



Configuring SDM Templates

- [Information About SDM Templates, on page 1](#)
- [SDM Templates and Switch Stacks, on page 5](#)
- [How to Configure SDM Templates, on page 5](#)
- [Monitoring and Maintaining SDM Templates, on page 7](#)
- [Configuration Examples for SDM Templates, on page 7](#)
- [Additional References for SDM Templates, on page 10](#)
- [Feature History for SDM Templates, on page 10](#)

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 9500 Series Switches support the following templates:

- Core
- SDA
- NAT
- Distribution

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.

Customizable SDM Template

Overview of Customizable SDM Template

Switch Device Manager (SDM) templates can be used to configure system resources and optimize support for specific features. However standard SDM templates are defined based on how the device is deployed in the network.

A custom SDM template will allow you to configure the features of the template based on your requirements and not the location of the device in the network. Starting with the Cisco IOS XE Amsterdam 17.3.1 release, you can configure a custom SDM template for Forwarding Information Base (FIB) using the **sdm prefer custom fib** command.

Starting with the Cisco IOS XE Bengaluru 17.4.1 release, you can configure a custom SDM template for Access Control List (ACL) features using the **sdm prefer custom acl** command.

Starting with the Cisco IOS XE Bengaluru 17.5.1 release, you can configure a custom SDM template for 4k VLAN using the **sdm prefer custom vlan** command.

A Customizable SDM template supports the following FIB features:

- Unicast MAC addresses
- Layer 3 Unicast forwarding
- Layer 2 Multicast forwarding
- Layer 3 Multicast forwarding
- Ingress Netflow
- Egress Netflow
- SGT/DGT Index / MPLS VPN Label

A Customizable SDM template supports the following ACL features:

- Ingress Access Control List (ACL)
- Egress ACL
- Ingress Quality of Service (QoS)
- Egress QoS
- Netflow ACL
- Policy Based Routing (PBR)/ Network Address Translation (NAT)
- Locator/ID Separation Protocol (LISP)
- Tunnels

A Customizable SDM template for 4k VLAN supports only the 4K VLAN feature. You can increase the scale of VLAN from 1k to 4k.

A Customizable SDM template for 4k VLAN increases the number of supported Switch Virtual Interfaces (SVI) to 4000.

The following table shows the minimum and maximum scale values that can be configured for each of the FIB features, the step units and the default values that will be applied when no custom values are chosen for a feature.

Table 1: Scale values and Default values for FIB features

Feature name	Scale Values (Min-Max)	Step Units	Default Values
MAC addresses	32768 - 131072	16384	32768

Feature name	Scale Values (Min-Max)	Step Units	Default Values
Unicast routes	65536 - 262144	16384	65536
Layer 2 Multicast	0, 16384 - 32768	16384	16384
Layer 3 Multicast	0, 16384 - 32768	16384	16384
SG Hash/MPLS	0, 32768 - 65536	32768	32768
Ingress Netflow	0, 32768 - 65536	32768	32768
Egress NetFlow	0, 32768 - 65536	32768	0

The following table shows the minimum and maximum scale values that can be configured for each of the ACL features, the step units and the default values that will be applied when no custom values are chosen for a feature.

Table 2: Scale values and Default values for ACL features

Feature name	Scale Values (Min-Max)	Step Units	Default Values
Ingress ACL	4096 - 26624, 27648	2048	4096
Egress ACL	4096 - 26624, 27648	2048	4096
Ingress QoS	1024, 2048 - 16384	2048	1024
Egress QoS	1024, 2048 - 16384	2048	1024
Netflow ACL	1024 - 2048	1024	1024
PBR/ NAT	1024, 2048 - 16384	2048	1024
LISP	1024 - 2048	1024	1024
Tunnels	1024 - 3072	1024	1024

You can determine which features are allocated the resources first by assigning them a priority using the **priority** keyword. The lower the priority-value assigned to a feature the higher its priority in resource allocation. The total value that is assigned to all the features can exceed the maximum supported resource value of 416K for FIB features or 52 K for ACL features, where K is equal to 1024 entries. The resource allocation algorithm will use the priority-values to determine the number of resources assigned to each feature.

Once you have configured a customized template the device will have to be reloaded for the template to take effect.



Note For features where the scale value can be set to zero, you need to specify the scale value as zero. If not, the default value will be assigned as the scale value.

System resource allocation for Customizable SDM Template

The total number of system resources assigned to a Customizable SDM Template is 416K for FIB features and 52K for ACL features. If the total number of all the resources specified exceeds 416K for FIB features or 52K for ACL features, the system starts to lower the number of allotted resources starting with the feature assigned the highest number. A higher priority value or number assigned to a feature indicates a lower priority.

When the total number of resources assigned in the Customizable SDM Template is less than 416K for FIB features or less than 52K for ACL features:

- All the features specified in the template are allotted resources as customized in the template. Any features not specified in the template are allotted the default number of resources.
- If the total number of resources assigned to the FIB features multicast layer 2 and layer 3 exceeds 48K, then the scale of the multicast feature assigned the lower priority is reduced until the total number of resources assigned is equal to 48K.
- Resources that aren't allotted won't be distributed.

When the total number of resources assigned in the Customizable SDM Template is more than 416K for FIB features and more than 52K for ACL features:

- All the features for which a custom scale isn't specified are allotted the default values.
- If the total number of resources assigned to FIB features multicast layer 2 and layer 3 exceeds 48K, then the scale of the multicast feature that is assigned the lower priority is reduced until the total number of resources assigned is less than or equal to 48K.
- The number of resources allotted to the feature with the highest priority value are decreased by the step value.
- If the total number of resources still exceeds 416K for FIB features or 52K for ACL features, the resources allotted to the next feature with the highest priority value are decreased by the step value.
- While lowering the resources allotted to a feature, the scale is lowered only until the default value for that feature. If further adjustment is required, the resources allotted to the next feature on the priority list are reduced.



Note The custom value entered by you for any feature is rounded up to the next step value. For example, if you enter a value of 40K for SGT it's rounded up to 64K.

Customizable SDM Template and High Availability

On a device which supports High Availability, when a Customizable SDM Template is configured on the active Supervisor it also takes effect on the standby Supervisor.

If the standby Supervisor is configured with a different custom template than the active Supervisor, the Customizable SDM Template of the active Supervisor is configured on the standby Supervisor during initialization.

Customizable SDM Template and StackWise Virtual

On a device which supports StackWise Virtual, when an SDM Template is configured on the active Supervisor it also takes effect on the standby chassis.

If the standby chassis is configured with a different custom template than the active Supervisor, the SDM Template of the active Supervisor is configured on the standby chassis during initialization. The standby chassis undergoes an extra reload for the template to take effect.

Customizable SDM Template and ISSU

When a device undergoes an In-Service Software Upgrade (ISSU) to a higher release and there's a change in the resource allocation algorithm, this upgrade can result in a different scale for the same user input. The change in scale is detected and notified via a syslog message. The system continues to operate with the earlier scale.

You can view the change in scale by using the **show sdm prefer custom scale-change** command. You can apply this change in scale by using the **sdm prefer custom commit** command. The device has to be reloaded for the change to take effect.

When a device with a customizable SDM template for FIB features undergoes a downgrade to a release earlier than the Cisco IOS XE Amsterdam 17.3.1 release, you need to change the SDM template to a static SDM template before the downgrade. You can change the template using the **sdm prefer template name** command. Reload the system for the change to take effect before proceeding with the downgrade.

When a device with a customizable SDM template for ACL features undergoes a downgrade to a release earlier than the Cisco IOS XE Bengaluru 17.4.1 release, you need to change the SDM template to a static SDM template before the downgrade.

When a device has customizable SDM templates for both FIB and ACL features customized in the Cisco IOS XE Bengaluru 17.4.1 release and it downgrades to the Cisco IOS XE Amsterdam 17.3.1 release, the device will be restored with the customizations for the FIB features. The scale numbers for the ACL features will be allotted based on the scale values of the standard SDM template. The information about the customization of the ACL features will be preserved. The device will be restored with the customizations for the ACL features when it upgrades to the Cisco IOS XE Bengaluru 17.4.1 release.

SDM Templates and Switch Stacks

In a switch stack, all stack members must use the same SDM template that is stored on the active switch. When a new switch is added to a stack, the SDM configuration that is stored on the active switch overrides the template configured on an individual switch.

You can use the **show switch** privileged EXEC command to see if any stack members are in SDM mismatch mode.

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 Example: Device> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	sdm prefer { core nat sda distribution } Example: Device(config)# sdm prefer nat	Specifies the SDM template to be used on the switch. The keywords have these meanings: <ul style="list-style-type: none"> • core —Sets the Core template. • nat —Maximizes the NAT configuration on the switch. • sda —Sets the SDA template. • distribution —Sets the Distribution template. <p>Note The no sdm prefer command and a default template is not supported.</p>
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

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.

Configuration Examples for SDM Templates

Examples: Displaying SDM Templates

The following example output shows the core template information on Cisco Catalyst 9500 Series Switches:

```
Device# show sdm prefer core
This is the Core template.
Security Ingress IPv4 Access Control Entries*:      7168 (current) - 7168 (proposed)
Security Ingress Non-IPv4 Access Control Entries*:  5120 (current) - 5120 (proposed)
Security Egress IPv4 Access Control Entries*:       7168 (current) - 7168 (proposed)
Security Egress Non-IPv4 Access Control Entries*:   8192 (current) - 8192 (proposed)
QoS Ingress IPv4 Access Control Entries*:          5632 (current) - 5632 (proposed)
QoS Ingress Non-IPv4 Access Control Entries*:       2560 (current) - 2560 (proposed)
QoS Egress IPv4 Access Control Entries*:           6144 (current) - 6144 (proposed)
QoS Egress Non-IPv4 Access Control Entries*:       2048 (current) - 2048 (proposed)
Netflow Input Access Control Entries*:             1024 (current) - 1024 (proposed)
Netflow Output Access Control Entries*:            1024 (current) - 1024 (proposed)
Flow SPAN Input Access Control Entries*:           512 (current) - 512 (proposed)
Flow SPAN Output Access Control Entries*:          512 (current) - 512 (proposed)
Number of VLANs:                                  4094
Unicast MAC addresses:                             32768
Overflow Unicast MAC addresses:                     768
Overflow L2 Multicast entries:                     2304
L3 Multicast entries:                              32768
Overflow L3 Multicast entries:                     768
Ipv4/Ipv6 shared unicast routes:                  212992
Overflow shared unicast routes:                    1536
Policy Based Routing ACEs / NAT ACEs:              3072
Tunnels:                                           2816
LISP Instance Mapping Entries:                     512
Control Plane Entries:                             1024
Input Netflow flows:                               32768
```

```

Output Netflow flows:                32768
SGT/DGT (or) MPLS VPN entries:       32768
SGT/DGT (or) MPLS VPN Overflow entries: 768
Wired clients:                       2048
MACSec SPD Entries:                 256
MPLS L3 VPN VRF:                    1024
MPLS Labels:                        45056
MPLS L3 VPN Routes VRF Mode:        209920
MPLS L3 VPN Routes Prefix Mode:     32768
MVPN MDT Tunnels:                   1024
L2 VPN EOMPLS Attachment Circuit:    1024
MAX VPLS Bridge Domains :            1000
MAX VPLS Peers Per Bridge Domain:    128
MAX VPLS/VPWS Pseudowires :         16384
Ipv4/Ipv6 Direct and Indirect unicast routes share same space
* values can be modified by sdm cl
These values can vary depending on device and version.

```

The following example output shows the NAT template information on Cisco Catalyst 9500 Series Switches:

```

Device# show sdm prefer nat
This is the NAT template.
Security Ingress IPv4 Access Control Entries*: 7168 (current) - 7168 (proposed)
Security Ingress Non-IPv4 Access Control Entries*: 5120 (current) - 5120 (proposed)
Security Egress IPv4 Access Control Entries*: 3072 (current) - 3072 (proposed)
Security Egress Non-IPv4 Access Control Entries*: 5120 (current) - 5120 (proposed)
QoS Ingress IPv4 Access Control Entries*: 2560 (current) - 2560 (proposed)
QoS Ingress Non-IPv4 Access Control Entries*: 1536 (current) - 1536 (proposed)
QoS Egress IPv4 Access Control Entries*: 3072 (current) - 3072 (proposed)
QoS Egress Non-IPv4 Access Control Entries*: 1024 (current) - 1024 (proposed)
Netflow Input Access Control Entries*: 1024 (current) - 1024 (proposed)
Netflow Output Access Control Entries*: 1024 (current) - 1024 (proposed)
Flow SPAN Input Access Control Entries*: 512 (current) - 512 (proposed)
Flow SPAN Output Access Control Entries*: 512 (current) - 512 (proposed)
Number of VLANs: 4094
Unicast MAC addresses: 32768
Overflow Unicast MAC addresses: 768
Overflow L2 Multicast entries: 2304
L3 Multicast entries: 32768
Overflow L3 Multicast entries: 768
Ipv4/Ipv6 shared unicast routes: 212992
Overflow shared unicast routes: 1536
Policy Based Routing ACEs / NAT ACEs: 15872
Tunnels: 1792
LISP Instance Mapping Entries: 1024
Control Plane Entries: 1024
Input Netflow flows: 32768
Output Netflow flows: 32768
SGT/DGT (or) MPLS VPN entries: 32768
SGT/DGT (or) MPLS VPN Overflow entries: 768
Wired clients: 2048
MACSec SPD Entries: 256
MPLS L3 VPN VRF: 1024
MPLS Labels: 45056
MPLS L3 VPN Routes VRF Mode: 209920
MPLS L3 VPN Routes Prefix Mode: 32768
MVPN MDT Tunnels: 1024
L2 VPN EOMPLS Attachment Circuit: 1024
MAX VPLS Bridge Domains : 1000
MAX VPLS Peers Per Bridge Domain: 128
MAX VPLS/VPWS Pseudowires : 16384
Ipv4/Ipv6 Direct and Indirect unicast routes share same space
* values can be modified by sdm cli

```

The following example output shows the SDA template information on Cisco Catalyst 9500 Series Switches:


```

Device# show sdm prefer sda
This is the SDA template.
  Security Ingress IPv4 Access Control Entries*:      2048 (current) - 2048 (proposed)
  Security Ingress Non-IPv4 Access Control Entries*:  3072 (current) - 3072 (proposed)
  Security Egress IPv4 Access Control Entries*:      16384 (current) - 16384 (proposed)
  Security Egress Non-IPv4 Access Control Entries*:   6144 (current) - 6144 (proposed)
  QoS Ingress IPv4 Access Control Entries*:          5632 (current) - 5632 (proposed)
  QoS Ingress Non-IPv4 Access Control Entries*:      2560 (current) - 2560 (proposed)
  QoS Egress IPv4 Access Control Entries*:           6144 (current) - 6144 (proposed)
  QoS Egress Non-IPv4 Access Control Entries*:       2048 (current) - 2048 (proposed)
  Netflow Input Access Control Entries*:             1024 (current) - 1024 (proposed)
  Netflow Output Access Control Entries*:            1024 (current) - 1024 (proposed)
  Flow SPAN Input Access Control Entries*:           512 (current) - 512 (proposed)
  Flow SPAN Output Access Control Entries*:          512 (current) - 512 (proposed)
  Number of VLANs:                                  4094
  Unicast MAC addresses:                             32768
  Overflow Unicast MAC addresses:                     768
  Overflow L2 Multicast entries:                      2304
  L3 Multicast entries:                              32768
  Overflow L3 Multicast entries:                     768
  Ipv4/Ipv6 shared unicast routes:                  212992
  Overflow shared unicast routes:                    1536
  Policy Based Routing ACEs / NAT ACEs:              2048
  Tunnels:                                           2816
  LISP Instance Mapping Entries:                     2048
  Control Plane Entries:                             1024
  Input Netflow flows:                               32768
  Output Netflow flows:                              32768
  SGT/DGT (or) MPLS VPN entries:                    32768
  SGT/DGT (or) MPLS VPN Overflow entries:            768
  Wired clients:                                     2048
  MACSec SPD Entries:                               256
  MPLS L3 VPN VRF:                                  1024
  MPLS Labels:                                       45056
  MPLS L3 VPN Routes VRF Mode:                      209920
  MPLS L3 VPN Routes Prefix Mode:                   32768
  MVPN MDT Tunnels:                                 1024
  L2 VPN EOMPLS Attachment Circuit:                 1024
  MAX VPLS Bridge Domains :                          1000
  MAX VPLS Peers Per Bridge Domain:                  128
  MAX VPLS/VPWS Pseudowires :                       16384
Ipv4/Ipv6 Direct and Indirect unicast routes share same space
* values can be modified by sdm cli

```

The following example output shows the distribution template information on Cisco Catalyst 9500 Series Switches:

```

Device# show sdm prefer distribution
This is the Distribution template.
  Security Ingress IPv4 Access Control Entries*:      7168 (current) - 7168 (proposed)
  Security Ingress Non-IPv4 Access Control Entries*:  5120 (current) - 5120 (proposed)
  Security Egress IPv4 Access Control Entries*:      7168 (current) - 7168 (proposed)
  Security Egress Non-IPv4 Access Control Entries*:   8192 (current) - 8192 (proposed)
  QoS Ingress IPv4 Access Control Entries*:          5632 (current) - 5632 (proposed)
  QoS Ingress Non-IPv4 Access Control Entries*:      2560 (current) - 2560 (proposed)
  QoS Egress IPv4 Access Control Entries*:           6144 (current) - 6144 (proposed)
  QoS Egress Non-IPv4 Access Control Entries*:       2048 (current) - 2048 (proposed)
  Netflow Input Access Control Entries*:             1024 (current) - 1024 (proposed)
  Netflow Output Access Control Entries*:            1024 (current) - 1024 (proposed)
  Flow SPAN Input Access Control Entries*:           512 (current) - 512 (proposed)
  Flow SPAN Output Access Control Entries*:          512 (current) - 512 (proposed)
  Number of VLANs:                                  4094
  Unicast MAC addresses:                             81920
  Overflow Unicast MAC addresses:                     768

```

```

Overflow L2 Multicast entries:                2304
L3 Multicast entries:                        16384
Overflow L3 Multicast entries:               768
Ipv4/Ipv6 shared unicast routes:            114688
Overflow shared unicast routes:              1536
Policy Based Routing ACEs / NAT ACEs:        3072
Tunnels:                                     2816
LISP Instance Mapping Entries:               1024
Control Plane Entries:                       1024
Input Netflow flows:                         49152
Output Netflow flows:                        49152
SGT/DGT (or) MPLS VPN entries:               32768
SGT/DGT (or) MPLS VPN Overflow entries:      768
Wired clients:                               2048
MACSec SPD Entries:                          256
MPLS L3 VPN VRF:                             1024
MPLS Labels:                                 45056
MPLS L3 VPN Routes VRF Mode:                 112640
MPLS L3 VPN Routes Prefix Mode:              32768
MVPN MDT Tunnels:                            1024
L2 VPN EOMPLS Attachment Circuit:            1024
MAX VPLS Bridge Domains :                    1000
MAX VPLS Peers Per Bridge Domain:            128
MAX VPLS/VPWS Pseudowires :                  16384
Ipv4/Ipv6 Direct and Indirect unicast routes share same space
* values can be modified by sdm cli

```

Examples: Configuring SDM Templates

```

Device(config)# sdm prefer distribution
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.	<i>Command Reference (Catalyst 9500 Series Switches)</i>

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. Support for this feature was introduced only on the C9500-12Q, C9500-16X, C9500-24Q, C9500-40X models of the Cisco Catalyst 9500 Series Switches.
Cisco IOS XE Fuji 16.8.1a	SDM Template	Support for this feature was introduced only on the C9500-32C, C9500-32QC, C9500-48Y4C, and C9500-24Y4C models of the Cisco Catalyst 9500 Series Switches.

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>.

