



SDM テンプレートの設定

- [Switch Device Manager テンプレートの制約事項 \(1 ページ\)](#)
- [SDM テンプレートに関する情報 \(2 ページ\)](#)
- [SDM テンプレートの設定方法 \(7 ページ\)](#)
- [SDM テンプレートのモニターリングおよびメンテナンス \(15 ページ\)](#)
- [SDM テンプレートの設定例 \(16 ページ\)](#)
- [SDM テンプレートに関する追加情報 \(25 ページ\)](#)
- [SDM テンプレートの機能履歴 \(25 ページ\)](#)

Switch Device Manager テンプレートの制約事項

- デバイスが NAT テンプレートで動作している場合、Switch Device Manager (SDM) テンプレートはカスタマイズできません。
- カスタマイズ可能な SDM テンプレートで、レイヤ 2 およびレイヤ 3 のマルチキャストエントリの合計制限は 48K (K = 1024 エントリ) です。
- SDM テンプレートをカスタマイズする場合は、各機能にプライオリティ値を割り当てる必要があります。プライオリティ値は、カスタマイズ可能な SDM テンプレートで指定されたすべてのリソースの総数が、カスタマイズ可能な SDM テンプレートに割り当てられたシステムリソースの総数を超える場合に、機能のリソース割り当てを決定します。
- 各機能のプライオリティ値は一意である必要があります。異なる機能に同じプライオリティ値を割り当てることはできません。
- RMA またはスーパーバイザの交換の場合、バックアップ設定を復元しても、カスタマイズされたテンプレートは復元されません。カスタマイズされたテンプレートは再設定する必要があります。
- 4K VLAN 機能は、4K VLAN のカスタマイズ可能な SDM テンプレートを介してのみイネーブルにできます。
- 4K VLAN のカスタマイズ可能な SDM テンプレートは、4K VLAN 機能のみをサポートします。カスタム VLAN テンプレートの他の FIB または ACL 関連機能はカスタマイズできません。

- 4K VLAN のカスタマイズ可能な SDM テンプレートでは、VLAN の規模を 1K から 4K に増やすことしかできません。1K ~ 4K のカスタム VLAN 値は設定できません。1K VLAN テーブルの制限事項によって制限されるその他の機能の規模は変わりません。

SDM テンプレートに関する情報

SDM テンプレートを使用してシステム リソースを設定すると、特定の機能に対するサポートをネットワーク内でのデバイスの使用方法に応じて最適化することができます。一部の機能に最大システム使用率を提供するように標準テンプレートを選択できます。

Cisco Catalyst 9600 シリーズ スイッチは、次の標準テンプレートをサポートしています。

- コア
- NAT
- 配信

SDM テンプレートに変更を加えたらすぐにシステムをリロードすることを推奨します。テンプレートを変更し、システムを再起動した後、**show sdm prefer** 特権 EXEC コマンドを使用して、新しいテンプレート設定を確認できます。**reload** 特権 EXEC コマンドを入力する前に、**show sdm prefer** コマンドを入力すると、**show sdm prefer** コマンドにより、現在使用しているテンプレートおよびリロード後にアクティブになるテンプレートが表示されます。



(注) デフォルトの標準 SDM テンプレートは、コアテンプレートです。



(注) NAT テンプレートは、カスタマイズ可能な SDM テンプレートの作成には使用できません。

カスタマイズ可能な SDM テンプレート

カスタマイズ可能な SDM テンプレートの概要

Switch Device Manager (SDM) テンプレートを使用すると、システムリソースを設定して、特定の機能のサポートを最適化できます。ただし、標準 SDM テンプレートは、デバイスがネットワークでどのように展開されているかに基づいて定義されます。

カスタム SDM テンプレートでは、ネットワーク内でのデバイスの場所ではなく、要件に基づいてテンプレートの機能を設定できます。Cisco IOS XE Amsterdam 17.3.1 リリース以降では、**sdm prefer custom fib** コマンドを使用して転送情報ベース (FIB) のカスタム SDM テンプレートを設定できます。

Cisco IOS XE Bengaluru 17.4.1 リリース以降では、**sdm prefer custom acl** コマンドを使用して、アクセスコントロールリスト (ACL) 機能のカスタム SDM テンプレートを設定できます。

Cisco IOS XE Bengaluru 17.5.1 リリース以降では、**sdm prefer custom vlan** コマンドを使用して 4k VLAN 用のカスタム SDM テンプレートを設定できます。

カスタマイズ可能な SDM テンプレートは、次の FIB 機能をサポートしています。

- ユニキャスト MAC アドレス
- レイヤ 3 ユニキャストルーティング
- レイヤ 2 マルチキャスト転送
- レイヤ 3 マルチキャスト転送
- 入力 NetFlow
- 出力 NetFlow
- SGT/DGT インデックス/MPLS VPN ラベル

カスタマイズ可能な SDM テンプレートは、次の ACL 機能をサポートしています。

- イングレス アクセス コントロール リスト (ACL)
- Egress ACL
- 入力 Quality of Service (QoS)
- 出力 QoS
- Netflow ACL
- ポリシーベースルーティング (PBR) /ネットワークアドレス変換 (NAT)
- Locator/ID Separation Protocol (LISP)
- トンネル

4K VLAN のカスタマイズ可能な SDM テンプレートは、4K VLAN 機能のみをサポートします。VLAN の規模を 1k から 4k に増やすことができます。

4k VLAN 用のカスタマイズ可能な SDM テンプレートでは、サポートされるスイッチ仮想インターフェイス (SVI) の数が 4000 に増加します。

次の表に、各 FIB 機能に設定できる最小および最大スケール値、ステップ単位、および機能にカスタム値が選択されていない場合に適用されるデフォルト値を示します。

表 1: FIB 機能のスケール値とデフォルト値

機能名	スケール値 (最小～最大)	ステップ単位	デフォルト値
MAC アドレス	32768 ~ 131072	16384	32768

機能名	スケール値（最小～最大）	ステップ単位	デフォルト値
ユニキャスト ルート	65536 ～ 262144	16384	65536
レイヤ2 マルチキャスト	0、16384 ～ 32768	16384	16384
レイヤ3 マルチキャスト	0、16384 ～ 32768	16384	16384
SG ハッシュ/MPLS	0、32768 ～ 65536	32768	32768
入力 NetFlow	0、32768 ～ 65536	32768	32768
出力 NetFlow	0、32768 ～ 65536	32768	0

次の表に、各 ACL 機能に設定できる最小および最大スケール値、ステップ単位、および機能にカスタム値が選択されていない場合に適用されるデフォルト値を示します。

表 2: ACL 機能のスケール値とデフォルト値

機能名	スケール値（最小～最大）	ステップ単位	デフォルト値
Ingress ACL	4096 ～ 26624、27648	2048	4096
Egress ACL	4096 ～ 26624、27648	2048	4096
入力 QoS	1024、2048 ～ 16384	2048	1024
出力 QoS	1024、2048 ～ 16384	2048	1024
Netflow ACL	1024 ～ 2048	1024	1024
PBR/NAT	1024、2048 ～ 16384	2048	1024
LISP	1024 ～ 2048	1024	1024
トンネル	1024 ～ 3072	1024	1024

priority キーワードを使用して優先順位を割り当てることで、最初にどの機能にリソースを割り当てるかを決定できます。機能に割り当てられた優先順位の値が小さいほど、リソース割り当ての優先順位が高くなります。すべての機能に割り当てられる合計値は、サポートされる最大リソース値（FIB 機能の場合は 416K、ACL 機能の場合は 52 K。K は 1024 エントリに相当）を超える場合があります。リソース割り当てアルゴリズムは、優先順位の値を使用して、各機能に割り当てられるリソースの数を決定します。

カスタマイズしたテンプレートを設定したら、テンプレートを有効にするためにデバイスをリロードする必要があります。



- (注) スケール値をゼロに設定できる機能では、スケール値をゼロとして指定する必要があります。そうでない場合、デフォルト値がスケール値として割り当てられます。

カスタマイズ可能な SDM テンプレートのシステムリソース割り当て

カスタマイズ可能な SDM テンプレートに割り当てられたシステムリソースの総数は、FIB 機能に対して 416K、ACL 機能に対して 52K です。指定されたすべてのリソースの合計数が、FIB 機能の場合 416K、ACL の場合 52K を超えると、システムは最も大きい数が割り当てられた機能からリソースの割り当て数を減らし始めます。機能に割り当てられた優先順位値または数が高いほど、優先順位は低くなります。

カスタマイズ可能な SDM テンプレートに割り当てられたリソースの総数が、FIB 機能では 416K 未満、ACL 機能では 52K の場合：

- テンプレートで指定されたすべての機能には、テンプレートでカスタマイズされたリソースが割り当てられます。テンプレートで指定されていない機能には、デフォルトのリソース数が割り当てられます。
- FIB 機能のマルチキャストレイヤ 2 およびレイヤ 3 に割り当てられたリソースの合計数が 48K を超えると、割り当てられたリソースの合計数が 48K になるまで、優先順位の低いマルチキャスト機能のスケールが縮小されます。
- 割り当てられていないリソースは配分されません。

カスタマイズ可能な SDM テンプレートに割り当てられたリソースの総数が、FIB 機能では 416K を超える、ACL 機能では 52K を超える場合：

- カスタムスケールが指定されていないすべての機能には、デフォルト値が割り当てられます。
- FIB 機能のマルチキャストレイヤ 2 およびレイヤ 3 に割り当てられたリソースの合計数が 48K を超えると、割り当てられたリソースの合計数が 48K 以下になるまで、優先順位の低いマルチキャスト機能のスケールが縮小されます。
- 優先順位の値が最も高い機能に割り当てられたリソースの数は、ステップ値だけ減少します。
- リソースの総数がまだ、FIB 機能では 416K、ACL 機能では 52K を超えている場合は、優先順位の値が最も高い次の機能に割り当てられたリソースが、ステップ値だけ減少します。
- 機能に割り当てられたリソースを下げる時、スケールはその機能のデフォルト値までしか下げられません。さらに調整が必要な場合は、優先順位のリストで次の機能に割り当てられたリソースが削減されます。



(注) 機能に対して入力したカスタム値は、次のステップ値に切り上げられます。たとえば、SGTに40Kの値を入力すると、64Kに切り上げられます。

カスタマイズ可能な SDM テンプレートと高可用性

高可用性をサポートするデバイスでは、アクティブスーパーバイザでカスタマイズ可能な SDM テンプレートが設定されると、スタンバイスーパーバイザでも有効になります。

スタンバイスーパーバイザがアクティブスーパーバイザとは異なるカスタムテンプレートで設定されている場合、アクティブスーパーバイザのカスタマイズ可能な SDM テンプレートは初期化中にスタンバイスーパーバイザで設定されます。

カスタマイズ可能な SDM テンプレートと StackWise Virtual

StackWise Virtual をサポートするデバイスでは、アクティブスーパーバイザで SDM テンプレートが設定されると、スタンバイシャーシでも有効になります。

スタンバイシャーシがアクティブスーパーバイザとは異なるカスタムテンプレートで設定されている場合、アクティブスーパーバイザの SDM テンプレートは初期化中にスタンバイシャーシで設定されます。スタンバイシャーシは、テンプレートを有効にするために追加のリロードを実行します。

カスタマイズ可能な SDM テンプレートと ISSU

デバイスが In-Service Software Upgrade (ISSU) によって上位リリースにアップグレードされ、リソース割り当てアルゴリズムが変更された場合、このアップグレードによって同じユーザー入力に対して異なるスケールになる可能性があります。スケールの変更が検出され、syslog メッセージで通知されます。システムは以前のスケールで動作し続けます。

スケールの変更を表示するには、**show sdm prefer custom scale-change** コマンドを使用します。このスケール変更は、**sdm prefer custom commit** コマンドを使用して適用できます。変更を有効にするには、デバイスのリロードが必要です。

FIB 機能用のカスタマイズ可能な SDM テンプレートを持つデバイスを Cisco IOS XE Amsterdam 17.3.1 リリースよりも前のリリースにダウングレードする場合は、ダウングレードの前に SDM テンプレートを静的な SDM テンプレートに変更する必要があります。テンプレートを変更するには、**sdm prefer template name** コマンドを使用します。ダウングレードに進む前に、変更を有効にするためにシステムをリロードします。

ACL 機能用のカスタマイズ可能な SDM テンプレートを持つデバイスを Cisco IOS XE Bengaluru 17.4.1 リリースよりも前のリリースにダウングレードする場合は、ダウングレードの前に SDM テンプレートを静的な SDM テンプレートに変更する必要があります。

デバイスに Cisco IOS XE Bengaluru 17.4.1 リリースでカスタマイズされた FIB 機能と ACL 機能の両方のカスタマイズ可能な SDM テンプレートがあり、Cisco IOS XE Amsterdam 17.3.1 リリースにダウングレードすると、デバイスは FIB 機能用のカスタマイズで復元されます。ACL 機能のスケール番号は、標準 SDM テンプレートのスケール値に基づいて割り当てられます。ACL

機能のカスタマイズに関する情報は保持されます。Cisco IOS XE Bengaluru 17.4.1 リリースにアップグレードすると、ACL 機能のカスタマイズを使用してデバイスが復元されます。

SDM テンプレートの設定方法

SDM テンプレートの設定

SDM テンプレートを使用して機能動作を最適にサポートするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 3	sdm prefer { core nat distribution custom } 例： Device(config)# sdm prefer distribution	スイッチで使用する SDM テンプレートを指定します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • core : コアテンプレートを設定します。 • nat : スイッチでの NAT コンフィギュレーションを最大化します。 • distribution : ディストリビューションテンプレートを設定します。 • custom : FIB、ACL 機能、または VLAN のカスタムテンプレートを設定します。カスタムテンプレートを使用すると、特定の FIB 機能、ACL 機能、または VLAN 機能の値を設定できます。

	コマンドまたはアクション	目的
		(注) no sdm prefer コマンドとデフォルトテンプレートはサポートされません。
ステップ 4	end 例： Device(config)# end	特権 EXEC モードに戻ります。
ステップ 5	reload 例： Device# reload	オペレーティング システムをリロードします。 システムの再起動後、 show sdm prefer 特権 EXEC コマンドを使用して、新しいテンプレート設定を確認できます。 reload 特権 EXEC コマンドを入力する前に、 show sdm prefer コマンドを入力すると、 show sdm prefer コマンドにより、現在使用しているテンプレートおよびリロード後にアクティブになるテンプレートが表示されます。

FIB 機能用のカスタマイズ可能な SDM テンプレートの設定

FIB 機能用のカスタマイズ可能な SDM テンプレートを作成するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	sdm prefer custom fib 例：	FIB 機能用のカスタマイズ可能な SDM テンプレートを作成します。機能をカ

	コマンドまたはアクション	目的
	Device (config) #sdm prefer custom fib	スタマイズする場合は、サブモードを開始します。
ステップ 4	mac-address number-of-entries priority priority-value 例： Device (config-sdm-fib) #mac-address 128 priority 1	MAC アドレスに割り当てるエントリの数を指定します。値の範囲は 32K ~ 128K です。値は次の 16K 単位に切り上げられます。優先順位の値の範囲は 1 ~ 7 です。
ステップ 5	ipv4_and_ipv6 unicast number-of-entries priority priority-value 例： Device (config-sdm-fib) #ipv4_and_ipv6 unicast 256 priority 2	IPv4 および IPv6 ユニキャストに割り当てるエントリの数を指定します。値の範囲は 64K ~ 256K です。優先順位の値の範囲は 1 ~ 7 です。
ステップ 6	ipv4_and_ipv6 multicast l3 number-of-entries priority priority-value 例： Device (config-sdm-fib) #ipv4_and_ipv6 multicast l3 32 priority 3	レイヤ 3 IPv4 および IPv6 マルチキャストに割り当てるエントリの数を指定します。値の範囲は 16 ~ 32 で、0 (ゼロ) も値として入力できます。優先順位の値の範囲は 1 ~ 7 です。
ステップ 7	ipv4_and_ipv6 multicast l2 number-of-entries priority priority-value 例： Device (config-sdm-fib) #ipv4_and_ipv6 multicast l2 32 priority 4	レイヤ 2 IPv4 および IPv6 マルチキャストに割り当てるエントリの数を指定します。値の範囲は 16 ~ 32 で、0 (ゼロ) も値として入力できます。優先順位の値の範囲は 1 ~ 7 です。
ステップ 8	netflow_out number-of-entries priority priority-value 例： Device (config-sdm-fib) #netflow_out 64 priority 5	NetFlow 出力に割り当てるエントリの数を指定します。値の範囲は 32K ~ 64K です。値としてゼロを入力することもできます。優先順位の値の範囲は 1 ~ 7 です。
ステップ 9	netflow-in number-of-entries priority priority-value 例： Device (config-sdm-fib) # netflow_in 64 priority 6	NetFlow 入力に割り当てるエントリの数を指定します。値の範囲は 32K ~ 64K です。値としてゼロを入力することもできます。優先順位の値の範囲は 1 ~ 7 です。
ステップ 10	sgt_or_mpls_vpn number-of-entries priority priority-value 例： Device (config-sdm-fib) # sgt_or_mpls_vpn 64 priority 7	SGT または MPLS VPN に割り当てるエントリの数を指定します。値の範囲は 32K ~ 64K です。値としてゼロを入力することもできます。優先順位の値の範囲は 1 ~ 7 です。

	コマンドまたはアクション	目的
ステップ 11	end 例： Device(config-sdm-fib)# end	特権 EXEC モードに戻ります。
ステップ 12	show sdm prefer custom 例： Device# show sdm prefer custom	カスタマイズ可能な SDM テンプレートの機能に適用されるカスタム値を表示します。
ステップ 13	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 14	sdm prefer custom commit 例： Device(config)# sdm prefer custom commit	実行中の SDM 設定を、カスタマイズされたテンプレートの値に変更します。新しいテンプレートは、次のリロード時に有効になります。
ステップ 15	end 例： Device(config)# end	特権 EXEC モードに戻ります。
ステップ 16	reload 例： Device# reload	デバイスをリロードし、カスタマイズされた SDM テンプレートを適用します。

次のタスク

show sdm prefer custom コマンドを使用して、カスタマイズ可能な SDM テンプレートの機能に適用されるカスタム値を表示したら、必要に応じて値を変更できます。カスタマイズされた SDM テンプレートの機能に割り当てたすべてのカスタム値をクリアするには、**sdm prefer custom fib clear** コマンドを使用します。

優先順位の値を変更せずに機能に割り当てられたカスタム値を変更する場合は、機能に割り当てられたカスタム値を上書きできます。たとえば、**mac-address 128 priority 1** を割り当てた場合、これを **mac-address 32 priority 1** に上書きできます。機能に割り当てられた優先順位の値を変更する場合、およびその優先順位の値がすでに別の機能に割り当てられている場合は、その機能のコマンドの **no** 形式を使用して、他の機能に割り当てられているカ

スタム値をクリアする必要があります。その後、優先順位の値を最初の機能に割り当てることができます。デフォルト以外の値にするには、他の機能を再設定する必要があります。

現在のカスタマイズコンテキストは、**sdm prefer custom commit** コマンドが発行されるまでのみ有効です。コミット CLI の発行後に値を変更する場合は、新しいカスタマイズコンテキストと見なされます。必要なすべての機能値を再入力する必要があります。

ACL 機能用のカスタマイズ可能な SDM テンプレートの設定

ACL 機能用のカスタマイズ可能な SDM テンプレートを作成するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	sdm prefer custom acl 例： Device(config)# sdm prefer custom acl	ACL 機能用のカスタマイズ可能な SDM テンプレートを作成します。機能をカスタマイズする場合は、サブモードを開始します。
ステップ 4	acl-ingress number-of-entries priority <i>priority-value</i> 例： Device(config-sdm-acl)# acl-ingress 26 priority 1	入力 ACL に割り当てるエントリの数を指定します。値の範囲は 4K ~ 27K です。値は次の 2K 単位に切り上げられます。優先順位の値の範囲は 1 ~ 8 です。
ステップ 5	acl-egress number-of-entries priority <i>priority-value</i> 例： Device(config-sdm-acl)# acl-egress 20 priority 2	出力 ACL に割り当てるエントリの数を指定します。値の範囲は 4K ~ 27K です。値は次の 2K 単位に切り上げられます。優先順位の値の範囲は 1 ~ 8 です。
ステップ 6	qos-ingress number-of-entries priority <i>priority-value</i> 例：	入力 QoS に割り当てるエントリの数を指定します。値の範囲は 2K ~ 16K です。値は次の 2K 単位に切り上げられ

	コマンドまたはアクション	目的
	<code>Device(config-sdm-acl)#qos-ingress 2 priority 3</code>	ます。優先順位の値の範囲は 1 ~ 8 です。
ステップ 7	qos-egress number-of-entries priority priority-value 例： <code>Device(config-sdm-acl)#qos-egress 2 priority 4</code>	出力 QoS に割り当てるエントリの数を指定します。値の範囲は 2K ~ 16K です。値は次の 2K 単位に切り上げられます。優先順位の値の範囲は 1 ~ 8 です。
ステップ 8	nfl number-of-entries priority priority-value 例： <code>Device(config-sdm-acl)#nfl 2 priority 5</code>	NetFlow ACL に割り当てるエントリの数を指定します。値の範囲は 1K ~ 2K です。優先順位の値の範囲は 1 ~ 8 です。NetFlow ACL に割り当てられたエントリは、入力エントリと出力エントリに均等に分割されます。
ステップ 9	pbr number-of-entries priority priority-value 例： <code>Device(config-sdm-acl)#pbr 2 priority 6</code>	PBR/NAT に割り当てるエントリの数を指定します。値の範囲は 2K ~ 16K です。値は次の 2K 単位に切り上げられます。優先順位の値の範囲は 1 ~ 8 です。
ステップ 10	lisp number-of-entries priority priority-value 例： <code>Device(config-sdm-acl)#lisp 2 priority 7</code>	LISP に割り当てるエントリの数を指定します。値の範囲は 1K ~ 2K です。優先順位の値の範囲は 1 ~ 8 です。
ステップ 11	tunnels number-of-entries priority priority-value 例： <code>Device(config-sdm-acl)#tunnels 1 priority 8</code>	トンネル終端エントリに割り当てるエントリの数を指定します。値の範囲は 1K ~ 3K です。指定された値から 256 エントリ減少します。1K、2K、3K のトンネルスケールは、それぞれ 0.75K、1.75K、2.75K にマッピングされます。優先順位の値の範囲は 1 ~ 8 です。
ステップ 12	end 例： <code>Device(config-sdm-acl)# end</code>	特権 EXEC モードに戻ります。
ステップ 13	show sdm prefer custom 例： <code>Device# show sdm prefer custom</code>	カスタマイズ可能な SDM テンプレートの機能に適用されるカスタム値を表示します。

	コマンドまたはアクション	目的
ステップ 14	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 15	sdm prefer custom commit 例： Device (config)# sdm prefer custom commit	実行中の SDM 設定を、カスタマイズされたテンプレートの値に変更します。新しいテンプレートは、次のリロード時に有効になります。
ステップ 16	end 例： Device (config)# end	特権 EXEC モードに戻ります。
ステップ 17	reload 例： Device# reload	デバイスをリロードし、カスタマイズされた SDM テンプレートを適用します。

次のタスク

show sdm prefer custom コマンドを使用して、カスタマイズ可能な SDM テンプレートの機能に適用されるカスタム値を表示したら、必要に応じて値を変更できます。カスタマイズされた SDM テンプレートの機能に割り当てたすべてのカスタム値をクリアするには、**sdm prefer custom acl clear** コマンドを使用します。

優先順位の値を変更せずに機能に割り当てられたカスタム値を変更する場合は、機能に割り当てられたカスタム値を上書きできます。たとえば、**acl-ingress 26 priority 1** を割り当てた場合、これを **acl-ingress 24 priority 1** に上書きできます。機能に割り当てられた優先順位の値を変更する場合、およびその優先順位の値がすでに別の機能に割り当てられている場合は、その機能のコマンドの **no** 形式を使用して、他の機能に割り当てられているカスタム値をクリアする必要があります。その後、優先順位の値を最初の機能に割り当てることができます。デフォルト以外の値にするには、他の機能を再設定する必要があります。

現在のカスタマイズコンテキストは、**sdm prefer custom commit** コマンドが発行されるまでのみ有効です。コミット CLI の発行後に値を変更する場合は、新しいカスタマイズコンテキストと見なされます。必要なすべての機能値を再入力する必要があります。

4k VLAN 用のカスタマイズ可能な SDM テンプレートの設定

4k VLAN 用のカスタマイズ可能な SDM テンプレートを作成するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	sdm prefer custom vlan 例： Device(config)# sdm prefer custom vlan	4k VLAN 用のカスタマイズ可能な SDM テンプレートを作成します。
ステップ 4	end 例： Device(config-sdm-vlan)# end	特権 EXEC モードに戻ります。
ステップ 5	show sdm prefer custom 例： Device# show sdm prefer custom	カスタマイズ可能な SDM テンプレートの機能に適用されるカスタム値を表示します。
ステップ 6	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 7	sdm prefer custom commit 例： Device(config)# sdm prefer custom commit	実行中の SDM 設定を、カスタマイズされたテンプレートの値に変更します。新しいテンプレートは、次のリロード時に有効になります。
ステップ 8	end 例： Device(config)# end	特権 EXEC モードに戻ります。
ステップ 9	reload 例： Device# reload	デバイスをリロードし、カスタマイズされた SDM テンプレートを適用します。

SDM テンプレートのカスタマイズ値のクリア

カスタマイズされた SDM テンプレートの機能に割り当てたカスタム値をクリアするには、**sdm prefer custom fib clear** コマンドまたは **sdm prefer custom acl clear** コマンドを使用します。

このコマンドは、まだコミットされていないカスタマイズ設定をクリアします。

このコマンドを発行したら、機能のすべてのカスタム値を再設定する必要があります。

SDM テンプレートのモニターリングおよびメンテナンス

SDM テンプレートの確認

SDM テンプレートをモニターおよびメンテナンスするには、次のコマンドを使用します。

コマンド	目的
show sdm prefer	使用中の SDM テンプレートを表示します。



(注) SDM テンプレートには、テンプレートの一部として定義されているコマンドのみが含まれています。テンプレートで定義されていない別の関連コマンドがテンプレートで有効になっている場合、**show running config** コマンドを入力すると、該当するコマンドが表示されます。たとえば、SDM テンプレートで **switchport voice vlan** コマンドが有効になっている場合、(SDM テンプレートでは定義されていませんが) **spanning-tree portfast edge** コマンドも有効にすることができます。

SDM テンプレートを削除すると、そのような他の関連するコマンドも削除されるため、明示的に再設定しなければならなくなります。

カスタマイズ可能な SDM テンプレートの確認

適用されるカスタマイズ可能な SDM テンプレートを確認するには、次のコマンドを使用します。

表 3: カスタマイズ可能な SDM テンプレートを確認するコマンド

コマンド	説明
show sdm prefer custom	カスタマイズ可能な SDM テンプレートの機能に適用されるカスタム値を表示します。
show sdm prefer custom user-input	カスタマイズ可能な SDM テンプレートでユーザーが入力した値を表示します。
show sdm prefer	現在アクティブなカスタマイズされた SDM テンプレートを表示します。

カスタマイズ可能な SDM テンプレートのいずれかの機能にゼロのスケール値が割り当てられた場合、デバイスがリロードされた後、その機能は **show sdm prefer custom** コマンドの出力に表示されません。

SDM テンプレートの設定例

例 : SDM テンプレートの表示

次に、コアテンプレート情報を表示する出力例を示します。

```
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*:          4096 (current) - 4096 (proposed)
QoS Ingress Non-IPv4 Access Control Entries*:      4096 (current) - 4096 (proposed)
QoS Egress IPv4 Access Control Entries*:           4096 (current) - 4096 (proposed)
QoS Egress Non-IPv4 Access Control Entries*:       4096 (current) - 4096 (proposed)
Netflow Input Access Control Entries*:              512 (current) - 512 (proposed)
Netflow Output Access Control Entries*:             512 (current) - 512 (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:                     2048
Control Plane Entries:                             512
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

```

次に、NAT テンプレート情報を表示する出力例を示します。

```

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

```

次に、ディストリビューションテンプレート情報を表示する出力例を示します。

```

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

```

例 : SDM テンプレートの設定

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

例：カスタマイズされた SDM テンプレートの設定

次の出力例は、FIB 機能用のカスタマイズされた SDM テンプレートを設定する方法を示しています。この例では、SG ハッシュ/MPLS 機能と入力 NetFlow 機能にはカスタマイズされたテンプレートのリソースが割り当てられていないため、デフォルト値に従ってリソースが割り当てられます。

```
Device(config)# sdm prefer custom fib
Device(config-sdm-fib)# mac-address 128 priority 1
Device(config-sdm-fib)# ipv4_and_ipv6 unicast 256 priority 2
Device(config-sdm-fib)# ipv4_and_ipv6 multicast 13 32 priority 3
Device(config-sdm-fib)# ipv4_and_ipv6 multicast 12 32 priority 4
Device(config-sdm-fib)# netflow_out 64 priority 5
Device(config-sdm-fib)# end
```

次の例では、SGT/MPLS VPN 機能にゼロリソースが割り当てられているため、これらの機能にリソースは割り当てられません。

```
Device(config)# sdm prefer custom fib
Device(config-sdm-fib)# ipv4_and_ipv6 unicast 164 priority 1
Device(config-sdm-fib)# mac-address 80 priority 2
Device(config-sdm-fib)# ipv4_and_ipv6 multicast 12 16 priority 4
Device(config-sdm-fib)# ipv4_and_ipv6 multicast 13 16 priority 3
Device(config-sdm-fib)# sgt_or_mpls_vpn 0
Device(config-sdm-fib)# netflow_in 32 priority 5
Device(config-sdm-fib)# netflow_out 32 priority 6
Device(config-sdm-fib)# end
```

次の出力例は、ACL 機能用のカスタマイズされた SDM テンプレートを設定する方法を示しています。この例では、トンネル機能にはカスタマイズされたテンプレートのリソースが割り当てられていないため、デフォルト値に従ってリソースが割り当てられます。

```
Device(config)# sdm prefer custom acl
Device(config-sdm-acl)# acl-ingress 26 priority 1
Device(config-sdm-acl)# acl-engress 20 priority 2
Device(config-sdm-acl)# lisp 2 priority 3
Device(config-sdm-acl)# nfl 2 priority 4
Device(config-sdm-acl)# pbr 2 priority 5
Device(config-sdm-acl)# qos-ingress 2 priority 6
Device(config-sdm-acl)# qos-egress 2 priority 7
Device(config-sdm-acl)# end
```

次の出力例は、4k VLAN 用にカスタマイズされた SDM テンプレートを設定する方法を示しています。

```
Device(config)# sdm prefer custom VLAN
Device(config-sdm-vlan)# end
```

例：カスタマイズされた SDM テンプレートの表示

次の出力例は、FIB および ACL 機能のカスタマイズされた SDM テンプレートの推奨値を示しています。

```
Device# show sdm prefer custom
Showing SDM Template Info

This is the Custom template
<SNIP>
Number of VLANs:                               4094
Unicast MAC addresses*:                         32768 (current) - 131072 (proposed)

Overflow Unicast MAC addresses*:                 768 (current) - 1536 (proposed)

L2 Multicast entries*:                          0 (current) - 16384 (proposed)

Overflow L2 Multicast entries*:                 2304 (current) - 768 (proposed)

L3 Multicast entries*:                          32768 (current) - 16384 (proposed)

Overflow L3 Multicast entries*:                 768 (current) - 768 (proposed)

Ipv4/Ipv6 shared unicast routes*:              212992 (current) - 180224 (proposed)

Overflow shared unicast routes*:                1536 (current) - 2304 (proposed)

Ingress Security Access Control Entries*:       24576 (current) - 26624 (proposed)

Egress Security Access Control Entries*:        3072 (current) - 20480 (proposed)

Ingress QoS Access Control Entries*:            8192 (current) - 1024 (proposed)

Egress QoS Access Control Entries*:            8192 (current) - 1024 (proposed)

Policy Based Routing ACEs / NAT ACEs*:         3072 (current) - 1024 (proposed)

Netflow Input ACEs*:                           256 (current) - 512 (proposed)

Netflow Output ACEs*:                          768 (current) - 512 (proposed)

Flow SPAN ACEs*:                              256 (current) - 512 (proposed)

Output Flow SPAN ACEs*:                       256 (current) - 512 (proposed)

Tunnels*:                                     2816 (current) - 768 (proposed)

LISP Instance Mapping Entries*:                 2048 (current) - 1024 (proposed)

Control Plane Entries*:                        512 (current) - 512 (proposed)

Input Netflow flows*:                          32768 (current) - 32768 (proposed)

Output Netflow flows*:                        32768 (current) - 0 (proposed)

SGT/DGT (or) MPLS VPN entries*:                32768 (current) - 32768 (proposed)

SGT/DGT (or) MPLS VPN Overflow entries*:       768 (current) - 768 (proposed)

Wired clients:                                2048
MACSec SPD Entries*:                          256 (current) - 256 (proposed)
```

```

VRF: 1024
MPLS Labels: 45056
MPLS L3 VPN Routes VRF Mode*: 209920 (current) - 180224 (proposed)

MPLS L3 VPN Routes Prefix Mode*: 32768 (current) - 32768 (proposed)

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 proposed values will take effect post reload.

次の出力例は、カスタムテンプレートでユーザーが指定した値と優先順位を示しています。SG
 ハッシュ/MPLS機能、入力NetFlow機能、およびトンネル機能にはカスタマイズされたテンプレートのリソースが割り当てられていないため、デフォルト値に従ってリソースが割り当てられます。

```
Device# show sdm prefer custom user-input
```

```
FIB FEATURE USER INPUT
```

```
User Input values
```

```
=====
```

FEATURE NAME	PRIORITY	SCALE
Unicast MAC addresses:	1	128*1024
L2 Multicast entries:	4	32*1024
L3 Multicast entries:	3	32*1024
Ipv4/Ipv6 shared unicast routes:	2	256*1024
Output Netflow flows:	5	64*1024

```
System Default values
```

```
=====
```

FEATURE NAME	PRIORITY	SCALE
Input Netflow flows:	NA	32768
SGT/DGT (or) MPLS VPN entries:	NA	32768

```
ACL FEATURE USER INPUT
```

```
User Input values
```

```
=====
```

FEATURE NAME	PRIORITY	SCALE
Security Access Control Entries:	1	26*1024
Egress Security Access Control Entries:	2	20*1024
QoS Access Control Entries:	3	2*1024
Egress QoS Access Control Entries:	4	2*1024
Policy Based Routing ACEs / NAT ACEs:	5	2*1024
Netflow ACEs:	6	2*1024
LISP Instance Mapping Entries:	7	2*1024

```
System Default values
```

```
=====
```

FEATURE NAME	PRIORITY	SCALE
--------------	----------	-------

例: カスタマイズされた SDM テンプレートの表示

```
-----
Tunnels:                                     NA          1024
```

次の出力例は、カスタマイズされた SDM テンプレートの推奨値を示しています。SGT/MPLS VPN機能にゼロリソースが割り当てられているため、これらの機能にリソースは割り当てられません。

```
Device#show sdm prefer custom
Showing SDM Template Info
```

```
This is the Custom template
<SNIP>
```

```
Unicast MAC addresses*:                    32768 (current) - 81920 (proposed)

Overflow Unicast MAC addresses*:           768 (current) - 1536 (proposed)

L2 Multicast entries*:                    0 (current) - 16384 (proposed)

Overflow L2 Multicast entries*:           2304 (current) - 768 (proposed)

L3 Multicast entries*:                    32768 (current) - 16384 (proposed)

Overflow L3 Multicast entries*:           768 (current) - 768 (proposed)

Ipv4/Ipv6 shared unicast routes*:        212992 (current) - 180224 (proposed)

Overflow shared unicast routes*:          1536 (current) - 2304 (proposed)

Ingress Security Access Control Entries*: 24576 (current) - 26624 (proposed)

Egress Security Access Control Entries*:  3072 (current) - 20480 (proposed)

Ingress QoS Access Control Entries*:      8192 (current) - 1024 (proposed)

Egress QoS Access Control Entries*:       8192 (current) - 1024 (proposed)

Policy Based Routing ACEs / NAT ACEs*:   3072 (current) - 1024 (proposed)

Netflow Input ACEs*:                     256 (current) - 512 (proposed)

Netflow Output ACEs*:                    768 (current) - 512 (proposed)

Flow SPAN ACEs*:                         256 (current) - 512 (proposed)

Output Flow SPAN ACEs*:                  256 (current) - 512 (proposed)

Tunnels*:                                 2816 (current) - 768 (proposed)

LISP Instance Mapping Entries*:           2048 (current) - 1024

Input Netflow flows*:                    32768 (current) - 32768 (proposed)

Output Netflow flows*:                   32768 (current) - 32768 (proposed)

SGT/DGT (or) MPLS VPN entries*:          32768 (current) - 0 (proposed)

SGT/DGT (or) MPLS VPN Overflow entries*:  768 (current) - 768 (proposed)

Wired clients:                            2048

MACSec SPD Entries*:                     256 (current) - 256 (proposed)

VRF:                                       1024

MPLS Labels:                              45056

MPLS L3 VPN Routes VRF Mode*:            209920 (current) - 180224 (proposed)
```

```

MPLS L3 VPN Routes Prefix Mode*:          32768 (current) - 32768 (proposed)

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

```

次の出力例は、カスタムテンプレートでユーザーが指定した値と優先順位を示しています。
SGT/MPLS VPN 機能に割り当てられているリソースはありません。

```

Device#show sdm prefer custom user-input
FIB FEATURE USER INPUT
User Input values
=====

```

FEATURE NAME	PRIORITY	SCALE
Unicast MAC addresses:	2	80*1024
L2 Multicast entries:	4	16*1024
L3 Multicast entries:	3	16*1024
Ipv4/Ipv6 shared unicast routes:	1	164*1024
Input Netflow flows:	5	32*1024
Output Netflow flows:	6	32*1024
SGT/DGT (or) MPLS VPN entries:	NA	0

```

ACL FEATURE USER INPUT
User Input values
=====

```

FEATURE NAME	PRIORITY	SCALE
Security Access Control Entries:	1	26*1024
Egress Security Access Control Entries:	2	20*1024
QoS Access Control Entries:	3	2*1024
Egress QoS Access Control Entries:	4	2*1024
Policy Based Routing ACEs / NAT ACEs:	5	2*1024
Netflow ACEs:	6	2*1024
LISP Instance Mapping Entries:	7	2*1024

```

System Default values
=====

```

FEATURE NAME	PRIORITY	SCALE
Tunnels:	NA	1024

次の出力例は、4k VLAN 用のカスタマイズされた SDM テンプレートの推奨値を示しています。

```

Device#show sdm prefer custom
Showing SDM Template Info

This is the Custom 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*:                   512 (current) - 512 (proposed)
Netflow Output Access Control Entries*:                  512 (current) - 512 (proposed)
Flow SPAN Input Access Control Entries*:                 512 (current) - 512 (proposed)

```

例：カスタマイズされた SDM テンプレートの適用

```

Flow SPAN Output Access Control Entries*:          512 (current) - 512 (proposed)
Number of VLANs:                                  4094
Unicast MAC addresses*:                            98304
Overflow Unicast MAC addresses*:                   768
Overflow L2 Multicast entries*:                    2048
L3 Multicast entries*:                             16384
Overflow L3 Multicast entries*:                    768
Ipv4/Ipv6 shared unicast routes*:                 81920
Overflow shared unicast routes*:                   1536
Policy Based Routing ACEs / NAT ACEs*:            3072
Tunnels*:                                          2816
LISP Instance Mapping Entries*:                    2048
Control Plane Entries*:                            512
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
VRF:                                               1024
MPLS Labels:                                       45056
MPLS L3 VPN Routes VRF Mode*:                      81920
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
VLAN Filter Entries:                               16384

```

例：カスタマイズされた SDM テンプレートの適用

次の出力例は、カスタマイズされた SDM テンプレートを適用する方法を示しています。

```

Device(config)# sdm prefer custom commit
Changes to the running SDM preferences have been stored and will take effect on the next
reload.
Device(config)# exit
Device# reload

```

例：SDM テンプレートのカスタマイズ値のクリア

次に、テンプレートを再カスタマイズできるように、FIB 機能用のカスタマイズされた SDM テンプレートをクリアする出力例を示します。

```

Device(config)# sdm prefer custom fib clear
FIB customization changes, not yet committed will be cleared
Device(config-sdm-fib)# end

```

次に、テンプレートを再カスタマイズできるように、ACL 機能用のカスタマイズされた SDM テンプレートをクリアする出力例を示します。

```

Device(config)# sdm prefer custom acl clear
ACL customization changes, not yet committed will be cleared
Device(config-sdm-fib)# end

```

SDM テンプレートに関する追加情報

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	<i>Command Reference (Catalyst 9600 Series Switches)</i>

SDM テンプレートの機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Gibraltar 16.11.1	SDM テンプレート	標準の SDM テンプレートを使用すると、システムリソースを設定して、特定の機能のサポートを最適化できます。
Cisco IOS XE Amsterdam 17.3.1	FIB 機能用のカスタマイズ可能な SDM テンプレート	FIB 機能のカスタマイズ可能な SDM テンプレートのサポートが導入されました。カスタマイズ可能な SDM テンプレートを使用すると、ユーザーの要件に応じてテンプレートの機能を設定できます。
Cisco IOS XE Bengaluru 17.4.1	ACL 機能用のカスタマイズ可能な SDM テンプレート	ACL 機能のカスタマイズ可能な SDM テンプレートのサポートが導入されました。カスタマイズ可能な SDM テンプレートを使用すると、ユーザーの要件に応じてテンプレートの機能を設定できます。
Cisco IOS XE Bengaluru 17.5.1	4k VLAN 用のカスタマイズ可能な SDM テンプレート	4k VLAN 用のカスタマイズ可能な SDM テンプレートのサポートが導入されました。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。

