate the server that you wish to publish an SSH key to by mapping a Keyfactor Command user to a Linux logon on that server.
4. Right-click the server and choose **Edit Access** from the right-click menu or highlight the row in the servers grid and click **Edit Access** at the top of the grid.

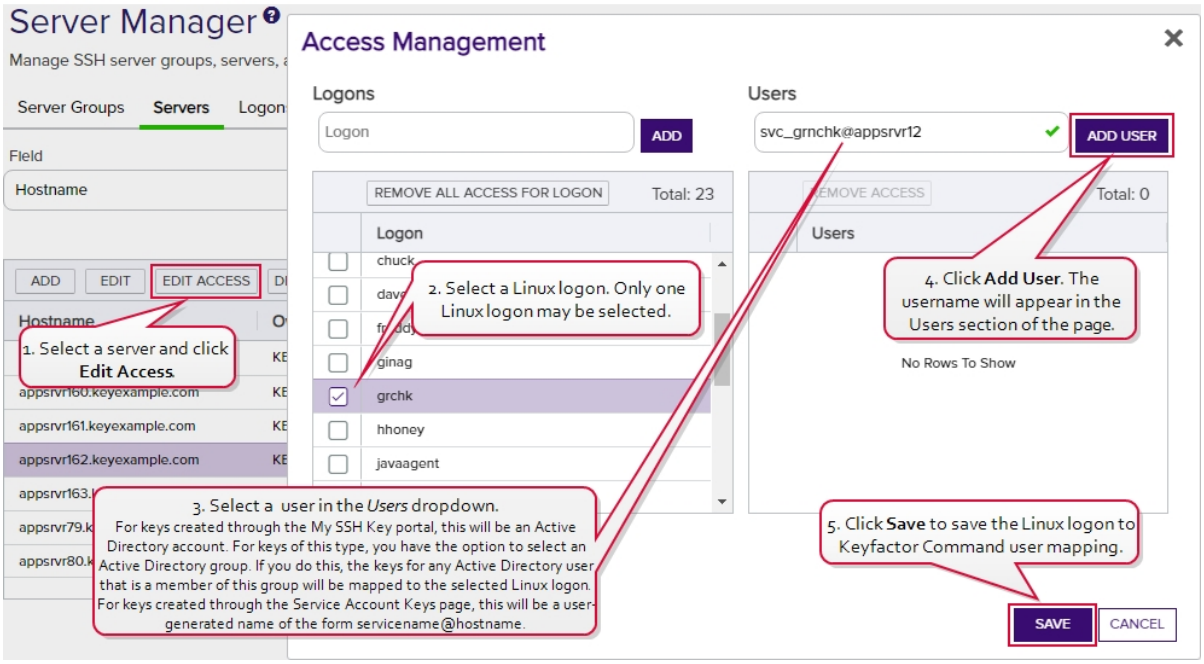


Figure 325: Edit Access for an SSH Server

5. On the Access Management page, select an existing Logon on the left side of the page. If you wish to add a new logon, enter the new logon name in the Logon field at the top of the left side of the page and click **Add Logon**. The new logon appears at the bottom of the Logon list. Click the **Logon** list title to sort the list, if desired. Select the new logon. Only one logon may be selected.

> **Tip:** If you have enabled SSSD support for your Keyfactor Bash Orchestrator and are adding a domain user, specify the user in username@domain format. For example bbrown@keyexample.com (or, depending on SSSD configuration, such as the case-

sensitivity setting; BBROWN@keyexample.com). Note that the logon may be modified by the SSSD configuration file in ways in which Keyfactor Command cannot know about. Refer to SSH-SSSD Case Sensitivity Flag on page 700 for guidance on what to enter based on how the SSSD case sensitivity flag is configured.

6. In the Users dropdown at the top of the right side of the page, select a *user* or *service account* to associate the logon with. Only Keyfactor users that have keys stored in Keyfactor Command, that have been designated as server group owners, or AD users or groups that have been previously entered for association with a logon will appear in the dropdown. If desired, you may enter an Active Directory user or group name in this field. Using an Active Directory group to create Linux logon to Keyfactor user mappings will cause the keys stored in Keyfactor Command for any Active Directory users that are members of this group to be mapped to the selected Linux logon and published to the server on which the Linux logon exists. Any Active Directory users that are members of this group but who do not have keys stored in Keyfactor Command will not be mapped to the selected Linux logon. Click **Add User**.

   Tip: For keys created through the My SSH Key portal (see My SSH Key on page 512), a Keyfactor user is an Active Directory user account. For keys created through the Service Account Keys page (see Service Account Keys on page 524), a Keyfactor user is a user-generated service account name of the form servicename@hostname.

7. Repeat step 6 for any other user or service accounts that you wish to map to this logon on this server.

8. Click **Save**.

To remove a mapping of a Linux logon to a Keyfactor Command user for a server, removing the public key from the Linux logon's authorized_keys file:

1. In the Management Portal, browse to *SSH > Server Manager*.

2. On the Server Manager page, select the Servers tab.

3. In the Servers grid, locate the server that you wish to remove an SSH key from by unmapping a Keyfactor Command user from a Linux logon on that server.

4. Right-click the server and choose **Edit Access** from the right-click menu or highlight the row in the servers grid and click **Edit Access** at the top of the grid.

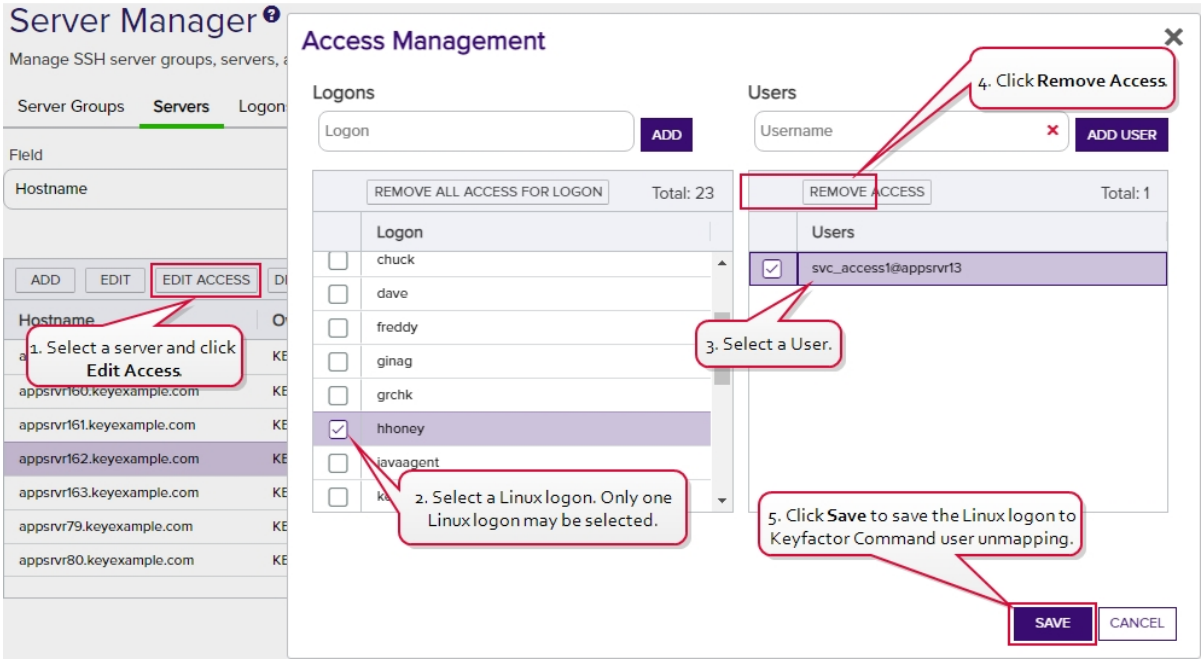


Figure 326: Edit Access for an SSH Server

5. On the Access Management page, select a Logon on the left side of the page. Only one logon may be selected.

6. In the Users section on the right side of the page, select a *user* or *service account* to unmap from the logon. Click **Remove Access** under *Users*. The Linux logon to Keyfactor user mapping for the *selected user* will be removed and the user's SSH key will be removed from the authorized_keys files of the Linux logon on the selected server.

   Tip: Clicking **Remove All Access for Logon** on the *Logons* side of the page removes *all* Linux logon to Keyfactor user mappings for the selected logon on the selected server with one click without the need to select the users on the *Users* side of the page. This option does not delete the logon from any servers (see Editing or Deleting a Logon on page 570).

7. Repeat step 6 for any other user or service accounts that you wish to unmap from this logon on this server.

8. Click **Save**.

Tip: The time it will take for changes to access mappings to appear on your Linux server will depend on the frequency of the server synchronization configured for the server group to which the server belongs (see Adding Server Groups on page 543).

Using the SSH Server Search

The search function allows you to query the database for information. The same query structure is used in multiple locations within the Keyfactor Command Management Portal.

When you first open the page, you will see the simple search option. To execute a search, select the field and comparison operators in the dropdowns and type something on which to search in the value field (if applicable). If you select an *is null* or *is not null* comparison operator, the value field will be grayed out. Click the **Search** button to execute the query.

Each query consists of three parts:

Query Field

The available fields for querying vary depending on the area of the Management Portal in which the search is used. On this page, the queries can be done on the following built-in fields:

Hostname

Complete or partial matches with the hostname of the SSH server.

Server Group Name

Complete or partial matches with the name of the server group to which the SSH servers belong.

Orchestrator

Complete or partial matches with the orchestrator controlling the SSH servers.

Enforce Publish Policy

Server is in *inventory only* mode or *inventory and publish policy* mode.

Server Group Owner

Complete or partial matches with the Active Directory username of the user who owns the server group to which the server belongs. The owner can only be set by a Keyfactor Command user with the SSH Enterprise Admin role.

Comparison Operator

The query comparison operators vary depending on the type of field selected and the specific properties of the field. The list below shows the dropdown list comparison operators, as well as the equivalent query language syntax (in parentheses).

Most string fields (the vast majority of the built-in fields) support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Contains (-contains)
- Does not contain (-notcontains)
- Starts with (-startswith)
- Ends with (-endswith)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Most date and integer fields support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Is greater than (-gt)
- Is greater than or equal to (-ge)

- Is less than (-lt)
- Is less than or equal to (-le)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Most Boolean (true/false) fields support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Comparison Value

The value you enter for comparison must match the field type. For example, integer fields only support numerical values. String fields support all alphanumeric characters. Boolean fields only support True or False. The value field is not case sensitive. Date fields support only properly formatted dates and will initially display as mm/dd/yyyy. You can choose to populate the date field by:

- Clicking in a date Value field to open a pop-up calendar to select a date that will populate the field.
- Clicking in a segment of the date format (i.e., mm/dd/yyyy) and entering a value. As you continue to type in any one segment, the cursor will keep moving onto the next segment.

The results that match your search criteria will be displayed in the results grid below the search selection options.

Advanced Searches

On any search page you can click **Advanced** to the right of the Search button to display the advanced search options. Click **Simple** to close the advanced search options again.

Multiple Criteria

Using the advanced search options, you can build a query based on multiple criteria using AND/OR logic. As with a simple search, you select a field and comparison operator in the drop-downs and then enter a comparison value, if applicable. Click **Insert** to add the search criteria to the query field below the selection fields. Use the selection fields to build multiple search criteria. Each time you click the insert button, an AND is added between the previous search criteria and the newly added one. You can change the AND to an OR if desired. You can use parentheses around portions of the query along with AND/OR to change the query meaning.

For example, for certificate searches:

```
(CN -contains "appsrvr" AND IssuedDate -ge "01/01/2022") OR (CN -contains "appsrvr" AND
TemplateShortName -contains "web")
```

This query will return all the certificates issued on or after January 1, 2022 with the string appsrvr in the CN and also all certificates issued at any time with the string appsrvr in the CN using a template referencing web. When you have entered all the desired search criteria, click **Search** to execute the query. If you wish to clear the query field and start over, click the **Clear** button.

Logons

On the Logons tab of the Server Manager page you can view all the Linux user accounts associated with authorized_keys files containing valid SSH public keys. The logons shown here include both those discovered on SSH servers during the initial discovery phase using the orchestrator and those created in Keyfactor Command and published to the SSH servers using the orchestrator.

On this tab you can create new logons, see the number of keys associated with each logon, and create mappings between Keyfactor Command users and the logons in order to allow the orchestrator to publish new SSH keys for those users to the SSH servers (see SSH on page 507).

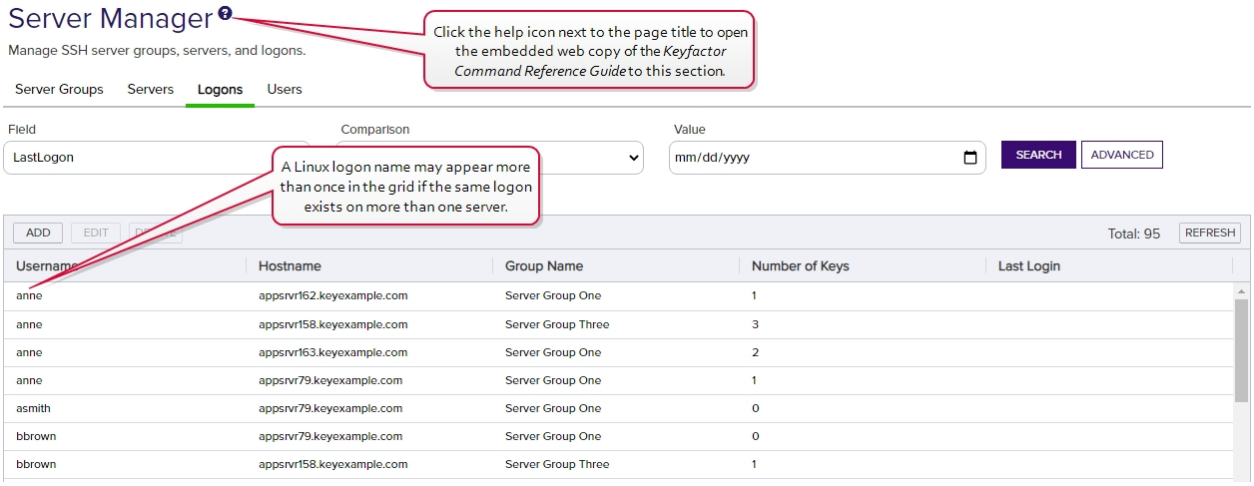


Figure 327: Linux Logons Grid

Tip: Click the help icon (?) next to the page title to open the embedded web copy of the *Keyfactor Command Reference Guide* to this section.
You can also find the help icon at the top of the page next to the **Log Out** button. From here you can choose to open either the *Keyfactor Command Documentation Suite* at the home page or the *Keyfactor API Endpoint Utility*.

Adding Logons

Before adding a new logon, be sure that you have switched the server to which you will add your logon (or its server group) to *inventory and publish policy* mode (see Server Manager on page 542) so that the new logon will be published to the server. If the server is in *inventory only* mode and you add a new logon for it in Keyfactor Command, the logon will appear in Keyfactor Command only and will not be published out to the server.

Tip: New logons can also be added from the access management options for server groups and servers while creating Linux logon to Keyfactor Command user mappings (see Editing

Access to an SSH Server Group on page 545 and Editing Access to an SSH Server on page 561).

To add a new logon:

1. In the Management Portal, browse to *SSH > Server Manager*.
2. On the Server Manager page, select the Logons tab.
3. On the Logons tab, click **Add**.

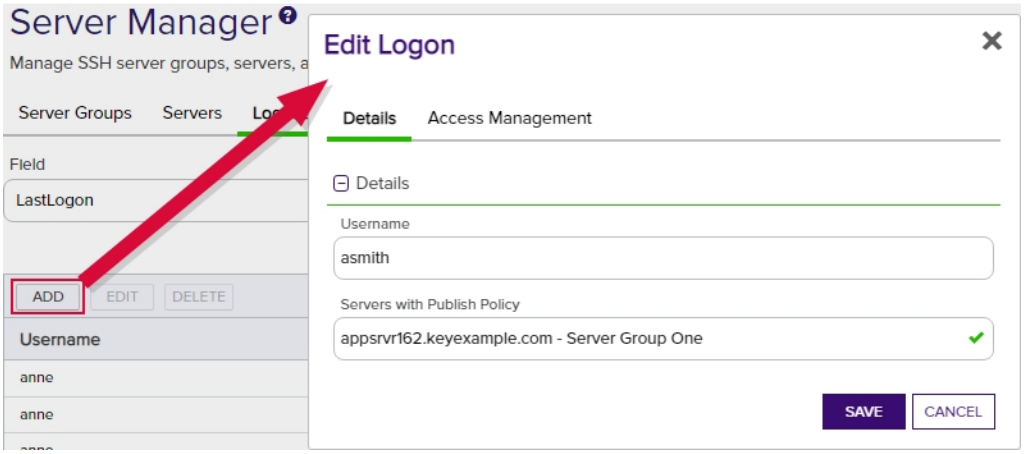


Figure 328: Add a Linux Logon—Basic Tab

4. In the Add Logon dialog on the Details tab, enter a Linux *Username* for the user.

   Tip: If you have enabled SSSD support for your Keyfactor Bash Orchestrator and are adding a domain user, specify the user in username@domain format. For example bbrown@keyexample.com (or, depending on SSSD configuration, such as the case-sensitivity setting; BBROWN@keyexample.com). Note that the logon may be modified by the SSSD configuration file in ways in which Keyfactor Command cannot know about. Refer to SSH-SSSD Case Sensitivity Flag on page 700 for guidance on what to enter based on how the SSSD case sensitivity flag is configured.

5. In the *Servers with Publish Policy* dropdown on the Details tab, select an available SSH server on which to create the logon. Only servers that are configured in *inventory and publish policy* mode (see Server Manager on page 542) will appear in this dropdown. **This field is required**.

6. On the Access Management tab in the Users & Groups with Login Access dropdown, select a *user* or *service account* to associate the logon with. Only accounts that have keys stored in Keyfactor Command or that have been designated as server group owners will appear in the dropdown. If desired, you may enter an Active Directory group name in this field. This will cause the keys stored in Keyfactor Command for any Active Directory users that are members of this

group to be mapped to the selected Linux logon and published to the server on which the Linux logon exists. Any Active Directory users that are members of this group but who do not have keys stored in Keyfactor Command will not be mapped to the selected Linux logon. Click **Add**. The Access Management tab is optional.

Tip: For keys created through the My SSH Key portal (see My SSH Key on page 512), a Keyfactor user is an Active Directory user account. For keys created through the Service Account Keys page (see Service Account Keys on page 524), a Keyfactor user is a user-generated service account name of the form servicename@hostname.

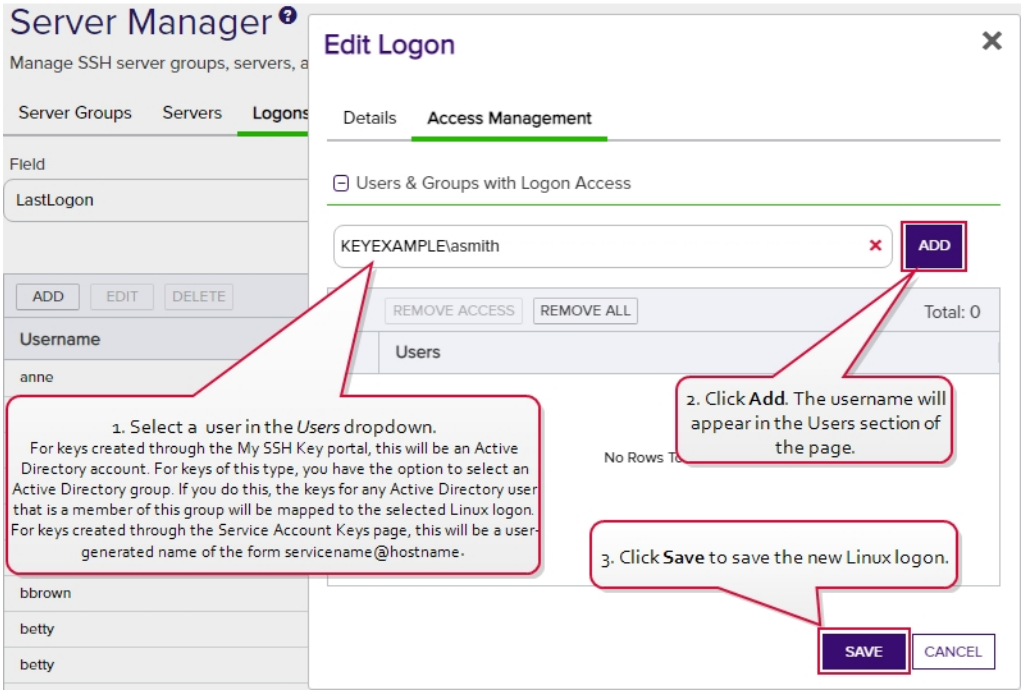


Figure 329: Add a Linux Logon—Access Management Tab

7. Click **Save** to save the new logon.

Note: When the logon is created on the Linux server, a home directory will be created for it and within this, the .ssh directory and authorized_keys file. The logon user will be made owner of the home directory and granted *rwx* permissions to it. No password is set for the user and as initially configured, the user will not be able to remotely login.

Tip: The time it will take for new logons to appear on your Linux server will depend on the frequency of the server synchronization configured for the server group to which the server belongs (see Adding Server Groups on page 543).

Editing or Deleting a Logon

On the Access Management tab of the Edit Logon dialog, you can map Keyfactor user accounts to Linux logon account to cause the SSH keys in Keyfactor Command associated with thoseKeyfactor users to be published to the authorized_keys file of the Linux user (see SSH on page 507).

To map an Keyfactor Command user to a Linux logon:

1. In the Management Portal, browse to *SSH > Server Manager*.
2. On the Server Manager page, select the Logons tab.
3. In the Logons grid locate the logon that you wish to publish an SSH key to by mapping an Active Directory account to it. Be sure to select the logon associated with the correct server, as the same logon name may appear for multiple servers.
4. Double-click the logon, right-click the logon and choose **Edit** from the right-click menu, or highlight the row in the logons grid and click **Edit** at the top of the grid.
5. On the Access Management tab in the Users & Groups with Login Access dropdown, select a *user* or *service account* to associate the logon with. Only Keyfactor users that have keys stored in Keyfactor Command, that have been designated as server group owners, or AD users or groups that have been previously entered for association with a logon will appear in the dropdown. If desired, you may enter an Active Directory user or group name in this field. Using an Active Directory group to create Linux logon to Keyfactor user mappings will cause the keys stored in Keyfactor Command for any Active Directory users that are members of this group to be mapped to the selected Linux logon and published to the server on which the Linux logon exists. Any Active Directory users that are members of this group but who do not have keys stored in Keyfactor Command will not be mapped to the selected Linux logon. Click **Add**.

   Tip: For keys created through the My SSH Key portal (see My SSH Key on page 512), a Keyfactor user is an Active Directory user account. For keys created through the Service Account Keys page (see Service Account Keys on page 524), a Keyfactor user is a user-generated service account name of the form servicename@hostname.

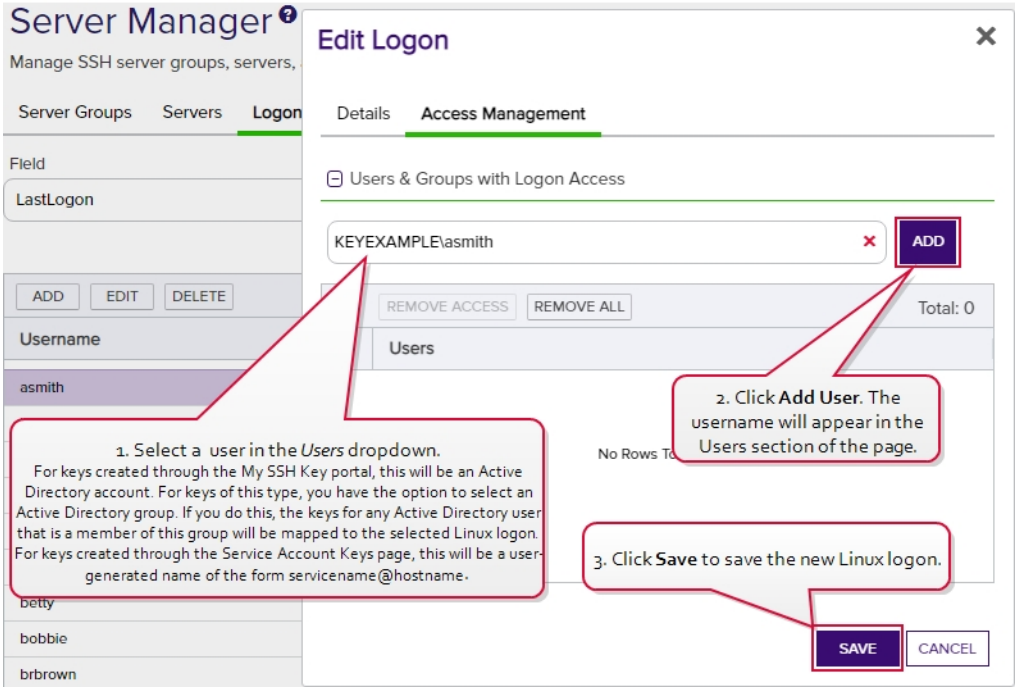


Figure 330: Edit Access for a Linux Logon

6. Click **Save** to save the access management settings.

Tip: Only the mappings of Keyfactor users to Linux logons on the Access Management tab are editable in an existing logon record. Nothing on the Details tab of the Edit Logon dialog is editable.

Note: If you opt to create Linux logon to Keyfactor user mapping using Active Directory groups, be aware that the key count values shown on the Logons grid will not reflect the keys associated with the members of the groups.

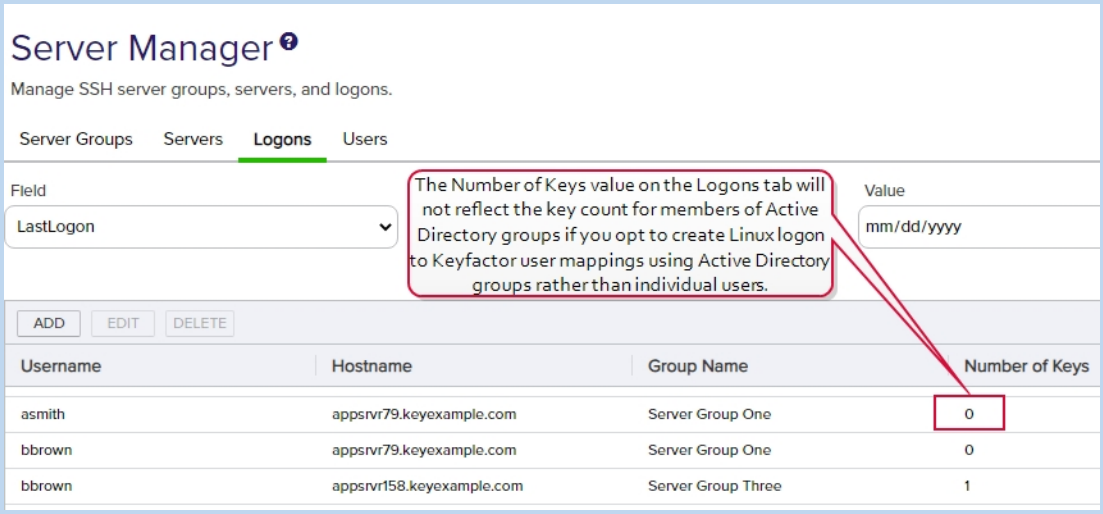


Figure 331: Creating Linux Logon to Keyfactor User Mappings Using Active Directory Groups Key Value

To delete a logon, highlight the row in the logons grid and click **Delete** at the top of the grid or right-click the logon in the grid and choose **Delete** from the right-click menu.

Note: Deleting a logon in Keyfactor Command does not delete it on the Linux server. It must be manually removed from the Linux server at the same time. If this is not done, when the next inventory of the Linux server is performed, the logon will be recreated in Keyfactor Command. This function is intended primarily to be used to clean up logons from SSH servers that have been retired.

Using the Logons Search

The search function allows you to query the database for information. The same query structure is used in multiple locations within the Keyfactor Command Management Portal.

When you first open the page, you will see the simple search option. To execute a search, select the field and comparison operators in the dropdowns and type something on which to search in the value field (if applicable). If you select an *is null* or *is not null* comparison operator, the value field will be grayed out. Click the **Search** button to execute the query.

Each query consists of three parts:

Query Field

The available fields for querying vary depending on the area of the Management Portal in which the search is used. On this page, the queries can be done on the following built-in fields:

Username	Hostname
Complete or partial matches with the Linux logon	Complete or partial matches with the hostname of

name of the user account on the SSH server.

the SSH server on which the logon resides.

LastLogon

The date on which the logon was last used to login to the given hostname.

UnmanagedKeyId

The Keyfactor Command reference ID of the unmanaged key(s) associated with the logon.

Comparison Operator

The query comparison operators vary depending on the type of field selected and the specific properties of the field. The list below shows the dropdown list comparison operators, as well as the equivalent query language syntax (in parentheses).

Most string fields (the vast majority of the built-in fields) support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Contains (-contains)
- Does not contain (-notcontains)
- Starts with (-startswith)
- Ends with (-endswith)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Most date and integer fields support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Is less than (-lt)
- Is less than or equal to (-le)
- Is greater than (-gt)
- Is greater than or equal to (-ge)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Most Boolean (true/false) fields support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Comparison Value

The value you enter for comparison must match the field type. For example, integer fields only support numerical values. String fields support all alphanumeric characters. Boolean fields only support True or False. The value field is not case sensitive. Date fields support only properly formatted dates and will initially display as mm/dd/yyyy. You can choose to populate the date field by:

- Clicking in a date Value field to open a pop-up calendar to select a date that will populate the field.
- Clicking in a segment of the date format (i.e., mm/dd/yyyy) and entering a value. As you continue to type in any one segment, the cursor will keep moving onto the next segment.

The results that match your search criteria will be displayed in the results grid below the search selection options.

Advanced Searches

On any search page you can click **Advanced** to the right of the Search button to display the advanced search options. Click **Simple** to close the advanced search options again.

Multiple Criteria

Using the advanced search options, you can build a query based on multiple criteria using AND/OR logic. As with a simple search, you select a field and comparison operator in the drop-downs and then enter a comparison value, if applicable. Click **Insert** to add the search criteria to the query field below the selection fields. Use the selection fields to build multiple search criteria. Each time you click the insert button, an AND is added between the previous search criteria and the newly added one. You can change the AND to an OR if desired. You can use parentheses around portions of the query along with AND/OR to change the query meaning.

For example, for certificate searches:

```
(CN -contains "appsrvr" AND IssuedDate -ge "01/01/2022") OR (CN -contains "appsrvr" AND
TemplateShortName -contains "web")
```

This query will return all the certificates issued on or after January 1, 2022 with the string appsrvr in the CN and also all certificates issued at any time with the string appsrvr in the CN using a template referencing web. When you have entered all the desired search criteria, click **Search** to execute the query. If you wish to clear the query field and start over, click the **Clear** button.

In addition to the options available in the query builder, three special values can be used in selected searches by typing them in directly:

- %TODAY%
  Use the TODAY special value in place of a specific date in date queries. This option supports math operations, so you can use TODAY-10 or TODAY+30. The built-in *Certificates Expiring in 7 Days* collection uses this special value (see Certificate Collection Manager on page 80).
- %ME%
  Use the ME special value in place of a specific domain\user name in queries that match a domain\user name. The built-in *My Certificates* collection uses this special value (see Certificate Collection Manager on page 80).
- %ME-AN%
  Use the ME-AN special value in place of a specific user name excluding the domain. This is beneficial in environments with multiple domains where there is a desire to query for a user's certificates even if they were requested across multiple domains.

> **Important:** The special query options of %TODAY%, %ME%, and %ME-AN% are only supported in uppercase. Lowercase equivalents (e.g. %me%) cannot be substituted.

SSH Users

On the Users tab of the Server Manager page you can view all the SSH users defined in Keyfactor Command. Both *users* and *service accounts* are included. See SSH on page 507 for more

information on the difference between users and service accounts. Active Directory groups may also be included if they have previously been used to create Linux logon to Keyfactor user mappings (see Editing Access to an SSH Server on page 561). Groups appear without associated keys (since keys are associated with the member users, not the groups). Users may appear here without associated keys if the user account has been used to grant ownership on a server group but the user has not requested an SSH key pair.

On this tab you can see the keys associated with each user and create mappings between the users and Linux logons in order to allow the orchestrator to publish new SSH keys for those users to the SSH servers associated with the selected Linux logons (see SSH on page 507).

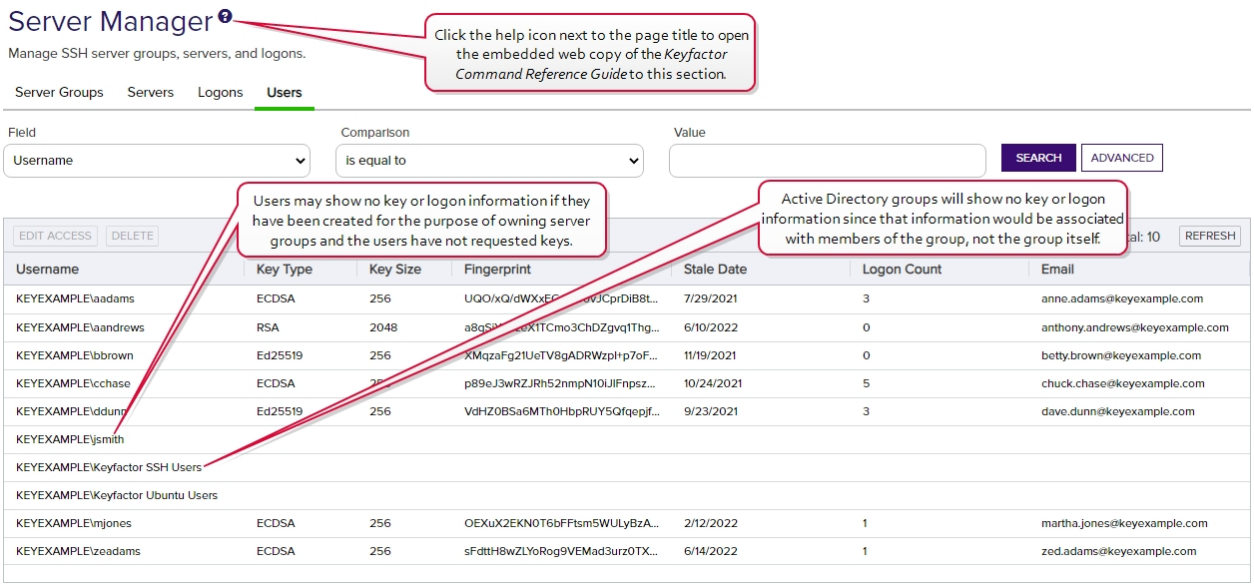


Figure 332: SSH Users Grid

Editing or Deleting an SSH User

On the Details tab of the Edit User dialog, you can view details about the user and associated key. On the Access Management tab of the Edit User dialog, you can map Keyfactor user accounts to Linux logon account to cause the SSH keys in Keyfactor Command associated with those Keyfactor users to be published to the authorized_keys file of the Linux user (see SSH on page 507).

Tip: For keys created through the My SSH Key portal (see My SSH Key on page 512), a Keyfactor user is an Active Directory user account. For keys created through the Service Account Keys page (see Service Account Keys on page 524), a Keyfactor user is a user-generated service account name of the form servicename@hostname.

To map an Keyfactor user to a Linux logon:

1. In the Management Portal, browse to *SSH > Server Manager*.
2. On the Server Manager page, select the Users tab.

3. In the Users grid locate the user whose key you wish to publish to one or more Linux logons.
4. Double-click the user, right-click the user and choose **Edit Access** from the right-click menu, or highlight the row in the users grid and click **Edit Access** at the top of the grid.
5. On the Access Management tab in the Login Access dropdown, select a logon to associate the user or service account with. A logon will appear more than once if it exists on more than one server. Be sure to select the logon on the correct server. Click **Add**.

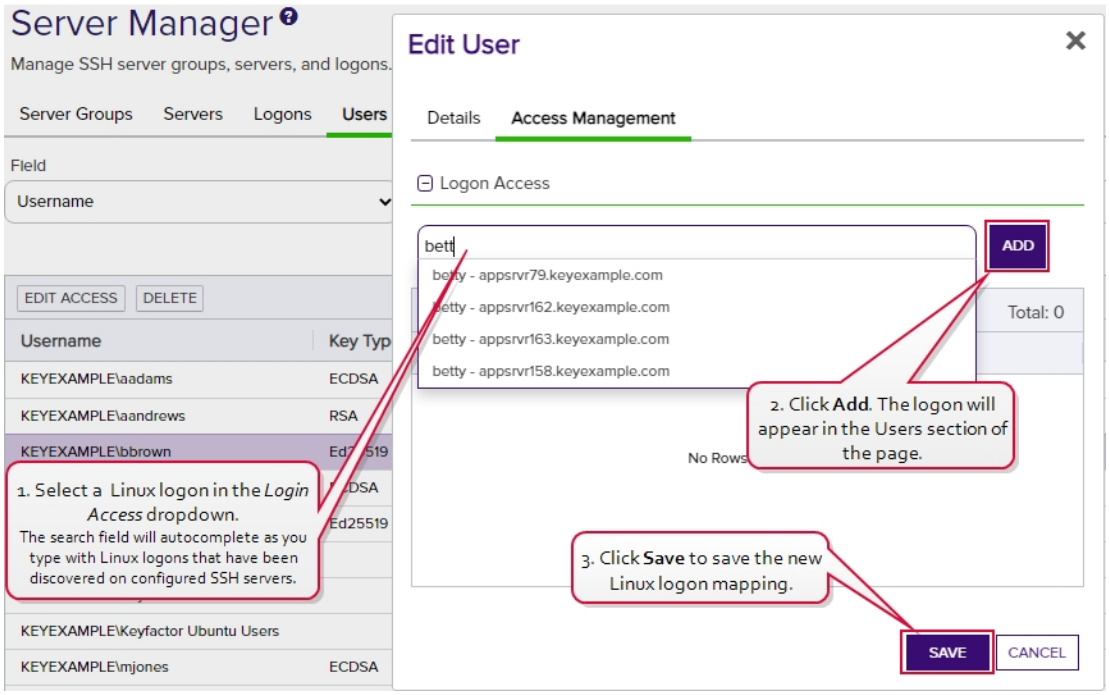


Figure 333: Edit Access for a Keyfactor User

6. Click **Save** to save the access management settings.

Tip: Only the mappings of Keyfactor users to Linux logons on the Access Management tab are editable in an existing user record. Nothing on the Details tab of the Edit Users dialog is editable.

To delete a user, highlight the row in the users grid and click **Delete** at the top of the grid or right-click the user in the grid and choose **Delete** from the right-click menu.

Using the SSH Users Search

The search function allows you to query the database for information. The same query structure is used in multiple locations within the Keyfactor Command Management Portal.

When you first open the page, you will see the simple search option. To execute a search, select the field and comparison operators in the dropdowns and type something on which to search in the value field (if applicable). If you select an *is null* or *is not null* comparison operator, the value field will be grayed out. Click the **Search** button to execute the query.

Each query consists of three parts:

Query Field

The available fields for querying vary depending on the area of the Management Portal in which the search is used. On this page, the queries can be done on the following built-in fields:

Username

Complete or partial matches with the username of the user. Keyfactor users (based on Active Directory users), Active Directory groups, and service accounts are included in the grid. For Active Directory users and groups, the username is in the form DOMAIN\username. For service accounts, the username is made up of the username and client hostname entered when the service account key was created (e.g. myapp@appsrvr75). Supports the %ME% token (see Advanced Searches on the next page).

Key Type

A number of cryptographic algorithms can be used to generate SSH keys. Keyfactor Command supports RSA, Ed25519, and ECDSA. RSA keys are more universally supported, and this is the default key type when generating a new key.

Key Length

The key size available when generating a new key depends on the key type selected. Keyfactor Command supports 256 bits for Ed25519 and ECDSA and 2048 or 4096 bits for RSA. The default key length is 2048.

Fingerprint

The fingerprint of the public key. Each SSH public key has a single cryptographic fingerprint that can be used to uniquely identify the key.

Email

The email address of the user requesting the key. This email address is used to alert the user when the key pair is approaching the end of its lifetime (see Key Rotation Alerts on page 193).

Stale Date

The date on which the SSH key pair is considered to have reached the end of its lifetime. By default, the lifetime of an SSH key pair is 365 days (see Application Settings: SSH Tab on page 604). Supports the %TODAY% token (see Advanced Searches on the next page).

Logon Count

The number of Linux logons associated with the user.

Comparison Operator

The query comparison operators vary depending on the type of field selected and the specific properties of the field. The list below shows the dropdown list comparison operators, as well as the equivalent query language syntax (in parentheses).

Most string fields (the vast majority of the built-in fields) support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Contains (-contains)
- Does not contain (-notcontains)
- Starts with (-startswith)
- Ends with (-endswith)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Most date and integer fields support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Is less than (-lt)
- Is less than or equal to (-le)
- Is greater than (-gt)
- Is greater than or equal to (-ge)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Most Boolean (true/false) fields support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Comparison Value

The value you enter for comparison must match the field type. For example, integer fields only support numerical values. String fields support all alphanumeric characters. Boolean fields only support True or False. The value field is not case sensitive. Date fields support only properly formatted dates and will initially display as mm/dd/yyyy. You can choose to populate the date field by:

- Clicking in a date Value field to open a pop-up calendar to select a date that will populate the field.
- Clicking in a segment of the date format (i.e., mm/dd/yyyy) and entering a value. As you continue to type in any one segment, the cursor will keep moving onto the next segment.

The results that match your search criteria will be displayed in the results grid below the search selection options.

Advanced Searches

On any search page you can click **Advanced** to the right of the Search button to display the advanced search options. Click **Simple** to close the advanced search options again.

Multiple Criteria

Using the advanced search options, you can build a query based on multiple criteria using AND/OR logic. As with a simple search, you select a field and comparison operator in the drop-downs and then enter a comparison value, if applicable. Click **Insert** to add the search criteria to the query field below the selection fields. Use the selection fields to build multiple search criteria. Each time you click the insert button, an AND is added between the previous search criteria and the newly added one. You can change the AND to an OR if desired. You can use parentheses around portions of the query along with AND/OR to change the query meaning.

For example, for certificate searches:

```
(CN -contains "appsrvr" AND IssuedDate -ge "01/01/2022") OR (CN -contains "appsrvr" AND
TemplateShortName -contains "web")
```

This query will return all the certificates issued on or after January 1, 2022 with the string appsrvr in the CN and also all certificates issued at any time with the string appsrvr in the CN using a template referencing web. When you have entered all the desired search criteria, click **Search** to execute the query. If you wish to clear the query field and start over, click the **Clear** button.

- %TODAY%
  Use the TODAY special value in place of a specific date in date queries. This option supports math operations, so you can use TODAY-10 or TODAY+30. The built-in *Certificates Expiring in 7 Days* collection uses this special value (see Certificate Collection Manager on page 80).
- %ME%
  Use the ME special value in place of a specific domain\user name in queries that match a domain\user name. The built-in *My Certificates* collection uses this special value (see Certificate Collection Manager on page 80).
- %ME-AN%
  Use the ME-AN special value in place of a specific user name excluding the domain. This is beneficial in environments with multiple domains where there is a desire to query for a user's certificates even if they were requested across multiple domains.

Important: The special query options of %TODAY%, %ME%, and %ME-AN% are only supported in uppercase. Lowercase equivalents (e.g. %me%) cannot be substituted.

2.1.10.5 SSH Permissions

Permissions to use the SSH areas of Keyfactor Command are controlled with three security roles specific to this purpose:

- Enterprise Admin
- Server Admin
- User

Most functions in the Management Portal are available to users with the Server Admin role for SSH. The Enterprise Admin role is used to grant administrators the permission to create server groups and change the owner of a server group (see SSH Server Groups on page 542). Other than these two things, users with the Server Admin role and those with the Enterprise Admin role have the same level of access. Users with the User role (and neither of the SSH admin roles) can access only the My SSH Key page to allow them to generate an SSH key pair for their own use.

Tip: Permissions for the SSH reports and the key rotation alerts (see Key Rotation Alerts on page 193) are covered by the standard reporting and workflow permission roles, not by the specialized SSH permission roles.

Table 19: SSH Permissions Table shows the access users with each of these roles has to the SSH functions within the Management Portal.

Table 19: SSH Permissions Table

Action	SSH Enterprise Admin	SSH Server Admin	SSH User
User Key: Generate and Rotate (My SSH Key)	Yes	Yes	Yes
User Key: Download (My SSH Key)	Yes	Yes	Yes
Service Account Key: View and Search for Service Account Keys	Yes	Limited[1]	No
Service Account Key: Add	Yes	Limited[2]	No
Service Account Key: Edit	Yes	Limited[3]	No
Service Account Key: Delete	Yes	Limited[4]	No
Service Account Key: Download	Yes	Limited[5]	No
Unmanaged Keys: View and Search for Unmanaged Keys	Yes	Yes[6]	No
Unmanaged Keys: Delete	Yes	Yes[7]	No
Server Group: View and Search for Server Groups	Yes	Limited[8]	No
Server Group: Add	Yes	No	No
Server Group: Edit	Yes	Limited[9]	No

[1]Users with the Server Admin role may only view and search for service account keys that are in server groups they own.
[2]Users with the Server Admin role may only create service account keys in server groups they own.
[3]Users with the Server Admin role may only view and edit service account keys that are in server groups they own.
[4]Users with the Server Admin role may only view and delete service account keys that are in server groups they own.
[5]Users with the Server Admin role may only view and download service account keys that are in server groups they own.
[6]Users with the Server Admin role may only view and delete unmanaged keys that are in server groups they own.
[7]Users with the Server Admin role may only view and delete unmanaged keys that are in server groups they own.
[8]Users with the Server Admin role may only view and search for server groups they own.
[9]Only users with the Enterprise Admin role may change the owner of a server group. Users with the Server Admin role may change other settings when editing a server group.

Action	SSH Enterprise Admin	SSH Server Admin	SSH User
Server Group: Delete	Yes	No	No
Server Group: View Members of a Server Group	Yes	Limited[1]	No
Server Group: Edit Access (map an SSH key to a logon for a server group)	Yes	Limited[2]	No
Server: View and Search for Servers	Yes	Limited[3]	No
Server: Add	Yes[4]	Limited[5]	No
Server: Edit	Yes	Limited[6]	No
Server: Edit Access (map an SSH key to a logon on a server)	Yes	Limited[7]	No
Server: Delete	Yes	Limited[8]	No
Logon: View and Search for Logons	Yes	Limited[9]	No
Logon: Add	Yes	Limited[10]	No

[1]Users with the Server Admin role may only view the servers in server groups they own.

[2]Users with the Server Admin role may only map SSH keys from user accounts to Linux logons on servers that are in server groups they own.

[3]Users with the Server Admin role may only view and search for servers that are in server groups they own.

[4]In order to create new servers, these users must also hold the Agent Management - Read role.

[5]Users with the Server Admin role may only create new servers as members of server groups that they own. In order to create new servers, these users must also hold the Agent Management - Read role.

[6]Users with the Server Admin role may only view and edit servers that are in server groups they own.

[7]Users with the Server Admin role may only map SSH keys from user accounts to Linux logons on servers that are in server groups they own.

[8]Users with the Server Admin role may only view and delete servers that are in server groups they own.

[9]Users with the Server Admin role may only view and search for logons that are in server groups they own.

[10]Users with the Server Admin role may only create new logons on servers that are members of server groups that they own.

Action	SSH Enterprise Admin	SSH Server Admin	SSH User
Logon: Edit	Yes	Limited[1]	No
Logon: Edit Access (map an SSH key to a logon)	Yes	Limited[2]	No
Logon: Delete	Yes	Limited[3]	No
User: View and Search for Users	Yes	Limited[4]	No
User: Edit Access (map an SSH key to a logon)	Yes	Limited[5]	No
User: Delete	Yes	Limited[6]	No

2.1.11 System Settings

System Settings are accessed via the settings icon at the top right of the Management Portal.

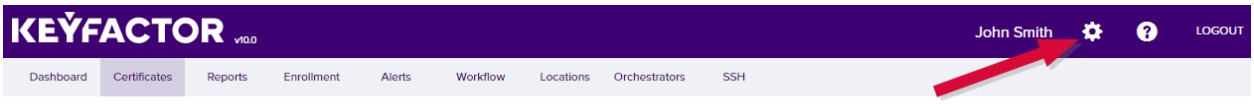


Figure 334: System Settings Icon

The options available in the System Settings section of the Management Portal are:

Application Settings

View or modify settings that control the Keyfactor Command applications.

Security Roles and Identities

Configure security roles to provide customized

Event Handler Registration

Configure built-in or custom event handlers.

Privileged Access Management

Configure PAM providers for use of Privileged Access Management (PAM) to secure certificate

---

[1]Users with the Server Admin role may only view and edit logons that are on servers in server groups they own.
[2]Users with the Server Admin role may only map SSH keys from user accounts to Linux logons on servers that are in server groups they own.
[3]Users with the Server Admin role may only view and delete logons that are on servers in server groups they own.
[4]Users with the Server Admin role may only view and search for users that are associated with logons that are in server groups they own.
[5]Users with the Server Admin role may only map SSH keys from user accounts to Linux logons on servers that are members of server groups that they own.
[6]Users with the Server Admin role may only view and delete users that are associated with logons that are in server groups they own.

levels of access to the Management Portal, configure users and/or groups and grant them access to the roles.

Certificate Store Types

Configure the types of certificate stores available for inventory, management, discovery, and reenrollment operations. This facilitates the creation of custom orchestrators to perform tasks against a wider set of certificate locations.

Certificate Metadata

Create custom metadata fields that can be used to capture additional data about certificates and report or alert based on it.

Audit Log

Display activity (e.g. creation, change, deletion) that has triggered an audit flag on a record in Keyfactor Command affecting an auditable area (e.g. Certificates, Security, Templates, Application Settings).

stores.

SMTP Configuration

Configure email.

Component Installations

View the servers on which Keyfactor Command server software is installed and the components installed on those servers.

Licensing

View or change your Keyfactor Command license.

2.1.11.1 Application Settings

Many of the settings that control the behavior of Keyfactor Command features are configurable from the **Applications Settings** on the System setting menu. Browse to *System Settings Icon* > *Application Settings*. The tables below provide a brief description of these settings.

Each tab of the Applications Settings page is organized into sections—a **General** section and additional sections based on the functionality controlled by each tab. Click the plus (+/−) next to a section to toggle expand/collapse that section.

Depending on your Keyfactor Command license, not all application settings may be applicable in your environment.

Application Settings: Console Tab

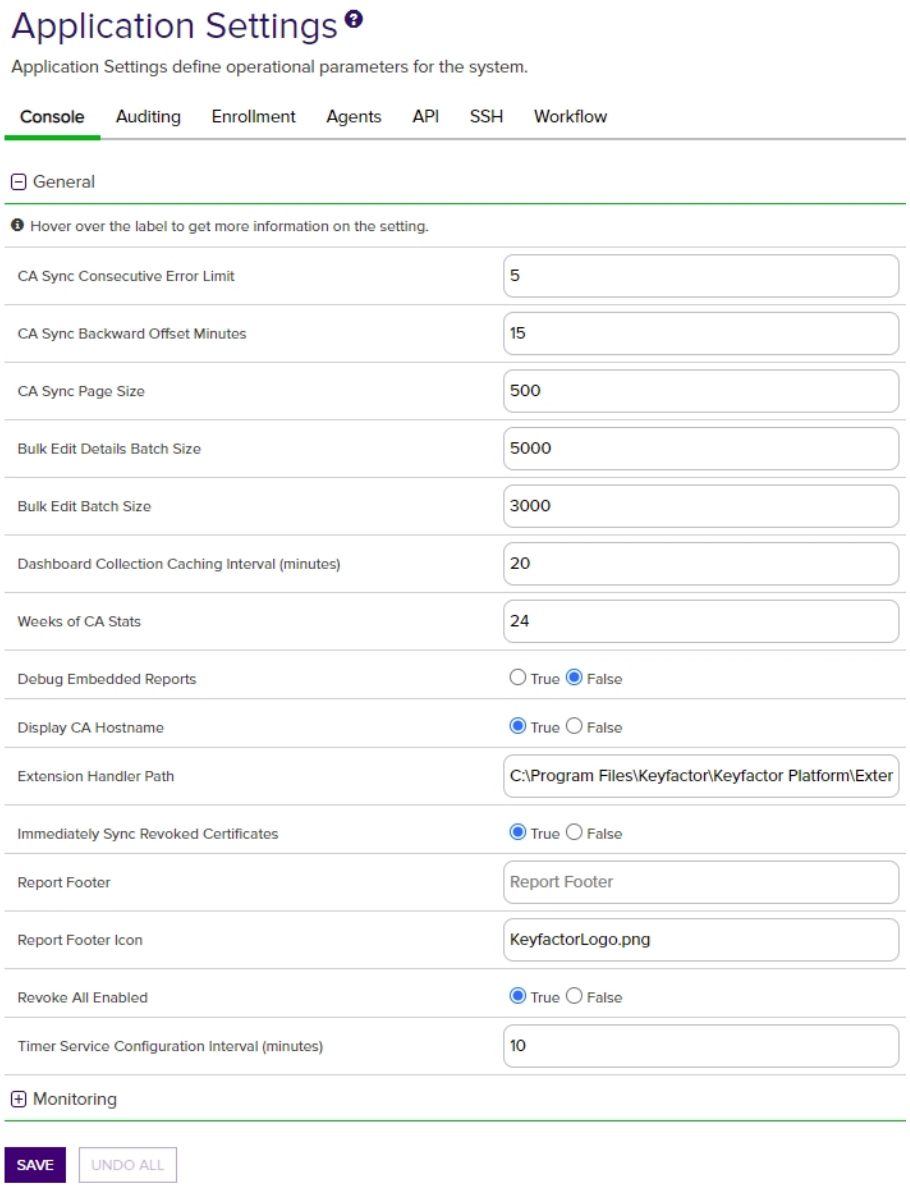


Figure 335: Console Application Settings: General

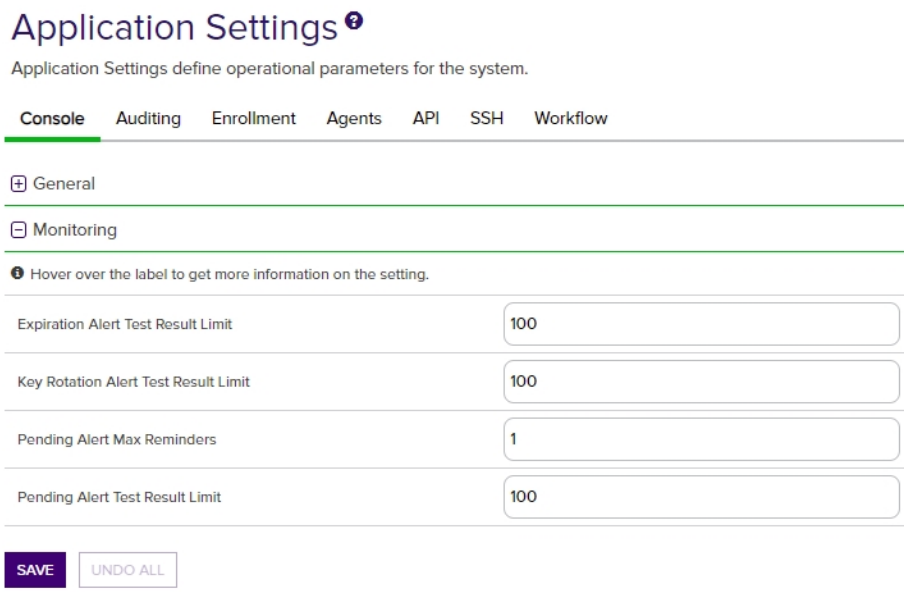
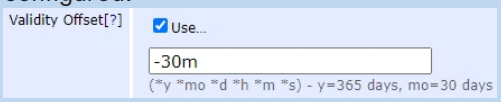


Figure 336: Console Application Settings: Monitoring

Table 20: Console Application Settings

Tab	Section	Field	Description
Console	General	Bulk Edit Details Batch Size	The number of certificates at a time that are read from the database when using the Edit All feature to edit certificate metadata. This setting can be adjusted if there are responsiveness issues when editing large numbers of certificates at once. The default value is 5000.
Console	General	Bulk Edit Batch Size	The number of certificates at a time that are saved to the database when using the Edit All feature to edit certificate metadata. This setting can be adjusted if there are responsiveness issues when editing large numbers of certificates at once. The default value is 3000.
Console	General	CA Sync Consecutive Error Limit	The number of errors a CA synchronization can encounter before the synchronization job stops (without running to completion).
Console	General	CA Sync Backward Offset	The number of minutes to offset when determining whether a certificate requested outside of

Tab	Section	Field	Description
		Minutes	Keyfactor Command should be included in an incremental synchronization. Adjusting this value can be helpful in situations of extreme clock skew or when the EJBCA *Validity Offset* setting is enabled. **Note:** For EJBCA CAs, if the certificate profile has a *Validity Offset* configured to a value greater than the value configured in the *CA Sync Backward Offset Minutes* application setting (15 minutes by default), certificates requested outside of Keyfactor Command will not be picked up on incremental scans. These certificates will only appear in Keyfactor Command on a full synchronization. The *CA Sync Backward Offset Minutes* application setting should be set to the same number of minutes as the *Validity Offset* value, if *Validity Offset* is configured.  *Figure 337: EJBCA Certificate Profile Validity Offset Greater than 15 Minutes*
Console	General	CA Sync Page Size	The number of records at a time that are read from the CA during a CA synchronization job. The default value is 500. **Note:** This setting applies only to EJBCA CAs.
Console	General	Dashboard Collection Caching Interval (minutes)	The number of minutes before data for the Collections dashboard panel is refreshed. The default value is 20.
Console	General	Weeks of CA Stats	The number of weeks of CA data to include in the dashboard graphs. The default value is 24.
Console	General	Debug Embedded	If set to **True**, causes an *Enable Debug* tickbox to

Tab	Section	Field	Description
		Reports	appear on the parameters page for reports you access and run from the Navigator (reports on the Reports menu dropdown of the Management Portal). This option does not appear for reports generated from the Report Manager grid. When enabled it allows the reports to output debug level information when they run. If set to **False**, does not display the *Enable Debug* option. The default value is False. **Tip:** When the debugging option is enabled, a small debug icon ( ) appears at the bottom of reports that generate successfully. You can click on it to see information about the report.
Console	General	Display CA Hostname	If set to **True**, causes both the CA's FQDN and logical name (e.g. ca2.keyexample.com\Corp Issuing CA Two) to display in the CA fields on the Certificate Authority, Certificate Requests and API Applications pages of the Management Portal. If set to **False**, only the CA's logical name (e.g. Corp Issuing CA Two) displays on these pages. The default value is True.
Console	General	Extension Handler Path	The path to the location on the Keyfactor Command server where the event handler .dll files are stored. By default this is: `C:\Program Files\Keyfactor\Keyfactor Platform\ExtensionLibrary\.` As of version 9.0 of Keyfactor Command, PowerShell scripts for alert handlers need to be in the extension path or a subdirectory of it specified by this application setting. For example, create a directory called *Scripts* under the ExtensionLibrary directory and then reference your PowerShell script as *Scripts\MyPowerShell.ps1*. Any scripts referenced by PowerShell handlers that are outside this path will fail to run.

Tab	Section	Field	Description
Console	General	Immediately Sync Revoked Certificates	If set to **True**, causes certificates to immediately sync to Keyfactor Command upon revocation rather than waiting for the next scheduled synchronization cycle. The default value is True.
Console	General	Report Footer	A string that appears at the bottom of Logi-based reports either generated from the Management Portal or generated with the Report Manager in PDF format. The report footer appears only at the very end of the report, not at the foot of every page in the report.
Console	General	Report Footer Icon	The file name of an image to be used at the bottom of each page of exported and scheduled PDF reports. You can use this to replace the Keyfactor logo with a custom image on your reports. The image is auto set to a height of 30px. This image should be placed in the **_SupportFiles** folder under the Logi folder (located at *C:\Program Files\Keyfactor\Keyfactor Platform\Logi* by default).
Console	General	Revoke All Enabled	If set to **True**, causes the Revoke All button to appear at the top of certificate search and collection grids to allow users with appropriate permissions to revoke all certificates shown in the grid or included in the certificate collection. If set to **False**, hides the Revoke All button and disables the POST /Certificates/RevokeAll API endpoint. The default value is False for new installations of Keyfactor Command beginning with release 10.4.
Console	General	Timer Service Configuration Interval (minutes)	The number of minutes between checks by the master scheduling service for changes to the synchronization schedules. Any changes made to this value will not be applied until the Keyfactor Command service is restarted. The default value is 10.
Console	Monitoring	Expiration Alert Test Result Limit	The maximum number of expiration alert emails that will be sent when an expiration alert test is run from within the Management Portal. If the number set here is exceeded during a test, emails will not be sent, but a portion of the alerts will be visible on the

Tab	Section	Field	Description
			expiration alerts test page (see Testing Expiration Alerts on page 166). The default value is 100.
Console	Monitoring	Key Rotation Alert Test Result Limit	The maximum number of key rotation alert emails that will be sent when a key rotation alert test is run from within the Management Portal. If the number set here is exceeded during a test, emails will not be sent, but a portion of the alerts will be visible on the key rotation alerts test page (see Testing Key Rotation Alerts on page 196). The default value is 100.
Console	Monitoring	Pending Alert Test Result Limit	The maximum number of pending alert emails that will be sent when a pending alert test is run from within the Management Portal. If the number set here is exceeded during a test, emails will not be sent, but a portion of the alerts will be visible on the pending alerts test page (see Testing Pending Request Alerts on page 176). The default value is 100.
Console	Monitoring	Pending Alerts Max Reminders	The maximum number of pending alert emails that will be sent for a given pending certificate. Every time a pending alert task is run, an email will be sent for a given pending certificate until the limit is reached. It is recommended that the number is kept at 5 or less. The default value is 1.

Application Settings: Auditing Tab

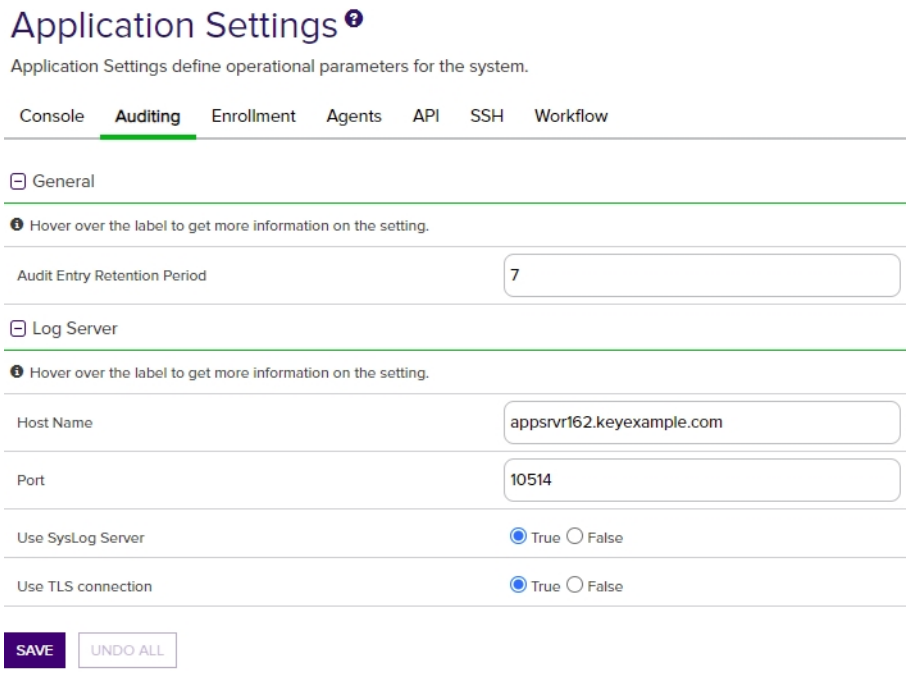


Figure 338: Audit Log Application Settings

Table 21: Audit Log Application Settings

Tab	Section	Field	Description
Auditing	General	Audit Entry Retention Period	The number of years to retain the audit log entry details. The default value is 7. **Note:** The audit log cleanup job runs once daily and removes any audit log entries older than the time specified in the retention parameter except those in the following protected categories: • Security • CertificateCollections • ApplicationSettings • SecurityIdentities • SecurityRoles Audit logs belonging to protected categories

Tab	Section	Field	Description
			are retained indefinitely and cannot be deleted. To retain all audit log entries indefinitely, disable the job in the Keyfactor Command configuration wizard. To do this, in the configuration wizard on the Service tab, uncheck the Everything box and then uncheck the Purge Audit Log History box.
Auditing	Log Server	Host Name	The host name of the centralized logging server to receive the Keyfactor Command audit log entries.
Auditing	Log Server	Port	The port to connect to the centralized logging server. The default port (configurable during install) is 514.
Auditing	Log Server	Use SysLog Server	If set to **True**, enables sending audit log details to a centralized logging server. See Audit Log Output to a Centralized Logging Solution on page 726.
Auditing	Log Server	Use TLS Connection	If set to **True**, enables sending audit log details to a centralized logging server over a TLS connection. See Audit Log Output to a Centralized Logging Solution on page 726.

Application Settings: Enrollment Tab

Note: Regular expressions for enrollment that were previously configured under application settings are now configured on the templates page (see Regular Expressions on page 375).

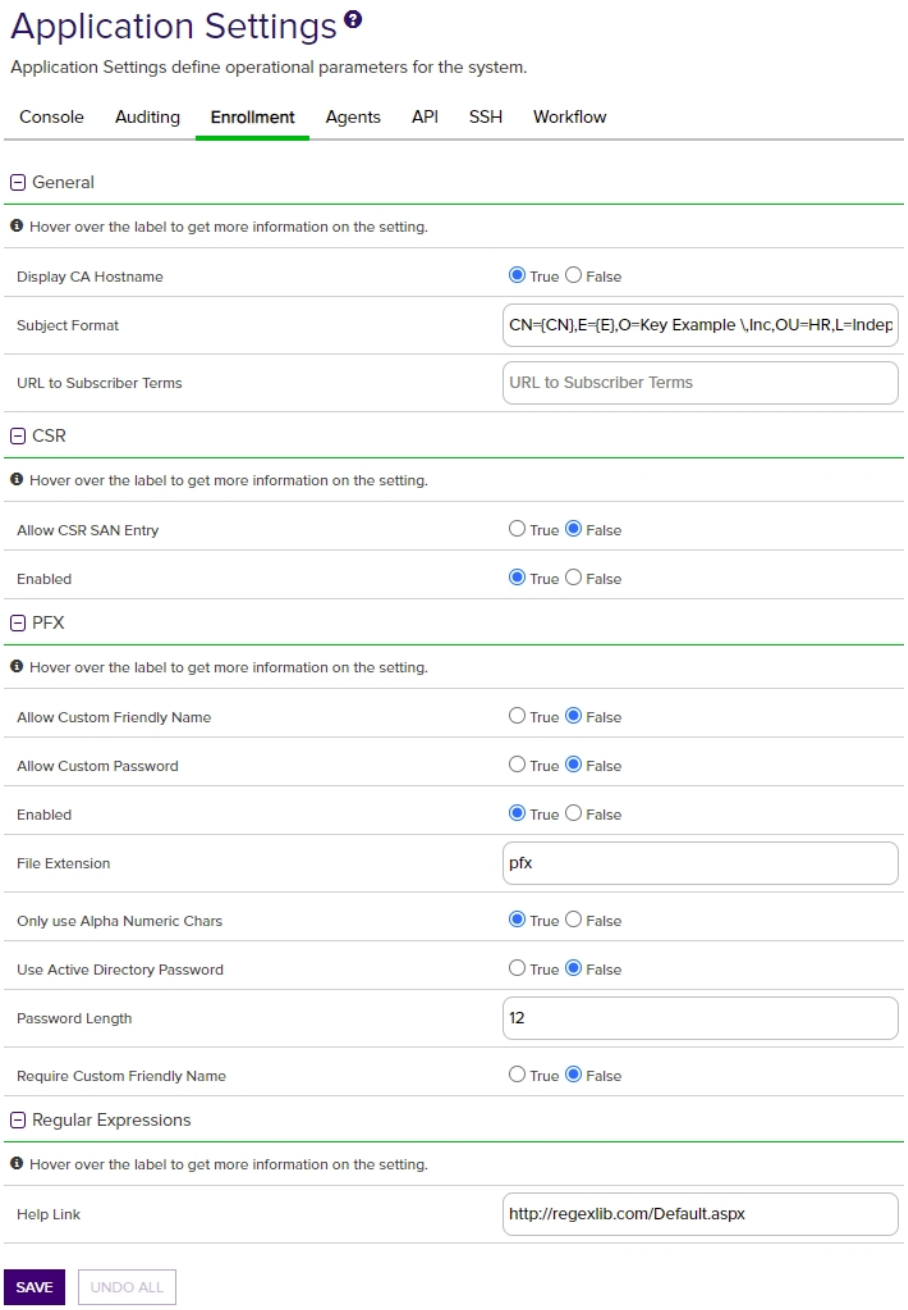


Figure 339: Enrollment Application Settings

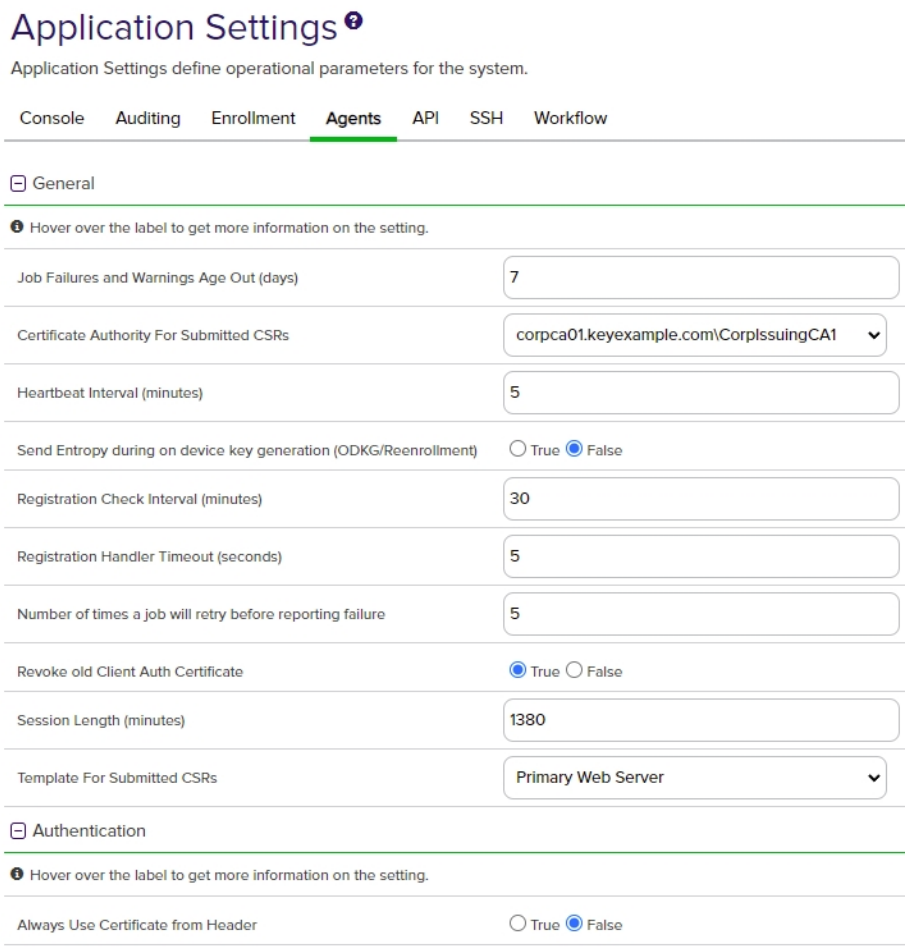
Table 22: Enrollment Application Settings

Tab	Section	Field	Description
Enrollment	General	Display CA Hostname	If set to **True**, causes both the CA's FQDN and logical name (e.g. ca2.keyexample.com\Corp Issuing CA Two) to display in the CA dropdowns in the Keyfactor Command Management Portal interfaces. If set to **False**, only the CA's logical name (e.g. Corp Issuing CA Two) displays in these dropdowns. The default value is True.
Enrollment	General	Subject Format	The format of the subject field that will be created for the certificates requested through the Keyfactor Command Management Portal if the template used for enrollment is set to supply in request. For example: `CN={CN},E={E},O=Key Example\, Inc.,OU={OU},L=Chicago,ST=IL,C=US` The data in the subject format takes precedence over any data entered during PFX enrollment or supplied by enrollment defaults (see Enrollment Defaults Tab on page 370). For example, with the above subject format, the organization for certificates generated through PFX enrollment will always be *Key Example, Inc.* regardless of what is shown on the PFX enrollment page during enrollment. This setting applies to CSRs generated using the CSR generation method in the Keyfactor Command Management Portal, CSR and PFX enrollments done in the Keyfactor Command Management Portal, and to CSR and PFX enrollments done using the Classic API. Data from the default subject *does not* display on the CSR or PFX enrollment page. To define defaults that will display in the PFX enrollment form (and can be modified by users), use enrollment defaults (see Enrollment Defaults Tab on page 370). **Note:** Backslashes are required before any commas embedded within values in the subject field (e.g. O=Key Example\, Inc.). Quotation marks should not be used in the

Tab	Section	Field	Description
			strings in the fields except in the case where these are part of the desired subject value, as they are processed as literal values. **Tip:** The default subject format *does not* apply to enrollments done using the Keyfactor API.
Enrollment	General	URL to Subscriber Terms	The URL for a web page providing terms and conditions to which a user must agree before being allowed to enroll for a certificate if the CA setting of *Require Subscriber Terms* is enabled.
Enrollment	CSR	Allow CSR SAN Entry	If set to **True**, enables the section of the CSR enrollment page that allows for entry of custom subject alternative names (SANs). The default value is False.
Enrollment	CSR	Enabled	If set to **True**, enables administrative CSR enrollment. The default value is True.
Enrollment	PFX	Allow Custom Friendly Name	If set to **True**, enables the section of the PFX enrollment page that allows for entry of a custom friendly name for the certificate. The default value is False.
Enrollment	PFX	Allow Custom Password	If set to **True**, enables the section of the PFX enrollment page that allows for entry of a custom password for the PFX file. The default value is False.
Enrollment	PFX	Enabled	If set to **True**, enables administrative PFX enrollment. The default value is True.
Enrollment	PFX	File Extension	The file extension that will be given to the certificate files. Typical extensions are PFX or P12. The default value is PFX.
Enrollment	PFX	Only use Alpha Numeric Chars	If set to **True**, the one-time password generated to encrypt the PFX file acquired through the Keyfactor Command Management Portal (if the user's Active Directory password is not used) will contain just numbers and letters. If set to **False**, the password will contain numbers, letters and special characters. This setting is ignored if PFX Use Active Directory Pass-

Tab	Section	Field	Description
			word is set to **True**. The default value is True.
Enrollment	PFX	Use Active Directory Password	If set to **True**, uses the user's Active Directory password to encrypt the PFX file containing the certificate acquired through the Keyfactor Command Management Portal and its private key. If set to **False**, generates a one-time password to encrypt the PFX file. The default value is False. ⚠ **Important:** If you change this setting in the application settings you must also change the authentication method configured on the IIS virtual application *KeyfactorPortal* through the IIS Manager. If you set this option to *True*, you should configure only Basic Authentication in IIS. If you set this option to *False*, you may configure either only Windows Authentication or both Basic Authentication and Windows Authentication (the default) in IIS. This is because when you authenticate to the Management Portal using integrated Windows authentication (Kerberos), Keyfactor Command does not have access to your credentials to apply your password to the PFX file.
Enrollment	PFX	Password Length	The number of characters in the one-time password generated to encrypt the PFX file acquired through the Keyfactor Command Management Portal. The minimum number is 8. The default value is 12.
Enrollment	PFX	Require Custom Friendly Name	If set to **True**, requires the user to enter a custom friendly name for the certificate. The default value is False.
Enrollment	PFX	Enable Legacy Encryption	If set to **True**, the historical algorithm set (3DES/SHA1/RC2) is used for PFX enrollments. If set to **False**, the newer algorithm set provided by Windows (AES256/SHA256/AES256) is used instead. The default value is False.

Application Settings: Agents Tab


Application Settings
Application Settings define operational parameters for the system.
Console
Auditing
Enrollment
Agents
API
SSH
Workflow
General
Hover over the label to get more information on the setting.
Job Failures and Warnings Age Out (days)
7
Certificate Authority For Submitted CSRs
corpca01.keyexample.com\CorpIssuingCA1
Heartbeat Interval (minutes)
5
Send Entropy during on device key generation (ODKG/Reenrollment)
True
False
Registration Check Interval (minutes)
30
Registration Handler Timeout (seconds)
5
Number of times a job will retry before reporting failure
5
Revoke old Client Auth Certificate
True
False
Session Length (minutes)
1380
Template For Submitted CSRs
Primary Web Server
Authentication
Hover over the label to get more information on the setting.
Always Use Certificate from Header
True
False

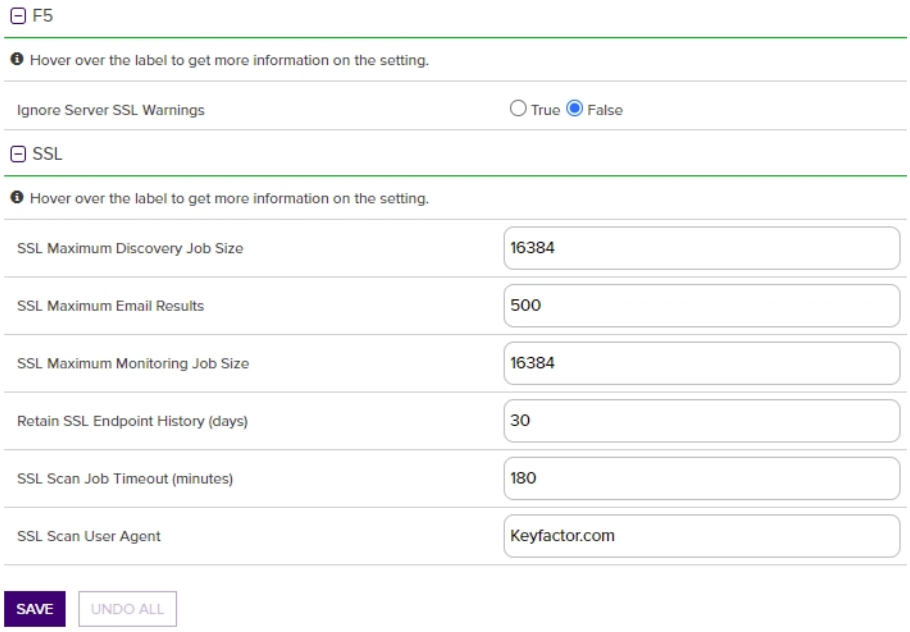


Figure 340: Agents Application Settings

Table 23: Agents Application Settings

Tab	Section	Field	Description
Agents	General	Job Failures and Warnings Age Out (days)	The number of days orchestrator job failures and warnings should be included in the count of failures on the orchestrator job history tab. The default value is 7.
Agents	General	Certificate Authority For Submitted CSRs	The certificate authority used for reenrollment requests made from the Certificate Stores page. See Certificate Store Reenrollment on page 412.
Agents	General	Heartbeat Interval (minutes)	The frequency, in minutes, with which an orchestrator (e.g. Keyfactor Universal Orchestrator, Keyfactor Java Agent or Keyfactor Mac Auto-Enrollment Agent) should query the Keyfactor Command orchestrator server for a status on the accuracy of its jobs list. The default value is 5.

Tab	Section	Field	Description
Agents	General	Send Entropy during on device key generation (ODKG/Reenrollment)	Whether the configure call returns the property *Entropy* containing 2048 bytes. This property is optional via this app setting. The default is false on upgrades and new installs.
Agents	General	Registration Check Interval (minutes)	The frequency, in minutes, with which an orchestrator should check with the Keyfactor Command server to see if it has been approved as an orchestrator. The default value is 30.
Agents	General	Registration Handler Timeout (seconds)	The maximum number of seconds an auto-registration handler is allowed to attempt to run before being halted and declared to be deferred. The default value is 90 for more recently installed systems. Keyfactor recommends using a value of at least 60 seconds.
Agents	General	Number of times a job will retry before reporting failure	The number of times an orchestrator job will attempt to retry running if it encounters an error before failing. The default value is 5.
Agents	General	Revoke old Client Auth Certificate	If set to **True**, revokes the previous certificate used for orchestrator client certificate authentication after the certificate has successfully been renewed using the client certificate authentication renewal extension. The default value is True.
Agents	General	Session Length (minutes)	The frequency, in minutes, with which an orchestrator renews its session with the Keyfactor Command server and obtains a new session token in the absence of any other reason for the orchestrator to renew the session token. The session token is also renewed when an orchestrator job changes (e.g. an inventory schedule changes, a certificate is scheduled for addition to a certificate store, or

Tab	Section	Field	Description
			a certificate is scheduled for removal from a store) or the orchestrator is restarted. The default value is 1380.
Agents	General	Template For Submitted CSRs	The template used for reenrollment requests made from the Certificate Stores page. See Certificate Store Reenrollment on page 412. The template selected for this value must be available for enrollment against the CA listed in the Certificate Authority For Submitted CSRs setting.
Agents	Authentication	Always Use Certificate from Header	If set to **True**, the orchestrator will be authenticated using the client certificate provided in the header from the orchestrator rather than client certificate used to make the connection to Keyfactor Command. This is useful in configurations where one certificate is used to authenticate the orchestrator to a proxy and a second certificate is used to authenticate the proxy to Keyfactor Command. The original certificate from the orchestrator can be preserved in the header to present to Keyfactor Command for authentication. The default value is False.
Agents	F5	Ignore Server SSL Warnings	If set to **True**, the orchestrator will connect to the F5 device using SSL even if it detects a problem with the certificate on the F5 device (e.g. it doesn't trust the issuer of the certificate because the certificate is self-signed). This option applies only to the F5 methods based on the F5 SOAP API (see Certificate Stores on page 380). The F5 methods based on the F5 iControl REST API automatically ignore SSL warnings without the need to set this option. The default value is False.

Tab	Section	Field	Description
Agents	SSL	SSL Maximum Discovery Job Size	The maximum number of endpoints for scanning that will be assigned to any one orchestrator for a given discovery scan job part. Together with the *SSL Scan Job Timeout* setting, this can be used to fine tune the running of SSL discovery scan jobs. The default value is 16,384. **Note:** A change made to this setting takes effect with the next discovery scan job. It does not affect currently running jobs.
Agents	SSL	SSL Maximum Email Results	The maximum number of results to display in an SSL monitoring results email message table of certificates that have expired or are expiring shortly. The default value is 500.
Agents	SSL	SSL Maximum Monitoring Job Size	The maximum number of endpoints for scanning that will be assigned to any one orchestrator for a given monitoring scan job part. Together with the *SSL Scan Job Timeout* setting, this can be used to fine tune the running of SSL monitoring scan jobs. The default value is 16,384. **Note:** A change made to this setting takes effect with the next monitoring scan job. It does not affect currently running jobs.
Agents	SSL	Retain SSL Endpoint History (days)	The number of days old an endpoint history record must be before it is available for deletion by the endpoint history cleanup process. Endpoint history records older than this will be retained if they are the last records for the given endpoint. Both the last discovery and last monitoring records will be retained regardless of age. The default value is

Tab	Section	Field	Description
			30.
Agents	SSL	SSL Scan Job Timeout (minutes)	The maximum number of minutes any one orchestrator is allowed to attempt to run an SSL scan job before the job for that orchestrator is abandoned and given to the next orchestrator in the orchestrator pool to run (if applicable). The default value is 180. **Note:** A change made to this setting takes effect immediately. It applies to currently running jobs as well as future jobs.
Agents	SSL	SSL Scan User Agent	Defines what is sent to endpoints when Request Robots.txt is enabled on a SSL Network.

Application Settings: API Tab

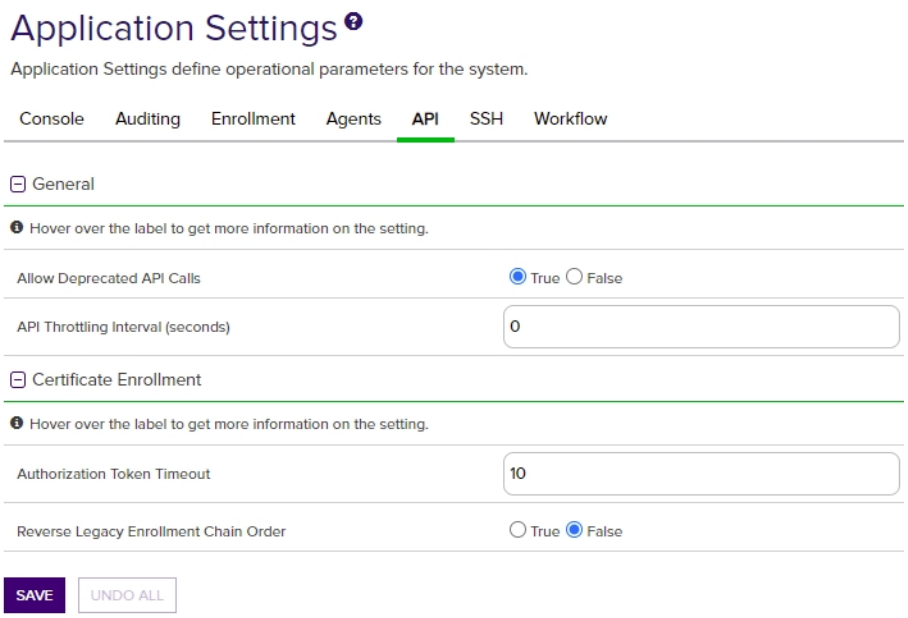


Figure 341: API Application Settings

Table 24: API Application Settings

Tab	Section	Field	Description
API	General	Allow Deprecated API Calls	If set to **False**, API applications will not be able to access earlier versions of API methods or other legacy API methods that have been replaced or updated. Many of the updated methods offer additional security measures, so this setting can reduce the risk of unauthorized API access, but may cause API applications written against these earlier versions to stop functioning correctly. If you do not have any such applications, this should be set to **False**. The default is True. For more information, see *Versioning* in the *Keyfactor Web APIs Reference Guide*.
API	General	API Throttling Interval (seconds)	The maximum rate at which API applications can make requests to the API. A larger value will mitigate risks from certain denial of service and brute-force/-dictionary attacks, but will limit the performance of applications needing to make multiple API calls. This can be set to zero to disable throttling.
API	Certificate Enrollment	Authorization Token Timeout	The number of minutes for which a token (from a GET token request such as GET /CertEnroll/1/Token) is valid as an HTTP request header for authentication. This setting also controls the number of minutes in the past a /CertEnroll/3 request timestamp can be and still be accepted.
API	Certificate Enrollment	Reverse Legacy Enrollment Chain Order	If set to **True**, switches the order of the certificates returned in the certificate chain from an enrollment request with the Classic API (such as a POST /CertEnroll/3/Pkcs10 request). For example, if the certificates are being returned with the CA's root certificate as the first certificate in the list and the end entity certificate as the last certificate in the list while this value is **False**, changing this value to **True** will cause the certificates to be returned with the end entity certificate first in the list and the CA's root certificate last in the list. The default value is False.

Application Settings: SSH Tab

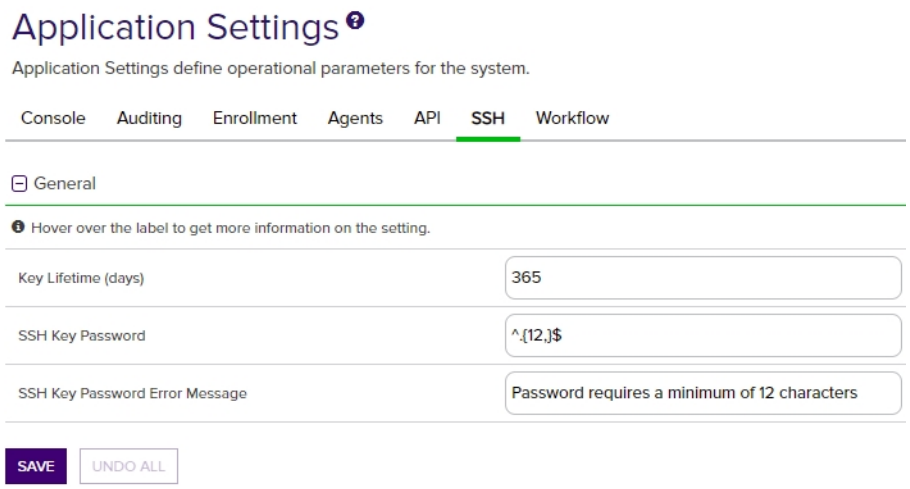


Figure 342: SSH Settings

Table 25: SSH Application Settings

Tab	Section	Field	Description
SSH	General	Key Lifetime (days)	The number of days for which an SSH key generated through My SSH Key (see Generating a New Key on page 518) or Service Account Keys (see Creating a Service Account Key on page 527) is considered valid. The default is 365 days.
SSH	General	SSH Key Password	The regular expression against which the password entered when creating, rotating or downloading keys for both user SSH keys (My SSH Key on page 512) and service account SSH keys (Service Account Keys on page 524) will be validated. The default is a minimum of 12 characters configured as: `^.{12,}$`
SSH	General	SSH Key Password Error Message	The error message displayed to the user in the relevant SSH pages of the Keyfactor Command Management Portal when the password referenced does not match the regular expression defined for the password using the SSH Key Password setting.

Application Settings: Workflow Tab

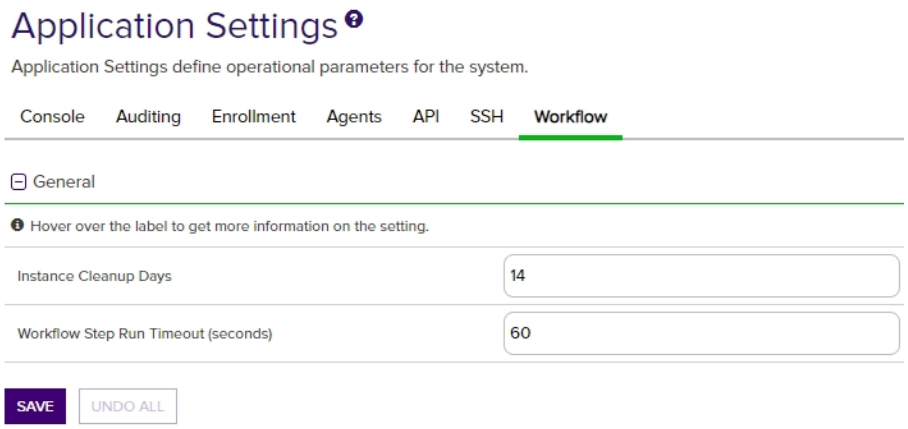


Figure 343: Workflow Settings

Table 26: Workflow Application Settings

Tab	Section	Field	Description
Workflow	General	Workflow Step Run Timeout (seconds)	The number of seconds a workflow instance step will be allowed to run before timing out and setting the instance to a status of Failed. The default is 60 seconds.
Workflow	General	Instance Cleanup Days	The number of days to retain completed workflow instances (successful or failed) before they are purged. The cleanup job runs daily at midnight. The default value is 14.

Tip: Click the help icon (?) next to the page title to open the embedded web copy of the *Keyfactor Command Documentation Suite* to this section.
You can also find the help icon at the top of the page next to the **Log Out** button. From here you can choose to open either the *Keyfactor Command Documentation Suite* at the home page or the *Keyfactor API Endpoint Utility*.

2.1.11.2 Security Overview

There are several elements that make up Keyfactor Command Security infrastructure. To define your security design you will use these elements in combinations that meet your needs. You can limit user menu access through global permissions, and user certificate access through collection and certificate stores permissions.

- Security Roles—Menu and Certificate Permissions

  Define the naming convention and structure of your security design by creating a name and description for your roles. These roles will then hold the definition of your security design based on the menu access, collection access or stores access as applied to them. The roles will then be applied to AD users or groups to complete the security set-up. These roles are used to:

  - Grant access to the Management Portal, by selecting menu access permissions for a role—at what level of permission the user/group can access certificates functionality on the Keyfactor Command management portal. See Security Role Permissions on page 611 and Security Role Operations on page 628.
  - Grant certificate collections access by selecting role permissions per collection—at which level of permission the user/group can access collections functionality and/or which collections they can access. See Certificate Permissions on page 621.
  - Grant certificate store containers access by selecting role permissions per container—at which level of permission the user/groups can access certificate stores functionality, and/or which stores they can access. See Container Permissions on page 624.
- Security Identities

  Assign combinations of **Roles** to AD users or groups to apply your security design to your users. See Security Identity Operations on page 632.
- SSH Permissions

  Permissions to use the SSH areas of Keyfactor Command are controlled with three security roles (See SSH Permissions on page 579) specific to this purpose:

  - Enterprise Admin
  - Server Admin
  - User

Keyfactor Command Security Design Considerations

- Determine the list of users or groups who will have access to Keyfactor Command. Access in Keyfactor Command is based on Active Directory users and groups. These will be used to create **Security Identities** in Keyfactor Command (using the *DOMAIN\group name* format) to which **Security Roles** will be assigned.

  Note: If you require only one layer of security (all users will have full access) you can simply use the Administrator Role that was created during installation (see *Install the Main Keyfactor Command Components on the Keyfactor Command Server(s): Keyfactor Portal Tab Administration Section* in the *Keyfactor Command Server Installation Guide*).

  Note: When defining the AD groups/users you will use to form **Identities**, consider whether you will have a one-to-one or one-to many relationship between **Identities** and **Roles**.

- Define the naming convention for **Security Roles**. Menu access and certificate security will be assigned to **Roles** which in turn will be applied to **Security Identities.**
- Determine the Keyfactor Command menu access and level of functionality you want to apply to each **Role** using the permissions information found Security Role Permissions on page 611.
- Determine certificate security based on collections and certificate store permissions based on containers, if any. See below for more information.

Certificate Store Container Permissions

When designing a container permission scheme, you need to think first about whether you want your users to have access to all the certificate stores in your Keyfactor Command database or whether you need to limit your users to having access to only a subset of your stores. If you're comfortable granting access to all the stores, you can use the global Read permission. If you're not comfortable with this, you need to use container-level permissions and grant Read permissions on a container-by-container basis. These can be granted separately on a group-by-group (or user-by-user) basis, so group A can be granted global Read while group B is only granted Read to a certain container.

Next, you need to think about what you want your users to be able to do with the stores they have access to. By granting Read access to the stores, you're allowing your users to browse to the certificate stores page and see all the stores and containers that they've been granted access to, but they can perform no operations related to the stores. These are controlled with additional permissions (see below) that can also be set either globally or on a container-by-container basis. You can combine global and container-level security.

Example: You've decided that you need to use container-level security at the *Read* level on three different containers rather than granting global *Read* to your Web Server Managers group. You want these users to be able to push new certificates out to certificate stores in the IIS Personal, PEM and Java containers but not to stores on your F5 and NetScaler devices. You could either grant them the *Schedule* permission on a container-by-container basis or you could grant them the global *Schedule* permission for Certificate Store Management. Since the users have neither the global *Read* permission nor container permission for the containers for the F5 and NetScaler devices, these two settings would accomplish the same goal.

In addition to the permissions that must be considered when designing a permission scheme for certificate stores, you must also give consideration to permissions for certificates. Users must have permissions to certificates in order to use the certificate store operations. See Certificate Permissions on page 621 and Container Permissions on page 624.

Note: Setting permissions on a container-by-container basis automatically grants the lower permissions (e.g. setting *Schedule* automatically grants *Read*). The same is not true for permissions set at the global level.
Any containers that do not have container-by-container permissions applied fall back to the global permissions, if any global permissions have been set.

Certificate and Collection-by-Collection Permissions

When designing a certificate permission scheme, you need to think first about whether you want your users to have access to all the certificates in your Keyfactor Command database or whether you need to limit your users to having access to only a subset of your certificates. If you're comfortable granting access to all the certificates, you can use the global Read permission. If you're not comfortable with this, you need to use collection-level permissions and grant Read permissions on a collection-by-collection basis. These can be granted separately on a group-by-group (or user-by-user) basis, so group A can be granted global Read while group B is only granted Read to a certain collection.

Next, you need to think about what you want your users to be able to do with the certificates they can view. There are certificate operation permissions (see Certificate Permissions on page 621) that you can set that control what your users can do with the certificates. These can be set either globally or on a collection-by-collection basis. You can combine global and collection-level security.

Example: You've decided that you need to use collection-level security at the Read level on four different collections to grant Read access to your PKI Help Desk group and will not grant them global Read permissions. You also want these users to be able to edit the metadata fields of the certificates in all four of these collections. You could either grant them the Edit Metadata permission on a collection-by-collection basis or you could grant them the global Edit Metadata permission. Since the users don't have the global Read permission (and thus can't read the other collections), these two settings would accomplish the same goal.

At the global level, the **Certificates** Read role permission grants access to both the certificate search page and all certificate collections. Users who have been granted only collection-level Read permissions and not global Read permissions have access only to the collections to which they have been granted access and not to the certificate search page. See Security Role Permissions on page 611 and Certificate Permissions on page 621.

In addition to the **Certificates** role permissions that must be considered when designing a permission scheme for certificates, you must also give consideration to the **Certificate Collections** and **Certificate Store Management** global role permissions.

- Enabling the Certificate Collections Modify global role permission allows users to use the Save, Save As and Delete buttons for a collection. This allows users to create new certificate collections based on existing collections (Save As), delete existing collections (Delete), or modify select settings about an existing collection (Save). Typically, Certificate Collections permissions would only be granted to users who also had at least global Read permissions to allow them to do certificate searches from which to create new collections.
- You will need to consider the Certificate Store Management role permissions if you use certificate stores and want any of your limited access users to make use of the Add to Certificate Store, Remove from Certificate Store, or Renew/Reissue operations on certificates. These certificate operations are only available to users who have also been granted the Read and Schedule role permissions for Certificate Store Management. Permissions to certificate stores can be

granted either globally or via container security (see Certificate Permissions on page 621 and Container Permissions on page 624).

Security Roles and Identities

Security Roles are used in conjunction with Security Identities to define much of the user access to entities within Keyfactor Command. From the *Securities Roles and Identities* page you can view the lists of security roles and security identities and manage your security configuration. For more information on security considerations in Keyfactor Command see Keyfactor Command Security Design Considerations on page 606.

Security Roles

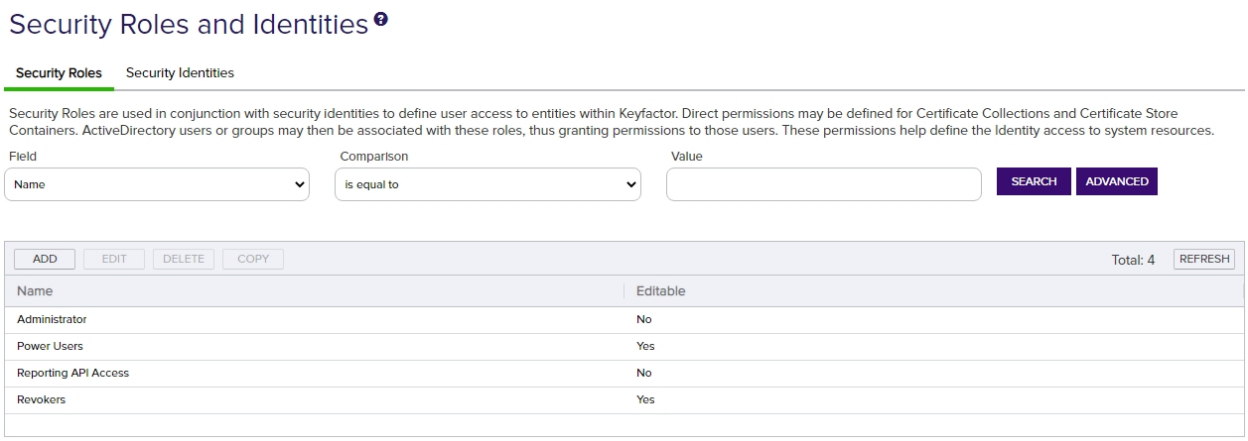


Figure 344: Security Roles

During the Keyfactor Command installation and configuration process, the security role **Administrators** is created (see *Install the Main Keyfactor Command Components on the Keyfactor Command Server(s): Keyfactor Portal Tab Administration Section* in the *Keyfactor Command Server Installation Guide*). The **Administrators** role grants full permissions to the Management Portal and cannot be edited or deleted. If all users of the Management Portal should have full access to all features within the portal, this one role will be sufficient for your needs. However, if you would like to grant access to other users but limit the functionality available to those users, you need to add one or more new security roles for this purpose.

A **Reporting API Access** role is automatically created during installation to support the dashboard and reporting access required by the Logi Analytics Platform. The service account used for the IIS application pool on the Keyfactor Command Management Portal server (where Logi is installed) is automatically created as an identity and associated with this role if you've opted to use integrated Windows authentication. If you've opted to use basic authentication, the user you enter on the Dashboard and Reporting tab of the configuration wizard in the *Keyfactor API User* field will be created as an identity and associated with this role.

Configuring security roles within Keyfactor Command (see Security Role Operations on page 628) has several effects. These roles are used to:

- Grant access to the Management Portal, by selecting menu access permissions for a role. See Security Role Permissions on the next page.
- Grant certificate collections access by selecting role permissions per collection. See Certificate Permissions on page 621.
- Grant certificate store containers access by selecting role permissions per container. You can set and view the role container permissions from the Container Permissions page. See Container Permissions on page 624.

Note: For the most part, when you grant Modify role permissions to an area in the Management Portal, you must also grant Read role permissions to that same area for that security role to receive full functionality. Granting Modify without Read to a user or a group can result in unexpected behavior. See also Certificate Permissions on page 621.

Security roles affect the Management Portal and the APIs only.

Security roles for SSH key management are structured somewhat differently than those for most of the rest of the product set, as they don't use the standard Read and Modify convention. For more information, see SSH Permissions on page 579.

Security Identities

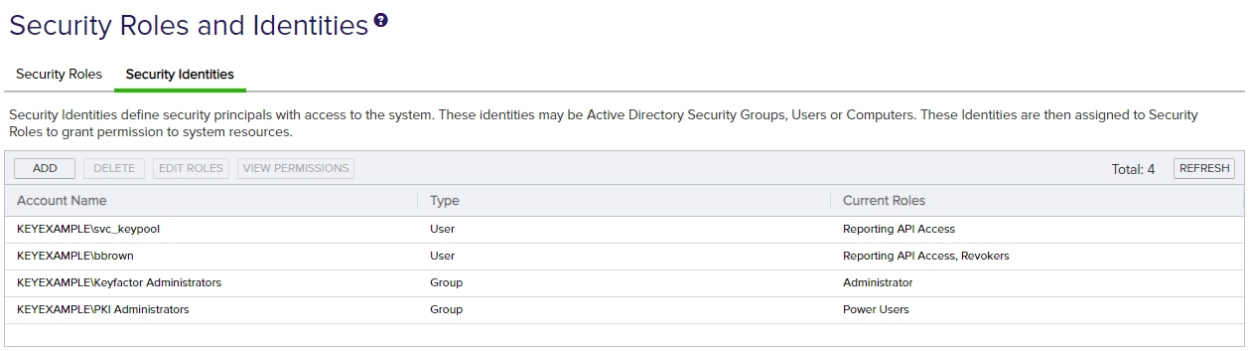


Figure 345: Security Identities

Identities are created in Keyfactor Command using Active Directory users or groups. During the Keyfactor Command installation and configuration process, administrative security identities are created using the Active Directory user or group record you entered on the Keyfactor Portal tab of the configuration wizard in the *Administrative Users* field (see *Install the Main Keyfactor Command Components on the Keyfactor Command Server(s): Keyfactor Portal Tab Administration Section* in the *Keyfactor Command Server Installation Guide*). More than one user or group may be entered during configuration, if desired. Identities entered in the configuration wizard are associated with the **Administrators** role that grants all permissions to the Management Portal.

If you would like to grant access to other users but limit the functionality available to those users, you need to add one or more new security identities for this purpose and link them to one or more appropriate security roles. See Security Identity Operations on page 632.

Tip: Click the help icon (?) next to the page title to open the embedded web copy of the *Keyfactor Command Documentation Suite* to this section.
You can also find the help icon at the top of the page next to the **Log Out** button. From here you can choose to open either the *Keyfactor Command Documentation Suite* at the home page or the *Keyfactor API Endpoint Utility*.

Security Role Permissions

The Security Role Permissions that are available to be assigned to security roles within Keyfactor Command are documented below.

Agent Auto-Registration

Table 27: Agent Auto-Registration Security Role Permissions

UI Permission	API Permission	Description
Read	AgentAutoRegistration: *Read*	Users can view the orchestrator auto-registration settings; users must also have *Read* permissions for Agent Management to access this page in the Management Portal.
Modify	AgentAutoRegistration: *Modify*	Users can modify the orchestrator auto-registration settings.

Agent Management

Table 28: Agent Management Security Role Permissions

UI Permission	API Permission	Description
Read	AgentManagement: *Read*	Users can: • View orchestrators, including filtering the Orchestrator Management grid • View orchestrator jobs, including status, schedules, failures and warnings
Modify	AgentManagement: *Modify*	Users can: • Manage orchestrators, including approving and disapproving them • Unschedule and reschedule orchestrator jobs

Alerts

Table 29: Alerts Security Role Permissions

UI Permission	API Permission	Description
Read	WorkflowManagement: *Read*	Users can view the pending, issued, and denied workflow alerts.
Modify	WorkflowManagement: *Modify*	Users can modify the pending, issued, and denied workflow alerts, including the alert text, recipients, and event handlers. Users can also add new alerts, delete alerts, and configure the pending alert delivery schedule.
Test	WorkflowManagement: *Test*	Users can test the pending alerts, including sending email to recipients. Users must also have Read permissions for Alerts.

API

Table 30: API Security Role Permissions

UI Permission	API Permission	Description
Read	API: *Read*	Users can call the Classic (CMS) API endpoints. This permission is not needed to use the Keyfactor API endpoints.

Application Settings

Table 31: Application Settings Security Role Permissions

UI Permission	API Permission	Description
Read	ApplicationSettings: *Read*	Users can view the application settings.
Modify	ApplicationSettings: *Modify*	Users can modify the application settings.

Auditing

Table 32: Auditing Security Role Permissions

UI Permission	API Permission	Description
Read	Auditing: *Read*	Users can access the Audit Log page in the Management Portal,

UI Permission	API Permission	Description
		and will be able to make API requests to obtain data from the audit log (query, etc.). The System Settings dropdown menu will display the Audit Log option to users with the **Auditing** Read permission.

Certificate Collections

Table 33: Certificate Collections Security Role Permissions

UI Permission	API Permission	Description
Modify	CertificateCollections: *Modify*	Users can add or edit Certificate Collections. See Certificate Permissions on page 621 for more information.

Certificate Enrollment

Table 34: Certificate Enrollment Security Role Permissions

UI Permission	API Permission	Description
Enroll PFX	CertificateEnrollment: *EnrollPFX*	Users can use the PFX Enrollment page in the Management Portal and the equivalent API functions.
Enroll CSR	CertificateEnrollment: *EnrollCSR*	Users can use the CSR Enrollment page in the Management Portal and the equivalent API functions.
CSR Generation	CertificateEnrollment: *CsrGeneration*	Users can use the CSR Generation page in the Management Portal and the equivalent API functions.
Manage Pending CSRs	CertificateEnrollment: *PendingCsr*	Users can use the Pending CSRs page in the Management Portal and the equivalent API functions.

Certificate Metadata Types

Table 35: Certificate Metadata Types Security Role Permissions

UI Permission	API Permission	Description
Read	CertificateMetadataTypes: *Read*	Users can read custom metadata attribute definitions on the Certificate Metadata page in the Management Portal and the equivalent API functions.
Modify	CertificateMetadataTypes:	Users can add, edit, and delete custom metadata

UI Permission	API Permission	Description
	Modify	attribute definitions on the Certificate Metadata page in the Management Portal and the equivalent API functions.

Certificate Requests

Table 36: Certificate Requests Security Role Permissions

UI Permission	API Permission	Description
Manage	WorkflowManagement: *Participate*	Users can participate in the pending, issued, and denied alerts by approving or denying certificate requests from the Certificate Requests page, from the individual pages reached from links included in alerts, or using the Keyfactor API /Workflow/Certificates endpoints. **Note:** In previous versions of Keyfactor Command, this permission was *Workflow Management: Participate*.

Certificate Store Management

Table 37: Certificate Store Management Security Role Permissions

See Container Permissions on page 624, Certificate Operations on page 42, Certificate Store Types on page 635 and Certificate Store Operations on page 385 for more information.

UI Permission	API Permission	Description
Read	CertificateStoreManagement: *Read*	Users can view the certificate stores and containers tabs on the *Locations > Certificate Stores* menu, and view certificate store types.
Schedule	CertificateStoreManagement: *Schedule*	Users can add certificates to certificate stores, renew/reissue certificates, schedule and remove certificates from certificate stores.
Modify	CertificateStoreManagement: *Modify*	Users can manage all operations regarding certificate stores—including the stores, containers, and discovery process—and certificate store types.

Certificates

Table 38: Certificates Security Role Permissions

UI Permission	API Permission	Description
Read	Certificates: *Read*	Users can view certificates, including certificate history, and can download certificates. Users who also have Read permissions for Certificate Store Management or container permissions can add certificates to certificate stores from Certificate Search and Certificate Collections. See Certificate Permissions on page 621 for more information.
Edit Metadata	Certificates: *EditMetadata*	Users can modify certificate metadata for certificates accessed through Certificate Search and Certificate Collections in the Management Portal and the equivalent API functions.
Import	Certificates: *Import*	Users can import certificates using the Management Portal Add Certificate page or the Keyfactor API POST /Certificates/Import method. Users who also have Read permissions for Certificate Store Management or container permissions can add certificates to certificate stores from Add Certificate.
Download with Private Key	Certificates: *Recover*	Users can download the certificates with their private key.
Revoke	Certificates: *Revoke*	Users can revoke certificates through Keyfactor Command.
Delete	Certificates: *Delete*	Users can delete certificates and, if applicable, the private keys of the certificates from the Keyfactor Command database.
Import Private Key	Certificates: *ImportPrivateKey*	Users can save the private key for the certificate in the Keyfactor Command database.

Dashboard

Table 39: Dashboard Security Role Permissions

UI Permission	API Permission	Description
Read	Dashboard: *Read*	Users can view the panels on their personalized dashboard and add and remove them.
Risk Header	Dashboard: *RiskHeader*	Users can view the risk header at the top of the dashboard.

Event Handler Registration

Table 40: Event Handler Registration Security Role Permissions

UI Permission	API Permission	Description
Read	EventHandlerRegistration: *Read*	Users can view the event handler registration settings.
Modify	EventHandlerRegistration: *Modify*	Users can modify the event handler registration settings.

Mac Auto-Enroll Management

Table 41: Mac Auto-Enroll Management Security Role Permissions

UI Permission	API Permission	Description
Read	MacAutoEnrollManagement: *Read*	Users can view the Mac Auto-Enroll Management settings.
Modify	MacAutoEnrollManagement: *Modify*	Users can modify the Mac Auto-Enroll Management settings.

Management Portal

Table 42: Management Portal Security Role Permissions

UI Permission	API Permission	Description
Read	AdminPortal: *Read*	Users can access the Management Portal. This permission must be enabled for all roles that will access the Management Portal.

Monitoring

Table 43: Monitoring Security Role Permissions

UI Permission	API Permission	Description
Read	Monitoring: *Read*	Users can view the expiration alerts in the Certificate Alerts in the Management Portal and the equivalent API functions, including the alert schedule.
Modify	Monitoring:	Users can modify the expiration alerts, including the alert text,

UI Permission	API Permission	Description
	Modify	recipients and event handlers. Users can also add new alerts, delete alerts and configure the expiration alert delivery schedule.
Test	Monitoring: *Test*	Users can test the expiration alerts, including sending email to recipients. Users must also have Read permissions for Monitoring to access this in the Management Portal.

PKI Management

Table 44: PKI Management Security Role Permissions

UI Permission	API Permission	Description
Read	PkiManagement: *Read*	Users can view PKI management settings within: • Certificate Authorities • Certificate Templates • Revocation Monitoring
Modify	PkiManagement: *Modify*	Users can modify PKI management settings to: • Import, add, edit, and delete certificate authorities • Import and edit certificate templates • Add, edit, delete, and test revocation monitoring endpoints • Configure revocation monitoring schedule • Configure revocation monitoring recipients

Privileged Access Management

Table 45: Privileged Access Management Security Role Permissions

UI Permission	API Permission	Description
Read	PrivilegedAccessManagement: *Read*	Users can view PAM providers.
Modify	PrivilegedAccessManagement: *Modify*	Users can add, edit, and delete PAM providers.

Reports

Table 46: Reports Security Role Permissions

UI Permission	API Permission	Description
Read	Reports: *Read*	Users can generate and view reports.
Modify	Reports: *Modify*	Users can modify the delivery schedule for reports in Report Manager in the Management Portal and the equivalent API functions and add, edit, and delete custom reports. **Note:** Report scheduling is limited by collection permissions. Users in roles that have *Reports: Read and Modify* permissions will also need to have *Read* collection permissions on individual collections to have the ability to add, edit, and delete schedules associated with collections. The user will not have access to add, edit, and delete schedules for any collections for which they do not have collection *Read* permissions in addition to *Reports* permissions.

Security Settings

Table 47: Security Settings Security Role Permissions

UI Permission	API Permission	Description
Read	SecuritySettings: *Read*	Users can view the settings for Security Roles and Security Identities. Users must also have the Read permission for System Settings to access this in the Management Portal.
Modify	SecuritySettings: *Modify*	Users can modify the settings for Security Roles and Security Identities.

SSH

Table 48: SSH Security Role Permissions

UI Permission	API Permission	Description
User	SSH: *User*	Users can generate their own SSH keys.
Server Admin	SSH: *ServerAdmin*	Users can use all SSH functions, except creating server groups and assigning server group owners. Users have limited

UI Permission	API Permission	Description
		access to some functions based on server group ownership (see SSH Permissions on page 579).
Enterprise Admin	SSH: *EnterpriseAdmin*	Users can use all SSH functions (see SSH Permissions on page 579).

SSL Management

Table 49: SSL Management Security Role Permissions

UI Permission	API Permission	Description
Read	SslManagement: *Read*	Users can view the SSL Discovery pages in the Management Portal and the equivalent API functions, including defined networks and the network ranges configured for them, agent pools, and scan results. Users can use the query tool on the Results tab to find discovered endpoints and then view the discovered endpoints, including the details for the endpoints.
Modify	SslManagement: *Modify*	Users can modify the SSL Discovery settings: • Create, edit, and delete networks, including scan schedules and notification recipients • Add, edit, and delete network ranges for networks • Add, edit, and delete agent pools • Add and remove discovered endpoints from monitoring

System Settings

Table 50: System Settings Security Role Permissions

UI Permission	API Permission	Description
Read	SystemSettings: *Read*	Users can view the orchestrator auto-registration settings; users must also have *Read* permissions for Agent Management to access this in the Management Portal. Users can view the System Settings for: • SMTP Configuration for email delivery of reports and alerts • Installed components • Licensing • General Alerts and Warnings about the health of the Keyfactor Command system (not related to a specific area of the product)

UI Permission	API Permission	Description
Modify	SystemSettings: *Modify*	Users can modify the System Settings for: • Update SMTP Configuration for email delivery of reports and alerts • Installed components, including removing servers from use • Licensing, including the option to replace the existing license file

Workflow Definitions

Table 51: Workflow Definitions Security Role Permissions

UI Permission	API Permission	Description
Read	WorkflowDefinitions: *Read*	Users can view the configured workflow definitions.
Modify	WorkflowDefinitions: *Modify*	Users can modify both the built-in and any custom workflow definitions, including the name and description and the configuration for the steps. Users can also add new workflow definitions, delete workflow definitions, publish workflow definitions, and import and export workflow definitions.

Workflow Instances

Table 52: Workflow Instances Security Role Permissions

UI Permission	API Permission	Description
ReadAll	WorkflowInstances: *ReadAll*	Users can view all the workflow instances that have been initiated.
Read - Assigned To Me	WorkflowInstances: *ReadAssignedToMe*	Users can view the workflow instances that have been initiated and are awaiting input from them. **Tip:** There is not a security permission at this level that controls whether users can provide input (a signal) to a workflow instance. This is controlled using the security roles configured on the specific workflow definition. Any user who holds one of the roles configured in the workflow step that requires a signal may provide the necessary input. The user does not need to hold the *Read - Assigned To Me*

UI Permission	API Permission	Description
		Workflow Instances permission in order to provide the input.
Read - Started By Me	WorkflowInstances: *ReadMy*	Users can view the workflow instances that have been initiated by them (e.g. because they enrolled for a certificate).
Manage	WorkflowInstances: *Manage*	Users can manage initiated workflow instances, including stopping, restarting, and deleting them.

Certificate Permissions

Permissions on certificates and their collections are controlled at two levels—globally at the certificate level and on a collection-by-collection basis. Global certificate permissions are controlled on the **Certificates** role permissions. Global collection permissions are controlled with the **Certificate Collections** role *Modify* permission used in conjunction with the collection-by-collection basis permissions controlled on the **Collections Permissions tab**.

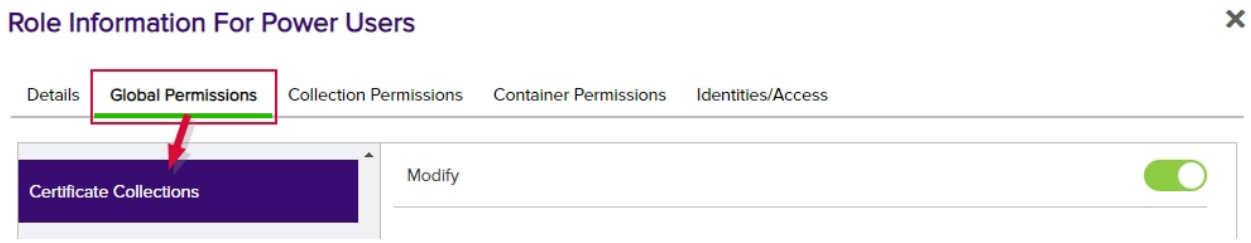


Figure 346: Certificate Collection Global Permissions

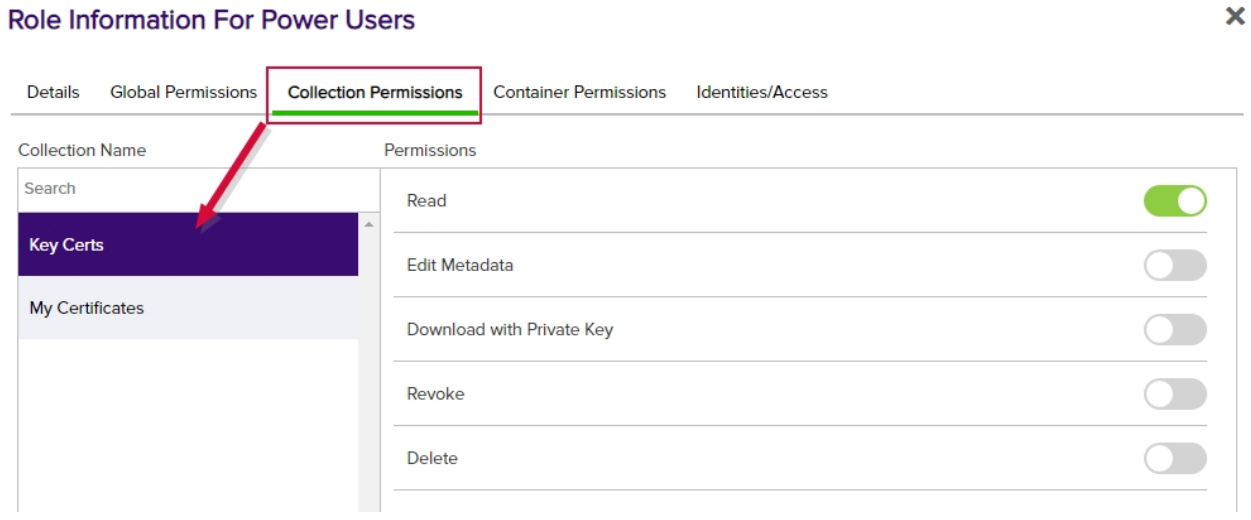


Figure 347: Certificate Collection per Collection Permissions

Certificate-related permissions can be granted globally (per global permissions—Certificates on page 615) or on a collection basis (per the Certificate Permissions on the previous page tab). Both options share the same permissions options, except global certificate permissions have the additional role permissions of *Import Private Key* and *Import*, which can not be assigned at the collection level.

Read role permission for Certificates

Users with **global Read** role permission for **Certificates** can browse to Certificate Search in the Management Portal and view all saved certificate collections. They can view any certificate in the Keyfactor Command database and are not limited to just those returned by select collections. Users with this permission can view the certificates returned by searches and open the details of the certificates.

Users with **collection-level Read** role permissions on a collection will see the collections to which they have been granted access appear on the Certificate Collections menu (if they have been configured to appear on the menu (see Certificate Collection Manager on page 80). The users will be able to view all the certificates in the collections and open the details of the certificates.

The certificate operations available to these users are:

- Add to Certificate Store (Also requires the *Read* and *Schedule Certificate Store Management* permissions)
- Edit
- Download
- Get CSV
- Identity Audit (Also requires the *Read Security Settings* permission)
- Include Revoked checkbox
- Include Expired checkbox
- Renew (Also requires the *Read* and *Schedule Certificate Store Management* permissions)
- Remove from Certificate Store (Also requires the *Read* and *Schedule Certificate Store Management* permissions)

In the case of collections, users will be able to further refine the collection query by including additional selection criteria in the query field, but these are used in addition to the base query. Users are not allowed to clear the base query for the collection, which is displayed above the query field. For example, for the collection shown in Figure 348: Collection with Read Collection-Level Security, if the user added this in the query field:

```
CN -notcontains "keyother"
```

The query would return all the certificates issued in the last 30 days with the string appsrvr in the CN using a template referencing web but without the string keyother in the CN—in other words, the web server certificates for application servers issued in the last 30 days for the keyexample.com domain but not the web server certificates for application servers issued in the last 30 days for the keyother.com domain.

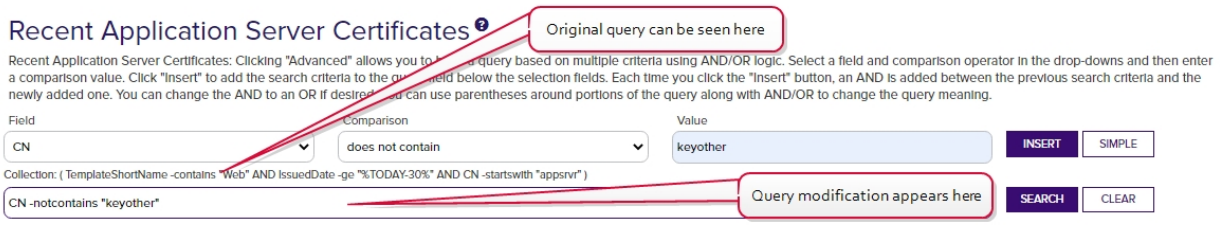


Figure 348: Collection with Read Collection-Level Security

Edit Metadata role permission for Certificates

Users with the **Edit Metadata** role permission for **Certificates** can edit the certificates in the Certificate Details on page 19 dialog (only information on the metadata tab can be edited) for which they have been given access.

If the users have also been granted global *Read* permission on **Certificates**, they can modify the metadata of any certificates within the Keyfactor Command database. If the users have not been granted the global *Read* permission, they can only modify the certificates found in collections to which they have been granted collection-level *Read* access.

Note: If you plan to edit metadata via the Keyfactor API, the user running the API needs only *Edit Metadata* permissions. *Read* permissions are not required.

Import role permission for Certificates

Users with the **Import** role permission for **Certificates** can use the Add Certificate option under the Certificate Locations menu (see Add Certificate on page 69). This is a global role only and not set on a collection-by-collection basis.

Download with Private Key role permission for Certificates

Users with the **Download with Private Key** role permission for **Certificates** will need to also have their security permissions set to *Include Private Key* option (see Security Role Permissions on page 611) to allow the users to download the private key of a certificate on any certificates to which they have been granted access if it is stored in the Keyfactor Command database or recoverable using Microsoft key recovery.

Revoke role permission for Certificates

Users with the **Revoke** role permission for **Certificates** can use the revoke certificate operation on any certificates to which they have been granted access. This includes certificates that have been issued by a local Microsoft CA or by a cloud-based certificate vendor that is managed via a Keyfactor certificate gateway.

Important: In order to successfully revoke certificates, the service account under which the Keyfactor Command application pool is running must be granted "Issue and Manage Certificates" and "Manage CA" permissions to the CA database as per *Create Active Directory Groups to Control Access to Keyfactor Command Features* in the *Keyfactor Command Server Installation Guide*, or, if delegation is configured for the CA, the user executing the revoke must have the "Issue and Manage Certificates" permissions while the application pool service account has the "Manage CA" permissions. If you are using explicit credentials to authenticate your CA (see Adding or Modifying a CA Record on page 330), it is the user specified on the CA configuration in Keyfactor Command who must have permissions on the CA.

Delete role permission for Certificates

Users with the **Delete** role permission for **Certificates** can delete certificates and private keys from the Keyfactor Command database.

Import Private Key role permission for Certificates

Users with the **Import Private Key** role permission for **Certificates** can add a certificate with an associated private key through the Add Certificate option under the Certificate Locations menu (see Add Certificate on page 69) and the private key will be stored in the Keyfactor Command database. Users must also be granted the *Import* role in order to be able to use the Add Certificate feature. This is a global role only and not set on a collection-by-collection basis.

Container Permissions

Permissions on certificate stores are controlled at two levels—globally and on a certificate store container-by-container basis. When designing a certificate store permission scheme, you may use entirely global permissions or you may use a combination of global permissions and container permissions. Both global and container permissions are configured through Security Roles (see Security Role Operations on page 628).

Global certificate store permissions are controlled with the **Certificate Store Management** role permissions on the **Global Permissions** tab of the Security Role Information dialog.

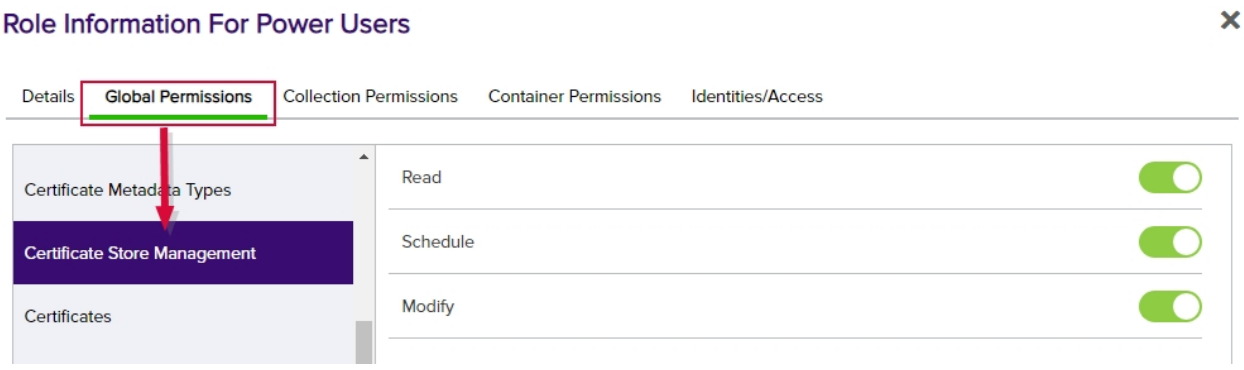


Figure 349: Certificate Store Management - Global Permissions

Container-by-container permissions are set on the **Container Permissions** tab of the Role Information dialog for each container by name using the same set of permissions.

Any containers that do not have container-by-container permissions applied fall back to the global permissions, if any global permissions have been set for that role.

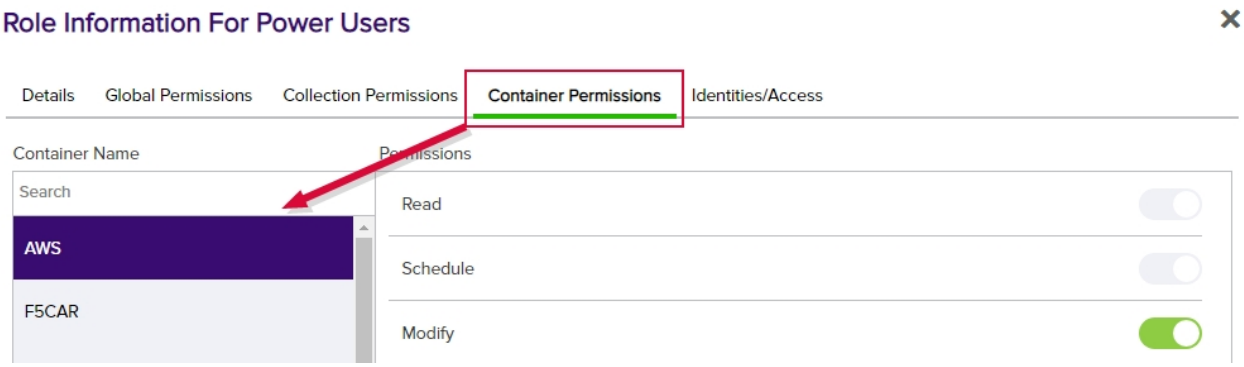


Figure 350: Certificate Store Management - Container Permissions

Container permissions work in conjunction with many other security permissions to control access to certificate stores related functionality.

Tip: See the detailed tip sections of Certificate Operations on page 42 , Certificate Store Operations on page 385 and Certificate Store Types on page 635 for more information regarding which combination of security permissions are required for various operations.

Table 53: Permissions for Certificate Operations - Certificate Search Page

UI Permission	Description
Read	Users can view the certificate stores and containers tabs on the *Locations > Certificate Stores* menu, and view certificate store types.
Schedule	Users can add certificates to certificate stores, renew/reissue certificates, schedule and remove certificates from certificate stores.
Modify	Users can manage all operations regarding certificate stores—including the stores, containers, and discovery process—and certificate store types.

View Permissions of Security Identities

To view permissions for a security identity, highlight the row in the security identity grid and click **View Permissions** at the top of the grid or right-click the row in the grid and choose **View Permissions** from the right-click menu. Within this dialog you can view the global permissions for the identity, certificate store container permissions, or certificate collection permissions.

If the user or group has been granted more than one role, you see the permissions of all the roles granted to the user or group consolidated together on the **View Permissions** dialog for easy viewing. Hover over a specific permission to see how that permission we granted.

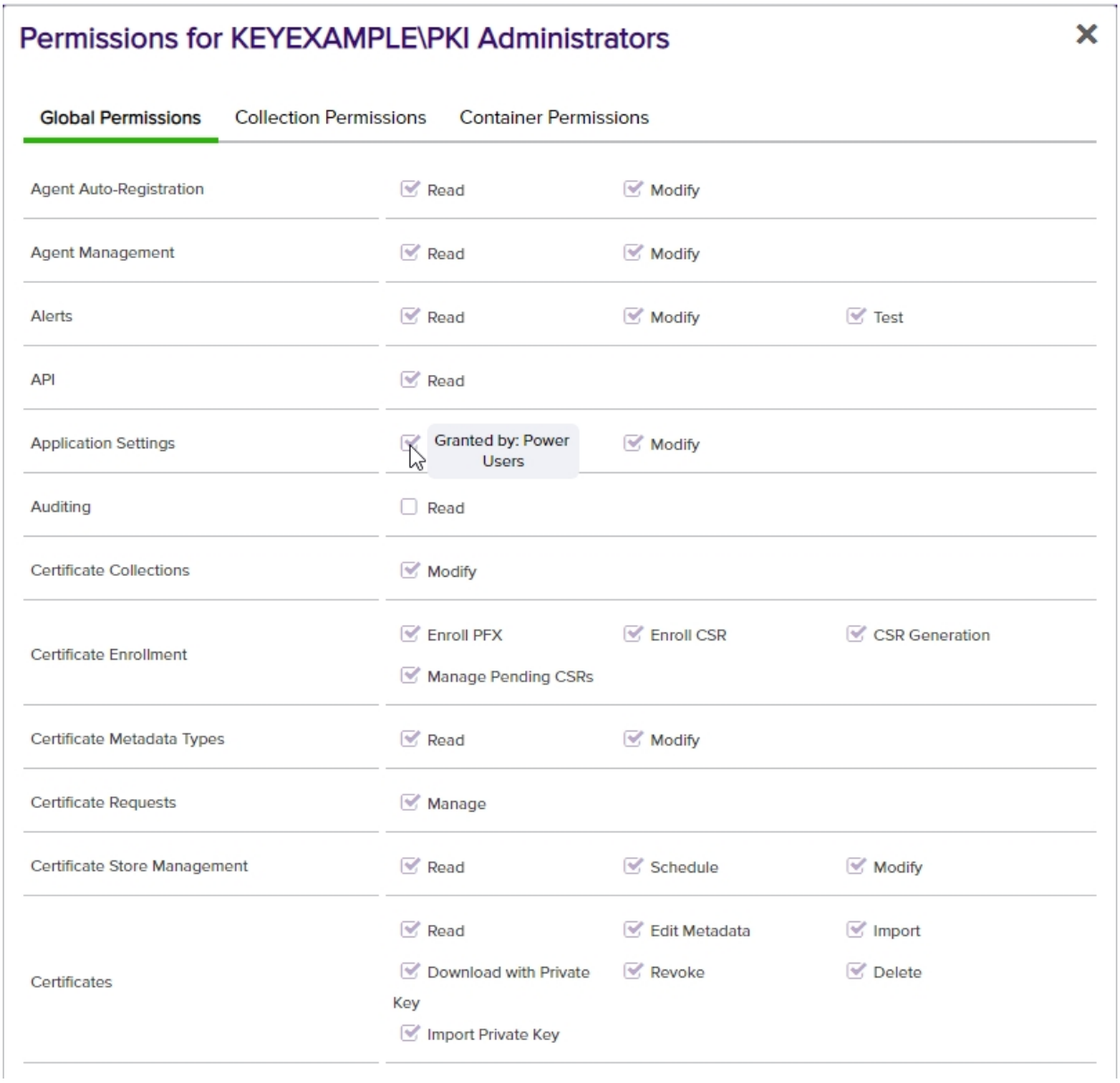


Figure 351: View Global Permissions for a Security Identity

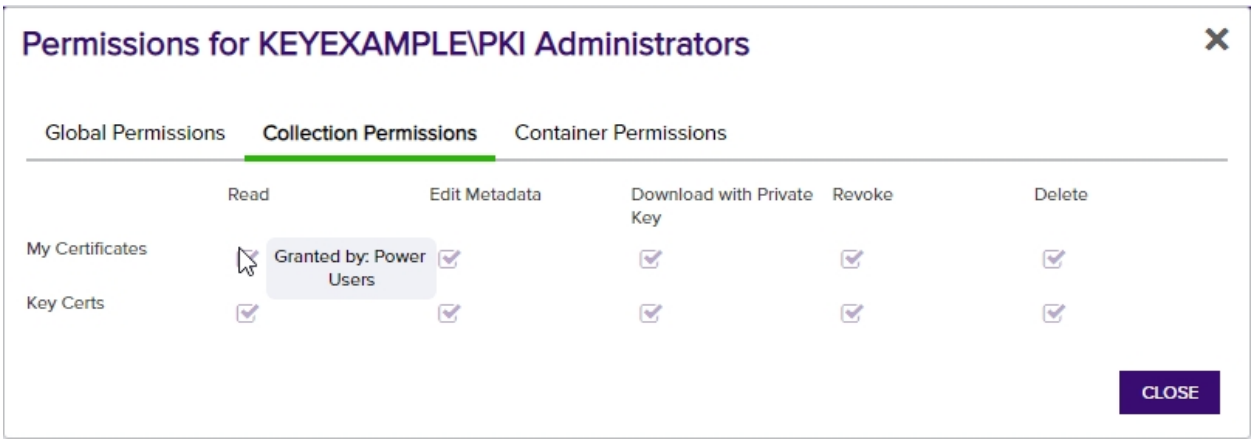


Figure 352: Collection Permissions for a Security Identity

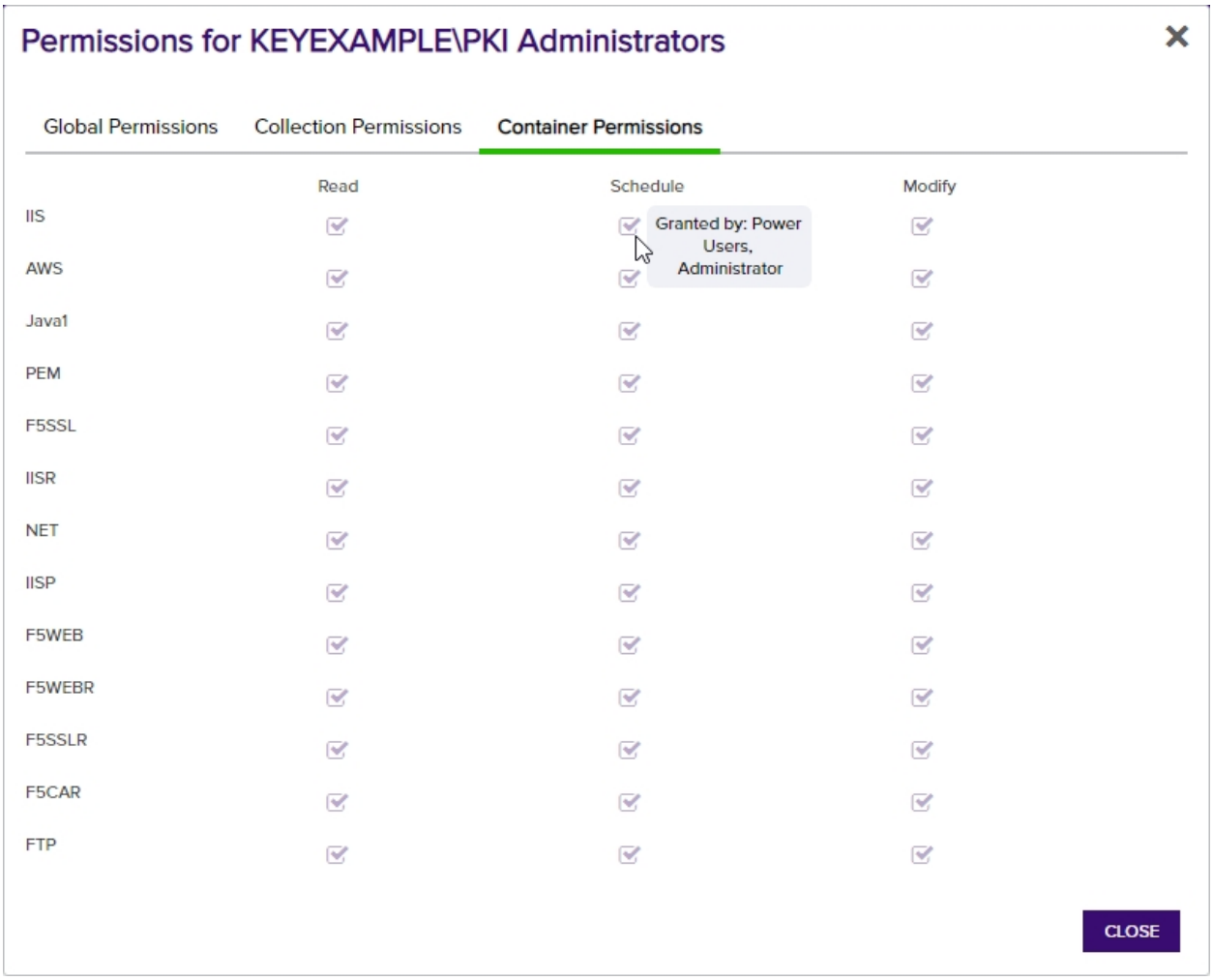


Figure 353: Container Permissions for a Security Identity

Adding or Modifying a Security Role

1. In the Management Portal, browse to *System Settings Icon* > *Security Roles and Identities.*
2. On the Security Roles and Identities page, select the Security Role tab and click **Add** from the menu at the top of the grid to add a new security role, or highlight a row and click **Edit** from the top of the grid or from the right click menu to modify an existing role.

   Note: The Administrators and Reporting API Access roles cannot be edited or deleted.

3. Either the **Add Security Role** dialog or **Role information For <role>** dialog will open. Fill in each tab of the dialog with the information desired for the selected security role.

   a. On the Global Permissions tab, click the toggle buttons for the permissions that are appropriate for the new role (see Security Role Permissions on page 611).

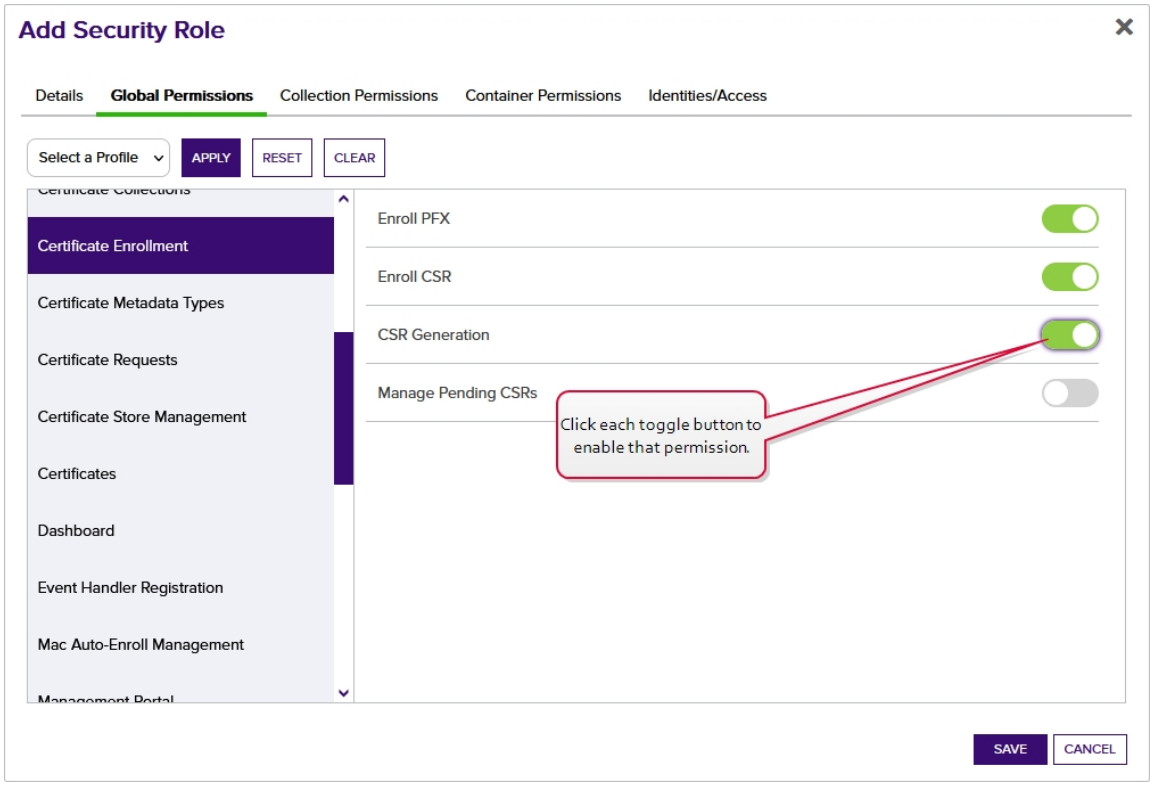


Figure 354: Grant Global Permissions to a Security Role

Tip: If desired, use the dropdown at the top to enable all the read toggle buttons (*Read Only*) or all the toggle buttons (*Select All*). Click **Apply** to apply the selection in

the dropdown across all permissions. Click **Reset** to return the dialog to the state it was in when last saved and remove any changes made since opening the permission for editing. Click **Clear** to disable all the toggle buttons.

b. Optionally, on the Collection Permissions tab, highlight each certificate collection you would like to set permissions for and click the toggle button for each desired permission (see Certificate Permissions on page 621). If you do not select any collections, the permissions set on the Global Permissions tab will apply to all collections. A search bar has been added to the top of Collection Name column on the collections tab of the security dialog to make it easier to find and assign permissions.

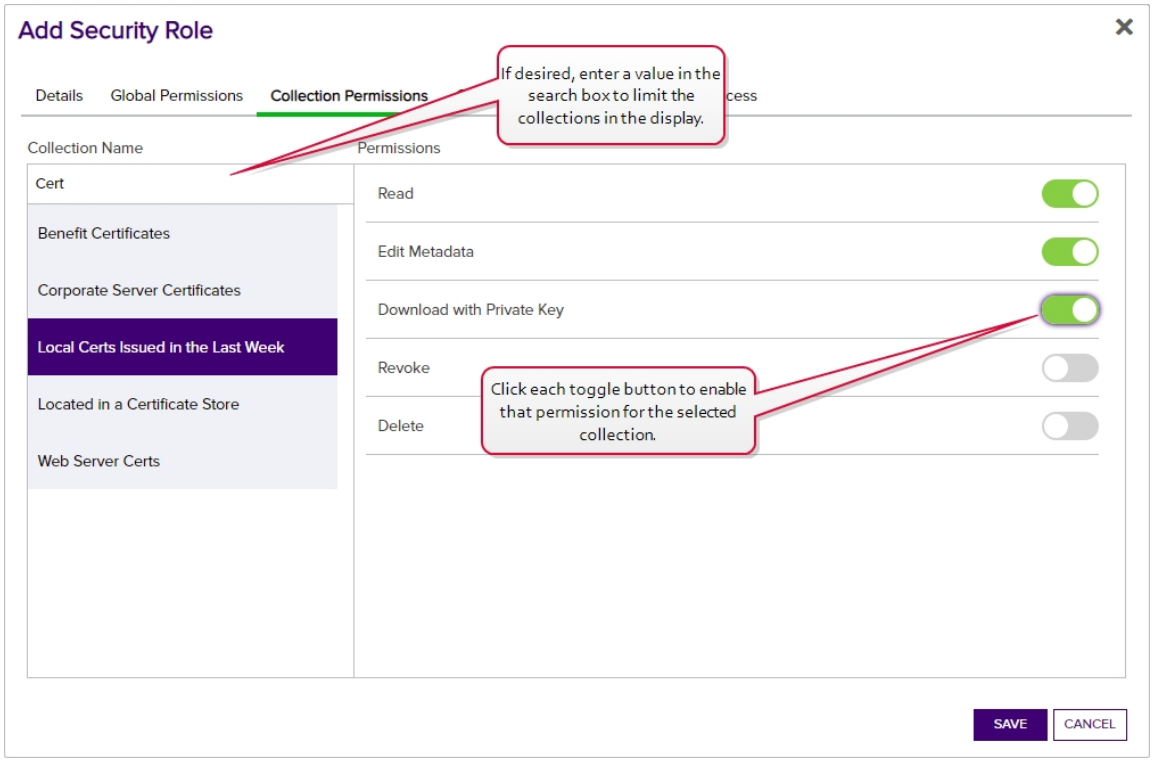


Figure 355: Grant Collection Permissions to a Security Role

c. Optionally, on the Container Permissions tab, highlight each container you would like to set permissions for and click the toggle button for each desired permission (see Container Permissions on page 624). If you do not select any containers, the permissions set on the Global Permissions tab will apply to all containers. A search bar has been added to the top of Container Name column on the containers tab of the security dialog to make it easier to find and assign permissions.

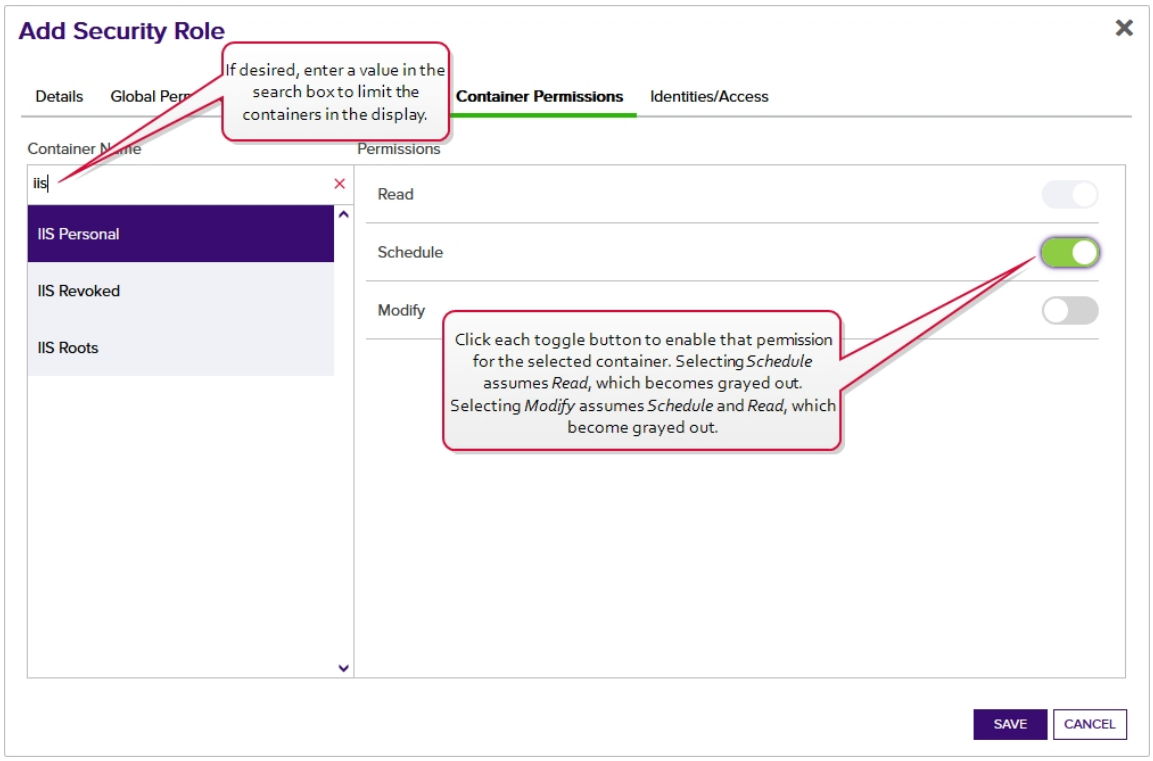


Figure 356: Grant Container Permissions to a Security Role

d. On the Identities/Access tab, click **Add** to open the Add Security Identities dialog, which shows all unassigned identities created in Keyfactor Command (see Security Identity Operations on page 632). Check the box next to each desired identity and click **Add** or **Add and Close** to add the identity to the list for this role. Or select one or more existing identities and click **Remove** to remove them from this security role

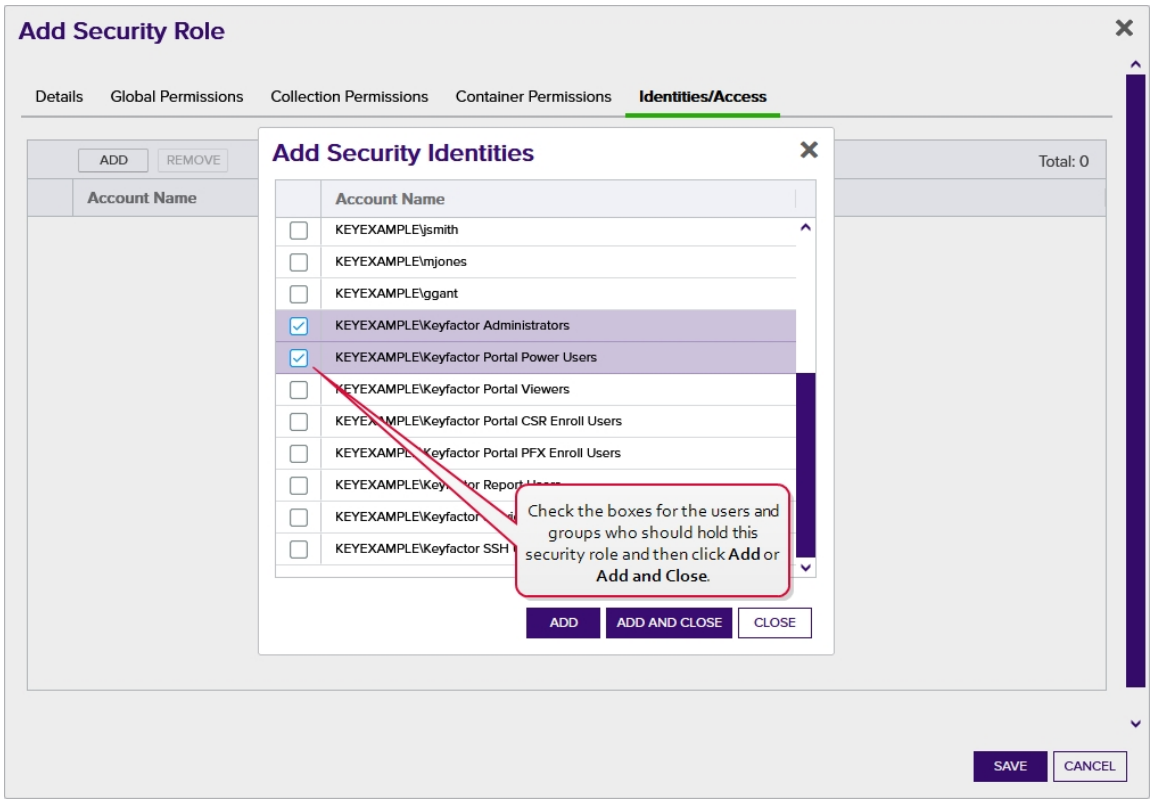


Figure 357: Associate Security Identities with a Security Role

4. Click **Save** to save the new role or your changes.

Copying a Security Role

1. In the Management Portal, browse to *System Settings Icon* > *Security Roles and Identities*.
2. On the Security Roles and Identities page, select the Security Role tab. Highlight a row and click **Copy** from the top of the grid or from the right click menu to copy an existing role.
3. Click OK to the Confirm Operation message.

   Note: Copying a security role will also assign the new role to all the same security identities as the original role.

4. The name will automatically be set to *Copy of (original role name)* with the same description as the original role. Update the name and description and click **Save**.

Note: The Administrators and Reporting API Access roles cannot be copied.

Deleting a Security Role

1. In the Management Portal, browse to *System Settings Icon* > *Security Roles and Identities.*
2. On the Security Roles and Identities page, select the Security Role tab. Highlight a row and click **Delete** from the top of the grid or from the right click menu to delete an existing role.

Note: The Administrators and Reporting API Access roles cannot be edited or deleted.

Tip: You can view all the permissions set for a given role at a glance by granting *one* role to *one* identity only (and no other roles) and then using the View Permissions option for the identity (see View Permissions of Security Identities on page 625).

Security Identity Operations

From the *Securities Identities* tab of the Security Role and Identities page in Keyfactor Command you can create the individual identities that will be associated with one or more security roles to define the user access to Keyfactor Command. Prior to adding new security identities, it is recommended that you create all of the security roles you require (see Security Role Operations on page 628) so they can be assigned to the new security identities. You can also get a complete view of permissions for an identity (see View Permissions of Security Identities on page 625).

Adding a Security Identity

1. In the Management Portal, browse to *System Settings Icon* > *Security Roles and Identities.*
2. Select the **Security Identity tab** of the page. Click **Add** to add a new security identity.
3. The **Add Security Identities** dialog will open. Enter an AD user or security group name using *DOMAIN\group name* format and click **Save** to save the new identity. If the user or group cannot be resolved, you will receive an error.

Important: The built-in Active Directory groups Domain Admins and Enterprise Admins cannot be used directly to grant access to the Management Portal due to how these groups function within Windows. You can create a custom Active Directory group, reference that group in the Management Portal, and add the built-in Domain Admins or Enterprise Admins group to that custom group, if desired.

Adding or Modifying Security Identity Roles

1. In the Management Portal, browse to *System Settings Icon* > *Security Roles and Identities.*

Important: The built-in Active Directory groups Domain Admins and Enterprise Admins cannot be used directly to grant access to the Management Portal due to how these

groups function within Windows. You can create a custom Active Directory group, reference that group in the Management Portal, and add the built-in Domain Admins or Enterprise Admins group to that custom group, if desired.

2. Select the **Security Identity tab** of the page. Highlight the identity in the grid and choose **Edit Roles** from the right-click menu, or click **Edit Roles** at the top of the identity grid.

3. In the **Roles** dialog, select the appropriate role in the **Available Roles** list and use the right arrow to move the role to the **Current Roles** list. Repeat for all desired roles. Click **Save** to assign the role(s) to the identity.

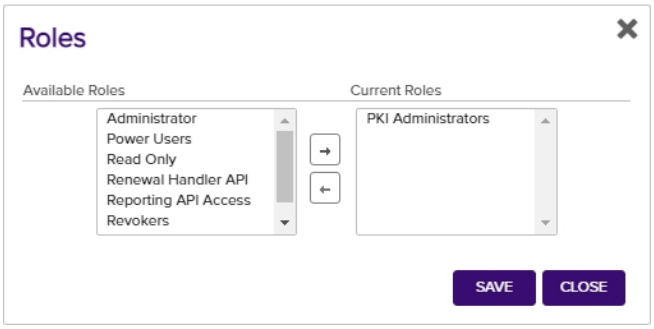


Figure 358: Grant Roles to a Security Identity

Deleting a Security Identity

1. In the Management Portal, browse to *System Settings Icon* > *Security Roles and Identities.*

2. Select the **Security Identity tab** of the page. Highlight the identity you want to delete and click **Delete** at the top of the grid. Or right-click the row in the grid and choose **Delete** from the right-click menu.

Important: Do not delete the last identity associated with the Administrator role or you will lose access to the administrative features of the Management Portal.

Using the Security Role Search Feature

Note: The security role search skips the validation check when loading for improved performance. The validation still occurs when loading a single record, so users will encounter an error when trying to work with an invalid role.

The search function allows you to query the database for information. The same query structure is used in multiple locations within the Keyfactor Command Management Portal.

When you first open the page, you will see the simple search option. To execute a search, select the field and comparison operators in the dropdowns and type something on which to search in the value field (if applicable). If you select an *is null* or *is not null* comparison operator, the value field will be grayed out. Click the **Search** button to execute the query.

Each query consists of three parts:

Query Field

The available fields for querying vary depending on the area of the Management Portal in which the search is used. On this page, the queries can be done on the following built-in fields:

Name
Complete or partial matches with the name of the security role.

Comparison Operator

The query comparison operators vary depending on the type of field selected and the specific properties of the field. The list below shows the dropdown list comparison operators, as well as the equivalent query language syntax (in parentheses).

Most string fields (the vast majority of the built-in fields) support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Contains (-contains)
- Does not contain (-notcontains)
- Starts with (-startswith)
- Ends with (-endswith)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Most date and integer fields support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Is less than (-lt)
- Is less than or equal to (-le)
- Is greater than (-gt)
- Is greater than or equal to (-ge)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Most Boolean (true/false) fields support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Comparison Value

The value you enter for comparison must match the field type. For example, integer fields only support numerical values. String fields support all alphanumeric characters. Boolean fields only support True or False. The value field is not case sensitive. Date fields support only properly

formatted dates and will initially display as mm/dd/yyyy. You can choose to populate the date field by:

- Clicking in a date Value field to open a pop-up calendar to select a date that will populate the field.
- Clicking in a segment of the date format (i.e., mm/dd/yyyy) and entering a value. As you continue to type in any one segment, the cursor will keep moving onto the next segment.

The results that match your search criteria will be displayed in the results grid below the search selection options.

Advanced Searches

On any search page you can click **Advanced** to the right of the Search button to display the advanced search options. Click **Simple** to close the advanced search options again.

Multiple Criteria

Using the advanced search options, you can build a query based on multiple criteria using AND/OR logic. As with a simple search, you select a field and comparison operator in the drop-downs and then enter a comparison value, if applicable. Click **Insert** to add the search criteria to the query field below the selection fields. Use the selection fields to build multiple search criteria. Each time you click the insert button, an AND is added between the previous search criteria and the newly added one. You can change the AND to an OR if desired. You can use parentheses around portions of the query along with AND/OR to change the query meaning.

For example, for certificate searches:

```
(CN -contains "appsrvr" AND IssuedDate -ge "01/01/2022") OR (CN -contains "appsrvr" AND
TemplateShortName -contains "web")
```

This query will return all the certificates issued on or after January 1, 2022 with the string appsrvr in the CN and also all certificates issued at any time with the string appsrvr in the CN using a template referencing web. When you have entered all the desired search criteria, click **Search** to execute the query. If you wish to clear the query field and start over, click the **Clear** button.

2.1.11.3 Certificate Store Types

Certificate store types allow you to define types of locations to contain certificates. These locations can be defined for operations such as inventory, management, discovery, and reenrollment.

Several built-in certificate store types are provided for use by the standard Keyfactor Command orchestrators. These include:

- Amazon Web Services
- F5 SSL Profiles
- F5 Web Services
- F5 CA Bundles REST

- F5 SSL Profiles REST
- F5 Web Server REST
- File Transfer Protocol
- IIS Personal
- IIS Revoked
- IIS Roots
- Java Keystore
- NetScaler
- PEM File

Custom certificate store types can be created for use with the AnyAgent Framework (see Certificate Store Type Operations below).

Tip: Click the help icon (?) next to the page title to open the embedded web copy of the *Keyfactor Command Documentation Suite* to this section.
You can also find the help icon at the top of the page next to the **Log Out** button. From here you can choose to open either the *Keyfactor Command Documentation Suite* at the home page or the *Keyfactor API Endpoint Utility*.

Certificate Store Type Operations

Certificate store types define locations against which Keyfactor Command can perform predefined operations. New ones are commonly added for custom orchestrators created with the Keyfactor AnyAgent, the Keyfactor Native Agent, or another of the tools in the Keyfactor Integration SDK (see Orchestrators on page 470).

The certificate store types page displays a list of the currently defined types and offers the options to create new types, edit existing types and delete types. It is not possible to update built-in certificate store types because doing so will break the associated orchestrator functionality.

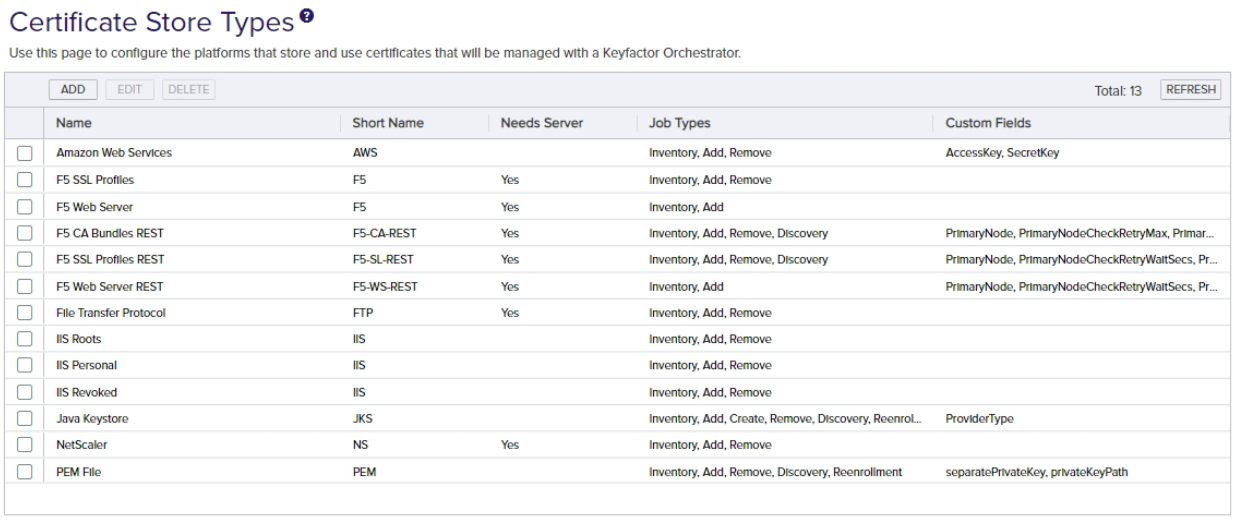


Figure 359: Certificate Store Types

Adding or Editing a Certificate Store Type

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:
Certificate Store Management: *Read*
Certificate Store Management: *Modify*
System Settings: *Read*
System Settings: *Modify*

To create or modify a certificate store type:

1. In the Management Portal, browse to *System Settings Icon* > *Certificate Store Types*.
2. On the Certificate Store Types page, click **Add** to create a new certificate store type, or click **Edit** from either the top or right-click menu to modify an existing one.
3. In the Certificate Store Types dialog, you will see four tabs. Complete the dialog with appropriate information using the following information:

Basic Tab

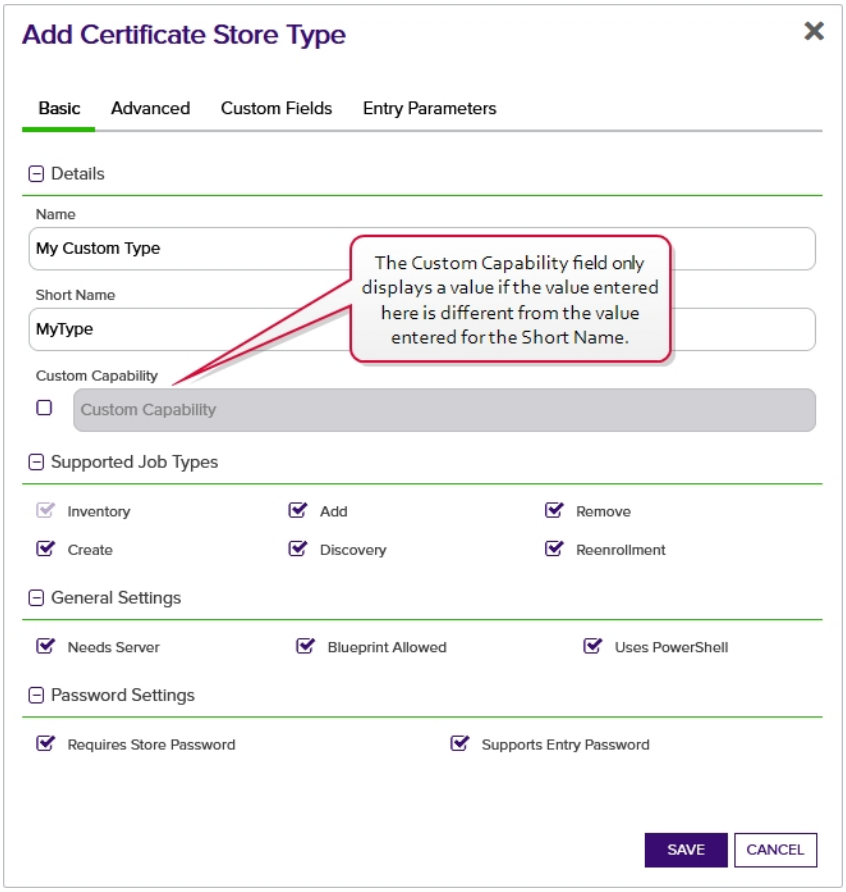


Figure 360: Add New Certificate Store Type: Basic Tab

- **Name:** Enter a user friendly recognizable name for the certificate store type.
- **Short Name:** Enter a short name identifier for the certificate store type. This value is used by the Keyfactor Universal Orchestrator and Windows Orchestrator installation and configuration tools to validate the orchestrator capabilities.
- **Custom Capability:** If desired, check this box to allow you to define a custom capability name. By default, the Short Name is used as the capability name, and in most cases a separate capability name is not needed. The capability name you set here corresponds to configurations made in the manifest.json file for your custom orchestrator extension.

  Tip: This box shows as checked only if the value entered in the *Custom Capability* does not match the value entered in the *Short Name*. If you check the box, enter a value that matches the short name value, save the record and open it again, the

box will show unchecked and the *Custom Capability* field will show empty since the value matches the *Short Name* value.

Note: The *Custom Capability* cannot be changed on an edit if an orchestrator has registered with Keyfactor Command, been approved, and included the certificate store type in its capability list. If you change the *Short Name* in this circumstance, the *Custom Capability* box will be checked and the value set to the original value of the *Short Name*.

- **Supported Job Types**
  Select the job capabilities required to support the store type.
  - **Inventory:** Determine what is in the certificate store(s) and report the contents to Keyfactor Command. This capability is required for all store types.
  - **Add:** Add new certificates to a certificate store.
  - **Remove:** Remove certificates from a certificate store.
  - **Create:** Create a new certificate store.
  - **Discovery:** Determine what certificate stores of this type are on the device.
  - **Reenrollment:** Generate a keypair on the device and submit a certificate signing request using on-device key generation (ODKG).
- **General Settings**
  - **Needs Server:** Select if server access is required for adding certificate stores to the certificate store type. If selected, a user will be prompted for a username and password to connect to the remote server.
  - **Blueprint Allowed:** Select whether certificate stores of this type will be included when creating or applying blueprints. For more details, see Generating and Applying Blueprints on page 486.
  - **Uses PowerShell:** Select if the jobs for this store type are implemented by PowerShell instead of a .NET class.
- **Password Settings**
  - **Requires Store Password:** Select to mandate that a password be entered and authenticated when creating stores of this type. This password secures the store as a whole.
  - **Supports Entry Password:** Select to allow an entry password to be entered and authenticated when adding a certificate to a store. This password secures a single certificate within the store.

Advanced Tab

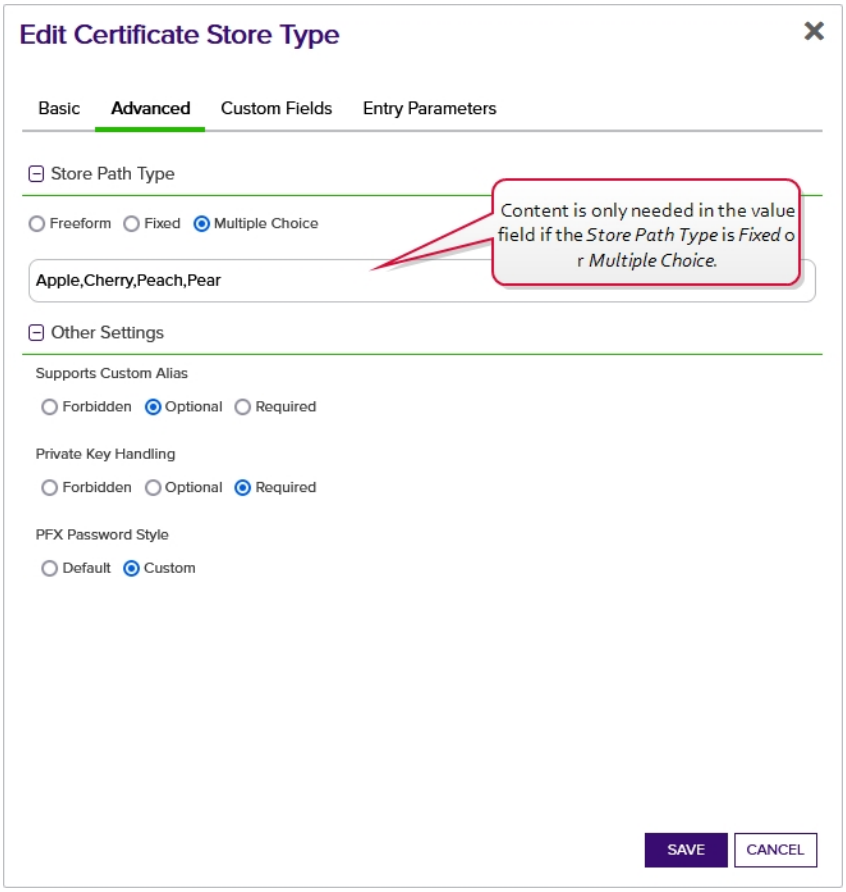


Figure 361: Add New Certificate Store Type: Advanced Tab

- **Store Path Type:**
  - **Freeform:** Select if users are required to enter a path defining the store location.
  - **Fixed:** Select if a store path does not apply, generally one store per device (e.g. IIS).
  - **Multiple Choice:** Select to allow users to select an option during certificate store creation.

  If *Store Path Type* is *Fixed* or *Multiple Choice*, a value should be provided in the value field. For multiple choice, this should be a comma separated list of values that users will be able to select from when defining a certificate store location.

- Other Settings
    - **Supports Custom Alias:**
        - **Forbidden:** Select if a custom alias is not required.

          Note: If this is set to **Forbidden**, the **Alias** field will not display on the Add to Certificate Store page unless *Overwrite* is checked on the page.

        - **Optional:** Select if the custom alias is optional.
        - **Required:** Select if the custom alias is required.
    - **Private Key Handling:**
        - **Forbidden:** Select if a private key is not required; generally, applies to trust stores (e.g. Root CA certificates).
        - **Optional:** Select if the private key is optional; applies to store types that could represent either a Trust Store or End-Entity Store.
        - **Required:** Select if the private key is required; applies to stores that hold an End-Entity Certificate (server or client authorization).
    - **PFX Password Style:**
        - **Default:** Opt to have Keyfactor Command randomly generate a password.
        - **Custom:** Opt to allow a password to be entered and authenticated when enrolling a certificate through the Keyfactor Command Management Portal when installing a store of this type. The Custom option can be selected only if **Allow Custom Password** in the Application Settings is equal to *True*. For more details, see Application Settings on page 583.

Custom Fields Tab

Custom fields define unique properties for the given certificate store type. Click **Add** on this tab to open the Add Custom Field dialog box.

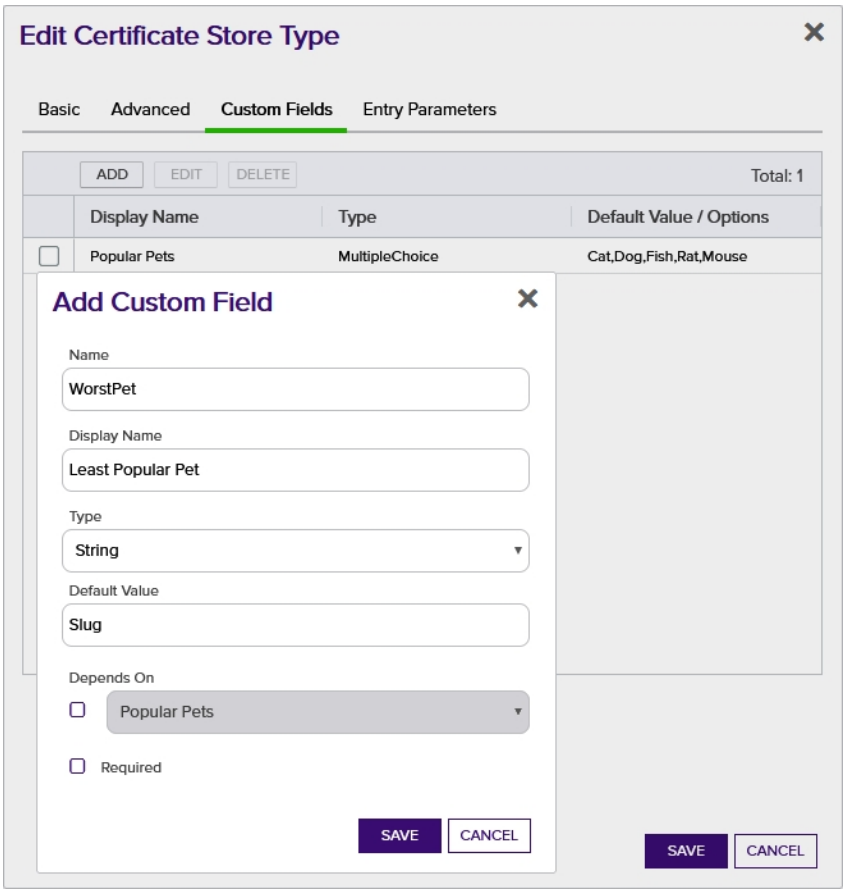


Figure 362: Add New Certificate Store Type: Custom Fields Tab

- **Name:** Enter the name submitted to the orchestrator and referenced in the extension module custom code.
- **Display Name:** Enter a user-friendly recognizable name.
- **Type:** Select whether parameter information is stored as a string, Boolean, multiple choice or secret.
- **Default Value / Multiple Choice Options:** Add a default value that will pre-populate the parameter field in the *Add New Certificate Store* dialog box. If you select a type of Multiple Choice, populate this field with a comma-separated list of multiple choice options for this parameter. If you select a type of Boolean, you will be given the option of True or False here.
- **Depends On:** Check this box if you have another custom field for this certificate store type and want to create a relationship between that one and this one. Then select the custom field on which this custom field depends in the dropdown. This option configures

one custom field to display in the certificate store configuration dialog only if another custom field contains a value.

- **Required:** Select whether a value for this parameter must be entered before a certificate store can be added to Keyfactor Command.

Entry Parameters Tab

Entry parameters define unique properties that are required when performing management jobs on a certificate store of this type. Click **Add** on this tab to open the Add Entry Parameter dialog box.

Tip: What's the difference between custom fields and entry parameters?

- Custom fields are about the certificate store definition itself and are static. For example, you might use a custom field to define the primary node name of an F5 instance. This node name is the same no matter what inventory or management jobs you do with the F5 device(s). Values for custom fields are entered in the certificate store record when creating or editing the certificate store record.
- Entry parameters are about the specific certificate within the certificate store. They are used to send additional information related to the certificate to the server or device that hosts the certificate store when running management jobs for that certificate store. Often this is more fluid information that isn't the same for every use of that certificate store. For example, several virtual servers with separate certificates in the same folder may exist on a NetScaler device. When replacing one certificate, updates may need to be made to only the virtual server that is using the certificate. In this case, the authorized user will be prompted to enter the virtual server name based on an entry parameter. Values for entry parameters are entered at the time a management job is initiated (e.g. adding a certificate to a certificate store).

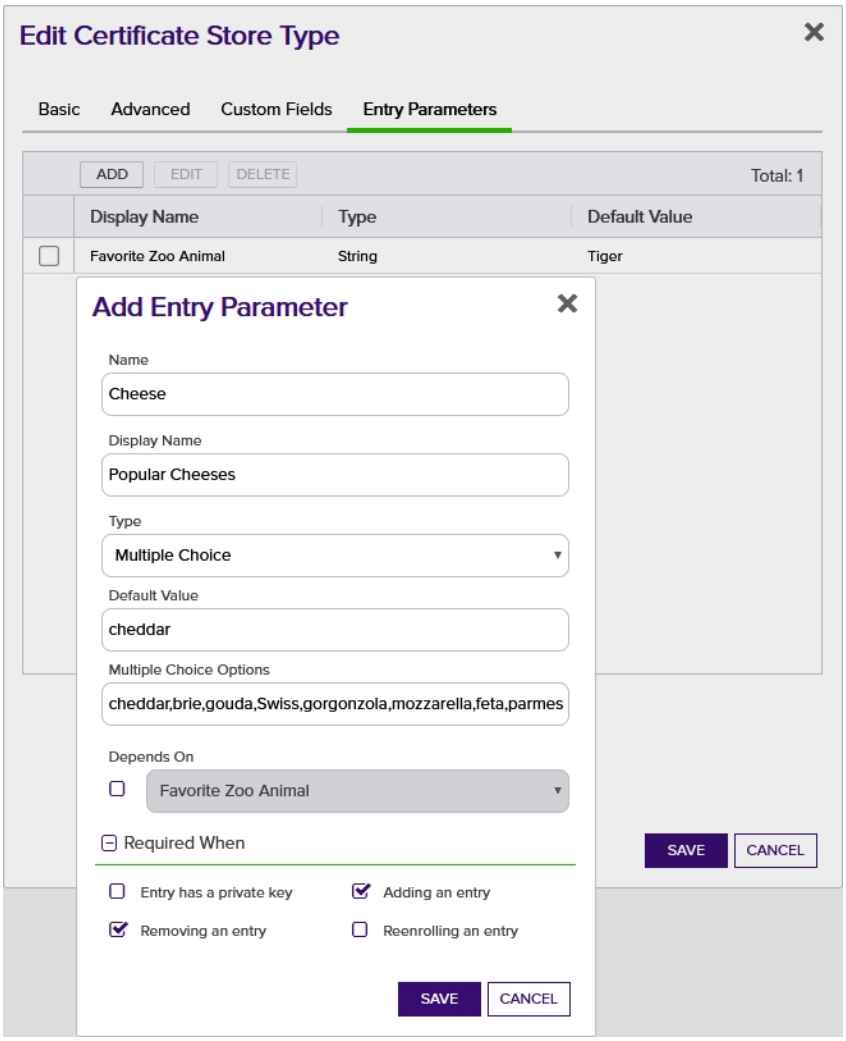


Figure 363: Add New Certificate Store Type: Entry Parameters Tab

- **Name:** Enter the name for the entry parameter. This value must be unique.
- **Display Name:** Enter a user-friendly recognizable name. This value must be unique.
- **Type:** Select whether parameter information is stored as a string, Boolean, multiple choice or secret.
- **Default Value:** Add a default value that will pre-populate the parameter field in the *Add New Certificate Store* dialog box. If you select a type of Boolean, you will be given the option of True, False, or Not Set here.

- **Multiple Choice Options:** Populate this field with a comma-separated list of multiple choice options if you selected a *Type* of multiple choice. This field will be grayed out if you selected a *Type* other than multiple choice.
- **Depends On:** Check this box if you have another entry parameter for this certificate store type and want to create a relationship between that one and this one. Then select the entry parameter on which this entry parameter depends in the dropdown. This option configures one entry parameter to display in the certificate store configuration dialog only if another entry parameter contains a value.
- **Required When:**
    - **Entry has a private key**: If set to *true*, a value must be provided for this field when configuring a management job (either add or remove) if the certificate has an associated private key in Keyfactor Command. This would be the case, for example, when doing a PFX enrollment and adding the resulting certificate to a certificate store.
    - **Adding an entry**: If set to *true*, a value must be provided for this field when configuring an add certificate job.
    - **Removing an entry**: If set to *true*, a value must be provided for this field when configuring a remove certificate job.
    - **Reenrolling an entry**: If set to *true*, a value must be provided for this field when configuring a reenrollment job.

4. Click **Save** to save the new certificate store type.

Note: Built-in certificate store types cannot be edited.

Deleting a Certificate Store Type

You may delete one store type at a time.

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:
Certificate Store Management: *Read*
Certificate Store Management: *Modify*
System Settings: *Read*
System Settings: *Modify*

To delete a certificate store type:

1. In the Management Portal, browse to *System Settings Icon* > *Certificate Store Types*.
2. On the Certificate Store Types page, highlight the row in the grid of the certificate store type to delete and click **Delete** at the top of the grid or right-click the type in the grid and choose **Delete** from the right-click menu.
3. On the Confirm Operation alert, click **OK** to confirm or **Cancel** to cancel the operation.

2.1.11.4 Certificate Metadata

Using user-defined certificate metadata you can tag certificates with additional information you want to assign to certificates at the point of enrollment, such as points of contact or certificate/app owners. Metadata fields can be defined as being *required* or *optional* during enrollment. The data from the metadata fields can then be used for queries and alerts in the Management Portal.

First, you must add all the metadata fields you will use across the platform via *System Settings Icon* ⚙ *> Certificate Metadata* (see Metadata Field Operations below). These *system-wide* settings will then become the default metadata settings for all templates and they will be assigned to certificates during enrollment via the selected template. You may choose to modify the *system-wide* metadata field(s) for specific templates by creating *template-specific* metadata settings. See Certificate Template Operations on page 353 and Enrollment on page 130 for more information.

Tip: Click the help icon (?) next to the page title to open the embedded web copy of the *Keyfactor Command Documentation Suite* to this section.
You can also find the help icon at the top of the page next to the **Log Out** button. From here you can choose to open either the *Keyfactor Command Documentation Suite* at the home page or the *Keyfactor API Endpoint Utility*.

Metadata Field Operations

To select a single row in the certificate metadata field grid, click to highlight it and then select an operation from either the top of the grid or the right-click menu.

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:
System Settings: *Read*
Certificate Metadata Types: *Read*
Certificate Metadata Types: *Modify*

Adding or Modifying a Metadata Field

To create a new metadata field or edit an existing one:

1. In the Management Portal, browse to the *System Settings Icon* ⚙ *> Certificate Metadata.*
2. On the Certificate Metadata page, click **Add** to create a new metadata field, or, to edit an existing one, double-click the row in the metadata grid, right-click the row and choose **Edit** from the right-click menu, or highlight the row in the grid and click **Edit** at the top of the grid.

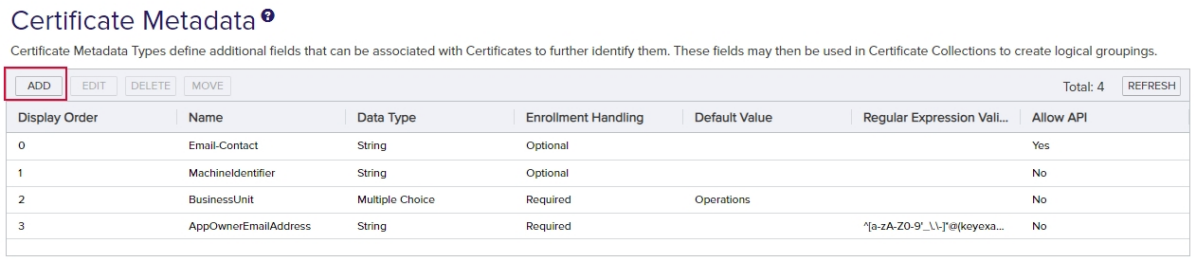


Figure 364: Certificate Metadata

3. In the Metadata Edit dialog, enter a **Name** for your metadata field. This name appears in interfaces where you can use metadata, such as certificate details dialogs, alert dialogs, certificate imports and certificate requests. Once this field has a value associated with it for at least one certificate, you cannot change this name. The metadata name field cannot contain spaces; dashes and underscores are supported.

   Important: Be sure to review the list of existing queryable certificate fields on the Certificate Search Page on page 32 before adding a new metadata field, so you do not add a field of the same name or alias as an existing field. Doing so would cause a search or alert on that field to fail. For example, do not create a metadata field called *NetBIOSRequester* or its alias *RequesterName*, as this would match is an existing certificate field, and having a metadata field with this name would create issues.

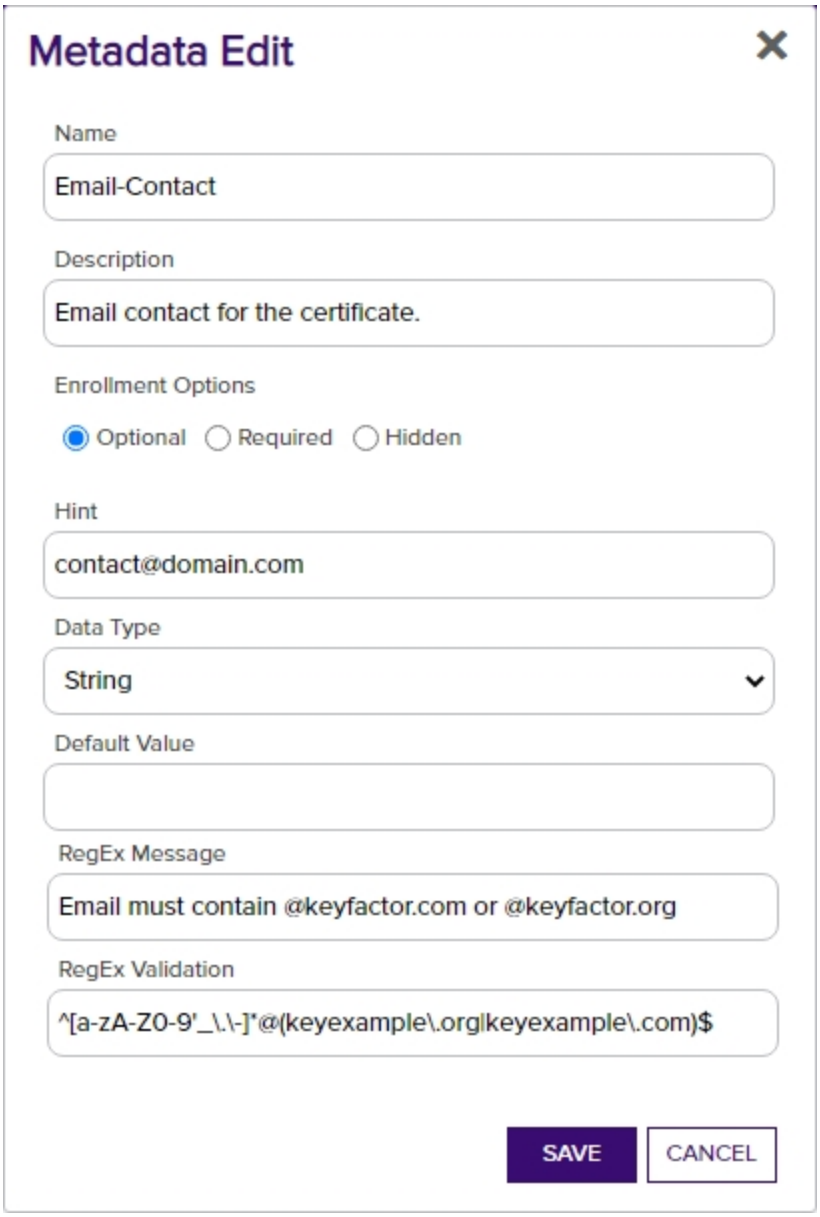


Figure 365: Create or Edit Certificate Metadata Field

4. Enter a **Description** for the metadata field.
5. The **Enrollment Options** provide three possible settings for the metadata field:
    - Select the **Optional** radio button to allow users the option to either enter a value or not enter a value in the field when populating metadata fields.

- Select the **Required** radio button to force users to enter a value in the field when populating metadata fields. Required fields will be marked with *Required next to the field label on the Certificate Details dialog for a certificate and on the certificate enrollment pages.
- To hide the field on the enrollment pages (see Enrollment on page 130), select the **Hidden** radio button. Selecting the **Hidden** option does not hide the field in the certificate details (see Metadata Tab on page 20) or on the Add Certificate page (see Add Certificate on page 69).

6. Enter a short hint in the **Hint** field. This hint appears in unpopulated metadata string, integer, big text and date fields on editing interfaces to provide the user with a clue as to what type of data should be entered in the field.

   Note: The Hint field is not used for some selections of the Data Type field (see the next step) and will disappear from the screen if a Data Type that does not use a Hint is selected.

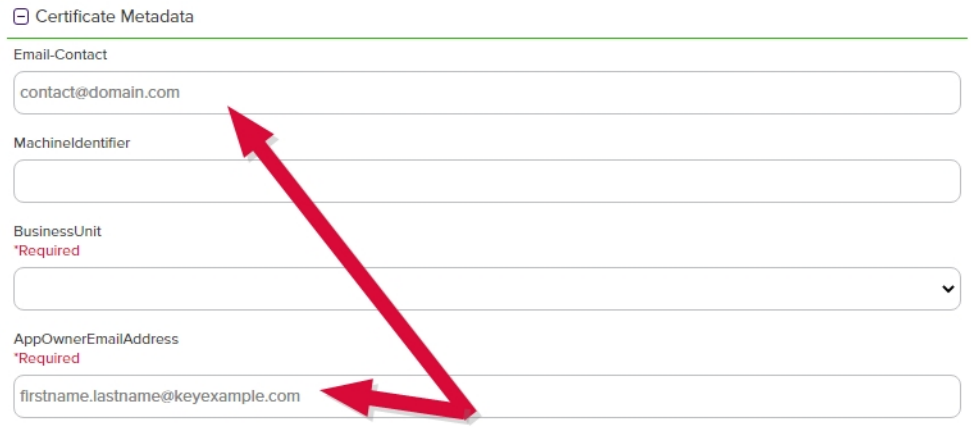


Figure 366: Metadata Hints in a Certificate Details Dialog

7. Select the **Data Type** for the field in the dropdown. The available field types are String (alphanumeric), Integer (whole numbers), Date, Multiple Choice, Big Text, and Boolean (True/False). String fields are limited to 400 characters. Big text fields are limited to 4000 characters. String fields support additional indexing, and so may be preferable for large databases where possible. The data type cannot be edited if the metadata field is associated with any certificate values.

   The remaining fields on the dialog—plus the *Hint*—will vary depending on the data type selected. Table 54: Certificate Metadata Data Type Dialog Options shows the fields that appear based on the data type selected.

Table 54: Certificate Metadata Data Type Dialog Options

Data Type	Character Limit	Hint	Default Value	RegEx Message	RegEx Validation	Options
String	400 alpha-numeric with indexing	✓	✓	✓	✓	
Integer		✓	✓			
Date		✓				
Boolean			✓			
Multiple Choice	4,000		✓			✓
Big Text	4000	✓				

8. To set a default value with which to pre-populate the metadata field for new certificate requests made using the Management Portal enrollment pages, enter the desired value in the **Default Value** box, or, for Boolean fields, select the desired radio button. The default value option appears for string, integer, Boolean and multiple choice fields.

9. For string fields, you can choose to enter a regular expression against which entered data will be validated in the **RegEx Validation** field. When a user enters information in a metadata field that does not match the specified regular expression, he or she will see the warning message specified in the **RegEx Message** field. The example regular expression shown in Figure 365: Create or Edit Certificate Metadata Field is:

   ```
   ^[a-zA-Z0-9'_\.\-]*@(keyexample\.org|keyexample\.com)$
   ```

   This regular expression specifies that the data entered in the field must consist of some number of characters prior to the *@* made up only of lowercase letters, uppercase letters, numbers, apostrophes, underscores, periods, and/or hyphens followed by exactly either *@keyexample.org* or *keyexample.com*. For more examples of regular expressions, see Regular Expressions on page 375.

10. For multiple choice fields, enter the series of values that should appear in the field dropdown as a comma delimited list in the **Options** field.

    For example:

Accounting,HR,IT,Marketing,Sales

Note: The multiple choice options are displayed in the order entered in the comma delimited list. When a user selects a multiple choice value in a metadata field while editing a certificate, the value is saved to the database as the string (e.g. Marketing). Subsequently editing the series of values for the metadata field or rearranging them will not affect existing certificates configured with values for this field.

11. Click **Save** to save your metadata field.

Sorting Metadata Fields

You may change the display order for metadata fields. This affects how the fields display on the certificate details, certificate template details when configuring the metadata tab, and on enrollment pages.

To change the display order of a metadata field:

1. Browse to *System Settings Icon* > *Certificate Metadata.*
2. Right-click a grid row and choose **Move** from the right-click menu, or highlight the row in the grid and click **Move** at the top of the grid.
3. In the Display Order dialog enter the desired display order number and click **Save**. The value entered must fall without the current display order range. For example, if the current range is 0-12, enter 12 to move a field to the end of the list, not 13. The metadata field will move to the entered display order row and the metadata fields from the rows above and below will be re-ordered.

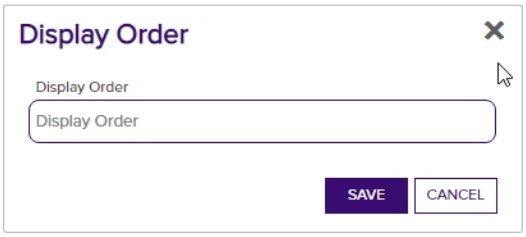


Figure 367: Metadata Display Order

Deleting a Metadata Field

Metadata fields cannot be deleted if they are associated with any certificate values.

To delete a metadata field:

1. Browse to *System Settings Icon* > *Certificate Metadata.*
2. Right-click a grid row and choose **Delete** from the right-click menu, or highlight the row in the grid and click **Delete** at the top of the grid.

2.1.11.5 Audit Log

PKI is more than Keyfactor Command, CAs, and certificates. It also includes the people and polices that interact with these entities. It is therefore critical to track the actions taken within Keyfactor Command that enable management of all entities that make up a PKI, as most attack vectors are only exposed internally. The Keyfactor Command audit logs are an immutable record of all changes made to the state of the application.

The information collected in the audit logs is available for viewing and analysis by several means:

- The data is available for viewing within the Keyfactor Command Management Portal, where a search tool may be used to search for specific logs (see Using the Audit Log Search Feature on the next page).
- The data is output to text-based logs on the Keyfactor Command server and stored for 14 days, by default (see Log Monitoring on page 707). From here, the logs may be collected by a centralized logging solution for analysis.
- The data is output to the Windows event log on the Keyfactor Command server in the Windows application event log. From here, the logs may be collected by a centralized logging solution for analysis. See Keyfactor Command Windows Event IDs on page 727. When analyzing audit logs as written to the Windows event log, it can be helpful to have the translations for the operation codes handy (see Audit Log Reference Codes on page 663). Audit log failures (when Keyfactor Command fails to log to the audit log) are also logged to the Windows event log.
- The data may optionally be copied in real time to a separate server for analysis with a centralized logging solution (e.g. rsyslog, Logstash). For more information, see Audit Log Output to a Centralized Logging Solution on page 726.

Any activity that triggers an audit flag generates an audit record. Auditable activities include actions (e.g. creation, change, deletion) on records in Keyfactor Command that have been configured as auditable (e.g. Certificates, Security, Templates, Application Settings). For a complete list of Keyfactor Command activity that is tracked through the audit log, see Audit Log Reference Codes on page 663.

The audit log page in the Keyfactor Command Management Portal allows you to view all the audit logs stored in Keyfactor Command and perform searches on them. Audit logs are stored for seven years, by default (see Application Settings: Auditing Tab on page 590).

The audit log grid includes these fields:

- Level
  The logging level of the message. Most messages are generated at Information level.
- Category
  The area of Keyfactor Command that generated the audit log (see Audit Log Categories on page 665).
- Message
  The audit log message. The message is made up of the user who took the auditable action, the action the user took, the category the user acted upon, and the name of the object acted upon.
- Timestamp
  The time and date that the message was generated.

The grid can be sorted by clicking on a column header. All columns except Message may be sorted. Click the column header again to reverse the sort order. The grid columns can be arranged in any order desired by click-holding and dragging the header of the column you wish to move. The column widths may be adjusted by click-holding and dragging the line separating two column headers.

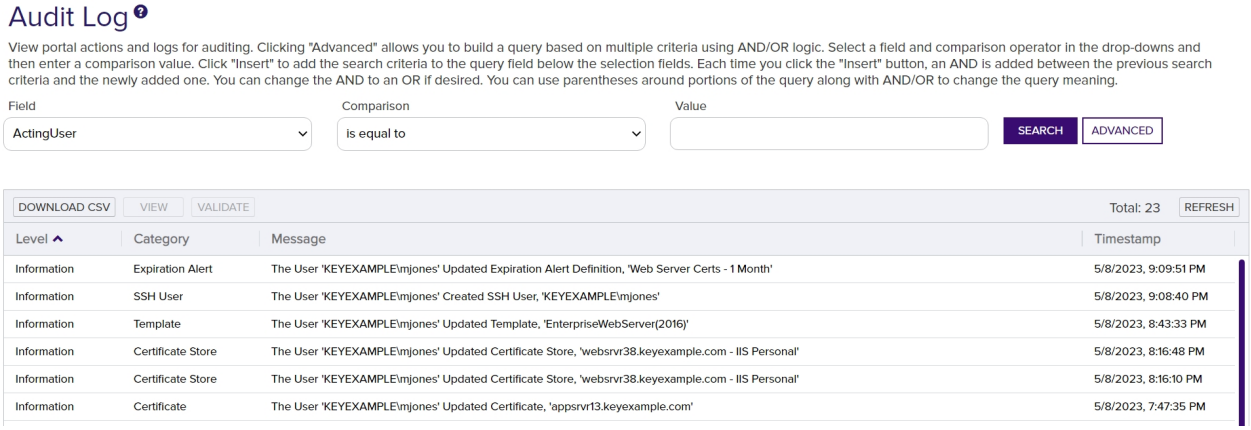


Figure 368: Audit Log

Tip: Click the help icon (?) next to the page title to open the embedded web copy of the *Keyfactor Command Documentation Suite* to this section.
You can also find the help icon at the top of the page next to the **Log Out** button. From here you can choose to open either the *Keyfactor Command Documentation Suite* at the home page or the *Keyfactor API Endpoint Utility*.

Using the Audit Log Search Feature

The search function allows you to query the database for information. The same query structure is used in multiple locations within the Keyfactor Command Management Portal.

When you first open the page, you will see the simple search option. To execute a search, select the field and comparison operators in the dropdowns and type something on which to search in the value field (if applicable). If you select an *is null* or *is not null* comparison operator, the value field will be grayed out. Click the **Search** button to execute the query.

Each query consists of three parts:

Query Field

The available fields for querying vary depending on the area of the Management Portal in which the search is used. On this page, the queries can be done on the following built-in fields:

Acting User	Name

The user who performed the audited action, generally in the format DOMAIN\username, though for actions initiated by the Keyfactor Command Service, this will be *Timer Service*. Supports the %ME% token (see Advanced Searches on page 656).

Level

The logging level of the message:

- Information
  A successful operation that changes the state of the data in the application
- Warning
  Notification of a possible malicious access attempt (e.g. an unauthorized user attempting to access a web page)
- Failure
  Notification that a user was denied access to an activity (this can be used to alert to a possible internal role security issue)

Timestamp

The time at which an action took place. Supports the %TODAY% token (see Advanced Searches on page 656).

Category

The area of the product in which the auditable activity occurred. This list is built dynamically to show only those categories that are actually in your audit log. Select a category (e.g. Template) and for most categories an optional subsearch field (e.g. Template Defaults for templates) to find entries related to

The name of the object being audited. The name of the object is related to the category of auditable activity. If the category is template, the name will be the template name. If the category is SSH user, the name will be the username of the user owning the SSH key. If the category is expiration alert, the name will be the expiration alert name. Some category to name relationships are more clear than others.

For example, in the following audit message for a certificate enrollment, the name is the DN of the certificate:

```
The user 'KEYEXAMPLE\ggant' Created Certificate,
'CN=appsrvr12.keyexample.com,L=Chicago,ST=IL,C=US'
```

In the following workflow instance message, the name is the entire title of the workflow instance:

```
The User 'KEYEXAMPLE\mjones' Completed Workflow
Instance, 'KEYEXAMPLE\mjones is enrolling for a
certificate with CN=websrvr12.keyexample.com.'
```

In the following certificate collection message, the name is the name of the certificate collection that was created:

```
The user 'KEYEXAMPLE\jsmith' Created Certificate
Query, 'Revoked Certs'
```

When you open the details for an audit log record, the name appears at the top of the details dialog as the second part of the dialog title (see View: Audit Log Details on page 659).

Operation

The type of operation performed. See Audit Log Operations on page 663 for a complete list of the available operations.

that category and optional subsearch field (e.g. any changes made to template default settings). See Audit Log Categories on page 665 for a complete list of possible categories.

Comparison Operator

The query comparison operators vary depending on the type of field selected and the specific properties of the field. The list below shows the dropdown list comparison operators, as well as the equivalent query language syntax (in parentheses).

Most string fields (the vast majority of the built-in fields) support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Contains (-contains)
- Does not contain (-notcontains)
- Starts with (-startswith)
- Ends with (-endswith)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Most date and integer fields support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Is less than (-lt)
- Is less than or equal to (-le)
- Is greater than (-gt)
- Is greater than or equal to (-ge)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Most Boolean (true/false) fields support:

- Is equal to (-eq)
- Is not equal to (-ne)
- Is null (-eq NULL)
- Is not null (-ne NULL)

Comparison Value

The value you enter for comparison must match the field type. For example, integer fields only support numerical values. String fields support all alphanumeric characters. Boolean fields only support True or False. The value field is not case sensitive. Date fields support only properly formatted dates and will initially display as mm/dd/yyyy. You can choose to populate the date field by:

- Clicking in a date Value field to open a pop-up calendar to select a date that will populate the field.
- Clicking in a segment of the date format (i.e., mm/dd/yyyy) and entering a value. As you continue to type in any one segment, the cursor will keep moving onto the next segment.

The results that match your search criteria will be displayed in the results grid below the search selection options.

Tip: The *Message* field in the audit log grid is built from the *Acting User*, *Operation*, *Category*, and *Name* fields and is not searchable as the Message. Instead, search by Acting User, Operation, Category, and/or Name.

When you select Category in the query field, a fourth dropdown will appear. This *Property Field* allows you to further refine the search. The options available in this field vary depending on the selection made in the comparison value. Select *Any* to display all of the results for the selected category search combination. Select a specific value in the property field to display all the audit records that had changes to the selected field.

Example: To see only changes made to the template default settings for certificate templates, select *Category* in the query field, *is equal to* in the comparison operator, *Template* in the comparison value, *Template Defaults* in the property field, and click **Search**.

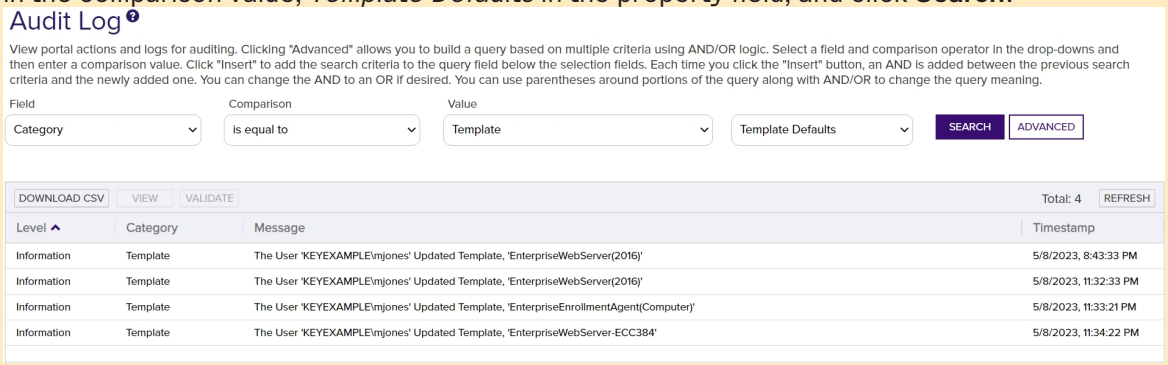


Figure 369: Audit Log Search Selections for Template Property Field Search

Advanced Searches

On any search page you can click **Advanced** to the right of the Search button to display the advanced search options. Click **Simple** to close the advanced search options again.

Multiple Criteria

Using the advanced search options, you can build a query based on multiple criteria using AND/OR logic. As with a simple search, you select a field and comparison operator in the drop-downs and then enter a comparison value, if applicable. Click **Insert** to add the search criteria to the query field below the selection fields. Use the selection fields to build multiple search criteria. Each time you click the insert button, an AND is added between the previous search criteria and the newly added one. You can change the AND to an OR if desired. You can use parentheses around portions of the query along with AND/OR to change the query meaning.

For example, for certificate searches:

```
(CN -contains "appsrvr" AND IssuedDate -ge "01/01/2022") OR (CN -contains "appsrvr" AND
TemplateShortName -contains "web")
```

This query will return all the certificates issued on or after January 1, 2022 with the string appsrvr in the CN and also all certificates issued at any time with the string appsrvr in the CN using a template referencing web. When you have entered all the desired search criteria, click **Search** to execute the query. If you wish to clear the query field and start over, click the **Clear** button.

In addition to the options available in the query builder, three special values can be used in selected searches by typing them in directly:

- %TODAY%
  Use the TODAY special value in place of a specific date in date queries. This option supports math operations, so you can use TODAY-10 or TODAY+30. The built-in *Certificates Expiring in 7 Days* collection uses this special value (see Certificate Collection Manager on page 80).
- %ME%
  Use the ME special value in place of a specific domain\user name in queries that match a domain\user name. The built-in *My Certificates* collection uses this special value (see Certificate Collection Manager on page 80).
- %ME-AN%
  Use the ME-AN special value in place of a specific user name excluding the domain. This is beneficial in environments with multiple domains where there is a desire to query for a user's certificates even if they were requested across multiple domains.

Important: The special query options of %TODAY%, %ME%, and %ME-AN% are only supported in uppercase. Lowercase equivalents (e.g. %me%) cannot be substituted.

Audit Log Operations

The audit log page in the Keyfactor Command Management Portal allows you to perform searches for all the audit logs stored in Keyfactor Command, view details for them, validate that they have not been tampered with, and output selections of them in CSV format.

Download CSV

Click the **Download CSV** button at the top of the audit log grid to generate and download a comma-delimited CSV file containing all audit log records per the search criteria applied to the grid. The CSV file will contain the information shown in Table 55: Audit Download CSV Records for each exported record.

Table 55: Audit Download CSV Records

Field	Description
Id	Sequential Internal reference number
Timestamp	The date and time the auditable change was made.
Message	The message displayed on the audit log grid. This field contains a human-readable summary of the change and is made up of the user who took the auditable action, the

Field	Description
	action the user took, the category the user acted upon, and the name of the object acted upon.
Operation	The operation type (e.g. Created, Updated, Deleted). For a list of possible operations, see Audit Log Operations on page 663.
Level	The logging level of the message (e.g. Info, Warning). Most messages are generated at Information level.
User	The user taking the action that generated that audit log, generally in DOMAIN\username format, though for actions initiated by the Keyfactor Command Service, this will be *Timer Service*.
Category	The area of the product in which the change was made (e.g. Certificates, Templates, Application Settings) as per the available values in the *category* field in the audit grid. For a list of possible categories, see Audit Log Categories on page 665.
Name	The specific object the action was taken on (e.g. the template name for a template change or the application setting name for an application setting change).

XMLMessage	The details of the change that was made in XML format. This field contains both the before state and the after state where applicable (e.g. an application setting that was configured as *true* before the change and *false* after the change). For example, this entry indicates that a change was made to the key retention policy (the template name the change was made to is specified in the Name field) to change the number of days for retention from four days to seven days:
	
	`<AuditAction>`
	`  <ModelState>`
	`  <Template>`
	`  <KeyRetention enum-type=CSS.CMS.Core.Enums.KeyRetentionPolicy">3</KeyRetention>`
	`  <KeyRetentionDays>7</KeyRetentionDays>`
	`  <AllowedEnrollmentTypesDisplay ienumerable="true">`
	`  <string>PFX Enrollment</string>`
	`  <string>CSR Enrollment</string>`
	`  <string>CSR Generation</string>`
	`  </AllowedEnrollmentTypesDisplay>`
	`  </Template>`
	`  </ModelState>`
	`  <PreviousModelState>`
	`  <Template>`
	`  <KeyRetention enum-type="CSS.CMS.Core.Enums.KeyRetentionPolicy">3</KeyRetention>`
	`  <KeyRetentionDays>4</KeyRetentionDays>`

Field	Description
	<AllowedEnrollmentTypesDisplay ienumerable="true"> <string>PFX Enrollment</string> <string>CSR Enrollment</string> <string>CSR Generation</string> </AllowedEnrollmentTypesDisplay> </Template> </PreviousModelState> </AuditAction>"

View: Audit Log Details

To view audit log details for an audit log record, double-click the audit log entry in the audit log grid, right-click the row in the grid and choose **View** from the right-click menu, or highlight the row in the grid and click **View** at the top of the grid. The information on the detail dialog will vary depending on the type of activity that was logged.

The contents of the audit log details dialog will vary depending on the category and object type audited and whether the log item is a new entry or has been updated. The details dialog has four sections.

Name

The Keyfactor Command audit **Name** for the selected audit log entry is in the gray title bar at the top of the dialog. This is a useful field to use in the search criteria.

Entry Metadata

Directly below the **Name** at the top left of the dialog is the **Entry Metadata** section, which displays the internal metadata information about the currently displayed detail record:

- Operation
  The type of activity that generated the audit log record (see Audit Log Operations on page 657).
- Time
  The time and date that the audit log entry was generated.
- User
  The user who carried out the activity that generated the audit log.
- Category
  The area of the product in which the auditable activity occurred (see Audit Log Categories on page 665).
- Validation Status
  Whether the audit log entry in the database is valid or invalid.

Selecting a different entry in the **Related Entries** section will change the display in this section.

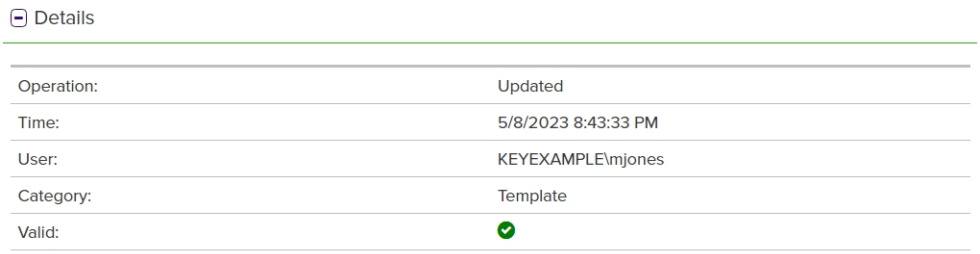


Figure 370: Audit Log Details: Entry Metadata Section

Related Entries

The **Related Entries** tab displays the history of all the related audit log items (e.g. changes to the same template or certificate) for the selected audit log entry. Click a row in the related entries grid and click **View** to update the details dialog with the details of the audit log item for the selected related entry.

The related entries can be sorted by clicking on a the *Time* or *User* column headers in the results grid. Click the column header again to reverse the sort order.

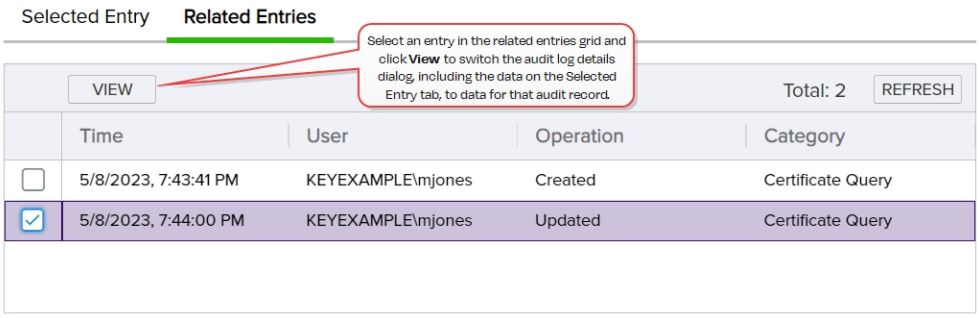


Figure 371: Audit Log Details: Related Entries Section

Note: The Related Entries tab includes all entries, including the initial entry that you opened to reach the tab.

Selected Entries: Audit Details Pane

The Selected Entry tab of the audit log details dialog will either have one column (for new, or single event, entries) or two (for updated items) showing the details of the auditable action.

The title of a single column pane changes depending on the audit entry event that triggered the entry. It is made up of the category and operation performed to create the entry. The details displayed vary depending on the type object being audited.

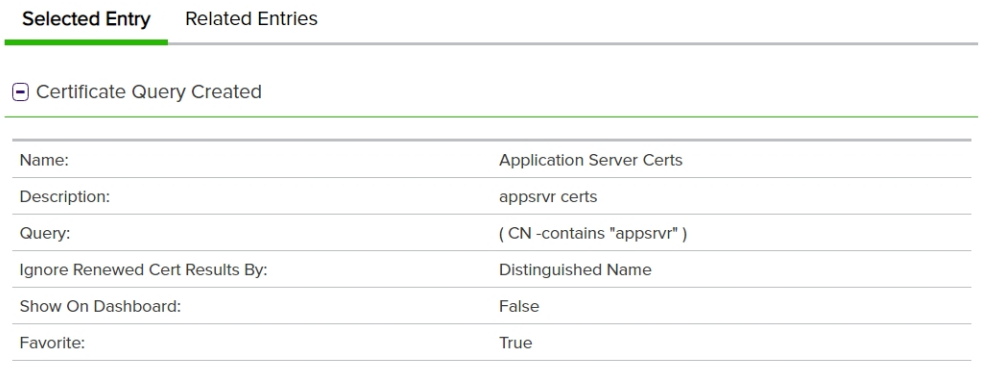


Figure 372: Audit Log Details: Single Column Audit Details Pane

The two column pane includes **Before Changes** and **After Changes** sections. Only those details that have a different value as a result of a particular audit event will be displayed. Changed fields with sensitive data will display as ******.

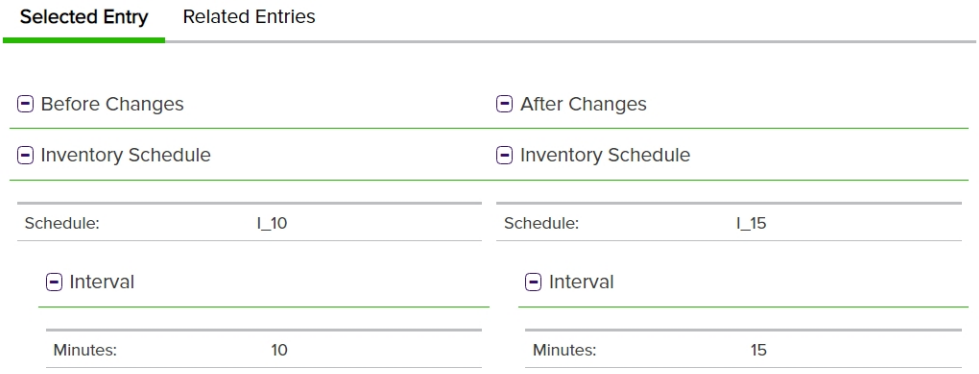


Figure 373: Audit Log Details: Two Column Audit Details Pane

Note: Updates where a field had no value before the update will appear in the single column format.

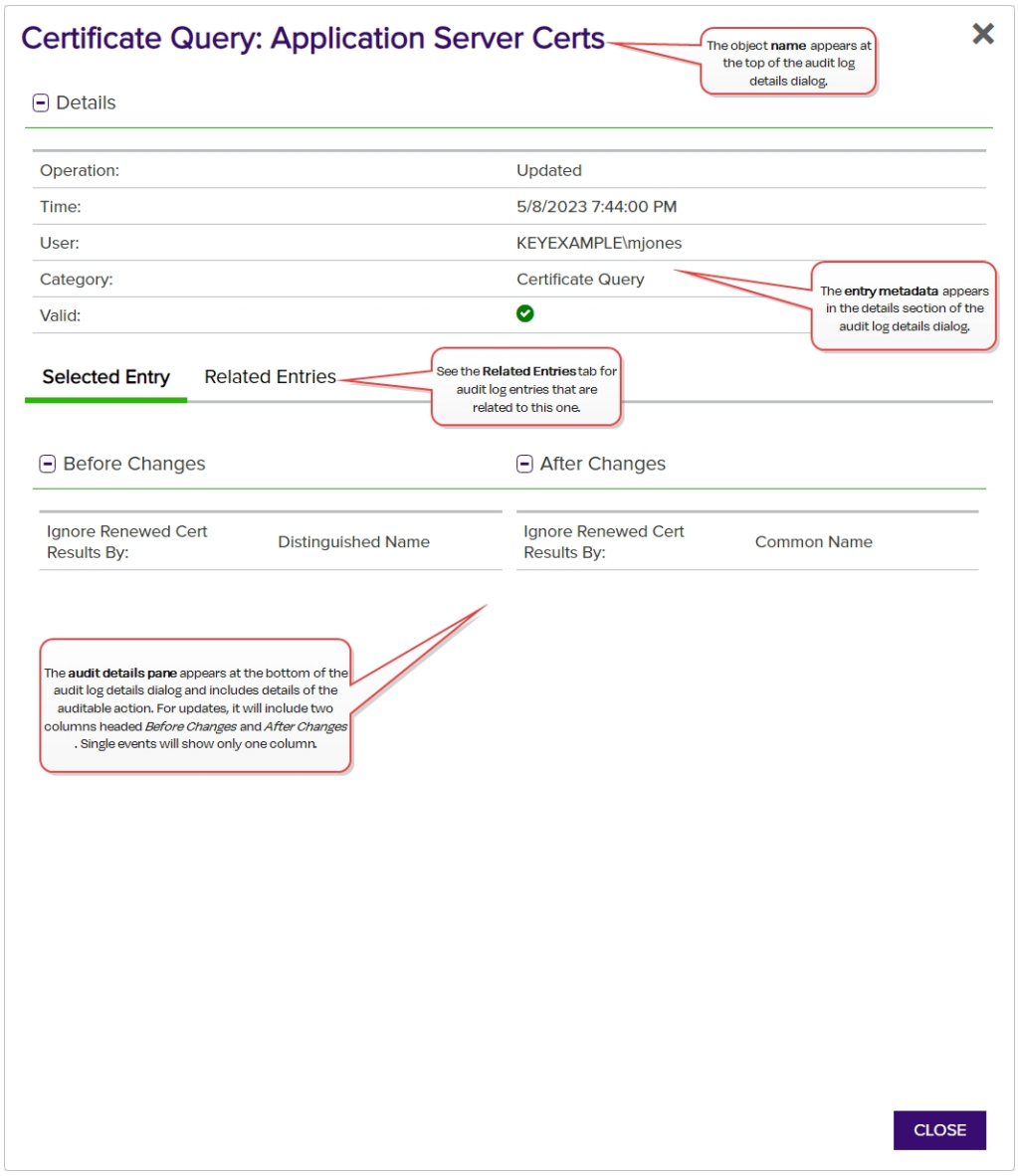


Figure 374: Audit Log Details Dialog

Click **Close** to close the details dialog.

Validate

Highlight a row in the audit log grid and click the **Validate** button to verify whether the selected item is valid or not valid. This function checks the integrity of the audit log data for that grid row to determine whether the data has been tampered with. If the status of the selected item is valid, the validate dialog will indicate this. If the selected item has been tampered with, the validate dialog will indicate that the selected item is not valid.

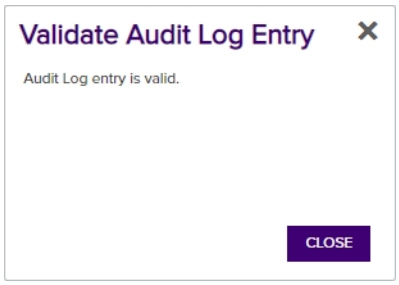


Figure 375: Audit Log Record is Valid

The validation status of any audit log item can also be viewed in the details dialog, where a status of **Valid:** ✔ or **Valid:** ✖ will be shown.

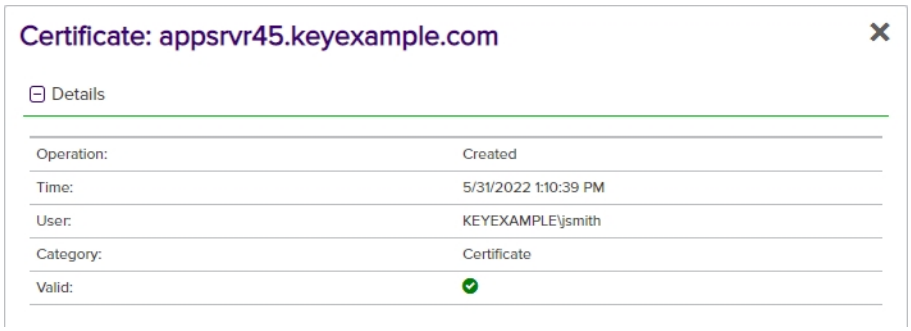


Figure 376: Audit Log Details Showing Valid Status

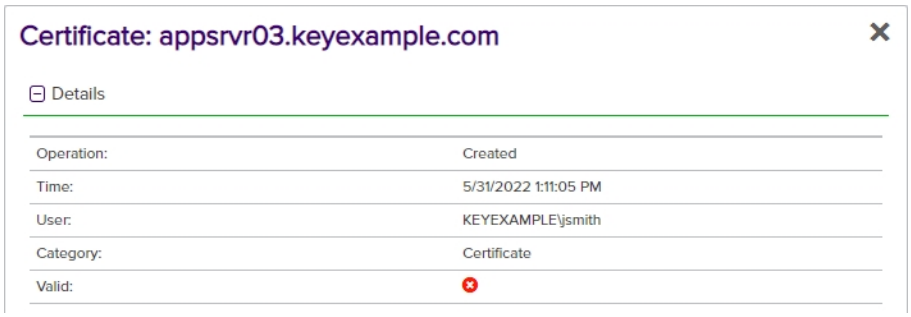


Figure 377: Audit Log Details Showing Invalid Status

Audit Log Reference Codes

The Keyfactor Command audit logs are a record of historical changes that have been made within the product to key systems. The following shows the full list of currently audited areas (areas of the product) and operations (types of activity). The equivalent numeric codes are included for those interested in viewing or analyzing raw log data.

Audit Log Operations

The type of operation performed.

Table 56: Audit Operations

Value	Description
1	Created
2	Updated
3	Deleted
4	Approved
5	Denied
6	Revoked
7	Downloaded
8	Deleted Private Key
9	Renewed
10	Encountered
11	Scheduled Replacement
12	Recovered
13	Imported
14	Removed from Hold
15	Scheduled Add
16	Scheduled Removal
17	Download with Private Key
18	Scheduled
19	Reset
20	Disapproved
21	Restarted
22	Sent

Value	Description
23	Failed
24	Completed
25	Rejected

Audit Log Categories

The area of the product in which the auditable activity occurred. The subcategory name is primarily used in the Keyfactor API or when reviewing downloaded CSV files.

Table 57: Audit Categories

Value	**Subcategory Name**	Description
2001	Certificate	Certificate
2001	AuditingCertificateScheduledReplacement	Auditing Certificate Scheduled Replacement
2001	AuditingCertificateRequest	Certificate Request
2002	ApiApplication	API Application
2003	Template	Template
2004	CertificateQuery	Certificate Collection/Query
2005	ExpirationAlert	Expiration Alert
2005	ExpirationAlertDefinitionContextModel	Expiration Alert
2006	PendingAlert	Pending Alert
2006	PendingAlertDefinitionContextModel	Pending Alert
2007	ApplicationSetting	Application Setting
2008	IssuedAlert	Issued Alert
2008	IssuedAlertDefinitionContextModel	Issued Alert
2009	DeniedAlert	Denied Alert
2009	DeniedAlertDefinitionContextModel	Denied Alert

Value	**Subcategory Name**	Description
2010	ADIdentityModel	Security Identity
2011	SecurityRole	Security Role
2012	AuthorizationFailure	Authorization Failure
2013	CertificateSigningRequest	CSR
2014	ServerGroup	SSH Server Group
2015	Server	SSH Server
2016	DiscoveredKey	Rogue Key for Logon
2016	Key	SSH Key
2017	ServiceAccount	SSH Service Account
2018	Logon	SSH Logon
2019	SshUser	SSH User
2020	KeyRotationAlertDefinitionContextModel	SSH Key Rotation Alert
2021	CertificateStore	Certificate Store
2022	JobType	Orchestrator Job Type
2023	AgentSchedule	Orchestrator Job
2024	BulkAgentSchedule	Bulk Orchestrator Job
2025	CertificateStoreContainer	Store Container
2026	Agent	Orchestrator
2027	RevocationMonitoring	Monitoring
2028	License	License
2029	WorkflowDefinition	Workflow Definition
2030	WorkflowInstance	Workflow Instance
2031	WorkflowInstanceSignal	Workflow Instance Signal

Tip: The Category code of the auditable activity matches the Windows Event ID of the activity.

Audit Logging Specifics

While the Keyfactor Command audit log functionality covers the entire product, the following areas may be of particular interest.

Access Control

When a user tries to access a page in the Management Portal or an API endpoint that they don't have access to, they will receive an error and a warning will be logged in the audit log.

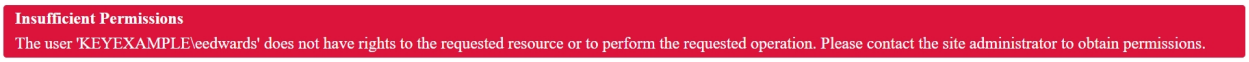


Figure 378: Management Portal Access Denied Message

The audit log shows the level as *Warning* and the category as *Authorization Failure* with a message detailing the user and the requested page.

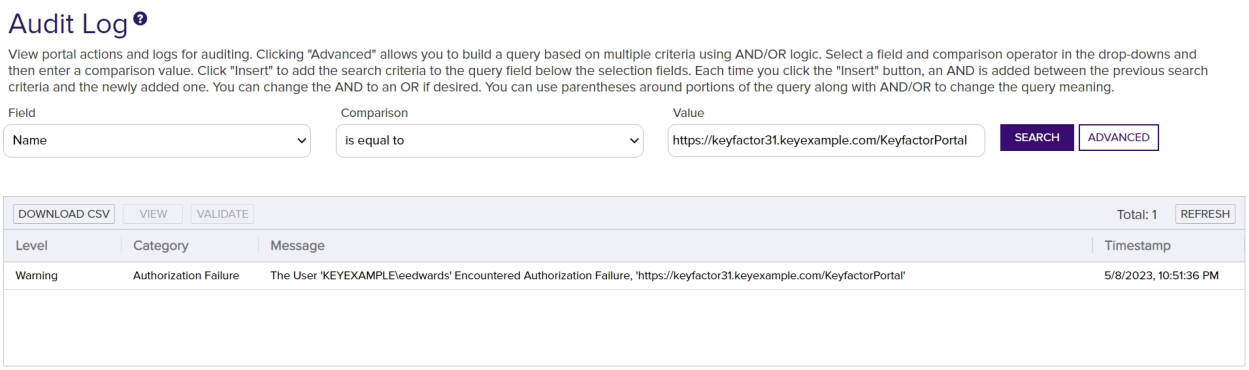


Figure 379: Audit Log Authorization Failure Messages

Click **View** to see the details dialog:

- Username
  The user making the page request.
- Request Route
  The page the user requested.
- Request Type
  Either *API Endpoint* or *Portal Page*.
- HTTP Verb
  This appears for both API requests and portal requests. For API requests, this can help to determine which action was denied.

- User's Roles
  The security role or roles that the user holds (see Security Roles and Identities on page 609). A role will not be listed if the user denied access is not a user in Keyfactor Command.

For more information about the audit log details, see View: Audit Log Details on page 659.

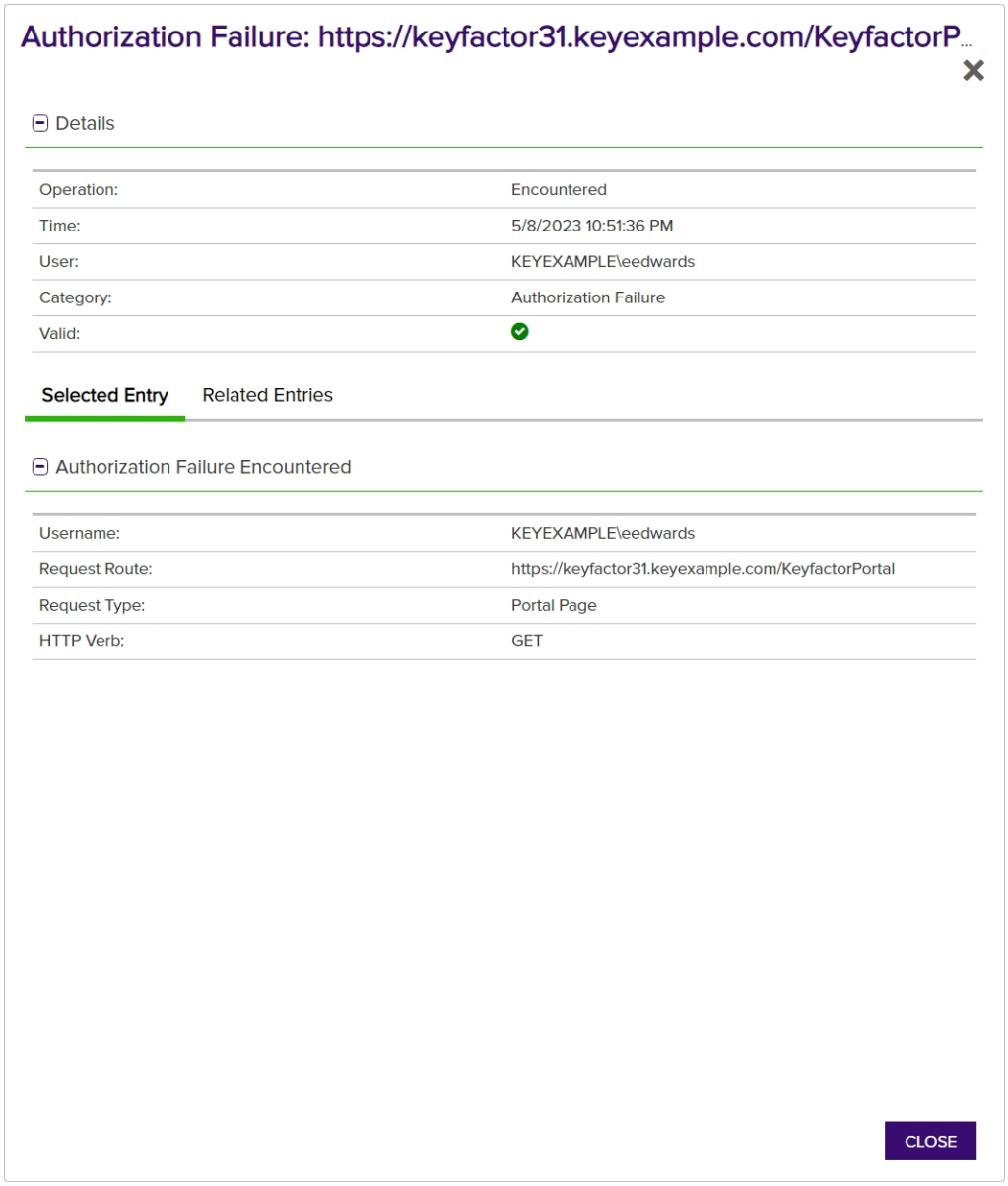


Figure 380: Authorization Failure Audit Log Detail

Certificate Operations

Tracking of operations related to certificates is especially extensive. Certificate-related operations that are audited include:

- Certificate revocation (Category: Certificate)
- Certificate download (Category: Certificate)
- Enrollment for certificates via PFX enrollment and CSR enrollment (Category: Certificate)
- Certificate renewal via one-click or seeded renewal (Category: Certificate)
- CSR generation, re-download and deletion (Category: CSR)
- Approval of certificate requests made using templates requiring manager approval at the CA level (Category: Certificate Request—see also Workflow on page 672)
- Certificate deletion (Category: Certificate)
- Certificate metadata operations—addition of or updates to metadata tags on certificates (Category: Certificate)
- Certificate collection creation or modification (Category: Certificate)
- Addition of certificates to and removal from certificate stores (Category: Certificate Store)

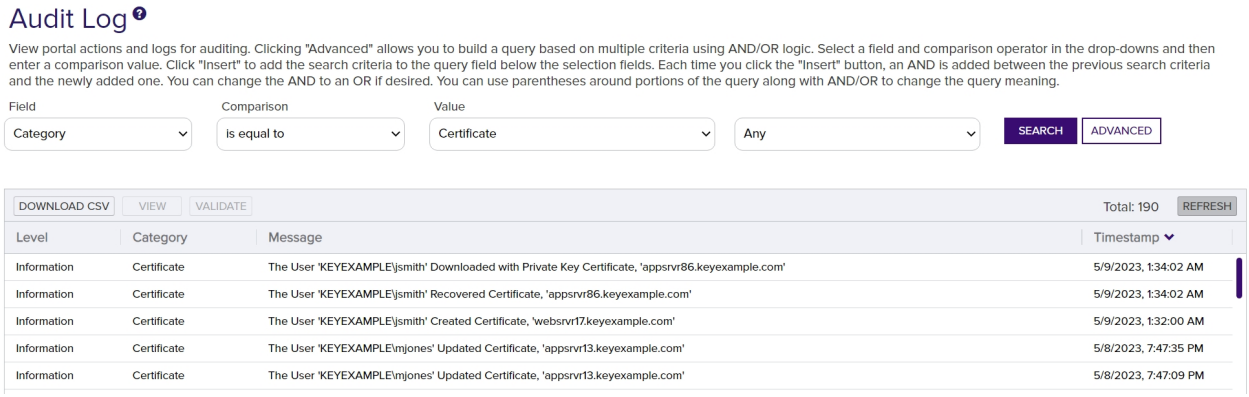


Figure 381: Audit Logs for Certificates

Security

The management of security identities and roles to limit access to the Keyfactor Command Management Portal and Keyfactor API generates audit log entries as roles and identities are created, updated, and deleted. This includes the granting of permissions to roles and the assigning of roles to identities (these are considered updates). The Security Identity and Security Role categories do not cover any attempts to access the system. These are tracked separately using the Authorization Failure category (see Access Control on page 667). Successful authorizations are not logged.

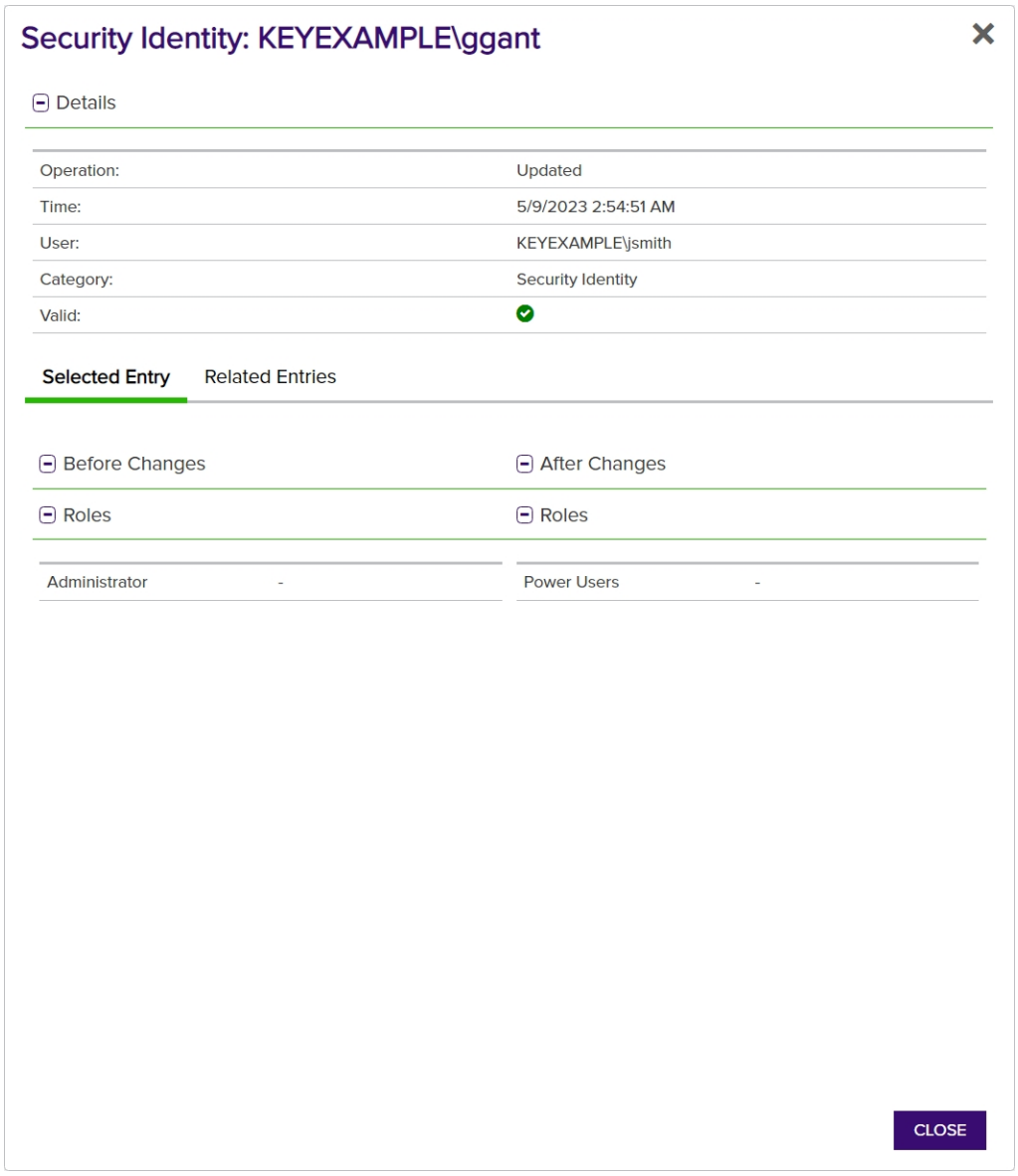


Figure 382: Audit Log Details for Security

SSH

SSH key management with the Keyfactor Bash Orchestrator generates a wide variety of audit log entries, including:

- An SSH user key is created or updated (with an object name of the user)
- An SSH service account key is created, updated, or deleted (with an object name of the service account)
- An SSH key is updated or deleted (with an object name of the public key fingerprint rather than user or service account name—this references the same key as issued for the user or service

account)

- An SSH logon is created, updated, or deleted
- An SSH server is created, updated, or deleted
- An SSH server group is created, updated, or deleted
- A rogue SSH key is identified associated with a logon while scanning a server configured for SSH key management
- An SSH key rotation alert is created, updated or deleted

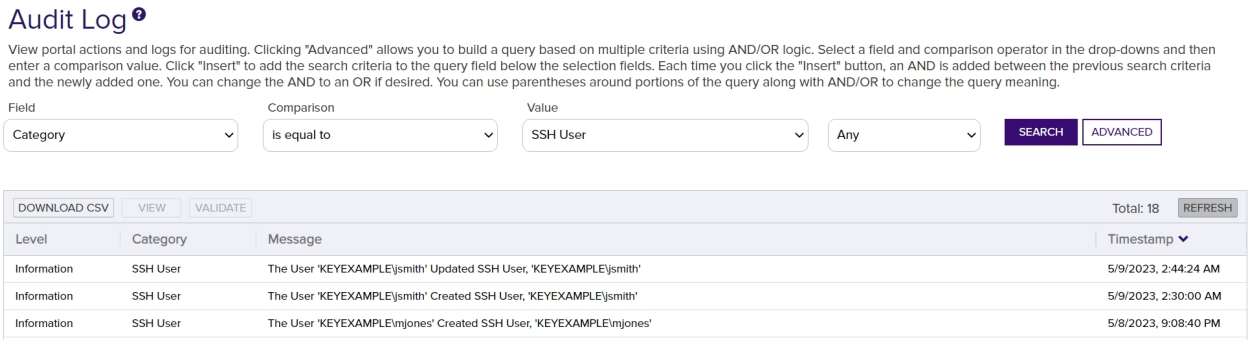


Figure 383: Audit Logs for SSH Management

System Audit Logs

Audit log entries are created during the initial Keyfactor Command installation process when the initial templates and API applications are configured and application settings established. Audit log entries may also be created when you re-run the Keyfactor Command configuration wizard if you make an auditable change in the wizard. When you upgrade from a previous version of Keyfactor Command or make a change in the configuration wizard to an existing Keyfactor Command installation, the audit log entries will show as *Updated*. The exact number of entries created depends on the configuration options selected, number of templates, and the templates configured for enrollment in Keyfactor Command.

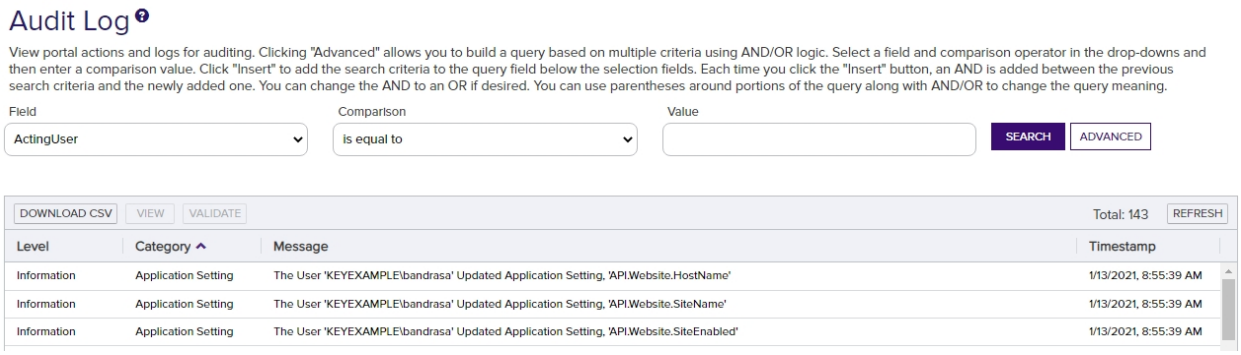


Figure 384: Automated Entries Created by the System in the Audit Log

Workflow

Audit log entries that are generated for workflow include:

- Workflow definition is created
- Workflow definition is imported
- Workflow definition is edited and saved
- Workflow definition is published
- Workflow definition is deleted
- Workflow instance is initiated (created)
- Workflow instance is suspended due to workflow configuration (e.g. the workflow requires approval)
- Workflow instance is stopped manually (this appears as an update to the status of the workflow from Can Receive Signals = True to Can Receive Signals = False)
- Workflow instance is restarted
- Workflow instance failed
- Workflow instance completed

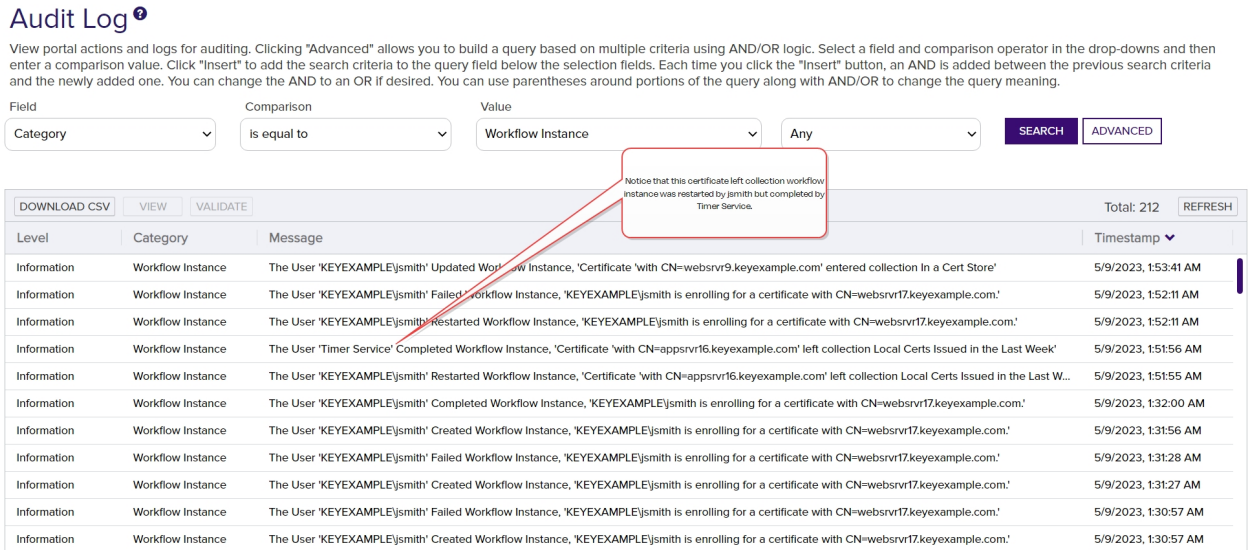


Figure 385: Audit Log Entries for Workflow

For more information about the audit log and using the audit log search feature, see Audit Log on page 652.

Audit Log Security

Keyfactor considers the security and integrity of the audit log to be of the utmost importance and takes steps to ensure that transactions are recorded to the audit log accurately and retained

without tampering until they are purged (by default, after 7 years—see Application Settings: Auditing Tab on page 590).

When Keyfactor Command is installed, a 64-byte key is generated for use in securing audit logs. This key is unique for the implementation. The key is encrypted and stored in the secrets table in SQL using either SQL-level encryption or application-level encryption, depending on the level of encryption selected during installation (see *Install the Main Keyfactor Command Components on the Keyfactor Command Server(s): Database Tab* in the *Keyfactor Command Server Installation Guide*). If application-level encryption is selected, use of a hardware security module (HSM) is supported. For more information, see *Acquire a Public Key Certificate for the Keyfactor Command Server* in the *Keyfactor Command Server Installation Guide*.

When an audit log record is created, the key components of it are signed using the unique 64-byte key and stored in the SQL database. The signature is retained and tracked. When the audit log is read, it is validated using the signature. If the signature does not match, the audit log is flagged as invalid (see Validate on page 662), as this could indicate that the record has been tampered with. The following data is included in the key components:

- The date and time at which the action took place.
- The audit message content, which will vary depending on the type of action that was audited. For example, for a modification to a template, this would include:
  - Template common name (short name)
  - Template name
  - Template OID
  - Key size
  - Key type
  - Configuration tenant (forest)
  - Private key retention setting
  - Key archival setting
  - Allowed requesters setting

  See also Download CSV on page 657.
- The operation type (see Audit Log Operations on page 663).
- The user who performed the auditable action.

In order to access the audit logs, users must be granted the **Read** role permission for the **Auditing** role (see Security Roles and Identities on page 609). Users with auditing Read permissions are allowed to access the audit log page and make API requests to obtain data from the audit log.

Important: Be aware that this permission essentially grants a user global read access to the product since the user will be able to view, from the audit log, many of the actions being taken in Keyfactor Command.

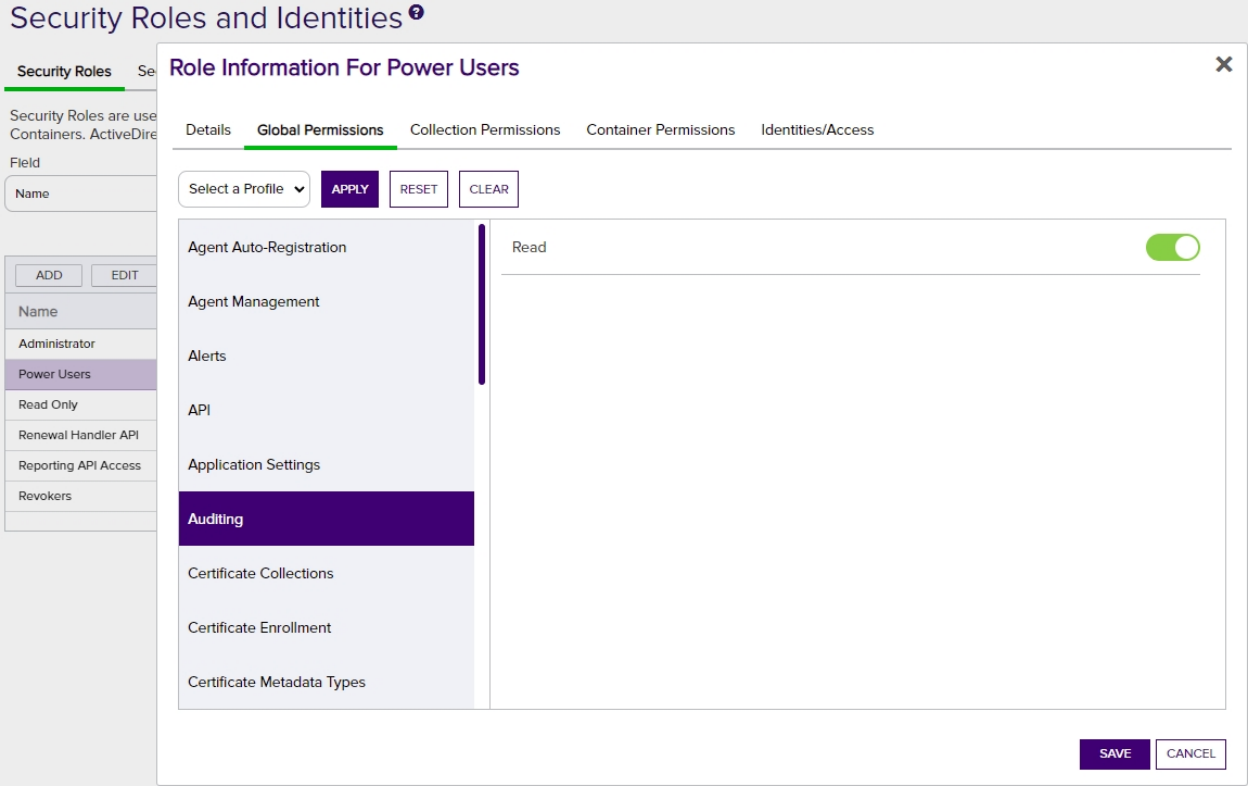


Figure 386: Security Role Showing Auditing Permissions Setting

2.1.11.6 Event Handler Registration

Event handlers are used with expiration and enrollment (pending, issued and denied certificate requests) alerts to trigger additional automated tasks at the time the alerts are run. Keyfactor Command workflows (see Workflow Definitions on page 218) **do not** use event handlers.

Keyfactor provides several event handlers out of the box:

Expiration Logger

Log events to the Keyfactor Command server Windows event log (or other machine event log) for each expiration alert when the alert task is triggered.

Expiration PowerShell

Run a PowerShell script on the Keyfactor Command server for each expiration alert when the alert task is triggered.

Expiration Renewal

Issued PowerShell

Run a PowerShell script on the Keyfactor Command server for each issued certificate alert when the alert task is triggered.

Denied Logger

Log events to the Keyfactor Command server Windows event log (or other machine event log) for each denied request alert when the alert task is triggered.

Denied PowerShell

Execute a certificate renewal for each expiring certificate that is found in a supported certificate store for each expiration alert when the alert task is triggered.

Pending Logger

Log events to the Keyfactor Command server Windows event log (or other machine event log) for each pending request alert when the alert task is triggered.

Pending PowerShell

Run a PowerShell script on the Keyfactor Command server for each pending request alert when the alert task is triggered.

Issued Logger

Log events to the Keyfactor Command server Windows event log (or other machine event log) for each issued certificate alert when the alert task is triggered.

Run a PowerShell script on the Keyfactor Command server for each denied request alert when the alert task is triggered.

SSH Key Rotation Logger

Log events to the Keyfactor Command server Windows event log (or other machine event log) for each SSH key rotation alert when the alert task is triggered.

SSH Key Rotation PowerShell

Run a PowerShell script on the Keyfactor Command server for each SSH key rotation alert when the alert task is triggered.

For information on using built-in event handlers, see Using Event Handlers on page 207.

Tip: Click the help icon (?) next to the page title to open the embedded web copy of the *Keyfactor Command Documentation Suite* to this section.
You can also find the help icon at the top of the page next to the **Log Out** button. From here you can choose to open either the *Keyfactor Command Documentation Suite* at the home page or the *Keyfactor API Endpoint Utility*.

Custom Event Handler Operations

Custom event handlers are used by expiration and enrollment alerts (see Alerts on page 160) but **not** by Keyfactor Command workflows (see Workflow on page 218).

Registering a Custom Event Handler

The built-in event handlers are registered as part of the Keyfactor Command installation. You should only need to use this option if you have a custom event handler.

To register custom event handlers:

1. In the Management Portal, browse to *System Settings Icon* > *Event Handler Registration.*
2. On the Event Handler Registration page, click **Analyze Handler File**.

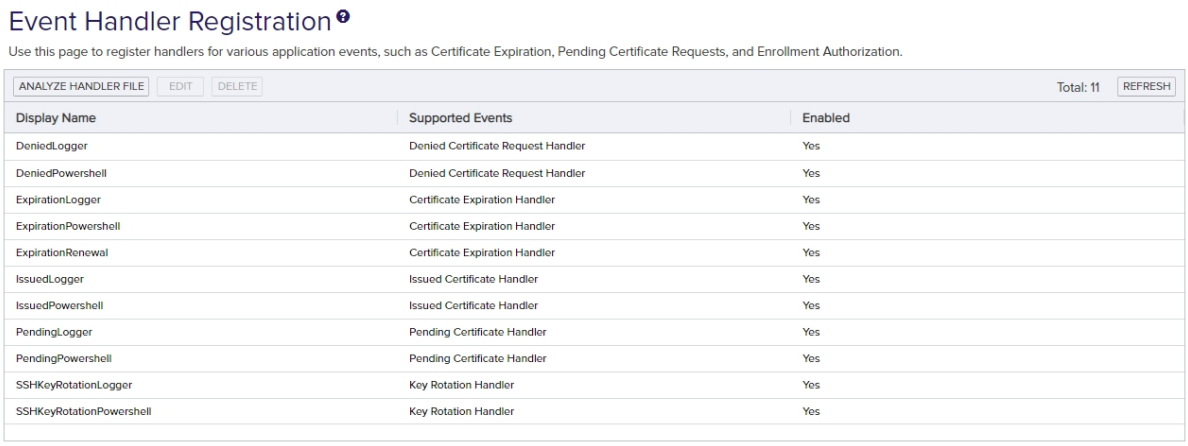


Figure 387: Event Handler Registration Grid

3. In the Analyze Event Handler Assembly File dialog, enter the file name for the event handler file (provided by Keyfactor if the file has been created by Keyfactor) for analysis and click **Save**.

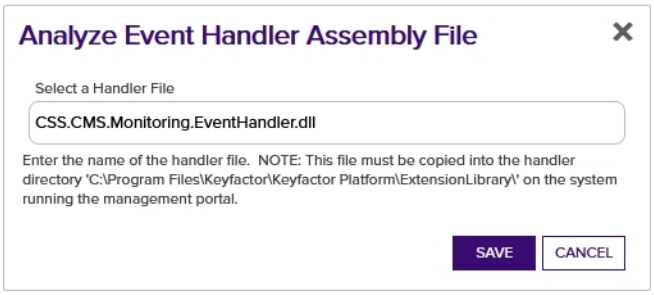


Figure 388: Event Handler Registration

Deleting an Event Handler

To delete an event handler:

1. Browse to *System Settings Icon* > *Event Handler Registration.*
2. Highlight the row in the grid and click **Delete** at the top of the grid.

Editing an Event Handler

To edit an event handler:

1. Browse to *System Settings Icon* > *Event Handler Registration.*
2. Double-click the event handler or highlight the row in the grid and click **Edit** at the top of the grid.
3. In the Event Handler Registration dialog, you can change the **Display Name** for the event handler, if desired. This name appears in the dropdowns in the expiration, pending request, issued certificate, and denied request alert configuration dialogs. You can also disable the event handler by unchecking the **Enabled** box. If you disable an event handler, it will not appear in the dropdowns in the alert configuration dialogs.
4. Click **Save**.

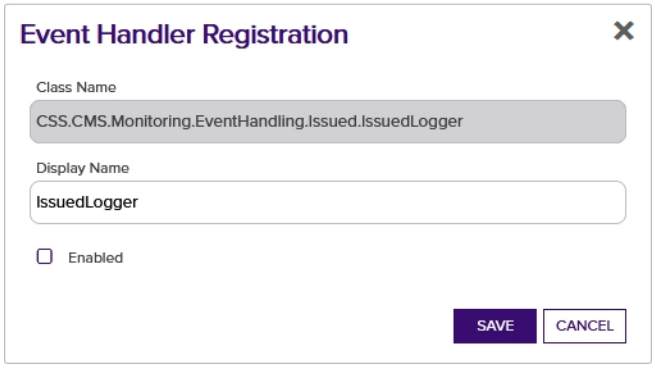


Figure 389: Event Handler Registration Editor

2.1.11.7 Privileged Access Management (PAM)

Privileged access management (PAM) functionality in Keyfactor Command allows for configuration of third party PAM providers to secure certificate stores. In the current release, both CyberArk and Delinea (formerly Thycotic) are supported. The Keyfactor Command PAM solution is made up of three elements:

- Dependencies for your PAM third party solution must be met in order to interoperate with Keyfactor Command (see Preparing Third Party PAM Providers to Work with Keyfactor Command on the next page).
- The PAM provider(s) must be configured in the Keyfactor Command Management Portal (see PAM Provider Configuration in Keyfactor Command on page 691).
- PAM provider security needs to be applied to individual certificate stores (see Adding or Modifying a Certificate Store on page 385).

Tip: Click the help icon (?) next to the page title to open the embedded web copy of the *Keyfactor Command Documentation Suite* to this section.
You can also find the help icon at the top of the page next to the **Log Out** button. From here you can choose to open either the *Keyfactor Command Documentation Suite* at the home page or the *Keyfactor API Endpoint Utility*.

Preparing Third Party PAM Providers to Work with Keyfactor Command

Before you can begin to use one of the third party PAM providers with Keyfactor Command, you may need to complete some initial steps to prepare it for use so that it will be available for interaction with Keyfactor Command. CyberArk requires several configuration steps to install prerequisite software, create required components in the CyberArk PrivateArk software, and register components on the Keyfactor Command server (see Preparing CyberArk to Work with Keyfactor Command below). Keyfactor Command is delivered with the Delinea (formerly Thycotic) dependencies included, but still requires that you have a Delinea Secret Server installed and configured appropriately to work with Keyfactor Command (see Preparing Delinea (formerly Thycotic) to Work with Keyfactor Command on page 686).

Preparing CyberArk to Work with Keyfactor Command

Configuring the CyberArk Credential Provider to interoperate with Keyfactor Command and store Keyfactor Command credentials in the CyberArk vault involves these preparatory steps before configuration in Keyfactor Command can begin:

- Install required software on the Keyfactor Command server.
- Create a safe for the Keyfactor Command credentials in the CyberArk PrivateArk (or identify an existing safe).
- Create passwords in your CyberArk safe for use with your Keyfactor Command certificate stores.
- Create an application user for Keyfactor Command use in the CyberArk PrivateArk.
- Grant the application user and Keyfactor Command provider account in CyberArk appropriate permissions in PrivateArk to the safe.
- Create a credential file on the Keyfactor Command server for use with CyberArk.
- Register the CyberArk software assembly file with Keyfactor Command.

Software Prerequisites

CyberArk has the following software requirements for interoperability with Keyfactor Command:

- Microsoft Visual C++ 2013 (x64)
- Microsoft Visual C++ 2013 (x86)
- CyberArk Credential Provider

Both versions of Microsoft Visual C++ must be installed on the Keyfactor Command server along with the CyberArk Credential Provider software before you proceed to creating a credential file on the Keyfactor Command server or registration of the CyberArk software on the Keyfactor Command server.

Create a CyberArk Application User

Keyfactor Command uses an application user account within CyberArk to retrieve credentials.

To create an application user in CyberArk:

1. Open the CyberArk Password Vault web portal.
2. In the Password Vault web portal, expand the left-hand menu and choose **Applications** > **Add Application**.
3. On the Add Application page, enter a *Name* and *Description* for your application. If desired, enter *Business owner* information. Select **Applications** in the *Location* dropdown. No other configuration changes are required on this page for interoperability with Keyfactor Command, but you may have other configuration settings you may wish to make. Click **Add** to save the record.

   Important: The name you enter in the *Name* field should begin with *App_* (e.g. App_Keyfactor). Make note of the name you enter here. This name becomes your application ID and you will need to reference this from Keyfactor Command.

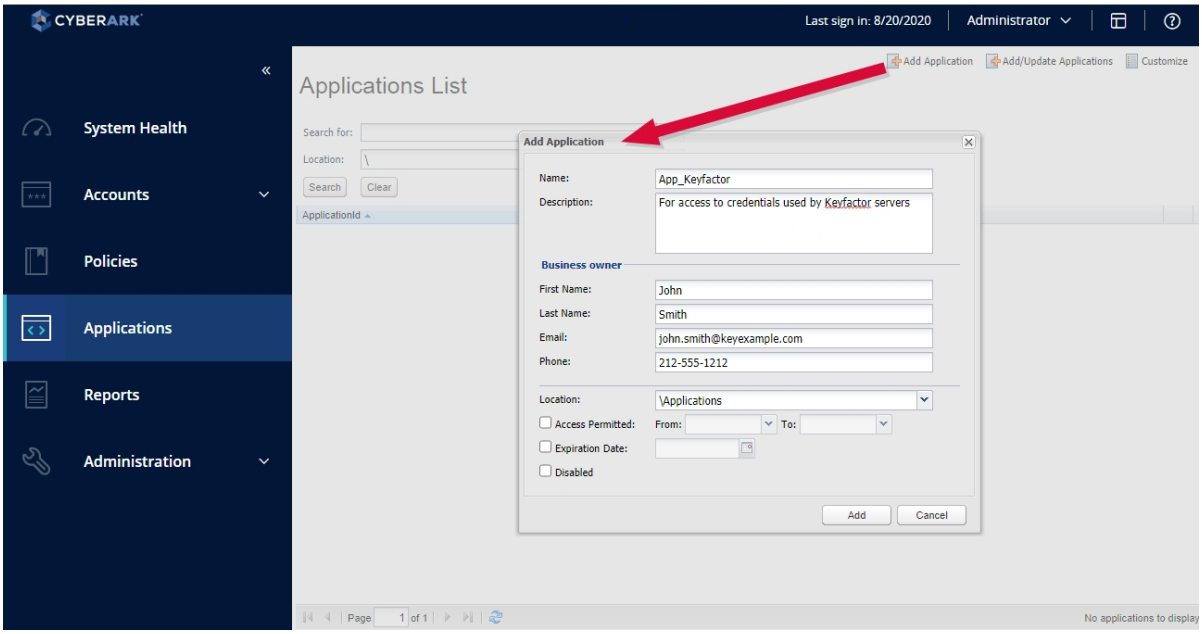


Figure 390: Add an Application User in CyberArk for Use with Keyfactor Command

Create a CyberArk Safe

You will need a CyberArk safe in which to store the certificate store credentials for Keyfactor Command that you wish to manage with CyberArk. You may either create a new one or leverage an existing one. This documentation assumes you will create a new one.

To create a safe in CyberArk:

1. Open the CyberArk Password Vault web portal.
2. In the Password Vault web portal, expand the left-hand menu and choose **Policies** > **Access Control (Safes)** > **Add Safe**.
3. On the Add Safe page, enter a *Safe name* and *Description* for your safe. No other configuration changes are required on this page for interoperability with Keyfactor Command, but you may have other configuration settings you may wish to make. Click **Save** to save the record.

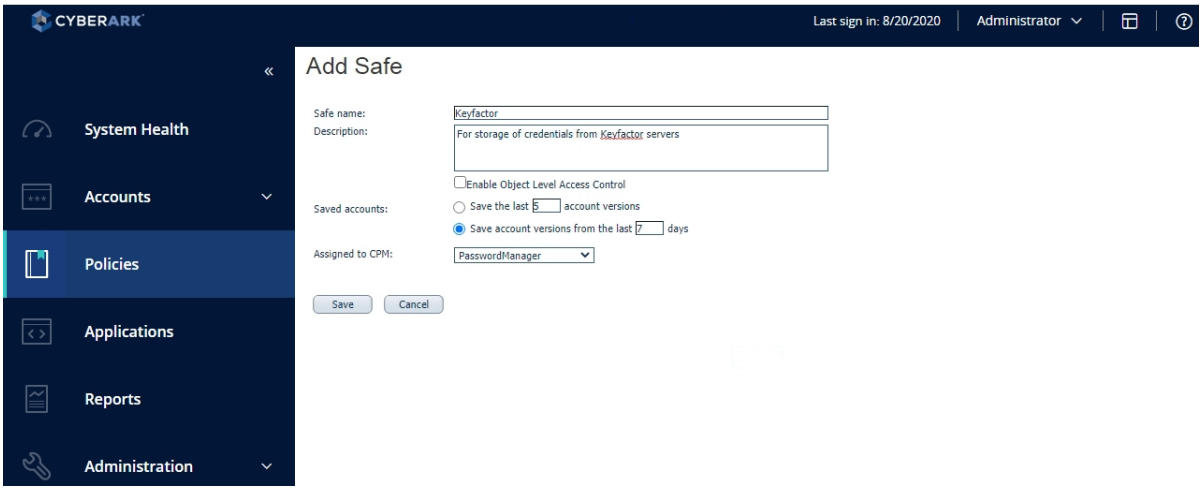


Figure 391: Create a CyberArk Safe for Keyfactor Command

Grant Permissions to the CyberArk Safe

Once an application account and a safe you will use for Keyfactor Command certificate store credentials have been created in CyberArk, you need to grant both the account and the credential provider user on the Keyfactor Command server appropriate permissions to the safe. You may immediately be informed of this upon creating the safe with a warning that "Object level access is not enabled" for the safe. If you receive this message, begin with step three of the instructions for granting permissions.

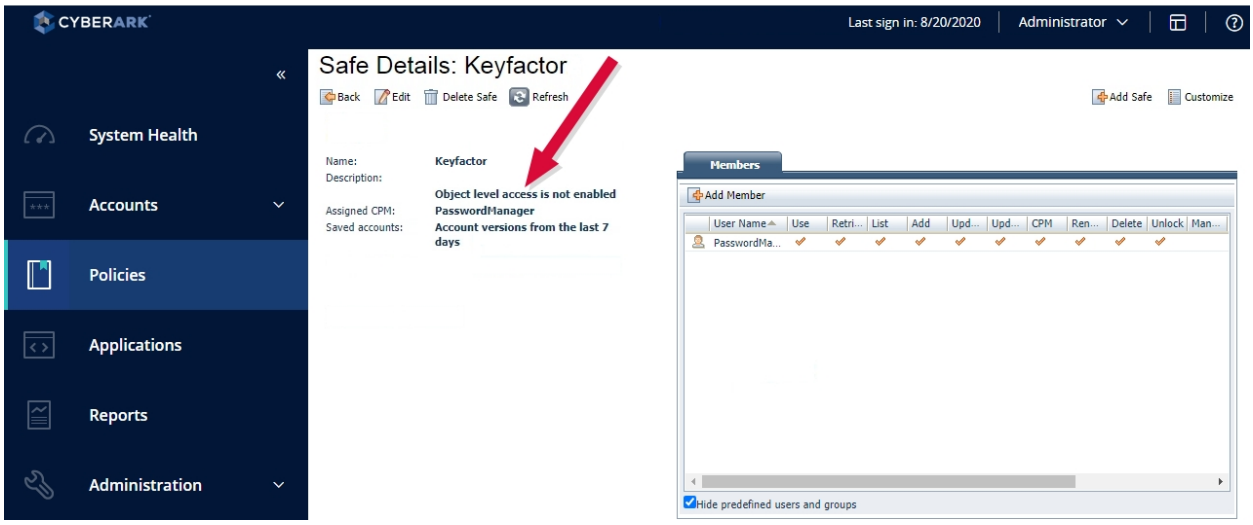


Figure 392: Warning that Access is Not Enabled for CyberArk Safe

To grant permissions to the safe in CyberArk:

1. Open the CyberArk Password Vault web portal.
2. In the Password Vault web portal, expand the left-hand menu, choose **Policies** > **Access Control (Safes)**, and highlight the safe you created for Keyfactor Command credentials. On the lower right part of the screen, click the **Members** icon.

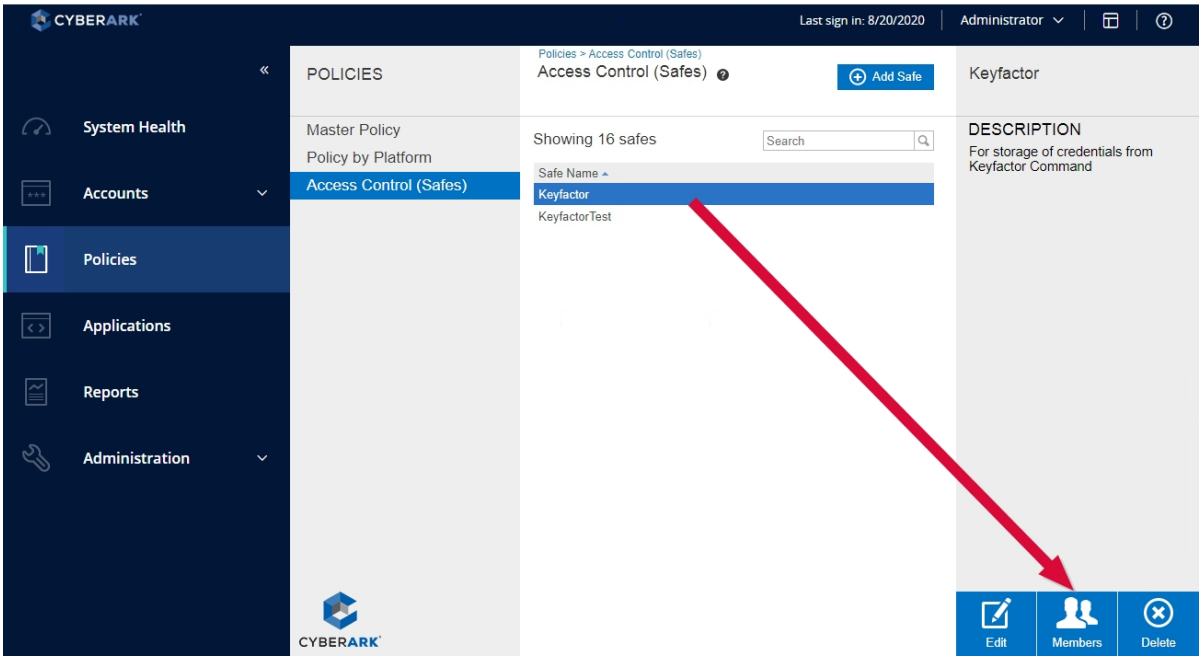


Figure 393: Open Members for the Application User on the Keyfactor Command CyberArk Safe

3. On the Safe Details page in the Members section, click **Add Member**.

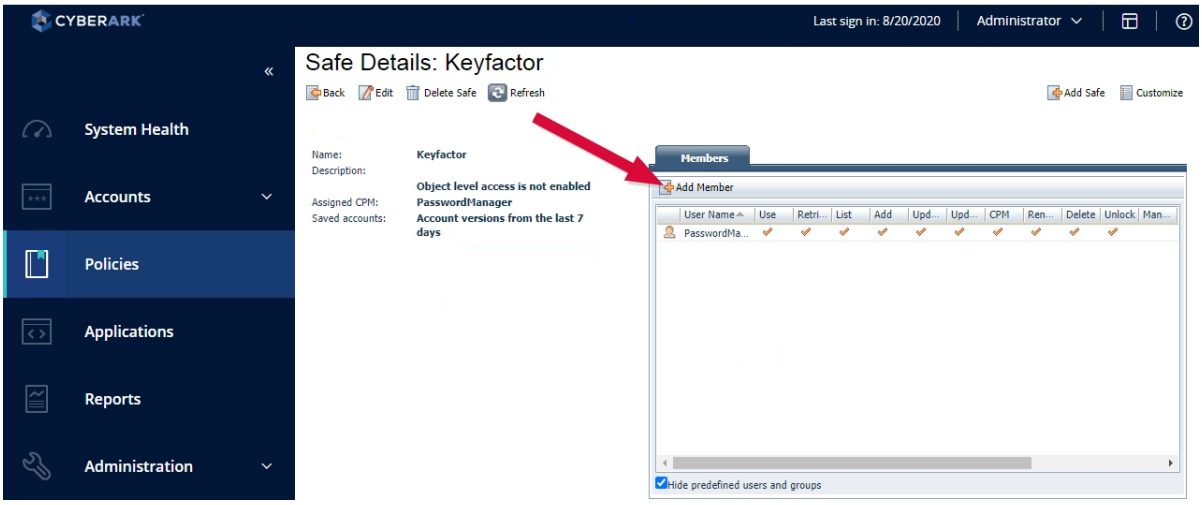


Figure 394: Safe Details for the Application User on the Keyfactor Command CyberArk Safe

4. In the Add Safe Members dialog, search for your application user (e.g. App_Keyfactor), select it in the search results list, and grant the user at minimum the *Retrieve accounts* and *List accounts* permissions under Access and *View Safe Members* permission under Monitor. Click **Add** to save

the permission settings.

Tip: Since Keyfactor Command is designed to read existing passwords from CyberArk and not write passwords to CyberArk, these permissions are sufficient for full functionality.

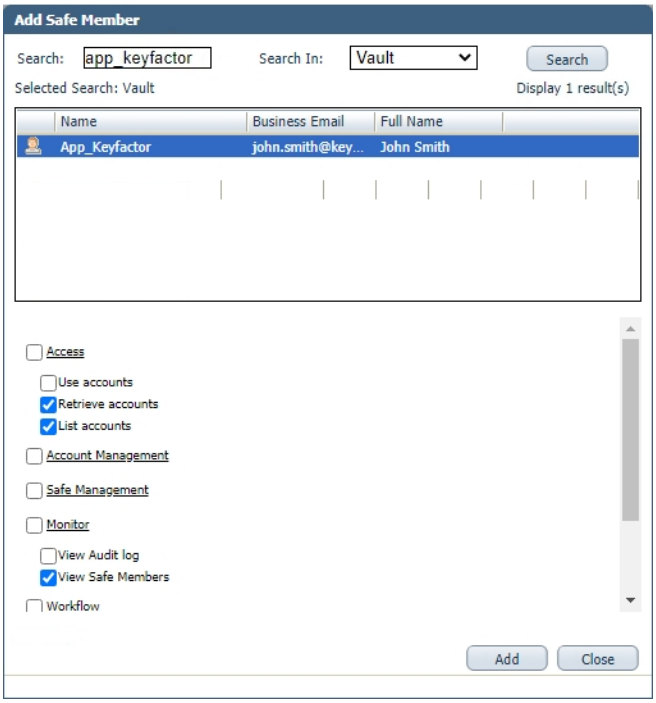


Figure 395: Grant Permissions for the Application User on the Keyfactor Command CyberArk Safe

5. Repeat the previous step for the credential provider user. Typically, this username is Prov_*HOSTNAME* (where *HOSTNAME* is the short hostname of your Keyfactor Command server). You can find the credential provider username in the AppProviderUser.cred file in the ApplicationPasswordProvider\Vault directory under your CyberArk credential provider directory.

Create a CyberArk Password

You will need at least one CyberArk password for each certificate store in Keyfactor Command that you wish to manage with CyberArk.

Tip: Some types of certificates stores (e.g. Java keystores) use the CyberArk safe to store passwords only. Other types of certificates stores (e.g. F5 SSL Profiles, FTP, AWS) can use the CyberArk safe to store both a username and a password for the store in separate PrivateArk objects. For stores that use both a username and password, you have the option to store the username in Keyfactor Command and the password in the CyberArk safe. Both usernames and passwords are stored in the CyberArk safe as password objects.

To create a password in CyberArk:

1. Open the CyberArk PrivateArk application and open your vault.
2. In PrivateArk, locate your safe, right-click and choose **Open and Step Into**.
3. Once the safe opens, optionally create a folder structure on the left under Root and drill down into it to the level where you would like to create your password (e.g. Root\ftp).
4. In your selected folder, right-click in the main window on the right and choose **New** > **PrivateArk Protected Object** > **Password**.

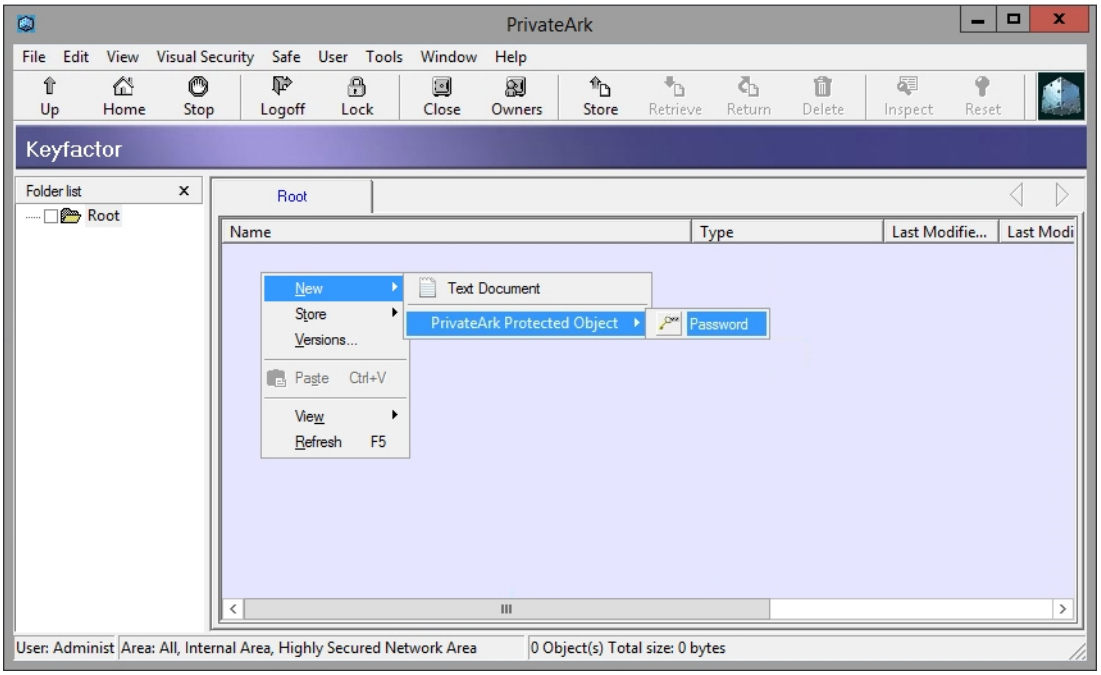


Figure 396: Create a Password for a Keyfactor Command Certificate Store in the CyberArk Safe

5. Enter a name for the object and either generate or enter a password or username.

Register the CyberArk Software Assembly

To register the CyberArk software on the Keyfactor Command server:

1. Acquire a copy of the CyberArk NetPasswordSDK.dll. This is one of the files installed with the CyberArk Credential Provider. Its installed location may vary depending on the CyberArk version and installation options. In some implementations it is found in:

   ```
   C:\Program Files (x86)\CyberArk\ApplicationPasswordSdk\NetPasswordSDK.dll
   ```

2. On the Keyfactor Command server, place a copy of the assembly in the WebAgentServices\bin, KeyfactorAPI\bin, WebConsole\bin, and Service directories under your Keyfactor Command

installation directory. By default, the directory paths for these will be:

C:\Program Files\Keyfactor\Keyfactor Platform\WebAgentServices\bin

C:\Program Files\Keyfactor\Keyfactor Platform\KeyfactorAPI\bin

C:\Program Files\Keyfactor\Keyfactor Platform\WebConsole\bin

C:\Program Files\Keyfactor\Keyfactor Platform\Service

3. On the Keyfactor Command server, open a text editor (e.g. Notepad) using the "Run as administrator" option.

4. In the text editor, browse to open the web.config file in the WebAgentService directory. By default, this file is located in the following directory path:

   C:\Program Files\Keyfactor\Keyfactor Platform\WebAgentServices\web.config

5. If you are using NetPasswordSDK versions 10.5.1.3 , or higher, in the web.config file, locate the **assemblyBinding** section and add a new **dependentAssembly** section containing the following code.

```
<dependentAssembly>
  <publisherPolicy apply="no" />
  <assemblyIdentity name="NetPasswordSDK" publicKeyToken="40be1dbc8718670f"  />
  <bindingRedirect oldVersion="10.5.1.0-10.5.1.3" newVersion="12.4.1.0" />
</dependentAssembly>
```

   Important: The redirect newVersion is 12.4.1.0 for the DLL version 12.4.1.8. The 4th number for the build revision is omitted in the redirect and should be `0` instead for any version targeted.

6. In the web.config file, locate the **container** section and locate the commented out registration section containing the following code, as shown in Figure 397: Enable Registration Entry for CyberArk in web.config File:

```
<register type="IPAMProvider" mapTo="Keyfactor.Command.PAMProviders.CyberArkProvider,
Keyfactor.Command.PAMProviders" name="CyberArk" />
```

Remove the comments to activate the registration section so that it appears exactly as the above code.

```
<!--The following are PAM Provider registrations. Uncomment them to use them in the Keyfactor Product:-->
<register type="IPAMProvider" mapTo="Keyfactor.Command.PAMProviders.CyberArkProvider, Keyfactor.Command.PAMProviders" name="CyberArk" />
<!--<register type="IPAMProvider" mapTo="Keyfactor.Command.PAMProviders.ThycoticProvider, Keyfactor.Command.PAMProviders" name="Thycotic" />-->
</container>
```

Figure 397: Enable Registration Entry for CyberArk in web.config File

7. Repeat the previous two steps for the web.config files found in the KeyfactorAPI and WebConsole directories and the CMSTimerService.exe.config file found in the Service directory. By default, these files are found in the following directory paths:

   C:\Program Files\Keyfactor\Keyfactor Platform\WebConsole\web.config

   C:\Program Files\Keyfactor\Keyfactor Platform\KeyfactorAPI\web.config

   C:\Program Files\Keyfactor\Keyfactor Platform\Service\CMSTimerService.exe.config

Preparing Delinea (formerly Thycotic) to Work with Keyfactor Command

Configuring the Delinea Secret Server to interoperate with Keyfactor Command and store Keyfactor Command credentials in the Delinea vault involves these preparatory steps before configuration in Keyfactor Command can begin:

- Install the required Delinea Secret Server software on a web server in the same forest as the Keyfactor Command server.
- Create at least one secret in Delinea Secret Server for use with your Keyfactor Command certificate stores.
- Create an API user for Keyfactor Command use in the Delinea Secret Server.
- Grant the API user appropriate permissions to the secret(s) you created in Delinea Secret Server.
- Create an API application in Delinea Secret Server.
- Grant the Keyfactor Command application pool user local administrative permissions on the Keyfactor Command server to allow the Delinea SDK to create credential files in C:\Windows\System32\inetsrv.

Software Prerequisites

The Delinea Secret Server software needs to be installed on a web server in the same forest as the Keyfactor Command server. Keyfactor does not recommend installing the Delinea software on the Keyfactor Command server. Please see the Delinea documentation for system requirements and installation guidance. Keyfactor Command is delivered with the Delinea dependencies included and enabled to allow interoperability with Delinea Secret Server, so no configuration steps are required on the Keyfactor Command server to enable to Delinea software.

Note: Keyfactor Command interoperates with Delinea/Thycotic version 10.x. Support for version 11.0 and greater will be available in a future release.

Create a Delinea Secret Server Secret

You need to create a secret or secrets in the Delinea Secret Server for each certificate store in Keyfactor Command that you wish to manage with Delinea.

To create a secret in Delinea Secret Server:

1. Open the Delinea Secret Server application in a web browser.
2. In Secret Server, select **Secrets** from the left menu.
3. On the Secrets page, click the plus button in the top right of the window and choose **New Secret**.
4. In the Create New Secret dialog, select a template type of Password (for passwords, usernames, access keys and all similar types of data).
5. In the Create New Secret dialog, enter at a minimum a **Name** and the password, username, access key or other information to pass to Keyfactor Command in the **Password** field.
6. Click **Create Secret**.
7. Back on the screen where you are viewing your freshly created secret, look up at the URL and make note of the number near the end of the URL (see Figure 398: Delinea Secret Key ID Identification). This is the ID for your secret. You will need this when configuring the secret in Keyfactor Command.

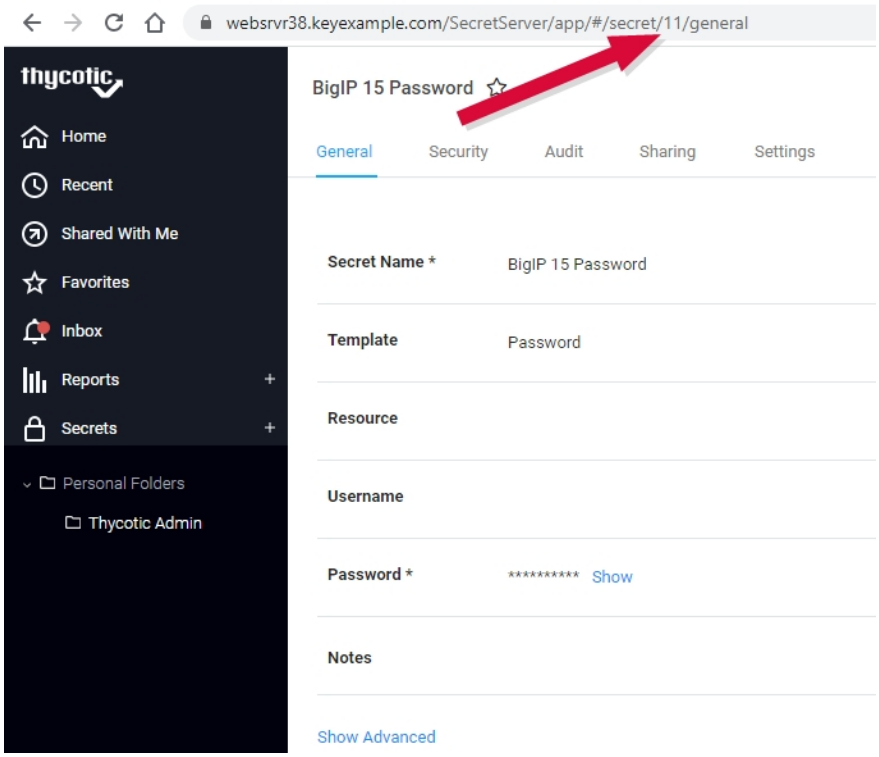


Figure 398: Delinea Secret Key ID Identification

Add an API User for Keyfactor Command in Delinea Secret Server

Keyfactor Command uses an application user account within Delinea Secret Server to retrieve secrets.

To create an application user account in Delinea Secret Server:

1. Open the Delinea Secret Server application in a web browser.
2. In Secret Server, select **Admin** from the left menu and then select **Users**.
3. On the Users page, click **Create New**.
4. Towards the bottom of the Edit User page, click **Advanced**.
5. Enter a **User Name**, **Display Name**, **Email Address** and **Password** for the API user.
6. Under Advanced, check the **Application Account** box.
7. Save the user account.

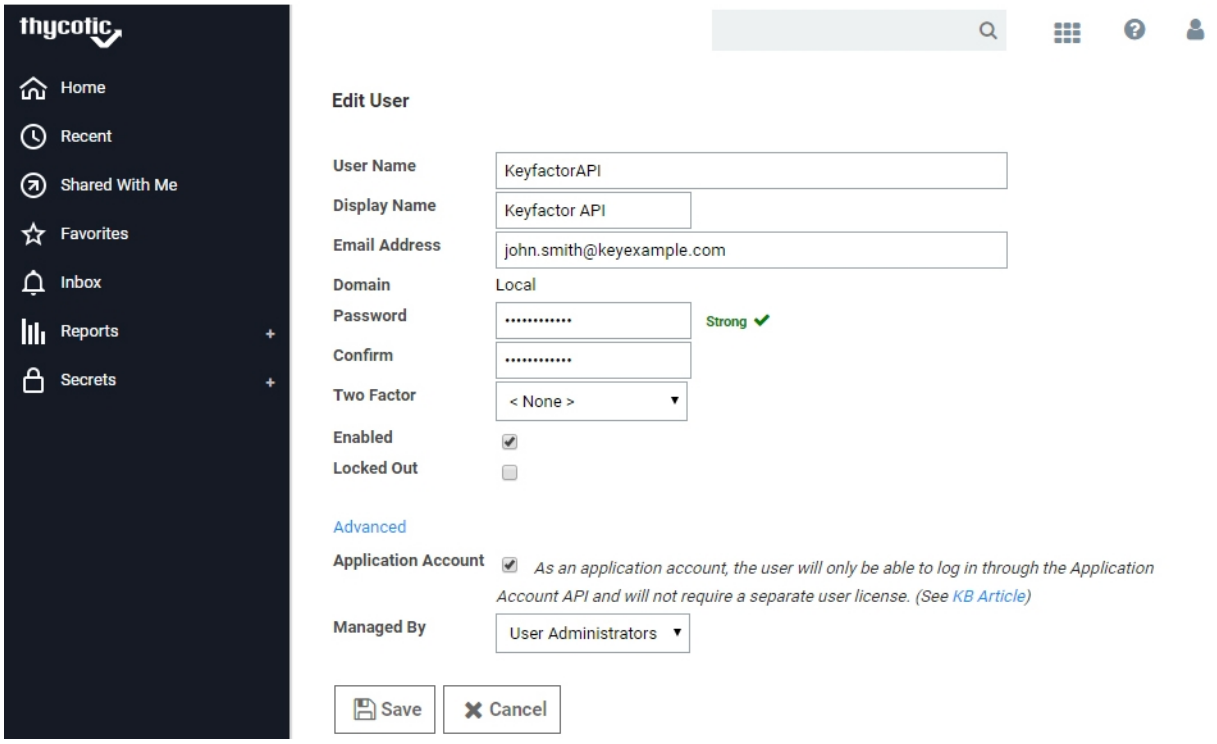


Figure 399: Create a New Application User in Delinea Secret Server

Grant the Keyfactor Command API User Permissions to the Secret(s)

The application user in Delinea Secret Server needs to have permissions to read the secrets that you create for the Keyfactor Command certificate stores. You will need to grant permission separately to each secret you create.

To grant permission to a secret in Delinea Secret Server:

1. Open the Delinea Secret Server application in a web browser.
2. In Secret Server, select **Secrets** from the left menu.
3. On the Secrets page, select one of your secrets to open it.
4. On your the page for your secret, go to the **Sharing** tab.
5. On the Sharing tab, click **Edit**.
6. In the **Add Groups** / **Users** box near the bottom, type in the name of your application user, search and select your user.
7. Give the user, at minimum, the **View** permission.
8. Save the secret record.

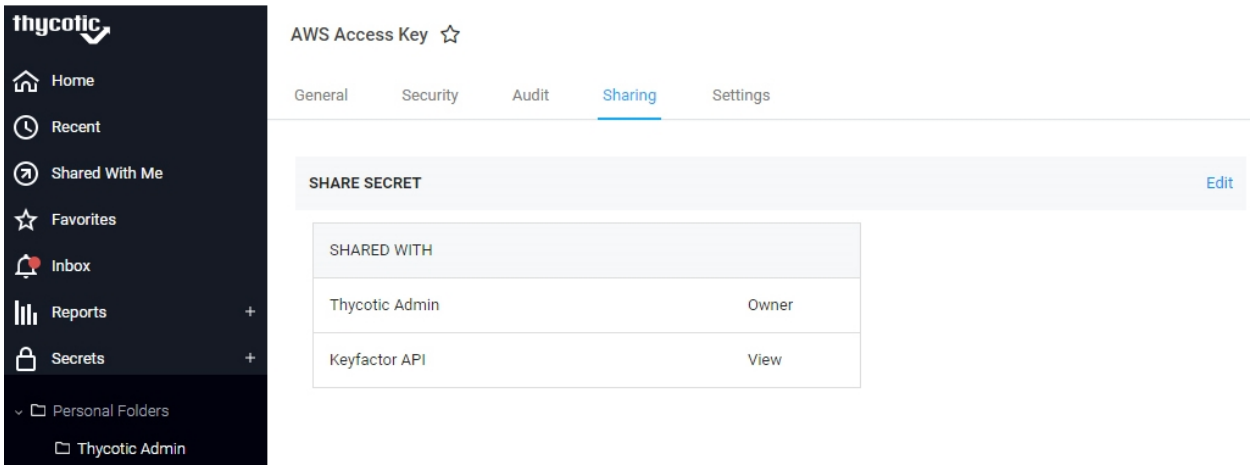


Figure 400: Grant the Application User Permissions to a Secret in Delinea Secret Server

Create an API Application in Delinea Secret Server

Keyfactor Command uses an API application in Delinea Secret Server to interact with Secret Server.

To create an API application in Delinea Secret Server:

1. Open the Delinea Secret Server application in a web browser.
2. In Secret Server, select **Admin** from the left menu and then select **See All**.
3. On the full Administration menu, select **SDK Client Management**.
4. On the SDK Client Management page, click **Client OnBoarding**.
5. At the top right, move the **Disabled**/**Enabled** slider to the right enable this functionality.
6. At the bottom right, click the plus next to **Rule**.
7. Enter a **Name** for the rule. Make note of this name. You will reference it when creating a PAM provider in Keyfactor Command (see PAM Provider Configuration in Keyfactor Command on the next page).
8. In this **Details** field, enter the IP address of your Keyfactor Command server.
9. In the Assignment dropdown, select the application user you created for API use with Keyfactor Command.
10. Check the *Require this generated onboarding key* box.
11. Click Save to save the application.
12. On the SDK Client Management page, click **Show Key** for your new application (see Figure 401: Locate the Delinea Rule Key). Make note of the key shown. This is your rule key. You will need

this when creating a PAM provider in Keyfactor Command (see PAM Provider Configuration in Keyfactor Command below).

Tip: It is very easy when copying the rule key to accidentally grab an extra space at the end of the key. If you paste the key into Keyfactor Command this way when configuring the PAM provider, the error you will receive back from Delinea Secret Server when Keyfactor Command attempts to connect to Delinea Secrect Server does not indicate this is the issue and instead says:

> Object reference not set to an instance of an object

Take care to paste the key in with no leading or trailing spaces.

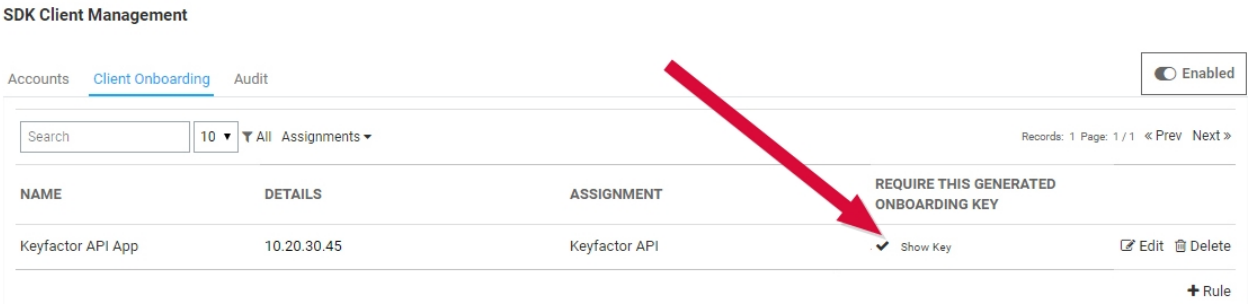


Figure 401: Locate the Delinea Rule Key

Grant the Keyfactor Command Service Account Users Extended Permissions on the Keyfactor Command Server

Keyfactor Command connects to the Delinea Secret Server using Delinea's SDK. The Delinea SDK component on the Keyfactor Command server generates credential files in the C:\Windows\System32\inetsrv directory that allow Keyfactor Command to access Delinea Secret Server. In order to create the files, the service accounts under which the Keyfactor Command application pool and service are running need write access to that directory. Because this is a protected system directory, the only practical way to grant these users the needed access to this directory is to grant the application pool user and service user local administrative permissions on the Keyfactor Command server. Your Keyfactor Command implementation may be using the same service account for both the application pool role and the service role.

PAM Provider Configuration in Keyfactor Command

Any third-party privilege access management (PAM) providers you wish to configure for use with Keyfactor Command must be defined first on the PAM Providers page before they can be assigned to certificate stores (see Certificate Stores on page 380) or used for explicit credentials on a CA (see Adding or Modifying a CA Record on page 330). You can create a single provider for each provider type (e.g. CyberArk), however, if you have opted to organize your certificate stores into containers, you will need to create multiple providers to match your container organization structure (see Certificate Store Containers on page 418). The container field in the PAM provider definition is

not required, but if one is supplied when creating a PAM provider, the PAM provider can only be used with certificate stores in the matching container and it cannot be used with a CA. Likewise, a PAM provider defined with no container would be available for selection when setting passwords for any certificate store that also did not specify a container. A PAM provider configured in this way could be used across a variety of certificate stores or with a CA.

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:
Privileged Access Management: *Read*
Privileged Access Management: *Modify*
Certificate Store Management: *Modify*

Permissions for certificate stores can be set at either the global or certificate store container level. See *Container Permissions* in the *Keyfactor Command Reference Guide* for more information about global vs container permissions.

Adding or Modifying a PAM Provider

To define a new PAM provider or modify an existing one:

1. In the Management Portal, browse to *System Settings Icon* > *Privileged Access Management.*
2. On the PAM Providers page, click **Add** to create a new provider, or, to modify an existing provider, double-click the provider, right-click the provider and choose **Edit** from the right-click menu, or highlight the row in the providers grid and click **Edit** at the top of the grid.
3. In the PAM Providers dialog, select a **Provider Type** in the dropdown. This is the name of the software vendor that provides your Privilege Access Management Solution. This field cannot be modified on an edit.
4. In the **Name** field, enter a name to be used to identify the PAM provider throughout Keyfactor Command.
5. In the **Container** field, select an existing certificate store container in the dropdown, if desired. If you select a certificate store container, the PAM provider will be available to select when creating a certificate store with that same container. If you leave this field blank the PAM provider will be available to select when creating a certificate store without a container or when setting explicit credentials for a CA.
6. The remainder of the fields in the dialog will vary depending on the provider type selected:

   CyberArk

   - **PrivateArk Safe**: Enter the name of the safe containing the certificate store password you wish to use (see Create a CyberArk Safe on page 679).
   - **Application ID**: Enter the name of the application created for Keyfactor Command (see Create a CyberArk Application User on page 678).

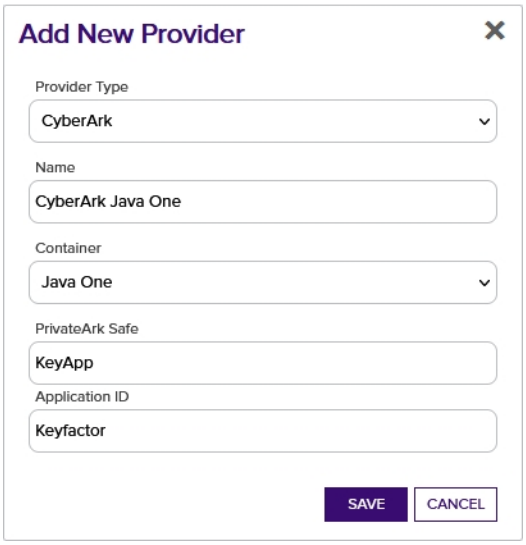


Figure 402: CyberArk Provider with Associated Container

Thycotic (Delinea)

- **Server URL**: Enter the URL to the Secret Server instance in your environment (e.g. https://websrvr38.keyexample.com/SecretServer).
- **Rule Name**: Enter the name of the rule for the API application you created for Keyfactor Command in Delinea Secret Server (see Create an API Application in Delinea Secret Server on page 690).
- **Rule Key**: Enter and confirm the rule key value for the API application you created for Keyfactor Command in Delinea Secret Server (see Create an API Application in Delinea Secret Server on page 690).

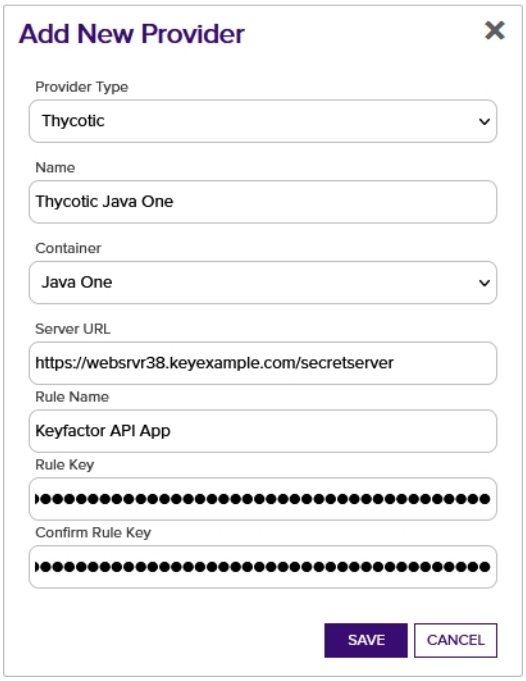


Figure 403: Create Delinea PAM Provider with Associated Container

7. Click **Save** to save the provider.

Deleting a PAM Provider

To delete a provider, highlight the row in the providers grid and click **Delete** at the top of the grid or right-click the provider in the grid and choose **Delete** from the right-click menu.

Tip: If a PAM provider has been associated with any certificate stores or CAs, it cannot be deleted.

2.1.11.8 SMTP Configuration

SMTP settings to enable Keyfactor Command to deliver reports and alerts via email are generally specified during initial Keyfactor Command installation and configuration, but can be modify through the Management Portal if needed.

Tip: The following permissions (see Security Overview on page 605) are required to use this feature:
System Settings: *Read*
System Settings: *Modify*

To make a change to these settings:

1. In the Management Portal, browse to *System Settings Icon* > *SMTP Configuration.*
2. On the SMTP Configuration page, modify the configuration as needed.

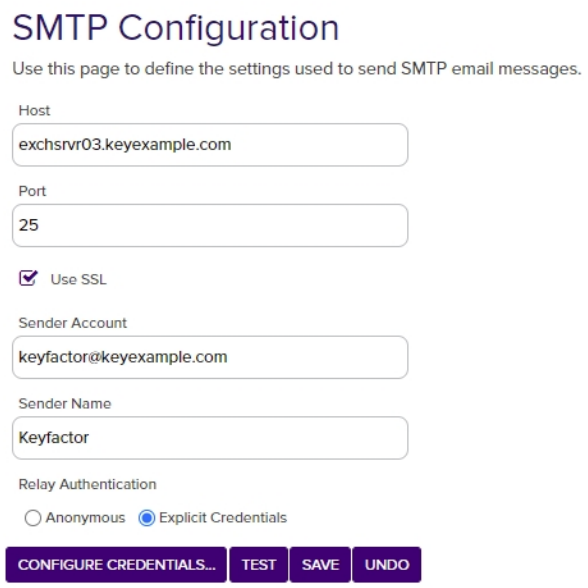


Figure 404: SMTP Configuration

3. Enter the FQDN of your SMTP server in the **Host** field.
4. Enter the SMTP port (default is 25) in the **Port** field.
5. Check the **Use SSL** box if this option is supported by your mail server. Your mail server may not be configured to support TLS/SSL.
6. Set the **Sender Account** name in the form of an email address (e.g. user@keyexample.com). Depending on the email configuration in your environment, the sender account may need to be a valid user on your mail server or you may be able to put anything in this field.
7. Set the **Sender Name** as desired. This is the name that appears as the ”from” in the user’s mail client both with anonymous authentication and explicit credentials.
8. Select the appropriate authentication method for your environment. Some mail servers will accept anonymous. Others may not. If your mail server requires that you provide a username and password for a specific valid user, select the **Explicit Credentials** radio button and click **Configure Credentials**. Enter the valid user’s Active Directory username and password in DOMAIN\username format in the Configure SMTP Relay Authorization Settings dialog. For most mail server configurations, the user you select here must have as a valid email address the email address you set in the *Sender Account* field.
9. You may test the settings prior to saving them. To test the SMTP settings, click the **Test** button, enter a valid email address for a mailbox you can open in the **Send a Test SMTP Message** dialog

and click **Send**. Verify that the test email is delivered.

Figure 405: Send an SMTP Test Message

10. Click **Save** to save any changes you have made.

To cancel any changes you've made without saving, click the **Undo** button.

2.1.11.9 Component Installations

On the Component Installations page you can view the components installed on each of your Keyfactor Command servers and, optionally, delete a server if it has been removed from service.

To delete a server, highlight the row in the component grid and click **Delete** at the top of the grid or right-click the row in the grid and choose **Delete** from the right-click menu. Servers should not be deleted if they are serving any active role in the Keyfactor Command environment, as this operation cannot be undone.

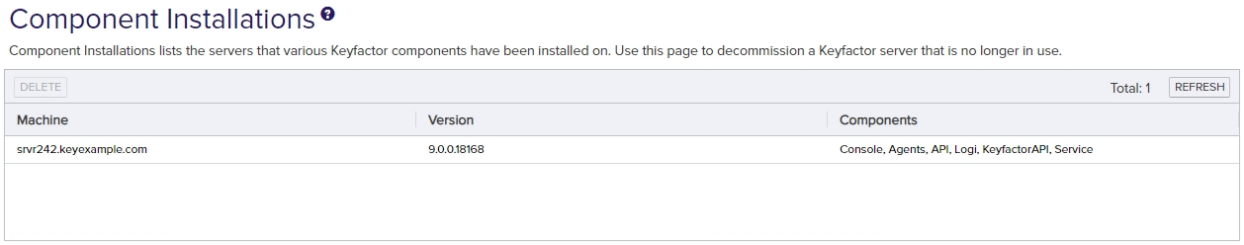


Figure 406: Component Installations

Tip: Click the help icon (?) next to the page title to open the embedded web copy of the *Keyfactor Command Documentation Suite* to this section.
You can also find the help icon at the top of the page next to the **Log Out** button. From here you can choose to open either the *Keyfactor Command Documentation Suite* at the home page or the *Keyfactor API Endpoint Utility*.

2.1.11.10 Licensing

In the Licensing section of the Management Portal you can view the details of your existing license and replace it with a new license, if desired.

To view your existing license, browse to *System Settings Icon* > *Licensing.* The license shows you the features that are enabled for your Keyfactor Command implementation.

For information on monitoring for license expiration, see License Expiration Monitoring and Rotation on page 741.

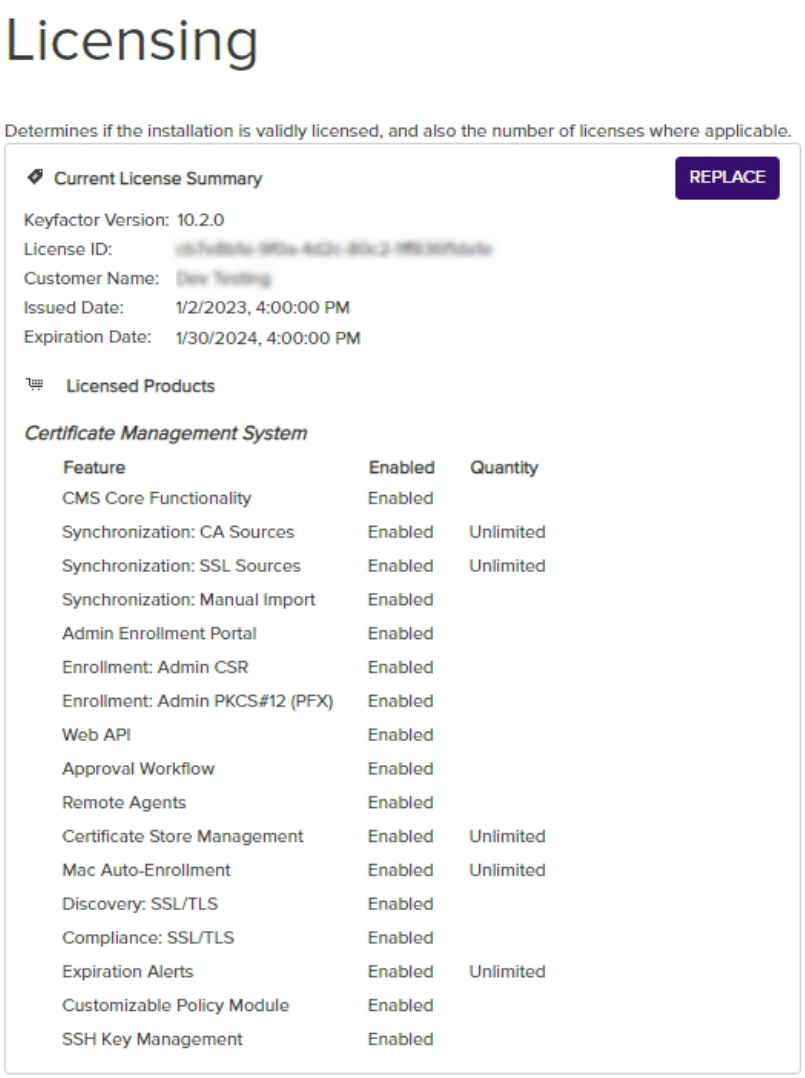


Figure 407: Keyfactor Command License

If you purchase a new license from Keyfactor that enables additional features or extends the expiration date, you can upload it on the Licensing page. To do this:

1. In the Management Portal, browse to *System Settings Icon* > *Licensing.*
2. On the Licensing page, click **Replace**. The Confirm Operation dialog box will open.
3. Click **OK** to open the dialog to upload a new license.

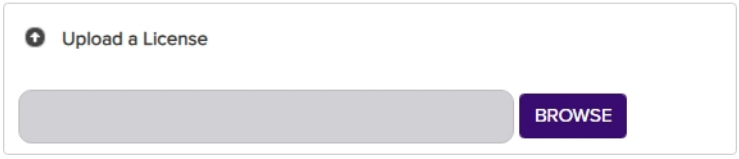


Figure 408: Upload a New Keyfactor Command License

4. Click the **Browse** button and browse to the location on the file system where the new license file provided by Keyfactor is stored.

5. The new license will appear next to the existing license. Compare them to confirm that you wish to install the new license and then click the **Save** to button to complete the license change.

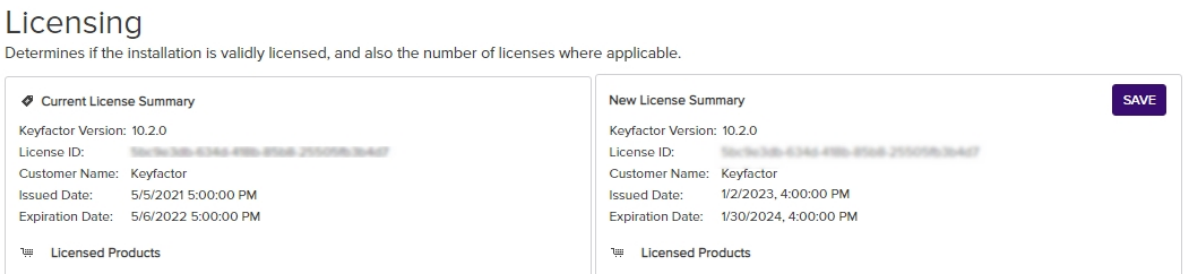


Figure 409: Save a New Keyfactor Command License

6. On the Keyfactor Command server, restart the IIS services (iisreset) and refresh the browser.

Important: If you are installing a new license because your existing license is expiring and you use the Keyfactor CA Policy Module, be aware that the license needs to be installed separately for the policy module (see License Expiration Monitoring and Rotation on page 741).

Tip: Click the help icon (?) next to the page title to open the embedded web copy of the *Keyfactor Command Documentation Suite* to this section.
You can also find the help icon at the top of the page next to the **Log Out** button. From here you can choose to open either the *Keyfactor Command Documentation Suite* at the home page or the *Keyfactor API Endpoint Utility*.

2.2 Operations

Once your Keyfactor Command implementation is up and running, there are a few things you should do regularly to make sure that it stays that way, including backing up to prepare for disaster recovery and monitoring logs and alerts to identify potential issues early and have an overall sense of the health of your Keyfactor Command environment.

2.2.1 SSH Reference

Please see the pages indicated for more detailed information about those specific SSH topics.

- SSH-Bash Orchestrator Job History Warning Resolution below
- SSH-SSSD Case Sensitivity Flag on the next page

2.2.1.1 SSH-Bash Orchestrator Job History Warning Resolution

Previously, it was unlikely the Bash orchestrator would fail during a sync job once it was configured correctly. With the introduction of SSSD support, there is additional validation the orchestrator must do as it applies the configured state that is being passed down from the server. Namely, we must validate that:

- The home directory known by SSSD falls directly underneath the LogonHomeDirectories setting value.
- The location of the authorized_keys directory as understood by SSHD is the home directory known by SSSD.
- The given logon must be resolvable in SSSD.

In the case where one or more of these criteria aren't valid assumptions, the logon won't be created or its keys will not be published. In this case, a message is returned on the Orchestrator Jobs page for the sync job with a Warning result (see Job History on page 498). These messages will continue to be returned until all issues are resolved. The intended resolution for this issue depends on the issue itself. See Table 58: Bash Orchestrator Job History Warning Resolution for examples of possible solutions to issues.

Table 58: Bash Orchestrator Job History Warning Resolution

Issue	Resolution
The home directory known by SSSD doesn't fall directly underneath the *LogonHomeDirectories* setting value.	Change the logon's home directory in the identity source that SSSD is pulling the identity from to be exactly one directory level under the configured value for the *LogonHomeDirectories* setting.
The location of the authorized_keys directory as understood by SSHD is not the home directory known by SSSD.	Modify the local SSHD configuration to ensure that the authorized_keys file can be resolved to the user's home directory and that the user's home directory is nested directly beneath the bash orchestrator's *LogonHomeDirectories* setting value.
A given logon cannot be resolved in SSSD.	• Ensure that the given logon name is valid in SSSD. **Tip:** The bash orchestrator will treat SSSD logon names as

Issue	Resolution
	case sensitive despite the fact that the look up will succeed regardless of case sensitivity. Ensure that the logon name entered matches the logon name as presented by SSSD (see SSH-SSSD Case Sensitivity Flag below). • If the logon is found not be a valid logon on the server, delete the logon on the Keyfactor Command server and try adding the correct one.

2.2.1.2 SSH-SSSD Case Sensitivity Flag

As of RHEL 6 (SSSD package 1.6), a case_sensitive option was added to the valid list of parameters for a given provider in the */etc/sssd/sssd.conf* file. When this value is false, querying SSSD for a given user will return the username in all lower case, regardless of the casing in Active Directory. This value can be set to *Preserving*, which will return the casing used in the username in Active Directory.

The case sensitivity flag is important since attempting to create a new SSH logon in Keyfactor Command (see Adding Logons on page 567) requires that the username is entered as it appears in SSSD, regardless of this setting's value. Using *Preserving* makes the logons look like they do in Active Directory so it may be a less confusing experience for system administrators or those in charge of provisioning the accounts. If this flag is set to false, SSSD will return the name as all lower case characters to preserve POSIX compliance, which is how usernames will need to be entered into Keyfactor Command to create them.

Note: Besides the case-sensitive option setting, there are other SSSD settings that can affect how the username is presented which are not covered in this discussion.

Run the command below in your environment to determine how the username should be formatted.

```
getent passwd username@domain
```

Example:

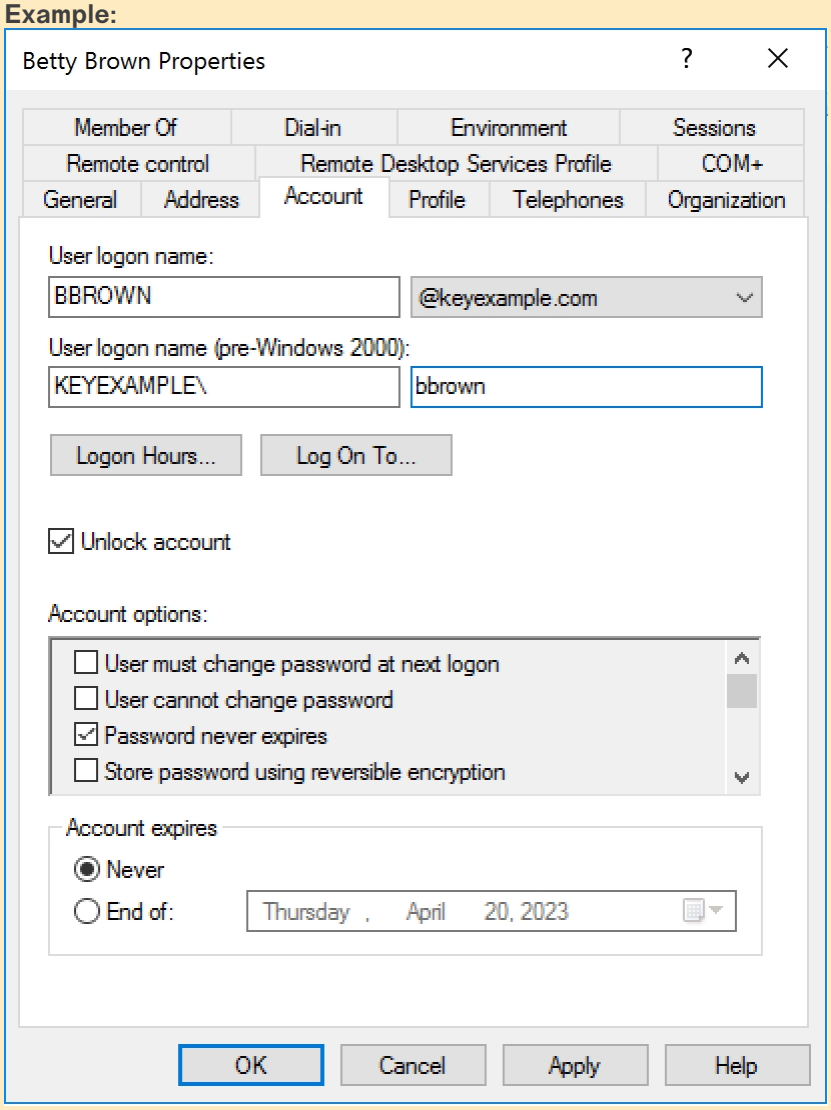


Figure 410: Active Directory Account Properties

The results for the above user with the setting as *false* would be: bbrown@keyexample.com.

```
getent passwd bbrown@keyexample.com
bbrown@keyexample.com:*1689201158:1689200513:Bbrown:/home/bbrown@keyexample.com:/bin/bash
```

The result for the above user with the setting as *Preserving* would be: BBROWN@keyexample.com.

```
getent passwd bbrown@keyexample.com
BBROWN@keyexample.com:*1689201158:1689200513:Bbrown:/home/BBROWN@keyexample.com:/bin/bash
```

Important: This value should not be changed once home directories have already been created on the server, even if done so prior to installing the Bash Orchestrator. Doing so will result in a conflict between Keyfactor Command's understanding of a login's casing and SSSD's. You will then receive an error until this logon is removed or its home directory is updated on the target server.

Example: User *BBROWN@keyexample.com* has a home directory */home/BBROWN@keyexample.com* that is out of compliance with SSSD known directory /home/*bbrown@keyexample.com*.The resolution of this error, in the case of the case_sensitivity property, is to either update the logon's home directory in AD or remove the logon's home directory on the local server and re-add it through Keyfactor Command.

Example: It is also possible for SSSD's understanding of a logon's home directory or account name to change if name of the domain changes in the SSSD config file. In this case, it's expected that the logon is removed from Keyfactor Command, in addition to its home directory on the Linux server, and re-added.

2.2.2 Customize the Management Portal Banner Logo

You can replace the Keyfactor logo at the top left of the Management Portal with your logo, or any .png image, to customize the appearance for your users. The new image will be displayed across the product for every user accessing the Management Portal. This cannot be selectively applied.

To replace the Keyfactor logo:

1. In Windows Explorer, navigate to the \WebConsole\Images directory under the directory in which Keyfactor Command is installed. By default, this is:

   ```
   C:\Program Files\Keyfactor\Keyfactor Platform\WebConsole\Images
   ```

2. Rename the Keyfactor *Banner.png* file to *Banner-original.png* (or any unique name of your choosing).
3. Copy the desired .png image to the folder above.
4. Rename it *Banner.png*.
5. Return to the Management Portal and refresh your browser (CTRL+F5 or F12) to display the changes.

Note: The image must be a .png format. Using any other format will cause an error.

Tip: The default Keyfactor logo size is 310 x 42 pixels. If you choose a different sized image, the spacing on the browser screens will change.

2.2.3 System Alerts

The System Alerts panel appears at the top of the Management Portal page just below the menu bar to display any errors or warnings found within Keyfactor Command. Click on the alerts indicator to toggle the System Alerts panel open/close. Warnings indicate things that may be of concern and appear in yellow. Errors indicate things that may be more urgent and appear in red. Click on the link included at the bottom of the system alert to be taken to the relevant page in the Management Portal to make the required configuration changes or corrections, if applicable. Some examples of conditions for which the system alerts appear include:

- The Keyfactor Command license is approaching expiration (warning)
- The Keyfactor Command license has expired (error)
- Certificate store job failures
- SSL scanning job failures
- NTLM authentication has been detected (and thus enrollment requests won't succeed)

Some system alerts are global and will appear on the system alerts panel regardless of where you are in the Management Portal. Other system alerts (such as some related to SSL scanning) are specific to a particular Management Portal page and will only appear when you are on that page.

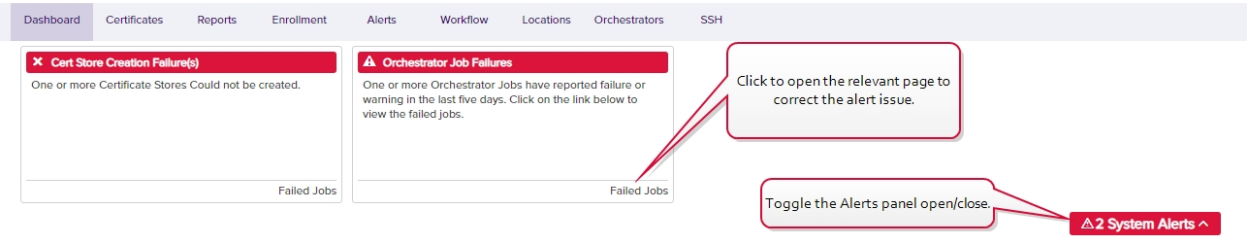


Figure 411: Management Portal Errors and Warnings

2.2.4 Disaster Recovery

Preparing for recovery of your Keyfactor Command server in the event of a disaster or in anticipation of a planned event such as a software upgrade or hardware migration involves backing up several different components. The bulk of the data for a Keyfactor Command server implementation is stored in a SQL database, so backing up this SQL database regularly is key. A portion of the data stored in this database is encrypted, so you will need the appropriate components to allow you to access this encrypted information.

Ideally, your disaster recovery plan would include backing up each server hosting a Keyfactor role as a whole entity. This greatly simplifies recovery. With a plan of this sort, you would need these backed up components:

- Keyfactor Servers

  Each server hosting a Keyfactor role—your Keyfactor Command servers, any Keyfactor orchestrators, etc.—should be backed up as entire entities with the full OS and installed applications.

- Your Keyfactor Command SQL Database

  All the Keyfactor Command data—both configuration data and synchronized data such as certificates—is contained within one database, which should be backed up regularly.

- The SQL server Database Master Key (DMK) and Service Master Key (SMK) for your SQL Database

  If you need to restore your SQL database to a different SQL server instance than the one from which it was backed up, you will need either the DMK or the SMK. There are pros and cons to restoring with each of these, so it can be useful to have both available when you make the restore decision. These only need to be backed up once unless you change either of these in SQL. See SQL Encryption Key Backup on the next page.

If backing up each server as a whole entity is not feasible or you would like to also back up components on the servers that differ from a stock install, consider including the following items for backup:

- Your nlog.config Files

  The various Keyfactor Command server components and most other Keyfactor products have an nlog.config file that sets the logging level for the product and the output path for the log files. If you have made any customizations to any of these configuration files, you may find it useful to make a backup of them. For Keyfactor Command server, the Nlog.config files for the various Keyfactor Command components are in application-specific subdirectories under the installation directory, which is by default:

  ```
  C:\Program Files\Keyfactor\Keyfactor Platform
  ```

  For example:

  ```
  C:\Program Files\Keyfactor\Keyfactor Platform\WebConsole\NLog_Portal.config
  C:\Program Files\Keyfactor\Keyfactor Platform\KeyfactorAPI\NLog_KeyfactorAPI.config
  ```

- Customizations for PAM Configuration

  If you have implemented a PAM solution and manually made configuration changes for this (see Preparing Third Party PAM Providers to Work with Keyfactor Command on page 678), you may want to include these files in a one-time backup.

- Event Handler Scripts

  If you have implemented any event handler scripts for alerting (see Using Event Handlers on page 207), you may want to backup these files.

- PowerShell Scripts for Workflow

If you have implemented any custom PowerShell steps for that use external scripts (see Workflow Definitions on page 218), you may want to backup these files.

- Any Other Text-Based Files

  If you have modified any other text-based configuration files on your Keyfactor Command server (this is uncommon), you will want to have a one-time backup of these.

The process of restoring from backup depends on the components that have been affected. If only the Keyfactor Command server has been lost but the database is intact, the server may be restored from backup and re-connected to the existing database. If a whole server backup does not exist, a fresh server may be installed, Keyfactor Command installed again and connected to the existing database, and any customized files restored or recreated. If the SQL database is lost, the database must be restored from backup along with either the DMK or SMK (see SQL Encryption Key Backup below).

For assistance with disaster recovery planning or implementation, please contact Keyfactor support (support@keyfactor.com).

2.2.4.1 SQL Encryption Key Backup

Keyfactor Command uses Microsoft SQL Server Encryption to encrypt portions of the database to protect secret data, including service account credentials. Understanding Keyfactor Command's use of SQL Server Encryption is important to a successful disaster recovery strategy.

SQL Server Encryption uses a SQL Server instance-level service master key (SMK) and a database-level database master key (DMK) to provide the top-level encryption hierarchy used when encrypting SQL data. The DMK is protected by one or more passwords and optionally the SMK. For an application—such as Keyfactor Command—to access SQL encrypted data, the application must either provide one of the DMK passwords or ask SQL Server to access the data via the SMK. Keyfactor Command uses the SMK. For more details on the mechanics of SQL Server Encryption and related disaster recovery procedures, see the SQL Server documentation.

When the Keyfactor Command database is created, the DMK is configured to be protected by the SMK and then the DMK password is set to a random value, which is not retained. This means the only way to get to the encrypted data is by leveraging the SMK, which happens automatically without any user interaction or the need to store the DMK password in a potentially insecure location.

Different restoration scenarios may require a backup of the SMK or the DMK or neither. Some restoration possibilities include:

- In the case where a Keyfactor Command database needs to be restored to the same SQL server where the backup was taken **and** the SQL Server software itself is not being restored, the correct SMK will still be present on the SQL server and restoration of the database itself is sufficient to be able to access the encrypted data.
- In the case where a Keyfactor Command database is being restored to a SQL Server with a different SMK (either a different SQL Server or the same SQL server that has been reinstalled or had its SMK changed), the encrypted data will be inaccessible because the server level SMK is not the same as it was when the DMK was created. In this scenario, either the DMK needs to be restored from the backup taken when the Keyfactor Command database was created or a

known DMK password may be used to recover encrypted data within the Keyfactor Command database. To prepare for this scenario, the configuration wizard strongly encourages making a DMK backup when the Keyfactor Command database is created.

- In the case where a Keyfactor Command database needs to be restored to a SQL Server with a different SMK, the DMK cannot be restored and a DMK password is not known, a backup of the SMK may be used to restore the server, but this will affect any other databases on the server that make use of SQL encryption.

If no backup of the SMK or DMK exists, all DMK passwords are unknown, and the SQL server holding the SMK is lost, the encrypted data within Keyfactor Command is not recoverable (even with a database backup.)

To backup the DMK, as a user with *control* permission on the SQL server where the Keyfactor Command database is **select your Keyfactor Command database** and run the following SQL command:

```
BACKUP MASTER KEY TO FILE = 'path_to_file'
ENCRYPTION BY PASSWORD = 'SecurePassword#1234'
```

Replace ”path_to_file” with a path and filename for the output file. This can be either a local path on the SQL server or a UNC path. The selected output directory must be writable by the service account under which SQL Server is running. By default, the SQL backup directory has appropriate permissions. Replace ”SecurePassword#1234’ with a secure password to protect the file. Store the backup file and the password in a safe, well-documented location. For more information, see:

https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/back-up-a-database-master-key?view=sql-server-ver15
https://docs.microsoft.com/en-us/sql/t-sql/statements/backup-master-key-transact-sql?view=sql-server-2017

To backup the SMK, as a user with *control server* permission run the following SQL command on the SQL server where the Keyfactor Command database is:

```
BACKUP SERVICE MASTER KEY TO FILE = 'path_to_file'
ENCRYPTION BY PASSWORD = 'SecurePassword#1234'
```

Replace path_to_file with a path and filename for the output file. This can be either a local path on the SQL server or a UNC path. The selected output directory must be writable by the service account under which SQL Server is running. By default, the SQL backup directory has appropriate permissions. Replace SecurePassword#1234 with a secure password to protect the file. Store the backup file and the password in a safe, well-documented location. For more information, see:

https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/back-up-the-service-master-key?view=sql-server-ver15
https://docs.microsoft.com/en-us/sql/t-sql/statements/backup-service-master-key-transact-sql?view=sql-server-2017

To prepare for disaster recovery, you should have the DMK backup created during installation, an SMK backup, the passwords for these files and a recent database backup. You will likely only need either the DMK or the SMK if you need to restore to a SQL server instance other than the original SQL server instance, but it can be useful to have the flexibility to choose between the two at restoration time. If you need to restore to the original SQL server instance, you will only need a recent database backup and not either of the database keys. For information about restoring using the DMK or SMK, see Disaster Recovery on page 703.

2.2.5 Log Monitoring

Logging information from your Keyfactor Command implementation is available in a variety of places:

- Dedicated text files for each application are written to the server.

  The logs for the various components of Keyfactor Command are saved, by default, under the local folder C:\Keyfactor\logs\.... For more information, see Editing NLog on page 709.

- The Windows event log on the Keyfactor Command server.

  For more information, see Keyfactor Command Windows Event IDs on page 727.

- The Audit Log in the Keyfactor Command Management Portal.

  Logs of auditable changes that affect your Keyfactor Command implementation—e.g. creation, change, or deletion of a record in an area of the product such as Certificates or Security—are viewable in the Management Portal, are output to a text file on the Keyfactor Command server, and can optionally be collected to a separate server for analysis with a centralized logging solution. For more information, see Audit Log on page 652.

In addition, transactions coming into the Keyfactor Command Management Portal are written into the IIS logs. For the most part, there is no need to look in the IIS logs unless you encounter a problem you need to troubleshoot. However, it is a good practice to monitor the text logs, the audit log, and the Windows event logs to make sure the system is operating smoothly and no errors are occurring.

By default, 10 main text logs are retained before the oldest ones are automatically deleted. Logs are rotated daily or when they reach a maximum file size, whichever comes first. Depending on the volume of log information you're generating, 10 logs may cover 10 days or a much shorter period. If you're using a centralized logging solution that runs daily to copy these to another location for analysis, the default log configuration of 10 logs with a maximum file size of 50 MB may be a sufficient retention policy. If you intend to analyze them in place on the Keyfactor Command server, you may wish to extend this retention setting.

In both the text-based logs and the Windows event logs, errors will generally appear with a tag of Error. For the text log, an error entry would look something like this, with more information following this line (and perhaps before it) with some further details:

```
2021-08-16 10:00:21.7105 CSS.CMS.CA.Client.CertificateAuthority [Error] - An error
occurred while reading the CA database.
```

Some errors may be transitory. For example, a CA synchronization may fail because a CA was down for maintenance and then succeed on the next try when the server is back up. If you find errors in

your logs and need help tracking down their cause, contact Keyfactor support (support@key-factor.com).

When troubleshooting an error, it may be helpful to turn up the logging level in the Nlog.config file relevant to the component of interest to *debug* or *trace*. However, this can result in a large volume of messages that can be hard to wade through. It is sometimes useful to add further filters to the Nlog.config file relevant to the component of interest to filter out log traffic unrelated to the error you are trying to investigate. Some of the NLog files for the various log components contain pre-defined filters such as:

```
<when condition="ends-with('${logger}', 'WebSecurityContext') and level &lt;
LogLevel.Warn" action="Ignore" />
<when condition="ends-with('${logger}', 'AlertsController') and level &lt;
LogLevel.Warn" action="Ignore" />
<when condition="ends-with('${logger}', 'WebPrincipal') and level &lt; LogLevel.Warn"
action="Ignore" />
<when condition="ends-with('${logger}', 'CertStoreController') and level &lt;
LogLevel.Warn" action="Ignore" />
```

These filter out messages that contain the referenced string (e.g. WebSecurityContext) at the end of the log source string (e.g. CSS.CMS.Web.Security.WebSecurityContext) but only for messages that are at an Info, Debug or Trace level (less than Warn) as in this log line:

```
2021-08-11 04:38:04.0366 CSS.CMS.Web.Core.Security.WebSecurityContext [Trace] - User
'KEYEXAMPLE\ggant' (Cached) has area permission 'Reports_Read' as requested by 'Execute'
```

You can add more lines like this that do things like filter out the periodic report cleanup process, for example:

```
<when condition="ends-with('${logger}', 'ReportCleanupManager') and level &lt;
LogLevel.Warn" action="Ignore" />
```

You can also filter out messages based on all or part of the message. Say you want to look at CA synchronization messages, but want to eliminate some of the chatter related to that. You don't want to filter out all the CA synchronization source messages in that case, but you might choose to get rid of entries like this:

```
2020-05-20 08:41:00.0487 CSS.CMS.CA.Client.CertificateAuthorityConnector [Trace] - Fetch
succeeded
```

You can do that with a filter that looks like this:

```
<when condition="starts-with('${message}', 'Fetch succeeded') and level &lt;
LogLevel.Info" action="Ignore"/>
```

Note: For more information on how to make changes to your NLog configuration see Editing NLog below

Some informational, warning, and error messages generated by Keyfactor Command are coded in a manner to allow them to be redirected for output to the Windows Application event log. If you redirect these messages from being output to the event log to a file instead, they look something like:

```
2021-08-02 04:54:00.2260 CSS.CMS.Service.Jobs.CASync.LocalCASyncJob-EVENT [Info] -
eventID=200&categoryID=2&eventMessage=Beginning+Full+synchronization+of+Certificate+Auth
ority%3a+%27corpca02.keyexample.com
%5cCorpIssuing2.+Last+scan+time%3a+11%2f10%2f2020+10%3a20%3a00+AM%2c+last+row+read%3a+0%
27
```

The -EVENT tag (highlighted in red, above) is what codes these messages for redirection to the event log. There are two configuration lines in the NLog.config files for the various log components that relate to Windows event log redirection—the first formats the data correctly for event log usage and assigns a source to the messages while the second captures all the messages coded -EVENT, prevents them from going to the regular text log, and redirects them to the event log for all messages at info, warning or error level. Debug and trace level messages are not designed to be output to the event log. To reduce the volume of messages to the event log, you can change minlevel-l="Info" to minlevel="Warn" or minlevel="Error". Be aware that if you do this, more verbose messages (e.g. info level messages) will fall through to the text-based log.

```
    <target xsi:type="EventLog" name="eventLog" source="Keyfactor Command"
            eventId="${query-string:item=eventID}" category="${query-string:item=categoryID}" layout="${query-string:item=eventMessage}" />
</targets>
<rules>
  <!-- Internal ASP.NET logging, off by default -->
  <logger name="CSS.CMS.Web.API.SimpleTracer" minlevel="Off" writeTo="logfile" final="true" />
  <!-- Don't write events to the log file (log file should contain different, more verbose, logging) -->
  <logger name="CSS.CMS.Install.ConfigurationWizard.Console.Wizard" minlevel="Info" writeTo="console" />
  <logger name="*-EVENT" minlevel="Info" writeTo="eventLog" final="true" />
```

Figure 412: Nlog Configuration for Windows Event Logging

By default, messages redirected to the event log are marked with a source of *Keyfactor Command* for Keyfactor Command server, *Keyfactor Service* for the Keyfactor Command Service, and *Keyfactor Orchestrators* or *Keyfactor Orchestrator* for the Keyfactor Universal Orchestrator and Keyfactor Windows Orchestrator.

2.2.5.1 Editing NLog

Keyfactor Command provides extensive logging for visibility and troubleshooting. For more information about troubleshooting, see Troubleshooting on page 747.

By default, Keyfactor Command places its log files in the C:\Keyfactor\logs directory, generates logs at the *Info* logging level, and stores the primary logs for two days before deleting them. If you wish to change these defaults you can open the configuration file for each type of log on each Keyfactor Command server where you wish to adjust logging, and edit the file in a text editor (e.g. Notepad)

using the “Run as administrator” option. Each Keyfactor component has its own NLog configuration file and NLog logging output path.

Note: By default, the filename for each component log is unique. This allows you to isolate and research issues on a component-by-component basis by viewing a specific log file. Alternatively, you may wish to change the default output filename to be the same for all logging components so all activity is reported in a single log file. You will note that the default Audit and Alert filenames for each component (for those components that log audits or alerts) are the same so that all activity is logged in the same file across the platform for this reason.

Tip: If you use the default naming convention, and want to review an event that happened in the management portal, for instance, you would look in the Command_API_Log.txt and/or the Command_Portal_Log.txt.

Important: If you do choose to name the log files the same across the platform, it is recommended that you also set the **maxArchiveFiles** values the same in each Nlog config file. If there is a different value for **maxArchiveFiles** for files with the same filename/location, the smallest value will override all others.

To make changes to your NLog configuration:

1. On each Keyfactor Command server where you wish to adjust logging, open a text editor (e.g. Notepad) using the “Run as administrator” option.
2. In the text editor, browse to open the desired Nlog.config file for the appropriate Keyfactor components. The files are located in application subdirectories under the installed directory, which are the following directories by default:

    - **C:\Program Files\Keyfactor\Keyfactor Platform\WebConsole\NLog_Portal.config**

      The Portal file is for logging any activity to do with the Keyfactor CommandManagement Portal, including users connecting to the portal, loading various pages in the portal, and taking actions.

      Note: Many actions taken in the Keyfactor CommandManagement Portal are carried out using the Keyfactor API and Keyfactor is migrating the product to use the Keyfactor API more and more, so this file will have less and less activity going forward. See C:\Program Files\Keyfactor\Keyfactor Platform\KeyfactorAPI\NLog_KeyfactorAPI.config on page 713.

      ### Settings

      The Portal log is for logging any activity to do with the Keyfactor Command web portal. The fields you may wish to edit are:

- `fileName="C:\Keyfactor\logs\Command_Portal_Log.txt"`

  The path and file name of the active Keyfactor Command portal log file.

  > **Important:** If you choose to change the path for storage of the log files, you will need to create the new directory (e.g. D:\KeyfactorLogs) and grant both the service account under which the Keyfactor Command Service is running and the service account under which the IIS application pool for Keyfactor Command is running full control permissions on this directory. These roles may be served by the same service account.

- `archiveFileName="C:\Keyfactor\logs\Command_Portal_Log_Archive_{#}.txt"`

  The path and file name of previous days' Keyfactor Command portal log files. Keyfactor Command rotates log files daily and names the previous files using this naming convention.

- `fileName="C:\Keyfactor\logs\Command_Alert_Log.txt"`

  The path and file name of the active Keyfactor Command portal log file for alerting events. This entry is found on servers with the Keyfactor Command Service installed. Info level messages are written to this log whenever alerts (certificate expiration, pending certificate request, issued certificate, denied certificate request, or revocation monitoring) are run either as scheduled tasks or as tests. The log messages include the type of alert (e.g. expiration alert), the recipient of the alert (if an email was scheduled to be sent), and the alert subject line. You can change the level of logging in the log line that references writeTo="alertlogfile". These logs are generated separately from the general portal events to allow for separate tracking and log shipping of alerting events. By default, the alert log file-name/location for all components is the same to allow for a central source for tracking alert events across the platform.

- `archiveFileName="C:\Keyfactor\logs\Command_Alert_Log_Archive_{#}.txt""`

  The path and file name of previous days' Keyfactor Command portal log files for alert events.

- `fileName="C:\Keyfactor\logs\Command_Audit_Log.txt"`

  The path and file name of the active Keyfactor Command portal log file for auditable events. These logs are generated separately from the general portal events to allow for separate tracking of auditable events. By default, the audit log file-name/location for all components is the same to allow for a central source for tracking auditable events across the platform.

- `archiveFileName="C:\Keyfactor\logs\Command_Audit_Log_Archive_{#}.txt""`

  The path and file name of previous days' Keyfactor Command portal log files for auditable events.

- `name="EmailAlertLogger" minlevel="Info" writeTo="alertlogfile"`

  The level of log detail that should be generated for alert events and written to the alert logs.

- `maxArchiveFiles="10"`

  The number of archive files to retain before deletion. This field is listed multiple times in the NLog_Portal.config file on a server with the Keyfactor Command Service installed—once for the main logging section, once for the alert logging section, and once for the audit logging section. The default number of files to retain is 10 for the main log and the synchronization log but 14 for the alert log and audit log. The alert and audit logs are small by default, and retaining a larger number of them shouldn't create a disk space issue.

- `archiveAboveSize="52428800"`

  The maximum file size of each log file. Once a log file reaches this size (50 MB by default), it will be rotated to archive even if the end of the day has not been reached.

- `name="*" minlevel="Info" writeTo="logfile"`

  The level of log detail that should be generated. This line applies to all the logs in the portal file. The default *Info* level logs error and some informational data but at a minimal level to avoid generating large log files. For troubleshooting, it may be desirable to set the logging level to *Debug* or *Trace*. Available log levels (in order of increasing verbosity) are:

  - OFF – No logging
  - FATAL – Log severe errors that cause early termination
  - ERROR – Log severe errors and other runtime errors or unexpected conditions that may not cause early termination
  - WARN – Log errors and use of deprecated APIs, poor use of APIs, *almost* errors, and other runtime situations that are undesirable or unexpected but not necessarily *wrong*
  - INFO – Log all of the above plus runtime events (startup/shutdown)

- DEBUG – Log all of the above plus detailed information on the flow through the system
- TRACE – Maximum log information—this option can generate VERY large log files

Figure 413: Nlog_Portal.config

- **C:\Program Files\Keyfactor\Keyfactor Platform\KeyfactorAPI\NLog_KeyfactorAPI.config**

  The KeyfactorAPI file is the primary file for logging activity related to making requests with the Keyfactor API. Since many of the functions in the Management Portal use the Keyfactor API, this log also includes activity related to running the Management Portal.

Settings

The KeyfactorAPI file is the primary file for logging activity related to running Keyfactor Command API. The fields you may wish to edit are:

- `fileName="C:\Keyfactor\logs\Command_API_Log.txt"`

  The path and file name of the active Keyfactor Command primary log file.

  Important: If you choose to change the path for storage of the log files, you will need to create the new directory (e.g. D:\KeyfactorLogs) and grant both the service account under which the Keyfactor Command Service is running and the service account under which the IIS application pool for Keyfactor Command is running full control permissions on this directory. These roles may be served by the same service account.

- `archiveFileName="c:\Keyfactor\logs\Command_API_Log_Archive_{#}.txt"`

The path and file name of previous days' Keyfactor Command primary log files. Keyfactor Command rotates log files daily and names the previous files using this naming convention.

- `fileName="C:\Keyfactor\logs\Command_Alert_Log.txt"`

The path and file name of the active Keyfactor Command primary log file for alerting events. This entry is only found on servers with the Keyfactor Command Service installed. Info level messages are written to this log whenever alerts (certificate expiration, pending certificate request, issued certificate, denied certificate request, or revocation monitoring) are run either as scheduled tasks or as tests. The log messages include the type of alert (e.g. expiration alert), the recipient of the alert (if an email was scheduled to be sent), and the alert subject line. You can change the level of logging in the log line that references writeTo="alertlogfile". These logs are generated separately from the primary log events to allow for separate tracking and log shipping of alerting events. By default, the alert log file-name/location for all components is the same to allow for a central source for tracking alert events across the platform.

- `archiveFileName="c:\Keyfactor\logs\Command_Alert_Log_Archive_{#}.txt""`

The path and file name of previous days' Keyfactor Command primary log files for alert events.

- `fileName="C:\Keyfactor\logs\Command_Audit_Log.txt"`

The path and file name of the active Keyfactor Command primary log file for auditable events. These logs are generated separately from the primary log events to allow for separate tracking of auditable events. By default, the audit log file-name/location for all components is the same to allow for a central source for tracking auditable events across the platform.

- `archiveFileName="c:\Keyfactor\logs\Command_Audit_Log_Archive_{#}.txt""`

The path and file name of previous days' Keyfactor Command primary log files for auditable events.

- `name="EmailAlertLogger" minlevel="Info" writeTo="alertlogfile"`

The level of log detail that should be generated for alert events and written to the alert logs.

- `maxArchiveFiles="10"`

The number of archive files to retain before deletion. This field is listed multiple times in the NLog_KeyfactorAPI.config file —once for the main logging section, once for the alert logging section, and once for the audit logging section. The default number of files to retain is 10 for the main log and the synchronization log but 14 for the alert log and audit log. The alert and audit logs are small by default, and retaining a larger number of them shouldn't create a disk space issue.

- `archiveAboveSize="52428800"`

  The maximum file size of each log file. Once a log file reaches this size (50 MB by default), it will be rotated to archive even if the end of the day has not been reached.

- `name="*" minlevel="Info" writeTo="logfile"`

  The level of log detail that should be generated. This line applies to all the logs of the KeyfactorAPI file. The default *Info* level logs error and some informational data but at a minimal level to avoid generating large log files. For troubleshooting, it may be desirable to set the logging level to *Debug* or *Trace*. Available log levels (in order of increasing verbosity) are:

  - OFF – No logging
  - FATAL – Log severe errors that cause early termination
  - ERROR – Log severe errors and other runtime errors or unexpected conditions that may not cause early termination
  - WARN – Log errors and use of deprecated APIs, poor use of APIs, *almost* errors, and other runtime situations that are undesirable or unexpected but not necessarily *wrong*
  - INFO – Log all of the above plus runtime events (startup/shutdown)
  - DEBUG – Log all of the above plus detailed information on the flow through the system
  - TRACE – Maximum log information—this option can generate VERY large log files

Figure 414: Nlog_KeyfactorAPI.config

- **C:\Program Files\Keyfactor\Keyfactor Platform\Service\NLog_TimerService.config**

  The Timer Service file logs activity related to scheduled and automated events within Keyfactor Command such as CA synchronization, scheduled alerts, and scheduled reports.

  ## Settings

  The Timer Service file logs activity related to scheduled and automated events within Keyfactor Command and includes the CA sync logs. The fields you may wish to edit are:

  - `fileName="C:\Keyfactor\logs\Command_Service_Log.txt"`

    The path and file name of the active Keyfactor Command timer service log file.

    > **Important:** If you choose to change the path for storage of the log files, you will need to create the new directory (e.g. D:\KeyfactorLogs) and grant both the service account under which the Keyfactor Command Service is running and the service account under which the IIS application pool for Keyfactor Command is running full control permissions on this directory. These roles may be served by the same service account.

  - `archiveFileName="C:\Keyfactor\logs\Command_Service_Log_Archive_{#}.txt"`

    The path and file name of previous days' Keyfactor Command timer service log files. Keyfactor Command rotates log files daily and names the previous files using this naming convention.

  - `fileName="C:\Keyfactor\logs\Command_Alert_Log.txt"`

    The path and file name of the active Keyfactor Command timer service log file for alerting events. This entry is only found on servers with the Keyfactor Command

Service installed. Info level messages are written to this log whenever alerts (certificate expiration, pending certificate request, issued certificate, denied certificate request, or revocation monitoring) are run either as scheduled tasks or as tests. The log messages include the type of alert (e.g. expiration alert), the recipient of the alert (if an email was scheduled to be sent), and the alert subject line. You can change the level of logging in the log line that references writeTo=”alertlogfile”. These logs are generated separately from the general timer service events to allow for separate tracking and log shipping of alerting events. By default, the alert log filename/location for all components is the same to allow for a central source for tracking alert events across the platform.

- `archiveFileName="C:\Keyfactor\logs\Command_Alert_Log_Archive_{#}.txt""`

The path and file name of previous days’ Keyfactor Command timer service log files for alert events.

- `fileName="C:\Keyfactor\logs\Command_Audit_Log.txt"`

The path and file name of the active Keyfactor Command timer service log file for auditable events. These logs are generated separately from the general timer service events to allow for separate tracking of auditable events. By default, the audit log filename/location for all components is the same to allow for a central source for tracking auditable events across the platform.

- `archiveFileName="C:\Keyfactor\logs\Command_Audit_Log_Archive_{#}.txt""`

The path and file name of previous days’ Keyfactor Command timer service log files for auditable events.

- `name="EmailAlertLogger" minlevel="Info" writeTo="alertlogfile"`

The level of log detail that should be generated for alert events and written to the alert logs.

- `maxArchiveFiles="10"`

The number of archive files to retain before deletion. This field is listed multiple times in the NLog_TimerService.config file on a server with the Keyfactor Command Service installed—once for the main logging section, once for the alert logging section, and once for the audit logging section. The default number of files to retain is 10 for the main log and the synchronization log but 14 for the alert log and audit log. The alert and audit logs are small by default, and retaining a larger number of them shouldn’t create a disk space issue.

- `archiveAboveSize="52428800"`

The maximum file size of each log file. Once a log file reaches this size (50 MB by default), it will be rotated to archive even if the end of the day has not been reached.

- `name="*" minlevel="Info" writeTo="logfile"`

  The level of log detail that should be generated. This line applies to all the logs of the timer service file. The default *Info* level logs error and some informational data but at a minimal level to avoid generating large log files. For troubleshooting, it may be desirable to set the logging level to *Debug* or *Trace*. Available log levels (in order of increasing verbosity) are:

  - OFF – No logging
  - FATAL – Log severe errors that cause early termination
  - ERROR – Log severe errors and other runtime errors or unexpected conditions that may not cause early termination
  - WARN – Log errors and use of deprecated APIs, poor use of APIs, *almost* errors, and other runtime situations that are undesirable or unexpected but not necessarily *wrong*
  - INFO – Log all of the above plus runtime events (startup/shutdown)
  - DEBUG – Log all of the above plus detailed information on the flow through the system
  - TRACE – Maximum log information—this option can generate VERY large log files

```
<targets>
  <target xsi:type="File" name="logfile" fileName="C:\Keyfactor\logs\Command_Service_Log.txt" layout="${longdate} ${logger} [${level}] - ${message}"
          archiveFileName="c:\Keyfactor\logs\Command_Service_Log_Archive_{#}.txt" archiveEvery="Day" archiveNumbering="Rolling" maxArchiveFiles="10" archiveAboveSize="52428800"/>
  <target xsi:type="File" name="alertlogfile" fileName="C:\Keyfactor\logs\Command_Alert_Log.txt" layout="${longdate} ${logger} [${level}] - ${message}"
          archiveFileName="c:\Keyfactor\logs\Command_Alert_Log_Archive_{#}.txt" archiveEvery="Day" archiveNumbering="Date" archiveDateFormat="yyyyMMdd" maxArchiveFiles="14"/>
  <target xsi:type="File" name="auditlogfile" fileName="C:\Keyfactor\logs\Command_Audit_Log.txt" layout="${longdate} ${logger} [${level}] - ${message}"
          archiveFileName="c:\Keyfactor\logs\Command_Audit_Log_Archive_{#}.txt" archiveEvery="Day" archiveNumbering="Date" archiveDateFormat="yyyyMMdd" maxArchiveFiles="14"/>
  <target xsi:type="OutputDebugString" name="String" layout="${longdate} ${logger}::${message}"/>
  <target xsi:type="Debugger" name="debugger" layout="${longdate} ${logger}::${message}"/>
  <target xsi:type="Console" name="console" layout="${logger} ${message}"/>
  <target xsi:type="EventLog" name="eventLog" source="Keyfactor Command"
          eventId="${event-properties:item=eventID}" category="${event-properties:item=categoryID}" layout="${event-properties:item=message}" />
</targets>
<rules>
  <logger name="*-EVENT" minlevel="Info" writeTo="eventLog" final="true" />
  <logger name="*-AUDIT" minlevel="Info" writeTo="auditlogfile" final="true" />
  <logger name="*Quartz*" minlevel="Warn" writeTo="logfile" />
  <logger name="EmailAlertLogger" minlevel="Info" writeTo="alertlogfile" final="true"/>
  <logger name="*" minlevel="Info" writeTo="logfile" />
</rules>
</nlog>
```

Figure 415: Nlog_TimerService.config

- **C:\Program Files\Keyfactor\Keyfactor Platform\WebAgentServices\NLog_Orchestrators.config**

  The Orchestrators, or OrchestratorsAPI, file logs activity related to Keyfactor Orchestrators API. Look here for messages related to orchestrators communicating with Keyfactor Command.

Settings

The Orchestrators, or OrchestratorsAPI, file logs activity related to orchestrators API. The fields you may wish to edit are:

- `fileName="C:\Keyfactor\logs\Command_OrchestratorsAPI_Log.txt"`

  The path and file name of the active Keyfactor Command orchestrators log file.

  > **Important:** If you choose to change the path for storage of the log files, you will need to create the new directory (e.g. D:\KeyfactorLogs) and grant both the service account under which the Keyfactor Command Service is running and the service account under which the IIS application pool for Keyfactor Command is running full control permissions on this directory. These roles may be served by the same service account.

- `archiveFileName="C:\Keyfactor\logs\Command_OrchestratorsAPI_Log_Archive_{#}.txt"`

  The path and file name of previous days' Keyfactor Command orchestrators log files. Keyfactor Command rotates log files daily and names the previous files using this naming convention.

- `fileName="C:\Keyfactor\logs\Command_Alert_Log.txt"`

  The path and file name of the active Keyfactor Command orchestrators log file for alerting events. This entry is found on servers with the Keyfactor Command Service installed. Info level messages are written to this log whenever alerts (certificate expiration, pending certificate request, issued certificate, denied certificate request, or revocation monitoring) are run either as scheduled tasks or as tests. The log messages include the type of alert (e.g. expiration alert), the recipient of the alert (if an email was scheduled to be sent), and the alert subject line. You can change the level of logging in the log line that references writeTo="alertlogfile". These logs are generated separately from the general orchestrator events to allow for separate tracking and log shipping of alerting events. By default, the alert log filename/location for all components is the same to allow for a central source for tracking alert events across the platform.

- `archiveFileName="C:\Keyfactor\logs\Command_Alert_Log_Archive_{#}.txt""`

  The path and file name of previous days' Keyfactor Command orchestrators log files for alert events.

- `fileName="C:\Keyfactor\logs\Command_Audit_Log.txt"`

  The path and file name of the active Keyfactor Command orchestrators log file for auditable events. These logs are generated separately from the general orchestrator events to allow for separate tracking of auditable events. By default, the

audit log filename/location for all components is the same to allow for a central source for tracking auditable events across the platform.

- `archiveFileName="C:\Keyfactor\logs\Command_Audit_Log_Archive_{#}.txt""`

  The path and file name of previous days' Keyfactor Command orchestrators log files for auditable events.

- `name="EmailAlertLogger" minlevel="Info" writeTo="alertlogfile"`

  The level of log detail that should be generated for alert events and written to the alert logs.

- `maxArchiveFiles="10"`

  The number of archive files to retain before deletion. This field is listed multiple times in the NLog_Orchestrators.config file on a server with the Keyfactor Command Service installed—once for the main logging section, once for the alert logging section, and once for the audit logging section. The default number of files to retain is 10 for the main log and the synchronization log but 14 for the alert log and audit log. The alert and audit logs are small by default, and retaining a larger number of them shouldn't create a disk space issue.

- `archiveAboveSize="52428800"`

  The maximum file size of each log file. Once a log file reaches this size (50 MB by default), it will be rotated to archive even if the end of the day has not been reached.

  Note: The default value for the *archiveAboveSize* setting was significantly larger in versions of Keyfactor Command prior to 7.5. In addition, the default *maxArchiveFiles* value was 2 for the main and CA synchronization logging sections. In environments where the logging level is consistently set at debug level or greater, this change may result in the generation of several log files per day.

- `name="*" minlevel="Info" writeTo="logfile"`

  The level of log detail that should be generated. This line applies to all the logs of the orchestrators file. The default *Info* level logs error and some informational data but at a minimal level to avoid generating large log files. For troubleshooting, it may be desirable to set the logging level to *Debug* or *Trace*. Available log levels (in order of increasing verbosity) are:

- OFF – No logging
- FATAL – Log severe errors that cause early termination
- ERROR – Log severe errors and other runtime errors or unexpected conditions that may not cause early termination
- WARN – Log errors and use of deprecated APIs, poor use of APIs, *almost* errors, and other runtime situations that are undesirable or unexpected but not necessarily *wrong*
- INFO – Log all of the above plus runtime events (startup/shutdown)
- DEBUG – Log all of the above plus detailed information on the flow through the system
- TRACE – Maximum log information—this option can generate VERY large log files

Figure 416: Nlog_Orchestrators.config

- **C:\Program Files\Keyfactor\Keyfactor Platform\Configuration\NLog_Configuration.config**

  The Configuration file logs activity related to running the Keyfactor Command configuration wizard only. It may be useful to increase the logging level on this one if you are experiencing installation or upgrade issues.

Settings

The Configuration file logs activity related to running the Keyfactor Command configuration wizard only. The fields you may wish to edit are:

- `fileName="C:\Keyfactor\logs\Command_Configuration_Log.txt"`

  The path and file name of the active Keyfactor Command configuration wizard log file.

> **Important:** If you choose to change the path for storage of the log files, you will need to create the new directory (e.g. D:\KeyfactorLogs) and grant both the service account under which the Keyfactor Command Service is running and the service account under which the IIS application pool for Keyfactor

> ⚠ Command is running full control permissions on this directory. These roles may be served by the same service account.

- ```
  archiveFileName="C:\Keyfactor\logs\Command_Configuration_Log_Archive_{#}.txt"
  ```

  The path and file name of previous days' Keyfactor Command configuration wizard log files. Keyfactor Command rotates log files daily and names the previous files using this naming convention.

- ```
  fileName="C:\Keyfactor\logs\Command_Audit_Log.txt"
  ```

  The path and file name of the active Keyfactor Command log file for auditable configuration wizard events. These logs are generated separately from the configuration log events to allow for separate tracking of auditable events. By default, the audit log filename/location for all components is the same to allow for a central source for tracking auditable events across the platform.

- ```
  archiveFileName="C:\Keyfactor\logs\Command_Audit_Log_Archive_{#}.txt""
  ```

  The path and file name of previous days' Keyfactor Command log files for auditable configuration wizard events.

- ```
  maxArchiveFiles="10"
  ```

  The number of archive files to retain before deletion. This field is listed multiple times in the NLog_Configuration.config file on a server —once for the main logging section and once for the audit logging section. The default number of files to retain is 10 for the main log and 14 for the audit log. The audit logs are small by default, and retaining a larger number of them shouldn't create a disk space issue.

- ```
  archiveAboveSize="52428800"
  ```

  The maximum file size of each log file. Once a log file reaches this size (50 MB by default), it will be rotated to archive even if the end of the day has not been reached.

- ```
  name="*" minlevel="Info" writeTo="logfile"
  ```

  The level of log detail that should be generated. This line applies to all the logs in the configuration file. The default *Info* level logs error and some informational data but at a minimal level to avoid generating large log files. For troubleshooting, it may be desirable to set the logging level to *Debug* or *Trace*. Available log levels (in order of increasing verbosity) are:

- OFF – No logging
- FATAL – Log severe errors that cause early termination
- ERROR – Log severe errors and other runtime errors or unexpected conditions that may not cause early termination
- WARN – Log errors and use of deprecated APIs, poor use of APIs, *almost* errors, and other runtime situations that are undesirable or unexpected but not necessarily *wrong*
- INFO – Log all of the above plus runtime events (startup/shutdown)
- DEBUG – Log all of the above plus detailed information on the flow through the system
- TRACE – Maximum log information—this option can generate VERY large log files

Figure 417: Nlog_Configuration.config

- **C:\Program Files\Keyfactor\Keyfactor Platform\WebAPI\NLog_ClassicAPI.config**

  The ClassicAPI file logs activity involving the ClassicAPI from Keyfactor Command. You will only need to modify the logging settings on this one if you have upgraded from a previous version of Keyfactor Command and have implemented a custom application built with the Classic API.

Settings

The ClasssicAPI file logs activity related to invoking the ClassicAPI from Keyfactor Command. The fields you may wish to edit are:

- `fileName="C:\Keyfactor\logs\Command_ClassicAPI_Log.txt"`

  The path and file name of the active Keyfactor Command classic API log file.

  Important: If you choose to change the path for storage of the log files, you will need to create the new directory (e.g. D:\KeyfactorLogs) and grant both the service account under which the Keyfactor Command Service is running and the service account under which the IIS application pool for Keyfactor Command is running full control permissions on this directory. These roles may be served by the same service account.

- ```
  archiveFileName="C:\Keyfactor\logs\Command_ClassicAPI_Log_Archive_
  {#}.txt"
  ```

  The path and file name of previous days' Keyfactor Command classic API log files. Keyfactor Command rotates log files daily and names the previous files using this naming convention.

- ```
  fileName="C:\Keyfactor\logs\Command_Alert_Log.txt"
  ```

  The path and file name of the active Keyfactor Command classic API log file for alerting events. This entry is found on servers with the Keyfactor Command Service installed. Info level messages are written to this log whenever alerts (certificate expiration, pending certificate request, issued certificate, denied certificate request, or revocation monitoring) are run either as scheduled tasks or as tests. The log messages include the type of alert (e.g. expiration alert), the recipient of the alert (if an email was scheduled to be sent), and the alert subject line. You can change the level of logging in the log line that references writeTo="alertlogfile". These logs are generated separately to allow for separate tracking and log shipping of alerting events. By default, the alert log filename/location for all components is the same to allow for a central source for tracking alert events.

- ```
  archiveFileName="C:\Keyfactor\logs\Command_Alert_Log_Archive_{#}.txt"
  ```

  The path and file name of previous days' Keyfactor Command classic API log files for alert events.

- ```
  fileName="C:\Keyfactor\logs\Command_Audit_Log.txt"
  ```

  The path and file name of the active Keyfactor Command classic API log file for auditable events. These logs are generated separately from the general classic API events to allow for separate tracking auditable events. By default, the audit log file-name/location for all components is the same to allow for a central source for tracking auditable events across the platform.

- ```
  archiveFileName="C:\Keyfactor\logs\Command_Audit_Log_Archive_{#}.txt"
  ```

  The path and file name of previous days' Keyfactor Command classic API log files for auditable events.

- ```
  name="EmailAlertLogger" minlevel="Info" writeTo="alertlogfile"
  ```

  The level of log detail that should be generated for alert events and written to the alert logs.

- maxArchiveFiles="10"

The number of archive files to retain before deletion. This field is listed multiple times in the Nlog_ClassicAPI.config file —once for the main logging section, once for the alert logging section, and once for the audit logging section. The default number of files to retain is 10 for the main log and the synchronization log but 14 for the alert log and audit log. The alert and audit logs are small by default, and retaining a larger number of them shouldn't create a disk space issue.

- ```
  archiveAboveSize="52428800"
  ```

  The maximum file size of each log file. Once a log file reaches this size (50 MB by default), it will be rotated to archive even if the end of the day has not been reached.

- ```
  name="*" minlevel="Info" writeTo="logfile"
  ```

  The level of log detail that should be generated. This line applies to all the logs of the classicAPI file. The default *Info* level logs error and some informational data but at a minimal level to avoid generating large log files. For troubleshooting, it may be desirable to set the logging level to *Debug* or *Trace*. Available log levels (in order of increasing verbosity) are:

  - OFF – No logging
  - FATAL – Log severe errors that cause early termination
  - ERROR – Log severe errors and other runtime errors or unexpected conditions that may not cause early termination
  - WARN – Log errors and use of deprecated APIs, poor use of APIs, *almost* errors, and other runtime situations that are undesirable or unexpected but not necessarily *wrong*
  - INFO – Log all of the above plus runtime events (startup/shutdown)
  - DEBUG – Log all of the above plus detailed information on the flow through the system
  - TRACE – Maximum log information—this option can generate VERY large log files

```
<targets>
  <target xsi:type="File" name="logfile" fileName="C:\Keyfactor\logs\Command_ClassicAPI_Log.txt" layout="${longdate} ${logger} [${level}] - ${message}"
          archiveFileName="c:\Keyfactor\logs\Command_ClassicAPI_Log_Archive_{#}.txt" archiveEvery="Day" archiveNumbering="Rolling" maxArchiveFiles="10" archiveAboveSize="52428800"/>

  <target xsi:type="File" name="alertlogfile" fileName="C:\Keyfactor\logs\Command_Alert_Log.txt" layout="${longdate} ${logger} [${level}] - ${message}"
          archiveFileName="c:\Keyfactor\logs\Command_Alert_Log_Archive_{#}.txt" archiveEvery="Day" archiveNumbering="Date" archiveDateFormat="yyyyMMdd" maxArchiveFiles="14"/>

  <target xsi:type="File" name="auditlogfile" fileName="C:\Keyfactor\logs\Command_Audit_Log.txt" layout="${longdate} ${logger} [${level}] - ${message}"
          archiveFileName="c:\Keyfactor\logs\Command_Audit_Log_Archive_{#}.txt" archiveEvery="Day" archiveNumbering="Date" archiveDateFormat="yyyyMMdd" maxArchiveFiles="14"/>
  <target xsi:type="OutputDebugString" name="String" layout="${longdate} ${logger}::${message}"/>

  <target xsi:type="Debugger" name="debugger" layout="${longdate} ${logger}::${message}"/>
  <target xsi:type="Console" name="console" layout="${logger} ${message}"/>
  <target xsi:type="EventLog" name="eventLog" source="Keyfactor Command"
          eventId="${event-properties:item=eventID}" category="${event-properties:item=categoryID}" layout="${event-properties:item=message}" />
</targets>
<rules>
  <!-- Internal ASP.NET logging, off by default -->
  <logger name="CSS.CMS.Web.API.SimpleTracer" minlevel="Off" writeTo="logfile" final="true" />
  <logger name="*-EVENT" minlevel="Info" writeTo="eventLog" final="true" />
  <logger name="*-AUDIT" minlevel="Info" writeTo="auditlogfile" final="true" />
  <logger name="EmailAlertLogger" minlevel="Info" writeTo="alertlogfile" final="true"/>
  <logger name="*" minlevel="Info" writeTo="logfile">
    <filters>
      <when condition="ends-with('${logger}', 'WebSecurityContext') and level &lt; LogLevel.Warn" action="Ignore" />
    </filters>
  </logger>
</rules>
</nlog>
```

Figure 418: Nlog_ClassicAPI.config

Once configured, the log file location defined will look similar to this:

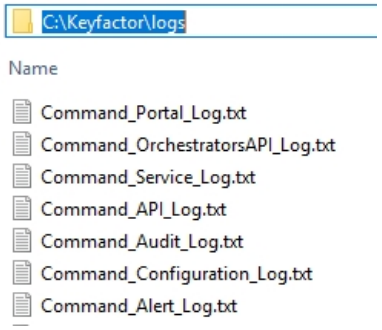


Figure 419: C:\Keyfactor\logs logs

3. Change the respective files and save your changes.

2.2.5.2 Audit Log Output to a Centralized Logging Solution

Keyfactor Command audit logging supports collecting audit entries in real time, as they are generated, to a separate server for analysis by a centralized logging solution. A variety of solutions can be supported. Typically the logs are either delivered to an rsyslog daemon on a Linux server, where they are consolidated with other logs and delivered on to a centralized solution, or delivered straight into the receiving pipeline of a centralized solution using a tool such as Splunk or Logstash. Delivery of the logs over a TLS connection is supported for backend solutions that support this option. Configuration of a centralized logging solution for delivery of the audit logs to a backend solution is beyond the scope of this guide. However, a sample rsyslog.conf file showing typical TLS configuration can be found in *Prepare for External Log Shipping over TLS (Optional)* in the *Keyfactor Command Server Installation Guide*.

The log output settings can be initially configured during installation and can be updated on the auditing tab of the applications settings page. The application settings that relate to log output are:

- Host Name
  Set this to the fully qualified domain name of the server that will be receiving the logs.

- Port
  Set this to the TCP port on which your log receipt application is listening to receive the logs. The default value is 514 (the default rsyslog port).
- Use SysLog Server
  This option defaults to **False**. Set it to **True** to enable delivery of logs to an outside server.
- Use TLS Connection
  This option defaults to **False**. Set it to **True** to enable delivery of logs to an outside server over TLS.

When you click **Save**, Keyfactor Command will verify that a connection can be made to the specified server on the specified port.

2.2.5.3 Keyfactor Command Windows Event IDs

Both Keyfactor Command and Keyfactor Orchestrators generate Windows event log messages for both normal activity and errors in the Windows application event log. Table 59: Keyfactor Command Windows Event IDs shows some of the more common event IDs generated by the Keyfactor Command server (source Certificate Management System or CMS Timer Job Servce). Table 61: Keyfactor Windows Orchestrator and Keyfactor Universal Orchestrator Windows Event IDs shows some of the more common event IDs generated by the Keyfactor Orchestrator (source Certificate Management System Agent). Depending on the features in use on your server, you may not see all these events in your log. These codes can be useful to set up log analysis platforms such as Splunk and Kibana.

Table 59: Keyfactor Command Windows Event IDs

Event ID	Task Category	Description
200	CA Synchron-ization	Incremental CA synchronization started
201	CA Synchron-ization	Incremental CA synchronization finished
210	CA Synchron-ization	An error occurred during CA synchronization
220	CA Synchron-ization	Unable to connect to the CA during incremental CA synchronization
221	CA Synchron-ization	Unable to validate Keyfactor Command product license
222	CA Synchron-ization	Unable to read the Keyfactor Command database during incremental CA synchronization
230	CA Synchron-ization	Unable to connect to the CA during full CA synchronization

Event ID	Task Category	Description
300	Monitoring	Monitoring service started
301	Monitoring	Monitoring engine started
304	Monitoring	Monitoring service timer elapsed
305	Monitoring	Monitoring service execution skipped
306	Monitoring	Monitoring job completed successfully
307	Monitoring	Monitoring engine failed
310	Monitoring	Monitoring job completed with errors
322	Monitoring	Unable to read the Keyfactor Command database during monitor job run
323	Monitoring	An error occurred refreshing a key rotation, cert expiration, CA Health, cert issued, pending cert, or query item alert service job
330	Monitoring	OCSP endpoint is unavailable
331	Monitoring	OCSP endpoint is responding successfully
340	Monitoring	An error occurred configuring an expiration alert
350	Monitoring	An error occurred configuring a pending alert
360	Monitoring	An error occurred configuring an SSL alert
370	Monitoring	An error occurred configuring the CRL
371	Monitoring	CRL endpoint location could not be contacted
372	Monitoring	CRL at the endpoint is stale (past the CA's next publish date for the CRL but not yet at the expiration date) **Note:** If a CRL is both in the warning period and stale, only the event log message for stale will appear in the log.
373	Monitoring	CRL at the endpoint is in the warning period configured for email alerts (X days before expiration)
374	Monitoring	CRL is in a good state
375	Monitoring	CRL at the endpoint has expired

Event ID	Task Category	Description
380	Monitoring	An error occurred configuring a SSRS reporting job, CRL alert jobs, or certificate authority threshold jobs
390	Monitoring	Failed to configure the certificate authority threshold jobs
391	Monitoring	CA has failed to meet one of the threshold monitoring requirements
410	Web API	A general error occurred during a Keyfactor API request
411	Web API	Invalid token error occurred during a Keyfactor API request
413	Web API	Invalid template error occurred during a Keyfactor API request
419	Web API	Invalid user error occurred during a Keyfactor API request
800	Timer Service	Keyfactor Command Service started
801	Timer Service	Keyfactor Command Service stopped
810	Maintenance	A general Keyfactor Command Service maintenance error occurred.
822	Timer Service	Unable to read the Keyfactor Command database during Keyfactor Command Service job
830	Timer Service	Keyfactor Command Service jobs failed to start (alerts, monitoring, sync, other)
930	Timer Service	An orchestrator job configuration failed
931	Timer Service	An orchestrator job execution failed
1001	Maintenance	Keyfactor Command product license is approaching expiration
1002	Maintenance	Audit logs failed to write to the audit log destination
1900	Configuration Wizard	The configuration wizard was started
1910	Configuration Wizard	The configuration wizard finished
1911	Configuration Wizard	The configuration wizard database creation process started
1912	Configuration Wizard	The configuration wizard database upgrade process started

Event ID	Task Category	Description
1913	Configuration Wizard	The configuration wizard database conversion process started
1914	Configuration Wizard	The configuration wizard database upgrade process completed successfully
1915	Configuration Wizard	The configuration wizard database creation process completed successfully
1916	Configuration Wizard	The configuration wizard database conversion process completed successfully
1920	Configuration Wizard	A general failure occurred for the configuration wizard
1921	Configuration Wizard	The configuration wizard database upgrade process failed
1922	Configuration Wizard	The configuration wizard database creation process failed
1940	Configuration Wizard	Configuration wizard general warning
1941	Configuration Wizard	Configuration wizard SSRS reporting config warning
1942	Configuration Wizard	Configuration wizard agent pool config warning
2000	Alert	Whitelist policy failure
2300	Expiration Renewal	Renewal handler was able to successfully renew a certificate
2310	Expiration Renewal	Renewal handler failed to renew a certificate
2800	User Authentic-ation	User login to Management Portal was authenticated
3000	Alert	Execution of an alert (pending, issued, expiration, or key rotation) configured in the Management Portal failed.
3001	Alert	Execution of an alert (pending, issued, expiration, or key rotation) configured in the Management Portal succeeded.
3002	Alert	Execution of an alert (pending, issued, expiration, or key rotation)

Event ID	Task Category	Description
		configured in the Management Portal was canceled.
3003	Alert	Execution of an alert (pending, issued, expiration, or key rotation) configured in the Management Portal started.
3004	Alert	A CA threshold monitoring alert failed.
3005	Alert	A CA threshold monitoring alert succeeded.
3006	Alert	A CA threshold monitoring alert was canceled.
3007	Alert	A CA threshold monitoring alert started.
3008	Alert	A CRL alert for a revocation monitoring location configured in the Management Portal failed.
3009	Alert	A CRL alert for a revocation monitoring location configured in the Management Portal succeeded.
3010	Alert	A CRL alert for a revocation monitoring location configured in the Management Portal was canceled.
3011	Alert	A CRL alert for a revocation monitoring location configured in the Management Portal started.
3012	Certificate Authority	Local CA sync failed.
3013	Certificate Authority	Local CA sync succeeded.
3014	Certificate Authority	Local CA sync was canceled.
3015	Certificate Authority	Local CA sync started.
3016	Other	Delivery of regularly scheduled reports has failed.
3017	Other	Delivery of regularly scheduled reports has succeeded.
3018	Other	Delivery of regularly scheduled reports has been canceled.
3019	Other	Delivery of regularly scheduled reports has started.
3020	Maintenance	The process to generate and assign metadata to certificates when they are imported into Keyfactor Command has started.

Event ID	Task Category	Description
3021	Maintenance	The process to generate and assign metadata to certificates when they are imported into Keyfactor Command has failed.
3022	Maintenance	The process to generate and assign metadata to certificates when they are imported into Keyfactor Command has been canceled.
3023	Maintenance	The periodic process to generate and assign metadata to certificates when they are imported into Keyfactor Command has succeeded.
3024	Maintenance	The periodic process to remove any stored private keys in the Keyfactor Command database that have expired and are eligible for deletion has started.
3025	Maintenance	The periodic process to remove any stored private keys in the Keyfactor Command database that have expired and are eligible for deletion has failed.
3026	Maintenance	The periodic process to remove any stored private keys in the Keyfactor Command database that have expired and are eligible for deletion has been canceled.
3027	Maintenance	The periodic process to remove any stored private keys in the Keyfactor Command database that have expired and are eligible for deletion has succeeded.
3028	Maintenance	The periodic process to add audit log entries for large jobs started.
3029	Maintenance	The periodic process to add audit log entries for large jobs failed.
3030	Maintenance	The periodic process to add audit log entries for large jobs was canceled.
3031	Maintenance	The periodic process to add audit log entries for large jobs succeeded.
3032	Maintenance	The periodic process to remove any audit log history in the Keyfactor Command database that has expired and is eligible for deletion started.
3033	Maintenance	The periodic process to remove any audit log history in the Keyfactor Command database that has expired and is eligible for deletion failed.
3034	Maintenance	The periodic process to remove any audit log history in the Keyfactor Command database that has expired and is eligible for deletion was

Event ID	Task Category	Description
		canceled.
3035	Maintenance	The periodic process to remove any audit log history in the Keyfactor Command database that has expired and is eligible for deletion succeeded.
3036	Maintenance	The periodic process to remove any SSL endpoint history in the Keyfactor Command database that is eligible for deletion started.
3037	Maintenance	The periodic process to remove any SSL endpoint history in the Keyfactor Command database that is eligible for deletion failed.
3038	Maintenance	The periodic process to remove any SSL endpoint history in the Keyfactor Command database that is eligible for deletion was canceled.
3039	Maintenance	The periodic process to remove any SSL endpoint history in the Keyfactor Command database that is eligible for deletion succeeded.
3040	Alert	The periodic process to update the temporary tables that store information on which certificates are in which certificate collections started.
3041	Alert	The periodic process to update the temporary tables that store information on which certificates are in which certificate collections failed.
3042	Alert	The periodic process to update the temporary tables that store information on which certificates are in which certificate collections was canceled.
3043	Alert	The periodic process to update the temporary tables that store information on which certificates are in which certificate collections succeeded.
3044	Maintenance	The periodic process to remove records from temporary files generated while running reports started.
3045	Maintenance	The periodic process to remove records from temporary files generated while running reports failed.
3046	Maintenance	The periodic process to remove records from temporary files generated while running reports was canceled.
3047	Maintenance	The periodic process to remove records from temporary files gener-

Event ID	Task Category	Description
		ated while running reports succeeded.
3048	Other	The periodic process to attempt to continue all suspended workflows that may be eligible to continue but have not done so due to locking conflicts started.
3049	Other	The periodic process to attempt to continue all suspended workflows that may be eligible to continue but have not done so due to locking conflicts failed.
3050	Other	The periodic process to attempt to continue all suspended workflows that may be eligible to continue but have not done so due to locking conflicts was canceled.
3051	Other	The periodic process to attempt to continue all suspended workflows that may be eligible to continue but have not done so due to locking conflicts succeeded.
3052	Maintenance	The periodic process to identify and schedule SSL discovery and monitoring jobs started.
3053	Maintenance	The periodic process to identify and schedule SSL discovery and monitoring jobs failed.
3054	Maintenance	The periodic process to identify and schedule SSL discovery and monitoring jobs was canceled.
3055	Maintenance	The periodic process to identify and schedule SSL discovery and monitoring jobs succeeded.
3056	Maintenance	The periodic process to synchronize certificate templates from a source (e.g. Active Directory) to pick up new templates started.
3057	Maintenance	The periodic process to synchronize certificate templates from a source (e.g. Active Directory) to pick up new templates failed.
3058	Maintenance	The periodic process to synchronize certificate templates from a source (e.g. Active Directory) to pick up new templates was canceled.
3059	Maintenance	The periodic process to synchronize certificate templates from a source (e.g. Active Directory) to pick up new templates succeeded.
3060	Maintenance	The periodic process to run the Microsoft SQL update statistics function in the Keyfactor Command database started.

Event ID	Task Category	Description
3061	Maintenance	The periodic process to run the Microsoft SQL update statistics function in the Keyfactor Command database failed.
3062	Maintenance	The periodic process to run the Microsoft SQL update statistics function in the Keyfactor Command database was canceled.
3063	Maintenance	The periodic process to run the Microsoft SQL update statistics function in the Keyfactor Command database succeeded.
3064	Maintenance	The periodic process to remove any completed workflow instances (both successful and failed) in the Keyfactor Command database that have aged past the date as defined in that application started.
3065	Maintenance	The periodic process to remove any completed workflow instances (both successful and failed) in the Keyfactor Command database that have aged past the date as defined in that application failed.
3066	Maintenance	The periodic process to remove any completed workflow instances (both successful and failed) in the Keyfactor Command database that have aged past the date as defined in that application canceled.
3067	Maintenance	The periodic process to remove any completed workflow instances (both successful and failed) in the Keyfactor Command database that have aged past the date as defined in that application succeeded.
9999		Unknown error

Table 60: Keyfactor Command Windows Event IDs for Audit Log

Event ID	Task Category	Description
2001	Audit Log	Auditable event in the Certificate area of the product
2002	Audit Log	Auditable event in the API Application area of the product
2003	Audit Log	Auditable event in the Template area of the product
2004	Audit Log	Auditable event in the Certificate Collection area of the product
2005	Audit Log	Auditable event in the Expiration Alert area of the product
2006	Audit Log	Auditable event in the Pending Alert area of the product
2007	Audit Log	Auditable event in the Application Setting area of the product

Event ID	Task Category	Description
2008	Audit Log	Auditable event in the Issued Alert area of the product
2009	Audit Log	Auditable event in the Denied Alert area of the product
2010	Audit Log	Auditable event in the Security Identity area of the product
2011	Audit Log	Auditable event in the Security Role area of the product
2012	Audit Log	Auditable event related to an Authorization Failure
2013	Audit Log	Auditable event related to CSR enrollment
2014	Audit Log	Auditable event related to SSH Server Groups
2015	Audit Log	Auditable event related to SSH Servers
2016	Audit Logs	Auditable event related to SSH Keys
2017	Audit Log	Auditable event related to SSH Service Accounts
2018	Audit Log	Auditable event related to SSH Key Rotation Alerts
2019	Audit Log	Auditable event related to SSH Users
2020	Audit Log	Auditable event related to Key Rotation Alerts
2021	Audit Log	Auditable event related to Certificate Stores
2022	Audit Log	Auditable event related to Orchestrator Job Types
2023	Audit Log	Auditable event related to Orchestrator Jobs
2024	Audit Log	Auditable event related to Bulk Orchestrator Job
2025	Audit Log	Auditable event related to Certificate Store Container
2026	Audit Log	Auditable event related to Orchestrator
2027	Audit Log	Auditable event related to Monitoring
2028	Audit Log	Auditable event related to License
2029	Audit Log	Auditable event related to Workflow Definition
2030	Audit Log	Auditable event related to Workflow Instance
2031	Audit Log	Auditable event related to Workflow Instance Signal

Table 61: Keyfactor Windows Orchestrator and Keyfactor Universal Orchestrator Windows Event IDs

Event ID	Task Category	Description
400	Monitoring	Job manager for the Keyfactor Windows Orchestrator starting
401	Monitoring	Job manager for the Keyfactor Windows Orchestrator stopping
1300	F5 Inventory	Keyfactor Windows Orchestrator: Starting inventory job for F5 certificate store (SSL Profile and Web Server) **Note:** This does not include F5 REST jobs, which are part of the AnyAgent and appear with AnyAgent messages.
1310	F5 Inventory	Keyfactor Windows Orchestrator: Completed inventory job for F5 certificate store (SSL Profile and Web Server)
1320	F5 Inventory	Keyfactor Windows Orchestrator: Error while performing an F5 inventory job
1400	F5 Management	Keyfactor Windows Orchestrator: Starting management job for F5 certificate store (SSL Profile and Web Server)
1410	F5 Management	Keyfactor Windows Orchestrator: Completed management job for F5 certificate store (SSL Profile and Web Server)
1420	F5 Management	Keyfactor Windows Orchestrator: Error while performing an F5 management job
1500	SSL Discovery	Starting SSL discovery job
1510	SSL Discovery	Completed SSL discovery job
1520	SSL Discovery	Error while performing SSL discovery job
1600	SSL Monitor	Starting SSL monitoring job
1610	SSL Monitor	Completed SSL monitoring job
1620	SSL Monitor	Error while performing SSL monitoring job
1630	SSL Monitor	Error connecting to an endpoint during an SSL scan
1640	SSL Monitor	Certificate approaching expiration found at endpoint during an SSL scan
1700	IIS Inventory	Keyfactor Windows Orchestrator: Starting inventory job for IIS certificate store (IIS Personal, IIS Trusted Root, and IIS Revoked)

Event ID	Task Category	Description
1710	IIS Inventory	Keyfactor Windows Orchestrator: Completed inventory job for IIS certificate store (IIS Personal, IIS Trusted Root, and IIS Revoked)
1720	IIS Inventory	Keyfactor Windows Orchestrator: Error while performing an IIS inventory job
1800	IIS Management	Keyfactor Windows Orchestrator: Starting management job for IIS certificate store (IIS Personal, IIS Trusted Root, and IIS Revoked)
1810	IIS Management	Keyfactor Windows Orchestrator: Completed management job for IIS certificate store (IIS Personal, IIS Trusted Root, and IIS Revoked)
1820	IIS Management	Keyfactor Windows Orchestrator: Error while performing an IIS management job
2100	NetScaler Inventory	Keyfactor Windows Orchestrator: Starting inventory job for NetScaler certificate store
2110	NetScaler Inventory	Keyfactor Windows Orchestrator: Completed inventory job for NetScaler certificate store
2120	NetScaler Inventory	Keyfactor Windows Orchestrator: Error while performing a NetScaler inventory job
2200	NetScaler Management	Keyfactor Windows Orchestrator: Starting management job for NetScaler certificate store
2210	NetScaler Management	Keyfactor Windows Orchestrator: Completed management job for NetScaler certificate store
2220	NetScaler Management	Keyfactor Windows Orchestrator: Error while performing a NetScaler management job
2400	AnyAgent Inventory	Keyfactor Windows Orchestrator: Starting inventory job for an AnyAgent (e.g. FTP, F5 REST) certificate store Keyfactor Universal Orchestrator: Starting inventory job for an AnyAgent (e.g. FTP, IIS) certificate store
2410	AnyAgent Inventory	Keyfactor Windows Orchestrator: Completed inventory job for an AnyAgent (e.g. FTP, F5 REST) certificate store Keyfactor Universal Orchestrator: Completed inventory job for an AnyAgent (e.g. FTP, IIS) certificate
2420	AnyAgent Inventory	Keyfactor Windows Orchestrator: Error while performing inventory job for an AnyAgent (e.g. FTP, F5 REST) certificate store

Event ID	Task Category	Description
		Keyfactor Universal Orchestrator: Error while performing inventory job for an AnyAgent (e.g. FTP, IIS) certificate store
2500	AnyAgent Management	Keyfactor Windows Orchestrator: Starting management job for an AnyAgent (e.g. FTP, F5 REST) certificate store Keyfactor Universal Orchestrator: Starting management job for an AnyAgent (e.g. FTP, IIS) certificate store
2510	AnyAgent Management	Keyfactor Windows Orchestrator: Completed management job for an AnyAgent (e.g. FTP, F5 REST) certificate store Keyfactor Universal Orchestrator: Completed management job for an AnyAgent (e.g. FTP, IIS) certificate
2520	AnyAgent Management	Keyfactor Windows Orchestrator: Error while performing management job for an AnyAgent (e.g. FTP, F5 REST) certificate store Keyfactor Universal Orchestrator: Error while performing management job for an AnyAgent (e.g. FTP, IIS) certificate store
2800	Audit Log	Keyfactor Universal Orchestrator: Starting fetch logs job
2810	Audit Log	Keyfactor Universal Orchestrator: Completed fetch logs job
2820	Audit Log	Keyfactor Universal Orchestrator: Error while performing fetch logs job
2900	Agent Service	Job manager for the Keyfactor Universal Orchestrator starting
2920	Agent Service	Job manager for the Keyfactor Universal Orchestrator stopped

2.2.6 Keyfactor Command Service Settings

The Keyfactor Command Service job has multiple parameters that control the jobs managed by the Keyfactor Command Service. Many of these can be updated through the configuration wizard by enabling or disabling specific jobs on the Service tab (see Service Tab in the *Keyfactor Command Server Installation Guide*).

> ⚠ **Important:** Keyfactor recommends that you make service setting adjustments only in consultation with your Keyfactor Customer Success Manager or support@keyfactor.com. Caution should be used when directly editing configuration files.

Some settings that may be of interest that can be directly edited in the configuration file include:

- Keyfactor.Sql.DbCommandTimeout

  The amount of time to allow a SQL request to run before canceling it with a timeout. This setting is used primarily to control the timeout on running upgrade scripts. For more information, see Troubleshooting in the *Keyfactor Command Upgrade Overview*. The value is given in seconds, so a value of 1800 seconds is 30 minutes.

- Keyfactor.TimerJobs.LockTimeout

  The amount of time to wait while attempting to acquire a SQL lock. This setting is primarily used for workflow and typically released in a second or so. The three SQL lock settings are only significant in environments where the Keyfactor Command service is running on more than one server. The value is given in milliseconds, so a value of 5000 milliseconds is 5 seconds.

- Keyfactor.TimerJobs.LockHeartbeatInterval

  The amount of time to wait before performing a SQL lock heartbeat. The lock heartbeat updates the LastTouched column in the Locks table. The three SQL lock settings are only significant in environments where the Keyfactor Command service is running on more than one server. The value is given in milliseconds, so a value of 60,000 milliseconds is 1 minute.

- Keyfactor.TimerJobs.LockHoldTimeout

  The amount of time before a SQL lock is considered lost and can be reacquired by a new job. If a Keyfactor Command service node cannot communicate with the database, the LastTouched column in the Locks table will not be updated. If the LastTouched time is further back than the LockHoldTimeout, the lock can be acquired by a new job. The three SQL lock settings are only significant in environments where the Keyfactor Command service is running on more than one server. The value is given in milliseconds, so a value of 900,000 milliseconds is 15 minute.

In addition to the settings that are in the configuration file by default, additional settings may be added as needed to support other features. One such feature is auditing of bulk metadata edits (see Certificate Details: Metadata Tab on page 20). When a bulk operation is performed, audit log entries for the activity are not immediately added to the audit log. Instead, these audit log updates are made periodically as a function of the Keyfactor Command Service. This is done to improve performance and avoid any delays that might be introduced for the user performing the bulk operation as audit entries are added. Parameters can be added to the configuration file to fine-time these updates as follows:

- Parallelism

  The number of threads used to handle bulk audit jobs. The default value if this is not configured is 2.

- JobSize

  The number of jobs that are put into memory during the execution of a single job. The default value if this is not configured is 5000.

When the audit entries are added to the SQL logger, the timestamp of the time the bulk job was requested is used, rather than the time that the job is run by the service. This allows the audit log entries for bulk jobs to appear chronologically alongside other jobs that occurred in the same time-frame when viewed in the Management Portal. However, other event sources, such as Linux syslog or Windows Event Viewer do not allow you to inject a timestamp into the action being logged. This

means that the timestamp for bulk jobs when viewed in this manner will be from the time they were added, and not the time the action actually occurred.

To update the configuration file:

1. On the Keyfactor Command server, open a text editor (e.g. Notepad) using the "Run as administrator" option.
2. In the text editor, browse to open the *CMSTimerService.exe.config* file in the Service directory under the installed directory. By default, this is:

   ```
   C:\Program Files\Keyfactor\Keyfactor Platform\Service\CMSTimerService.exe.config
   ```

3. To update one of the existing settings, locate the appSettings section and within this the setting you wish to update. These will look something like:

   ```
   <add key="Keyfactor.Sql.DbCommandTimeout" value="1800" />
   <add key="Keyfactor.TimerJobs.LockTimeout" value="5000" />
   <add key="Keyfactor.TimerJobs.LockHeartbeatInterval" value="60000" />
   <add key="Keyfactor.TimerJobs.LockHoldTimeout" value="900000" />
   ```

4. Adjust the values as needed.
5. To update the bulk metadata audit configuration, scroll to find the *container* section of the file and add the following register values within the container section:

   ```
   <register type="ITimerJobListener" mapTo-
   o="CSS.CMS.Service.Maintenance.Managers.BulkAuditJobManager, CSS.CMS.Service.Jobs" name-
   e="BulkAuditJobManager">
      <property name="Parallelism" value="2" />
      <property name="JobSize" value="5000" />
   </register>
   ```

   Adjust the values as needed.
6. Save the file.

2.2.7 License Expiration Monitoring and Rotation

As your license is approaching expiration, warnings will be written to the Windows event log on the server running the Keyfactor Command service 60 days, 30 days and 5 days in advance of the license expiration (or at the next start of the Keyfactor Command service that falls within these time periods) using event ID 1001.

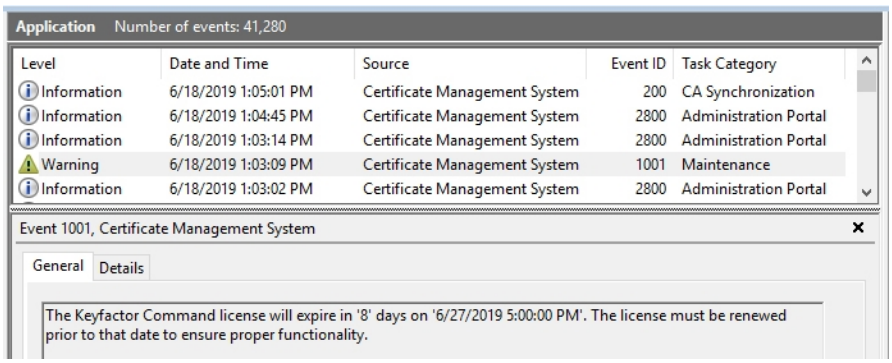


Figure 420: License Expiration Event Log

New primary Keyfactor Command licenses may be updated on the Licenses page of the Keyfactor Command Management Portal (see Licensing on page 696).

Tip: An error message of "Denied by Policy Module" with "Class is not licensed for use 0x80040112" on an attempt to enroll against a CA running the Keyfactor CA Policy Module can be an indication that the license for the policy module has expired.

New licenses for the Keyfactor CA Policy Module should be installed on the CA where the policy module is installed as follows:

1. On the CA where the policy module is installed, open the Certification Authority management tool.
2. In the Certification Authority management tool, right-click the CA name at the top of the tree and choose **Properties**.
3. In the Properties dialog for the CA on the CA Policy Module tab, confirm that the *Keyfactor Custom Policy Module* is the selected module and click **Properties**.
4. On the Licensing tab of the Policy Module Configuration Properties page, click **Upload License** and browse to locate the license file provided to you by Keyfactor. This file should have the extension CMSLICENSE.

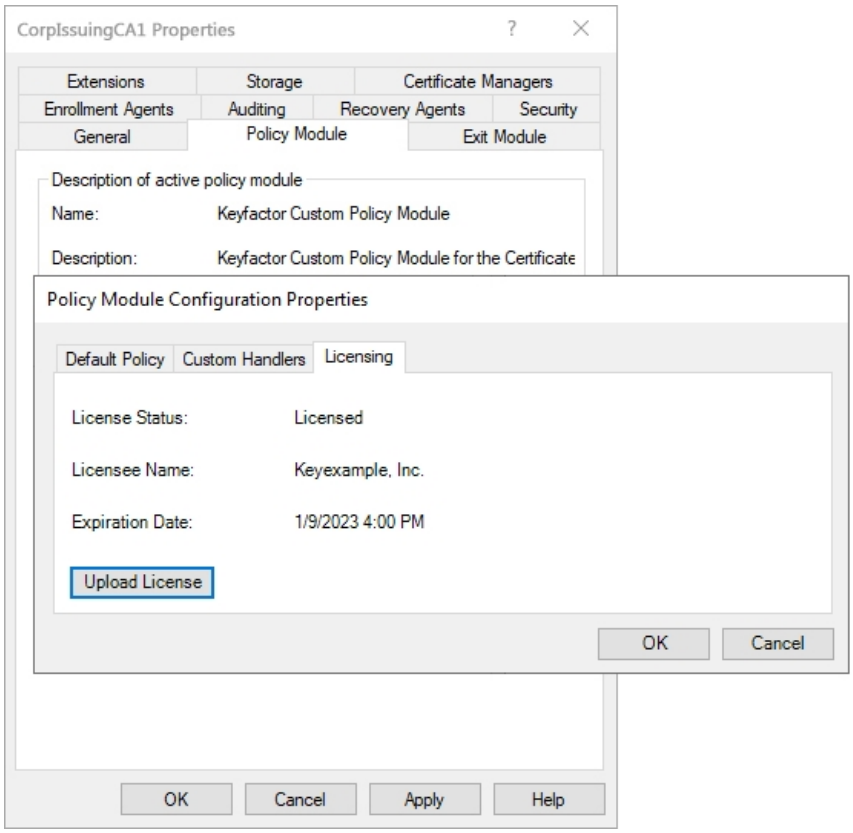


Figure 421: Upload a New Keyfactor Command License

5. Click **OK** as many times as needed to close the configuration dialogs and save the configuration.
6. Restart the CA services.

2.2.8 SQL Database Migration

If you need to move your Keyfactor Command database from one SQL server to another, the process is similar to a controlled disaster recovery. You will need a backup of your Keyfactor Command database and the ability to decrypt the encrypted content within the database (see SQL Encryption Key Backup on page 705). By default, a new SQL server will have a different service master key (SMK) than your original SQL server. To support the migration, you have a few options:

- Set the SMK on the new server to match that of the old server and do a simple restore of the database. This may not be a feasible solution if there are any other applications on the new server that use SQL encryption.
- Temporarily add a known password to the database master key (DMK) on the Keyfactor Command database (if one is not known already).

To transfer a Keyfactor Command database between two SQL servers that do not share the same SMK, as a user with *control* permission on the Keyfactor Command database:

1. Add a known password to the DMK by issuing the following SQL command in the Keyfactor Command database. You can specify any password you want that meets the Windows password complexity rules.

    ```
    ALTER MASTER KEY ADD ENCRYPTION BY PASSWORD = 'SecurePassword#1234'
    ```

    Important: Note that at this point, in addition to the backup you are about to manually make, any automated backups of the Keyfactor Command database will contain this DMK password and anyone with access to the backup media and the password would be able to decrypt the sensitive information within the Keyfactor Command database.

2. Use your preferred SQL server tools to back up the database, copy the backup media to the target server, and restore the database on the target server.

3. Use the following SQL commands on the target server to manually open the DMK, protect the DMK with the target server's SMK, and remove the DMK password (referencing the password you used on your DMK):

    ```
    OPEN MASTER KEY DECRYPTION BY PASSWORD = 'SecurePassword#1234'

    ALTER MASTER KEY ADD ENCRYPTION BY SERVICE MASTER KEY

    ALTER MASTER KEY DROP ENCRYPTION BY PASSWORD = 'SecurePassword#1234'
    ```

4. Open a new query window on the target server and use the following SQL to validate that the DMK is properly encrypted by the SMK and that the Keyfactor Command application will be able to ask SQL server to decrypt information in the database. The commands should run without error.

    ```
    OPEN SYMMETRIC KEY [CMS_SecretsSymmetricKey] DECRYPTION BY CERTIFICATE [CMS_
    SecretsCertificate];

    CLOSE SYMMETRIC KEY [CMS_SecretsSymmetricKey]
    ```

5. On the source server, if you are not going to remove the Keyfactor Command database, issue the following SQL command to remove the DMK that was added (referencing the password you used on your DMK):

    ```
    ALTER MASTER KEY DROP ENCRYPTION BY PASSWORD = 'SecurePassword#1234'
    ```

6. Delete the backup or securely store the backup media that was used, along with the temporary DMK password, as it can be used to obtain the encrypted Keyfactor Command information.

2.2.9 Configuring Key Recovery for Keyfactor Command

The following instructions for configuring CA-level key recovery within Keyfactor Command assume that your Microsoft CA is already configured for key recovery and that you have the key recovery agent (KRA) certificate available as a PFX file for import on the Keyfactor Command administration server. Instructions for configuring key recovery on a Microsoft CA are beyond the scope of this guide.

Tip: CA-level key recovery is supported for Microsoft CAs to allow recovery of private keys for certificates enrolled outside of Keyfactor Command. CA-level key archiving is not supported for enrollments done through Keyfactor Command. CA-level key recovery is not supported for EJBCA CAs. For enrollments done through Keyfactor Command for either Microsoft or EJBCA CAs, use Keyfactor Command private key retention (see Details Tab on page 360).

To configure your Keyfactor Command administration server to support key recovery:

1. Login on the Keyfactor Command administration server as the service account under which the Keyfactor Command application pool is running and open a command prompt. Alternately, if you have previously logged on as this service account and created a user profile for the service account, you can open a command prompt as the service account using Shift-Right-Click and choose "Run as different user". Within the command prompt type the following to open the certificates MMC for the service account user:

   ```
   certmgr.msc
   ```

2. Import the KRA PFX file into the service account user's personal certificate store.

This process needs to be repeated using the KRA certificate(s) from each CA for which you want to enable recovery within the Management Portal.

Note: To provide additional security over KRA private key(s), Keyfactor strongly recommends the use of a Hardware Security Module (HSM) such as the Thales NetHSM.

Tip: CA-level key recovery is not supported for EJBCA CAs. Instead, use private key retention within Keyfactor Command (see Details Tab on page 360).

2.2.10 Disable Loopback Checking

For some features of the Management Portal to function correctly when using Kerberos authentication (e.g. delegation of CA functions, alerting using the event logging event handler and a DNS alias or alternate target machine), it may be necessary to disable loopback checking on the Keyfactor Command server.

To disable loopback checking for selected FQDNs:

1. On the Keyfactor Command server, open the registry editor and browse to:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

2. Right-click the Parameters registry key and choose **New** > **DWORD (32-bit) Value**. Name the new DWORD value **DisableStrictNameChecking**. Set the **DisableStrictNameChecking** value to 1.

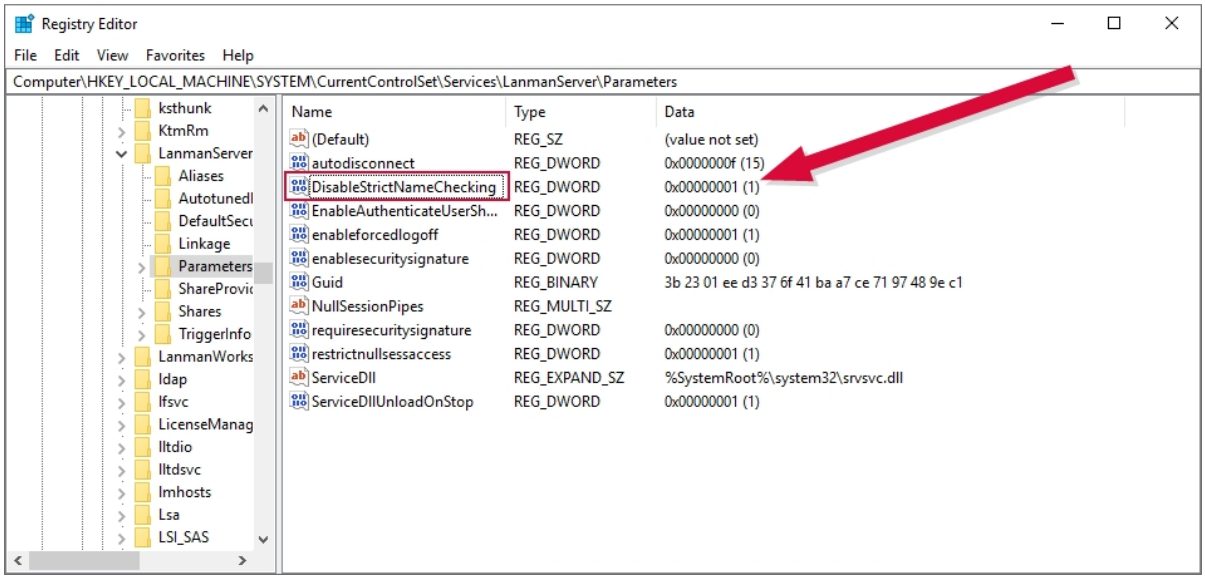


Figure 422: Disable Loopback Checking: DisableStrictNameChecking

3. In the registry editor browse to:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0

4. Right-click the MSV1_0 registry key and choose **New** > **Multi-String Value**. Name the new value **BackConnectionHostNames**. Edit the **BackConnectionHostNames** value and enter each fully qualified domain name—actual name or DNS alias—for a server that needs this feature on a separate line. For example, for full DNS alias support with CA delegation functions, you need to enter the DNS alias of the Keyfactor Command server. For event logging to a machine other than the Keyfactor Command server, you need to enter the name of that server.

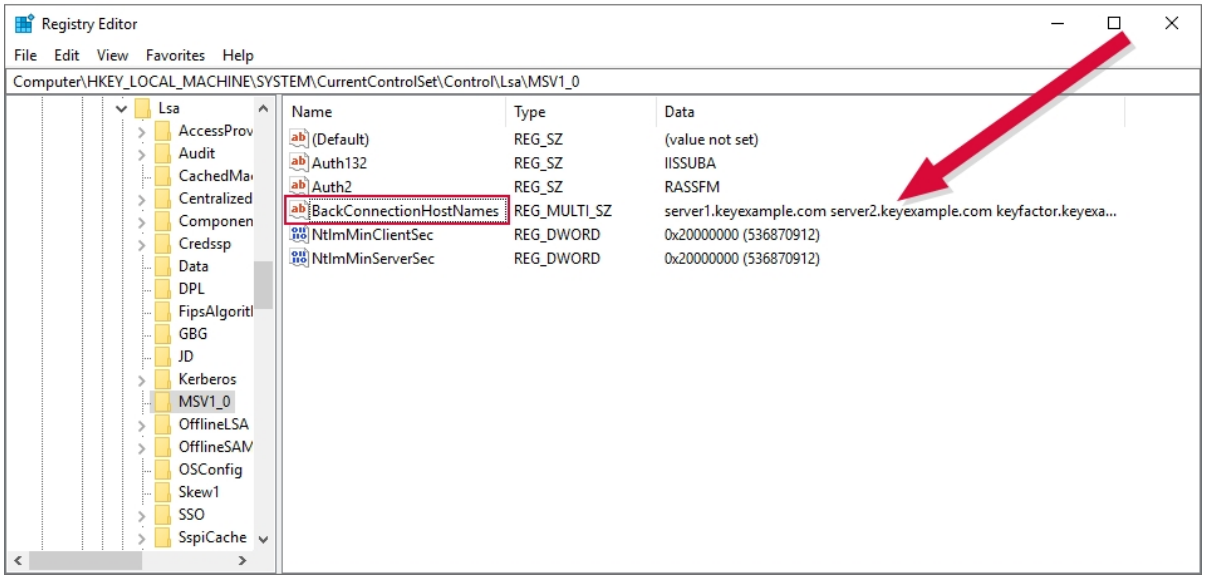


Figure 423: Disable Loopback Checking: BackConnectionHostNames

5. After completing the registry configuration you must reboot the Keyfactor Command server before the changes will take effect.

2.2.11 Troubleshooting

The following error conditions and general troubleshooting tips may be helpful in resolving issues with the Keyfactor Command server. Generally speaking, issues on installation or upgrade are often related to SQL connectivity or permissions. Certificate enrollment issues are often related to Kerberos configuration problems.

Debug Logging and Error Messages

It is often helpful to enable debug logging on the server. For information on configuring this, see Editing NLog on page 709.

Once the logging is set at debug or trace level, it can be helpful to watch the logs live while activity is going on. There are tools on Windows with functionality similar to the Linux tail function to watch the log in real time. Notepad++, for example, has this functionality built in. Be sure to review all the logs that could be relevant. For example, installation and configuration messages are found in the configuration log. Messages related to using the Management Portal can be found in both the portal log and the Keyfactor API log.

Some messages in the Keyfactor API and orchestrators API logs include a correlation ID that helps to identify log messages that originated from the same request. The correlation ID is a randomly generated GUID that often appears just after the date in the log entry (C282ACA1-DED5-4F2E-B83B-F3F9E865E371 in the following example) and is the same for all log messages for the given request until the request completes.

```
2022-09-13 04:51:18.6884 C282ACA1-DED5-4F2E-B83B-F3F9E865E371 CSS.CMS.We-
b.KeyfactorApi.Controllers.Enrollment.Enrollment2Controller [Trace] - Starting PFX Enrollment Process
2022-09-13 04:51:19.0477 C282ACA1-DED5-4F2E-B83B-F3F9E865E371 Keyfactor.Com-
mand.Workflows.Engine.WorkflowGraph [Error] - Invalid O provided: Value must be Key Example, Inc or
Key Example.
```

General Errors

Below are some possible errors you might encountered and some suggested troubleshooting tips or solutions.

A connection was successfully established with the server, but then an error occurred during the login process. (provider: SSL Provider, error: 0 - The certificate chain was issued by an authority that is not trusted.)

You many encounter this error when trying to install or upgrade to Keyfactor Command version 10 or later:

```
2022-03-04 09:58:55.7262 CSS.CMS.Install.ConfigurationWizard.ViewModels.DatabaseViewModel [Error] -
Unable to configure database
2022-03-04 09:58:55.9821 CSS.CMS.Install.ConfigurationWizard.ViewModels.DatabaseViewModel [Error] -
An error occurred while preparing the database
at CSS.CMS.Install.ConfigurationWizard.ViewModels.DatabaseViewModel.b(Object A_0, RunWork-
erCompletedEventArgs A_1)

A connection was successfully established with the server, but then an error occurred during the
login process. (provider: SSL Provider, error: 0 - The certificate chain was issued by an authority
that is not trusted
```

Keyfactor Command version 10 requires an encrypted connection to the SQL server. If the SQL server is not configured correctly to receive a secure connection (is not configured with a valid certificate that is trusted by the Keyfactor Command server), you may receive this message.

For information about configuring TLS for SQL server, see:

> https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/enable-encrypted-connections-to-the-database-engine?view=sql-server-ver15

The request subject name is invalid or too long

```
The certificate request failed with the reason 'The request subject name is invalid or
too long. (Exception from HRESULT: 0x80094001).'
```

You may encounter this error on an enrollment when the CA rejects the request. If the request is clearly not excessively long, review the request for invalid characters. Be sure to also check the default subject (see the Subject Format application setting on the Application Settings: Enrollment

Tab on page 591 and the subject defaults in certificate templates for both Configuring System-Wide Settings on page 355 and Enrollment Defaults Tab on page 370). Quotation marks should not be used in the fields of the default subject except in the case where these are part of the desired subject value, as they are processed as literal values. This is a change from earlier versions of Keyfactor Command where quotation marks were used around fields containing embedded commas.

This error can also appear of the CA receives an enrollment request with no subject at all.

Request failed with status code 405

You may encounter this error either in the Keyfactor Command Management Portal or when submitting a Keyfactor API request. This error is typically not accompanied by any error in the Keyfactor Command logs. This error can occur if the IIS *WebDAV Publishing* feature is installed on the Keyfactor Command server. Keyfactor Command is not compatible with this IIS feature. Uninstall the *WebDAV Publishing* feature, reboot if required, and try your command again.

Denied by Policy Module: Class is not licensed for use 0x80040112

This error may appear during certificate enrollment against a certificate authority running the Keyfactor CA Policy Module if the license for the policy module has expired. See License Expiration Monitoring and Rotation on page 741 for license update information.

Error: Unable to acquire lock on resource TimerServiceJob

You may occasionally see error messages in the service log similar to the following if you are running Keyfactor Command in a redundant environment:

```
2023-01-12 16:55:00.0618  Keyfactor.LockProviders.SqlLockProvider [Error] - Unable to acquire lock
on resource 'TimerServiceJob_https://ejbca3_keyother_com:8443 - CorpIssuingCA2 - Differencing
1/13/2023 12:55:00 AM'.

2023-01-12 16:55:00.0618  b [Error] - An error occured attempting to produce an instance of 'NoOver-
lapJobLoggingWrapper`1': Unable to acquire lock on resource 'TimerServiceJob_https://ejbca3_
keyother_com:8443 - CorpIssuingCA2 - Differencing 1/13/2023 12:55:00 AM'.
at System.Runtime.ExceptionServices.ExceptionDispatchInfo.Throw()
at Keyfactor.LockProviders.SqlLockProvider.AcquireLock(LockType type, String key)
at b.NewJob(TriggerFiredBundle bundle, IScheduler scheduler)

2023-01-12 16:55:00.0618  Quartz.Core.ErrorLogger [Error] - An error occurred instantiating job to
be executed. job= 'DEFAULT.CASynchronizationService-56'
2023-01-12 16:55:00.0618  Quartz.Core.ErrorLogger [Error] - An error occurred instantiating job to
be executed. job= 'DEFAULT.CASynchronizationService-56'
2023-01-12 16:55:00.0618  Quartz.Simpl.RAMJobStore [Info] - All triggers of Job DEFAULT.CASyn-
chronizationService-56 set to ERROR state.
```

These message indicate that the Keyfactor Command Service on two different Keyfactor Command servers both attempted to run the same job at the same time and this server was unable to acquire a lock to run that job—the other server ran the job instead. This normally does not indicate any problem. If these errors occur frequently, it may be helpful to increase the timeout value for the job locking mechanism. To do this:

1. On each Keyfactor Command server, open a text editor (e.g. Notepad) using the "Run as administrator" option.

2. In the text editor, browse to open the *CMSTimerService.exe.config* file. This file is located in the Service directory within the install directory, which is the following directory by default:

   C:\Program Files\Keyfactor\Keyfactor Platform\Service

3. In the *CMSTimerService.exe.config* file, locate the *Keyfactor.TimerJobs.LockTimeout* key in the *appSettings* section and increase the value appropriately for your environment. The value is specified in milliseconds, so the default value of 5000 indicates that the Keyfactor Command Service will attempt to acquire a lock on the job for 5 seconds before producing an error if the lock cannot be obtained.

   ```
   <appSettings>
     <add key="Keyfactor.Sql.DbCommandTimeout" value="120" />
     <add key="PurgeSSLDbCommandTimeout" value="600" />
     <add key="PurgeAuditLogsDbCommandTimeout" value="600" />
     <add key="UpdateStatsDbCommandTimeout" value="1800" />
     <add key="ClientSettingsProvider.ServiceUri" value="" />
     <add key="NLogConfigFile" value="NLog_TimerService.config" />
     <add key="Keyfactor.TimerJobs.iOSCleanup" value="true" />
     <add key="Keyfactor.TimerJobs.PfxCleanup" value="true" />
     <add key="Keyfactor.TimerJobs.PendingAlerts" value="true" />
     <add key="Keyfactor.TimerJobs.LockTimeout" value="5000" />
     <add key="MetadataGeneration.MetadataVersion" value="1" />
   ```

   Figure 424: Adjust the Keyfactor.TimerJobs.LockTimeout Value

4. Restart the Keyfactor Command Service (see Enable and Start the Keyfactor Command Service in the *Keyfactor Command Server Installation Guide*) to read the updated configuration.

Note: Keyfactor recommends that any edits to this lockout value are made in consultation with Keyfactor support.

Certificate Validation Errors

On the Validation tab of the certificate details you will sometimes see a fail result for some of the validation tests. The following are some possible reasons why this might occur.

- If you see both *Full Chain* and *CRL Online* in a fail state, this generally indicates that you have not imported the root and/or intermediate certificate for the certificate into the appropriate store on the Keyfactor Command server (see *Configure Certificate Chain Trusts for CAs* in the

Keyfactor Command Server Installation Guide).

- If you see just *CRL Online* in a fail state, this generally indicates that the Certificate Revocation List (CRL) for the CA could not be reached.

  > ⚠ **Important:** Because a "+" (plus sign) in a URL can represent either a space or a "+" Keyfactor Command has chosen to read "+" as a space. For CRL URLs that require a "+" (plus sign), rather than a space, replace plus signs in your CRL's URL with "`%2B`". Only replace the plus signs you don't wish to be treated as a space.

- If you see *Revocation Status* in a fail state but *CRL Online* is in a pass state, this can indicate that the CRL is accessible but expired, that the CRL is not fully configured, or that the Authority Information Access (AIA) for the CA has not been configured correctly or could not be reached.

  For EJBCA CAs, CRLs and AIA need to be configured both at the CA level and at the certificate profile level. One way to do this is:

  - AIA: Set the path to the AIA in the *CA issuer Default URI* field in the CA. You can find this on the *Fetch CA certificates* page of your EJBCA public web. Check both the *Authority Information Access* box and the *Use CA defined CA issuer* box in each certificate profile.
  - CRL: Set the path to the CRL distribution point (CDP) in the *Default CRL Distribution Point* field in the CA. If appropriate for your environment, set also the *Default CRL Issuer* and/or *Default Freshest CRL Distribution Point* (delta CRLs). Check both the *CRL Distribution Points* box and the *Use CA defined CRL Distribution Point* box in each certificate profile.

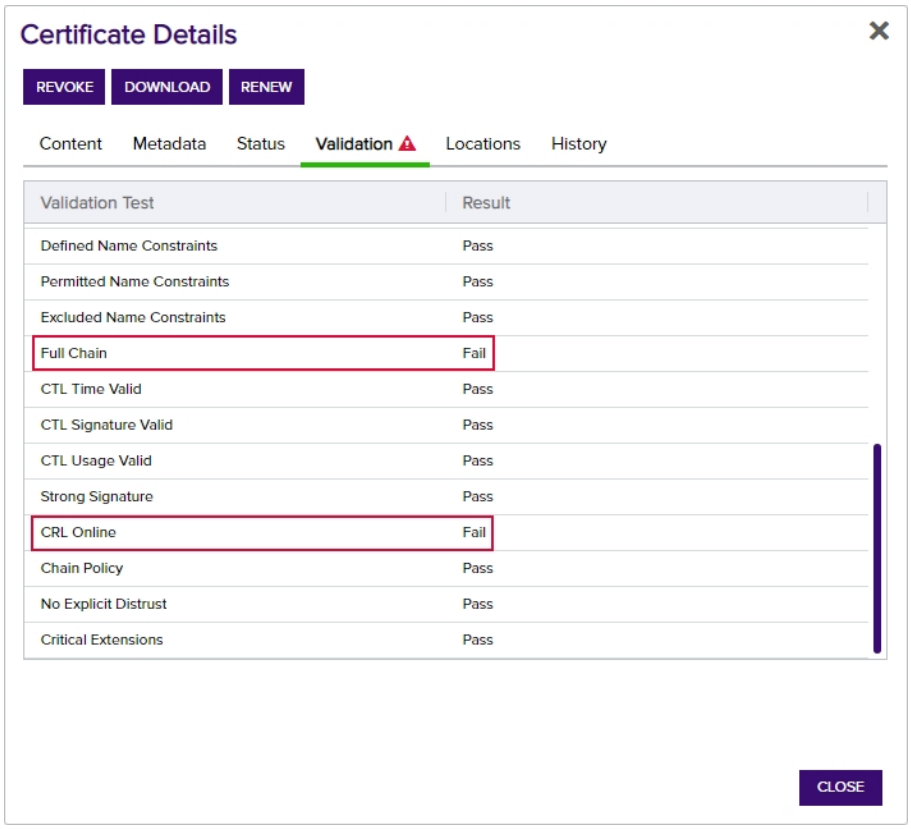


Figure 425: Certificate Validation Fails for Full Chain and CRL Online

Slow SSL Jobs

If SSL jobs are taking longer to complete than expected and you check the log on the orchestrator and find messages similar to the following:

```
2021-08-24 17:22:48.4463 Keyfactor.WindowsAgent.Jobs.SSL.SslDiscovery [Error] - Error
while sending SSL Batch for audit id 158558. Check the CMS Server log for more details.
Response status code does not indicate success: 413 (Request Entity Too Large).
at System.Net.Http.HttpResponseMessage.EnsureSuccessStatusCode()
at Keyfactor.WindowsAgent.Jobs.GenericJobExecutor`7.f.h()
2021-08-24 17:22:48.4463 Keyfactor.WindowsAgent.Jobs.SSL.SslDiscovery [Info] - Splitting
endpoint result batch of 29 into smaller pieces and retrying
```

You may want to make modifications to the IIS maximum request size settings on your Keyfactor Command server to allow it to accept larger incoming pieces of content to streamline SSL scanning. You can do this using the configuration editor built into the IIS management console. Make the setting changes at the Default Web Site level (or other web site, if you installed your Keyfactor Command in an alternate web site). There are three settings to change:

- system.webServer/security/requestFiltering/requestLimits/maxAllowedContentLength
- system.webServer/serverRuntime/uploadReadAheadSize
- system.web/httpRuntime/maxRequestLength

Set each system.webServer value to at least 1,000,000 bytes for best SSL scanning performance. The default value of 4096 KB for the maxRequestLength will probably be sufficient for SSL scanning in most environments, but if it has been reduced in your environment, you may need to increase it. (The system.webServer values are set in bytes while the system.web values are set in kilobytes.) If you are scanning networks with especially large numbers of returned certificates, you may need to increase all these values. Monitor the orchestrator logs after modifying the values to confirm that you have achieved the desired effect.

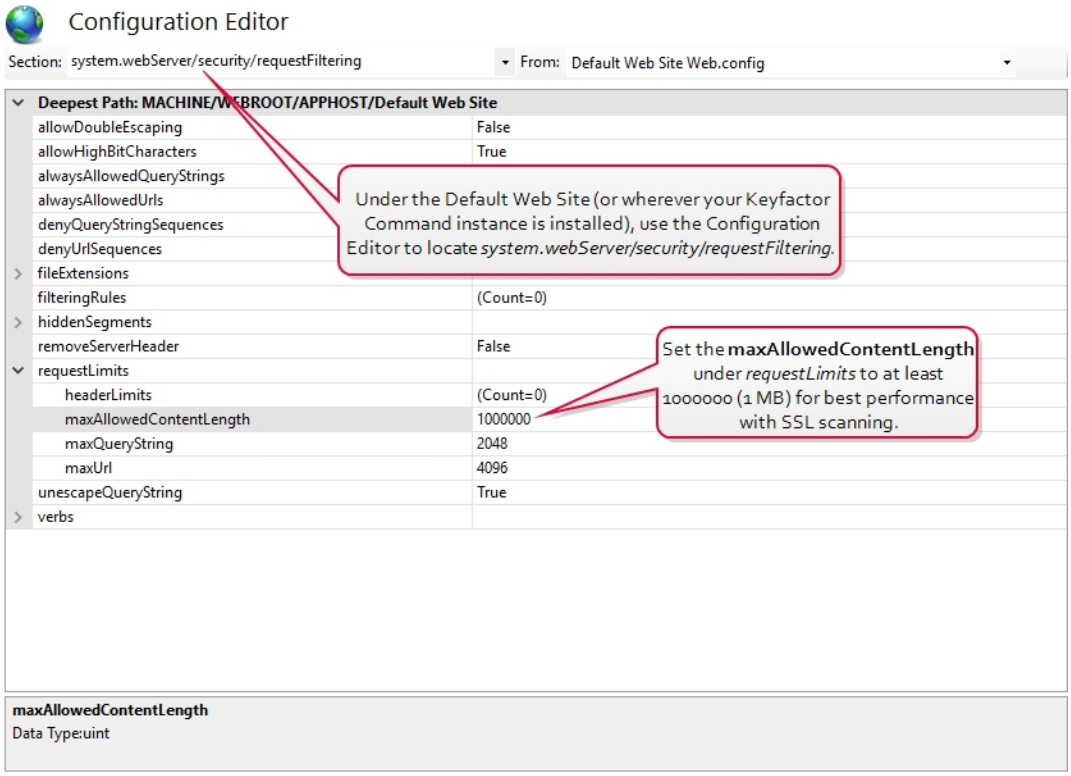


Figure 426: Modify IIS Settings for SSL Scanning: maxAllowedContentLength

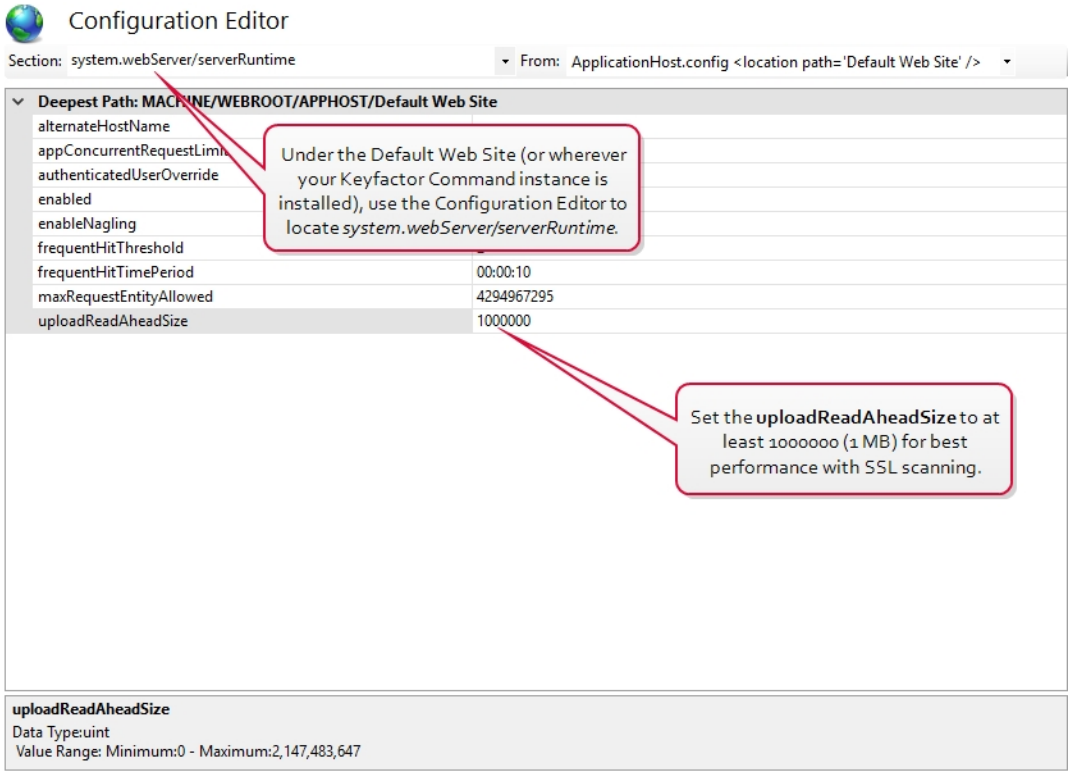


Figure 427: Modify IIS Settings for SSL Scanning:uploadReadAheadSize

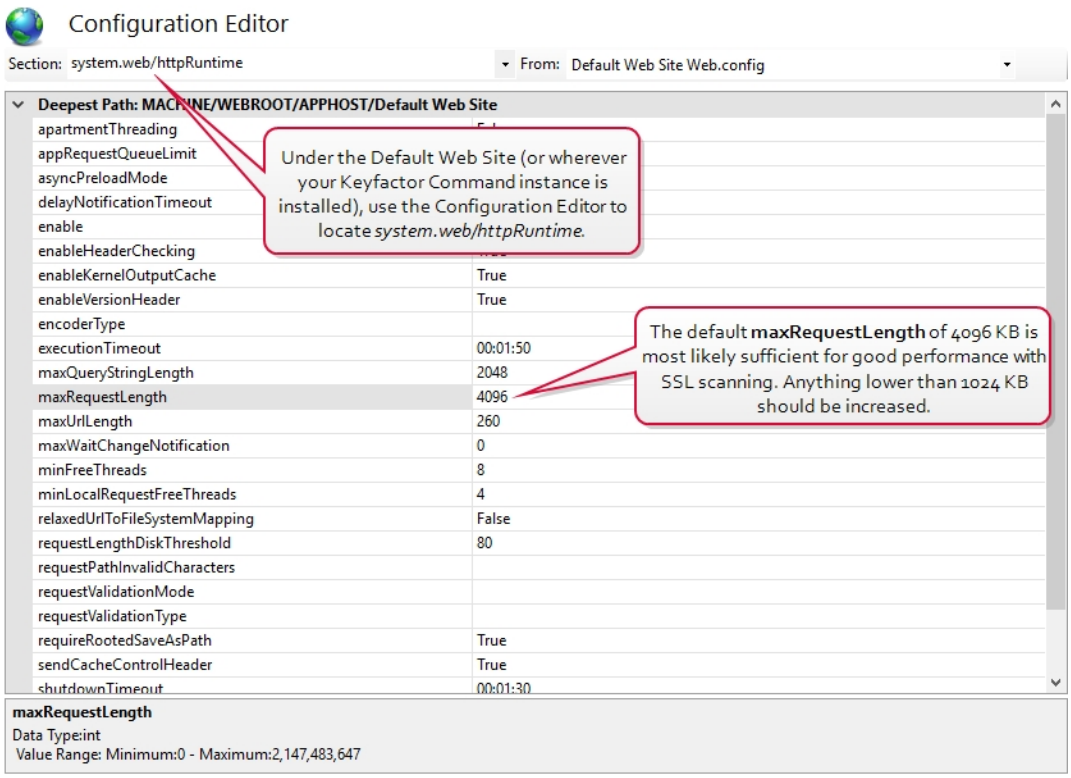


Figure 428: Modify IIS Settings for SSL Scanning: maxRequestLength

2.3 Appendices

- Appendix - References below
- Appendix - Third-Party Notices for Keyfactor Command Software below

2.3.1 Appendix - References

CIDR, Classless Inter-Domain Routing

http://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing

2.3.2 Appendix - Third-Party Notices for Keyfactor Command Software

This Software from Keyfactor incorporates or interacts with third-party material from the files listed below. While Keyfactor is not the original author of the third-party material, Keyfactor licenses this material under the terms set forth in the license agreements below.

Keyfactor Command distributions may include the following Third-Party Materials. Since many of these materials use the same copyright text, a copy of the applicable text from each license is provided below.

Table 62: Third-Party Notices for Keyfactor Command Software Distributions

Description	Version	Copyright Holder	License
ADOObjectPicker	1.0.0	Tulpep	Microsoft Public
ajaxFileInput	1.0.0	OpenJs	MIT
Apache Codec	1.6	Apache.org	Apache 2.0
Apache Commons	4.3.3	Apache.org	Apache 2.0
Apache http client	4.3.6	Apache.org	Apache 2.0
at-caret	1.3.1	Gideon Sireling	BSD
BouncyCastle	1.8.1	BouncyCastle	MIT
Chosen	1.0.0	Patrick Filler	MIT
Common Logging	3.2.0	(Multiple)	Apache 2.0
contextmenu	1.1	Matt Kruse	MIT
DateTimeEntry	2.0.0	Keith Wood	MIT
Filedownload	1.4.2	John Culviner	MIT
Flexigrid	1.1	Paolo Marinas	MIT
History.js	1.8b2	Community	BSD
Iframe	1.8.2	Sebastion Tschan	MIT
Joda Time	2.8.1	Apache.org	Apache 2.0
jqPlot	1.0.8	Chris Leonello	MIT
jQuery	2.1.0	jQuery Foundation	MIT
jQuery UI	1.10.3	jQuery Foundation	MIT
jQuery Validate	1.9	Jorn Zaeffer	MIT
jsTree	3.1.0	Ivan Bozhanov	MIT
Layout	1.3.0	Kevin Dalman	MIT
Log4j2	2.1	Apache.org	Apache 2.0

Description	Version	Copyright Holder	License
NewtonSoft	6.0.8	James Newton-King	MIT
NLog	4	(Multiple)	MIT
Quartz	2.3.3	Marko Lahama	Apache 2.0
Unity	4.0.1	Microsoft	Microsoft Public
WiX	3.1	.NET Foundation	Microsoft Reciprocal
WPF Extensions	2.2.0	Microsoft	Microsoft Public

A copy of the applicable text from each license is provided below.

2.3.2.1 Apache 2.0 License Text:

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

“License” shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

“Licensor” shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

“Legal Entity” shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, “control” means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

“You” (or “Your”) shall mean an individual or Legal Entity exercising permissions granted by this License.

“Source” form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

“Object” form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License.

Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License.

Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution.

You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

You must give any other recipients of the Work or Derivative Works a copy of this License; and

You must cause any modified files to carry prominent notices stating that You changed the files; and

You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions.

Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks.

This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty.

Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability.

In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work

stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability.

While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

2.3.2.2 BSD License Text:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the copyright holder nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

2.3.2.3 MIT License Text:

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

2.3.2.4 Microsoft Public License (MS-PL) Text:

This license governs use of the accompanying software. If you use the software, you accept this license. If you do not accept the license, do not use the software.

1. Definitions

The terms “reproduce,” “reproduction,” “derivative works,” and “distribution” have the same meaning here as under U.S. copyright law.

A “contribution” is the original software, or any additions or changes to the software.

A “contributor” is any person that distributes its contribution under this license.

“Licensed patents” are a contributor’s patent claims that read directly on its contribution.

2. Grant of Rights

(A) Copyright Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free copyright license to reproduce its contribution, prepare derivative works of its contribution, and distribute its contribution or any derivative works that you create.

(B) Patent Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free license under its licensed patents to make, have made, use, sell, offer for sale, import, and/or otherwise dispose of its contribution in the software or derivative works of the contribution in the software.

3. Conditions and Limitations

(A) No Trademark License- This license does not grant you rights to use any contributors’ name, logo, or trademarks.

(B) If you bring a patent claim against any contributor over patents that you claim are infringed by the software, your patent license from such contributor to the software ends automatically.

(C) If you distribute any portion of the software, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.

(D) If you distribute any portion of the software in source code form, you may do so only under this license by including a complete copy of this license with your distribution. If you distribute any portion of the software in compiled or object code form, you may only do so under a license that complies with this license.

(E) The software is licensed “as-is.” You bear the risk of using it. The contributors give no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this license cannot change. To the extent permitted under your local laws, the contributors exclude the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

2.3.2.5 Microsoft Reciprocal License (MS-RL) Text:

This license governs use of the accompanying software. If you use the software, you accept this license. If you do not accept the license, do not use the software.

1. Definitions

The terms “reproduce,” “reproduction,” “derivative works,” and “distribution” have the same meaning here as under U.S. copyright law.

A “contribution” is the original software, or any additions or changes to the software.

A “contributor” is any person that distributes its contribution under this license.

“Licensed patents” are a contributor’s patent claims that read directly on its contribution.

2. Grant of Rights

(A) Copyright Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free copyright license to reproduce its contribution, prepare derivative works of its contribution, and distribute its contribution or any derivative works that you create.

(B) Patent Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free license under its licensed patents to make, have made, use, sell, offer for sale, import, and/or otherwise dispose of its contribution in the software or derivative works of the contribution in the software.

3. Conditions and Limitations

(A) Reciprocal Grants- For any file you distribute that contains code from the software (in source code or binary format), you must provide recipients the source code to that file along with a copy of this license, which license will govern that file. You may license other files that are entirely your own work and do not contain code from the software under any terms you choose.

(B) No Trademark License- This license does not grant you rights to use any contributors’ name, logo, or trademarks.

(C) If you bring a patent claim against any contributor over patents that you claim are infringed by the software, your patent license from such contributor to the software ends automatically.

(D) If you distribute any portion of the software, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.

(E) If you distribute any portion of the software in source code form, you may do so only under this license by including a complete copy of this license with your distribution. If you distribute any portion of the software in compiled or object code form, you may only do so under a license that complies with this license.

(F) The software is licensed “as-is.” You bear the risk of using it. The contributors give no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this license cannot change. To the extent permitted under your local laws, the contributors exclude the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

3.0 Glossary

A

AIA

The authority information access (AIA) is included in a certificate--if configured--and identifies a location from which the chain certificates for that certificate may be retrieved.

AnyAgent

The AnyAgent, one of Keyfactor's suite of orchestrators, is used to allow management of certificates regardless of source or location by allowing customers to implement custom agent functionality via an API.

AnyGateway

The Keyfactor AnyGateway is a generic third party CA gateway framework that allows existing CA gateways and custom CA connections to share the same overall product framework.

API

A set of functions to allow creation of applications. Keyfactor offers the Keyfactor API, which allows third-party software to integrate with the advanced certificate enrollment and management features of Keyfactor Command.

Argument

A parameter or argument is a value that is passed into a function in an application.

Authority Information Access

The authority information access (AIA) is included in a certificate--if configured--and identifies a location from which the chain certificates for that certificate may be retrieved.

B

Bash Orchestrator

The Bash Orchestrator, one of Keyfactor's suite of orchestrators, is used to discover and manage SSH keys across an enterprise.

Blueprint

A snapshot of the certificate stores and scheduled jobs on one orchestrator, which can be used to create matching certificate stores and jobs on another orchestrator with just a few clicks.

C

CA

A certificate authority (CA) is an entity that issues digital certificates. Within Keyfactor Command, a CA may be a Microsoft CA or a Keyfactor gateway to a cloud-based or remote CA.

Certificate Authority

A certificate authority (CA) is an entity that issues digital certificates. Within Keyfactor Command, a CA may be a Microsoft CA or a Keyfactor gateway to a cloud-based or remote CA.

Certificate Revocation List

A Certificate Revocation List (CRL) is a list of digital certificates that have been revoked by the issuing Certificate Authority (CA) before their scheduled expiration date and should no longer be trusted.

Certificate Signing Request

A CSR or certificate signing request is a block of encoded text that is submitted to a CA when enrolling for a certificate. When you generate a CSR within Keyfactor

Command, the matching private key for it is stored in Keyfactor Command in encrypted format and will be married with the certificate once returned from the CA.

CN

A common name (CN) is the component of a distinguished name (DN) that represents the primary name of the object. The value varies depending on the type of object. For a user object, this would be the user's name (e.g. CN=John Smith). For SSL certificates, the CN is typically the fully qualified domain name (FQDN) of the host where the SSL certificate will reside (e.g. servername.keyexample.com or www.keyexample.com).

Collection

The certificate search function allows you to query the Keyfactor Command database for certificates from any available source based on any criteria of the certificates and save the results as a collection that will be availble in other places in the Management Portal (e.g. expiration alerts and certain reports).

Common Name

A common name (CN) is the component of a distinguished name (DN) that represents the primary name of the object. The value varies depending on the type of object. For a user object, this would be the user's name (e.g. CN=John Smith). For SSL certificates, the CN is typically the fully qualified domain name (FQDN) of the host where the SSL certificate will reside (e.g. servername.keyexample.com or www.keyexample.com).

Configuration Tenant

A grouping of CAs. The Microsoft concept of forests is not used in EJBCA so to accommodate the new EJBCA functionality, and to avoid confusion, the term forest needed to be renamed. The new name is configuration tenant. For EJBCA, there would be one configuration tenant per EJBCA server install. For Microsoft, there would be one per forest. Note that configuration tenants cannot be mixed, so Microsoft and EJBCA cannot exist on the same configuration tenant.

CRL

A Certificate Revocation List (CRL) is a list of digital certificates that have been revoked by the issuing Certificate Authority (CA) before their scheduled expiration date and should no longer be trusted.

CSR

A CSR or certificate signing request is a block of encoded text that is submitted to a CA when enrolling for a certificate. When you generate a CSR within Keyfactor Command, the matching private key for it is stored in Keyfactor Command in encrypted format and will be married with the certificate once returned from the CA.

D

DER

A DER format certificate file is a DER-encoded binary certificate. It contains a single certificate and does not support storage of private keys. It sometimes has an extension of .der but is often seen with .cer or .crt.

Distinquished Name

A distinguished name (DN) is the name that uniquely identifies an object in a directory. In the context of Keyfactor Command, this directory is generally Active Directory. A DN is made up of attribute=value pairs,

separated by commas. Any of the attributes defined in the directory schema can be used to make up a DN.

DN

A distinguished name (DN) is the name that uniquely identifies an object in a directory. In the context of Keyfactor Command, this directory is generally Active Directory. A DN is made up of attribute=value pairs, separated by commas. Any of the attributes defined in the directory schema can be used to make up a DN.

DNS

The Domain Name System is a service that translates names into IP addresses.

E

ECC

Elliptical curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers.

Endpoint

An endpoint is a URL that enables the API to gain access to resources on a server.

Enrollment

Certificate enrollment refers to the process by which a user requests a digital certificate. The user must submit the request to a certificate authority (CA).

EOBO

A user with an enrollment agent certificate can enroll for a certificate on behalf of another user. This is often used when provisioning technology such as smart cards.

F

Forest

An Active Directory forest (AD forest) is the top most logical container in an Active Directory configuration that contains domains, and objects such as users and computers.

G

Gateway Connector

The Keyfactor Gateway Connector is installed in the customer forest to provide a connection between the on-premise CA and the Azure-hosted, Keyfactor managed Hosted Configuration Portal to provide support for synchronization, enrollment and management of certificates through the Azure-hosted instance of Keyfactor Command for the on-premise CA. It is supported on both Windows and Linux.

H

Host Name

The unique identifier that serves as name of a computer. It is sometimes presented as a fully qualified domain name (e.g. servername.keyexample.com) and sometimes just as a short name (e.g. servername).

Hosted Config Portal

The Keyfactor Hosted Configuration Portal is used to configure connections between on-premise instances of the Keyfactor

Gateway Connector and and on-premise CAs to make them available to Azure-hosted instance of Keyfactor Command.The portal is Azure-hosted and managed by Keyfactor.

Hosted Configuration Portal

The Keyfactor Hosted Configuration Portal is used to configure connections between on-premise instances of the Keyfactor Gateway Connector and and on-premise CAs to make them available to Azure-hosted instance of Keyfactor Command.The portal is Azure-hosted and managed by Keyfactor.

Hostname

The unique identifier that serves as name of a computer. It is sometimes presented as a fully qualified domain name (e.g. servername.keyexample.com) and sometimes just as a short name (e.g. servername).

J

Java Agent

The Java Agent, one of Keyfactor's suite of orchestrators, is used to perform discovery of Java keystores and PEM certificate stores, to inventory discovered stores, and to push certificates out to stores as needed.

Java Keystore

A Java KeyStore (JKS) is a file containing security certificates with matching private keys. They are often used by Java-based applications for authentication and encryption.

JKS

A Java KeyStore (JKS) is a file containing security certificates with matching private keys. They are often used by Java-based applications for authentication and encryption.

K

Key Length

The key size or key length is the number of bits in a key used by a cryptographic algorithm.

Key Pair

In asymmetric cryptography, public keys are used together in a key pair with a private key. The private key is retained by the key's creator while the public key is widely distributed to any user or target needing to interact with the holder of the private key.

Key Size

The key size or key length is the number of bits in a key used by a cryptographic algorithm.

Key Type

The key type identifies the type of key to create when creating a symmetric or asymmetric key. It references the signing algorithm and often key size (e.g. AES-256, RSA-2048, Ed25519).

Keyfactor CA Management Gateway

The Keyfactor CA Management Gateway is made up of the Keyfactor Gateway Connector, installed in the customer forest to provide a connection to the local CA, and the Azure-hosted and Keyfactor managed Hosted Configuration Portal. The solution is used to provide a connection between a customer's on-premise CA and an Azure-hosted instance of Keyfactor Command for synchronization, enrollment, and management of certificates.

Keyfactor Gateway Connector

The Keyfactor Gateway Connector is installed in the customer forest to provide a connection between the on-premise CA and the Azure-hosted, Keyfactor managed Hosted Configuration Portal to provide support for synchronization, enrollment and management of certificates through the Azure-hosted instance of Keyfactor Command for the on-premise CA. It is supported on both Windows and Linux.

Keyfactor Universal Orchestrator

The Keyfactor Universal Orchestrator, one of Keyfactor's suite of orchestrators, is used to interact with Windows servers (a.k.a. IIS certificate stores) and FTP capable devices for certificate management, run SSL discovery and management tasks, and manage synchronization of certificate authorities in remote forests. With the addition of custom extensions, it can run custom jobs to provide certificate management capabilities on a variety of platforms and devices (e.g. F5 devices, NetScaler devices, Amazon Web Services (AWS) resources) and execute tasks outside the standard list of certificate management functions. It runs on either Windows or Linux.

Keystore

A Java KeyStore (JKS) is a file containing security certificates with matching private keys. They are often used by Java-based applications for authentication and encryption.

L

Logical Name

The logical name of a CA is the common name given to the CA at the time it is created. For Microsoft CAs, this name can be seen at the top of the Certificate Authority MMC snap-in. It is part of the FQDN\Logical Name string that is used to refer to CAs when using command-line tools and in some Keyfactor Command configuration settings (e.g. ca2.keyexample.-com\Corp Issuing CA Two).

M

MAC Agent

The MAC Agent, one of Keyfactor's suite of orchestrators, is used to manage certificates on any keychains on the Mac on which the Keyfactor MAC Agent is installed.

Metadata

Metadata provides information about a piece of data. It is used to summarize basic information about data, which can make working with the data easier. In the context of Keyfactor Command, the certificate metadata feature allows you to create custom metadata fields that allow you to tag certificates with tracking information about certificates.

O

Object Identifier

Object identifiers or OIDs are a standardized system for identifying any object, concept, or "thing" with a globally unambiguous persistent name.

OID

Object identifiers or OIDs are a standardized system for identifying any object, concept, or "thing" with a globally unambiguous persistent name.

Orchestrator

Keyfactor orchestrators perform a variety of functions, including managing certificate

stores and SSH key stores.

P

P12

A PFX file (personal information exchange format), also known as a PKCS#12 archive, is a single, password-protected certificate archive that contains both the public and matching private key and, optionally, the certificate chain. It is a common format for Windows servers.

P7B

A PKCS #7 format certificate file is a base64-encoded certificate. Since it's presented in ASCII, you can open it in any text editor. PKCS #7 certificates always begin and end with entries that look something like ---- BEGIN CERTIFICATE---- and ----END CERTIFICATE----. Unlike PEM files, PKCS #7 files can contain only a certificate and its certifiate chain but NOT its private key. Extensions of .p7b or .p7c are usually seen on certificate files of this format.

P7C

A PKCS #7 format certificate file is a base64-encoded certificate. Since it's presented in ASCII, you can open it in any text editor. PKCS #7 certificates always begin and end with entries that look something like ---- BEGIN CERTIFICATE---- and ----END CERTIFICATE----. Unlike PEM files, PKCS #7 files can contain only a certificate and its certifiate chain but NOT its private key. Extensions of .p7b or .p7c are usually seen on certificate files of this format.

Parameter

A parameter or argument is a value that is passed into a function in an application.

PEM

A PEM format certificate file is a base64-encoded certificate. Since it's presented in ASCII, you can open it in any text editor. PEM certificates always begin and end with entries like ---- BEGIN CERTIFICATE---- and ----END CERTIFICATE----. PEM certificates can contain a single certificate or a full certifiate chain and may contain a private key. Usually, extensions of .cer and .crt are certificate files with no private key, .key is a separate private key file, and .pem is both a certificate and private key.

PFX

A PFX file (personal information exchange format), also known as a PKCS#12 archive, is a single, password-protected certificate archive that contains both the public and matching private key and, optionally, the certificate chain. It is a common format for Windows servers.

PKCS #7

A PKCS #7 format certificate file is a base64-encoded certificate. Since it's presented in ASCII, you can open it in any text editor. PKCS #7 certificates always begin and end with entries that look something like ---- BEGIN CERTIFICATE---- and ----END CERTIFICATE----. Unlike PEM files, PKCS #7 files can contain only a certificate and its certifiate chain but NOT its private key. Extensions of .p7b or .p7c are usually seen on certificate files of this format.

PKCS#12

A PFX file (personal information exchange format), also known as a PKCS#12 archive, is a single, password-protected certificate archive that contains both the public and matching private key and, optionally, the certificate chain. It is a common format for Windows servers.

PKI

A public key infrastructure (PKI) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption.

Private Key

Private keys are used in cryptography (symmetric and asymmetric) to encrypt or sign content. In asymmetric cryptography, they are used together in a key pair with a public key. The private or secret key is retained by the key's creator, making it highly secure.

Public Key

In asymmetric cryptography, public keys are used together in a key pair with a private key. The private key is retained by the key's creator while the public key is widely distributed to any user or target needing to interact with the holder of the private key.

Public Key Infrastructure

A public key infrastructure (PKI) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption.

R

Rogue Key

A rogue key, in the context of Keyfactor Command, is an SSH public key that appears in an authorized_keys file on a server managed by the SSH orchestrator without authorization.

Root of Trust

A root of trust (RoT) is a source within a cryptographic system that can always be trusted. It is typically a hardened hardware module. HSMs (hardware security modules) and TPMs (trusted platform modules) are examples of RoTs.

RoT

A root of trust (RoT) is a source within a cryptographic system that can always be trusted. It is typically a hardened hardware module. HSMs (hardware security modules) and TPMs (trusted platform modules) are examples of RoTs.

RPC

Remote procedure call (RPC) allows one program to call a function from a program located on another computer on a network without specifying network details. In the context of Keyfactor Command, RPC errors often indicate Kerberos authentication or delegation issues.

rsyslog

Rsyslog is an open-source software utility used on UNIX and Unix-like computer systems for forwarding log messages in an IP network.

S

SAN

The subject alternative name (SAN) is an extension to the X.509 specification that allows you to specify additional values when enrolling for a digital certificate. A variety of SAN formats are supported, with DNS name being the most common.

server name indication

Server name indication (SNI) is an extension to TLS that provides for including the hostname of the target server in the initial handshake request to allow the server to respond with the correct SSL certificate or allow a proxy to forward the request to the appropriate target.

SMTP

Short for simple mail transfer protocol, SMTP is a protocol for sending email messages between servers.

SNI

Server name indication (SNI) is an extension to TLS that provides for including the hostname of the target server in the initial handshake request to allow the server to respond with the correct SSL certificate or allow a proxy to forward the request to the appropriate target.

SSH

The SSH (secure shell) protocol provides for secure connections between computers. It provides several options for authentication, including public key, and protects the communications with strong encryption.

SSL

TLS (Transport Layer Security) and its predecessor SSL (Secure Sockets Layer) are protocols for establishing authenticated and encrypted links between networked computers.

Subject Alternative Name

The subject alternative name (SAN) is an extension to the X.509 specification that allows you to specify additional values when enrolling for a digital certificate. A variety of SAN formats are supported, with DNS name being the most common.

T

Template

A certificate template defines the policies and rules that a CA uses when a request for a certificate is received.

TLS

TLS (Transport Layer Security) and its predecessor SSL (Secure Sockets Layer) are protocols for establishing authenticated and encrypted links between networked computers.

Trusted CA

A certificate authority in the forest in which Keyfactor Command is installed or in a forest in a two-way trust with the forest in which Keyfactor Command is installed.

U

Untrusted CA

A certificate authority in a forest in a one-way trust with the forest in which Keyfactor Command is installed or in a forest that is untrusted by the forest in which Keyfactor Command is installed. Non-domain-joined standalone CAs also fall into this category.

W

Web API

A set of functions to allow creation of applications. Keyfactor offers the Keyfactor API, which allows third-party software to integrate with the advanced certificate enrollment and management features of Keyfactor Command.

Windows Orchestrator

The Windows Orchestrator, one of Keyfactor's suite of orchestrators, is used to manage synchronization of certificate authorities in remote forests, run SSL discovery and management tasks, and interact with Windows servers as well as F5 devices, NetScaler devices, Amazon Web Services (AWS) resources, and FTP capable devices, for certificate management. In addition, the AnyAgent capability of the Windows Orchestrator allows it to be extended to create custom certificate store types and management capabilities regardless of source platform or location.

Workflow

A workflow is a series of steps necessary to complete a process. In the context of Keyfactor Command, it refers to the workflow builder, which allows you automate event-driven tasks when a certificate is requested or revoked.

X

x.509

In cryptography, X.509 is a standard defining the format of public key certificates. An X.509 certificate contains a public key and an identity (e.g. a host name or an organization or individual name), and is either signed by a certificate authority or self-signed. When a certificate is signed by a trusted certificate authority it can be used to establish trusted secure communications with the owner of the corresponding private key. It can also be used to verify digitally signed documents and emails.

4.0 Copyright Notice