Security Virtual Image

vManage uses a Security Virtual Image to enable security features such as IPS, URL-Filtering, and AMP on Cisco IOS XE SD-WAN Devices. Before you use these features, you must upload the relevant Security Virtual Image to vManage. After upgrading the software on the device, you must also upgrade the Security Virtual Image.

This chapter describes how to perform these tasks.

Install and Configure IPS/IDS, URL-F, or AMP Security Policies

Installing and configuring IPS/IDS, URL-F, or AMP security policies require the following workflow:

Task 1: Create a Security Policy Template for IPS/IDS, URL-F, or AMP Filtering

Task 2: Create a Feature Template for Security App Hosting

Task 3: Create a Device Template

Task 4: Attach Devices to the Device Template

Create a Security Policy Template

1. From the Cisco vManage menu, choose **Configuration** > **Security**.
2. Click **Add Security Policy**.
3. In the **Add Security Policy** window, select your security scenario from the list of options.
4. Click **Proceed**.

Create a Feature Template for Security App Hosting

The feature profile template configures two functions:

- **NAT:** Enables or disables Network Address Translation (NAT), which protects internal IP addresses when outside the firewall.

- **Resource Profile:** Allocates default or high resources to different subnets or devices.

Note A feature profile template, while not strictly required, is recommended.

To create a feature profile template, follow these steps:

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates** and then click **Add Template**.

   Note In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is called **Feature**.

3. From the **Select Devices** list, choose the devices that you want to associate with the template.
4. Under **Basic Information**, click **Security App Hosting**.
5. Enter **Template Name** and **Description**.
6. Under **Security Policy Parameters**, customize the security policy parameters if required.
   - Enable or disable the Network Address Translation (NAT) feature, based on your use case. By default, **NAT** is on.
   - Click the drop-down arrow to set boundaries for the policy. The default is **Default**.

     Global: Enables NAT for all devices attached to the template.

     Device Specific: Enables NAT only for specified devices. If you select **Device Specific**, enter the name of a device key.

     Default: Enables the default NAT policy for devices attached to the template.
   - Set **Resource Profile**. This option sets the number of snort instances to be used on a router. The default is **Low** that indicates one snort instance. **Medium** indicates two instances and **High** indicates three instances.
   - Click the drop-down arrow to set boundaries for the resource profile. The default is **Global**.

     Global: Enables the selected resource profile for all devices attached to the template.

     Device Specific: Enables the profile only for specified devices. If you select **Device Specific**, enter the name of a device key.

     Default: Enables the default resource profile for devices attached to the template.
7. Set **Download URL Database on Device** to **Yes** if you want to download the URL-F database on the device. In this case, the device looks up in the local database before trying the cloud lookup.
8. Click **Save**.

Create a Device Template

To activate the policies you want to apply, you can create a device template that will push the policies to the devices that need them. The available options vary with the device type. For example, Cisco vManage devices require a more limited subset of the larger device template. You will see only valid options for that device model.

To create a security device template, follow this example for vEdge 2000 model routers:

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**, and then choose **Create Template** > **From Feature Template**.

Note In Cisco vManage Release 20.7.1 and earlier releases, **Device Templates** is called **Device**.

3. From the **Device Model** drop-down list, choose the device model.
4. From the **Device Role** drop-down list, choose the device role.
5. Enter **Template Name** and **Description**.
6. Scroll down the page to the configuration submenus that let you select an existing template, create a new template, or view the existing template. For example, to create a new System template, click **Create Template**.

Attach Devices to the Device Template

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**, and then choose **Create Template** > **From Feature Template**.

Note In Cisco vManage Release 20.7.1 and earlier releases, **Device Templates** is called **Device**.

3. In the row of the desired device template, click **...** and choose **Attach Devices**.
4. In the **Attach Devices** window, select the desired devices from the **Available Devices** list, and click the right-pointing arrow to move them to the **Selected Devices** list.
5. Click **Attach**.

Identify the Recommended Security Virtual Image Version

At times, you may want to check the recommended Security Virtual Image (SVI) release number for a given router. To check this using vManage:

Step 1 From the vManage dashboard, select **Monitor** > **Network**.

Step 2 Choose **WAN – Edge**.

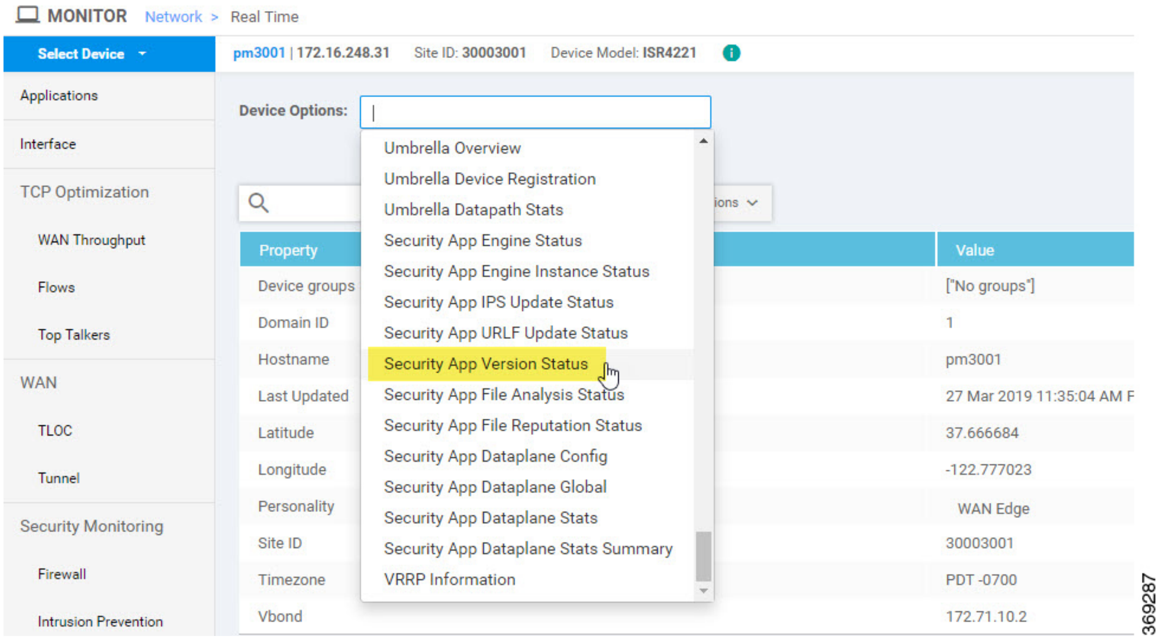
Step 3 Select the device that will run the SVI.

The System Status page displays.

Step 4 Scroll to the bottom of the device menu, and click **Real Time**.

The System Information page displays.

Step 5 Click the **Device Options** field, and select **Security App Version Status** from the menu list.



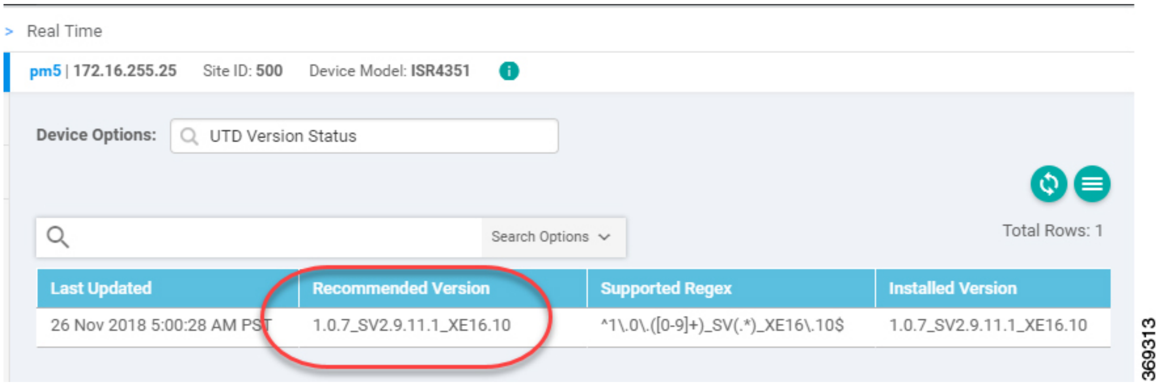
MONITOR Network > Real Time
Select Device
Applications
Interface
TCP Optimization
WAN Throughput
Flows
Top Talkers
WAN
TLOC
Tunnel
Security Monitoring
Firewall
Intrusion Prevention
Umbrella Overview
Umbrella Device Registration
Umbrella Datapath Stats
Security App Engine Status
Security App Engine Instance Status
Security App IPS Update Status
Security App URLF Update Status
Security App Version Status
Security App File Analysis Status
Security App File Reputation Status
Security App Dataplane Config
Security App Dataplane Global
Security App Dataplane Stats
Security App Dataplane Stats Summary
VRRP Information
369287

pm3001 | 172.16.248.31 Site ID: 30003001 Device Model: ISR4221

Device Options:

Property	Value
Device groups	["No groups"]
Domain ID	1
Hostname	pm3001
Last Updated	27 Mar 2019 11:35:04 AM F
Latitude	37.666684
Longitude	-122.777023
Personality	WAN Edge
Site ID	30003001
Timezone	PDT -0700
Vbond	172.71.10.2

Step 6 Note the image name in the Recommended Version column. It should match the available SVI for your router from the Cisco downloads website.



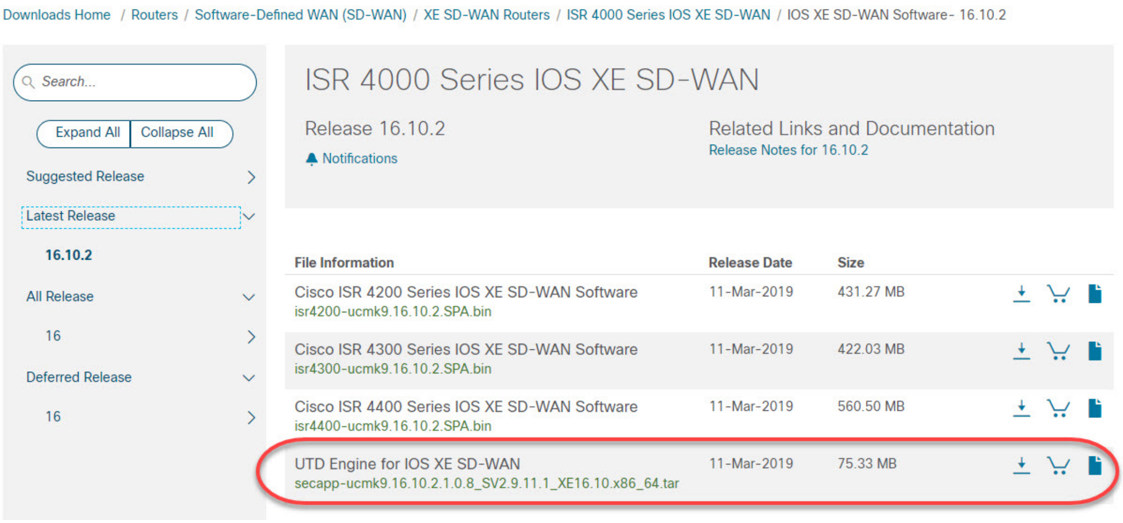
pm5 | 172.16.255.25 Site ID: 500 Device Model: ISR4351

Device Options: UTD Version Status

Last Updated	Recommended Version	Supported Regex	Installed Version
26 Nov 2018 5:00:28 AM PST	1.0.7_SV2.9.11.1_XE16.10	^1\.0\.([0-9]+)_SV(.*)_XE16\.10$	1.0.7_SV2.9.11.1_XE16.10

Upload the Cisco Security Virtual Image to vManage

Each router image supports a specific range of versions for a hosted application. For IPS/IDS and URL-Filtering, you can find the range of supported versions (and the recommended version) for a device on its Device Options page.



Downloads Home / Routers / Software-Defined WAN (SD-WAN) / XE SD-WAN Routers / ISR 4000 Series IOS XE SD-WAN / IOS XE SD-WAN Software- 16.10.2

ISR 4000 Series IOS XE SD-WAN

Release 16.10.2

Notifications

Related Links and Documentation

Release Notes for 16.10.2

File Information	Release Date	Size
Cisco ISR 4200 Series IOS XE SD-WAN Software isr4200-ucmk9.16.10.2.SPA.bin	11-Mar-2019	431.27 MB
Cisco ISR 4300 Series IOS XE SD-WAN Software isr4300-ucmk9.16.10.2.SPA.bin	11-Mar-2019	422.03 MB
Cisco ISR 4400 Series IOS XE SD-WAN Software isr4400-ucmk9.16.10.2.SPA.bin	11-Mar-2019	560.50 MB
UTD Engine for IOS XE SD-WAN secapp-ucmk9.16.10.2.1.0.8_SV2.9.11.1_XE16.10.x86_64.tar	11-Mar-2019	75.33 MB

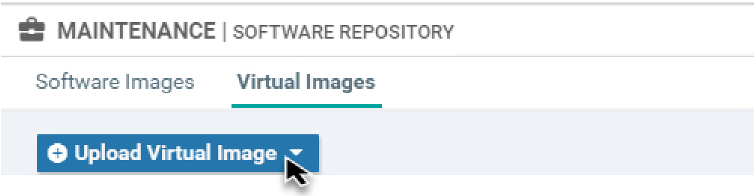
369288

Step 1 From the Software Download page for your router, locate the image "**UTD Engine for IOS XE SD-WAN**."

Step 2 Click the **download** icon on the right-hand side of the window to download the image file.

Step 3 From the vManage dashboard, select **Maintenance** > **Software Repository**.

Step 4 Select **Virtual Images** from the top options.



369320

Step 5 Click **Upload Virtual Image**, and select either **vManage** or **Remote Server – vManage**. The Upload Virtual Image to vManage window opens.

Step 6 Drag and drop, or browse to the image file and select it.

Step 7 Click **Upload**. When the upload completes, a confirmation message displays. The new virtual image displays in the Virtual Images Software Repository.

Upgrade a Security Virtual Image

When a Cisco IOS-XE SD-WAN router is upgraded to a new software image, the security virtual image must also be upgraded to match.

Note If the IPS Signature Update option is enabled, the matching IPS signature package is automatically updated as a part of the upgrade. You can enable the setting from **Administration** > **Settings** > **IPS Signature Update**.

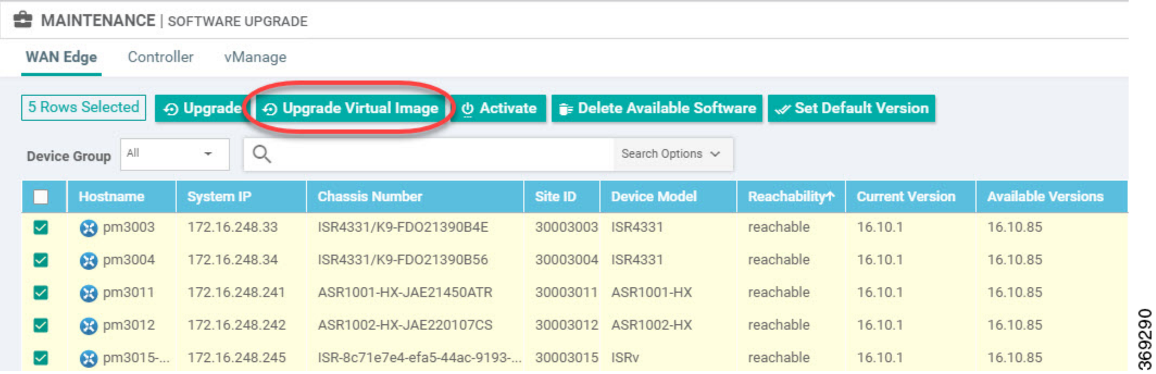
To upgrade the application hosting virtual image for a device, follow these steps:

Step 1 Follow the steps in "Upload the Correct Cisco Security Virtual Image to vManage" to download the recommended version of the SVI for your router. Note the version name.

Step 2 From the vManage menu, select **Maintenance** > **Software Repository** > **Virtual Images** to verify that the image version listed under the Recommended Version column matches a virtual image listed in the Virtual Images table.

Step 3 Select **Maintenance** > **Software Upgrade**. The WAN Edge Software upgrade page displays.

Step 4 Select the devices you want to upgrade by clicking the boxes in the leftmost column. When you have selected one or more devices, a row of options display, as well as the number of rows you selected.

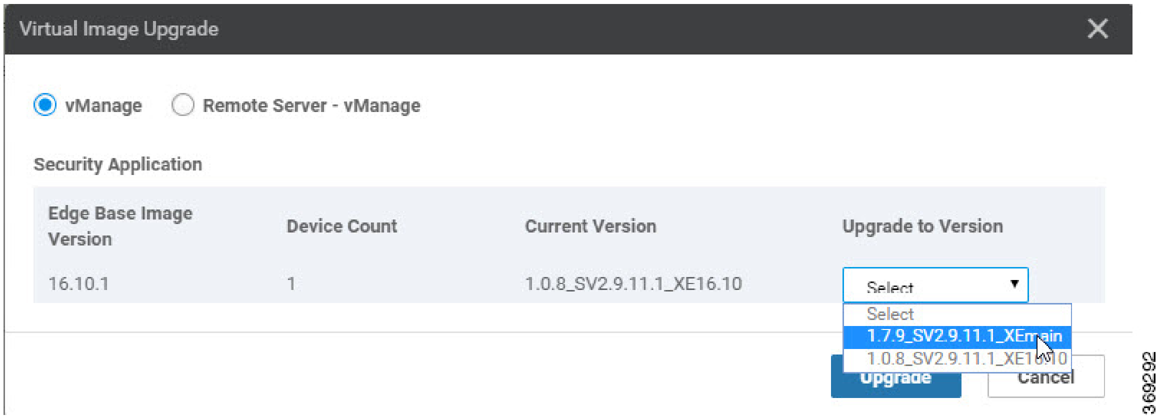


Device Group: All

☐	Hostname	System IP	Chassis Number	Site ID	Device Model	Reachability↑	Current Version	Available Versions
☑	pm3003	172.16.248.33	ISR4331/K9-FDO21390B4E	30003003	ISR4331	reachable	16.10.1	16.10.85
☑	pm3004	172.16.248.34	ISR4331/K9-FDO21390B56	30003004	ISR4331	reachable	16.10.1	16.10.85
☑	pm3011	172.16.248.241	ASR1001-HX-JAE21450ATR	30003011	ASR1001-HX	reachable	16.10.1	16.10.85
☑	pm3012	172.16.248.242	ASR1002-HX-JAE220107CS	30003012	ASR1002-HX	reachable	16.10.1	16.10.85
☑	pm3015-...	172.16.248.245	ISR-8c71e7e4-efa5-44ac-9193-...	30003015	ISRv	reachable	16.10.1	16.10.85

Step 5 When you are satisfied with your choices, select **Upgrade Virtual Image** from the options menu. The Virtual Image Upgrade dialog box opens.

Step 6 For each device you selected, select the correct upgrade version from the **Upgrade to Version** drop-down list.



● vManage ○ Remote Server - vManage

Security Application

Edge Base Image Version	Device Count	Current Version	Upgrade to Version
16.10.1	1	1.0.8_SV2.9.11.1_XE16.10	Select

Step 7 When you have selected an upgrade version for each device, click **Upgrade**. When the update completes, a confirmation message displays.