

Unified Threat Defense Resource Profiles

Table 1: Feature History

Feature Name	Release Information	Description
Configure Unified Threat Defense Resource Profiles	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This feature lets you customize the amount of resources that Unified Threat Defense features use on a router. You can use larger resource profiles to process packets simultaneously. Simultaneously processing packets reduces the latency that security features can introduce to the packet processing of the device.
Unified Threat Defense Support for Cisco 8100, 8200 and 8300 Series Secure Routers	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a	UTD supports the following next-generation devices: • Cisco 8100 Series Secure Routers: C8151-G2 and C8161-G2 • Cisco 8200 Series Routers: C8235-E-G2, C8231-E-G2, C8235-G2 and C8231-G2 • Cisco 8300 Series Routers: C8355-G2
Unified Threat Defense Support for Cisco 8100 Series Secure Routers	Cisco Catalyst SD-WAN Manager Release 26.1.1.1	UTD extends support on next-generation Cisco 8100 Series Secure Routers: C8131-G2, C8151-CVAI-G2, C8151-CVAP-G2.

Unified Threat Defense features use the Snort engine to process packets. Snort is an open source network Intrusion Prevention System, capable of performing real-time traffic analysis and packet logging on IP networks. Unified Threat Defense deploys Snort as a single instance on the device to process packets. To

improve performance, use the Security App Hosting feature template to allow Unified Threat Defense to use more resources.

You can use the Security App Hosting feature template to modify the resource profile as follows:

- Deploy more instances of Snort: When you enable Unified Threat Defense, the device sends each packet from the data plane to the service plane. Unified Threat Defense serially inspects each packet. Once inspected, Unified Threat Defense returns the packet to the data plane. Unified Threat Defense holds each packet to analyze it. These processes introduce latency to the flow of packets that affects the throughput of the device. To combat this latency, you can deploy more instances of Snort. With multiple instances of Snort available, Unified Threat Defense can simultaneously process multiple packets to reduce latency and increase throughput. This feature uses more systems resources.
- Download URL databases to the devices: This feature allows the URL Filtering feature of Unified Threat Defense to use a downloaded URL database on the device to find a URL. If the device downloads the database, Unified Threat Defense first uses the database on the device to find the URL. If a URL is not in the downloaded database, Unified Threat Defense connects to the Cloud for the URL information. This Cloud result is saved to a local cache for any subsequent requests to the same URL. This feature requires at least 16 GB bootflash and 16 GB RAM.

Note The Next-Generation Firewall (NGFW) features like, Intrusion Prevention System (IPS), Advanced Malware Protection (AMP), and URL Filtering (URL-F) with data plane heavy profiles are not supported.

- Supported Platforms, on page 2
- Configure Unified Threat Defense Resource Profiles , on page 4
- Verify Unified Threat Defense Resource Profiles, on page 5

Supported Platforms

Note To download the database, the device must have at least 16 GB bootflash and 16 GB RAM.

Platform	Download Database Options	Supported Resource Profile
Cisco Integrated Services Routers (ISR) 1000 C1111	No	low
Cisco ISR1100X-4G	No	low
Cisco ISR1100X-6G	Yes	low
Cisco ISR 4221 and Cisco ISR 4321	No	low
Cisco Integrated Services Virtual Router (ISRv)	No	low

Platform	Download Database Options	Supported Resource Profile
Cisco ISR4331, Cisco ISR4351, Cisco ISR4431 Cisco ISR4451, and Cisco ISR4461	Yes	low, medium, high
Cisco Catalyst 8000V	Yes	low low, medium, high for Cisco IOS XE Catalyst SD-WAN Release 17.12.1, Cisco IOS XE Catalyst SD-WAN Release 17.15.1 and later releases.
Cisco Catalyst 8200 Series Edge Platforms	Yes	low, medium, high
Cisco Catalyst 8300 Series Edge Platforms	Yes	low, medium, high
Cisco Catalyst 8500 Series Edge Platform C8500L-8S4X	Yes	low, medium, high
Cisco 8100 Series Secure Routers C8151-G2, C8161-G2	No **Note** C8100-G2 doesn't support download database as it has 8 GB memory.	low, medium, cloud-low, cloud-medium **Note** Supported from Cisco IOS XE Catalyst SD-WAN Release 17.18.1a
Cisco 8100 Series Secure Routers C8131-G2, C8151-CVAI-G2, C8151-CVAP-G2	No **Note** C8100-G2 doesn't support download database as it has 8 GB memory.	low, medium, cloud-low, cloud-medium **Note** Supported from Cisco IOS XE Catalyst SD-WAN Release 26.1.1
Cisco 8200 Series Secure Routers: C8235-E-G2, C8231-E-G2, C8235-G2 and C8231-G2	Yes	low, medium, cloud-low, cloud-medium **Note** Supported from Cisco IOS XE Catalyst SD-WAN Release 17.18.1a
Cisco 8300 Series Secure Routers: C8375-E-G2	Yes	low, medium, cloud-low, cloud-medium **Note** Supported from Cisco IOS XE Catalyst SD-WAN 17.15.3
Cisco 8300 Series Secure Routers: C8355-G2	Yes	low, medium, cloud-low, cloud-medium **Note** Supported from Cisco IOS XE Catalyst SD-WAN Release 17.18.1a

Platform	Download Database Options	Supported Resource Profile
Cisco 8400 Series Secure Routers: C8400-G2	Yes	low, medium, cloud-low, cloud-medium **Note** Supported from Cisco IOS XE Catalyst SD-WAN 17.15.3
Cisco Catalyst IR8140 Heavy Duty Series Router	No	Cloud-low
Cisco Catalyst IR8340 Rugged Series Router	No	Cloud-low
Cisco Catalyst IR1835 Rugged Router	No	Cloud-low

Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.12.2, for all ISR1100 platforms, you must reboot the device to change resource profiles to allocate sufficient resources to the service plane to run containers. Use the **platform resource service-plane-heavy** command to allocate resources.

Note IR8140 does not support SSL proxy.

Configure Unified Threat Defense Resource Profiles

Configure the Unified Threat Defense Resource Profiles Using Cisco SD-WAN Manager

You can configure the Unified Threat Defense resource profiles using Cisco Catalyst SD-WAN Manager by doing the following:

1. From the Cisco SD-WAN Manager 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. Choose the device(s).
4. Click **Security App Hosting**.

Note Starting with Cisco Catalyst SD-WAN Manager Release 20.15.1 and Cisco Catalyst SD-WAN Manager Release 26.1.1.1, when configuring Unified Threat Defense, both the VirtualPortGroup interface IP address and the guest interface IP address are automatically allocated from the same /16 subnet. This ensures proper communication between the gateway and application, and resolves previous issues where addresses could be assigned from different /24 subnets in large-scale deployments. No manual intervention is required.

5. Enter a template name and description.
6. Choose whether to enable or disable NAT. NAT is enabled by default.

   To use Unified Threat Defense features that connect to the internet, you must enable NAT. For example, URL Filtering and Advanced Malware Protection connect to the internet to perform Cloud lookups. To use these features, enable NAT.
7. To download the URL database on the device, choose **Yes**.
8. To deploy more instances of Snort, choose one of the following resource profiles:
   - **Low**: This is the default profile.
   - **Medium**.
   - **High**.

   When you specify a larger resource profile, the device deploys more Snort instances to increase throughput. The larger resource profiles also use more resources on the device. The number of Snort instances deployed by the device differs by platform and software release.
9. Click **Save**.
10. Add this template to the device template.
11. Attach the device template to the device.

Verify Unified Threat Defense Resource Profiles

To view the Unified Threat Defense resource profiles that you configured, run the following commands:

```
show app-resource package-profile
show run | section app-hosting appid utd
show app-hosting detail appid utd | section Activated profile name
```

To view the resource usage between activated resource profiles, run the following commands:

```
show platform software status control-processor brief
show platform hardware qfp active datapath utilization
show utd engine standard utilization cpu
show utd engine standard utilization memory
show app-hosting resource
```

To view the health of one or more Snort instances and the memory usage of UTD, run the following command:

```
show utd engine standard status
```