

Keyfactor Command 10.1

Release Notes

Table of Contents

1.0 Introduction	1
2.0 Release Notes	2
2.1 Major Release 10.0 Notes	2
2.1.1 Incremental Release 10.1 Notes	16
2.2 Major Release 9.0 Notes	18
2.2.1 Incremental Release 9.1 Notes	31
2.2.2 Incremental Release 9.2 Notes	34
2.2.3 Incremental Release 9.3 Notes	38
2.2.4 Incremental Release 9.4 Notes	39
2.2.5 Incremental Release 9.5 Notes	41
2.2.6 Incremental Release 9.6 Notes	43
2.2.7 Incremental Release 9.7 Notes	44
2.2.8 Incremental Release 9.8 Notes	45
2.2.9 Incremental Release 9.9 Notes	46
2.2.10 Incremental Release 9.10 Notes	48
2.3 Major Release 8.0 Notes	49
2.3.1 Incremental Release 8.1 Notes	52
2.3.2 Incremental Release 8.2 Notes	55
2.3.3 Incremental Release 8.3 Notes	56
2.3.4 Incremental Release 8.4 Notes	59
2.3.5 Incremental Release 8.5 Notes	60
2.3.6 Incremental Release 8.6 Notes	61
2.3.7 Incremental Release 8.7 Notes	62
3.0 Glossary	64
4.0 Copyright Notice	72

List of Figures

Figure 1: Example Navigation Menu Before Upgrade to 9.0	20
Figure 2: Example Navigation Menu After Upgrade to 9.0	21
Figure 3: New Risk Header	22
Figure 4: Template Level Metadata	23
Figure 5: Navigate Forward and Backwards Through Pages	24
Figure 6: Entry of gMSA Users in the Administrative Users Field	33
Figure 7: Keyfactor Logi License Expiration Alert	36
Figure 8: Keyfactor Logi License Expiration Alert on the Dashboard	36
Figure 9: Keyfactor Logi License Expiration Alert on Report	37
Figure 10: Keyfactor Expired Logi Error Message	37

List of Tables

Table 1: API Change Log	12
Table 2: API Change Log	17
Table 3: Keyfactor Universal Orchestrator vs Windows Orchestrator Capabilities	29
Table 4: API Change Log	30
Table 5: API Change Log	34
Table 6: API Change Log	38
Table 7: API Change Log	39
Table 8: API Change Log	41
Table 9: API Change Log	43
Table 10: API Change Log	45
Table 11: API Change Log	48

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*

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 Release Notes

The Keyfactor Command suite of documentation is released as both major releases, with version numbers ending in zero, and minor releases, with incremental fixes and updates following the major release. When reviewing release notes, be sure to review those for both the minor releases and their corresponding major release.

2.1 Major Release 10.0 Notes

September 2022

We're thrilled to announce Keyfactor Command 10.0, which includes some major new features and updates to improve the user experience, enhance automation, and provide native integration with EJBCA.



Important: The MicrosoftECCurveUpgradeModule may fail due to a pre-v10 issue in which Certificate Request Contents were truncated to 4k characters when saved to the database. If your upgrade fails when the MicrosoftECCurveUpgradeModule is run contact Keyfactor Support to obtain assistance with the scripts that will have to be run to fix this issue.



Tip: We encourage customers to contact their customer success manager to discuss the new features and functionality in Keyfactor Command 10, and to schedule an upgrade. Please refer to the [Keyfactor Command Upgrade Overview](#)¹ for important information about the upgrade process.

Workflow Builder Highlight

Workflows in Keyfactor Command allow for automation and governance of certificate enrollment and revocation. The workflow builder makes it easy to define workflows within the Keyfactor Command Management Portal to automate event-driven tasks when a certificate is requested (including renewals) or revoked. The workflows can be built with multiple steps between the start and end of the operation that offer a simple way to send notifications, submit approvals, and configure end-to-end automation throughout the environment. This provides for operational agility in an intuitive and easy-to-user tool. Supported built-in steps that can be used in the workflow builder include one or more approval steps supporting one or more approvers, calls to REST APIs, calls to PowerShell, sending emails, and updating enrollment requests with changes to the submitted subject or SANs, if needed. Custom steps can also be built to address specific needs. The workflow builder provides an easy-to-use experience to create rich workflows with multiple steps.

¹Embedded links to external documents point to the document on the Keyfactor Client Portal. Access to the portal requires a login. See your administrator or your Keyfactor Client Success representative to obtain a login to the portal.

EJBCA Integration with Keyfactor Command Highlight

EJBCA is a robust and highly scalable certificate authority. Keyfactor Command now natively integrates with EJBCA version 7.8.1 or higher without the need for a gateway, providing a simpler architecture. The Certificate Authorities area of Keyfactor Command now allows an administrator to enter connection information to an EJBCA CA to manage certificates and support enrollment. With native EJBCA integration, Keyfactor Command offers an alternative to Microsoft CAs. EJBCA is a much more scalable CA with options for multiple CAs on a single server and high availability configuration options that the Microsoft CA lacks. It can also handle a much larger number of certificates than the Microsoft CA.

CA Gateway 22.1 required for Keyfactor Command v10 Highlight

Upgrade to AnyGateway 22.1 if using gateways on Keyfactor Command v10.

Expanded Template Functionality

- System-wide settings for enrollment templates have moved from the application settings to the templates page.
- Templates can be configured to set policies for the following at both the template level and the system-wide configuration level:
 - Allow Wildcards
 - Allow Public Key Reuse
 - Enforce RFC 2818 Compliance
 - Supported Key Types
- Added a new configuration tab at both the template level and the system-wide configuration level called "Enrollment Defaults" that allows for defining default values for select certificate subject parts that will auto-populate on the PFX Enrollment and CSR Generation pages.
- "Template RegExes" has been renamed to "Enrollment RegExes". Regular expressions for certificate subject values can be defined at both the template level and the system-wide configuration level.
- Metadata can be configured on a per-template basis to control which fields are shown during enrollment and what default values they have.
- 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.
 - 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.
- During the upgrade process Keyfactor Command prevents duplicate template records from being inserted into the database. Duplicate templates could be found if there are templates in different forests with the same

name. If you receive an error message during upgrade, contact Keyfactor Support. We will be able to support you through the process of resolving the issue and completing the upgrade. See the [Keyfactor Command Upgrade Overview](#) for more information.

Keyfactor API Endpoints

The Keyfactor API now has endpoints for most of the functionality found in the product. See the [API Endpoint Change Log on page 12](#) for information on new and updated API endpoints.

Updates Changes & Improvements Fixes Deprecated Future

Changes & Improvements Changes & Improvements

- **CARecordID Replaces CARequestID**

The field CARecordID has been added and the field CARequestID has been removed.

- **Forest has been Renamed *Configuration Tenant***

- To broaden Keyfactor Command's compatibility with certificate authorities, the Microsoft-centric term "forest" has been renamed to "configuration tenant". For EJBCA, there should be one configuration tenant per EJBCA server install. For Microsoft, there should be one per forest. Note that configuration tenants cannot be mixed, so Microsoft and EJBCA CAs cannot exist on the same configuration tenant.
- Added the ability to search templates by configuration forest and key type. The option to search by forest has been retained for backwards compatibility.

- **SQL Server Connection over SSL**

As of Keyfactor Command version 10.0, by default Keyfactor Command connects to SQL using an encrypted connection using an SSL certificate configured on your SQL server. Customers should acquire and install an SSL certificate for the SQL server before upgrading to Keyfactor Command 10.0 (see *Using SSL to Connect to SQL Server* in the *Keyfactor Command Server Installation Guide*). If you would prefer not to use an encrypted channel for your connection to SQL, see *Configurable SQL Connection Strings*.

- **SQL Encryption Key Backup**

When Keyfactor Command is installed, the option is presented to make a backup of the SQL database master key (DMK). In previous versions of Keyfactor Command, this option backed up the service master key (SMK) instead. For more information about how Keyfactor Command uses the DMK and SMK, see *SQL Encryption Key Backup* in the *Keyfactor Command Reference Guide*.

- **SQL Server 2022 Compatibility**

Keyfactor Command is compatible with SQL Server 2022.

- **Certificate Requests**

- The Certificate Requests page is now sorted in descending order by submission date by default. This has been done to cause the more recent requests to appear at the top of the page.
- The Certificate Requests page is now separated into tabs for pending, external validation, and denied/-failed certificate requests.

- The Denied/Failed tab on the Certificate Requests page now includes only certificate requests denied through Keyfactor Command (see *Viewing Certificate Requests* in the *Keyfactor Command Reference Guide*).
- The Revoked view filter has been removed from the Certificate Requests page since the expectation is that Keyfactor Command workflows will be used for enrollments and the history can be viewed as part of that (see *Workflow Instances* in the *Keyfactor Command Reference Guide*).
- **Alerts**
 - When an alert is copied, " - Copy" is appended to the display name to prevent alert display names being duplicated.
 - To aid in clarity, changed the wording on templates when configuring alerts from "None" to "All Templates".
- **SMTP Application Settings**

When making changes to the SMTP configuration, the test email can be sent without saving the configuration changes.
- **Certificate Authorities**
 - Added an option to delegate enrollment requests to the Authorization Methods tab. This is in addition to the option to delegate management functions. This allows Keyfactor Command to delegate the authenticated user's credentials to the CA during enrollment to provide end-to-end authentication without unpacking the credentials at the Keyfactor Command layer. If this is not enabled the "Allowed Requesters" will be used instead. Please see the *Certificate Authority Operations: Adding or Modifying a CA Record Authorization Methods Tab* in the *Keyfactor Command Reference Guide* for more information.
 - When configuring a new certificate authority in the Management Portal, there is now an option to test the connection to the CA before saving the configuration, and CAs will be tested and must be verified and valid to be saved.
 - Updated the CA synchronization so that it logs a message if it could not chain a certificate up to a CA in the system instead of throwing an error.
 - Added a new application setting, *CA Sync Consecutive Error Limit*, which controls the number of times an error can occur before the synchronization job is abandoned.
 - There is no longer the need to register offline CAs, as the root/policy CA certificates can be imported from the issuing CA sync without them. Additionally, the new CA validation makes it impossible to save offline CAs.
- **Certificate Stores**
 - Added the ability for users with only container-level permission to create and use certificate stores in the container, including certificate store types that have a server component. Users will not be able to access certificate stores outside of the containers they have permissions to manage. (Previously, users needed to have Certificate Store Manage permissions in order to change client machine credentials as certificate store servers was shared across all certificate stores with the same type and server name. Now, certificate store servers are partitioned by container.)
 - Added the ability to import PEM certificates that have comments in them when doing an inventory of an

F5 REST certificate store.

- On the Discover tab the label for "Approve" has been changed to "Manage" for clarity.

- **Dashboard and Reporting**

- The Risk header can now be hidden via security role permissions.
- Some cosmetic updates have been made to the Risk header.
- The Collections Dashboard widget is limited to only displaying the first 25 collections configured to be on the dashboard. It sorts the list alphabetically.
- The stale date is visible in the CRL Monitoring Dashboard widget as a new column and is called "Next Publish by Date". The stale date should not be used for calculating the status of the CRL. A stale CRL is a valid state and not something that needs to be warned on. If a CRL is stale, the system will check how far it is from expiration and if it is within the warning period it will have a status of "Warning" or "Valid" if outside the warning period.
- Keyfactor Command v10 ships with a newer version of Logi Analytics (v14) which drives the Reports and Dashboards. This version provides a number of improvements and fixes some security vulnerabilities.
- CRL dates are always shown in UTC on the Revocation Monitoring Dashboard.
- A new report—SSH Key Usage—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 Risk header on the dashboard has been updated to avoid awkward text formatting and scrolling when resizing the page.
- The Risk header titles have been updated for consistency and clarity. "Expiring" titles are now all in the "Expiring" tense and consistent with each other. "Weak Keys" has been renamed to "Certs with Weak Keys".
- The *Certificate Count by Template* has been updated so that it takes the same parameters as the *Certificate Count per User by Template* report for consistency. This included changing the "Evaluation Date" to "Start Date" and adding an "End Date" field.
- All reports have been updated to reference UTC time to avoid confusion about which time zone is being applied.
- The *PKI Status for Collection* report has been updated to provide clarity on the meaning of "Total Active Certificates".

- **Agent, Orchestrators, and Orchestrator Management**

- The Orchestrator Details dialog has been updated to show more information about the orchestrator:
 - Legacy Thumbprint
 - Current Thumbprint
 - Last Thumbprint Used
 - Last Register Status
 - Certificate Rotation Status
- The Job History now shows the time the job completed.

- The default value for the *Registration Handler Timeout (seconds)* application setting has been extended to 90 seconds for new implementations only. Keyfactor recommends any existing customers using or planning to use custom registration handlers consider extending this timeout to at least 60 seconds.
- SSL scan job parts are now grabbed more deterministically to help keep the job assignments more predictable. For more information, see *SSL Network Operations* in the *Keyfactor Command Reference Guide*.
- The SSL Scan Now option now allows you to select whether to start a discovery job, a monitoring job, or both (see *SSL Network Operations: Initiating a Manual Scan* in the *Keyfactor Command Reference Guide*).
- The Keyfactor Universal Orchestrator now does CRL checking when contacting Keyfactor Command over an encrypted channel (when you configure the orchestrator with a URL referencing https) both when certificate authentication is used and when basic authentication is used. Previously this was only done when certificate authentication was used. If you attempt to connect your orchestrator using SSL and do not have a valid CRL available to the orchestrator, you will get an error message similar to the following:

The remote certificate is invalid because of errors in the certificate chain:
RevocationStatusUnknown, OfflineRevocation
For troubleshooting information, see *Troubleshooting* in the *Keyfactor Orchestrators Installation and Configuration Guide*.

- **Reenrollment**

A certificate authority and template can now be specified when scheduling a reenrollment job.

- **Certificate Metadata**

- A certificate metadata field now cannot be deleted if it is in use in a certificate collection definition.
- When creating a new certificate metadata type, different fields will be displayed depending on the value selected in the Data Type dropdown field. For more information, see *Metadata Field Operations: Adding or Modifying a Metadata Field* in the *Keyfactor Command Reference Guide*.

- **Security Identities and Roles**

- A search bar has been added to search for the collections and containers in the security roles dialog.
- Improvements were made to performance when loading a large number of security roles in the portal.
- When copying a security role, a new disclaimer will appear to advise the user that copying a security role will also assign the new role to all the same security identities as the target role.
- The security roles dialog has been updated to be a tabbed dialog box.

- **UI Changes**

- Some edit dialogs have been changed to use sliding panels to accommodate two different views within the same page rather than pop up windows.
- Added scroll bars to the certificate details pop ups.
- Added the ability to copy data from grid information (e.g. SSL location information when expanding the certificate locations). Information in a grid field can be **copied** to the clipboard by highlighting text in a grid field and clicking **Ctrl+C**.
- Performance improvements have been made in loading large data sets in the Management Portal results grids.

- **System Alerts**

The alerts that are displayed in the UI for notification of things like failed orchestrator jobs have been renamed "System Alerts" for clarity.

- **Logging**

- The Keyfactor API and Orchestrator API logs on the Keyfactor Command server and the log for the Keyfactor Universal Orchestrator 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 and is the same for all log messages for the given request until the request completes.
- Lowered the logging level for the user's authentication from Info to Trace to avoid cluttering log files.

- **Mac Auto-Enrollment**

The Mac auto-enrollment process now identifies all the CAs that have the auto-enrollment template(s) available for enrollment and makes a determination as to whether the enrolling user has permissions to enroll on a CA and whether that CA is online before submitting a request to the CA. Previously, a CA was selected randomly among the CAs that had the template(s) available without regard to the user's permissions on the CA or the availability of the CA.

- **Auditing**

Orchestrator reset, approval, disapproval will now properly audit under the new 'Orchestrator' category and their respective operation.

- **Installation**

- On installation, Keyfactor Command creates an initial record in the DatabaseUpgradeLog table that indicates the exact version of Keyfactor Command that created the database. This can be helpful for troubleshooting.
- If you are upgrading from an older version of Keyfactor Command the installation directory changed, as of Keyfactor Command v9, to C:\Program Files\Keyfactor. Move any scripts or files that are held in the old directory structure to the new location.

- **Policy Modules**

The policy modules have been migrated to leverage .NET Core.

- **Custom Registration Handlers**

A custom registration handler can now be designed to enroll against a specific certificate authority and template combination. The registration handler chooses which combination to use. If no combination is requested by the registration handler, then the certificate authority and template from the application settings are used. For more information, see *Register a Client Certificate Renewal Extension* in the *Keyfactor Orchestrators Installation and Configuration Guide*.

- **Application-Level Encryption Certificate Thumbprint**

The reference thumbprint for the application-level encryption certificate, if configured, is now stored in the registry on the Keyfactor Command server(s) instead of the SQL database to provide a further level of separation from SQL.

- **Keyfactor Command**

- Revocation Monitoring Dashboard panel no longer stalls as perpetually "Loading" for OCSP endpoints.
- Certificate subjects for PFX enrollment via the legacy API have been fixed so they can be formatted according to the API.CertEnroll.Pkcs12CertificateSubjectFormat app setting.
- Fixed an issue when parsing the CSR so that CSRs containing IP or Email SANs no longer cause excess warnings in CA syncs, and IP and Email SANs show up in the pending request details.
- Fixed an issue where syncing external certificates would cause an "object reference not set to an instance of an object" error.
- Fixed an issue with revocation monitoring alerts reporting time in the local time zone instead of UTC. Emails now have the time in UTC. The time is explicitly labeled UTC.
- Fixed an issue where special characters like apostrophes would appear HTML-encoded in the collection name.
- Fixed an issue in certificate enrollment where SANs for IPv4 and IPv6 addresses were not being validated properly.
- Fixed an issue where an untrusted certificate chain would prevent the certificate details dialog from opening. An error will still occur if a certificate chain is attempted to be downloaded and the chain build fails, but will not prevent the dialog from opening.
- Fixed an issue where the Identity Audit table wasn't populating from the Certificate Search page.
- Fixed an issue where unscheduling an orchestrator management job failed to cancel the previously staged job.
- Fixed an issue in enrollment where the subject incorrectly added an extra quotation mark when the subject format default was set in certain ways.
- Fixed an issue where SQL would timeout when deleting over 1,000 certificates from the Keyfactor Command Management Portal.
- Fixed an issue where the gateway configured to run as a domain service account and running on the same server as Keyfactor Command caused RPC errors.
- Fixed an issue where the gateway configured to run as a domain service account caused RPC errors.
- Lowered the logging level for the user's authentication from Info to Trace to avoid cluttering log files.
- Fixed an issue where PEM files with headers could not convert to DER with BouncyCastle 1.9.0 and Keyfactor.PKI.dll v4.x.
- Fixed an issue for certificate store types with the *Advanced>Supports Custom Alias* setting set to **Forbidden**, so that the custom alias should only show on the Add to Certificate Store page when the **Overwrite** checkbox is checked.
- Fixed an issue where using *Delete All* on the Certificate Search page would not delete revoked and expired certificates.
- Fixed an issue in the *Issued Certificates Per Certificate Authority* report that was caused by having templates with the same name in separate forests.

- Fixed an issue with certificate store inventories where a certificate store that had completed an inventory scheduled for an interval would fail if it then was scheduled to run immediately.
- **Keyfactor Agents and Orchestrators**
 - Fixed an issue so that CRLs are now checked regardless of the authentication method being used by the orchestrator.
 - Fixed an issue where permissions were not being set correctly on the appsettings.json and orchestratorsettings.json file that prevented the files being read or updated if the service was running as the Network Service.
 - Fixed an issue where a misconfigured orchestrator using certificate authentication would renew certificate multiple times.
 - Fixed an issue where an orchestrator's registration session was still allowed even when denied by a registration handler and added an auditing event for the orchestrator session registration.

Deprecation Deprecated

- **Windows Server 2016**

As of Keyfactor Command version 10.0, Windows Server 2016 is no longer supported.

- **Deprecated Certificate Search Fields**

The *KeyfactorRequestId*, *RequestResolutionDate*, and *CARequestId* certificate search fields parsers are deprecated due to native EJBCA support in Keyfactor Command as of v10. Any certificate collections using them must be changed before upgrading to v10+.

- **Archive Key on Templates**

As of Keyfactor Command v10 we no longer support enrolling for certificates that have the archive key option turned on in the template to enable the certificate to store the private key for the certificate in the CA. Attempting to enroll using a template that has this option turned on will result in the following error: *"The certificate request failed with the reason 'The request is missing a required private key for archival by the server.'"*

- **CA Policy module v7.0**

You will need to upgrade the CA Policy module to v7.1 before running the Keyfactor Command 10.0 upgrade.

- **Reports**

The Resolution Date field has been removed from the *Certificate Count by User By Template* report.

Future Changes Future

- **Microsoft .NET Runtime version 3.1**

By the end of 2022, Microsoft will no longer be supporting .NET Runtime version 3.1. Currently both Microsoft .NET Runtime version 6.0 (x64) and version 3.1 are supported by Keyfactor.

If you wish to continue using older versions of the Universal Orchestrator but the newer .NET Runtime, you can update the .NET Runtime version on the orchestrator server without needing to reinstall the orchestrator (see *System Requirements* in the *Keyfactor Orchestrators Installation and Configuration Guide*).

- **Intune Portal/SCEP Change-over**

Intune portal change-over will be required for SCEP when the old APIs are shut off by Microsoft's deprecation of ADAL at the end of the year.

Known Issues/Limitations Known Issues

- When editing a template, changes will be lost without warning if the "Save" button isn't clicked before navigating away. This is slated to be fixed in a future release.
- When editing a template, the checkboxes for the Metadata, Enrollment RegExes, and Enrollment Defaults tabs do not allow for multi-edit. This will be fixed in a future release.
- When copying a security role, the identities associated with the security role will also be copied.
- The Condition Variable field in a step of the workflow builder accepts input values that are not valid. Only "true", "false" and variables that will evaluate to "true" or "false" are supported.
- For most certificate stores, the "Client Machine" is the machine where the store is located, and the "Orchestrator" drop-down selects the orchestrator/agent. However, for the Java Keystore, the "Client Machine" field is actually the agent and there is no orchestrator dropdown. This will be made more clear in a future release.
- When creating a new certificate store type, the "Depends On Other" option may not be available when creating the parameter. The workaround is to save the certificate store type and then use edit to update the parameter.
- Using the browser back button after generating a report creates a nested instance of Keyfactor Command in Firefox.
- Occasionally, removing a widget from the Dashboard causes the dashboard to hang. Refreshing the browser should resolve this issue.
- The `-ne` operator in certificate search does not return NULL results for Boolean metadata fields. Search for `'Metadata' -ne "False" OR 'Metadata' -eq Null` to get the desired results.
- The *Certificate Count Grouped by Single Metadata Field* report falsely reports no results if using the default metadata value. This will be fixed in a future release.
- The *PKI Status for Collection* report click throughs do not retain the *Include Unknown* certificates option when clicking through to the certificate search results page. This will be fixed in a future release.
- SMTP Sender information isn't correctly saved by the Configuration Wizard. This will be fixed in a future release. It is recommended to check the SMTP Configuration page upon upgrade.
- Alert tests do not show certificate information if there is no recipient configured to receive an email even if **Send Alerts** is not selected. This will be fixed in a future release. The workaround is to add an email recipient when running the tests.
- Adding multiple enrollment fields at the same time is only saving the last field entered. This will be fixed in a future release. Workaround is to add and save each enrollment field one at a time.
- The *Certificates in Collection* report falsely reports ECC certificates with a certificate state of *Denied* rather than *Active*, revoked certificates with a certificate state of *Active* rather than *Revoked*, and shows an incorrectly

shows a revocation reason of *Unspecified* for certificates with an *Active* certificate state. This will be fixed in a future release.

API Endpoint Change Log

API

The following changes were made to the API endpoints. Please review these carefully if you have implemented any integration using these endpoints.

Table 1: API Change Log

Endpoint	Methods	Action	Notes
/Agents/{id}	GET	Add	
/Agents/Reset	POST	Add	
/AgentBlueprint	GET	Add	
/AgentBlueprint/{id}	GET, DELETE	Add	
/AgentBlueprint/{id}/Jobs	GET	Add	
/AgentBlueprint/{id}/Stores	GET	Add	
/AgentBluePrint/ApplyBlueprint	POST	Add	
/AgentBluePrint/GenerateBluePrint	POST	Add	
/Alerts/Denied	GET, PUT, POST	Add	
/Alerts/Denied/{id}	GET, DELETE	Add	
/Alerts/Expiration	GET, PUT, POST	Add	
/Alerts/Expiration/{id}	GET, DELETE	Add	
/Alerts/Expiration/Schedule	GET, PUT	Add	
/Alerts/Expiration/Test	POST	Add	
/Alerts/Expiration/TestAll	POST	Add	
/Alerts/IssuedAlerts	GET, PUT, POST	Add	
/Alerts/IssuedAlerts/{id}	GET, DELETE	Add	
/Alerts/Issued/Schedule	GET, PUT	Add	

Endpoint	Methods	Action	Notes
/Alerts/KeyRotation	GET, PUT, POST	Add	
/Alerts/KeyRotation/{id}	GET, DELETE	Add	
/Alerts/KeyRotation/Schedule	GET, PUT	Add	
/Alerts/KeyRotation/Test	POST	Add	
/Alerts/KeyRotation/TestAll	POST	Add	
/Alerts/Pending	GET, PUT, POST	Add	
/Alerts/Pending/{id}	GET, DELETE	Add	
/Alerts/Pending/Schedule	GET, PUT	Add	
/Alerts/Pending/Test	POST	Add	
/Alerts/Pending/Test/{id}	POST	Add	
/CertificateAuthorities	GET	Update	Schedules are now included in the results.
/CertificateAuthorities	POST	Update	Ability to turn off schedules, sessions are abandoned properly, and threshold monitoring schedule is included.
/CertificateAuthorities/{id}	PUT	Update	Ability to turn off schedules, sessions are abandoned properly, and threshold monitoring schedule is included.
/CertificateAuthorities/{id}	DELETE	Update	Deletion is now prevented if schedules are associated.
/CertificateCollections	POST	Update	Query parameter no longer needed when a valid CopyFromId is provided.
/CertificateCollections/{id}/Permissions	POST	Deprecated	Replaced by /Security/Roles/{id}/Permissions/Collection.
/Certificates/Analyze	POST	Add	

Endpoint	Methods	Action	Notes
/Certificates/IdentityAudit/{id}	GET	Add	
/CertificateStoreContainers	POST	Add	
/CertificateStoreContainers/{id}	PUT, DELETE	Add	
/CertificateStores/Server	GET, POST, PUT	To Be Deprec- ated	Server usernames, server passwords, and the UseSSL flag are managed by the /CertificateStores API endpoints directly as JobProperties using the Properties parameter, replacing the deprecated /CertificateStores/Server API endpoints.
/CertificateStores	GET, POST, PUT	Updated	Server usernames, server passwords, and the UseSSL flag are managed by the /CertificateStores API endpoints directly as JobProperties using the Properties parameter, replacing the deprecated /CertificateStores/Server API endpoints.
/Enrollment/PFX (v2)	POST	Add	
/Enrollment/Settings/{id}	GET	Add	
/JobTypes/Custom	POST	Update	DefaultValue property is no longer required, validation is now performed on the JobTypeFields/DefaultValue property, validation prevents names containing spaces.
/JobTypes/Custom/{id}	DELETE	Update	Includes validation so that deletion is prevented if at least one associated approved orchestrator implements the capability.
/MacEnrollment	GET, PUT	Add	
/Monitoring/Revocation	GET, POST	Update	Renamed from /Work-flow/RevocationMonitoring
/Monitoring/Revocation/{id}	GET, PUT, DELETE	Update	Renamed from /Work-flow/RevocationMonitoring/{id}

Endpoint	Methods	Action	Notes
/Monitoring/Revocation/Test	POST	Add	
/Monitoring/Revocation/TestAll	POST	Add	
/Orchestrators/JobHistory	GET	Update	Added JobId field.
/Orchestrators/ScheduledJobs	GET	Add	
/OrchestratorJobs/Reschedule	POST	Add	
/OrchestratorJobs/Unschedule	POST	Add	
/OrchestratorJobs/Acknowledge	POST	Add	
/Security/Identities/{id}	GET	Add	
/Security/Roles/{id}/Identities	GET, POST	Add	
/Security/Roles/{id}/Containers	GET, POST	Add	
/Security/Roles/{id}/Copy	POST	Add	
/Security/Roles/{id}/Permissions	GET	Add	
/Security/Roles/{id}/Permissions/Global	GET, POST, PUT	Add	
/Security/Roles/{id}/Permissions/Collections	GET, POST, PUT	Add	Replaced the /CertificateCollections/{id}/Permissions endpoint functionality.
/Security/Roles/{id}/Permissions/Containers	GET, POST, PUT	Add	Returns only containers that have a permission set for the selected security role.
/SMTP	GET, PUT	Add	
/SMTP/Test	POST	Add	
/Templates	GET, PUT	Update	Includes template-specific policy information.
/Templates/{id}	GET	Update	Includes template defaults.
/Templates/Settings	GET, PUT	Update	Includes global template policies.

Endpoint	Methods	Action	Notes
/Template/SubjectParts	GET	Add	
/Templates/Global/Settings	GET, PUT	Add	
/Templates/Import	POST	Add	
/Workflow/Certificates/Pending	GET	Update	Now supports query fields of Requester and RequestType.
/Workflow/Definitions/Steps/{extensionName}	GET	Add	
/Workflow/Definitions/{definitionId}	GET, PUT, DELETE	Add	
/Workflow/Definitions	GET, POST	Add	
/Workflow/Definitions/Steps	GET	Add	
/Workflow/Definitions/Types	GET	Add	
/Workflow/Definitions/{definitionId}/Steps	PUT	Add	
/Workflow/Definitions/{definitionId}/Publish	POST	Add	
/Workflow/Instances/{instanceId}	GET, DELETE	Add	
/Workflow/Instances	GET	Add	
/Workflow/Instances/My	GET	Add	
/Workflow/Instances/AssignedToMe	GET	Add	
/Workflow/Instances/{instanceId}/Stop	POST	Add	
/Workflow/Instances/{instanceId}/Signals	POST	Add	
/Workflow/Instances/{instanceId}/Restart	POST	Add	

2.1.1 Incremental Release 10.1 Notes

November 2022



Note: Keyfactor Command 10.1 is a minor release with incremental fixes and updates following the Keyfactor Command 10 major release. For more details on new features, improvements, and known limitations in Keyfactor Command 10.0, please review the [Major Release 10.0 Notes on page 2](#).

Updates and Fixes

- Update: All timer service jobs have consistent start and stop log messages in both the file and Windows Event Viewer
- Update: A PAM provider can be used directly by the Universal Orchestrator, such that the server does not retrieve, and does not have access to, the credential
- Update: Ed448 and Ed25519 keys are now supported for certificate enrollment, policy, import and search
- Update: Improved support for the Timer Service - including a job locking mechanism - in High-Availability implementations
- Fix: GET /SSL is returning duplicate info in some instances with endpoints sharing a common chain
- Fix: Certificate store Discovery jobs could not be executed
- Fix: AnyGateway was declaring all requests as new instead of renew or reissue
- Fix: The Sender Account was not populated during the configuration process
- Fix: SSL discovery scan job errors for entries with a null display name

Policy Module Updates

- Migrated the Policy Modules to .NET Core 6.
- Updated the Policy Module to create a Windows Event Log entry when the current license is within 60 days of expiration.
- Updated the Policy Module installer to include the EnterpriseLite, SubjectFormat and SCEPRequester modules.
- Updated the Policy Handler Configuration so that changes no longer require the ADCS service to be restarted.

API Endpoint Change Log

The following changes were made to the API endpoints. Please review these carefully if you have implemented any integration using these endpoints.

Table 2: API Change Log

Endpoint	Methods	Action	Notes
Template	PUT, GET, GETID	Update	Ed448 and Ed25519 keys are now supported for certificate enrollment, policy, import and search
Templates Settings	PUT, GET	Update	Ed448 and Ed25519 keys are now supported for certificate enrollment, policy, import and search

2.2 Major Release 9.0 Notes

August 2021

Release Highlights

We're thrilled to announce Keyfactor Command 9.0, which includes several new features and updates to improve the user experience, deployment flexibility, and risk awareness.

Highlights from the Keyfactor Command 9.0 release are listed here. More details are available in the New Features, and Updates and Improvements sections further down.



Important: There have been several UI updates to the navigation menu, drop-downs, and application settings. Thoroughly review these changes in the New Features section.

UI Enhancements Highlight

- **What problem does it solve?**

The Keyfactor Command interface should be easy to navigate and use.

- **How does it work?**

As we continue to improve the Keyfactor Command interface, we've added updates to the navigation menu, application settings, and dialogues, as well as an updated color scheme.

- **What's the benefit?**

Ease of Use: The Keyfactor Command interface is more intuitive for new and experienced users alike.

New Risk Header Highlight

- **What problem does it solve?**

PKI administrators and application owners want to easily identify risks and upcoming expirations for the certificates they have access to.

- **How does it work?**

A new fixed header above the dashboard displays expiring, weak, and revoked certificates for an at-a-glance view of risks.

- **What's the benefit?**

Risk Mitigation: Enables administrators to quickly identify the state of their certificates.

New Universal Orchestrator Orchestrator

- **What problem does it solve?**

The current Windows Orchestrator is only able to run on Windows systems.

- **How does it work?**

The new Keyfactor Universal Orchestrator runs on .NET Core 3.1, which allows it to be installed on servers/instances running either Linux or Windows.

- **What's the benefit?**

Flexibility: Enables customers to deploy orchestrators in cross-platform environments.

New Remote CA Gateway CA Gateway

- **What problem does it solve?**

Certain customers are unable to use Keyfactor PKI as-a-Service due to security or regulatory requirements, but they'd still like to leverage a SaaS-based solution for certificate management.

- **How does it work?**

The new Remote CA Gateway securely connects on-premise private PKI – Microsoft ADCS or PrimeKey EJBCA – to the Keyfactor Cloud. This allows customers to leverage Keyfactor Command as a Service (SaaS) while keeping their PKI within their datacenter.

- **What's the benefit?**

Cloud: On-premise customers now have more options to deploy Keyfactor in a SaaS model – while keeping their PKI in-house, if required.

Support for TLS 1.3 SSL/TLS

- **What problem does it solve?**

Before Keyfactor Command 9.0, Keyfactor Command did not support SSL/TLS scanning on endpoints using TLS 1.3.

- **How does it work?**

The Keyfactor Universal Orchestrator supports SSL/TLS scanning on endpoints using TLS 1.3.

- **What's the benefit?**

Increased Visibility: Organizations will have improved visibility over certificates.

Template-Level Metadata Highlight

- **What problem does it solve?**

Before Keyfactor Command 9.0, certificate metadata could only be applied system wide.

- **How does it work?**

Now administrators can apply metadata on a per-template basis, which will override system-wide settings for that specific template.

- **What's the benefit?**

Control: This gives administrators more granular control for metadata in certificate enrollment.

Ecosystem Updates

While separate from the Keyfactor Command 9.0 release, we've recently introduced several new integrations in GitHub to support more certificate authorities, applications, and services.

These include:

- Google Cloud CA Service: A new AnyCA Gateway implementation supports discovery and automation of certificates issued by Certificate Authority Service (CAS).
- Google Cloud IoT Core: The IoT Issued Alert Handler publishes device certificates to various cloud providers, including Google Cloud, Azure, and AWS.
- GoDaddy: The GoDaddy CA Gateway enables enrollment, renewal, re-issuance, and revocation of certificates via Keyfactor Command.
- Sectigo Certificate Manager: The Sectigo CA Gateway enables full lifecycle management of certificate issued by Sectigo via Keyfactor Command.
- Kubernetes: A proxy signs certificate-signing requests (CSRs) through Keyfactor via the Kubernetes CSR signer API.
- Azure Key Vault: Allows customers to inventory and manage certificates within their Azure Key Vault instances.

More information and developer resources can be found in the [Keyfactor GitHub](#).

New Features

UI Enhancements



Tip: We encourage existing Keyfactor Command customers to watch the [Keyfactor Command 9.0 UI Walk-through](#) demo and read through the detailed UI changes listed below before upgrading to Keyfactor Command 9.

Keyfactor Command 9.0 includes significant updates to the UI, as well as several changes to the main navigation menu and drop-downs with a focus on improved usability. Please continue reading to review and understand these changes.

Previously, the navigation menu looked like the example below:

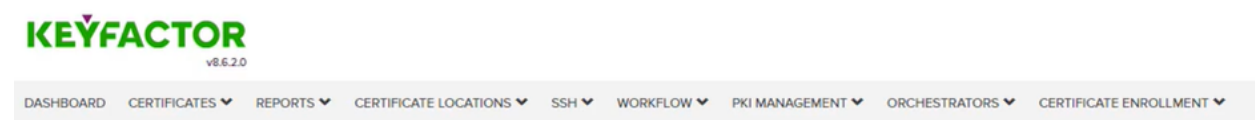


Figure 1: Example Navigation Menu Before Upgrade to 9.0

In Keyfactor Command 9.0, the navigation menu is more concise and user-centric:

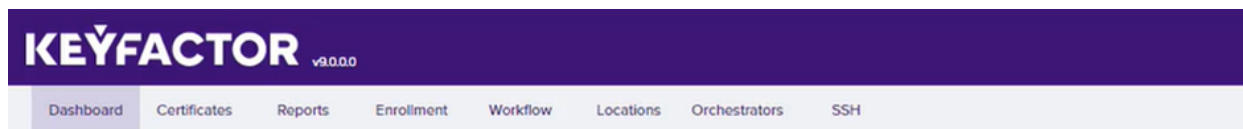


Figure 2: Example Navigation Menu After Upgrade to 9.0

Certificates drop-down

- Add Certificate: The Add Certificate selection is now located in the Certificates tab. Previously, it was accessed via the Certificate Locations tab.

Enrollment drop-down

- Certificate Requests: This option is now found in the new Enrollment tab, rather than the Workflow tab.

Workflow drop-down

- Revocation Monitoring: This option is now located in the Workflow tab. Previously, it was located in the PKI Management tab.
- Expiration: This selection was previously named Expiration Alerts.
- Pending Request: This selection was previously named Pending Request Alerts.
- Issued Request: This selection was previously named Issued Request Alerts.
- Denied Request: This selection was previously named Denied Request Alerts.
- Key Rotation: This selection was previously named Key Rotation Alerts.

Locations drop-down

- Certificate Stores: You will now access the Certificate Stores selection from the new Locations tab. Previously, it was accessed via the Certificate Locations tab.
- Certificate Authorities and Certificate Templates: These menu options are now found in the new Locations. Previously, they were located in the PKI Management tab.
- SSL Discovery: This selection is now located in the Locations tab. It was previously located in the Certificate Locations drop-down.

System Settings menu

- Certificate Store Types: You will now access the Certificate Store Types from the System Settings at the top-right of the screen. It was previously under Certificate Locations.

Certificate Search

- There is a new "ends with" operator. For example:
`CN -endswith "keyexample.com"`
- A new advanced search option has been added of %ME-AN%. This does a search for account name without domain. For example, the following search in certificate search:
`NetBIOSRequester -contains "%ME-AN%"`

Would return certificates requested by the current user as KEYEXAMPLE\jsmith and KEYOTHER\jsmith (assuming the current user is logged in with username jsmith in some domain).

New Risk Header

A "Risk Header" has been added to the Dashboard, which displays relevant information for certificates the user has permissions to. This includes a count of all active certificates, upcoming expirations, expired and revoked certificates, and weak keys (as seen below).

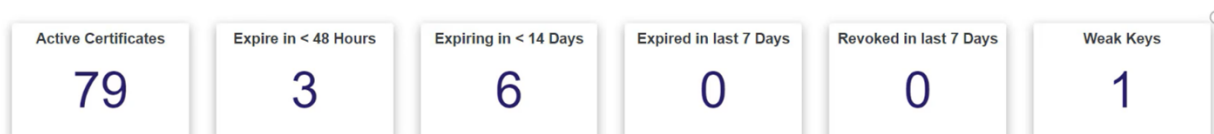


Figure 3: New Risk Header



Note: The new Risk Header is intended to provide an at-a-glance view of key metrics. Unlike items within the dashboard below it, the header cannot be moved or customized.

New Universal Orchestrator

Now available in Keyfactor Command 9.0, the new Keyfactor Universal Orchestrator can perform many of the same functions as the legacy Windows Orchestrator, such as IIS, SSL, FTP and CA management (we will continue to expand its functionality). However, unlike the legacy Windows Orchestrator, the new Keyfactor Universal Orchestrator is able to run on both Windows and Linux servers.

The purpose of orchestrators is to perform SSL scans, manage certificate stores (both Java Key Stores and Windows Certificate Stores), run custom certificate management jobs, inventory CAs, and collect logs to be viewed in the Keyfactor Command Console.

Please review the [Deprecation on page 27](#) section for more information about the eventual deprecation of the legacy Windows Orchestrator. Refer to the *Keyfactor Orchestrators Installation and Configuration Guide* for more information on the new Keyfactor Universal Orchestrator.

New Remote CA Gateway

Before Keyfactor Command 9.0, customers had the option to deploy Keyfactor Command on-premise or hosted in the cloud with a fully managed private PKI as a Service (PKIaaS). Now customers have the additional option to keep their PKI on-premise while leveraging Keyfactor Command in the cloud.

The Keyfactor Remote CA Gateway is the connection point between the new Keyfactor Command as-a-Service deployment model (aka Certificate Lifecycle Automation as a Service or CLaaS) and a customer's on-premise PKI behind their firewall.

The Remote CA Gateway synchronizes in real-time to provide full visibility and governance over the inventory, enrollment, issuance, revocation and renewal of certificates from your on premise CA, requiring just a single, secure API connection on port 443 back to the Keyfactor Command Cloud.

Template-level Metadata

Certificate metadata fields can now be defined on a per-template basis. Before Keyfactor Command 9.0, metadata fields could only be defined as a system-wide setting.

This allows administrators to apply required, hidden or optional settings to a metadata field on a per-template basis so that only certain metadata fields will appear on certain templates.

System-wide settings for metadata fields can be overridden, so customers can choose which fields are displayed, during enrollment for a certificate, based on the template the user selects when enrolling.

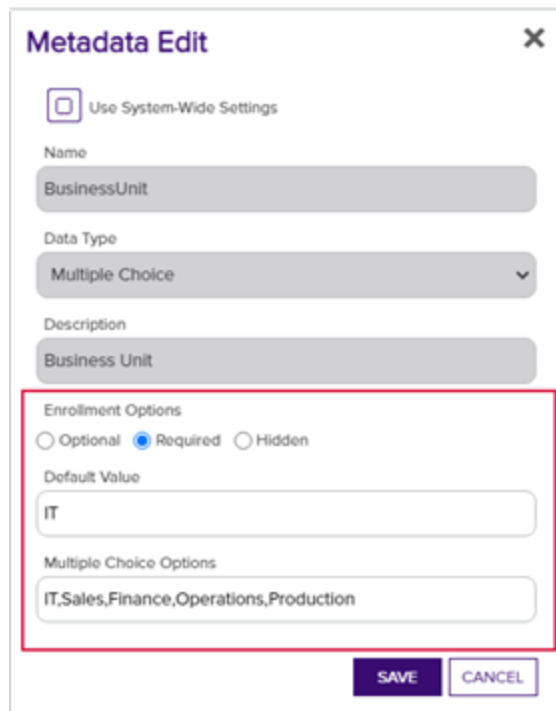


Figure 4: Template Level Metadata

Documentation Structure Updates

Next and Previous buttons have been added to the button row at the top of each page that allow you to navigate through the pages in the documentation in order.

The mini table of contents has been updated to only display by default on pages that contain subpages. This TOC displays—with links—any pages that appear below the current page in the document structure. The TOC button can be used to close and reopen the mini table of contents. The mini table of contents will not display on pages where no subpages are present.

The TOC button now appears when the documents are used in a small browser session (e.g. on a tablet).

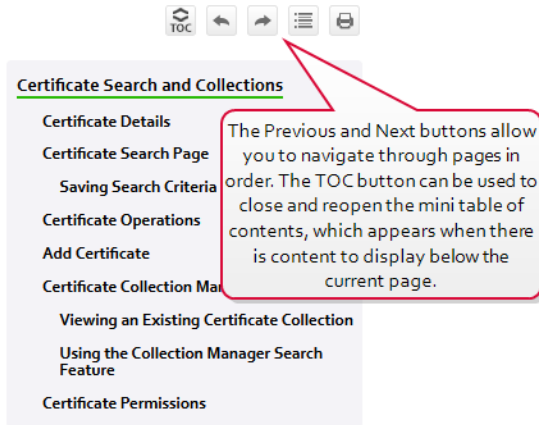


Figure 5: Navigate Forward and Backwards Through Pages

Updates and Improvements

- **Discovery** Changes & Improvements

SSL/TLS scanning has been updated to support discovery and monitoring of certificates at endpoints that serve certificates via TLS 1.3. The scan works with the TLS_AES_128_GCM_SHA256 cipher suite. TLS 1.3 connections will also work with SNI.

- **API** Changes & Improvements

More API endpoints have been added to do things such as manage security roles, configure certificate store jobs, and manage orchestrators. Please see the *Keyfactor Web APIs Reference Guide* for more details. You can access this and the API Endpoint Utility from the portal via the Help icon.

Additionally, the need for an API application key and secret has been removed. We now control certificate enrollment on the template level within the portal.

- **Logging** Changes

The log file default locations have moved from C:\CMS\Log to C:\Keyfactor\Log. In addition, the NLog.config files have moved from the C:\Program Files\Common Files location to application subfolders of the installation directory, which is C:\Program Files\Keyfactor\Keyfactor Platform by default. Instead of one large CMS_Log file, there are logs for each individual applications.

See *Editing NLog* in the *Keyfactor Command Reference Guide* for more information.



Tip: The API is used in conjunction with the applications and both the API log and the relevant other log (e.g. portal) should be consulted when troubleshooting.

- **Administration** Changes & Improvements

- There is now an option in the Application Settings to require users to agree to Subscriber Terms to enroll for a certificate. This setting also allows administrators to provide a link to those terms.

- CRL Stale Monitoring has been replaced with the ability for customers to define their own definition of "Stale" by generating alerts—and log entries—off the date that the CRL expires, rather than looking at the Next Publish date.

The main reason for that is that there is, by definition, a race condition between when the new CRL gets created (exactly at the Next Publish time), and when it is copied to the CRL distribution points. Basing alerts off CRL expiration allows customers to tune timeframes based on the way they handle their CRLs.

- **Automation** Changes & Improvements

A new constraint has been added to only allow the PowerShell event handlers to run scripts that are located in the path specified in the *Extension Handler Path* in the application settings. By default, this is "C:\Program Files\Keyfactor\Keyfactor Platform\ExtensionLibrary\". Customers should move scripts to this location or a subdirectory of it and test alerts before going into production. See *Adding PowerShell Handlers to Alerts* in *Keyfactor Command Reference Guide* for more information.

- **Certificates** Changes & Improvements

- A new field for "Import Date" has been added to the certificate details page to log when the certificate was imported into the Keyfactor Command database.
- Certificate Validation now shows the tests that are run when you click on a certificate and the results of those tests.
- SSL/TLS network name is now displayed on the certificate details dialog.
- Denied certificate requests now show the denial reason.
- The CSR generation page has been updated to show the Extended Key Usage of the selected template.

- **Certificates** Changes

Denied certificate requests are now labeled as "Denied/Failed" to align with public CA terminology.

- **Enrollment** Changes & Improvements

Email address subject alternative name option has been added to PFX enrollment.

- **Infrastructure** Changes

Application pool and service accounts are no longer configured with the db_owner role in SQL, but use a new custom role instead.

- **Orchestrator** Changes & Improvements

The certificate thumbprint has been added to the failed job message to help identify which certificate was unable to be deployed to an endpoint.

- **Certificate Authorities** Changes & Improvements

A new uniqueness constraint has been added to the CertificateAuthorities table. As a result, Keyfactor Command now checks that no CAs share the same logical name and host name combination.

- **Reporting** Changes & Improvements

- Added the ability to add a custom logo to scheduled reports.
- A new report has been added called *Expiration Report by Days* that allows for a number of days to be

specified to return a table of the certificates expiring in that timeframe.

- A column for Reverse DNS has been added to the *Certificates Found at TLS/SSL Endpoints* report.

- **Templates** Changes

RFC 2818 enforcement has moved from the CA to the template level since different templates have different requirements. Standalone CAs still have the RFC 2818 setting on the CA level.

- **Certificates** Fixes

- Fixed an issue where container level permissions were being ignored during enrollment preventing users from being able to add a certificate to a certificate store in that container.
- Fixed an issue where regular expressions were being applied to empty values when they should not have been.

- **Dashboard** Fixes

Resolved an issue where the dashboard CRL widget failed to load when configured with a high number of CRLs.

- **Email** Fixes

An issue is fixed where the emails sent from the SSL/TLS scans sometimes reported incorrect totals.

Upgrade Prerequisites

- **Keyfactor Orchestrators**

We encourage customers to use the new Keyfactor Universal Orchestrator moving forward, which requires .NET Core version 3.1. For existing deployments, .NET version 4.7.2 is required for systems running the legacy Windows Orchestrator.

- **SQL Server 2016**

Support for SQL Server 2016 has been removed in Keyfactor Command 9.0. Customers should upgrade to SQL Server 2016 Cumulative Update 2 or higher before upgrading to Keyfactor Command 9.0.

- **Database Compatibility**

Customers will also need to ensure the database compatibility is updated to support 2016 or higher. For more information on updating the compatibility level, please see System Requirements in the *Keyfactor Command Server Installation Guide*.

Upgrade Tasks

Pre-Installation

- If you are using the CA Policy module v7.0 on the same server that the Keyfactor Command Management Portal is installed on, you'll need to upgrade the module to v7.1 before running the Keyfactor Command 9.0 upgrade.
- Upgrade to SQL Server 2016 CU12 or higher and adjust the database compatibility level if needed (see above).

Post-Installation

After the upgrade is complete, some settings will need to be reconfigured due to changes in the way the Keyfactor Command Console handles tasks in Keyfactor Command 9.0:

- RFC 2818 enforcement has moved from the CA to the template level since different templates have different requirements. Standalone CAs still have the RFC 2818 setting on the CA level.
- Configure template-level metadata (if desired).
- Move all Event Handler scripts to the ExtensionLibrary folder under the Keyfactor program installation directory.
- Scripted alert handlers will fail to run if not in the path (or a subdirectory of it) specified by the "Extension Handler Path" application setting. By default, this is "C:\Program Files\Keyfactor\Keyfactor Platform\ExtensionLibrary\". Customers should move the scripts to this location and test them before moving to production.
- Update any monitoring or other processes that reference the log files to point to the new log file location.



Tip: We encourage customers to contact their customer success manager to discuss the new features and functionality in Keyfactor Command 9, and to schedule an upgrade.

Deprecation

• API Applications Deprecated

There is no longer the need to configure an API Application in the portal to allow for API enrollment for a certificate with a particular template. Template enrollment permissions are now controlled within the portal on the template level.

• Classic API Near-Term

The API calls that were previously in the Classic API (CMSAPI) have now been migrated to the Keyfactor API. Customers should use the Keyfactor API going forward and plan to migrate off the CMSAPI in the near future. Support for the CMSAPI will continue for the near future to allow customers time to migrate.

• Expiration Renewals Near-Term

Existing expiration renewals with Event Handlers will need to have the URLs updated to point to the Keyfactor API instead of the CMSAPI.

• Windows Orchestrator Future

We will continue to support the Windows Orchestrator. However, all new integrations and extensions will be delivered via the new Keyfactor Universal Orchestrator. We recommend customers use the Keyfactor Universal Orchestrator moving forward as new integrations become available.

• Verbosity in API Calls Future

In a future version of Keyfactor Command, the API will return all data regardless of the verbosity level. For backwards compatibility where performance is concerned, verbosity will be honored when loading certificate location data in the certificate query but has been replaced with new flags to include this data for future requests.

- **Active Directory** Future

In future releases, the ability to use the Active Directory (AD) password on PFX enrollment will be deprecated as we upgrade to allow authentication methods other than AD.

Known Issues/Limitations

Administration

- Daylight Savings Time (DST) is now shown as the time zone locale for clients using Keyfactor Command, rather than the UTC offset, which is the Microsoft CA default. This causes issues during DST to appear off by an hour, in time zones that do not have DST.
- Microsoft IIS settings to change authentication must be made manually to support the "Use Active Directory Password" application setting for the Keyfactor Command Management Portal.
- When using Basic Authentication, the authentication in Microsoft IIS may need to be configured manually for the KeyfactorAnalysis site.
- Authentication between the KeyfactorPortal, KeyfactorAPI, and KeyfactorAnalysis sites needs to be configured with the same authentication type, SSL, and host name.
- On the template RegEx settings, if you unselect use system-wide and do not enter a new RegEx the system-wide RegEx will still apply. To fix this, enter .* in the RegEx field to accept all values.
- When creating a new certificate store type, the "Depends On Other" option may not be available when creating the parameter. The workaround is to save the certificate store type and then use Edit to update the parameter.

Certificates

- Editing certificate details on a collection for a CA, while an initial sync is running on the CA, will cause inaccurate numbers to display in the Edit All window.
- If a CA is not scheduled to sync under Locations, it will not appear in lists to select for things like inclusion in Dashboards and Reports.
- Syncing an Issuing CA before syncing its parents in the chain causes Keyfactor Command to show the wrong requester for the chain certificates.

Keyfactor Command cannot support a CA in the local forest, with the same NetBIOS name as a CA in a trusted forest.

Infrastructure

- Running large SSL scans can impact Keyfactor Command application performance, if the Windows Agent/Orchestrator performing the scan is installed on the same server as the Keyfactor Command portal.
- If you receive an error when opening the portal that "the underlying connection was closed" please be sure you have the latest Windows Updates installed.

Reporting

- In Windows, drive mapping is done on a per-user basis. If you would like scheduled reports to be saved to a mapped drive, the timer service account needs to have that mapping created for them beforehand.
- Exporting a report to Microsoft Excel can fail with a 401 error in Microsoft Edge. Chrome or Firefox can successfully export to Excel. This problem is being worked on by the reporting engine vendor (Logi Analytics).
- Users configured for Logi Analytics reporting cannot have double quotes in the password field.

API

- The GET/Certificates API endpoint has a known issue where if a collection ID is not supplied the request fails. This will be fixed in an incremental release. The workaround in the meantime is to provide a collection ID of zero.

UI

- Occasionally, the "Please Wait" message will hang. Control + F5 will fix this.

Orchestrator

- There is an issue where the Universal Orchestrator is missing a task category in the Windows Event Log and instead reporting a task category of "(16)". This will be fixed in a future release.
- The new Keyfactor Universal Orchestrator provides much of the same functionality as the legacy Windows Orchestrator (see table below).

Table 3: Keyfactor Universal Orchestrator vs Windows Orchestrator Capabilities

Capabilities	Windows Orchestrator	Universal Orchestrator
IIS Management	✓	✓
CA Synchronization	✓	✓
SSL/TLS Discovery	✓	✓
FTP	✓	✓
F5 (SOAP/REST)	✓	
AWS	✓	
NetScaler	✓	
Fetch Logs (new)		✓

New capabilities will be added to the Keyfactor Universal Orchestrator in a future release as we phase out use of the existing Windows Orchestrator over time.

API Endpoint Change Log

The following changes were made to the API endpoints. Please review these carefully if you have implemented any integration using these endpoints.

Table 4: API Change Log

Endpoint	Method	Action	Notes
/Agents/Approve	POST	Add	
/Agents/Disapprove	POST	Add	
/CertificateCollections	PUT	Add	
/CertificateCollections/Copy	POST	Add	
/Certificates/{id}/History	GET	Add	
/Certificates/{id}/Security	GET	Add	
/Certificates/{id}/Validate	GET	Add	
/Certificates/Locations/{id}	GET	Add	
/Certificates/Metadata/Compare	GET	Add	
/Certificates/Metadata/All	PUT	Add	
/Certificates/RevokeAll	POST	Add	
/CertificateStoreContainers	GET	Add	
/CertificateStoreContainers/{id}	GET	Add	
/CertificateStores/Certificates/Add	POST	Add	
/CertificateStores/Certificates/Remove	POST	Add	
/Enrollment/CSR/Context/My	GET	Add	
/Enrollment/PFX/Context/My	GET	Add	
/JobTypes/Custom	GET, POST, PUT	Add	
/JobTypes/Custom/{id}	GET, DELETE	Add	

Endpoint	Method	Action	Notes
/OrchestratorJobs/Custom	POST	Add	
/OrchestratorJobs/JobHistory	GET	Add	
/OrchestratorJobs/JobStatus/Data	GET	Add	
/Reports	GET, PUT	Add	
/Reports/{id}	GET	Add	
/Reports/{id}/Parameters	GET, PUT	Add	
/Reports/{id}/Schedules	GET, POST, PUT	Add	
/Reports/Custom	GET, POST, PUT	Add	
/Reports/Custom/{id}	GET, DELETE	Add	
/Reports/Schedules/{id}	GET, DELETE	Add	
/Security/Identities	GET, POST	Add	
/Security/Identities/{id}	DELETE	Add	
/Security/Identities/Lookup	GET	Add	
/Security/Roles	GET, POST, PUT	Add	
/Security/Roles/{id}	GET, DELETE	Add	
/SSH/Keys/Unmanaged	DELETE	Add	
/SSH/ServiceAccounts	DELETE	Add	
/SSH/Users/Access	POST	Add	
/SSL/Networks/{id}/Scan	POST	Add	

2.2.1 Incremental Release 9.1 Notes

September 2021



Note: Keyfactor Command 9.1 is a minor release with incremental fixes and updates following the Keyfactor Command 9 major release. For more details on new features, improvements, and known limitations in Keyfactor Command 9.0, please review the [Major Release 9.0 Notes on page 18](#).

New Features

Custom Certificate Store Parameters Highlight

- **What problem does it solve?**

Provide the ability to associate custom parameters with certificate stores and certificate store entries to associate useful information.

- **How does it work?**

The certificate store type dialog now provides tabs for entry parameters, in addition to custom fields. These parameters and custom fields can be defined for input during enrollment, storage and management of certificate store inventory. For more information, see *Certificate Store Type Operations: Adding or Editing a Certificate Store Type Entry Parameters Tab* in the *Keyfactor Command Reference Guide*.

- **What's the benefit?**

Flexibility: Allows for further customization around certificate stores which can be dictated by customizable data.

Certificate Store Inventory Highlight

- **What problem does it solve?**

The previous version of certificate store inventory leveraged the certificate search functionality. While this worked, it was not always well-suited for the viewing of certificate store inventory.

- **How does it work?**

Clicking on the *View Inventory* button with a certificate store selected will now load a dialog with the inventory of the store.

- **What's the benefit?**

Ease-of-Use: Enables administrators to efficiently review certificate store inventory.

Certificate Store Type Parameters Highlight

- **What problem does it solve?**

The previous certificate store type parameters were defined via a comma-separated list and were not strongly typed.

- **How does it work?**

A formalized list is available to define parameters explicitly, including type (String, Boolean, Multiple Choice, Secret).

- **What's the benefit?**

Flexibility: Enables more powerful definition of certificate stores and data-validity checking.

Certificate Store Parameter Reporting Highlight

- **What problem does it solve?**

The current on-boarding of certificate stores requires manual data entry of custom fields and parameters.

- **How does it work?**

The Keyfactor Command orchestrator framework provides for orchestrators to report certificate store entry parameters.

- **What's the benefit?**

Flexibility: Enables customers to more easily track new certificate stores and changes to them made out-of-band from Keyfactor Command.

Keyfactor Command Configuration Wizard Highlight

The Keyfactor Command server configuration wizard now supports entry of group managed service accounts (gMSA) in the Administrative Users field on the Keyfactor Portal tab.

The screenshot shows the Keyfactor Command Configuration Wizard interface. On the left is a sidebar with tabs: Email, Keyfactor Portal (selected), Dashboard and Reports, Orchestrators, and API. The main area is divided into sections: Application Pool (Keyfactor), Administration (selected), Administrative Users (KEYFACTOR\GMSA_KyfUser\$), Enrollment, and Certificate Subject Format (CN={CN},E={E},O={O},OU=HR,L=Independence). A red callout box points to the Administrative Users field with the text: "Entry of gMSA users is supported in the Administrative Users field on the Keyfactor Portal tab."

Figure 6: Entry of gMSA Users in the Administrative Users Field



Note: Entry of gMSA users is not supported in the fields that require entry of a password in the configuration wizard (e.g. the service account on the Service tab) at this time. GMSA users cannot be selected using the people picker.

Updates and Improvements

- **Job Completion** Changes

Job completion handler is now provided the certificate identifier upon renewal so that the handler can perform any related tasks.

- **API Endpoint Deprecation** Changes

The CertificateCollections/{id}/Permissions endpoint due to an update slated for the Keyfactor Command v10 release and the fact that the endpoint is not updating permissions properly.

- **Permissions Message** Fixes

An incorrect error message was displayed to users without sufficient permissions to a certificate collection.

- **Certificate Store Deletion** Fixes

Fixed an issue in which a Certificate Store cannot be deleted if there is a job staged against it.

- **Pending Alerts** Fixes

Pending alerts were being sent on certificate issuance regardless of the associated template.

- **Certificate Inventory** Fixes

Corrected a permissions problem in which users with only read permissions on a Certificate Store were unable to view inventory of that certificate store.

Known Issues

- **CSR Enrollment**

In cases where there are duplicate template names in multiple forests, CSR enrollment can sometimes go to the wrong CA. This will be fixed in a future incremental release. Customers with environments with duplicate templates should wait to upgrade.

API Endpoint Change Log

The following changes were made to the API endpoints. Please review these carefully if you have implemented any integration using these endpoints.

Table 5: API Change Log

2.2.2 Incremental Release 9.2 Notes

October 2021



Note: Keyfactor Command 9.2 is a minor release with incremental fixes and updates following the Keyfactor Command 9 major release. For more details on new features, improvements, and known limitations in Keyfactor Command 9.0, please review the [Major Release 9.0 Notes on page 18](#).

New Features

UI Support for PAM CA Password Entry Highlight

- **What problem does it solve?**

The API previously supported the entry of certificate authority passwords to be stored within a Privileged Access Management (PAM) instance, but the UI did not implement this functionality.

- **How does it work?**

The certificate authority editor dialog allows for entry of a password to be stored in a PAM instance.

- **What's the benefit?**

Flexibility: Allows for multiple ways to securely store and manage certificate authority passwords

Custom Orchestrator Bulk Scheduling Highlight

- **What problem does it solve?**

Custom orchestrator jobs can currently only be scheduled individually.

- **How does it work?**

An API endpoint (POST OrchestratorJobs/Custom/Bulk) has been created to implement bulk schedules. The job identifiers along with the desired schedule can be provided in a single call.

- **What's the benefit?**

Ease-of-Use: Enables administrators to easily schedule large batches of custom orchestrator jobs.

Updates and Improvements

- **CA Management with PAM** Changes & Improvements

When configuring the *Use Explicit Credentials* option on a CA, you can now choose a PAM provider as the storage location for the credential password or the Keyfactor secrets table.

- **Logi Analytics License** Changes

A new license for Logi Analytics is required as the previous version is expiring. The 9.2 release includes the license update. Please see [Updating Logi Analytics License on the next page](#) for more information.

- **CSR Parsing Containing Spaces** Changes

CSRs containing spaces can now be parsed successfully during enrollment.

- **Robust SSL Certificate Parsing Error Handling** Fixes

Certificates that fail to be parsed during SSL scanning are now logged but do not cause the entire scan to immediately fail.

- **Robust Alert Failure Error Handling** Fixes

A failure processing an alert no longer prevents processing of subsequent alerts.

- **Hidden Metadata Enrollment Fields** Fixes

Metadata fields which are hidden during the enrollment process are now displayed properly in the resulting certificate details.

- **Collection-based Reports Failing** Fixes

Reports based on collections containing Revocation, Certificate State or Common Name no longer fail.

- **Incorrect CSR Enrollment CA** Fixes

The proper forest certificate authority is used for enrollment when using the API to enroll via CSR.

- **Denied Alerts Template** Fixes

The Denied Certificate Request alerts are once again properly scoped to the selected template. This was a regression from a previous release.

- **Java & C Agent Inventory Error** Fixes

An error was corrected in which an error was thrown if no entry updates were returned during inventory processing.

- **Orchestrator/Agent Re-Enrollment Error** Fixes

Fixed an issue in which an object reference error was thrown during re-enrollment operations.

- **Orchestrator Ceases Processing after Batch Submission** Fixes

Corrected an issue in which the orchestrators would cease processing after submission of a large batch of SSL results.

Updating Logi Analytics License

Logi is a 3rd party BI tool which is used by Keyfactor Command for its dashboard and report features. The license required for Logi is integrated into Keyfactor Command and resides within the product's Logi folder. The license's current term is 3 years with a 7-day grace period after expiration. During that grace period, an alert will appear, and a new license should be used to remediate the issue. Here are two examples:

- License close to expiration:



Figure 7: Keyfactor Logi License Expiration Alert

Dashboard:

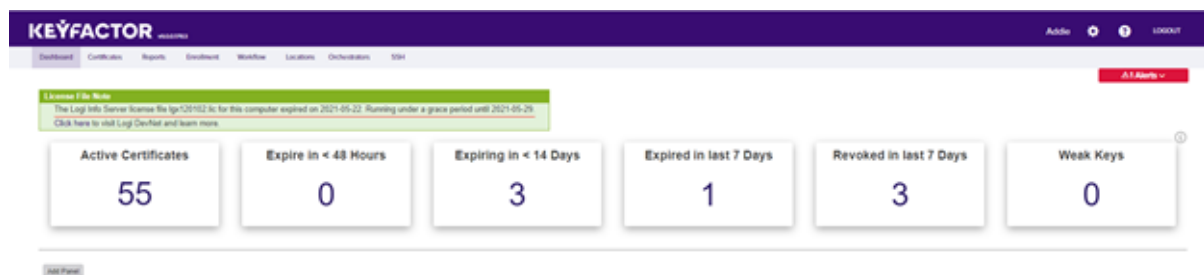


Figure 8: Keyfactor Logi License Expiration Alert on the Dashboard

Report:

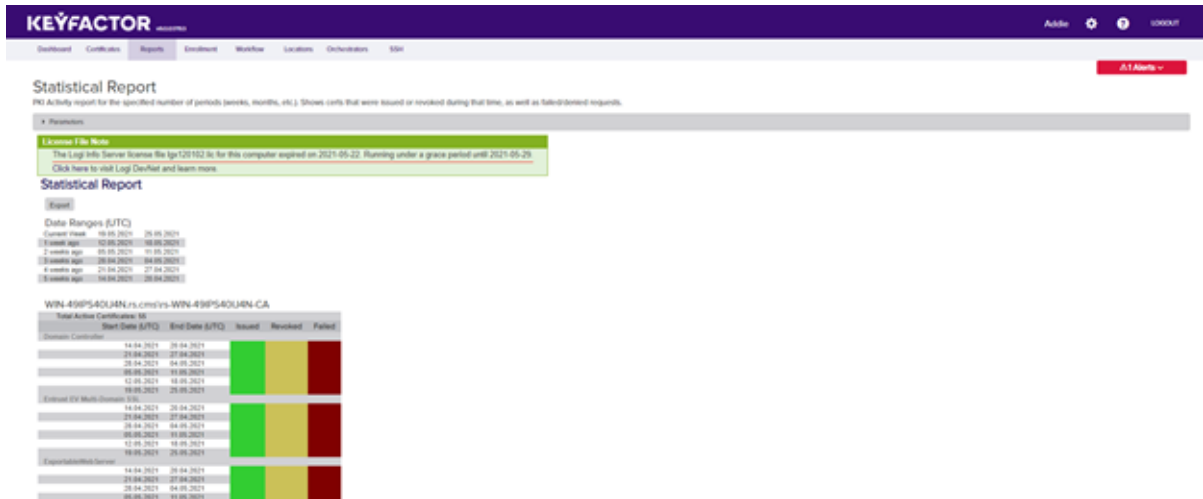


Figure 9: Keyfactor Logi License Expiration Alert on Report

- Expired license:

The Dashboard and Reporting capability is not available with an error message displayed like the one below.

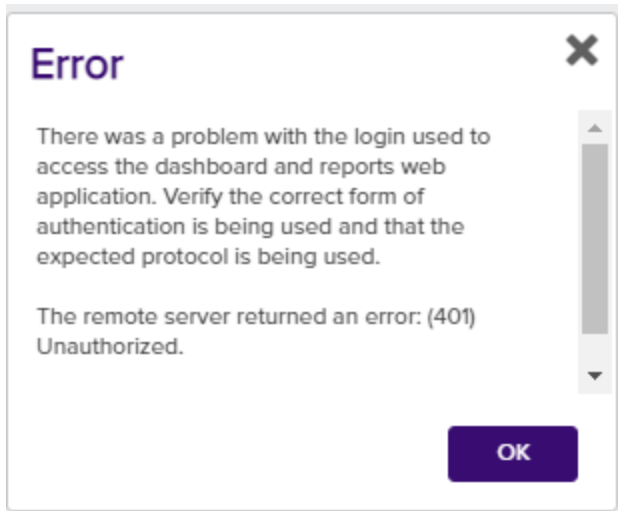


Figure 10: Keyfactor Expired Logi Error Message

Solution

The updated license for Logi is included in release 9.2 and will be installed automatically as part of the upgrade to or fresh installation of this version. If you are not installing Keyfactor Command v9.2, replace the license manually as follows:

1. On your Keyfactor Command server, navigate to the Logi folder in your Keyfactor Command instance. By default, this is:

C:\Program Files\Keyfactor\KeyfactorPlatform\Logi

If you are on an earlier version of Keyfactor Command your license file will by default be found in the following directory:

C:\Program Files\Certified Security Solutions\Certificate Management System\Logi]

2. The license file ends with an extension of *.lic*. Replace the license file with a valid one provided to you by Keyfactor. The license filename cannot be changed and should remain as "lgx120102.lic".

If the license has already expired, once it is replaced with a valid one and the browser is refreshed, the product will work as expected. The alert will no longer appear.

If you upgrade to a version of Keyfactor Command prior to v9.2 after replacing the license file, you will need to manually add the new license file again.

API Endpoint Change Log

The following changes were made to the API endpoints. Please review these carefully if you have implemented any integration using these endpoints.

Table 6: API Change Log

Endpoint	Methods	Action	Notes
/Certificates	GET	Fix	No longer fails if a collection id is not provided.
/OrchestratorJobs/JobHistory	GET	Fix	Request no longer fails for 'Dynamic' job types.
/Reports/Schedules/{id}	DELETE	Fix	Response code is now 200 when the user role does not have <i>Modify – Report</i> permission.

2.2.3 Incremental Release 9.3 Notes

November 2021



Note: Keyfactor Command 9.3 is a minor release with incremental fixes and updates following the Keyfactor Command 9 major release. For more details on new features, improvements, and known limitations in Keyfactor Command 9.0, please review the [Major Release 9.0 Notes on page 18](#).

Updates and Improvements

- **Certificate Search** Changes & Improvements

The certificate search functionality has been optimized to increase speed and efficiency, especially with higher numbers of certificates and associated certificate locations. This means certificate searches done in the management portal for large data sets that include certificates found in certificate stores (e.g. 250,000+ certificates each in 5 or more certificate stores) now complete more quickly.

- **Failed Certificate Management Jobs** Fixes

Certificate management jobs that have failed no longer continue to run.

- **PKI Status Report Time Zone**

Fixes

Corrected the format of time zones in the PKI Status for Collection Report.

- **Database Encryption Configuration**

Fixes

The Configuration Wizard now verifies the selected database encryption certificate has an associated valid private key.

- **SSL Scanning**

Fixes

Updates made to the SSL scanning process to be more efficient and eliminate potential process-locking scenarios.

- **Management Portal User Interface**

Fixes

Various Management Portal user interface fixes.

- **Management Portal Reports**

Fixes

Updates to Management Portal reports to handle upgrade scenarios and other user interface fixes.

API Endpoint Change Log

The following changes were made to the API endpoints. Please review these carefully if you have implemented any integration using these endpoints.

Table 7: API Change Log

Endpoint	Methods	Action	Notes
/JobTypes/Custom	POST	Fix	No longer requires default field values.

2.2.4 Incremental Release 9.4 Notes

December 2021



Note: Keyfactor Command 9.4 is a minor release with incremental fixes and updates following the Keyfactor Command 9 major release. For more details on new features, improvements, and known limitations in Keyfactor Command 9.0, please review the [Major Release 9.0 Notes on page 18](#).

Updates and Improvements

- **Log4j CVE Vulnerability**

Changes & Improvements

Keyfactor has conducted an assessment of the recently-announced CVE for the log4j library (<https://github.com/advisories/GHSA-jfh8-c2jp-5v3q>). We have identified that the vast majority of the Keyfactor suite of products are NOT affected. This includes EJBCA, SignServer, the Keyfactor Command platform, Keyfactor Control, and Code Assure.

The only component that does make use of the log4j library is the Java Agent for Keyfactor Command; for clarity, all other Keyfactor agents and gateways are NOT affected.

Details

According to the CVE, exploit of the vulnerability requires compelling log4j to log user-controlled input. In the case of the Java agent, there are mitigating factors, such as:

- The Java agent has an "outbound-only" connection pattern and does not accept inbound network connections of any kind.
- Users of the Java agent who could control such input are typically Keyfactor administrators.
- The limited nature of things the Java agent is expected to log.

From [Log4j – Apache Log4j Security Vulnerabilities](#):

- Mitigation: This behavior can be mitigated by setting either the system property log4j2.formatMsgNoLookups or the environment variable LOG4J_FORMAT_MSG_NO_LOOKUPS to true.

Patch Implementation—The 8.7.2 version of the Java Agent to utilize the patched version of Log4j, and mitigate the vulnerability.

- **Orchestrator Certs** Changes & Improvements

Ability for an orchestrator to use a TLS client authentication certificate to map to a Windows identity in IIS and to use a different TLS certificate provided in an HTTP header to identify the orchestrator to Keyfactor Command.

- **External Validation Certificate Requests** Changes & Improvements

Certificate requests returning a status of EXTERNAL_VALIDATION are not treated as failures and will be sync'd with appropriate metadata when the certificate is available.

- **Certificate Detail Data Efficiency** Changes & Improvements

The certificate details are obtained from the server when needed, and not as part of the initial certificate query. This greatly increases the efficiency and performance of the page.

- **Query Optimization for Large Scale Environments** Changes & Improvements

Multiple optimizations have been made to improve management portal query performance, scalability, and stability in large scale environments.

- **Pending Certificates API Endpoint** Changes & Improvements

Metadata for certificate requests in a pending state is now available for retrieval via the /Workflow/Certificates/Pending API endpoints (GET /Workflow/Certificates/{id} and GET /Workflow/Certificates/Pending).

- **SSL Scanning Chunk Sizes** Changes & Improvements

Distinct SSL scanning chunk size application settings are now available for discovery and monitoring to allow for greater control over performance tuning.

- **Dashboard Risk Header Clarifications** Changes & Improvements

The dashboard Risk Header now contains verbiage to clarify that no filtering exists for renewed certificates in expired query counts.

In addition, the dashboard Risk Header contains verbiage noting that the certificate counts are global and not limited to only those to which the current user has access.

- **Custom Job Blueprint Duplication** Fixes

An issue was fixed so that a copy operation on a blueprint successfully copies custom jobs.

- **Certificate Count by Template Report** Fixes

An issue was fixed so to properly retain the selected default certificate authority.

- **SSL Quiet Hours Daylight Savings** Fixes

Updates were made to the SSL Quiet Hours to better handle schedules involving Daylight Savings Times.

- **SSL Monitoring Emails** Fixes

SSL Monitoring emails now send the complete and correct data when multiple orchestrators are in simultaneous use.

- **Certificate Detail Before/Not After Dates** Fixes

Certificate details now display the time in addition to the date for Before and Not After dates.

- **SSL Scanning Certificate History** Fixes

A fix was implemented to properly display the history of certificates imported into the system via SSL scanning.

API Endpoint Change Log

The following changes were made to the API endpoints. Please review these carefully if you have implemented any integration using these endpoints.

Table 8: API Change Log

Endpoint	Methods	Action	Notes
/Workflow/Certificates/Pending	GET	Update	Now returns the associated metadata.

2.2.5 Incremental Release 9.5 Notes

January 2022



Note: Keyfactor Command 9.5 is a minor release with incremental fixes and updates following the Keyfactor Command 9 major release. For more details on new features, improvements, and known limitations in Keyfactor Command 9.0, please review the [Major Release 9.0 Notes on page 18](#).

Updates and Improvements

- **Agents and Orchestrators** Changes & Improvements

Several enhancements have been made to the orchestrators:

- The alias column size has increased to allow for longer alias names.
- A new setting allows the IIS stores to be accessed using WinRM over SSL (port 5986).
- The last thumbprint used for client certificate authentication by orchestrators is now tracked and can be returned using the GET /Agents API method.
- The UI now allows you to see why an orchestrator could not register for a session rather than having to look in the logs.
- A new API endpoint has been added to request or require that one or more orchestrators enroll for a new client authentication certificate on the orchestrator's next session registration (POST /Agent-s/SetAuthCertificateReenrollment).
- A new API endpoint has been added to reset an orchestrator (POST /Agents/{id}/Reset). Updates include removing orchestrator jobs, deleting associated certificate stores, setting the orchestrator status to new, and clearing thumbprint data as below.
- The orchestrator reset function in the UI and API now clears the orchestrator client authentication certificate thumbprint data to allow the orchestrator to be reconfigured with a new certificate.

- **Management Portal—Reports** Changes & Improvements

The "Expiring in less than two weeks" text in the *PKI Status for Collection* report has been updated to change the color scheme to be more readable (white text on a maroon background).

- **API** Fixes

Fixed an issue with the Enrollment/PFX API call not working without specifying a CA. The JobTypes/Custom API call now returns the Job Retry Count.

- **Certificates—Metadata** Fixes

Fixed an issue so that hidden metadata now shows when using "Edit All".

- **Certificate Stores—Scheduling** Fixes

Fixed an issue to now prompt the user to enter schedule values for "Exactly once" and for "Daily" schedules.

- **Certificate Store—Inventory** Fixes

Fixed an issue when viewing the inventory of certificate store that has an alias without a certificate.

- **Installation—Modify/Remove** Fixes

Corrected an issue where the MSI would freeze if trying to modify or uninstall an installation that had been done without any components selected to be installed.

- **Orchestrators and Agents—Custom Job Retry** Fixes

Corrected an issue where custom jobs would not retry if the job complete handlers failed.

- **Alerting—Email Address Format** Fixes

Fixed an issue where the email address validation was not allowing some valid subdomains.

- **Registration Handler—Enrollment** Fixes

The registration handler now receives the certificate chain for enrollments performed via the enrollment call-back.

- **Management Portal Reports** Fixes

Updates to Management Portal reports to handle upgrade scenarios and other user interface fixes.

API Endpoint Change Log

The following changes were made to the API endpoints. Please review these carefully if you have implemented any integration using these endpoints.

Table 9: API Change Log

Endpoint	Methods	Action	Notes
/Enrollment/PFX	POST	Update	No longer requires a certificate authority name to be provided.

2.2.6 Incremental Release 9.6 Notes

February 2022



Note: Keyfactor Command 9.6 is a minor release with incremental fixes and updates following the Keyfactor Command 9 major release. For more details on new features, improvements, and known limitations in Keyfactor Command 9.0, please review the [Major Release 9.0 Notes on page 18](#).

Updates and Improvements

- **Configuration Wizard** Fixes

Fixed an issue in which the SQL Server login for the application pool account was not created by the configuration wizard.

- **Azure Database Creation** Fixes

Fixed an issue in which database upgrades fail on Azure SQL for newly created databases.

- **Certificate Store—Scheduling** Fixes

Fixed an issue in which jobs rescheduled for *immediate* would not execute.

- **Command Line Configuration Wizard** Fixes

Fixed an issue in which the console configuration wizard cannot populate Azure SQL databases.

- **Custom Orchestrator Job Blueprint** Fixes

Corrected an issue where a duplicate custom job schedule was created when applying the same blueprint to orchestrator.

- **Expiration Report by Days** Fixes

Corrected an issue where the Expiration Report by Days would crash on DD/MM/YYYY formatted dates.

- **Certificate Renewal in Single Store** Fixes

Fixed an issue where a single certificate stored at multiple aliases within the same certificate store was not renewed successfully.

- **CRL Alert Emails** Fixes

Corrected an issue in which a CRL alert email would be sent even if a new CRL was available.



Note: No changes were made to the Keyfactor Universal Orchestrator in this release, as such the 9.5 version of the Universal Orchestrator should still be considered the latest and is fully compatible with the Keyfactor Command 9.6 release.

API Endpoint Change Log

No API endpoint changes were made in this release.

2.2.7 Incremental Release 9.7 Notes

March 2022



Note: Keyfactor Command 9.7 is a minor release with incremental fixes and updates following the Keyfactor Command 9 major release. For more details on new features, improvements, and known limitations in Keyfactor Command 9.0, please review the [Major Release 9.0 Notes on page 18](#).

Updates and Improvements

- **JavaScript Caching** Changes & Improvements

Updated pages not to cache static files, including JavaScript.



Note: After upgrading to 9.7, the cache will still need to be cleared one final time so that the latest version of the pages get loaded with the updated cache setting.

- **API CA Auto-selection** Changes & Improvements

The Keyfactor API will auto-select an enrollment certificate authority if one is not explicitly provided.

- **Certificate Stores** Fixes

Fixed an issue in which a user could assign a certificate store to a container without explicit permissions to that certificate store.

- **Certificate Stores** Fixes

Fixed an issue in which database upgrades fail on Azure SQL for newly created databases.

- **Certificate Stores—Scheduling** Fixes

Fixed an issue in which jobs could appear to be scheduled for a certificate store with no available agent.

- **Security Configuration** Fixes

Fixed an issue in which the security roles management page could not be loaded after deletion of an associated Active Directory (AD) group.

- **Metadata String & Integer Fields** Fixes

Corrected an issue where default values could not be set for metadata fields of type string or integer.

- **Certificate Store Deployment** Fixes

Fixed an issue where a certificate cannot be deployed to a certificate store when deploying using a property instead of a certificate store type or Id.



Note: No changes were made to the Keyfactor Universal Orchestrator in this release, as such the 9.5 version of the Universal Orchestrator should still be considered the latest and is fully compatible with the Keyfactor Command 9.7 release.

API Endpoint Change Log

The following changes were made to the API endpoints. Please review these carefully if you have implemented any integration using these endpoints.

Table 10: API Change Log

Endpoint	Methods	Action	Notes
/KeyfactorAPI/License	GET	Add	

2.2.8 Incremental Release 9.8 Notes

April 2022



Note: Keyfactor Command 9.8 is a minor release with incremental fixes and updates following the Keyfactor Command 9 major release. For more details on new features, improvements, and known limitations in Keyfactor Command 9.0, please review the [Major Release 9.0 Notes on page 18](#).

Updates and Improvements

- **PFX Generation** Changes & Improvements

Consolidated PFX generation code so that the PFX files are generated identically from the enrollment and download components.

- **SCEP Intune Integration** Changes & Improvements

Keyfactor's Simple Certificate Enrollment Protocol (SCEP) component has been updated to utilize the latest Intune API: Microsoft Authentication Library (MSAL) and Azure AD Graph API.

- **Pending Certificate Request SAN** Fixes

Fixed an issue in which pending certificate requests containing a User Principal Name (UPN) in the Subject Alternative Name (SAN) would be prefixed with '[O]', and IPv6 addresses were not displayed.

- **vSCEP Challenge Error** Fixes

Fixed an issue in which attempting to obtain a Validated SCEP (vSCEP) challenge resulted in an assembly loading error.

- **Denied Alert Email SAN** Fixes

Fixed an issue in which Denied Certificate Alert email did not contain the certificate Subject Alternative Names (SANs).

- **Expiration Alert Logging** Fixes

Fixed an issue in which excessive and superfluous log messages were generated during Expiration Alert processing.



Note: No changes were made to the Keyfactor Universal Orchestrator in this release, as such the 9.5 version of the Universal Orchestrator should still be considered the latest and is fully compatible with the Keyfactor Command 9.8 release.

API Endpoint Change Log

No API endpoint changes were made in this release.

2.2.9 Incremental Release 9.9 Notes

May 2022



Note: Keyfactor Command 9.9 is a minor release with incremental fixes and updates following the Keyfactor Command 9 major release. For more details on new features, improvements, and known limitations in Keyfactor Command 9.0, please review the [Major Release 9.0 Notes on page 18](#).

New Features

Metadata Access on View Inventory Dialog Highlight

- **What problem does it solve?**

The View Inventory dialog for certificate stores previously displayed each certificate found in the certificate store but did not include the Keyfactor Command metadata field values configured for the certificates.

- **How does it work?**

The View Inventory dialog on the Certificate Stores page now includes a Metadata section to allow you to view the metadata fields configured in Keyfactor Command for each certificate found in the certificate store.

- **What's the benefit?**

Streamlining: You no longer need to look up the metadata fields for the certificates separately.

Updates and Improvements

- **GET /Agents Keyfactor API Endpoint** Changes & Improvements

The GET /Agents Keyfactor API endpoint now includes a query parser to allow searching by AgentId. For example:

```
AgentId -eq "d2f0d545-c3b3-4ea3-bc0a-0232865e24c3"
```

- **Logging** Changes

Changes have been made to the way that Keyfactor Command logs are initialized to support logging from multiple source libraries including Quartz.

- **Alerts Do Not Resume After a Database Connection Failure** Fixes

Fixed an issue in which expiration alerts and pending, issued, and denied certificate alerts that failed due to a database connection problem would not restart on resolution of the database connection issues until the Keyfactor Command service was restarted.

- **Revoke All of Entirely Revoked or Expired Certificates Fails** Fixes

Fixed an issue in which attempting to revoke all for a group of certificates that contains only certificates that are revoked already and/or expired results in an error message.

- **SSH Server Groups Incompatible with Domain Names Containing Hyphens** Fixes

Fixed an issue in which SSH server groups could not be created in environments where the Keyfactor Command domain contains a hyphen because the SSH server group owner field would not support a hyphen in the domain name.

- **Certificate Signing Requests Can Produce an Error on Decoding** Fixes

Fixed an issue in which CSR decoder used in CSR enrollment can produce an error on decoding the CSR under select circumstances. These can include SCEP requests with no SANs and CSRs with no extensions.

- **Keyfactor API GET Requests with a Sort Produce a 500 Error** Fixes

Fixed an issue in which Keyfactor API GET endpoints that support query sorting in the URL would produce a 500 error if the sort field was not provided correctly (e.g. the fieldname was entered with a space or was a valid fieldname but not one that was supported for sorting).



Note: No changes were made to the Keyfactor Universal Orchestrator in this release, as such the 9.5 version of the Universal Orchestrator should still be considered the latest and is fully compatible with the Keyfactor Command 9.9 release.

API Endpoint Change Log

The following changes were made to the API endpoints. Please review these carefully if you have implemented any integration using these endpoints.

Table 11: API Change Log

Endpoint	Methods	Action	Notes
/Reports/<any>	GET	Fix	Spaces within the sortField no longer results in an exception.
/Reports/{id}/Schedules	GET	Fix	An invalid sortField no longer results in an exception.
/Agents	GET	Update	New query parser to support the AgentId GUID.

2.2.10 Incremental Release 9.10 Notes

June 2022



Note: Keyfactor Command 9.10 is a minor release with incremental fixes and updates following the Keyfactor Command 9 major release. For more details on new features, improvements, and known limitations in Keyfactor Command 9.0, please review the [Major Release 9.0 Notes on page 18](#).

Updates and Improvements

- **Enrollment** Changes & Improvements

The enrollment options in Keyfactor Command now support enrolling for SubCA type certificates.

- **Expiration Alert Renewal Handler** Fixes

- Fixed an issue where the expiration alert renewal handler would generate an error if the alert contained more than one email recipient.

- Fixed an issue where the expiration alert renewal handler would not run on databases that had been upgraded from versions of Keyfactor Command prior to 5.

- **PAM Secret Storage** Fixes

Fixed an issue where PAM parameters of type secret (often passwords) weren't being loaded in Keyfactor Command correctly when returned from the PAM provider.



Note: No changes were made to the Keyfactor Universal Orchestrator in this release, as such the 9.5 version of the Universal Orchestrator should still be considered the latest and is fully compatible with the Keyfactor Command 9.10 release.

API Endpoint Change Log

No API endpoint changes were made in this release.

2.3 Major Release 8.0 Notes

October 2020

New Features

SSH Key Management

Our new module, SSH Key Manager, gives security and network teams a simple, centralized solution to simplify SSH key management and mitigate the risk of emerging SSH-based attacks.

The SSH Key Manager allows you to:

- **Discover:** Inventory SSH authorized_keys across your servers and cloud infrastructure
- **Analyze:** Review your key inventory to detect and remediate things like unauthorized root access, stale keys, and keys that belong to users that should no longer have access
- **Rotate:** Configure automated key rotation alerts and enable self-service key generation and rotation by SSH users
- **Automate:** Keep DevOps and admin teams moving with automated key deployment, which can be baked into the server provisioning process in highly automated cloud environments
- **Report:** Generate reports to keep an eye on user and service account keys in your environment, including their lifecycle, access, and trust relationships



Note: If you are re-installing the Keyfactor Bash Orchestrator, you must run the uninstall.sh script before re-running the install.sh script.



Note: The certificate used during the Keyfactor Bash Orchestrator installation needs to be in PEM format.

User Interface Improvements

- Links to the specific areas of the Keyfactor Command documentation are now available in the application.
- Adding a certificate to a certificate store has been updated from the previous tree view control to a searchable grid to make management of certificate stores at scale more efficient.
- Grids have changed to allow selecting via checkboxes and to include tabs to make the less frequently used functions grouped in a less front and center way.
- Some areas of the application now have expandable/collapsible functionality to hide information when it isn't needed to provide a cleaner interface.

CA Authorization

You can now enter explicit credentials when contacting the CA. The requester will be provided in the request in order to track who is acting on the CA. Additionally, permissions for who can enroll for a certificate can be defined on a Keyfactor Command Security Role level.

Updates and Improvements

- **Installation** Changes

Default installation path changes from "Certified Security Solutions" to "Keyfactor".

- **Installation** Changes

Installation now requires Remote Server Administration Tools Active Directory PowerShell Module.

- **Administration** Changes & Improvements

Application Settings are now accessible via the gear icon.

- **Certificates** Changes

Certificate Collections are now under the Certificates menu item.

- **Certificate Revocation—Hold** Changes

Certificates that have been revoked with a reason of "Certificate Hold" can now have the hold removed.

Deprecation/Required Upgrades

- **Windows Server 2012 R2** Deprecated

Support for Windows Server 2012 R2 has been deprecated in Keyfactor Command 8, since it has also been deprecated by Microsoft, and is no longer functioning well with newer backend technologies that our software uses. Customers should upgrade to Windows Server 2019.

- **User Enrollment Portal** Deprecated

In Keyfactor Command 8, the support for the User Enrollment Portal (which allows users to go to a browser page to enroll for a certificate—this is NOT the enrollment section of the Keyfactor Command Management Portal)—are deprecated.

- iOS enrollment
- Android enrollment
- ActiveX PFX enrollment (based on whenever Microsoft phases out Internet Explorer as, at that point, ActiveX will not be available)
- User PFX enrollment (user build-from-AD certs, NOT the web server PFX in the main Management Portal)

It is recommended not to do new deployments of these features and to plan for migration away or an in-house support option.

- **Expiration Renewals** Near-Term

Existing expiration renewals will need to have the URLs updated to point to the KeyfactorAPI instead of the CMSAPI.

- **Active Directory** Future

In future releases the ability to use the Active Directory password on PFX enrollment will be deprecated as we upgrade to allow authentication methods other than Active Directory.

Known Issues/Limitations

Administration

- Daylight Savings Time (DST) is now shown as the time zone locale for the clients using Keyfactor Command, rather than as the UTC offset, which is what Microsoft CA uses. This causes issues during DST in time zones that do not have DST to appear off by an hour.
- Microsoft IIS settings to change authentication to support the "Use Active Directory Password" application setting for the Keyfactor Command portal must be made manually.
- When using Basic Authentication, the authentication in Microsoft IIS may need to be configured manually for the KeyfactorAnalysis portal.
- Authentication between the KeyfactorPortal, KeyfactorAPI, and KeyfactorAnalysis sites needs to be configured with the same authentication type, SSL, and host name.

Certificates

- Editing certificate details on a collection for a CA while an initial sync is running on the CA will cause inaccurate numbers to display in the Edit All window.
- If a CA is not scheduled to sync under "PKI Management" it will not appear in lists to select for things like inclusion in "Dashboards and Reports".
- Syncing an Issuing CA before syncing its parents in the chain causes Keyfactor Command to show the wrong requester for the chain certificates.

- Keyfactor Command cannot support a CA in the local forest with the same NetBIOS name as a CA in a trusted forest.
- In some upgrade cases, the Certificate Search page only partially loads or enrollment returns a System.Exception error. Opening the Developer Tools with F12 key and performing an Empty Cache and Hard Reload will resolve this problem.

Infrastructure

- Running large SSL scans can impact Keyfactor Command application performance if the Windows Agent/Orchestrator performing the scan is installed on the same server as the Keyfactor Command portal.
- If you receive an error when opening the portal that "the underlying connection was closed" please be sure you have all of the latest Windows Updates installed.

Reporting

- In Windows, drive mapping is done on a per-user basis. If you would like scheduled reports to be saved to a mapped drive, the timer service account needs to have that mapping created for them beforehand.
- Exporting a report to Microsoft Excel can fail with a 401 error in Microsoft Edge. Chrome or Firefox can successfully export to Excel. This problem is being worked on by the reporting engine vendor (Logi Analytics).
- Users configured for Logi Analytics reporting cannot have double quotes in the password field.

UI

- Occasionally, the "Please Wait" message will hang. Control + F5 will fix this.

2.3.1 Incremental Release 8.1 Notes

November 2020



Note: Keyfactor Command 8.1 is a minor release with incremental fixes and updates following the Keyfactor Command 8 major release. For more details on new features, improvements, and known limitations in Keyfactor Command 8.0, please review the [Major Release 8.0 Notes on page 49](#).

New Features

- **Scriptable Windows Orchestrator Installation**

The Windows Orchestrator now supports a fully scriptable installation.

- **Pending Requests Show AD Information**

Pending requests now show the information that would be populated from AD such as Distinguished Name, Common Name, and Subject Alternative Names.

- **AnyAgent Management Job can Trigger an Inventory Job**

If an inventory job id is returned to an AnyAgent in the completion call of a management job, the inventory job will be initiated after the management job completes.

- **UPN as SAN**

Added support for UPN as a SAN type when enrolling through Keyfactor Command.

- **P7B Import**

A P7B file can be imported into Keyfactor Command via the Certificate Import UI and API without having to be converted to another file format.

Updates and Improvements

- **Infrastructure**

Fixes

Fixed an issue in the configuration wizard with SQL authentication and with enabling the CMSAPI when using a saved configuration file.

- **SSL Discovery & Monitoring**

Fixes

Fixed an issue with network ranges disappearing in the UI on edit.

- **Expiration Alerts**

Changes & Improvements

Expiration renewal emails now contain the success or failure of the renewal job.

- **Certificate Templates**

Fixes

Fixed an issue that was preventing newly created certificate templates from being imported.

- **Reporting**

Fixes

Fixed an issue where the report manager incorrectly reported unsaved changes.

- **Certificate Stores**

Fixes

Fixed an issue to allow NetScaler certificates to be renewed even if the original certificate at the endpoint did not have the private key.

- **Certificate Metadata**

Fixes

Fixed an issue where big text metadata fields that contained XML or line breaks were causing an audit signing mismatch.

- **Management Portal**

Changes & Improvements

Updated the error message displayed when using IE to be more descriptive that IE is no longer supported.

- **Certificate Metadata**

Changes & Improvements

Added non-US date formats to the metadata date field validation.

- **Certificate Revocation**

Fixes

Fixed an issue with revocation and non-US date time formats.

- **Management Portal**

Changes & Improvements

Adjustments to font color in some areas of the portal and reports for better visibility.

- **Management Portal** Fixes
Minor UI fixes and updates.
- **SSL Discovery & Monitoring** Fixes
Fixed an issue with SSL endpoints being marked as reviewed or monitored in bulk.
- **API** Fixes
Fixed a problem where the GET SSL/Networks API endpoint was ignoring the querystring value passed to it.
- **API** Changes & Improvements
Updates to Swagger API documentation continue.
- **Certificate Stores** Changes
Certificate store management job custom fields now display when scheduling management job.
- **Certificate Stores** Changes
On PFX Enrollment, removed the requirement for the NetScaler server name when deploying to Netscaler.
- **Certificate Stores** Changes & Improvements
Revoked Certificates in Certificate Stores report now accepts a collection as a parameter.
- **Dashboard** Fixes
Fixes to allow parenthesis in the CRL Revocation Monitoring URLs used in the Dashboard.
- **Certificates** Fixes
Fixed a re-issued certificate problem that had a field incorrectly filled in.
- **SSL Discovery & Monitoring** Fixes
Fixed an issue in SSL network definitions to restore the ability to add a range of ports.
- **CSR Generation** Fixes
Fixed an issue with the CSR Generation page reporting an invalid template.
- **Orchestrators** Changes
Disapproved orchestrators are now hidden by default in the Orchestrator Management page.
- **Enrollment** Changes & Improvements
Allow enrollment with a CSR that has no CN and/or SAN.
- **CSR Generation** Changes
Removed the option for RSA 1024 from the CSR Generation page.
- **Reporting** Changes & Improvements
Added DNS name to the Full Certificate Extract report.
- **Reporting** Changes

Expiration Report sorts on Expiration Date by default.

Known Issues/Limitations

- **Version**

Version 8.0.4.0 is the correct version for Keyfactor Command 8.1.

- **Certificates**

Deleting a collection that is used in an alert or a report schedule will fail without saying why. This will be updated in a future version. The workaround is to remove the collection from the report schedules and/or alerts and then deleting it.

2.3.2 Incremental Release 8.2 Notes

December 2020



Note: Keyfactor Command 8.2 is a minor release with incremental fixes and updates following the Keyfactor Command 8 major release. For more details on new features, improvements, and known limitations in Keyfactor Command 8.0, please review the [Major Release 8.0 Notes on page 49](#).

New Features

- **SSL/TLS Scanning Scheduling Updates**

- The SSL scanning definitions have been updated to allow for multiple "Quiet Hours" windows. In addition, the API and UI now have support for a "Scan Now" option which will allow a scan to run if there is not already a current scan in process for that network definition.
- SSL scans can now be defined with IP Addresses that have port ranges extending to 65535.

- **Windows Orchestrator Service Account**

The Windows Orchestrator can now be configured to run with a service account without interactive logon rights.

- **API Updates**

- Ability to run a one-time "Scan Now" SSL/TLS job.
- Ability to search collections by the collection name.

- **Event Logging**

CRL Event monitoring now includes the Validity Period in the event log message to help distinguish between root and issuing CAs.

Updates and Improvements

- **Reporting** Fixes

Fixed an issue where reports failed to process de-duplication correctly using the "Ignore renewed certificate results by" option set on the certificate collection.

- **Reporting** Fixes

Certificates by Revoker report updated to be clearer on who the revoker was.

- **API** Fixes

Fixed an issue where metadata display order values were getting duplicated when updated via the API.

- **API** Fixes

Fixed an issue where an API call to revoke a certificate was not being scheduled at the correct time.

- **Certificate Revocation** Fixes

Addressed an issue where after revocation a certificate might still show up as Active in the Keyfactor Command Management Portal until the next sync.

- **Certificate Metadata** Fixes

Fixed an issue in date time queries that was causing some metadata fields not to get updated with doing an "Edit All".

- **Reporting** Fixes

Fixed an issue with editing report schedules failing to update the scheduled time.

- **Management Portal** Fixes

Minor visual UI updates.

Deprecation/Required Upgrades

- **.NET 4.7.2**

.NET version 4.7.2 is now required for systems hosting Keyfactor Windows Orchestrators.

2.3.3 Incremental Release 8.3 Notes

January 2021



Note: Keyfactor Command 8.3 is a minor release with incremental fixes and updates following the Keyfactor Command 8 major release. For more details on new features, improvements, and known limitations in Keyfactor Command 8.0, please review the [Major Release 8.0 Notes on page 49](#).

New Features

- **Increased Allowed Number of Certificate Store Types**

Added support for a larger number of custom certificate store types.

- **SSH Updates**

- An Access Management tab has been added to the user dialog that allows for the management of a user's logons.
- Addition of a new SSH Users Management page.
- Regular expressions have been added so administrators can put parameters around the strength of pass-phrases.

- **Default Certificate Collections on a New Installation**

A new installation of Keyfactor Command will provide a default "My Certificates" collection.

- **API Changes**

A certificate's SSL locations can now be returned from the API.

- **Certificate Changes**

- During a re-enrollment default metadata fields are populated if the old certificate had blank values for the metadata.
- Pending requests now show the denial reason.
- Added the internal Keyfactor Command ID to the certificate details page to aid in searching and in API calls.

Updates and Improvements

- **ACME** Fixes

Addressed an issue with the ACME server retrieving certs with PEM encoding.

- **Orchestrator** Changes

Added a check in the Java Agent installer for .NET framework 4.7.2.

- **Certificate Stores** Changes & Improvements

F5 Certificate Stores return the F5 version.

- **API** Fixes

Fixed an issue with PUT and POST endpoints for SSL/Networks not setting required default values.

- **API** Fixes

Fixed an issue with the Template PUT calls not setting RegEx values properly.

- **API** Changes & Improvements

Performance improvements made to the GET certificates API call.

- **Certificate Stores** Fixes

Fixed an issue where updating a certificate store causing credentials to be nulled out.

- **Installation** Changes

Added a check in the configuration wizard to ensure a second Azure SQL database cannot be created to help avoid inadvertent Azure costs being incurred and addressed a issue requiring access to the master database during configuration with Azure SQL.

- **API** Fixes

Fixed an issue where GET /Templates was returning incorrect values for UseAllowedRequesters and nothing for AllowedRequesters and EnrollmentFields.

- **API** Changes

PUT /CertificateStores/DiscoveryJob endpoint now sets the job as immediate when JobExecutionTimestamp is not provided.

- **Orchestrator Blueprints** Fixes

Fixed an error when manually applying a blueprint to an agent.

- **Certificate Metadata** Fixes

Fixed an issue with metadata history not being saved when updated via the API.

- **Security** Fixes

Addressed a security role permission that incorrectly disallowed Edit All on certificates.

- **Orchestrator** Fixes

Fixed an issue with the scripted installation of the Windows Agent not properly saving the configuration.

- **API** Fixes

Fixed an issue with setting the Java Agent password via the PUT CertificateStores/Password API call.

- **Auditing** Fixes

Fixed some issues with audit searching.

- **CA Synchronization** Fixes

Fixed an issue with the CA sync missing certificates if the CA database had deleted rows.

- **API** Changes & Improvements

Expanded permissions to the PUT Certificates/Collection API role so that administrator access is not required.

- **Certificate Search** Fixes

Fixed a UI issue with certificates searches returning revoked and expired certificates due to missing parenthesis in the query.

- **Orchestrator** Fixes

Fixed an issue with Mac Auto-enrollment failing.

- **Certificate** Changes & Improvements

Added the ability to expand the cert request ID information from the portal.

- **Expiration Alerts** Changes & Improvements

Added support in expiration alerts queries for '-includes' and '-notincludes' comparisons.

- **CRL Alerts** Fixes

Fixed an issue with removing a recipient from a CRL alert.

2.3.4 Incremental Release 8.4 Notes

January 2021



Note: Keyfactor Command 8.4 is a minor release with incremental fixes and updates following the Keyfactor Command 8 major release. For more details on new features, improvements, and known limitations in Keyfactor Command 8.0, please review the [Major Release 8.0 Notes on page 49](#).

New Features

- **Default Collections**

Certain default collections are now included with a new installation. These include:

- Certificates expiring in 7 days
- Revoked certificates
- Self-signed certificates
- Certificates with weak encryption



Note: Default collections are not included in upgrades.

- **Azure SQL Support in ACME**

Keyfactor ACME now natively supports Azure SQL.

Updates and Improvements

- **Enrollment** Fixes

Fixed an issue in which the PFX subject format from the application setting was not properly applied.

- **Dashboard** Fixes

A fix to the dashboard where the CRL panel is returning HTTP 404 errors.

- **Management Portal** Fixes

Custom banner widths are now fully supported and will not distort graphics.

2.3.5 Incremental Release 8.5 Notes

February 2021



Note: Keyfactor Command 8.5 is a minor release with incremental fixes and updates following the Keyfactor Command 8 major release. For more details on new features, improvements, and known limitations in Keyfactor Command 8.0, please review the [Major Release 8.0 Notes on page 49](#).

New Features

- **SAN Count**

The number of Subject Alternative Names (SANs) on a certificate is now available on the certificate details page as well as in the Full Certificate Extract Report.

Updates and Improvements

- **Orchestrator** Fixes

The F5 REST Orchestrator has been updated to address an issue with inventorying a store with more than 20 records.

- **Security** Fixes

Fixed an issue in which combining global and collection-level permissions for accounts resulted in an OutOfMemory exception.

- **Documentation** Changes & Improvements

The *Keyfactor Web APIs Reference Guide* is now available via the Management Portal.

- **Log Shipping** Changes & Improvements

Syslog is now supported over TLS for improved log shipping security.

- **Orchestrator** Changes

IAgentRegistrationHandler interface has been changed to IOrchestratorRegistrationHandler to provide for better namespace accuracy.

- **Active Directory** Fixes

Active Directory groups with an ampersand in the group name can now be used in Keyfactor Command security identities.

- **API** Changes & Improvements

An API endpoint has been added to the Keyfactor API to allow for deletion of a certificate from a certificate store.

- **Orchestrator** Changes & Improvements

The server name can be passed as a parameter to KeyfactorWindowsAgentConsoleConfig.exe to allow for more flexibility in scripted deployments.

- **Reporting** Changes & Improvements

The Full Certificate Extract Report now supports metadata parameters.

- **Reporting** Fixes

Fixed an issue with the Expiration Report not processing de-duplication correctly using the "Ignore renewed certificate results by" option set on the certificate collection.

Deprecation/Required Upgrades

- **Stale CRL Monitoring**

In a future version of Keyfactor Command, the CRL Stale monitoring will be replaced with letting customers define their own "Stale" by generating alerts—and log entries—off of the date that the CRL expires, rather than looking at the Next Publish date.

The main reason for that is that there is, by definition, a race condition between when the new CRL gets created (exactly at the Next Publish time), and when it is copied to the CRL distribution points. Basing alerts off CRL expiration allows customers to tune timeframes based on the way they handle their CRLs.

- **Verbosity in API Calls**

In a future version of Keyfactor Command, the Keyfactor API will return all data regardless of the verbosity level. For backwards compatibility where performance is concerned, verbosity will be honored when loading certificate location data in the certificate query but has been replaced with new flags to include this data for future requests.

2.3.6 Incremental Release 8.6 Notes

March 2021



Note: Keyfactor Command 8.6 is a minor release with incremental fixes and updates following the Keyfactor Command 8 major release. For more details on new features, improvements, and known limitations in Keyfactor Command 8.0, please review the [Major Release 8.0 Notes on page 49](#).

Updates and Improvements

- **Orchestrator** Changes & Improvements

Updates to Java Agent hostname support to allow for manual hostname entry.

- **Reporting** Changes & Improvements

Password encryption in the Logi Analytics configuration file.

- **Certificates** Fixes

Fixed an issue in saving certificate collections.

- **Certificates** Fixes

Fixed the issue in which searching for certificates by ECU was not working properly.

- **Auditing** Fixes

Modified audit logging to properly load certificate download operations.

- **SSL Discovery & Monitoring** Fixes

Corrected an issue in which SSL scan details could not be displayed if the associated schedule is not defined.

- **API** Fixes

Fixed an issue in which password regular expression validation was not enforced for API-based requests.

- **SSL Discovery & Monitoring** Fixes

Updated the SSL search parser to search all octets instead of only the first two.

- **Orchestrator** Fixes

Fixed an error in the Java Agent packaging in which the RPM and local did not build the correct commandline not providing the proper path.

2.3.7 Incremental Release 8.7 Notes

April 2021



Note: Keyfactor Command 8.7 is a minor release with incremental fixes and updates following the Keyfactor Command 8 major release. For more details on new features, improvements, and known limitations in Keyfactor Command 8.0, please review the [Major Release 8.0 Notes on page 49](#).

Updates and Improvements

- **Infrastructure** Changes

The SQL db_owner role is no longer required during operation of the Keyfactor Command platform.

- **Reporting** Changes & Improvements

A new report—Certificate Issuance Trends—is now available.

- **Management Portal** Fixes

Apostrophes are now permitted in Certificate Revocation Lists (CRL) display names.

- **Auditing** Changes & Improvements

Audit Syslog supports TLS 1.2.

- **Certificates** Fixes

Update to EV DigiCert renewal functionality to fix truncation of long Distinguished Names (DNs).

- **Security** Fixes

Fix so that Read permission on the System Settings is no longer required to edit certificate store containers.

- **Management Portal** Fixes

Fix to management portal data grids to prevent improper display when the last row is blocked by the scroll bar after resizing.

- **API** Fixes

Updated certificate store API endpoints to display them properly in the API endpoint utility (Swagger).

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. server-name.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 available 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. server-name.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.

Distinguished 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. server-name.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 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 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 certificate 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 certificate 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 certificate 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 certificate 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

User guides and related documentation from Keyfactor are subject to the copyright laws of the United States and other countries and are provided under a license agreement that restricts copying, disclosure, and use of such documentation. This documentation may not be disclosed, transferred, modified, or reproduced in any form, including electronic media, or transmitted or made publicly available by any means without the prior written consent of Keyfactor and no authorization is granted to make copies for such purposes.

Information described herein is furnished for general information only, is subject to change without notice, and should not be construed as a warranty or commitment by Keyfactor. Keyfactor assumes no responsibility or liability for any errors or inaccuracies that may appear in this document.

The software described in this document is provided under written license agreement, contains valuable trade secrets and proprietary information, and is protected by the copyright laws of the United States and other countries. It may not be copied or distributed in any form or medium, disclosed to third parties, or used in any manner not provided for in the software licenses agreement except with written prior approval from Keyfactor.