Revised: May 15, 2025

UTD Container Management for SD-Routing devices, Release 17.16.x

What's new and changed

Cisco IOS XE Release	Feature Name and Description	Supported Platforms
Cisco IOS XE 17.16.1a	**UTD Container Management for SD-Routing Devices** When Cisco IOS-XE autonomous devices transition to Cisco SD-Routing mode, the Unified Threat Defense (UTD) Container Migration feature ensures that existing container functionalities are preserved. From Cisco IOS XE 17.16.1a you can detect, upgrade, and manage UTD Security Virtual Images through Cisco Catalyst SD-WAN Manager. For devices without pre-existing containers, you can also install and manage UTD images using policy groups.	• Cisco Catalyst 8000V Edge Software • Cisco Catalyst 8500 Series Edge Platforms • Cisco Catalyst 8300 Series Edge Platforms • Cisco Catalyst 8200 Series Edge Platforms • Cisco 1000 Series Integrated Services Routers • Cisco 4000 Integrated Services Router • Cisco ASR 1000 Series Aggregation Services Routers • Cisco Catalyst 1835 Rugged Router • Cisco Catalyst IR8340 Rugged Series Routers

Overview on UTD Container Management for SD-Routing Devices

Unified Threat Defense (UTD) Container Migration feature facilitates seamless transition for existing IOS-XE autonomous routers as they migrate to SD-Routing mode. Many field-deployed routers run versions earlier than 17.12.1a and may have pre-configured containers. As these devices onboard to SD-Routing, it's critical that their existing container functionalities remain intact. This feature supports to detect, upgrade, and handle UTD Security Virtual Image updates for these devices using Cisco Catalyst SD-WAN manager when transitioning from autonomous to SD-Routing mode.

Cisco SD-WAN Manager uses UTD Security Virtual Image to enable features such as Intrusion Prevention System (IPS), Intrusion Detection System (IDS), URL Filtering (URL-F), and Advanced Malware Protection (AMP) on Cisco SD-Routing Devices. These features enable application hosting, real-time traffic analysis, and packet logging on IP networks. In cases where there are no pre-existing containers, users can have UTD Security Virtual Images freshly installed and managed through policy groups using SD-WAN Manager.

View and Manage UTD Security Virtual Images

For devices without pre-existing containers, the SD-WAN Manager supports fresh installation, deletion and management of UTD containers through policy groups. To know more about creating and deploying Configuration Groups refer, Create SD-Routing Configuration Groups Using Configuration Group Menu

For devices with pre-existing UTD configurations SD-WAN Manager can detect, upgrade, and handle UTD Security Virtual Image updates without affecting their current configuration and functionality.

View UTD Container Details

To view information about existing UTD container services, navigate to **Maintenance** > **Software Upgrade** > **WAN Edge**. Locate the **Available Services** column adjacent to the preferred device row. This column indicates the number of containers available for the device. Click on the number to view more details. The **Container Details** dialog box will open, displaying the following specifics.

Parameters	**Description**
Service Name	Name of the container services
Current Version	Version of the UTD Container
Service State	Current state of the UTD Service

Upload UTD Security Virtual Images to Software Repository

To upload the UTD Virtual Image to Cisco SD-WAN Manager, follow the below steps:

Step 1 From software.cisco.com page, locate the image UTD Engine for your SD-Routing device.

Step 2 Click **download** to save the image file.

Step 3 From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository**.

Step 4 Select **Virtual Images**.

Step 5 From the **Add New Virtual Image** Drop down, choose one of the following options:

- Remote Server (preferred)
- Manager
- Remote Server-Manager

Step 6 If **Remote Server (preferred)** is selected, configure the following:

a. Image File Name

b. (optional) Image Description

c. (optional) Add Tags

d. Select Service Type

e. In the Remote Server tab, Provide Remote Server Name and Image File Path

f. To add more servers Click **Add Remote Server**.

g. Click **Save**

Step 7 If **Manager** is selected

a. The **Upload VNF’s Package to Manager** window opens.

b. Drag and drop, or browse to the image file.

c. Click **Upload**.

Step 8 If **Remote Server-Manager** is selected

a. The **Upload VNF's Package to Remote Server Details** window opens.

b. Type the **Manager Hostname/ IP Address**

c. Drag and drop, or browse to the image file.

d. Click **Upload**

Upgrade UTD Security Virtual Image

When a Cisco IOS XE SD-Routing device is upgraded to a new software image, the UTD virtual image must also be upgraded so that they match.

To upgrade the UTD virtual image for a device, follow these steps:

Step 1 From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade**. The WAN Edge Software upgrade page displays.

Step 2 Choose the devices you want to upgrade, and select the check boxes in the leftmost column. When you have chosen one or more devices, a row of options display, as well as the number of rows you chose.

Step 3 From the **Virtual Image Actions** drop down list, choose **Upgrade Virtual Image**.

Step 4 The **Upgrade Virtual Image** dialog box displays. Select **Manager**.

Step 5 For each device you have chosen, choose the correct upgrade version from the **Upgrade to Version** drop-down menu.

Step 6 When you have chosen an upgrade version for each device, click **Upgrade**.

Activate UTD Security Virtual Image

To activate the virtual image for a device, follow these steps:

Step 1 From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade**. The WAN Edge Software upgrade page displays.

Step 2 Choose the devices you want to activate, and select the check boxes in the leftmost column. When you have chosen one or more devices, a row of options display, as well as the number of rows you chose.

Step 3 From the **Virtual Image Actions** drop down list, choose **Activate Virtual Image**.

Step 4 The **Activate Virtual Image** dialog box displays.

Step 5 For each device you have chosen, select the version you prefer to activate from the **Active Image** drop-down menu.

Step 6 Click **Activate**.

Delete a UTD Security Virtual Image

Active virtual images installed on the device cannot be deleted. You must deactivate them first before you can delete them.

Delete a virtual image for a device from the Software Upgrade

To delete a virtual image for a device from the **Software Upgrade** page, follow these steps

Step 1 From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade**. The WAN Edge Software upgrade page displays.

Step 2 Choose the devices you want to delete, and select the check boxes in the leftmost column. When you have chosen one or more devices, a row of options display, as well as the number of rows you chose.

Step 3 From the **Virtual Image Actions** drop down list, choose **Delete Virtual Image**.

Step 4 The **Delete Virtual Image** dialog box displays. Select **Manager**.

Step 5 Select the Image you prefer to delete.

Step 6 Click **Delete**

Delete a virtual image for a device from the Software Repository

To delete a virtual image for a device from the **Software Repository** page, follow these steps:

Step 1 In the **Cisco SD-WAN Manager**, navigate to **Maintenance** > **Software Repository**.

Step 2 Select **Virtual Images**.

Step 3 Find the image you prefer to delete and check the box in the leftmost column next to it.

Step 4 Click on the **ellipsis (...)** in the Action column.

Step 5 Select **Delete Image**.

Update UTD signature

Steps to Enable Signature Updates for UTD Snort Engine on SD-Routing Devices

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings.**

Step 2 Click **Edit** in the **UTD Snort Subscriber Signature** row.

Step 3 Enter the preferred interval in the **IPS Signature Download Interval Hours** and **Minute** fields. You can enter an interval from 2 hours to 24 hours. The default interval is 24 hours.

Step 4 To enable the IPS signature package update, enable the **IPS Signatures** option, then click one of the following radio buttons to specify how the IPS signature packages are distributed by Cisco SD-WAN Manager:

- **Cisco.com**: Downloads IPS packages from Cisco.com to SD-WAN Manager.
- **Remote Server**: Downloads from a configured remote server instead of Cisco SD-WAN Manager. Recommended to avoid scaling issues.
- **Local**: Upload IPS signature packages from a local computer to SD-WAN Manager.

Step 5 Configure Remote Server (if selected)

- From the **Select Remote Server** dropdown, choose an existing remote server or click **Add Remote Server** to configure a new one.

- Enter server details such as **Server Name**, **IP/DNS**, **Protocol**, **Port**, **Username**, and **Password**.
- In the **IPS Signature Filename** field, enter the filename or symbolic link for the IPS signature package.
- In the **IPS Signature Snort Version** field, specify the Snort engine version.

Step 6 : If using **Local** method, click **Choose Files** to select the IPS signature package or drag and drop the file, then click **Add**.

Step 7 Manage Custom Signature Rules (Optional)

- To append custom signature rules, enable **Custom Signature**.
- Choose the location for the custom signature rules file:
  - **Remote Server**: Download custom signature rules from a configured remote server.
  - **Local**: Upload a custom signature rules file from a local computer to SD-WAN Manager.
- Ensure the custom signature file meets the Snort version format and size requirements.

Step 8 After configuring the signature updates and custom signatures, click **Add** to save changes.