Cisco Secure Workload Upgrade Guide

First Published: 2021-10-29

Last Modified: 2024-04-09

Supported Upgrade Paths for Cisco Secure Workload

Table 1: Supported Upgrade Paths for Secure Workload

From	To	Upgrade Type
3.9.1.10 3.9.1.1	3.9.1.25	Patch upgrade
3.9.1.1	3.9.1.10	Patch upgrade
3.8.1.39 3.8.1.36 3.8.1.19 3.8.1.1	3.9.1.1	Major release upgrade
3.8.1.39 3.8.1.36 3.8.1.19 3.8.1.1	3.8.1.44	Patch upgrade
3.8.1.36 3.8.1.19 3.8.1.1	3.8.1.39	Patch upgrade
3.8.1.19 3.8.1.1	3.8.1.36	Patch upgrade
3.8.1.1	3.8.1.19	Patch upgrade
3.7.1.59 3.7.1.51 3.7.1.39	3.8.1.1	Major release upgrade

From	To	Upgrade Type
3.7.1.51 3.7.1.39 3.7.1.22 3.7.1.5	3.7.1.59	Patch upgrade
3.7.1.39 3.7.1.22 3.7.1.5	3.7.1.51	Patch upgrade
3.7.1.22 3.7.1.5	3.7.1.39	Patch upgrade
3.7.1.5	3.7.1.22	Patch upgrade
3.6.x	3.7.1.5	Major release upgrade
3.6.1.x	Any later 3.6 patch	Patch upgrade
3.5.1.x (Tetration branding)	3.6.1.5	Major release upgrade
Versions earlier than 3.6.	Any version earlier than 3.6. See specifics in the *Cisco Tetration Upgrade Guide*, available here.	–

Requirements and Limitations for Dual-Stack Mode (IPv6 Support)

Secure Workload clusters running on physical hardware can be configured to use IPv6 in addition to IPv4 for certain communications to and from the cluster.

Note

- You can use the Dual-Stack Mode (IPv6 support) feature when installing or upgrading to 3.6.1.5, 3.7.1.5, 3.8.1.1, and 3.9.1.1 releases. However, the option to enable the feature is not available when you are installing or upgrading to patch releases.
- Agents communicate with the cluster using IPv4 unless you configure them to use IPv6. For more information, see Cisco Secure Workload User Guide.

Limitations

If you are considering enabling dual stack mode, note the following:

- You can enable IPv6 connectivity only during initial deployment or upgrade to a major release (you cannot enable this feature during patch upgrades).
- Dual-stack mode is supported only on physical hardware or bare metal clusters.

- There is no support for IPv6-only mode.
- You cannot revert to IPv4-only mode after dual stack mode is enabled for the cluster.
- (Applicable for releases 3.8 and earlier) Data Backup and Restore (DBR) is not supported if dual-stack connectivity is enabled.
- Do not enable dual-stack mode for clusters that are configured with Federation.
- The following features always and only use IPv4 (note that IPv4 is always enabled even if IPv6 is enabled):
  - (Applicable for releases 3.9.1.1, 3.8.1.1, 3.7.1.5, and 3.6.x) Enforcement on AIX agents
  - (Applicable only for release 3.6.x) Hardware agent communication with the cluster
  - (Applicable only for release 3.6.x) Connectors for flow ingestion, inventory enrichment, or alert notifications

Requirements

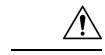
- Configure both A and AAAA DNS records for FQDN before enabling dual stack mode for your cluster.
- External services such as NTP, SMTP, and DNS must be available over both IPv4 and IPv6, for redundancy purposes.
- To configure dual stack mode for a cluster:
  - Each of the two cluster leaf switches must be allocated routable IPv6 addresses on two different networks, for redundancy, and default gateways must be provided for each network.
  - For 39RU clusters, a site routable IPv6 network with space for at least 29 host addresses is required.
  - For 8RU clusters, a site routable IPv6 network with space for at least 20 host addresses is required.
  - The first three host addresses of the site routable IPv6 network are reserved for the Cisco Secure Workload cluster HSRP configuration and must not be used by any other devices.

Upgrade to Secure Workload Release 3.9.x

Upgrade to Secure Workload Release 3.9.1.25

You can upgrade to this release from the 3.9.1.1 or 3.9.1.10 releases.

Before you begin



Caution Do not upgrade if any nodes are currently in a decommissioned state or any services are unhealthy. Contact the Cisco Technical Assistance Center (TAC) to remediate any issues before continuing.

- Download the installer package:

  In your browser, go to https://software.cisco.com/download/home/286309796/type/286309874/release/3.9.1.25.

  Download the following RPM: `tetration_os_patch_k9-3.9.1.25-1.noarch.rpm`

- Ensure that a **Customer Support** level account has an SSH key that is uploaded for troubleshooting purposes.
- You must perform the following procedure as a user with Site Administrator or Customer Support privileges.
- Google Chrome and Microsoft Edge are the supported browsers for upgrade.

Procedure

Step 1 Check the system's health. You cannot perform the upgrade if a service is unhealthy.

a) On the Secure Workload UI, from the navigation pane, choose **Troubleshoot** > **Service Status**.
b) Look for red circles in the graph, which indicate unhealthy services.

Alternatively, to see a table view of service health, click the list button at the top of the graph, click **Expand All**, and scroll down the page to view the status of all the services.

c) If a service is unhealthy, perform the necessary fix to render the service healthy before you proceed with the upgrade.

Step 2 From the navigation pane, choose **Platform** > **Upgrade/Reboot/Shutdown**.

Step 3 Follow the on screen instructions.

Troubleshoot issues, if any, identified by the prechecks before continuing.

Ensure that **Patch Upgrade** is selected. (This is a patch upgrade.)

Click **Send Upgrade Link**.

Step 4 Look for an email message with the following subject:

```
[Tetration][<cluster_name>] Patch Upgrade Initiation Link
```

This message includes a hyperlink that you must use to perform the upgrade.

Step 5 In the email message, click the **Patch Upgrade <Cluster>** link to open the Secure Workload Setup UI.

Step 6 Click **Choose File**.

Step 7 Select the downloaded patch RPM and click **Open**.

Step 8 Click **Upload**.

Uploading the RPM initiates the upgrade.

During this process, you will temporarily lose connectivity to the setup UI.

Step 9 Wait for a few minutes to regain access to the UI to view the upgrade results.

If there is a problem with the upgrade, a red banner is displayed. Click the book image to view the logs.

Step 10 Verify the upgrade:

a) Open the Secure Workload UI in your browser.
b) In the navigation pane, click **Platform > Upgrade/Reboot/Shutdown**.
c) Click **History**.
d) Verify that the status under the **Status** column is **Succeeded**.

Step 11 If the upgrade is successful, click **Disable Patch Upgrade Link**.

Upgrade to Secure Workload Release 3.9.1.10

You can upgrade to this release from the 3.9.1.1 release.

Before you begin

Caution Do not upgrade if any nodes are currently in a decommissioned state or any services are unhealthy. Contact the Cisco Technical Assistance Center (TAC) to remediate any issues before continuing.

- Download the installer package:

  In your browser, go to https://software.cisco.com/download/home/286309796/type/286309874/release/3.9.1.10.

  Download the following RPM: `tetration_os_patch_k9-3.9.1.10-1.noarch.rpm`
- Ensure that a **Customer Support** level account has an SSH key that is uploaded for troubleshooting purposes.
- You must perform the following procedure as a user with Site Administrator or Customer Support privileges.
- Google Chrome and Microsoft Edge are the supported browsers for upgrade.

Procedure

Step 1 Check the system's health. You cannot perform the upgrade if a service is unhealthy.

a) On the Secure Workload UI, from the navigation pane, choose **Troubleshoot** > **Service Status**.

b) Look for red circles in the graph, which indicate unhealthy services.

Alternatively, to see a table view of service health, click the list button at the top of the graph, click **Expand All**, and scroll down the page to view the status of all the services.

c) If a service is unhealthy, perform the necessary fix to render the service healthy before you proceed with the upgrade.

Step 2 From the navigation pane, choose **Platform** > **Upgrade/Reboot/Shutdown**.

Step 3 Follow the on screen instructions.

Troubleshoot issues, if any, identified by the prechecks before continuing.

Ensure that **Patch Upgrade** is selected. (This is a patch upgrade.)

Click **Send Upgrade Link**.

Step 4 Look for an email message with the following subject:

`[Tetration][<cluster_name>] Patch Upgrade Initiation Link`

This message includes a hyperlink that you must use to perform the upgrade.

Step 5 In the email message, click the **Patch Upgrade <Cluster>** link to open the Secure Workload Setup UI.

Step 6 Click **Choose File**.

Step 7 Select the downloaded patch RPM and click **Open**.

Step 8 Click **Upload**.

Uploading the RPM initiates the upgrade.

During this process, you will temporarily lose connectivity to the setup UI.

Step 9 Wait for a few minutes to regain access to the UI to view the upgrade results.

If there is a problem with the upgrade, a red banner is displayed. Click the book image to view the logs.

Step 10 Verify the upgrade:

a) Open the Secure Workload UI in your browser.
b) In the navigation pane, click **Platform > Upgrade/Reboot/Shutdown**.
c) Click **History**.
d) Verify that the status under the **Status** column is **Succeeded**.

Step 11 If the upgrade is successful, click **Disable Patch Upgrade Link**.

Upgrade to Secure Workload Release 3.9.1.1

You can upgrade to this release from any 3.8 release. However, we recommend that you upgrade to the latest 3.8.1.x patch release before upgrading to this release.

Before you begin

Caution Do not upgrade if any of the nodes are in a decommissioned state or if any of the services are unhealthy. Contact the Cisco Technical Assistance Center (TAC) to remediate any issues before continuing.

- Kubernetes AKS external orchestrators—After the upgrade, AKS external orchestrators will be read-only; if you want to make changes after the upgrade, create a new Azure connector, and enable the **Managed Kubernetes services** option.
- FMC external orchestrators—After the upgrade, FMC external orchestrators are migrated to connectors.
- Ensure that a *Customer Support* level account has an SSH key that is uploaded for troubleshooting purposes.
- You must perform the following procedure as a user with Site Administrator or Customer Support privileges.
- Google Chrome and Microsoft Edge are the supported browsers for the upgrade.
- If ISE connectors are configured, verify that their TLS certificates have Subject Alternative Name (SAN) sections. After the upgrade, the ISE connector will not connect to ISE endpoints that present legacy CN-only TLS certificates. Do not proceed with the upgrade before the ISE TLS certificates are regenerated with SAN extensions.
- **Licensing**

- If your Secure Workload deployment does not have valid Cisco Smart Licenses (or is outside the evaluation period), you must register valid licenses before you upgrade.
- Site Administration privileges are required to manage licenses.
- To view the status of your licenses: In the Cisco Secure Workload UI, choose **Manage** > **Service Settings** > **Licenses**. If your cluster license registration is out of compliance, you see a banner on the UI. For information about obtaining and registering licenses, in the Secure Workload UI, choose **Help** > **Page-level Help** and search for Smart Licensing.

Procedure

Step 1 Go to https://software.cisco.com/download/home/286309796/type and download the applicable RPM files for your deployment.

- For an 8-RU or 39-RU system, download the following RPMs:
  - tetration_os_UcsFirmware_k9-3.9.1.1-1.x86_64.rpm
  - tetration_os_base_rpm_k9-3.9.1.1-1.el7.x86_64.rpm
  - tetration_os_adhoc_k9-3.9.1.1-1.el6.x86_64.rpm
  - tetration_os_mother_rpm_k9-3.9.1.1-1.el6.x86_64.rpm
  - tetration_os_rpminstall_k9-3.9.1.1-1.noarch.rpm
  - tetration_os_enforcement_k9-3.9.1.1-1.el6.x86_64.rpm
  - tetration_os_nxos_k9-3.9.1.1-1.x86_64.rpm
- For a virtual system, download the following RPMs:
  - tetration_os_ova_k9-3.9.1.1-1.noarch.rpm
  - tetration_os_adhoc_k9-3.9.1.1-1.el6.x86_64.rpm
  - tetration_os_mother_rpm_k9-3.9.1.1-1.el6.x86_64.rpm
  - tetration_os_rpminstall_k9-3.9.1.1-1.noarch.rpm
  - tetration_os_enforcement_k9-3.9.1.1-5.el6.x86_64.rpm

Step 2 Verify that the MD5 checksum of the downloaded RPMs matches the MD5 checksum on Cisco.com.

Step 3 Check the system's health. You cannot perform the upgrade if a service is unhealthy.

a) On the Secure Workload UI, from the navigation pane, choose **Troubleshoot** > **Service Status**.

b) Look for red circles in the graph, which indicate unhealthy services.

Alternatively, to see a table view of service health, click the list button at the top of the graph, click **Expand All**, and scroll down the page to view the status of all the services.

c) If a service is unhealthy, perform the necessary fix to render the service healthy before you proceed with the upgrade.

Step 4 A snapshot of the cluster helps in troubleshooting issues, if any, during the upgrade. From the navigation pane, choose **Troubleshoot** > **Snapshots** > **Create Snapshot** > **Classic Snapshot**.

a) Do not change the default settings.
b) In the **Comments** field, enter comments about the snapshot.
c) Click **Create Snapshot**.

Step 5 From the navigation pane, choose **Platform** > **Upgrade/Reboot/Shutdown**.

Step 6 Under the **Upgrade** tab, follow the on-screen instructions. Ensure that you do not skip any of the steps.

Note Under **Select Operation**, choose **Upgrade** for this upgrade. *Do not* choose the **Patch Upgrade** option.

Step 7 Click **Send Upgrade Link**.

The logged-in site administrator or customer support user receive an email with the following subject:

```
[Tetration Analytics] Upgrade Initiation Link
```

Step 8 Click the link that is received in the email. Alternatively, you can fetch the upgrade URL by navigating to **Troubleshoot** > **Maintenance Explorer** and entering the following information:

- Snapshot Action: **POST**
- Snapshot Host: **orchestrator.service.consul**
- Snapshot Path: **upgrade_url**

Note Google Chrome and Microsoft Edge are the supported web browsers for this upgrade.

The Cisco Secure Workload Setup portal is displayed.

Step 9 In the Cisco Secure Workload Setup portal, upload the RPM files:

a) Click **Choose File**.
b) Navigate and select **tetration_os_rpminstall_k9-3.9.1.1-1.noarch.rpm**, and click **Open**.
c) Click **Upload**.
d) After the **tetration_os_rpminstall_k9-3.9.1.1-1.noarch.rpm** file is successfully uploaded, click **Install**. After the **tetration_os_rpminstall_k9-3.9.1.1-1.noarch.rpm** file is installed, the dependent RPM files are loaded and these RPM files can be staged for deployment. You can view the versions of the currently deployed RPM file and the staged RPM file.
e) Repeat steps **a** to **c** for the dependent RPM files based on your cluster deployment. See Step 1 for the list of RPM files.
The list of RPM files on the page does not get updated as you upload each RPM file. This is expected behavior. If you see an error after uploading the **tetration_os_mother_rpm_k9-3.9.1.1-1.el6.x86_64.rpm** file, wait for five to 10 minutes and then reload the page. You should now be able to view the list of uploaded RPMs.

Note If you are upgrading to this release from 3.8.1.1, upload the RPM files in the following order. After uploading the **tetration_os_mother_rpm_k9-3.9.1.1-1.el6.x86_64.rpm** file, the page gets refreshed, and you will notice that the uploaded RPM files are staged. You can now upload the other RPM files.

- For an 8-RU or 39-RU system:
  a. tetration_os_rpminstall_k9-3.9.1.1-1.noarch.rpm
  b. tetration_os_UcsFirmware_k9-3.9.1.1-1.x86_64.rpm
  c. tetration_os_nxos_k9-3.9.1.1-1.x86_64.rpm
  d. tetration_os_adhoc_k9-3.9.1.1-1.el6.x86_64.rpm
  e. tetration_os_mother_rpm_k9-3.9.1.1-1.el6.x86_64.rpm
- For a virtual system:
  a. tetration_os_rpminstall_k9-3.9.1.1-1.noarch.rpm
  b. tetration_os_adhoc_k9-3.9.1.1-1.el6.x86_64.rpm
  c. tetration_os_mother_rpm_k9-3.9.1.1-1.el6.x86_64.rpm

The rows that are highlighted in green indicate that the RPMs are successfully uploaded. If there are any issues, click **Status** to view the log.

Step 10 Click **Install** to deploy the RPM files.

Step 11 Click **Continue**.
The **Site Config** portal is displayed.

Note From Secure Workload Release 3.8 and later, non-ASCII characters cannot be entered in any of the text fields for site configurations using the Cisco Secure Workload Setup UI.

Step 12 (Optional) Under **General**, change the SSH public key and click **Next**.

Step 13 (Optional) Under **Email**, change the UI admin or the admin email address and click **Next**.

Step 14 (Optional) Under **L3**, enable the cluster to use IPv6 addresses in addition to IPv4 for certain cluster connectivity after the upgrade. To enable IPv6:

a) Check the **IPv6** check box.
b) Enter IPv6 addresses in CIDR notation for both Leaf 1 and Leaf 2 switches.
c) Enter the Leaf1 and Leaf2 IPv6 Default Gateway.
d) Click **Next**.

If you enable IPv6 on this page, you must also configure IPv6 fields on the **Network** page, described in Step 15.

For requirements and limitations on dual stack mode, see Requirements and Limitations for Dual-Stack Mode (IPv6 Support), on page 2.

Step 15 Under **Network**:

a) If necessary, change the values for **CIMC Internal Network**, **CIMC Internal Network Gateway**, **DNS Resolver**, and **DNS Domain**.

Note Do not change or remove the existing **External Network** value. However, you can add more IPv4 networks.

b) If you enabled IPv6 on the L3 page, the **IPv6** check box is automatically selected. Specify IPv6 addresses that are reserved for Secure Workload use by performing these tasks:

1. Enter the IPv6 External Network in CIDR notation.
2. (Optional) To use IPv6 only for specified addresses, enter individual External IPv6 IPs.

Note
- The first three IPv6 addresses in the **IPv6 External Network** field are always reserved for the switches of the Secure Workload cluster and should not be used for any other purpose.
- For a 39-RU cluster, ensure that at least 29 IPv6 addresses are available in the IPv6 External Network or the External IPv6 IPs list.
- For an 8-RU cluster, ensure that at least 20 IPv6 addresses are available in the IPv6 External Network or the External IPv6 IPs list.

c) Click **Next**.

Step 16 (Optional) Under **Service**, change the existing NTP and SMTP values and click **Next**.

Step 17 Under **Security**, enable or disable **Strong SSL Ciphers for Agent Connections** and click **Next**.

Note You cannot change the values under the **UI**, **Advanced**, and **Recovery** tabs.

Under **Recovery**, if the cluster is configured to be a standby cluster, the cluster deploys in standby mode which includes reduced functionality (supporting only warm standby mode).

Step 18 Click **Continue**.
During the upgrade process, Secure Workload runs certain validation tasks to ensure:

- The RPM versions are correct.
- The cluster is healthy.
- The site information that you provided is valid.
- The switches are configured correctly and can be upgraded to a newer version of NX-OS software.
- The information fields are validated.
- The NTP is synchronized before deployment starts.
- The name node and secondary name node are not in a failed-over state.

The checks can take several minutes to an hour if the cluster switches must be upgraded. After the checks are complete, you will receive an email with the subject: `TETRATION CLUSTER MyCluster: Verify Token` . The message contains a token that you need to continue the upgrade. Copy the token from this email.

Step 19 In the Cisco Secure Workload Setup portal, paste the token into the **Validation Token** field and click **Continue**.

Note Do not check the **Ignore instance stop failures** check box unless instructed to do so by Cisco TAC.

The upgrade process is initiated. In 3.9.1.1, 3.8.1.1, and 3.7.1.5 releases, the orchestrator VMs upgrade before the rest of the components. This can take between 30 to 60 minutes, during which the progress bar goes from 0 to 100 percent. After the upgrades to the orchestrators are completed, the rest of the components will be upgraded and the progress bar will start over at 0 percent. When the green progress bar reaches 100 percent, it means that the upgrade is complete. All the instances display the **Deployed** status.

Step 20 Verify the upgrade:

a) Open the Secure Workload UI in your browser.
b) From the navigation pane, choose **Platform > Upgrade/Reboot/Shutdown**.
c) Click **History**.
d) Verify that the status under the **Status** column is **Succeeded**.

What to do next

After upgrading, make changes to benefit from enhancements in this release:

- If you have enabled IPv6, you can access the Secure Workload UI by using either IPv4 or IPv6 address. By default, agents continue to connect to the cluster using IPv4. If you want software agents to be able to communicate with the cluster using IPv6:
  1. From the navigation pane, choose **Platform** > **Cluster Configuration**.
  2. Configure the **Sensor VIP FQDN** setting as described in Cisco Secure Workload User Guide.
- For improved clustering of plain-vanilla Kubernetes workloads within scopes, see Upgrades to Releases 3.9, 3.8, and 3.7: Enabling Improved Clustering of Kubernetes Workloads in Policy Discovery, on page 30.

Upgrade to Secure Workload Release 3.8.x

Upgrade to Secure Workload Release 3.8.1.39

You can upgrade to this release from the 3.8.1.1, 3.8.1.19, or 3.8.1.36 releases.

Before you begin

Caution Do not upgrade if any nodes are currently in a decommissioned state or any services are unhealthy. Contact the Cisco Technical Assistance Center (TAC) to remediate any issues before continuing.

- Download the installer package:

  In your browser, go to https://software.cisco.com/download/home/286309796/type/286309874/release/3.8.1.39.

  Download the following RPM: `tetration_os_patch_k9-3.8.1.39-1.noarch.rpm`
- Ensure that a **Customer Support** level account has an SSH key that is uploaded for troubleshooting purposes.

- You must perform the following procedure as a user with Site Administrator or Customer Support privileges.
- Google Chrome and Microsoft Edge are the supported browsers for upgrade.

Procedure

Step 1 Check system health. You cannot perform the upgrade if any services are unhealthy.

a) On the Secure Workload UI, from the navigation pane, choose **Troubleshoot** > **Service Status**.

b) Look for red circles in the graph, which indicate unhealthy services.

Alternatively, to see a table view of service health, click the list button at the top of the graph, click **Expand All**, and scroll down the page to view the status of all services.

c) If any services are unhealthy, perform any necessary fixes to make the services healthy before you proceed with the upgrade.

Step 2 From the navigation pane, choose **Platform** > **Upgrade/Reboot/Shutdown**.

Step 3 Follow the on screen instructions.

Troubleshoot any issues identified by the precheck before continuing.

Ensure that **Patch Upgrade** is selected. (This is a patch upgrade.)

Click **Send Upgrade Link**.

Step 4 Look for an email message with the following subject:

```
[Tetration][<cluster_name>] Patch Upgrade Initiation Link
```

This message includes a hyperlink that you must use to perform the upgrade.

Step 5 In the email message, click the **Patch Upgrade <Cluster>** link to open the Secure Workload Setup UI.

Step 6 Click **Choose File**.

Step 7 Select the downloaded patch RPM and click **Open**.

Step 8 Click **Upload**.

Uploading the RPM initiates the upgrade.

During this process, you will temporarily lose connectivity to the setup UI.

Step 9 Wait for a few minutes to regain access to the UI and view the upgrade results.

If there is a problem with the upgrade, a red banner is displayed. Click the book image to view the logs.

Step 10 Verify the upgrade:

a) Open the Secure Workload UI in your browser.

b) In the navigation pane, click **Platform > Upgrade/Reboot/Shutdown**.

c) Click **History**.

d) Verify that the Status column shows **Succeeded**.

Step 11 If the upgrade is successful, click **Disable Patch Upgrade Link**.

Upgrade to Secure Workload Release 3.8.1.36

You can upgrade to this release from the 3.8.1.1 or 3.8.1.19 release.

Before you begin

Caution Do not upgrade if any nodes are currently in a decommissioned state or any services are unhealthy. Contact the Cisco Technical Assistance Center (TAC) to remediate any issues before continuing.

- Download the installer package:

  In your browser, go to https://software.cisco.com/download/home/286309796/type/286309874/release/3.8.1.36.

  Download the following RPM: `tetration_os_patch_k9-3.8.1.36-1.noarch.rpm`
- Ensure that a **Customer Support** level account has an SSH key that is uploaded for troubleshooting purposes.
- You must perform the following procedure as a user with Site Administrator or Customer Support privileges.
- Google Chrome and Microsoft Edge are the supported browsers for upgrade.

Procedure

Step 1 Check system health. You cannot perform the upgrade if any services are unhealthy.

a) On the Secure Workload UI, from the navigation pane, choose **Troubleshoot** > **Service Status**.

b) Look for red circles in the graph, which indicate unhealthy services.

Alternatively, to see a table view of service health, click the list button at the top of the graph, click **Expand All**, and scroll down the page to view the status of all services.

c) If any services are unhealthy, perform any necessary fixes to make the services healthy before you proceed with the upgrade.

Step 2 From the navigation pane, choose **Platform** > **Upgrade/Reboot/Shutdown**.

Step 3 Follow the on screen instructions.

Troubleshoot any issues identified by the precheck before continuing.

Ensure that **Patch Upgrade** is selected. (This is a patch upgrade.)

Click **Send Upgrade Link**.

Step 4 Look for an email message with the following subject:

`[Tetration][<cluster_name>] Patch Upgrade Initiation Link`

This message includes a hyperlink that you must use to perform the upgrade.

Step 5 In the email message, click the **Patch Upgrade <Cluster>** link to open the Secure Workload Setup UI.

Step 6 Click **Choose File**.

Step 7 Select the downloaded patch RPM and click **Open**.

Step 8 Click **Upload**.

Uploading the RPM initiates the upgrade.

During this process, you will temporarily lose connectivity to the setup UI.

Step 9 Wait for a few minutes to regain access to the UI and view the upgrade results.

If there is a problem with the upgrade, a red banner is displayed. Click the book image to view the logs.

Step 10 Verify the upgrade:

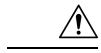
a) Open the Secure Workload UI in your browser.
b) In the navigation pane, click **Platform > Upgrade/Reboot/Shutdown**.
c) Click **History**.
d) Verify that the Status column shows **Succeeded**.

Step 11 If the upgrade is successful, click **Disable Patch Upgrade Link**.

Upgrade to Secure Workload Release 3.8.1.19

You can upgrade to this release from the 3.8.1.1 release.

Before you begin



Caution Do not upgrade if any nodes are currently in a decommissioned state or any services are unhealthy. Contact the Cisco Technical Assistance Center (TAC) to remediate any issues before continuing.

- Download the installer package:

  In your browser, go to https://software.cisco.com/download/home/286309796/type/286309874/release/3.8.1.19.

  Download the following RPM: `tetration_os_patch_k9-3.8.1.19-1.noarch.rpm`

- Ensure that a **Customer Support** level account has an SSH key that is uploaded for troubleshooting purposes.
- You must perform the following procedure as a user with Site Administrator or Customer Support privileges.
- Google Chrome and Microsoft Edge are the supported browsers for upgrade.

Procedure

Step 1 Check system health. You cannot perform the upgrade if any services are unhealthy.

a) On the Secure Workload UI, from the navigation pane, choose **Troubleshoot** > **Service Status**.
b) Look for red circles in the graph, which indicate unhealthy services.

Alternatively, to see a table view of service health, click the list button at the top of the graph, click **Expand All**, and scroll down the page to view the status of all services.

c) If any services are unhealthy, perform any necessary fixes to make the services healthy before you proceed with the upgrade.

Step 2 From the navigation pane, choose **Platform** > **Upgrade/Reboot/Shutdown**.

Step 3 Follow the on screen instructions.

Troubleshoot any issues identified by the precheck before continuing.

Ensure that **Patch Upgrade** is selected. (This is a patch upgrade.)

Click **Send Upgrade Link**.

Step 4 Look for an email message with the following subject:

```
[Tetration][<cluster_name>] Patch Upgrade Initiation Link
```

This message includes a hyperlink that you must use to perform the upgrade.

Step 5 In the email message, click the **Patch Upgrade <Cluster>** link to open the Secure Workload Setup UI.

Step 6 Click **Choose File**.

Step 7 Select the downloaded patch RPM and click **Open**.

Step 8 Click **Upload**.

Uploading the RPM initiates the upgrade.

During this process, you will temporarily lose connectivity to the setup UI.

Step 9 Wait for a few minutes to regain access to the UI and view the upgrade results.

If there is a problem with the upgrade, a red banner is displayed. Click the book image to view the logs.

Step 10 Verify the upgrade:

a) Open the Secure Workload UI in your browser.
b) In the navigation pane, click **Platform > Upgrade/Reboot/Shutdown**.
c) Click **History**.
d) Verify that the Status column shows **Succeeded**.

Step 11 If the upgrade is successful, click **Disable Patch Upgrade Link**.

Upgrade to Secure Workload Release 3.8.1.1

You must upgrade to the latest 3.7.1.x patch release before upgrading to this release.

Before you begin

⚠

Caution Do not upgrade if any nodes are currently in a decommissioned state or any services are unhealthy. Contact the Cisco Technical Assistance Center (TAC) to remediate any issues before continuing.

Keep these points in mind:

- Kubernetes AKS external orchestrators—After the upgrade, AKS external orchestrators will be read-only; if you want to make changes after the upgrade, create a new Azure connector and enable the **Managed Kubernetes services** option.

- FMC external orchestrators—After the upgrade, FMC external orchestrators are migrated to connectors.
- Ensure that a "Customer Support" level account has an SSH key uploaded for troubleshooting purposes.
- You must perform the following procedure as a user with Site Administrator or Customer Support privileges.
- Google Chrome and Microsoft Edge are the supported browsers for the upgrade.
- If ISE connectors are configured, verify that their TLS certificates have Subject Alternative Name (SAN) sections. After the upgrade, the ISE connector will not connect to ISE endpoints that present legacy CN-only TLS certificates. Do not proceed with the upgrade before the ISE TLS certificates are regenerated with SAN extensions.
- **Licensing**
  - If your Secure Workload deployment does not currently have valid Cisco Smart Licenses (or is outside the evaluation period), you must register valid licenses before you upgrade.
  - Site Administration privileges are required to manage licenses.
  - To view the status of your licenses: In the Cisco Secure Workload web portal, choose **Manage** > **Service Settings** > **Licenses**. If your cluster license registration is out of compliance, you will see a banner on the UI. For information about obtaining and registering licenses, in the Secure Workload web portal, select **Help** > **Page-level Help** and search for Smart Licensing.

Procedure

Step 1 Download the applicable RPM files for your deployment from Cisco.com:

a) Go to https://software.cisco.com/download/home/286309796/type.

b) Download as appropriate:

- For an 8-RU or 39-RU system, download the following RPMs:
  - tetration_os_UcsFirmware_k9-3.8.1.1-1.x86_64.rpm
  - tetration_os_base_rpm_k9-3.8.1.1-1.el7.x86_64.rpm
  - tetration_os_adhoc_k9-3.8.1.1-1.el6.x86_64.rpm
  - tetration_os_mother_rpm_k9-3.8.1.1-1.el6.x86_64.rpm
  - tetration_os_rpminstall_k9-3.8.1.1-1.noarch.rpm
  - tetration_os_enforcement_k9-3.8.1.1-1.el6.x86_64.rpm
  - tetration_os_nxos_k9-3.8.1.1-1.x86_64.rpm
- For a virtual system, download the following RPMs:
  - tetration_os_ova_k9-3.8.1.1-1.noarch.rpm
  - tetration_os_adhoc_k9-3.8.1.1-1.el6.x86_64.rpm
  - tetration_os_mother_rpm_k9-3.8.1.1-1.el6.x86_64.rpm
  - tetration_os_rpminstall_k9-3.8.1.1-1.noarch.rpm

- tetration_os_enforcement_k9-3.8.1.1-5.el6.x86_64.rpm

c) Verify the MD5 checksum of the downloaded RPMs matches the MD5 checksum in CCO.

Step 2 Check system health. You cannot perform the upgrade if any services are unhealthy.

a) On the Secure Workload UI, from the navigation pane, choose **Troubleshoot** > **Service Status**.
b) Look for red circles in the graph which indicate unhealthy services.

Alternatively, to see a table view of service health, click the list button at the top of the graph, click **Expand All** and scroll down the page to view status of all services.

c) If any services are unhealthy, perform any necessary fixes to make the services healthy before you proceed with the upgrade.

Step 3 From the left navigation pane, choose **Platform** > **Upgrade/Reboot/Shutdown**.

Step 4 Under the **Upgrade** tab, follow the instructions displayed on the screen. Ensure that you do not skip any of the steps.

Note Under **Select Operation**, choose **Upgrade**. DO NOT choose the Patch Upgrade option.

Step 5 Click **Send Upgrade Link**.

A user logged in with the site administrator or customer support role will receive an email with a hyperlink that must be used to perform the upgrade. The subject of the email will be:

```
[Tetration Analytics] Upgrade Initiation Link
```

Open the email and copy the **Upgrade Cluster** URL.

Alternatively, you can fetch the upgrade URL by clicking **Troubleshoot** > **Maintenance Explorer** and entering the following information:

- Snapshot Action: **POST**
- Snapshot Host: **orchestrator.service.consul**
- Snapshot Path: **upgrade_url**

Step 6 In the browser, paste the upgrade URL into the address field and press **Enter**.

The Cisco Secure Workload Setup portal is displayed. Note that Google Chrome and Microsoft Edge are the supported web browsers for the upgrade.

Step 7 In the Cisco Secure Workload Setup portal, you must upload the RPMs in a specific order depending on your setup. To upload the RPM files, perform the following actions:

a) Click **Choose File**.
b) Navigate and select a RPM file and click **Open**.
c) Click **Upload**.
d) Repeat steps **a** to **c** for each RPM file.
The list of RPMs on the page does not update as you upload each RPM and this is expected. If you see an error after uploading the *tetration_os_mother_rpm_k9-3.8.1.1-1.el6.x86_64.rpm* file, wait for five to 10 minutes and then reload the page. You should now be able to view the list of uploaded RPMs.

For an 8-RU or 39-RU system, upload the following files in the given order:

- tetration_os_rpminstall_k9-3.8.1.1-1.noarch.rpm

- tetration_os_UcsFirmware_k9-3.8.1.1-1.x86_64.rpm
- tetration_os_nxos_k9-3.8.1.1-1.x86_64.rpm
- tetration_os_adhoc_k9-3.8.1.1-1.el6.x86_64.rpm
- tetration_os_mother_rpm_k9-3.8.1.1-1.el6.x86_64.rpm
- tetration_os_enforcement_k9-3.3.8.1.1-1.el6.x86_64.rpm
- tetration_os_base_rpm_k9-3.3.8.1.1-1.el7.x86_64.rpm

For a virtual system, upload the following files in the given order:

- tetration_os_rpminstall_k9-3.8.1.1-1.noarch.rpm
- tetration_os_adhoc_k9-3.8.1.1-1.el6.x86_64.rpm
- tetration_os_mother_rpm_k9-3.8.1.1-1.el6.x86_64.rpm
- tetration_os_enforcement_k9-3.3.8.1.1-1.el6.x86_64.rpm
- tetration_os_ova_k9-3.8.1.1-1.noarch.rpm

Step 8 Click **Continue**.
The **Site Config** portal is displayed.

Note Starting from Secure Workload release 3.8 and later, non-ASCII characters are not allowed to be entered in any of the text fields for site configurations using the Cisco Secure Workload Setup User Interface.

Step 9 (Optional) Under **General**, change the SSH public key and click **Next**.

Step 10 (Optional) Under **Email**, change the UI admin or the admin email address and click **Next**.

Step 11 (Optional) Under **L3**, enable the cluster to use IPv6 addresses in addition to IPv4 for certain cluster connectivity after the upgrade. To enable IPv6:

a) Select the **IPv6** check box.
b) Enter IPv6 addresses in CIDR notation for both Leaf 1 and Leaf 2 switches.
c) Enter the Leaf1 and Leaf2 IPv6 Default Gateway.
d) Click **Next**.

If you enable IPv6 on this page, you must also configure IPv6 fields on the **Network** page, described in the next step.

Important For requirements and limitations on dual stack mode, see Requirements and Limitations for Dual-Stack Mode (IPv6 Support), on page 2.

Step 12 Under **Network**:

a) If necessary, change the values for **CIMC Internal Network**, **CIMC Internal Network Gateway**, **DNS Resolver**, and **DNS Domain**.
b) **Important!** Do not change or remove the existing **External Network** value. However, you can add additional IPv4 networks.
c) If you enabled IPv6 on the L3 page, **IPv6** check box is automatically selected. Specify IPv6 addresses reserved for Secure Workload use by:

1. Enter IPv6 External Network in CIDR notation.

2. (Optional) To use IPv6 only for specified addresses, enter individual External IPv6 IPs.

Note
- The first 3 IPv6 addresses in the IPv6 External Network field are always reserved for the switches of the Secure Workload cluster and should not be used for any other purpose.
- For a 39 RU cluster, ensure that at least 29 IPv6 addresses are available in the IPv6 External Network or the External IPv6 IPs list.
- For an 8 RU cluster, ensure that at least 20 IPv6 addresses are available in the IPv6 External Network or the External IPv6 IPs list.

d) Click **Next**.

Step 13 (Optional) Under **Service**, change the NTP and SMTP values and click **Next**.

Step 14 Under **Security**, enable or disable Strong SSL Ciphers for Agent Connections and click **Next**.

You cannot change the values under the **UI**, **Advanced**, and **Recovery** tabs.

Under **Recovery**, if the cluster is configured to be a standby cluster, the cluster will deploy in standby mode which includes reduced functionality (only to support warm standby mode).

Step 15 Click **Continue**.
The following checks are performed during the upgrade process to ensure:

- The RPM versions are correct
- The cluster is healthy
- The site information you provided is valid
- The switches are configured correctly and may be upgraded to a newer version of NX-OS software
- Info fields are validated
- NTP is synchronized before deployment starts
- Namenode and secondary namenode are not in a failed-over state

The checks can take several minutes to an hour if the cluster switches need to be upgraded. After the checks are complete, you will receive an email with the subject: `TETRATION CLUSTER MyCluster: Verify Token .` The message contains a token that you will need to continue the upgrade. Copy the token from this email.

Step 16 In the Cisco Secure Workload Setup portal, paste the token into the **Validation Token** field and click **Continue**.

Important Do not select the **Ignore instance stop failures** check box unless specifically instructed to do so by a Cisco employee.

The upgrade process is initiated. In 3.8.1.1 and 3.7.1.5 releases, the orchestrator VMs will upgrade before the rest of the components. This can take 30 to 60 minutes during which the progress bar will go from 0 to 100%. After the upgrades to the orchestrators are complete, the rest of the components will be upgraded and the progress bar will start over at 0%. When the green progress bar reaches 100%, the upgrade is complete. All the instances display the “Deployed” status.

Step 17 Verify the upgrade:

a) Open the Secure Workload UI in your browser.
b) From the left navigation pane, click **Platform > Upgrade/Reboot/Shutdown**.

c) Click **History**.
d) Verify that the status under the **Status** column is **Succeeded**.

What to do next

After upgrading, make changes to benefit from enhancements in this release:

- If you have enabled IPv6, you can access the Secure Workload web interface by using either IPv4 or IPv6 address. By default, agents continue to connect to the cluster using IPv4. If you want software agents to be able to communicate with the cluster using IPv6:
  1. From the navigation pane, choose **Platform** > **Cluster Configuration**.
  2. Configure the **Sensor VIP FQDN** setting as described in the User Guide available on the Secure Workload web portal.
- For improved clustering of plain-vanilla Kubernetes workloads within scopes, see Upgrades to Releases 3.9, 3.8, and 3.7: Enabling Improved Clustering of Kubernetes Workloads in Policy Discovery, on page 30.

Upgrade to Secure Workload Release 3.7.x

Upgrade to Secure Workload Release 3.7.1.59

You can upgrade to this release from 3.7.1.5, 3.7.1.22, 3.7.1.39, or 3.7.1.51 release.

Before you begin

Caution Do not upgrade if any nodes are currently in a decommissioned state or any services are unhealthy. Contact the Cisco Technical Assistance Center (TAC) to remediate any issues before continuing.

- Download the installer package:

  In your browser, go to https://software.cisco.com/download/home/286309796/type/286309874/release/3.7.1.59.

  Download the following RPM: `tetration_os_patch_k9-3.7.1.59-1.noarch.rpm`
- Ensure that a **Customer Support** level account has an SSH key uploaded for troubleshooting purposes.
- You must perform the following procedure as a user with Site Administrator or Customer Support privileges.
- Google Chrome is the only supported browser for part of this upgrade.

Procedure

Step 1 Check system health. You cannot perform the upgrade if any services are unhealthy.

a) In the Secure Workload web interface, choose **Troubleshoot > Service Status** from the navigation menu at the left side of the window.
b) Look for red circles in the graph, which indicate unhealthy services.

   Alternatively, to see a table view of service health, click the list button at the top of the graph, click **Expand All**, and scroll down the page to view status of all services.

c) If any services are unhealthy, perform any necessary fixes to make the services healthy before you proceed with the upgrade.

Step 2 In the Secure Workload web interface, from the menu at the left side of the window, click **Platform** > **Upgrade/Reboot/Shutdown**.

Step 3 Follow the instructions you see.

Address any issues found by the pre-check before continuing.

Ensure that **Patch Upgrade** is selected. (This is a patch upgrade.)

Click **Send Upgrade Link**.

Step 4 Look for an email message with the following subject:

```
[Tetration][<cluster_name>] Patch Upgrade Initiation Link
```

This message includes a hyperlink that you must use to perform the upgrade.

Step 5 In the email message, click the **Patch Upgrade <Cluster>** link to open the Secure Workload Setup user interface. You must use Google Chrome browser.

Step 6 Click **Choose File**.

Step 7 Navigate to the patch RPM that you downloaded above, select it, and click **Open**.

Step 8 Click **Upload**.

Uploading the RPM will initiate the upgrade.

During this process, you will temporarily lose connectivity to the setup user interface.

Step 9 Wait for a few minutes to regain access to the web interface and view upgrade results.

If there is a problem with the upgrade, a red banner appears. Click the book image to view logs.

Step 10 Verify the upgrade:

a) Open the Secure Workload web interface in your browser.
b) From the black navigation menu on the left, choose **Platform > Upgrade/Reboot/Shutdown**.
c) Click **History**.
d) Verify that the Status column shows **Succeeded**.

Step 11 If the upgrade was successful, click **Disable Patch Upgrade Link**.

Upgrade to Secure Workload Release 3.7.1.51

You can upgrade to this release from 3.7.1.5, 3.7.1.22, or 3.7.1.39 release.

Before you begin

Caution Do not upgrade if any nodes are currently in a decommissioned state or any services are unhealthy. Contact the Cisco Technical Assistance Center (TAC) to remediate any issues before continuing.

- Download the installer package:

  In your browser, go to https://software.cisco.com/download/home/286309796/type/286309874/release/3.7.1.51.

  Download the following RPM: `tetration_os_patch_k9-3.7.1.51-1.noarch.rpm`

- Ensure that a **Customer Support** level account has an SSH key uploaded for troubleshooting purposes.
- You must perform the following procedure as a user with Site Administrator or Customer Support privileges.
- Google Chrome is the only supported browser for part of this upgrade.

Procedure

Step 1 Check system health. You cannot perform the upgrade if any services are unhealthy.

a) In the Secure Workload web interface, choose **Troubleshoot > Service Status** from the navigation menu at the left side of the window.

b) Look for red circles in the graph, which indicate unhealthy services.

Alternatively, to see a table view of service health, click the list button at the top of the graph, click **Expand All**, and scroll down the page to view status of all services.

c) If any services are unhealthy, perform any necessary fixes to make the services healthy before you proceed with the upgrade.

Step 2 In the Secure Workload web interface, from the menu at the left side of the window, click **Platform** > **Upgrade/Reboot/Shutdown**.

Step 3 Follow the instructions you see.

Address any issues found by the pre-check before continuing.

Ensure that **Patch Upgrade** is selected. (This is a patch upgrade.)

Click **Send Upgrade Link**.

Step 4 Look for an email message with the following subject:

`[Tetration][<cluster_name>] Patch Upgrade Initiation Link`

This message includes a hyperlink that you must use to perform the upgrade.

Step 5 In the email message, click the **Patch Upgrade <Cluster>** link to open the Secure Workload Setup user interface. You must use Google Chrome browser.

Step 6 Click **Choose File**.

Step 7 Navigate to the patch RPM that you downloaded above, select it, and click **Open**.

Step 8 Click **Upload**.

Uploading the RPM will initiate the upgrade.

During this process, you will temporarily lose connectivity to the setup user interface.

Step 9 Wait for a few minutes to regain access to the web interface and view upgrade results.

If there is a problem with the upgrade, a red banner appears. Click the book image to view logs.

Step 10 Verify the upgrade:

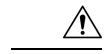
a) Open the Secure Workload web interface in your browser.
b) From the black navigation menu on the left, choose **Platform > Upgrade/Reboot/Shutdown**.
c) Click **History**.
d) Verify that the Status column shows **Succeeded**.

Step 11 If the upgrade was successful, click **Disable Patch Upgrade Link**.

Upgrade to Secure Workload Release 3.7.1.39

You can upgrade to this release from 3.7.1.5 or 3.7.1.22 release.

Before you begin



Caution Do not upgrade if any nodes are currently in a decommissioned state or any services are unhealthy. Contact the Cisco Technical Assistance Center (TAC) to remediate any issues before continuing.

- Download the installer package:

  In your browser, go to https://software.cisco.com/download/home/286309796/type/286309874/release/3.7.1.39.

  Download the following RPM: `tetration_os_patch_k9-3.7.1.39-1.noarch.rpm`

- Ensure that a “Customer Support” level account has an SSH key uploaded for troubleshooting purposes.
- You must perform the following procedure as a user with Site Administrator or Customer Support privileges.
- Google Chrome is the only supported browser for part of this upgrade.

Procedure

Step 1 Check system health. You cannot perform the upgrade if any services are unhealthy.

a) In the Secure Workload web interface, choose **Troubleshoot > Service Status** from the navigation menu at the left side of the window.
b) Look for red circles in the graph, which indicate unhealthy services.

   Alternatively, to see a table view of service health, click the list button at the top of the graph, click **Expand All**, and scroll down the page to view status of all services.

c) If any services are unhealthy, perform any necessary fixes to make the services healthy before you proceed with the upgrade.

Step 2 In the Secure Workload web interface, from the menu at the left side of the window, click **Platform** > **Upgrade/Reboot/Shutdown**.

Step 3 Follow the instructions you see.

Address any issues found by the pre-check before continuing.

Ensure that **Patch Upgrade** is selected. (This is a patch upgrade.)

Click **Send Upgrade Link**.

Step 4 Look for an email message with the following subject:

```
[Tetration][<cluster_name>] Patch Upgrade Initiation Link
```

This message includes a hyperlink that you must use to perform the upgrade.

Step 5 In the email message, click the **Patch Upgrade <Cluster>** link to open the Secure Workload Setup user interface. You must use Google Chrome browser.

Step 6 Click **Choose File**.

Step 7 Navigate to the patch RPM that you downloaded above, select it, and click **Open**.

Step 8 Click **Upload**.

Uploading the RPM will initiate the upgrade.

During this process, you will temporarily lose connectivity to the setup user interface.

Step 9 Wait for a few minutes to regain access to the web interface and view upgrade results.

If there is a problem with the upgrade, a red banner appears. Click the book image to view logs.

Step 10 Verify the upgrade:

a) Open the Secure Workload web interface in your browser.
b) From the black navigation menu on the left, choose **Platform > Upgrade/Reboot/Shutdown**.
c) Click **History**.
d) Verify that the Status column shows **Succeeded**.

Step 11 If the upgrade was successful, click **Disable Patch Upgrade Link**.

Upgrade to Secure Workload Release 3.7.1.22

You can upgrade to this release from 3.7.1.5 release.

Before you begin

Caution Do not upgrade if any nodes are currently in a decommissioned state or any services are unhealthy. Contact the Cisco Technical Assistance Center (TAC) to remediate any issues before continuing.

- Download the installer package:

  In your browser, go to https://software.cisco.com/download/home/286309796/type/286309874/release/3.7.1.22.

  Download the following RPM: `tetration_os_patch_k9-3.7.1.22-1.noarch.rpm`

- Ensure that a “Customer Support” level account has an SSH key uploaded for troubleshooting purposes.
- You must perform the following procedure as a user with Site Administrator or Customer Support privileges.
- Google Chrome is the only supported browser for part of this upgrade.

Procedure

Step 1 Check system health. You cannot perform the upgrade if any services are unhealthy.

a) In the Secure Workload web interface, choose **Troubleshoot > Service Status** from the navigation menu at the left side of the window.

b) Look for red circles in the graph, which indicate unhealthy services.

Alternatively, to see a table view of service health, click the list button at the top of the graph, click **Expand All**, and scroll down the page to view status of all services.

c) If any services are unhealthy, perform any necessary fixes to make the services healthy before you proceed with the upgrade.

Step 2 In the Secure Workload web interface, from the menu at the left side of the window, click **Platform** > **Upgrade/Reboot/Shutdown**.

Step 3 Follow the instructions you see.

Address any issues found by the pre-check before continuing.

Ensure that **Patch Upgrade** is selected. (This is a patch upgrade.)

Click **Send Upgrade Link**.

Step 4 Look for an email message with the following subject:

```
[Tetration][<cluster_name>] Patch Upgrade Initiation Link
```

This message includes a hyperlink that you must use to perform the upgrade.

Step 5 In the email message, click the **Patch Upgrade <Cluster>** link to open the Secure Workload Setup user interface. You must use Google Chrome browser.

Step 6 Click **Choose File**.

Step 7 Navigate to the patch RPM that you downloaded above, select it, and click **Open**.

Step 8 Click **Upload**.

Uploading the RPM will initiate the upgrade.

During this process, you will temporarily lose connectivity to the setup user interface.

Step 9 Wait for a few minutes to regain access to the web interface and view upgrade results.

If there is a problem with the upgrade, a red banner appears. Click the book image to view logs.

Step 10 Verify the upgrade:

a) Open the Secure Workload web interface in your browser.

b) From the black navigation menu on the left, choose **Platform > Upgrade/Reboot/Shutdown**.

c) Click **History**.

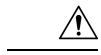
d) Verify that the Status column shows **Succeeded**.

Step 11 If the upgrade was successful, click **Disable Patch Upgrade Link**.

Upgrade to Secure Workload Release 3.7.1.5

You can upgrade to this release from any 3.6 release, but it is recommended to upgrade to the latest 3.6.1.x patch release before upgrading to this release.

Before you begin



Caution Do not upgrade if any nodes are currently in a decommissioned state or any services are unhealthy. Contact the Cisco Technical Assistance Center (TAC) to remediate any issues before continuing.

Keep these points in mind:

- Kubernetes AKS external orchestrators—After the upgrade, AKS external orchestrators will be read-only; if you want to make changes after the upgrade, create a new Azure connector and enable the **Managed Kubernetes services** option.
- Ensure that a "Customer Support" level account has an SSH key uploaded for troubleshooting purposes.
- You must perform the following procedure as a user with Site Administrator or Customer Support privileges.
- Google Chrome is the only supported browser for this upgrade.
- If ISE connectors are configured, verify that their TLS certificates have Subject Alternative Name (SAN) sections. After the upgrade, the ISE connector will not connect to ISE endpoints that present legacy CN-only TLS certificates. Do not proceed with the upgrade before the ISE TLS certificates are regenerated with SAN extensions.
- **Licensing**
  - If your Secure Workload deployment does not currently have valid licenses (or is outside the evaluation period), you must register valid licenses before you upgrade.
  - Site Administration privileges are required to manage licenses.
  - To view the status of your licenses: In the Cisco Secure Workload web portal, choose **Monitoring** > **Licenses**. If your cluster license registration is out of compliance, you will see a banner with a **Take action** link. For information about obtaining and registering licenses, in the Secure Workload web portal, select **Help** > **Page-level Help** and search for Licenses.

Procedure

Step 1 Download the applicable RPM files for your deployment from Cisco.com:

a) Go to https://software.cisco.com/download/home/286309796/type.

b) Download as appropriate:

- For an 8-RU or 39-RU system, download the following RPMs:

- tetration_os_UcsFirmware_k9-3.7.1.5-1.x86_64.rpm
- tetration_os_base_rpm_k9-3.7.1.5-1.el7.x86_64.rpm
- tetration_os_adhoc_k9-3.7.1.5-1.el6.x86_64.rpm
- tetration_os_mother_rpm_k9-3.7.1.5-1.el6.x86_64.rpm
- tetration_os_rpminstall_k9-3.7.1.5-1.noarch.rpm
- tetration_os_enforcement_k9-3.7.1.5-1.el6.x86_64.rpm
- tetration_os_nxos_k9-3.7.1.5-1.x86_64.rpm

- For a virtual system, download the following RPMs:
  - tetration_os_ova_k9-3.7.1.5-1.noarch.rpm
  - tetration_os_adhoc_k9-3.7.1.5-1.el6.x86_64.rpm
  - tetration_os_mother_rpm_k9-3.7.1.5-1.el6.x86_64.rpm
  - tetration_os_rpminstall_k9-3.7.1.5-1.noarch.rpm
  - tetration_os_enforcement_k9-3.7.1.5-5.el6.x86_64.rpm

c) Verify the MD5 checksum of the downloaded RPMs matches the MD5 checksum in CCO.

Step 2 Check system health. You cannot perform the upgrade if any services are unhealthy.

a) In the Secure Workload web interface, click **Settings** and select **Maintenance**.
b) In the left pane, select **Service Status**.
c) Look for red circles in the graph, which indicate unhealthy services.

Alternatively, to see a table view of service health, click the list button at the top of the graph, click **Expand All**, and scroll down the page to view status of all services.

d) If any services are unhealthy, perform any necessary fixes to make the services healthy before you proceed with the upgrade.

Step 3 In the navigation menu at the left, select **Maintenance** > **Upgrade**.

Step 4 If necessary, click the **Upgrade** tab.

Step 5 Follow the instructions displayed on the screen. Ensure that you do not skip any of the steps.

Use the **Upgrade** option, and NOT the patch upgrade option.

Step 6 Click **Send Upgrade Link**.

A user logged in with the site administrator or customer support role will receive an email with a hyperlink that must be used to perform the upgrade. The subject of the email will be:

```
[Tetration Analytics] Upgrade Initiation Link
```

Open the email and copy the **Upgrade Cluster** URL.

Alternatively, you can fetch the upgrade URL from the **Maintenance** > **Explore** page by entering the following information:

- Snapshot Action:**POST**

- Snapshot Host:**orchestrator.service.consul**
- Snapshot Path:**upgrade_url**

Step 7 In Google Chrome, paste the upgrade URL into the address field and press **Enter**.

The Cisco Secure Workload Setup portal is displayed. Note that Google Chrome is the only supported web browser for the upgrade.

Step 8 In the Cisco Secure Workload Setup portal, you must upload the RPMs in a specific order depending on your setup. To upload the RPM files, perform the following actions:

a) Click **Choose File**.
b) Navigate and select a RPM file and click **Open**.
c) Click **Upload**.
d) Repeat steps **a** to **c** for each RPM file.
The list of RPMs on the page does not update as you upload each RPM and this is expected. If you see an error after uploading the *tetration_os_mother_rpm_k9-3.7.1.5-1.el6.x86_64.rpm* file, wait for five to 10 minutes and then reload the page. You should now be able to view the list of uploaded RPMs.

For an 8-RU or 39-RU system, upload the following files in the given order:

- tetration_os_rpminstall_k9-3.7.1.5-1.noarch.rpm
- tetration_os_UcsFirmware_k9-3.7.1.5-1.x86_64.rpm
- tetration_os_nxos_k9-3.7.1.5-1.x86_64.rpm
- tetration_os_adhoc_k9-3.7.1.5-1.el6.x86_64.rpm
- tetration_os_mother_rpm_k9-3.7.1.5-1.el6.x86_64.rpm
- tetration_os_enforcement_k9-3.7.1.5-1.el6.x86_64.rpm
- tetration_os_base_rpm_k9-3.7.1.5-1.el7.x86_64.rpm

For a virtual system, upload the following files in the given order:

- tetration_os_rpminstall_k9-3.7.1.5-1.noarch.rpm
- tetration_os_adhoc_k9-3.7.1.5-1.el6.x86_64.rpm
- tetration_os_mother_rpm_k9-3.7.1.5-1.el6.x86_64.rpm
- tetration_os_enforcement_k9-3.7.1.5-1.el6.x86_64.rpm
- tetration_os_ova_k9-3.7.1.5-1.noarch.rpm

Step 9 Click **Continue**.
The **Site Config** portal is displayed.

Step 10 (Optional) Under **General**, change the SSH public key and click **Next**.

Step 11 (Optional) Under **Email**, change the UI admin or the admin email address and click **Next**.

Step 12 (Optional) Under **L3**, enable the cluster to use IPv6 addresses in addition to IPv4 for certain cluster connectivity after the upgrade. To enable IPv6:

a) Select the **IPv6** check box.
b) Enter IPv6 addresses in CIDR notation for both Leaf 1 and Leaf 2 switches.

c) Enter the Leaf1 and Leaf2 IPv6 Default Gateway.
d) Click **Next**.

If you enable IPv6 on this page, you must also configure IPv6 fields on the **Network** page, described in the next step.

Important For requirements and limitations on dual stack mode, see Requirements and Limitations for Dual-Stack Mode (IPv6 Support), on page 2.

Step 13 Under **Network**:

a) If necessary, change the values for **CIMC Internal Network**, **CIMC Internal Network Gateway**, **DNS Resolver**, and **DNS Domain**.
b) **Important!** Do not change or remove the existing **External Network** value. However, you can add additional IPv4 networks.
c) If you enabled IPv6 on the L3 page, **IPv6** check box is automatically selected. Specify IPv6 addresses reserved for Secure Workload use by:

1. Enter IPv6 External Network in CIDR notation.
2. (Optional) To use IPv6 only for specified addresses, enter individual External IPv6 IPs.

Note that:

- The first 3 IPv6 addresses in the IPv6 External Network field are always reserved for the switches of the Secure Workload cluster and should not be used for any other purpose.
- For a 39 RU cluster, ensure that at least 29 IPv6 addresses are available in the IPv6 External Network or the External IPv6 IPs list.
- For an 8 RU cluster, ensure that at least 20 IPv6 addresses are available in the IPv6 External Network or the External IPv6 IPs list.

d) Click **Next**.

Step 14 (Optional) Under **Service**, change the NTP and SMTP values and click **Next**.

If you need to change syslog values (if any) use the TAN appliance.

Step 15 Under **Security**, enable or disable Strong SSL Ciphers for Agent Connections and click **Next**.

You cannot change the values under the **UI**, **Advanced**, and **Recovery** tabs.

Under **Recovery**, if the cluster is configured to be a standby cluster, the cluster will deploy in standby mode which includes reduced functionality (only to support warm standby mode).

Step 16 Click **Continue**.
The following checks are performed during the upgrade process to ensure:

- The RPM versions are correct
- The cluster is healthy
- The site information you provided is valid
- The switches are configured correctly and may be upgraded to a newer version of NX-OS software
- Info fields are validated
- NTP is synchronized before deployment starts

- Namenode and secondary namenode are not in a failed-over state

The checks can take several minutes to an hour if the cluster switches need to be upgraded. After the checks are complete, you will receive an email with the subject: `TETRATION CLUSTER MyCluster: Verify Token .` The message contains a token that you will need to continue the upgrade. Copy the token from this email.

Step 17 In the Cisco Secure Workload Setup portal, paste the token into the **Validation Token** field and click **Continue**.

Important Do not select the **Ignore instance stop failures** check box unless specifically instructed to do so by a Cisco employee.

The upgrade process is initiated. In 3.7.1.5 release, the orchestrator VMs will upgrade before the rest of the components. This can take 30 to 60 minutes during which the progress bar will go from 0 to 100%. After the upgrades to the orchestrators are complete, the rest of the components will be upgraded and the progress bar will start over at 0%. When the green progress bar reaches 100%, the upgrade is complete. All the instances display the “Deployed” status.

Step 18 Verify the upgrade:

a) Open the Secure Workload web interface in your browser.
b) From the black navigation menu on the left, choose **Platform > Upgrade/Reboot/Shutdown**.
c) Click **History**.
d) Verify that the Status column shows **Succeeded**.

Step 19 If the upgrade was successful, click **Disable Patch Upgrade Link**.

What to do next

After upgrading, make changes to benefit from enhancements in this release:

- See What to do next, on page 44.
- For improved clustering of plain-vanilla Kubernetes workloads within scopes, see Upgrades to Releases 3.9, 3.8, and 3.7: Enabling Improved Clustering of Kubernetes Workloads in Policy Discovery, on page 30.

Upgrades to Releases 3.9, 3.8, and 3.7: Enabling Improved Clustering of Kubernetes Workloads in Policy Discovery

This feature applies to plain-vanilla Kubernetes only (In the orchestrator configuration, "K8s Manager Type" is "None".)

If you have already configured Kubernetes external orchestrators, you can enable an enhancement in releases 3.9, 3.8, and 3.7 that improves the accuracy of ADM clustering results for Kubernetes workloads, by using Kubernetes label metadata for clustering.

To enable this enhancement, do both of the following for each plain-vanilla Kubernetes orchestrator after upgrade:

- In the plain-vanilla Kubernetes external orchestrator configuration (under **Manage > External Orchestrators**), enable **Use for policy discovery clustering** and save the change.
- Add the following privileges to the ClusterRole bound to the service account.

Resources	Kubernetes Verbs
replicationcontrollers	[get list watch]
replicasets	[get list watch]
deployments	[get list watch]
daemonsets	[get list watch]
statefulsets	[get list watch]
jobs	[get list watch]
cronjobs	[get list watch]

A sample clusterrole.yaml that includes these privileges (your version may be slightly different):

```
kind: ClusterRole
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: tetration.read.only
rules:
  - apiGroups:
    - ""
      resources:
        - nodes
        - services
        - endpoints
        - namespaces
        - pods
        - replicationcontrollers
        - ingresses
      verbs:
        - get
        - list
        - watch
  - apiGroups:
    - extensions
    - networking.k8s.io
      resources:
        - ingresses
      verbs:
        - get
        - list
        - watch
  - apiGroups:
    - apps
      resources:
        - replicasets
        - deployments
        - statefulsets
        - daemonsets
      verbs:
        - get
        - list
        - watch
  - apiGroups:
    - batch
      resources:
        - jobs
        - cronjobs
```

```
verbs:
  - get
  - list
  - watch
```

Upgrade to Secure Workload Release 3.6.x

Upgrade to Secure Workload Release 3.6.1.47

You can upgrade to this release from any earlier 3.6 release.

Before you begin

Caution Do not upgrade if any nodes are currently in a decommissioned state or any services are unhealthy. Contact the Cisco Technical Assistance Center (TAC) to remediate any issues before continuing.

- Download the installer package:

  In your browser, go to https://software.cisco.com/download/home/286309796/type/286309874/release/3.6.1.47.

  Download the following RPM: `tetration_os_patch_k9-3.6.1.47-1.noarch.rpm`

- You should back up your system before performing an upgrade. For details, see information about Data Backup and Restore (DBR) in the user guide, including the subsection about upgrades.
- Ensure that a “Customer Support” level account has an SSH key uploaded for troubleshooting purposes.
- You must perform the following procedure as a user with Site Administrator or Customer Support privileges.
- Google Chrome is the only supported browser for part of this upgrade.

Procedure

Step 1 Check system health. You cannot perform the upgrade if any services are unhealthy.

a) In the Secure Workload web interface, choose **Troubleshoot** > **Service Status** from the navigation menu at the left side of the window.

b) Look for red circles in the graph, which indicate unhealthy services.

Alternatively, to see a table view of service health, click the list button at the top of the graph, click **Expand All**, and scroll down the page to view status of all services.

c) If any services are unhealthy, perform any necessary fixes to make the services healthy before you proceed with the upgrade.

Step 2 In the Secure Workload web interface, from the menu at the left side of the window, click **Platform** > **Upgrade/Reboot/Shutdown**.

Step 3 Follow the instructions you see.

Address any issues found by the pre-check before continuing.

Ensure that **Patch Upgrade** is selected. (This is a patch upgrade.)

Click **Send Upgrade Link**.

Step 4 Look for an email message with the following subject:

`[Tetration][<cluster_name>] Patch Upgrade Initiation Link`

This message includes a hyperlink that you must use to perform the upgrade.

Step 5 In the email message, click the **Patch Upgrade <Cluster>** link to open the Secure Workload Setup user interface. You must use Google Chrome browser.

Step 6 Click **Choose File**.

Step 7 Navigate to the patch RPM that you downloaded above, select it, and click **Open**.

Step 8 Click **Upload**.

Uploading the RPM will initiate the upgrade.

During this process, you will temporarily lose connectivity to the setup user interface.

Step 9 Wait for a few minutes to regain access to the web interface and view upgrade results.

If there is a problem with the upgrade, a red banner appears. Click the book image to view logs.

Step 10 Verify the upgrade:

a) Open the Secure Workload web interface in your browser.
b) From the black navigation menu on the left, choose **Platform > Upgrade/Reboot/Shutdown**.
c) Click **History**.
d) Verify that the Status column shows **Succeeded**.

Step 11 If the upgrade was successful, click **Disable Patch Upgrade Link**.

Upgrade to Secure Workload Release 3.6.1.36

You can upgrade to this release from any earlier 3.6 release.

Before you begin

Caution Do not upgrade if any nodes are currently in a decommissioned state or any services are unhealthy. Contact the Cisco Technical Assistance Center (TAC) to remediate any issues before continuing.

- Download the installer package:

  In your browser, go to https://software.cisco.com/download/home/286309796/type/286309874/release/3.6.1.36.

  Download the following RPM: `tetration_os_patch_k9-3.6.1.36-1.noarch.rpm`

- You should back up your system before performing an upgrade. For details, see information about Data Backup and Restore (DBR) in the user guide, including the subsection about upgrades.

- Ensure that a “Customer Support” level account has an SSH key uploaded for troubleshooting purposes.

- You must perform the following procedure as a user with Site Administrator or Customer Support privileges.
- Google Chrome is the only supported browser for part of this upgrade.

Procedure

Step 1 Check system health. You cannot perform the upgrade if any services are unhealthy.

a) In the Secure Workload web interface, choose **Troubleshoot > Service Status** from the navigation menu at the left side of the window.

b) Look for red circles in the graph, which indicate unhealthy services.

Alternatively, to see a table view of service health, click the list button at the top of the graph, click **Expand All**, and scroll down the page to view status of all services.

c) If any services are unhealthy, perform any necessary fixes to make the services healthy before you proceed with the upgrade.

Step 2 In the Secure Workload web interface, from the menu at the left side of the window, click **Platform** > **Upgrade/Reboot/Shutdown**.

Step 3 Follow the instructions you see.

Address any issues found by the pre-check before continuing.

Ensure that **Patch Upgrade** is selected. (This is a patch upgrade.)

Click **Send Upgrade Link**.

Step 4 Look for an email message with the following subject:

```
[Tetration][<cluster_name>] Patch Upgrade Initiation Link
```

This message includes a hyperlink that you must use to perform the upgrade.

Step 5 In the email message, click the **Patch Upgrade <Cluster>** link to open the Secure Workload Setup user interface. You must use Google Chrome browser.

Step 6 Click **Choose File**.

Step 7 Navigate to the patch RPM that you downloaded above, select it, and click **Open**.

Step 8 Click **Upload**.

Uploading the RPM will initiate the upgrade.

During this process, you will temporarily lose connectivity to the setup user interface.

Step 9 Wait for a few minutes to regain access to the web interface and view upgrade results.

If there is a problem with the upgrade, a red banner appears. Click the book image to view logs.

Step 10 Verify the upgrade:

a) Open the Secure Workload web interface in your browser.

b) From the black navigation menu on the left, choose **Platform > Upgrade/Reboot/Shutdown**.

c) Click **History**.

d) Verify that the Status column shows **Succeeded**.

Step 11 If the upgrade was successful, click **Disable Patch Upgrade Link**.

Upgrade to Secure Workload Release 3.6.1.21

You can upgrade to this release from any earlier 3.6 release.

Before you begin

Caution Do not upgrade if any nodes are currently in a decommissioned state or any services are unhealthy. Contact the Cisco Technical Assistance Center (TAC) to remediate any issues before continuing.

- Download the installer package:

  In your browser, go to https://software.cisco.com/download/home/286309796/type/286309874/release/3.6.1.21.

  Download the following RPM: `tetration_os_patch_k9-3.6.1.21-1.noarch.rpm`
- You should back up your system before performing an upgrade. For details, see information about Data Backup and Restore (DBR) in the user guide, including the subsection about upgrades.
- Ensure that a "Customer Support" level account has an SSH key uploaded for troubleshooting purposes.
- You must perform the following procedure as a user with Site Administrator or Customer Support privileges.
- Google Chrome is the only supported browser for part of this upgrade.

Procedure

Step 1 Check system health. You cannot perform the upgrade if any services are unhealthy.

a) In the Secure Workload web interface, choose **Troubleshoot > Service Status** from the navigation menu at the left side of the window.

b) Look for red circles in the graph, which indicate unhealthy services.

Alternatively, to see a table view of service health, click the list button at the top of the graph, click **Expand All**, and scroll down the page to view status of all services.

c) If any services are unhealthy, perform any necessary fixes to make the services healthy before you proceed with the upgrade.

Step 2 In the Secure Workload web interface, from the menu at the left side of the window, click **Platform** > **Upgrade/Reboot/Shutdown**.

Step 3 Follow the instructions you see.

Address any issues found by the pre-check before continuing.

Ensure that **Patch Upgrade** is selected. (This is a patch upgrade.)

Click **Send Upgrade Link**.

Step 4 Look for an email message with the following subject:

`[Tetration][<cluster_name>] Patch Upgrade Initiation Link`

This message includes a hyperlink that you must use to perform the upgrade.

Step 5 In the email message, click the **Patch Upgrade <Cluster>** link to open the Secure Workload Setup user interface. You must use Google Chrome browser.

Step 6 Click **Choose File**.

Step 7 Navigate to the patch RPM that you downloaded above, select it, and click **Open**.

Step 8 Click **Upload**.

Uploading the RPM will initiate the upgrade.

During this process, you will temporarily lose connectivity to the setup user interface.

Step 9 Wait for a few minutes to regain access to the web interface and view upgrade results.

If there is a problem with the upgrade, a red banner appears. Click the book image to view logs.

Step 10 Verify the upgrade:

a) Open the Secure Workload web interface in your browser.
b) From the black navigation menu on the left, choose **Platform > Upgrade/Reboot/Shutdown**.
c) Click **History**.
d) Verify that the Status column shows **Succeeded**.

Step 11 If the upgrade was successful, click **Disable Patch Upgrade Link**.

Upgrade to Secure Workload Release 3.6.1.17

You can upgrade to the 3.6.1.17 release from release 3.6.1.5.

Before you begin

Caution Do not upgrade if any nodes are currently in a decommissioned state or any services are unhealthy. Contact the Cisco Technical Assistance Center (TAC) to remediate any issues before continuing.

- Download the installer package:

  In your browser, go to https://software.cisco.com/download/home/286309796/type/286309874/release/3.6.1.17.

  Download the following RPM: `tetration_os_patch_k9-3.6.1.17-1.noarch.rpm`

- You should back up your system before performing an upgrade. For details, see information about Data Backup and Restore (DBR) in the user guide, including the subsection about upgrades.
- Ensure that a “Customer Support” level account has an SSH key uploaded for troubleshooting purposes.
- You must perform the following procedure as a user with Site Administrator or Customer Support privileges.
- Google Chrome is the only supported browser for part of this upgrade.

Procedure

Step 1 Check system health. You cannot perform the upgrade if any services are unhealthy.

a) In the Secure Workload web interface, choose **Troubleshoot > Service Status** from the navigation menu at the left side of the window.

b) Look for red circles in the graph, which indicate unhealthy services.

Alternatively, to see a table view of service health, click the list button at the top of the graph, click **Expand All**, and scroll down the page to view status of all services.

c) If any services are unhealthy, perform any necessary fixes to make the services healthy before you proceed with the upgrade.

Step 2 In the Secure Workload web interface, from the menu at the left side of the window, click **Platform** > **Upgrade/Reboot/Shutdown**.

Step 3 Follow the instructions you see.

Address any issues found by the pre-check before continuing.

Ensure that **Patch Upgrade** is selected. (This is a patch upgrade.)

Click **Send Upgrade Link**.

Step 4 Look for an email message with the following subject:

```
[Tetration][<cluster_name>] Patch Upgrade Initiation Link
```

This message includes a hyperlink that you must use to perform the upgrade.

Step 5 In the email message, click the **Patch Upgrade <Cluster>** link to open the Secure Workload Setup user interface. You must use Google Chrome browser.

Step 6 Click **Choose File**.

Step 7 Navigate to the patch RPM that you downloaded above, select it, and click **Open**.

Step 8 Click **Upload**.

Uploading the RPM will initiate the upgrade.

During this process, you will temporarily lose connectivity to the setup user interface.

Step 9 Wait for a few minutes to regain access to the web interface and view upgrade results.

If there is a problem with the upgrade, a red banner appears. Click the book image to view logs.

Step 10 Verify the upgrade:

a) Open the Secure Workload web interface in your browser.

b) From the black navigation menu on the left, choose **Platform > Upgrade/Reboot/Shutdown**.

c) Click **History**.

d) Verify that the Status column shows **Succeeded**.

Step 11 If the upgrade was successful, click **Disable Patch Upgrade Link**.

Upgrade to Secure Workload Release 3.6.1.5

You can upgrade to this release from any 3.5.1.x release, but it is recommended to upgrade to the latest 3.5.1.x patch release before upgrading to this release.

These instructions are valid for both hardware and virtual deployments.

Before you begin

Caution Do not upgrade if any nodes are currently in a decommissioned state or any services are unhealthy. Before continuing, contact the Cisco Technical Assistance Center (TAC) to remediate any issues.

Additional prerequisites:

- **Licensing**

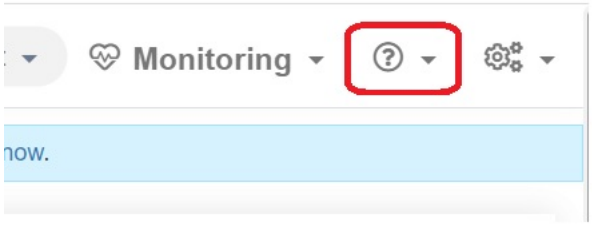
  If your Tetration deployment does not currently have valid licenses (or is outside the evaluation period), you must register valid licenses before you upgrade.

  Site Administration privileges are required to manage licenses.

  To see the status of your licenses:

  In the Tetration web portal, choose **Monitoring > Licenses**. If your cluster license registration is out of compliance, you will see a banner with a **Take action** link.

  For information about obtaining and registering licenses, see the User Guide in the Tetration web portal by clicking here:



  Search in the User Guide for "Licenses".

- **IPv6 support (dual-stack mode)**

  (Optional) Secure Workload clusters running on physical hardware can be configured to use IPv6 in addition to IPv4 for certain communications with and within the cluster. (Secure Workload already handles IPv6 traffic for policy purposes regardless.)

  You can enable this functionality only during initial deployment or upgrade to release 3.6.1.5.

  If you are considering enabling dual-stack (IPv6) connectivity, see Requirements and Limitations for Dual-Stack Mode (IPv6 Support), on page 2.

- **Other features**

  Feature-specific impacts that may require action before you upgrade:

  - **Firepower Management Center (FMC) integration:**

If you upgrade Secure Workload and you wish to continue to use this integration, you must upgrade the FMC to the required version first.

This integration in 3.6 is significantly different from the 3.5 implementation. Carefully read the description and requirements for version 3.6 in the *Cisco Secure Workload and Firepower Management Center Integration Guide*, available from https://www.cisco.com/c/en/us/support/security/tetration/products-installation-and-configuration-guides-list.html.

After the Secure Workload upgrade, prefilter policies in FMC will be converted to access control policies and inventory filters will be converted to dynamic objects.

- **AWS connectors:**

  Existing AWS connectors will be deleted upon upgrade. You must recreate new AWS cloud connectors after upgrade. If necessary, take note of configured information before upgrading.

- Kubernetes EKS external orchestrators

  After upgrade, EKS external orchestrators will be read-only; if you want to make changes after upgrade, create a new AWS connector and enable the **Managed Kubernetes services** option.

- **Data Export connector:**

  Support for Data Export connector (Alpha feature) has been removed from this release. If you have Data Export connector configured; it's recommended to disable or remove it before upgrading to this release.

- **Other changes:**

  Additional behavior changes that do not require action before upgrade are described in the release notes for version 3.6.1.5, available from https://www.cisco.com/c/en/us/support/security/tetration/products-release-notes-list.html.

- This upgrade does NOT require any new public routable IP addresses.
- Customer Support privileges are required to perform this upgrade.
- Ensure that a user account with Customer Support privileges has an SSH key uploaded for troubleshooting purposes. For more information, see "Importing SSH Public Key" in the User Guide available from the Tetration web portal.
- You should back up your system before performing an upgrade. For details, see information about Data Backup and Restore (DBR) in the user guide, including the subsection about upgrades.
- Google Chrome is the only supported browser for the Secure Workload Setup portal, a dedicated portal required for part of this upgrade.

Procedure

Step 1 Download the applicable RPM files for your deployment from Cisco.com:

a) Navigate to https://software.cisco.com/download/home/286309796/type.

b) Download as appropriate:

- For an 8-RU or 39-RU system, download the following RPMs:
  - `tetration_os_UcsFirmware_k9-3.6.1.5.rpm`

- `tetration_os_base_rpm_k9-3.6.1.5-1.el7.x86_64.rpm`
- `tetration_os_adhoc_k9-3.6.1.5-1.el6.x86_64.rpm`
- `tetration_os_mother_rpm_k9-3.6.1.5-1.el6.x86_64.rpm`
- `tetration_os_rpminstall_k9-3.6.1.5-1.noarch.rpm`
- `tetration_os_enforcement_k9-3.6.1.5-1.el6.x86_64.rpm`

- For a virtual system, download the following RPMs:
  - `tetration_os_ova_k9-3.6.1.5-1.el7.x86_64.rpm`
  - `tetration_os_adhoc_k9-3.6.1.5-1.el6.x86_64.rpm`
  - `tetration_os_mother_rpm_k9-3.6.1.5-1.el6.x86_64.rpm`
  - `tetration_os_rpminstall_k9-3.6.1.5-1.noarch.rpm`
  - `tetration_os_enforcement_k9-3.6.1.5-5.el6.x86_64.rpm`

c) Check to ensure the MD5 of each RPM download matches the MD5 in CCO.

Step 2 Check system health. You cannot perform the upgrade if any services are unhealthy.

a) In the Cisco Tetration GUI, click the settings button and choose **Maintenance**.
b) In the left pane, click **Service Status**.
c) Look for red circles in the graph, which indicate unhealthy services.

Alternatively, to see a table view of service health, click the list button at the top of the graph, click **Expand All**, and scroll down the page to view status of all services.

d) If any services are unhealthy, perform any necessary fixes to make the services healthy before you proceed with the upgrade.

Step 3 In the navigation menu at the left, click **Maintenance > Upgrade**.

Step 4 If necessary, click the **Upgrade** tab.

Step 5 Follow the steps on the screen. Do not skip any steps.

Use the **Upgrade** option, NOT the patch upgrade option.

Step 6 After you click **Send Upgrade Link**, look for the resulting email message.

A user who logged in with the site administrator or customer support role will receive an email with a hyperlink that must be used to perform the upgrade. The email's subject will be:

```
[Tetration Analytics] Upgrade Initiation Link
```

Open the email message and copy the **Upgrade Cluster** URL.

Alternatively, you can fetch the upgrade URL from the **Maintenance > Explore** page by entering the following information:

- Snapshot Action:**POST**
- Snapshot Host:**orchestrator.service.consul**
- Snapshot Path:**upgrade_url**

Step 7 Open a new Google Chrome browser tab, paste the upgrade URL into the address field, and then press **Enter**.

This opens the Cisco Secure Workload Setup portal, which is supported only with the Google Chrome browser.

Step 8 In the Cisco Secure Workload Setup portal, you must upload the RPMs in a specific order, depending on your setup.

For an 8-RU or 39-RU system, upload the following files in the given order:

a. `tetration_os_rpminstall_k9-3.6.1.5-1.noarch.rpm`

b. `tetration_os_UcsFirmware_k9-3.6.1.5.rpm`

c. `tetration_os_adhoc_k9-3.6.1.5-1.el6.x86_64.rpm`

d. `tetration_os_mother_rpm_k9-3.6.1.5-1.el6.x86_64.rpm`

e. `tetration_os_enforcement_k9-3.6.1.5-1.el6.x86_64.rpm`

f. `tetration_os_base_rpm_k9-3.6.1.5-1.el7.x86_64.rpm`

For a virtual system, upload the following files in the given order:

a. `tetration_os_rpminstall_k9-3.6.1.5-1.noarch.rpm`

b. `tetration_os_adhoc_k9-3.6.1.5-1.el6.x86_64.rpm`

c. `tetration_os_mother_rpm_k9-3.6.1.5-1.el6.x86_64.rpm`

d. `tetration_os_enforcement_k9-3.6.1.5-1.el6.x86_64.rpm`

e. `tetration_os_ova_k9-3.6.1.5-1.el7.x86_64.rpm`

To upload each RPM, perform the following substeps

a) Click **Choose File**.
b) Navigate to an RPM, choose it, and click **Open**.
c) Click **Upload**.

The list of RPMs on the page does not update as you upload each RPM. This is expected.

If you see an error after uploading the `tetration_os_mother_rpm_k9-3.6.1.5-1.el6.x86_64.rpm` file, simply wait about 5 to 10 minutes, then reload the page. You should see the list of uploaded RPMs after reloading the page.

d) Repeat these substeps for each RPM.

Step 9 Click **Continue**.

The **Site Config** portal opens.

Step 10 On the **General** tab:

(Optional) Change the SSH public key.

Step 11 Click **Next**.

Step 12 On the **Email** tab:

(Optional) Change the UI admin email address or the admiral alert email address.

Step 13 Click **Next**.

Step 14 On the **L3** tab:

(Optional) Enable the cluster to use IPv6 in addition to IPv4 for certain cluster connectivity after upgrade.

Important! For requirements and limitations, see the link in the prerequisites to this procedure.

To enable IPv6:

a) Select the **IPv6** checkbox.
b) Enter the **IPv6 address in CIDR notation** for both Leaf 1 and Leaf 2 switches.
c) Enter the Leaf1 and Leaf2 **IPv6 Default Gateway**.

If you enable IPv6 on this page, you must also configure IPv6 fields on the **Network** page, below.

Step 15 Click **Next**.

Step 16 On the **Network** tab:

- If necessary, change the values for **CIMC Internal Network**, **CIMC Internal Network Gateway**, **DNS Resolver**, and **DNS Domain**.
- **Important!** Do not change or remove the existing **External Network** value. However, you can add additional IPv4 networks.
- If you enabled IPv6 on the L3 page:

  The **IPv6** checkbox is automatically selected.

  Specify IPv6 addresses reserved for Secure Workload use:

  a. Enter the **IPv6 External Network in CIDR notation**.

  b. (Optional) To use IPv6 only for specified addresses, enter individual **External IPv6 IPs**.

  Keep in mind:

  - The first 3 IPv6 addresses in the IPv6 External Network field are always reserved for the switches of the Secure Workload cluster and should not be used for any other purpose.
  - For a 39 RU cluster, ensure that at least 29 IPv6 addresses are available in the IPv6 External Network or the External IPv6 IPs list.
  - For an 8 RU cluster, ensure that at least 20 IPv6 addresses are available in the IPv6 External Network or the External IPv6 IPs list.

Step 17 Click **Next**.

Step 18 On the **Service** tab:

(Optional) Change the NTP and SMTP values.

If you need to change syslog values (if any) use the TAN appliance.

Step 19 Click **Next**.

Step 20 On the **Security** tab:

Enable or disable the **Strong SSL Ciphers for Agent Connections**.

Step 21 Click **Next**.

You cannot change any of the values on the **UI** tab.

Step 22 Click **Next**.

You cannot change any of the values on the **Advanced** tab.

Step 23 Click **Next**.

Step 24 On the **Recovery** tab:

If the cluster is configured to be a standby cluster, the cluster will deploy in standby mode which includes reduced functionality (only to support warm standby mode.)

You cannot change any of the values on this tab.

Step 25 Click **Continue**.

The upgrade process begins.

The upgrade process checks to ensure:

- The RPM versions are correct
- The cluster is healthy
- The site information you provided is valid
- The switches are configured correctly
- Info fields are validated
- NTP is synchronized before deployment starts
- Namenode and secondary namenode are not in a failed-over state

The checks will take several minutes. After the checks are complete, you will receive an email with a subject similar to this:

```
TETRATION CLUSTER MyCluster: Verify Token
```

The message contains a token that you will need in order to continue the upgrade.

Step 26 Copy the token from the body of the email message.

Step 27 In the Cisco Secure Workload Setup portal, paste the token into the **Validation Token** field.

Important! Do not select the **Ignore instance stop failures** checkbox, unless specifically instructed to do so by a Cisco employee.

Step 28 Click **Continue**.

The upgrade installation begins. When the green progress bar reaches 100%, the upgrade is complete. All of the instances will show the “Deployed” status.

Step 29 Verify the upgrade:

a) Open the Cisco Secure Workload web portal in your browser.
b) From the black navigation menu on the left, choose **Platform > Upgrade/Reboot/Shutdown**.
c) Click **History**.
d) Verify that upgrade status shows **Succeeded**.

What to do next

If you have enabled IPv6:

- You can access the Secure Workload web interface using either IPv6 or IPv4.
- By default, software agents continue to connect to the cluster using IPv4. If you want software agents to be able to communicate with the cluster using IPv6, perform these actions:
  1. On the Secure Workload UI, in the left navigation pane, click **Platform** > **Cluster Configuration**.
  2. Configure the **Sensor VIP FQDN** setting. For more details, see the page-level help or the Secure Workload user guide available on Cisco.com.