Configuring SDM Templates

- Information About SDM Templates, on page 1
- How to Configure SDM Templates, on page 1
- Monitoring and Maintaining SDM Templates, on page 2
- Configuration Examples for SDM Templates, on page 3
- Additional References for SDM Templates, on page 6
- Feature History for SDM Templates, on page 6

Information About SDM Templates

You can use SDM templates to configure system resources to optimize support for specific features, depending on how your device is used in the network. You can select a template to provide maximum system usage for some functions.

Cisco Catalyst 9300 Series Switches supports the following templates:

- Access
- NAT

After you change the template and the system reboots, you can use the **show sdm prefer** privileged EXEC command to verify the new template configuration. If you enter the **show sdm prefer** command before you enter the **reload** privileged EXEC command, the **show sdm prefer** command shows the template currently in use and the template that will become active after a reload.

How to Configure SDM Templates

Setting the SDM Template

Follow these steps to use the SDM template to maximize feature usage:

Procedure

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**sdm prefer access | nat** **Example:** `Device(config)# sdm prefer access`	Sets the switch to the access template.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.
Step 5	**reload** **Example:** `Device# reload`	Reloads the operating system. After the system reboots, you can use the **show sdm prefer** privileged EXEC command to verify the new template configuration. If you enter the **show sdm prefer** command before you enter the reload privileged EXEC command, the **show sdm prefer** command shows the template currently in use and the template that will become active after a reload.

Monitoring and Maintaining SDM Templates

Verifying SDM Templates

Use the following commands to monitor and maintain SDM templates.

Command	Purpose
show sdm prefer	Displays the SDM template in use.
reload	Reloads the switch to activate the newly configured SDM template.

Note The SDM templates contain only those commands that are defined as part of the templates. If a template enables another related command that is not defined in the template, then this other command will be visible when the **show running config** command is entered. For example, if the SDM template enables the **switchport voice vlan** command, then the **spanning-tree portfast edge** command may also be enabled (although it is not defined on the SDM template).

If the SDM template is removed, then other such related commands are also removed and have to be reconfigured explicitly.

Verifying Customizable SDM Templates

Use the following commands to verify the customizable SDM Template that will be applied.

Table 1: Commands to verify the customizable SDM template

Command	Description
show sdm prefer custom	Displays the custom values that will be applied to the features in the customizable SDM template.
show sdm prefer custom user-input	Displays the values that were entered by the user in the customizable SDM template.
show sdm prefer	Displays the customized SDM template that is currently active.

If any feature in the Customizable SDM template has been assigned a scale value of zero, the feature will not be listed in the output of the **show sdm prefer custom** command after the device is reloaded.

Configuration Examples for SDM Templates

Examples: Displaying SDM Templates

The following example output shows the Access template information on Cisco Catalyst 9300 Series Switches:

```
Device# show sdm prefer access

This is the Access template.
  Number of VLANs:                                4094
  Unicast MAC addresses:                          32768
  Overflow Unicast MAC addresses:                 1024
  L2 Multicast entries:                           8192
  Overflow L2 Multicast entries:                  512
  L3 Multicast entries:                           8192
  Overflow L3 Multicast entries:                  512
  Directly connected routes:                      24576
  Indirect routes:                                8192
  Security Access Control Entries:                5120
  QoS Access Control Entries:                     5120
  Policy Based Routing ACEs:                      1024
  Netflow Input ACEs:                             256
```

```
  Netflow Output ACEs:                              768
  Ingress Netflow ACEs:                             256
  Egress Netflow ACEs:                              768
  Flow SPAN ACEs:                                   1024
  Tunnels:                                          512
  LISP Instance Mapping Entries:                    512
  Control Plane Entries:                            512
  Input Netflow flows:                              32768
  Output Netflow flows:                             32768
  SGT/DGT (or) MPLS VPN entries:                    8192
  SGT/DGT (or) MPLS VPN Overflow entries:           512
  Wired clients:                                    2048
  MACSec SPD Entries:                               256
  MPLS L3 VPN VRF:                                  255
  MPLS Labels:                                      2048
  MPLS L3 VPN Routes VRF Mode:                      7168
  MPLS L3 VPN Routes Prefix Mode:                   3072
  MVPN MDT Tunnels:                                 256
  L2 VPN EOMPLS Attachment Circuit:                 256
  MAX VPLS Bridge Domains :                         128
  MAX VPLS Peers Per Bridge Domain:                 32
  MAX VPLS/VPWS Pseudowires :                       1024

These numbers are typical for L2 and IPv4 features.
Some features such as IPv6, use up double the entry size;
so only half as many entries can be created.
* values can be modified by sdm cli.
```

The following example output shows the NAT template information on Cisco Catalyst 9300 Series Switches:

```
Device# show sdm prefer nat

This is the NAT template.
  Number of VLANs:                                  4094
  Unicast MAC addresses:                            32768
  Overflow Unicast MAC addresses:                   1024
  L2 Multicast entries:                             8192
  Overflow L2 Multicast entries:                    512
  L3 Multicast entries:                             8192
  Overflow L3 Multicast entries:                    512
  Directly connected routes:                        24576
  Indirect routes:                                  8192
  Security Access Control Entries:                  5120
  QoS Access Control Entries:                       1024
  Policy Based Routing ACEs:                        5120
  Netflow Input ACEs:                               256
  Netflow Output ACEs:                              768
  Flow SPAN ACEs:                                   1024
  Tunnels:                                          512
  LISP Instance Mapping Entries:                    512
  Control Plane Entries:                            512
  Input Netflow flows:                              32768
  Output Netflow flows:                             32768
  SGT/DGT (or) MPLS VPN entries:                    8192
  SGT/DGT (or) MPLS VPN Overflow entries:           512
  Wired clients:                                    2048
  MACSec SPD Entries:                               256
  MPLS L3 VPN VRF:                                  255
  MPLS Labels:                                      2048
  MPLS L3 VPN Routes VRF Mode:                      7168
  MPLS L3 VPN Routes Prefix Mode:                   8192
  MVPN MDT Tunnels:                                 256
  L2 VPN EOMPLS Attachment Circuit:                 256
  MAX VPLS Bridge Domains :                         128
  MAX VPLS Peers Per Bridge Domain:                 32
```

```
  MAX VPLS/VPWS Pseudowires :                          1024

These numbers are typical for L2 and IPv4 features.
Some features such as IPv6, use up double the entry size;
so only half as many entries can be created.
* values can be modified by sdm cli.
```

The following example output shows the Access template information on the C9300-24UB, C9300-24UXB, and C9300-48UB models of Cisco Catalyst 9300 Series Switches in Cisco IOS XE Amsterdam 17.3.1 and later releases:

```
Device# show sdm prefer access

 Number of VLANs:                                    4094
  Unicast MAC addresses:                             49152
  Overflow Unicast MAC addresses:                    1024
  L2 Multicast entries:                              16384
  Overflow L2 Multicast entries:                     1024
  L3 Multicast entries:                              32768
  Overflow L3 Multicast entries:                     1024
  Directly connected routes:                         49152
  Indirect routes:                                   65536
  Security Access Control Entries:                   18432
  QoS Access Control Entries:                        6144
  Policy Based Routing ACEs / NAT ACEs:              14336
  Netflow Input ACEs:                                1024
  Netflow Output ACEs:                               2048
  Flow SPAN ACEs:                                    1024
  Tunnels:                                           1024
  LISP Instance Mapping Entries:                     2048
  Control Plane Entries:                             512
  Input Netflow flows:                               65536
  Output Netflow flows:                              65536
  SGT/DGT (or) MPLS VPN entries:                     8192
  SGT/DGT (or) MPLS VPN Overflow entries:            512
  Wired clients:                                     2048
  MACSec SPD Entries:                                1024
  VRF:                                               256
  MPLS Labels:                                       12288
  MPLS L3 VPN Routes VRF Mode:                       32768
  MPLS L3 VPN Routes Prefix Mode:                    8192
  MVPN MDT Tunnels:                                  1024
  L2 VPN EOMPLS Attachment Circuit:                  1024
  MAX VPLS Bridge Domains :                          128
  MAX VPLS Peers Per Bridge Domain:                  32
  MAX VPLS/VPWS Pseudowires :                        4096

These numbers are typical for L2 and IPv4 features.
Some features such as IPv6, use up double the entry size;
so only half as many entries can be created.
```

Examples: Configuring SDM Templates

```
Device(config)# sdm prefer access
Device(config)# exit
Device# reload
  Proceed with reload? [confirm]
```

Additional References for SDM Templates

Related Documents

Related Topic	Document Title
For complete syntax and usage information for the commands used in this chapter.	*Command Reference (Catalyst 9300 Series Switches)*

Feature History for SDM Templates

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
Cisco IOS XE Everest 16.5.1a	SDM Template	Standard SDM templates can be used to configure system resources to optimize support for specific features.
Cisco IOS XE Gibraltar 16.12.3	Change in scalability metrics for C9300-24UB, C9300-24UXB, and C9300-48UB devices	The forwarding scale numbers for the following features on the C9300-24UB, C9300-24UXB, and C9300-48UB models of Cisco Catalyst 9300 Series Switches have changed: • Layer 2 Unicast MAC Addresses: 49152 • Layer 3 Multicast: 32768 • QoS Access Control Entries: 6144 • Policy Based Routing ACEs / NAT ACEs: 14336
Cisco IOS XE Amsterdam 17.3.1	Change in scalability metrics for C9300-24UB, C9300-24UXB, and C9300-48UB devices	The forwarding scale numbers for the following features on the C9300-24UB, C9300-24UXB, and C9300-48UB models of Cisco Catalyst 9300 Series Switches have changed: • Layer 2 Unicast MAC Addresses: 49152 • Layer 3 Multicast: 32768 • QoS Access Control Entries: 6144 • Policy Based Routing ACEs / NAT ACEs: 14336

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn.