Hosted Keyfactor Command 10.2

Upgrade Overview

Table of Contents

1.0 Introduction

The Keyfactor Command solution by Keyfactor allows organizations to issue and manage certificates across enterprise infrastructures. For a comprehensive description of the components that make up Keyfactor Command, please see the *Keyfactor Command Server Installation Guide*[1] and the *Keyfactor Orchestrators Installation and Configuration Guide*[1]. There are also Keyfactor installation guides for third-party CA gateways that interface with Keyfactor Command. For an overview of the key new features in the latest version of Keyfactor Command, please see the *Keyfactor Command Release Notes*.

This document provides guidance to help you prepare for and complete an upgrade. The Keyfactor Command server software will be upgraded for you, and in most cases, a Keyfactor Solution Architect will assist you with the upgrade and walk you through the process. Please contact your Client Success representative for assistance.

[1]Embedded 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.

2.0 Upgrading

Most Keyfactor Command upgrades are brief with a minimum of changes to existing user accounts, groups, CA templates, firewall settings, etc. The prerequisites have not materially changed from previous versions and the current version can generally be installed using the same hardware and existing instances of the supporting software. The upgrade process is often completed within three to four hours, including the time spent by your Keyfactor representative to upgrade your hosted environment.

The overall task flow consists of the following steps:

Upgrade of the Server Software

The Keyfactor Command server software will be installed and configured for you. Once this is complete, you may upgrade any orchestrators and gateways in your environment.

Update Windows Orchestrators

If you're upgrading from a version of Keyfactor Command prior to 8.0, you will need to update any Windows Orchestrators (a.k.a. Windows Agents) that are used for SSL scanning to support the current scanning architecture. Install and configure the Keyfactor Universal Orchestrator software as per the *Keyfactor Orchestrators Installation and Configuration Guide*[1].

The Keyfactor Universal Orchestrator replaces the Keyfactor Windows Orchestrator and runs on both Windows or Linux servers. As of this release, the following functions that were part of the Keyfactor Windows Orchestrator are only supported in the Keyfactor Universal Orchestrator with custom extensions:

- Interact with F5 devices for certificate management (available now on the Keyfactor GitHub site)
- Interact with NetScaler devices for certificate management (coming soon to the Keyfactor GitHub site)
- Interact with Amazon Web Services (AWS) resources for certificate management (coming soon to the Keyfactor GitHub site)

The final release of the Keyfactor Windows Orchestrator was version 8.7. This version of the Keyfactor Windows Orchestrator is fully compatible with Keyfactor Command version 10.2. Keyfactor will continue to support the Keyfactor Windows Orchestrator. However, all new integrations and extensions will be delivered via the new Keyfactor Universal Orchestrator. Keyfactor recommends that customers use the Keyfactor Universal Orchestrator moving forward as new extensions become available. Customers with one or more of these types of certificate stores may wish to retain one or more legacy Keyfactor Windows Orchestrators to manage these types of stores until such time as new extensions become available for the Keyfactor Universal Orchestrator. Currently, to manage NetScaler and AWS certificate stores, an 8.x version of the Keyfactor Windows Orchestrator must be used. If you're upgrading from a version of Hosted Keyfactor Command prior to 8.0, contact your Keyfactor representative to obtain the installation media for the 8.7 Keyfactor Windows Orchestrator.

Important: The Keyfactor Universal Orchestrator is only compatible with Keyfactor Command version 9.0 or later. The current version of the Keyfactor Universal Orchestrator is 10.1 and requires .NET 6.

Note: The orchestrator endpoint location changed for Keyfactor Command release 6 and may need to be modified in your orchestrator endpoint configuration—from CMSAgents to KeyfactorAgents.

Cloud Gateway

The latest version of the Keyfactor Cloud Gateway—used to support management of certificates in the hosted Keyfactor Command environment—is 22.2 released in late 2022. If you are already using this version, no configuration changes need to be made. Restart the gateway service to refresh the connection to the upgraded Keyfactor Command instance.

If you're using a recent version of the gateway (20.6 or newer), you don't need to upgrade the gateway unless the gateway contains a change that's needed in your environment. Some changes introduced since release 20.6 include:

- Improvements to Active Directory group syncing to address issues with multi-domain environments, domain local groups, and timeouts with occasional high server load in larger or more complex Active Directory environments (20.7)
- Certificate requests submitted through the gateway that are configured to populate from Active Directory on the gateway side and that require manager approval on the CA side will now correctly include the Common Name passed up from the gateway in the Issued Common Name field, in addition to SAN values passed up from the gateway retrieved from Active Directory in the gateway environment (20.9).
- A sync timeout option has been added to allow you to adjust the timeout when the synchronization service attempts to send data to the cloud-based receiver (21.3).
- The gateway now supports enroll on behalf of functionality (21.3). When configured in this way, the Keyfactor Cloud Gateway allows a user with an enrollment agent certificate to enroll for a certificate on behalf of another user—so John requests a certificate for Martha. This type of functionality is often used when provisioning smart cards or similar technology.
- The Keyfactor Managed CA Gateway service and Keyfactor Managed CA Sync service can now be installed separately to allow different servers to handle these roles (21.3).
- The gateway now sends the ObjectSID to the managed CA to support the changes made to the Microsoft CA based on KB5014754 (22.2). For more information, see:

  https://support.microsoft.com/en-us/topic/kb5014754-certificate-based-authentication-changes-on-windows-domain-controllers-ad2c23b0-15d8-4340-a468-4d4f3b188f16

In most cases, the Keyfactor gateway software can be installed over the existing software installation without uninstalling the previous version. Review the configuration for your gateway, and then install and configure the software as per the *Keyfactor Cloud Gateway Installation & Configuration Guide*, retaining the same installation location.

EJBCA CA Gateway

If you're using an EJBCA gateway and wish to make use of the new feature in Keyfactor Command for native support of EJBCA CAs, you will need to follow the EJBCA gateway upgrade process to unlink the EJBCA certificates in your Keyfactor Command database from your EJBCA gateway CA to enable them to be relinked to a native CA configured in Keyfactor Command. For more information, contact Keyfactor support.

Other CA Gateways

In most cases, the Keyfactor gateway software can be installed over the existing software installation without uninstalling the previous version. Review the configuration for your gateway, and then install and configure the software as per the Keyfactor gateway guide for the particular gateway, retaining the same installation location. The gateway configuration wizard has significantly changed in recent releases for many of the gateways, which may require modification to your configuration.

Tip: New versions of CA gateways are not necessarily released at the same time as new versions of Keyfactor Command and so gateways may not need upgrading at the same time as Keyfactor Command.

API

Please see the *Release Notes*[1] if you are using any custom scripts that leverage one of the APIs.

Post-Install Configuration and Testing

See Post-Upgrade Steps on page 5

The bulk of the time upgrading will be spent verifying that all functions and configurations have correctly carried over and the upgraded instance is performing correctly.

3.0 Post-Upgrade Steps

There is no particular order in which the tasks on the following pages must be accomplished.

Tip: If, following the upgrade, you open a page in the Keyfactor Command Management Portal and find it unexpectedly blank or otherwise displaying incorrectly, try refreshing the page with a CTRL-F5. If this doesn't resolve the problem, try clearing the browser cache and then reloading the page. It may be helpful to advise all end users to do this following an upgrade.

3.1 Testing

Once everything is up and running again, confirm that the following features are operating correctly:

- Does the Keyfactor Command Management Portal load correctly?
- Run a report in the Keyfactor Command Management Portal to confirm that the connectivity to LogiAnalytics is operating correctly.
- Issue a certificate in the Keyfactor Command Management Portal to confirm connectivity to CAs and that authentication is operating correctly.

3.2 Post-Install Configuration

If you are upgrading from any release of Keyfactor Command version 6 or greater, you may want to make some additional configuration changes post-installation:

- Upgrade any Keyfactor CA gateways in your environment that are based on the AnyGateway. The AnyGateway must be upgraded to at least 22.1 to be compatible with Keyfactor Command 10.0 and later.
- Consider whether you wish to implement Keyfactor Command workflows and whether a Keyfactor Command-level workflow could replace CA-level manager approval for any templates that are configured to require CA-level manager approval.
- Review the new enrollment default and policy settings for enrollment. Enrollment defaults and polices can be defined at two levels:
    - System-wide settings apply to all enrollments done through Keyfactor Command unless they are over-ridden by template-specific settings.
    - Template-level settings allow you to modify any established enrollment defaults or policies on a per-template basis.

  There are several settings available for configuration as part of the template policies:
    - Allow Wildcards
    - Allow Public Key Reuse

- Enforce RFC 2818 Compliance
- Supported Key Types

  Enrollment defaults allow you to pre-polulate the subject fields in PFX Enrollment and CSR Generation. Users are allowed to override these at enrollment.

- If you're using certificate metadata or regular expressions, optionally define these for each template. Certificate metadata fields and regular expressions can be defined at two levels:
  - System-wide settings apply to all enrollments done through Keyfactor Command unless they are overridden by template-specific settings.
  - Template-level settings allow you to modify any established certificate metadata or regular expressions on a per-template basis (for instance, for a metadata field, whether the field is required, what default value it should provide, or whether to hide the field during enrollment, regardless of system-wide setting).
- The enrollment configuration will have been carried over in the upgrade, however you may want to confirm the configuration of Certificate Authority and Template enrollment (PFX, CSR, and CSR generation) and make any changes.
- Review any template that is configured to require manager approval at the CA level and confirm that a Keyfactor Command private key retention policy in place.
- Review the new reports in the Keyfactor Command Report Manager and add them to the menu or favorite them, if desired.

4.0 Copyright Notice