C コマンド

この章では、C で始まる Cisco NX-OS Security コマンドについて説明します。

capture session

アクセス コントロール リスト（ACL）のキャプチャ セッションをイネーブルにするには、**capture session** コマンドを使用します。

capture session *session*

構文の説明

session	セッション ID。有効な範囲は 1 ～ 48 です。

デフォルト

なし

コマンド モード

ACL キャプチャコンフィギュレーション モード（config-acl-capture）

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
5.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、ACL キャプチャ セッションを設定する例を示します。

```
switch# configure terminal
switch(config)# ip access-list abc1234
switch(config-acl)# capture session 7
switch(config-acl)#
```

関連コマンド

コマンド	説明
ip access-list	アクセス リストを作成します。
monitor session *session* **type acl-capture**	ACL キャプチャ セッションを設定します。

class（ポリシー マップ）

コントロール プレーン ポリシー マップのコントロール プレーン クラス マップを指定するには、**class** コマンドを使用します。コントロール プレーン ポリシー マップからコントロール プレーン クラス マップを削除するには、このコマンドの **no** 形式を使用します。

class {*class-map-name* [**insert-before** *class-map-name2*] | **class-default**}

no class *class-map-name*

構文の説明

class-map-name	クラス マップ名です。
insert-before *class-map-name2*	（任意）コントロール プレーン ポリシー マップの別のコントロール プレーン クラス マップの前にコントロール プレーン クラス マップを挿入します。
class-default	デフォルト クラスを指定します。

デフォルト

なし

コマンド モード

ポリシー マップ コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドはデフォルトの仮想デバイス コンテキスト（VDC）内でのみ使用できます。

このコマンドには、ライセンスは必要ありません。

例

次に、コントロール プレーン ポリシー マップのクラス マップを設定する例を示します。

```
switch# configure terminal
switch(config)# policy-map type control-plane PolicyMapA
switch(config-pmap)# class ClassMapA
swtich(config-pmap-c)
```

次に、コントロール プレーン ポリシー マップからクラス マップを削除する例を示します。

```
switch# configure terminal
switch(config)# policy-map type control-plane PolicyMapA
switch(config-pmap)# no class ClassMapA
```

関連コマンド

コマンド	説明
policy-map type control-plane	コントロール プレーン ポリシー マップを指定し、ポリシー マップ コンフィギュレーション モードを開始します。
show policy-map type control-plane	コントロール プレーン ポリシー マップの設定情報を表示します。

class-map type control-plane

コントロール プレーン クラス マップを作成または指定して、クラス マップ コンフィギュレーション モードを開始するには、**class-map type control-plane** コマンドを使用します。コントロール プレーン クラス マップを削除するには、このコマンドの **no** 形式を使用します。

class-map type control-plane [**match-all** | **match-any**] *class-map-name*

no class-map type control-plane [**match-all** | **match-any**] *class-map-name*

構文の説明

match-all	（任意）クラス マップのすべての一致条件と一致するように指定します。
match-any	（任意）クラス マップの任意の一致条件と一致するように指定します。
class-map-name	クラス マップ名です。名前には英数字を使用します。大文字と小文字が区別され、最大で 64 文字の長さまで指定可能です。

デフォルト

match-any

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

コントロール プレーン クラス マップの名前として、match-all、match-any、または class-default は使用できません。

このコマンドはデフォルトの仮想デバイス コンテキスト（VDC）内でのみ使用できます。

このコマンドには、ライセンスは必要ありません。

例

次に、コントロール プレーン クラス マップを指定して、クラス マップ コンフィギュレーション モードを開始する例を示します。

```
switch# configure terminal
switch(config)# class-map type control-plane ClassMapA
switch(config-cmap)#
```

次に、コントロール プレーン クラス マップを削除する例を示します。

```
switch# configure terminal
switch(config)# no class-map type control-plane ClassMapA
```

関連コマンド

コマンド	説明
show class-map type control-plane	コントロール プレーン ポリシー マップの設定情報を表示します。

clear access-list counters

すべての IPv4 Access Control List（ACL; アクセス コントロール リスト）、IPv6 ACL、および MAC ACL、または単一の ACL のカウンタをクリアするには、**clear access-list counters** コマンドを使用します。

clear access-list counters [*access-list-name*]

構文の説明

access-list-name	（任意）デバイスがそのカウンタをクリアする ACL の名前。名前では最大 64 文字までの英数字を使用でき、大文字と小文字が区別されます。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.1(2)	IPv6 ACL カウンタのクリア操作のサポートが追加されました。
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、すべての IPv4 ACL、IPv6 ACL、および MAC ACL のカウンタをクリアする例を示します。

```
switch# clear access-list counters
switch#
```

次に、acl-ipv4-01 という名前の IPv4 ACL のカウンタをクリアする例を示します。

```
switch# clear access-list counters acl-ipv4-01
switch#
```

関連コマンド

コマンド	説明
clear ip access-list counters	IPv4 ACL のカウンタをクリアします。
clear ipv6 access-list counters	IPv6 ACL のカウンタをクリアします。

コマンド	説明
clear mac access-list counters	MAC ACL のカウンタをクリアします。
clear vlan access-list counters	VACL のカウンタをクリアします。
show access-lists	1 つまたはすべての IPv4 ACL、IPv6 ACL、および MAC ACL に関する情報を表示します。

clear accounting log

アカウンティング ログをクリアするには、**clear accounting log** コマンドを使用します。

clear accounting log [**logflash**]

構文の説明

logflash	（任意）現在の VDC の logflash に保存されているアカウンティング ログをクリアします。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
5.0(2)	**logflash** キーワードが追加されました。
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

clear accounting log コマンドは、デフォルトの仮想デバイス コンテキスト（VDC 1）でだけ機能します。

このコマンドには、ライセンスは必要ありません。

例

次に、アカウンティング ログをクリアする例を示します。

```
switch# clear accounting log
```

関連コマンド

コマンド	説明
show accounting log	アカウンティング ログを表示します。

clear copp statistics

Control Plane Policing（CoPP; コントロール プレーン ポリシング）統計情報をクリアするには、**clear copp statistics** コマンドを使用します。

clear copp statistics

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

なし

コマンド モード

任意のコンフィギュレーション モード

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドはデフォルトの仮想デバイス コンテキスト（VDC）内でのみ使用できます。

このコマンドには、ライセンスは必要ありません。

例

次に、コントロール プレーン クラス マップを指定して、クラス マップ コンフィギュレーション モードを開始する例を示します。

```
switch# clear copp statistics
```

関連コマンド

コマンド	説明
show policy-map interface control-plane	インターフェイスの CoPP 統計情報を表示します。

clear cts role-based counters

ロールベース アクセス コントロール リスト（RBACL）統計情報をすべてのカウンタが 0 にリセットされるようにクリアするには、**clear cts role-based counters** コマンドを使用します。

clear cts role-based counters

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

なし

コマンド モード

任意のコンフィギュレーション モード

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
5.0(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、RBACL 統計情報をクリアする例を示します。

```
switch# clear cts role-based counters
```

関連コマンド

コマンド	説明
cts role-based counters enable	RBACL 統計情報をイネーブルにします。
show cts role-based counters	RBACL 統計情報の設定ステータスを表示し、すべての RBACL ポリシーの統計情報を一覧表示します。

clear dot1x

802.1X オーセンティケータ インスタンスをクリアするには、**clear dot1x** コマンドを使用します。

clear dot1x {**all** | **interface ethernet** *slot*/*port*}

構文の説明

all	すべての 802.1X オーセンティケータ インスタンスを指定します。
interface ethernet *slot*/*port*	指定のインターフェイスの 802.1X オーセンティケータ インスタンスを指定します。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

802.1X を設定する前に、**feature dot1x** コマンドを使用する必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、すべての 802.1X オーセンティケータ インスタンスをクリアする例を示します。

```
switch# clear dot1x all
```

次に、インターフェイスの 802.1X オーセンティケータ インスタンスをクリアする例を示します。

```
switch# clear dot1x interface ethernet 1/1
```

関連コマンド

コマンド	説明
feature dot1x	802.1X 機能をイネーブルにします。
show dot1x all	すべての 802.1X 情報を表示します。

clear eou

Extensible Authentication Protocol over User Datagram Protocol（EAPoUDP）セッションをクリアするには、**clear eou** コマンドを使用します。

clear eou {**all** | **authentication** {**clientless** | **eap** | **static**} | **interface ethernet** *slot*/*port* | **ip-address** *ipv4-address* | **mac-address** *mac-address* | **posturetoken** *type*}

構文の説明

all	すべての EAPoUDP セッションを指定します。
authentication	EAPoUDP 認証を指定します。
clientless	クライアントレス ポスチャ検証を使用して認証されたセッションを指定します。
eap	EAPoUDP を使用して認証されたセッションを指定します。
static	静的に設定された例外リストを使用して認証するセッションを指定します。
interface ethernet *slot*/*port*	インターフェイスを指定します。
ip-address *ipv4-address*	IPv4 アドレスを設定します。形式は、A.B.C.D です。
mac-address *mac-address*	MAC アドレスを指定します。
posturetoken *type*	ポスチャ トークン名を指定します。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

feature eou コマンドを使用して EAPoUDP をイネーブルにしてから、**clear eou** コマンドを使用する必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、すべての EAPoUDP セッションをクリアする例を示します。

```
switch# clear eou all
```

次に、静的に認証された EAPoUDP セッションをクリアする例を示します。

```
switch# clear eou authentication static
```

次に、インターフェイスの EAPoUDP セッションをクリアする例を示します。

```
switch# clear eou interface ethernet 1/1
```

次に、IP アドレスの EAPoUDP セッションをクリアする例を示します。

```
switch# clear eou ip-address 10.10.1.1
```

次に、MAC アドレスの EAPoUDP セッションをクリアする例を示します。

```
switch# clear eou mac-address 0019.076c.dac4
```

次に、ポスチャ トークンのタイプが Checkup である EAPoUDP セッションをクリアする例を示します。

```
switch# clear eou posturetoken healthy
```

関連コマンド

コマンド	説明
feature eou	EAPoUDP をイネーブルにします。
show eou	EAPoUDP 情報を表示します。

clear hardware rate-limiter

レート制限統計情報をクリアするには、**clear hardware rate-limiter** コマンドを使用します。

clear rate-limiter {**access-list-log** | **all** | **copy** | **layer-2** {**l2pt** | **mcast-snooping** | **port-security** | **storm-control** | **vpc-low**} | **layer-3** {**control** | **glean** | **mtu** | **multicast** {**directly-connected** | **local-groups** | **rpf-leak**} | **ttl**} | **receive**}

構文の説明

access-list-log	アクセスリスト ログ パケットのレート制限統計情報をクリアします。
all	すべてのレート制限統計情報をクリアします。
copy	コピーパケットのレート制限統計情報をクリアします。
layer-2	レイヤ 2 パケットのレート制限を指定します。
l2pt	レイヤ 2 トンネル プロトコル（L2TP）パケットのレート制限統計情報をクリアします。
mcast-snooping	レイヤ 2 マルチキャスト スヌーピング パケットのレート制限統計情報をクリアします。
port-security	レイヤ 2 ポート セキュリティ パケットのレート制限統計情報をクリアします。
storm-control	レイヤ 2 ストーム制御パケットのレート制限統計情報をクリアします。
vpc-low	VPC low キューでのレイヤ 2 制御パケットのレート制限統計情報をクリアします。
layer-3	レイヤ 3 パケットのレート制限を指定します。
control	レイヤ 3 制御パケットのレート制限統計情報をクリアします。
glean	レイヤ 3 グリーニング パケットのレート制限統計情報をクリアします。
mtu	レイヤ 3 Maximum Transmission Unit（MTU; 最大伝送ユニット）パケットのレート制限統計情報をクリアします。
multicast	レイヤ 3 マルチキャストのレート制限を指定します。
directly-connected	レイヤ 3 マルチキャスト直接接続パケットのレート制限統計情報をクリアします。
local-groups	レイヤ 3 マルチキャスト ローカル グループ パケットのレート制限統計情報をクリアします。
rpf-leak	レイヤ 3 マルチキャスト Reverse Path Forwarding（RPF; リバース パス転送）リーク パケットのレート制限統計情報をクリアします。
ttl	レイヤ 3 Time-to-Live（TTL; 存続可能時間）パケットのレート制限統計情報をクリアします。
receive	受信パケットのレート制限統計情報をクリアします。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin

コマンド履歴

リリース	変更箇所
5.0(2)	**l2pt** キーワードが追加されました。
4.0(3)	**port-security** キーワードが追加されました。
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、デフォルトの仮想デバイス コンテキスト（VDC）でだけ使用できます。
このコマンドには、ライセンスは必要ありません。

例

次に、すべてのレート制限統計情報をクリアする例を示します。

```
switch# clear hardware rate-limiter all
```

次に、アクセス リスト ログ パケットのレート制限統計情報をクリアする例を示します。

```
switch# clear hardware rate-limiter access-list-log
```

次に、レイヤ 2 ストーム制御パケットのレート制限統計情報をクリアする例を示します。

```
switch# clear hardware rate-limiter layer-2 storm-control
```

次に、レイヤ 3 グリーニング パケットのレート制限統計情報をクリアする例を示します。

```
switch# clear hardware rate-limiter layer-3 glean
```

次に、レイヤ 3 マルチキャスト直接接続パケットのレート制限統計情報をクリアする例を示します。

```
switch# clear hardware rate-limiter layer-3 multicast directly-connected
```

次に、受信パケットのレート制限統計情報をクリアする例を示します。

```
switch# clear hardware rate-limiter receive
```

関連コマンド

コマンド	説明
hardware rate-limiter	レート制限を設定します。
show hardware rate-limiter	レート制限情報を表示します。

clear ip access-list counters

すべてまたは 1 つの IPv4 アクセス コントロール リスト（ACL）のカウンタをクリアするには、**clear ip access-list counters** コマンドを使用します。

clear ip access-list counters [*access-list-name*]

構文の説明

access-list-name	（任意）デバイスがそのカウンタをクリアする IPv4 ACL の名前。名前では最大 64 文字までの英数字を使用でき、大文字と小文字が区別されます。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、すべての IPv4 ACL のカウンタをクリアする例を示します。

```
switch# clear ip access-list counters
switch#
```

次に、acl-ipv4-101 という名前の IP ACL のカウンタをクリアする例を示します。

```
switch# clear ip access-list counters acl-ipv4-101
switch#
```

関連コマンド

コマンド	説明
clear access-list counters	IPv4 ACL、IPv6 ACL、および MAC ACL のカウンタをクリアします。
clear ipv6 access-list counters	IPv6 ACL のカウンタをクリアします。
clear mac access-list counters	MAC ACL のカウンタをクリアします。
clear vlan access-list counters	VACL のカウンタをクリアします。

コマンド	説明
show access-lists	1 つまたはすべての IPv4 ACL、IPv6 ACL、および MAC ACL に関する情報を表示します。
show ip access-lists	1 つまたはすべての IPv4 ACL に関する情報を表示します。

clear ip arp inspection log

Dynamic ARP Inspection（DAI; ダイナミック ARP 検査）ログ バッファをクリアするには、**clear ip arp inspection log** コマンドを使用します。

clear ip arp inspection log

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、DAI ロギング バッファをクリアする例を示します。

```
switch# clear ip arp inspection log
switch#
```

関連コマンド

コマンド	説明
ip arp inspection log-buffer	DAI のログ バッファ サイズを設定します。
show ip arp inspection	DAI 設定ステータスを表示します。
show ip arp inspection log	DAI のログ設定を表示します。
show ip arp inspection statistics	DAI 統計情報を表示します。

clear ip arp inspection statistics vlan

指定の VLAN のダイナミック ARP 検査（DAI）統計情報をクリアするには、**clear ip arp inspection statistics vlan** コマンドを使用します。

clear ip arp inspection statistics vlan *vlan-list*

構文の説明

vlan *vlan-list*	このコマンドによってその DAI 統計情報がクリアされる VLAN を指定します。*vlan-list* 引数を使用すると、単一の VLAN ID、VLAN ID の範囲、またはカンマで区別された ID および範囲を指定できます（「例」を参照）。指定できる VLAN ID は 1 ～ 4094 です。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、VLAN 2 の DAI 統計情報をクリアする例を示します。

```
switch# clear ip arp inspection statistics vlan 2
switch#
```

次に、VLAN 5 ～ 12 の DAI 統計情報をクリアする例を示します。

```
switch# clear ip arp inspection statistics vlan 5-12
switch#
```

次に、VLAN 2 および VLAN 5 ～ 12 の DAI 統計情報をクリアする例を示します。

```
switch# clear ip arp inspection statistics vlan 2,5-12
switch#
```

関連コマンド

コマンド	説明
clear ip arp inspection log	DAI ロギング バッファをクリアします。
ip arp inspection log-buffer	DAI のログ バッファ サイズを設定します。
show ip arp inspection	DAI 設定ステータスを表示します。
show ip arp inspection vlan	VLAN の指定されたリストの DAI ステータスを表示します。

clear ip device tracking

IP デバイス トラッキング情報をクリアするには、**clear ip device tracking** コマンドを使用します。

clear ip device tracking {**all** | **interface ethernet** *slot*/*port* | **ip-address** *ipv4-address* | **mac-address** *mac-address*}

構文の説明

all	すべての IP デバイス トラッキング情報をクリアします。
interface ethernet *slot*/*port*	インターフェイスの IP デバイス トラッキング情報をクリアします。
ip-address *ipv4-address*	A.B.C.D 形式の IPv4 アドレスの IP デバイス トラッキング情報をクリアします。
mac-address *mac-address*	XXXX.XXXX.XXXX 形式の MAC アドレスの IP トラッキング情報をクリアします。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
vdc-admin
VDC ユーザ

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、すべての IP デバイス トラッキング情報をクリアする例を示します。

```
switch# clear ip device tracking all
```

次に、インターフェイスの IP デバイス トラッキング情報をクリアする例を示します。

```
switch# clear ip device tracking interface ethernet 1/1
```

次に、IP アドレスの IP デバイス トラッキング情報をクリアする例を示します。

```
switch# clear ip device tracking ip-address 10.10.1.1
```

次に、MAC アドレスの IP デバイス トラッキング情報をクリアする例を示します。

```
switch# clear ip device tracking mac-address 000c.30da.86f4
```

関連コマンド

コマンド	説明
ip device tracking	IP デバイス トラッキングをイネーブルにします。
show ip device tracking	IP デバイス トラッキングの情報を表示します。

clear ip dhcp snooping binding

DHCP スヌーピング バインディング データベースをクリアするには、**clear ip dhcp snooping binding** コマンドを使用します。

clear ip dhcp snooping binding

clear ip dhcp snooping binding [**vlan** *vlan-id* **mac** *mac-address* **ip** *ip-address* **interface ethernet** *slot*/*port*[**.***subinterface-number*]]

clear ip dhcp snooping binding [**vlan** *vlan-id* **mac** *mac-address* **ip** *ip-address* **interface port-channel** *channel-number*[**.***subchannel-number*]]

構文の説明

vlan *vlan-id*	（任意）*vlan-id* 引数およびその後に続く追加のキーワードと引数によって指定された VLAN ID で識別されるエントリの DHCP スヌーピング バインディング データベースをクリアします。
mac-address *mac-address*	クリアするバインディング データベース エントリの MAC アドレスを指定します。ドット付き 16 進表記で *mac-address* 引数を入力します。
ip *ip-address*	クリアするバインディング データベース エントリの IPv4 アドレスを指定します。ドット付き 10 進表記で *ip-address* 引数を入力します。
interface ethernet *slot*/*port*	（任意）クリアするバインディング データベース エントリのイーサネット インターフェイスを指定します。
.*subinterface-number*	（任意）イーサネット インターフェイスのサブインターフェイスの番号 **（注）** *port* 引数と *subinterface-number* 引数間には、ドット区切り文字が必要です。
interface port-channel *channel-number*	（任意）クリアするバインディング データベース エントリのイーサネット ポートチャネルを指定します。
.*subchannel-number*	（任意）イーサネット ポートチャネルのサブチャネルの番号 **（注）** *channel-number* 引数と *subchannel-number* 引数間には、ドット区切り文字が必要です。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
vdc-admin
VDC ユーザ

コマンド履歴

リリース	変更箇所
4.0(3)	このコマンドは、特定のバインディング データベース エントリのクリアをサポートするように変更されました。オプションの **vlan** キーワードおよびそれに続く引数とキーワードが追加されました。
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、DHCP スヌーピング バインディング データベースをクリアする例を示します。

```
switch# clear ip dhcp snooping binding
switch#
```

次に、DHCP スヌーピング バインディング データベースの特定のエントリをクリアする例を示します。

```
switch# clear ip dhcp snooping binding vlan 23 mac 0060.3aeb.54f0 ip 10.34.54.9 interface
ethernet 2/11
switch#
```

関連コマンド

コマンド	説明
ip dhcp snooping	デバイスの DHCP スヌーピングをグローバルにイネーブルにします。
show ip dhcp snooping	DHCP スヌーピングに関する一般的な情報を表示します。
show ip dhcp snooping binding	スタティック IP ソース エントリを含めて、IP-MAC アドレス バインディングを表示します。
show ip dhcp snooping statistics	DHCP スヌーピング統計情報を表示します。
show running-config dhcp	IP ソース ガード設定を含む、DHCP スヌーピング設定を表示します。

clear ipv6 access-list counters

すべてまたは 1 つの IPv6 アクセス コントロール リスト（ACL）のカウンタをクリアするには、**clear ipv6 access-list counters** コマンドを使用します。

clear ipv6 access-list counters [*access-list-name*]

構文の説明

access-list-name	（任意）デバイスがそのカウンタをクリアする IPv6 ACL の名前。名前では最大 64 文字までの英数字を使用でき、大文字と小文字が区別されます。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.1(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、すべての IPv6 ACL のカウンタをクリアする例を示します。

```
switch# clear ipv6 access-list counters
switch#
```

次に、acl-ipv6-3A という名前の IPv6 ACL のカウンタをクリアする例を示します。

```
switch# clear ipv6 access-list counters acl-ipv6-3A
switch#
```

関連コマンド

コマンド	説明
clear access-list counters	IPv4 ACL、IPv6 ACL、および MAC ACL のカウンタをクリアします。
clear ip access-list counters	IPv4 ACL のカウンタをクリアします。
clear mac access-list counters	MAC ACL のカウンタをクリアします。
clear vlan access-list counters	VACL のカウンタをクリアします。

コマンド	説明
show access-lists	1 つまたはすべての IPv4 ACL、IPv6 ACL、および MAC ACL に関する情報を表示します。
show ipv6 access-lists	1 つまたはすべての IPv6 ACL に関する情報を表示します。

clear ldap-server statistics

Lightweight Directory Access Protocol（LDAP）サーバ統計情報をクリアするには、**clear ldap-server statistics** コマンドを使用します。

clear ldap-server statistics {*ipv4-address* | *ipv6-address* | *host-name*}

構文の説明

ipv4-address	*A.B.C.D* 形式のサーバの IPv4 アドレス
ipv6-address	*X:X:X:X* 形式のサーバの IPv6 アドレス
host-name	サーバ名。名前は、英数字で指定します。大文字と小文字が区別され、最大文字数は 256 です。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更箇所
5.0(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、LDAP サーバの統計情報をクリアする例を示します。

```
switch# clear ldap-server statistics 10.10.1.1
```

関連コマンド

コマンド	説明
feature ldap	LDAP をイネーブルにします。
ldap-server host	LDAP サーバの IPv4 または IPv6 アドレス、あるいはホスト名を指定します。
show ldap-server statistics	LDAP サーバの統計情報を表示します。

clear mac access-list counters

すべてまたは 1 つの MAC アクセス コントロール リスト（ACL）のカウンタをクリアするには、**clear mac access-list counters** コマンドを使用します。

clear mac access-list counters [*access-list-name*]

構文の説明

access-list-name	（任意）デバイスがそのカウンタをクリアする MAC ACL の名前。名前では最大 64 文字までの英数字を使用でき、大文字と小文字が区別されます。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、すべての MAC ACL のカウンタをクリアする例を示します。

```
switch# clear mac access-list counters
switch#
```

次に、acl-mac-0060 という名前の MAC ACL のカウンタをクリアする例を示します。

```
switch# clear mac access-list counters acl-ipv4-0060
switch#
```

関連コマンド

コマンド	説明
clear access-list counters	IPv4 ACL、IPv6 ACL、および MAC ACL のカウンタをクリアします。
clear ip access-list counters	IPv4 ACL のカウンタをクリアします。
clear ipv6 access-list counters	IPv6 ACL のカウンタをクリアします。
clear vlan access-list counters	VACL のカウンタをクリアします。

コマンド	説明
show access-lists	1 つまたはすべての IPv4 ACL、IPv6 ACL、および MAC ACL に関する情報を表示します。
show mac access-lists	1 つまたはすべての MAC ACL に関する情報を表示します。

clear port-security

動的に学習された単一のセキュア MAC アドレス、または特定のインターフェイスの動的に学習されたすべてのセキュア MAC アドレスをクリアするには、**clear port-security** を使用します。

clear port-security dynamic interface ethernet *slot*/*port* [**vlan** *vlan-id*]

clear port-security dynamic interface port-channel *channel-number* [**vlan** *vlan-id*]

clear port-security dynamic address *address* [**vlan** *vlan-id*]

構文の説明

dynamic	動的に学習されたセキュア MAC アドレスをクリアするように指定します。
interface	クリアする対象の動的に学習されたセキュア MAC アドレスのインターフェイスを指定します。
ethernet *slot*/*port*	クリアする対象の動的に学習されたセキュア MAC アドレスのイーサネット インターフェイスを指定します。
vlan *vlan-id*	（任意）クリアするセキュア MAC アドレスの VLAN を指定します。有効な VLAN ID は、1 ～ 4096 です。
port-channel *channel-number*	クリアする対象の動的に学習されたセキュア MAC アドレスのポート チャネル インターフェイスを指定します。
address *address*	クリアする単一の MAC アドレスを指定します。*address* は、ドット付き 16 進表記の MAC アドレスです。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.2(1)	ポート チャネル インターフェイス上でのポート セキュリティのサポートが追加されました。
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

feature port-security コマンドを使用してポート セキュリティをイネーブルにしてから、**clear port-security** コマンドを使用する必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、イーサネット 2/1 インターフェイスから動的に学習されたセキュア MAC アドレスを削除する例を示します。

```
switch# configure terminal
switch(config)# clear port-security dynamic interface ethernet 2/1
```

次に、動的に学習されたセキュア MAC アドレス 0019.D2D0.00AE を削除する例を示します。

```
switch# configure terminal
switch(config)# clear port-security dynamic address 0019.D2D0.00AE
```

関連コマンド

コマンド	説明
debug port-security	ポート セキュリティのデバッグ情報を提供します。
feature port-security	ポート セキュリティをグローバルにイネーブル化します。
show port-security	ポート セキュリティに関する情報を表示します。
switchport port-security	レイヤ 2 インターフェイス上のポート セキュリティをイネーブルにします。

clear radius-server statistics

RADIUS サーバ ホストの統計情報をクリアするには、**clear radius-server statistics** コマンドを使用します。

clear radius-server statistics {*ipv4-address* | *ipv6-address* | *server-name*}

構文の説明

ipv4-address	*A.B.C.D* 形式の RADIUS サーバ ホストの IPv4 アドレス。
ipv6-address	*A:B::C:D* 形式の RADIUS サーバ ホストの IPv6 アドレス。
server-name	RADIUS サーバ ホストの名前。名前では、大文字と小文字が区別されます。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、RADIUS サーバの統計情報をクリアする例を示します。

```
switch# clear radius-server statistics 10.10.1.1
```

関連コマンド

コマンド	説明
show radius-server statistics	RADIUS サーバ ホストの統計情報を表示します。

clear ssh hosts

仮想デバイス コンテキスト（VDC）の Secure Shell（SSH; セキュア シェル）ホスト セッションおよび既知のホスト ファイルをクリアするには、**clear ssh hosts** コマンドを使用します。

clear ssh hosts

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、すべての SSH ホスト セッションおよび既知のホスト ファイルをクリアする例を示します。

```
switch# clear ssh hosts
```

関連コマンド

コマンド	説明
ssh server enable	SSH サーバをイネーブルにします。

clear tacacs-server statistics

TACACS+ サーバ ホストの統計情報をクリアするには、**clear tacacs-server statistics** コマンドを使用します。

clear tacacs-server statistics {*ipv4-address* | *ipv6-address* | *server-name*}

構文の説明

ipv4-address	*A.B.C.D* 形式の TACACS+ サーバ ホストの IPv4 アドレス。
ipv6-address	*A:B::C:D* 形式の TACACS+ サーバ ホストの IPv6 アドレス。
server-name	TACACS+ サーバ ホストの名前。名前では、大文字と小文字が区別されます。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、TACACS+ サーバの統計情報をクリアする例を示します。

```
switch# clear tacacs-server statistics 10.10.1.1
```

関連コマンド

コマンド	説明
show tacacs-server statistics	TACACS+ サーバ ホストの統計情報を表示します。

clear user

仮想デバイス コンテキスト（VDC）のユーザ セッションをクリアするには、**clear user** コマンドを使用します。

clear user *user-id*

構文の説明

user-id	ユーザ ID

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

デバイスで現在のユーザ セッションを表示するには、**show users** コマンドを使用します。

このコマンドには、ライセンスは必要ありません。

例

次に、すべての SSH ホスト セッションをクリアする例を示します。

```
switch# clear user user1
```

関連コマンド

コマンド	説明
show users	ユーザ セッション情報を表示します。

clear vlan access-list counters

すべてまたは 1 つの VLAN アクセス コントロール リスト（VACL）のカウンタをクリアするには、**clear vlan access-list counters** コマンドを使用します。

clear vlan access-list counters [*access-map-name*]

構文の説明

access-map-name	（任意）デバイスがそのカウンタをクリアする VLAN アクセス マップの名前。名前では最大 64 文字までの英数字を使用でき、大文字と小文字が区別されます。

デフォルト

なし

コマンド モード

特権 EXEC

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、すべての VACL のカウンタをクリアする例を示します。

```
switch# clear vlan access-list counters
switch#
```

次に、vlan-map-101 という名前の VACL のカウンタをクリアする例を示します。

```
switch# clear vlan access-list counters vlan-map-101
switch#
```

関連コマンド

コマンド	説明
clear access-list counters	IPv4 ACL、IPv6 ACL、および MAC ACL のカウンタをクリアします。
clear ip access-list counters	IPv4 ACL のカウンタをクリアします。
clear ipv6 access-list counters	IPv6 ACL のカウンタをクリアします。
clear mac access-list counters	MAC ACL のカウンタをクリアします。
show access-lists	1 つまたはすべての IPv4 ACL、IPv6 ACL、および MAC ACL に関する情報を表示します。
show vlan access-map	1 つまたはすべての VACL に関する情報を表示します。

copp copy profile

コントロール プレーン ポリシング（CoPP）ベスト プラクティス ポリシーのコピーを作成するには、**copp clone profile** コマンドを使用します。

copp copy profile {**lenient** | **moderate** | **strict**} {**prefix** | **suffix**} *string*

構文の説明

lenient	緩いプロファイルを指定します。
moderate	中程度のプロファイルを指定します。
strict	厳密なプロファイルを指定します。
prefix	クローニングされたポリシーで使用されるプレフィクスを指定します。
suffix	クローニングされたポリシーに使用するサフィクスを指定します。
string	プレフィクスまたはサフィクス文字列。プレフィクスまたはサフィクスは 8 文字以内の英数字のストリングで指定できます。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
5.2(1)	このコマンドが追加されました。

使用上のガイドライン

copp copy profile コマンドを使用した場合、CoPP は、指定したプレフィクスまたはサフィックスを持つすべてのクラス マップとポリシー マップの名前を変更します。

このコマンドには、ライセンスは必要ありません。

例

次に、CoPP ベスト プラクティス ポリシーのクローンを作成する例を示します。

```
switch # copp copy profile moderate abc
```

関連コマンド

コマンド	説明
copp profile	Cisco NX-OS デバイスにデフォルトの CoPP ベスト プラクティス ポリシーを適用します。
show copp status	最後の設定動作およびそのステータスなど、CoPP のステータスを表示します。
show running-config copp	実行コンフィギュレーション内の CoPP 設定を表示します。

copp profile

設定ユーティリティを再実行せずに Cisco NX-OS デバイスにデフォルトのコントロール プレーン ポリシング（CoPP）ベスト プラクティス ポリシーを適用するには、**copp profile** コマンドを使用します。Cisco NX-OS デバイスからデフォルトの CoPP ポリシーを削除するには、このコマンドの **no** 形式を使用します。

copp profile {**dense** | **lenient** | **moderate** | **strict**}

no copp profile {**dense** | **lenient** | **moderate** | **strict**}

構文の説明

dense	高密度のプロファイルを指定します。
lenient	緩いプロファイルを指定します。
moderate	中程度のプロファイルを指定します。
strict	厳密なプロファイルを指定します。

デフォルト

strict

コマンド モード

グローバル コンフィギュレーション（config）

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
5.2(1)	このコマンドが追加されました。
6.0(1)	dense キーワードが追加されました。

使用上のガイドライン

5.2(1) よりも前の Cisco NX-OS リリースでは、デフォルトの CoPP ポリシーを変更または再適用するには設定ユーティリティを使用する必要があります。設定ユーティリティにアクセスするには **setup** コマンドを使用します。

Cisco NX-OS Release 5.2 から、CoPP のベスト プラクティス ポリシーは読み取り専用です。設定を変更する場合は、**copp clone profile** コマンドでクローニングする必要があります。クローニングされたポリシーは、ユーザの設定として扱われます。

Cisco NX-OS Release 5.2 へのアップグレードにインサービス ソフトウェア ダウングレード（ISSU）を使用する場合、コントロール プレーンにアタッチされたポリシーは、ユーザ設定ポリシーとして扱われます。**show copp profile** コマンドを使用して CoPP プロファイルを確認し、必要な変更を加えます。

Cisco NX-OS Release 5.2 からのダウングレードに ISSU を使用する場合、CoPP は互換性のない設定を報告し、CoPP プロファイルを複製するように指示します。それ以前のバージョンでは、すべての設定がユーザ設定モードに復元されます。

このコマンドには、ライセンスは必要ありません。

例

次に、Cisco NX-OS デバイスにデフォルトの CoPP ベスト プラクティス ポリシーを適用する例を示します。

```
switch# configure terminal
switch(config)# copp profile moderate
switch(config)#
```

次に、Cisco NX-OS デバイスからデフォルトの CoPP ベスト プラクティス ポリシーを削除する例を示します。

```
switch(config)# no copp profile moderate
switch(config)#
```

関連コマンド

コマンド	説明
copp copy profile	CoPP ベスト プラクティス ポリシーのコピーを作成します。
show copp profile	CoPP ベスト プラクティス ポリシーの詳細を表示します。
show copp status	最後の設定動作およびそのステータスなど、CoPP のステータスを表示します。
show running-config copp	実行コンフィギュレーション内の CoPP 設定を表示します。

CRLLookup

検索クエリーを Lightweight Directory Access Protocol（LDAP）サーバに送信するために、証明書失効リスト（CRL）検索操作の属性名、検索フィルタ、ベース DN を設定するには、**CRLLookup** コマンドを使用します。この設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

CRLLookup attribute-name *attribute-name* **search-filter** *filter* **base-DN** *base-DN-name*

no CRLLookup

構文の説明

attribute-name *attribute-name*	LDAP 検索マップの属性名を指定します。名前は、英数字で指定します。大文字と小文字が区別され、最大文字数は 128 です。
search-filter *filter*	LDAP 検索マップ用のフィルタを指定します。名前は、英数字で指定します。大文字と小文字が区別され、最大文字数は 128 です。
base-DN *base-DN-name*	LDAP 検索マップのベース指定名を指定します。名前は、英数字で指定します。大文字と小文字が区別され、最大文字数は 128 です。

デフォルト

なし

コマンド モード

Lightweight Directory Access Protocol（LDAP）検索マップ コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
5.0(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、LDAP をイネーブルにする必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、検索クエリーを LDAP サーバに送信するために、CRL 検索操作の属性名、検索フィルタ、ベース DN を設定する例を示します。

```
switch# conf t
switch(config)# ldap search-map s0
switch(config-ldap-search-map)# CRLLookup attribute-name certificateRevocationList
search-filter (&(objectClass=cRLDistributionPoint)) base-DN CN=CDP,CN=Public Key
Services,CN=Services,CN=Configuration,DC=mdsldaptestlab,DC=com
switch(config-ldap-search-map)#
```

関連コマンド

コマンド	説明
feature ldap	LDAP をイネーブルにします。
ldap search-map	LDAP 検索マップを設定します。
show ldap-search-map	設定された LDAP 検索マップを表示します。

crypto ca authenticate

Certificate Authority（CA; 認証局）を関連付けて認証し、その CA 証明書（または証明書チェーン）を設定するには、**crypto ca authenticate** コマンドを使用します。関連付けと認証を削除するには、このコマンドの **no** 形式を使用します。

crypto ca authenticate *trustpoint-label*

no crypto ca authenticate *trustpoint-label*

構文の説明

trustpoint-label	トラストポイントの名前。名前は英数字で指定します。大文字と小文字が区別され、最大文字長は 64 文字です。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.1(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用すると、CA の公開キーに含まれる CA の自己署名証明書を取得することによって、Cisco NX-OS デバイスに対して CA を認証できます。CA では、証明書が自己署名されるため、このコマンドを実行するときは、CA 管理者に問い合わせて、CA の公開キーを手作業で認証する必要があります。CA 証明書または証明書チェーンは、Privacy Enhanced Mail（PEM; プライバシー エンハンスト メール）（base-64）暗号化形式で使用可能である必要があります。

このコマンドは、デバイスで認証局を初期設定するときに、使用します。まず、CA によって発行された CA 証明書フィンガープリントを使用し、**crypto ca trustpoint** コマンドを使用して、トラストポイントを作成します。CA によって発行された証明書フィンガープリントでの認証中に、表示される証明書フィンガープリントを比較する必要があり、一致する場合だけ、CA 証明書が受け付けられます。

認証する CA が下位認証局（自己署名ではない）の場合は、自己署名証明書が存在するまで、別の CA がそれを証明し、それがまた、別の CA によって代わりに証明されることがあります。この場合、下位証明書には、CA 証明書チェーンが存在します。CA 認証中は、チェーン全体を入力する必要があります。CA 証明書チェーンがサポートする最大長は、10 です。

トラストポイント CA は、信頼済み CA としてデバイスに設定する認証局です。デバイスでは、ローカルに信頼済みの CA またはその下位 CA によって、ピア証明書が署名されている場合に、受け付けられます。

（注） **crypto ca trustpoint** コマンドで作成するトラストポイント設定は、**copy running-config startup-config** コマンドを使用して明示的に保存する場合だけ、デバイスがリブートしても設定が引き継がれます。トラストポイントに関連付けられている証明書および CRL は、スタートアップ コンフィギュレーションでトラストポイントを設定する場合には、自動的に引き継がれます。スタートアップ コンフィギュレーションでトラストポイントを保存しない場合、関連付けられている証明書および CRL は、デバイスのリブート後に対応するトラストポイントなしでは終了できないため、自動的には引き継がれません。

設定された証明書、CRL、キー ペアが引き継がれるようにするには、スタートアップ コンフィギュレーションで実行コンフィギュレーションを常に保存する必要があります。

このコマンドには、ライセンスは必要ありません。

例

次の例では、myCA という名前の CA 証明書を認証する方法を示します。

```
switch# configure terminal
switch(config)# crypto ca authenticate myCA
input (cut & paste) CA certificate (chain) in PEM format;
end the input with a line containing only END OF INPUT :
-----BEGIN CERTIFICATE-----
MIIC4jCCAoygAwIBAgIQBWDSiay0GZRPSRIljK0ZejANBgkqhkiG9w0BAQUFADCB
kDEgMB4GCSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAklO
MRIwEAYDVQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UE
ChMFQ2lzY28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBD
QTAeFw0wNTA1MDMyMjQ2MzdaFw0wNzA1MDMyMjU1MTdaMIGQMSAwHgYJKoZIhvcN
AQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UEBhMCSU4xEjAQBgNVBAgTCUth
cm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4wDAYDVQQKEwVDaXNjbzETMBEG
A1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBhcm5hIENBMFwwDQYJKoZIhvcN
AQEBBQADSwAwSAJBAMW/7b3+DXJPANBsIHHzluNccNM87ypyzwuoSNZXOMpeRXXI
OzyBAgiXT2ASFuUOwQ1iDM8rO/41jf8RxvYKvysCAwEAAaOBvzCBvDALBgNVHQ8E
BAMCAcYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJyjyRoMbrCNMRU2OyRhQ
GgsWbHEwawYDVR0fBGQwYjAuoCygKoYoaHR0cDovL3NzZS0wOC9DZXJ0RW5yb2xs
L0FwYXJuYSUyMENBLmNybDAwoC6gLIYqZmlsZTovL1xcc3NlLTA4XENlcnRFbnJv
bGxcQXBhcm5hJTIwQ0EuY3JsMBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3DQEB
BQUAA0EAHv6UQ+8nE399Tww+KaGr0g0NIJaqNgLh0AFcT0rEyuyt/WYGPzksF9Ea
NBG7E0oN66zex0EOEfG1Vs6mXp1//w==
-----END CERTIFICATE-----
 END OF INPUT
Fingerprint(s): MD5 Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12
Do you accept this certificate? [yes/no]: y
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイントを設定します。
show crypto ca certificates	設定されているトラストポイント証明書を表示します。
show crypto ca trustpoints	トラストポイント設定を表示します。

crypto ca crl request

認証局（CA）からダウンロードされた新規の証明書失効リスト（CRL）を設定するには、**crypto ca crl request** コマンドを使用します。

crypto ca crl request *trustpoint-label source-file*

構文の説明

trustpoint-label	トラストポイントの名前。最大で 64 文字のサイズまで指定可能です。
source-file	**bootflash**:*filename* の形式での CRL の場所。最大サイズは 512 です。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.1(2)	このコマンドが追加されました。

使用上のガイドライン

crypto ca crl request コマンドを使用すると、トラストポイントに対して CRL を事前ダウンロードし、証明書（cert）ストアに CRL をキャッシュ保存できます。指定した CRL ファイルは、プライバシー エンハンスト メール（PEM）形式または Distinguished Encoding Rules（DER）形式のいずれかで最新の CRL を含める必要があります。

（注）

crypto ca trustpoint コマンドで作成するトラストポイント設定は、**copy running-config startup-config** コマンドを使用して明示的に保存する場合だけ、デバイスがリブートしても設定が引き継がれます。トラストポイントに関連付けられている証明書および CRL は、スタートアップ コンフィギュレーションでトラストポイントを設定する場合には、自動的に引き継がれます。スタートアップ コンフィギュレーションでトラストポイントを保存しない場合、関連付けられている証明書および CRL は、デバイスのリブート後に対応するトラストポイントなしでは終了できないため、自動的には引き継がれません。

設定された証明書、CRL、キー ペアが引き継がれるようにするには、スタートアップ コンフィギュレーションで実行コンフィギュレーションを常に保存する必要があります。

このコマンドには、ライセンスは必要ありません。

例

次の例では、トラストポイントで CRL を設定するか、または現在の CRL を置き換える方法を示します。

```
switch# configure teminal
switch(config)# crypto ca crl request admin-ca bootflash:admin-ca.crl
```

関連コマンド

コマンド	説明
revocation-check	トラストポイント失効チェック方法を設定します。
show crypto ca crl	設定済みの証明書失効リスト（CRL）を表示します。

crypto ca enroll

このトラストポイント CA 用に作成されるデバイス RSA キー ペアの認証を要求するには、**crypto ca enroll** コマンドを使用します。

crypto ca enroll *trustpoint-label*

構文の説明

trustpoint-label	トラストポイントの名前。最大で 64 文字のサイズまで指定可能です。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.1(2)	このコマンドが追加されました。

使用上のガイドライン

Cisco NX-OS デバイスは、トラストポイント CA とともに登録され、アイデンティティ証明書が取得されます。複数のトラストポイントとともにデバイスを登録し、各トラストポイントから別のアイデンティティ証明書を取得できます。

トラストポイントを登録するときには、認証する RSA キー ペアを指定する必要があります。登録要求を生成する前に、キー ペアを生成し、トラストポイントに関連付ける必要があります。

crypto ca enroll コマンドを使用すると、認証済みの CA に対応する各トラストポイントから、アイデンティティ証明書を取得する要求を生成できます。生成される Certificate Signing Request（CSR; 証明書署名要求）は、Public-Key Cryptography Standards（PKCS; 公開キー暗号化規格）の規格 #10 に準拠し、PEM 形式で表示されます。証明書をカット アンド ペーストし、電子メールを介してか、または CA Web サイトで、対応する CA に送信します。CA 管理者は、証明書を発行し、Web サイトを介してか、電子メールで送信して、その証明書を使用可能にします。トラストポイントに対応する、取得済みのアイデンティティ証明書は、**crypto ca import** *trustpoint-label* **certificate** コマンドを使用してインポートする必要があります。

（注） デバイスの設定では、チャレンジ パスワードは保存されません。証明書を破棄する場合に必要な場合に指定できるよう、このパスワードを記録します。

このコマンドには、ライセンスは必要ありません。

例

次の例では、認証済み CA に対する証明書の要求を生成する方法を示します。

```
switch# configure terminal
switch(config)# crypto ca enroll myCA
 Create the certificate request ..
 Create a challenge password. You will need to verbally provide this
  password to the CA Administrator in order to revoke your certificate.
  For security reasons your password will not be saved in the configuration.
  Please make a note of it.
  Password:nbv123
 The subject name in the certificate will be: Vegas-1.cisco.com
 Include the switch serial number in the subject name? [yes/no]:no
 Include an IP address in the subject name [yes/no]:yes
ip address:209.165.200.226
 The certificate request will be displayed...
-----BEGIN CERTIFICATE REQUEST-----
MIIBqzCCARQCAQAwHDEaMBgGA1UEAxMRVmVnYXMtMS5jaXNjby5jb20wgZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBAL8Y1UAJ2NC7jUJ1DVaSMqNIgJ2kt8rl4lKY
0JC6ManNy4qxk8VeMXZSiLJ4JgTzKWdxbLDkTTysnjuCXGvjb+wj0hEhv/y51T9y
P2NJJ8ornqShrvFZgC7ysN/PyMwKcgzhbVpj+rargZvHtGJ91XTq4WoVkSCzXv8S
VqyH0vEvAgMBAAGgTzAVBgkqhkiG9w0BCQcxCBMGbmJ2MTIzMDYGCSqGSIb3DQEJ
DjEpMCcwJQYDVR0RAQH/BBswGYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwDQYJ
KoZIhvcNAQEEBQADgYEAkT60KER6Qo8nj0sDXZVHSfJZh6K6JtDz3Gkd99GlFWgt
PftrNcWUE/pw6HayfQl2T3ecgNwel2d15133YBF2bktExiI6Ul88nTOjglXMjja8
8a23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbjfngPNTZacJCUS6ZqKCMetbKytUx0=
-----END CERTIFICATE REQUEST-----
```

関連コマンド

コマンド	説明
crypto ca import trustpoint-label certificate	CA から取得されたアイデンティティ証明書を、トラストポイントへインポートします。
crypto key generate rsa	RSA キー ペアを生成します。
rsakeypair	RSA キー ペアの詳細を設定し、トラストポイントへ関連付けます。
show crypto key mypubkey rsa	すべての RSA 公開キーの設定を表示します。

crypto ca export

RSA キー ペアと、公開キー暗号化規格（PKCS）の規格 #12 形式のファイル内のトラストポイントの関連付け済み証明書（アイデンティティおよび CA）を、指定する場所へエクスポートするには、**crypto ca export** コマンドを使用します。

crypto ca export *trustpoint-label* **pkcs12** *destination-file-url pkcs12-password*

構文の説明

trustpoint-label	トラストポイントの名前。最大で 64 文字のサイズまで指定可能です。
pkcs12 *destination-file-url*	**bootflash**:*filename* の形式で、宛先ファイルを指定します。ファイル名は、英数字で指定します。大文字と小文字が区別され、最大文字数は 512 です。
pkcs12-password	エクスポートされるファイルで RSA 秘密キーを保護するために使用するパスワード。パスワードは、英数字で指定します。大文字と小文字が区別され、最大文字数は 64 です。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.1(2)	このコマンドが追加されました。

使用上のガイドライン

バックアップの目的で、関連付けられている RSA キー ペアと CA 証明書（または証明書チェーン）とともに、アイデンティティ証明書を PKCS #12 形式のファイルにエクスポートできます。あとで証明書と RSA キー ペアをインポートして、デバイスのシステム障害から回復できます。

このコマンドには、ライセンスは必要ありません。

例

次に、PKCS #12 形式で証明書とキー ペアをエクスポートする例を示します。

```
switch# configure terminal
switch(config)# crypto ca export admin-ca pkcs12 bootflash:adminid.p12 nbv123
```

関連コマンド

コマンド	説明
crypto ca import trustpoint-label certificate	CA から取得されたアイデンティティ証明書を、トラストポイントへインポートします。
crypto ca import trustpoint-label pkcs12	アイデンティティ証明書、関連付けられている RSA キー ペア、CA 証明書（チェーン）を、トラストポイントへインポートします。
crypto key generate rsa	RSA キー ペアを生成します。
rsakeypair	RSA キー ペアの詳細を設定し、トラストポイントへ関連付けます。
show crypto key mypubkey rsa	任意の RSA 公開キーの設定を表示します。

crypto ca import

Privacy Enhanced Mail（PEM）形式のアイデンティティ証明書、または公開キー暗号化規格（PKCS）の規格 #12 形式のアイデンティティ証明書、関連付けられている RSA キー ペア、および CA 証明書（または証明書チェーン）をインポートするには、**crypto ca import** コマンドを使用します。

crypto ca import *trustpoint-label* {**certificate** | **pkcs12** *source-file-url pkcs12-password*}

構文の説明

trustpoint-label	トラストポイントの名前。最大で 64 文字のサイズまで指定可能です。
certificate	コマンド ライン インターフェイス（CLI）プロンプトで、トラストポイント証明書をペーストします。
pkcs12 *source-file-url*	**bootflash**:*filename* の形式で、トラストポイント証明書が含まれている発信元ファイルを指定します。ファイル名では、大文字と小文字が区別されます。
pkcs12-password	インポートされる PKCS#12 ファイルで RSA 秘密キーを保護するために使用するパスワード。パスワードでは大文字と小文字が区別されます。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.1(2)	このコマンドが追加されました。

使用上のガイドライン

トラストポイントで前に生成された登録要求に対応し、CA に送信された、CA から取得されたアイデンティティ証明書を（カット アンド ペーストする方法で）インポートするには、**certificate** キーワードを使用します。

完全なアイデンティティ情報を空のトラストポイントにインポートするには、**pkcs12** *source-file-url pkcs12-password* キーワードと引数を使用します。これには、アイデンティティ証明書、関連付けられている RSA キー ペア、および、CA 証明書または証明書チェーンが含まれます。この方法を使用すると、システム障害の発生後に、設定を復元することができます。

（注） **crypto ca trustpoint** コマンドで作成するトラストポイント設定は、**copy running-config startup-config** コマンドを使用して明示的に保存する場合だけ、デバイスがリブートしても設定が引き継がれます。トラストポイントに関連付けられている証明書および CRL は、スタートアップ コンフィギュレーションでトラストポイントを設定する場合には、自動的に引き継がれます。スタートアップ コンフィギュレーションでトラストポイントを保存しない場合、関連付けられている証明書および CRL は、デバイスのリブート後に対応するトラストポイントなしでは終了できないため、自動的には引き継がれません。

設定された証明書、CRL、キー ペアが引き継がれるようにするには、スタートアップ コンフィギュレーションで実行コンフィギュレーションを常に保存する必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、行われた登録要求に対応し、前に送信された CA から取得されたアイデンティティ証明書をインストールする例を示します。

```
switch# configure terminal
switch(config)# crypto ca import myCA certificate
input (cut & paste) certificate in PEM format:
-----BEGIN CERTIFICATE-----
MIIEADCCA6qgAwIBAgIKCjOOoQAAAAAAdDANBgkqhkiG9w0BAQUFADCBkDEgMB4G
CSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAklOMRIwEAYD
VQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UEChMFQ2lz
Y28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBDQTAeFw0w
NTExMTIwMzAyNDBaFw0wNjExMTIwMzEyNDBaMBwxGjAYBgNVBAMTEVZlZ2FzLTEu
Y2lzY28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/GNVACdjQu41C
dQ1WkjKjSICdpLfK5eJSmNCQujGpzcuKsZPFXjF2UoiyeCYE8ylncWyw5E08rJ47
glxr42/sI9IRIb/8udU/cj9jSSfKK56koa7xWYAu8rDfz8jMCnIM4W1aY/q2q4Gb
x7RifdV06uFqFZEgs17/Elash9LxLwIDAQABo4ICEzCCAg8wJQYDVR0RAQH/BBsw
GYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwHQYDVR0OBBYEFKCLi+2sspWEfgrR
bhWmlVyo9jngMIHMBgNVHSMEgcQwgcGAFCco8kaDG6wjTEVNjskYUBoLFmxxoYGW
pIGTMIGQMSAwHgYJKoZIhvcNAQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UE
BhMCSU4xEjAQBgNVBAgTCUthcm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4w
DAYDVQQKEwVDaXNjbzETMBEGA1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBh
cm5hIENBghAFYNKJrLQZlE9JEiWMrRl6MGsGA1UdHwRkMGIwLqAsoCqGKGh0dHA6
Ly9zc2UtMDgvQ2VydEVucm9sbC9BcGFybmElMjBDQS5jcmwwMKAuoCyGKmZpbGU6
Ly9cXHNzZS0wOFxDZXJ0RW5yb2xsXEFwYXJuYSUyMENBLmNybDCBigYIKwYBBQUH
AQEEfjB8MDsGCCsGAQUFBzAChi9odHRwOi8vc3NlLTA4L0NlcnRfbnJvbGwvc3Nl
LTA4X0FwYXJuYSUyMENBLmNydDA9BggrBgEFBQcwAoYxZmlsZTovL1xcc3NlLTA4
XENlcnRfbnJvbGxcc3NlLTA4X0FwYXJuYSUyMENBLmNydDANBgkqhkiG9w0BAQUF
AANBADbGBGsbe7GNLh9xeOTWBNbm24U69ZSuDDcOcUZUUTgrpnTqVpPyejtsyflw
E36cIZu4WsExREqxbTk8ycx7V5o=
-----END CERTIFICATE-----
```

次の例では、公開キー暗号化規格（PKCS）#12 形式のファイルに証明書とキー ペアをインポートする例を示します。

```
switch# configure terminal
witch(config)# crypto ca import admin-ca pkcs12 bootflash:adminid.p12 nbv123
```

関連コマンド

コマンド	説明
crypto ca export trustpoint-label pkcs12	関連付けられているトラストポイントの証明書と RSA キー ペアをエクスポートします。
crypto ca enroll	トラストポイントに対する証明書署名要求を生成します。
crypto key generate rsa	RSA キー ペアを生成します。
rsakeypair	トラストポイントの RSA キー ペアの詳細を設定します。
show crypto ca certificates	アイデンティティと CA 証明書の詳細を表示します。
show crypto key mypubkey rsa	任意の RSA 公開キーの設定を表示します。

crypto ca lookup

証明書認証に使用する証明書ストアを指定するには、**crypto ca lookup** コマンドを使用します。

crypto ca lookup {**local** | **remote** | **both**}

構文の説明

local	証明書認証にローカル証明書ストアを指定します。
remote	証明書認証にリモート証明書ストアを指定します。
both	証明書認証にローカル証明書ストアを指定しますが、認証が失敗するか、CA 証明書が見つからない場合は、リモート証明書ストアを使用します。

デフォルト

local

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
5.0(2)	このコマンドが追加されました。

使用上のガイドライン

リモート証明書ストアを設定する場合は、リモート デバイスに LDAP サーバを設定し、認証に使用する CA 証明書が Active Directory にロードされていることを確認する必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、証明書認証にリモート証明書ストアを指定する例を示します。

```
switch(config)# crypto ca lookup remote
```

関連コマンド

コマンド	説明
crypto ca remote ldap crl-refresh-time	リモート証明書ストアから証明書失効リストを更新するリフレッシュ時間を設定します。
crypto ca remote ldap server-group	LDAP との通信中に使用する LDAP サーバ グループを設定します。

コマンド	説明
show crypto ca certstore	設定済みの証明書ストアを表示します。
show crypto ca remote-certstore	リモートの cert-store の設定を表示します。

crypto ca remote ldap crl-refresh-time

リモート証明書ストアから証明書失効リスト（CRL）を更新するリフレッシュ時間を設定するには、**crypto ca remote ldap crl-refresh-time** コマンドを使用します。

crypto ca remote ldap crl-refresh-time *hours*

構文の説明

hours	時間単位でのリフレッシュ時間。範囲は 0 ～ 744 時間です。0 を入力すると、リフレッシュ ルーチンが 1 回実行されます。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
5.0(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、リモート証明書ストアと LDAP サーバ グループを設定する必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、リモート証明書ストアから CRL を更新するリフレッシュ時間を設定する例を示します。

```
switch(config)# crypto ca remote ldap crl-refresh-time 10
```

関連コマンド

コマンド	説明
crypto ca lookup	証明書認証に使用する証明書ストアを指定します。
crypto ca remote ldap server-group	LDAP との通信中に使用する LDAP サーバ グループを設定します。

crypto ca remote ldap server-group

Lightweight Directory Access Protocol（LDAP）との通信中に使用する LDAP サーバ グループを設定するには、**crypto ca remote ldap server-group** コマンドを使用します。

crypto ca remote ldap server-group *group-name*

構文の説明

group-name	サーバ グループ名。最大 64 文字の英数字を入力できます。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
5.0(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、リモート証明書ストアを設定する必要があります。

このコマンドには、ライセンスは必要ありません。

例

次の例に、LDAP との通信中に使用する LDAP サーバ グループを設定する例を示します。

```
switch(config)# crypto ca remote ldap server-group group1
```

関連コマンド

コマンド	説明
crypto ca lookup	証明書認証に使用する証明書ストアを指定します。
crypto ca remote ldap crl-refresh-time	リモート証明書ストアから証明書失効リストを更新するリフレッシュ時間を設定します。

crypto ca test verify

証明書ファイルを確認するには、**crypto ca test verify** コマンドを使用します。

crypto ca test verify *certificate-file*

構文の説明

certificate-file	**bootflash**:*filename* の形式でファイル名を認証します。ファイル名では、大文字と小文字が区別されます。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.1(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用すると、設定されている信頼済みの CA を使用して、また、必要に応じて、失効チェック設定で示されているとおりに証明書失効リスト（CRL）に問い合せることによって、PEM 形式で指定されている証明書を確認できます。

このコマンドには、ライセンスは必要ありません。

例

次の例では、証明書ファイルを確認する方法を示します。

```
switch(config)# crypto ca test verify bootflash:id1.pem
verify status oode:0
verify error msg:
```

（注） 確認ステータス コードの値 0 は、確認が正常終了したことを示します。

関連コマンド

コマンド	説明
show crypto ca certificates	設定されているトラストポイント証明書を表示します。

crypto ca trustpoint

デバイスが信頼し、トラストポイント コンフィギュレーション モードに入る必要があるトラストポイント認証局（CA）を作成するには、**crypto ca trustpoint** コマンドを使用します。トラストポイントを削除するには、このコマンドの **no** 形式を使用します。

crypto ca trustpoint *trustpoint-label*

no crypto ca trustpoint *trustpoint-label*

構文の説明

trustpoint-label	トラストポイントの名前。名前は、英数字で指定します。大文字と小文字が区別され、最大文字数は 64 です。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.1(2)	このコマンドが追加されました。

使用上のガイドライン

トラストポイントには、次のような特性があります。

- 1 つのトラストポイントは、単一の CA に対応します。Cisco NX-OS デバイスは、任意のアプリケーションに対するピア証明書確認のために、CA を信頼します。
- CA は、**crypto ca authenticate** コマンドを使用して、トラストポイントに明示的に関連付けられる必要があります。
- Cisco NX-OS デバイスでは、デバイス上に多くのトラストポイントを置くことができ、デバイス上のすべてのアプリケーションは、任意のトラストポイント CA によって発行されたピア証明書を信頼できます。
- トラストポイントは、特定のアプリケーションによる制限は受けません。
- Cisco NX-OS デバイスは、オプションで、トラストポイント CA とともに登録し、そのデバイスそのものに対する保障証明書を取得できます。

アプリケーションに対して、1 つまたは複数のトラストポイントを指定する必要はありません。証明書がアプリケーションの要件を満たしている限り、アプリケーションでは、トランスポイントによって発行されたどの証明書も使用できます。

トランスポイントからは、2 つ以上のアイデンティティ証明書も、トランスポイントに関連付けられている 2 つ以上のキー ペアも、必要ではありません。CA 証明書は、付与されたアイデンティティ（の名前）を一度だけ使用し、同じサブジェクト名で複数の証明書は発行しません。CA で複数のアイデンティティ証明書が必要な場合、CA で同じサブジェクト名の複数の証明書が認められる場合には、同じ CA に対して別のトラストポイントを定義し、それに別のキー ペアを関連付け、それを認証します。

（注） **no crypto ca trustpoint** コマンドを使用してトランスポイントを削除する前に、まず、アイデンティティ証明書と CA 証明書（または証明書チェーン）を削除し、次に、トラストポイントから RSA キーペアの関連付けを解除する必要があります。デバイスでは、このアクションのシーケンスを実行することにより、証明書でトラストポイントを誤って削除することを防ぎます。

このコマンドには、ライセンスは必要ありません。

例

次に、デバイスが信頼し、トラストポイント コンフィギュレーション モードに入る必要があるトラストポイント CA を宣言する例を示します。

```
switch# configure terminal
switch(config)# crypto ca trustpoint admin-ca
switch(config-trustpoint)#
```

次に、トラストポイント CA を削除する例を示します。

```
switch# configure terminal
switch(config)# no crypto ca trustpoint admin-ca
```

関連コマンド

コマンド	説明
crypto ca authenticate	認証局の証明書を認証します。
crypto ca enroll	トラストポイントに対する証明書署名要求を生成します。
show crypto ca certificates	アイデンティティと CA 証明書の詳細を表示します。
show crypto ca trustpoints	トラストポイント設定を表示します。

crypto certificatemap mapname

フィルタ マップを作成するには、**crypto certificatemap mapname** コマンドを使用します。

crypto certificatemap mapname *map-name*

構文の説明

map-name	フィルタ マップ名です。最大 64 文字の英数字を入力できます。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
5.0(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、証明書認証に証明書ストアを設定する必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、新しいフィルタ マップを作成する例を示します。

```
switch(config)# crypto certificatemap mapname filtermap1
```

関連コマンド

コマンド	説明
filter	フィルタ マップ内で証明書マッピングのフィルタを 1 つまたは複数設定します。
show crypto certificatemap	証明書マッピングのフィルタを表示します。

crypto cert ssh-authorize

SSH プロトコルの証明書マッピング フィルタを設定するには、**crypto cert ssh-authorize** コマンドを使用します。

crypto cert ssh-authorize [**default** | *issuer-CAname*] [**map** *map-name1* [*map-name2*]]

構文の説明

default	SSH 認可用のデフォルトのフィルタ マップを指定します。
issuer-CAname	CA 証明書の発行者。最大 64 文字の英数字を入力できます。最大 64 文字の英数字を入力できます。
map	適用するマッピング フィルタを指定します。
map-name1, *map-name2*	すでに設定されているデフォルトのマッピング フィルタの名前。最大 64 文字の英数字を入力できます。 デフォルトのマップを使用しない場合は、認証用のフィルタ マップを 1 つまたは 2 つ指定できます。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
5.0(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、フィルタ マップを作成する必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、SSH プロトコルの証明書マッピング フィルタを設定する例を示します。

```
switch(config)# crypto cert ssh-authorize default map filtermap1
```

関連コマンド

コマンド	説明
crypto certificatemap mapname	フィルタ マップを作成します。

コマンド	説明
filter	フィルタ マップ内で証明書マッピングのフィルタを 1 つまたは複数設定します。
show crypto ssh-auth-map	SSH 認証用に設定されたマッピングのフィルタを表示します。

cts device-id

Cisco TrustSec デバイス ID を設定するには、**cts device-id** コマンドを使用します。

cts device-id *device-id* **password** [**7**] *password*

構文の説明

device-id	Cisco TrustSec デバイス ID 名。名前には英数字を使用します。大文字と小文字が区別され、最大長は 32 文字です。
7	（任意）パスワードを暗号化します。
password *password*	EAP-FAST 処理中に使用するパスワードを指定します。名前には英数字を使用します。大文字と小文字が区別され、最大長は 32 文字です。

デフォルト

Cisco TrustSec デバイス ID なし
クリア テキスト パスワード

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

Cisco TrustSec デバイス ID 名は、Cisco TrustSec ネットワーク クラウド内で一意でなければなりません。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、Cisco TrustSec デバイス ID を設定する例を示します。

```
switch# configure terminal
swtich(config)# cts device-id DeviceA password Cisco321
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts credentials	Cisco TrustSec クレデンシャル情報を表示します。

cts dot1x

インターフェイスで Cisco TrustSec 認証をイネーブルにして、Cisco TrustSec 802.1X コンフィギュレーション モードを開始するには、**cts dot1x** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

cts dot1x

no cts dot1x

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ディセーブル

コマンド モード

インターフェイス コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、F1 シリーズ モジュールおよび F2 シリーズ モジュールではサポートされません。

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドを使用したあと、設定を有効にするには、**shutdown**/**no shutdown** コマンド シーケンスを使用することによってインターフェイスをイネーブルおよびディセーブルにする必要があります。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、インターフェイスで Cisco TrustSec 認証をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# cts dot1x
switch(config-if-cts-dot1x)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

次に、インターフェイスで Cisco TrustSec 認証をディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# no cts dot1x
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts interface	インターフェイスの Cisco TrustSec 設定情報を表示します。

cts manual

インターフェイスの Cisco TrustSec 手動設定を開始するには、**cts manual** コマンドを使用します。手動設定を削除するには、このコマンドの **no** 形式を使用します。

cts manual

no cts manual

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドを使用したあと、設定を有効にするには、**shutdown**/**no shutdown** コマンド シーケンスを使用することによってインターフェイスをイネーブルおよびディセーブルにする必要があります。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、インターフェイスの Cisco TrustSec 手動コンフィギュレーション モードを開始する例を示します。

```
switch# configure terminal
switch(config)# interface etherent 2/4
switch(config-if)# cts manual
switch(config-if-cts-manual)#
```

次に、インターフェイスから Cisco TrustSec 手動設定を削除する例を示します。

```
switch# configure terminal
switch(config)# interface etherent 2/4
switch(config-if)# no cts manual
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts interface	インターフェイスの Cisco TrustSec 設定情報を表示します。

cts refresh role-based-policy

Cisco Secure ACS からダウンロードした Cisco TrustSec Security Group Access Control List（SGACL; セキュリティ グループ アクセス コントロール リスト）ポリシーをリフレッシュするには、**cts refresh role-based-policy** コマンドを使用します。

cts refresh role-based-policy

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

なし

コマンド モード

任意のコンフィギュレーション モード

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、インターフェイスの Cisco TrustSec 手動コンフィギュレーション モードを開始する例を示します。

```
switch# cts refresh role-based-policy
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts role-based policy	Cisco TrustSec SGACL ポリシー設定を表示します。

cts rekey

Cisco TrustSec ポリシーのインターフェイス キーを再生成するには、**cts rekey** コマンドを使用します。

cts rekey ethernet *slot*/*port*

構文の説明

ethernet *slot*/*port*	イーサネット インターフェイスを指定します。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、Cisco TrustSec のインターフェイス キーを再生成する例を示します。

```
switch# cts rekey ethernet 2/3
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts interface	インターフェイスの Cisco TrustSec 設定情報を表示します。

cts role-based access-list

Cisco TrustSec セキュリティ グループ アクセス コントロール リスト（SGACL）を作成または指定して、ロールベース アクセス コントロール リスト コンフィギュレーション モードを開始するには、**cts role-based access-list** コマンドを使用します。SGACL を削除するには、このコマンドの **no** 形式を使用します。

cts role-based access-list *list-name*

no cts role-based access-list *list-name*

構文の説明

list-name	SGACL の名前。名前には英数字を使用します。大文字と小文字が区別され、最大長は 32 文字です。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、Cisco TrustSec SGACL を作成して、ロールベース アクセス リスト コンフィギュレーション モードを開始する例を示します。

```
switch# configure terminal
switch(config)# cts role-based access-list MySGACL
switch(config-rbacl)#
```

次に、Cisco TrustSec SGACL を削除する例を示します。

```
switch# configure terminal
switch(config)# no cts role-based access-list MySGACL
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts role-based access-list	Cisco TrustSec SGACL の設定を表示します。

cts role-based counters enable

ロールベース アクセス コントロール リスト（RBACL）統計情報をイネーブルにするには、**cts role-based counters enable** コマンドを使用します。RBACL 統計情報をディセーブルにするには、このコマンドの **no** 形式を使用します。

cts role-based counters enable

no cts role-based counters enable

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
5.0(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドを使用するには、VLAN および VRF への RBACL ポリシーの適用をイネーブルにする必要があります。

RBACL 統計情報をイネーブルにするには、ハードウェアのエントリが各ポリシーに 1 つずつ必要です。ハードウェアに十分な領域がない場合、エラー メッセージが表示され、統計情報をイネーブルにできません。

RBACL ポリシーを変更するとき、割り当て済みの Access Control Entry（ACE; アクセス コントロール エントリ）の統計情報が表示され、新しく割り当てられた ACE 統計情報が 0 に初期化されます。

RBACL 統計情報は、Cisco NX-OS デバイスのリロード時または統計情報を故意にクリアしたときにだけ失われます。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、RBACL 統計情報をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# cts role-based counters enable
```

次に、RBACL 統計情報をディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# no cts role-based counters enable
```

関連コマンド

コマンド	説明
clear cts role-based counters	すべてのカウンタが 0 にリセットされるように、RBACL 統計情報をクリアします。
show cts role-based counters	RBACL 統計情報の設定ステータスを表示し、すべての RBACL ポリシーの統計情報を一覧表示します。

cts role-based enforcement

VLAN または Virtual Routing and Forwarding（VRF; 仮想ルーティング/転送）インスタンスで Cisco TrustSec セキュリティ グループ アクセス コントロール リスト（SGACL）強制をイネーブルにするには、**cts role-based enforcement** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

cts role-based enforcement

no cts role-based enforcement

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション
VLAN コンフィギュレーション
VRF コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、デフォルト VRF で Cisco TrustSec SGACL 強制をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# cts role-based enforcement
```

次に、VLAN で Cisco TrustSec SGACL 強制をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# vlan 1
switch(config-vlan)# cts role-based enforcement
```

次に、非デフォルト VRF で Cisco TrustSec SGACL 強制をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# vrf context MyVRF
switch(config-vrf)# cts role-based enforcement
```

次に、Cisco TrustSec SGACL 強制をディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# no cts role-based enforcement
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts role-based enable	Cisco TrustSec SGACL ポリシー強制の設定を表示します。

cts role-based sgt

セキュリティ グループ アクセス コントロール リスト（SGACL）と Cisco TrustSec Security Group Tag（SGT; セキュリティ グループ タグ）のマッピングを手動で設定するには、**cts role-based sgt** コマンドを使用します。SGACL と SGT のマッピングを削除するには、このコマンドの **no** 形式を使用します。

cts role-based sgt {*sgt-value* | **any** | **unknown**} **dgt** {*dgt-value* | **unknown**} **access-list** *list-name*

no cts role-based sgt {*sgt-value* | **any** | **unknown**} **dgt** {*dgt-value* | **unknown**}

構文の説明

sgt-value	送信元 SGT の値。有効範囲は 0 ～ 65533 です。
any	任意の SGT を指定します。
unknown	未知の SGT を指定します。
dgt	宛先 SGT を指定します。
dgt-value	宛先 SGT の値。有効範囲は 0 ～ 65533 です。
access-list *list-name*	SGACL の名前を指定します。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

SGT のマッピングを設定する前に SGACL を設定する必要があります。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、SGACL の SGT マッピングを設定する例を示します。

```
switch# configure terminal
switch(config)# cts role-based sgt 3 dgt 10 access-list MySGACL
```

次に、SGACL の SGT マッピングを削除する例を示します。

```
switch# configure terminal
switch(config)# no cts role-based sgt 3 sgt 10
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts role-based policy	SGACL の Cisco TrustSec SGT マッピングを表示します。

cts role-based sgt-map

IP アドレスと Cisco TrustSec セキュリティ グループ タグ（SGT）のマッピングを手動で設定するには、**cts role-based sgt-map** コマンドを使用します。SGT を削除するには、このコマンドの **no** 形式を使用します。

cts role-based sgt-map *ipv4-address sgt-value*

no cts role-based sgt-map *ipv4-address*

構文の説明

ipv4-address	IPv4 アドレス。形式は、*A.B.C.D* です。
sgt-value	SGT 値。有効範囲は 0 ～ 65533 です。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション
VLAN コンフィギュレーション
VRF コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

Cisco TrustSec では、IPv4 アドレッシングだけを使用できます。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、Cisco TrustSec SGT のマッピングを設定する例を示します。

```
switch# configure terminal
switch(config)# cts role-based sgt-map 10.10.1.1 3
switch(config-rbacl)#
```

次に、Cisco TrustSec SGT のマッピングを削除する例を示します。

```
switch# configure terminal
switch(config)# no ccts role-based sgt-map 10.10.1.1
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts role-based sgt-map	Cisco TrustSec SGT のマッピングを表示します。

cts sgt

Cisco TrustSec セキュリティ グループ タグ（SGT）を設定するには、**cts sgt** コマンドを使用します。

cts sgt *tag*

構文の説明

tag	**0x***hhhh* 形式の 16 進値であるデバイスのローカル SGT。有効範囲は 0x0 ～ 0xffff です。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、デバイスの Cisco TrustSec SGT を設定する例を示します。

```
switch# configure terminal
switch(config)# cts sgt 0x3
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts environment-data	Cisco TrustSec 環境データを表示します。

cts sxp connection peer

Cisco TrustSec の SGT Exchange Protocol（SXP）ピア接続を設定するには、**cts sxp connection peer** コマンドを使用します。SXP 接続を削除するには、このコマンドの **no** 形式を使用します。

cts sxp connection peer *peer-ipv4-addr* [**source** *src-ipv4-addr*] **password** {**default** | **none** | **required** {*password* | **7** *encrypted-password*}} **mode** {**speaker | listener**} [**vrf** *vrf-name*]

no cts sxp connection peer *peer-ipv4-addr* [**vrf** *vrf-name*]

構文の説明

peer-ipv4-addr	ピア デバイスの IPv4 アドレス
source *src-ipv4-addr*	（任意）送信元デバイスの IPv4 アドレスを指定します。
password	SXP 認証に使用するパスワード オプションを指定します。
default	SXP がピア接続のデフォルト SXP パスワードを使用するように指定します。
none	SXP がパスワードを使用しないように指定します。
required	SXP がこのピア接続で使用する必要があるパスワードを指定します。
password	テキスト パスワードをクリアします。パスワードには英数字を使用します。大文字と小文字が区別され、最大長は 32 文字です。
7 *encrypted password*	暗号化パスワードを指定します。最大長は 32 文字です。
mode	ピア デバイスのモードを指定します。
speaker	ピアがスピーカとなるように指定します。
listener	ピアがリスナーとなるように指定します。
vrf *vrf-name*	（任意）ピアの VRF を指定します。

デフォルト

デバイスに設定されたデフォルト SXP パスワード
デバイスに設定されたデフォルト SXP 送信元 IPv4 アドレス
デフォルト VRF

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.1(3)	暗号化パスワードの使用を可能にするため、**7** オプションが追加されました。
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

Cisco TrustSec では、IPv4 アドレッシングだけを使用できます。

送信元 IPv4 アドレスを指定しない場合は、**cts sxp default source-ip** コマンドを使用してデフォルト SXP 送信元 IPv4 アドレスを設定する必要があります。

デフォルトをパスワード モードで指定する場合は、**cts sxp default password** コマンドを使用してデフォルト SXP パスワードを設定する必要があります。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、SXP ピア接続を設定する例を示します。

```
switch# configure terminal
switch(config)# cts sxp connection peer 10.10.1.1 source 10.10.2.2 password default mode
listener
```

次に、SXP ピア接続を削除する例を示します。

```
switch# configure terminal
switch(config)# no cts sxp connection peer 10.10.1.1
```

関連コマンド

コマンド	説明
cts sxp default password	デバイスのデフォルト SXP パスワードを設定します。
cts sxp default source-ip	デバイスのデフォルト SXP 送信元 IPv4 アドレスを設定します。
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts sxp connection	Cisco TrustSec SXP ピア接続情報を表示します。

cts sxp default password

デバイスのデフォルト SGT Exchange Protocol（SXP）パスワードを設定するには、**cts sxp default password** コマンドを使用します。デフォルトを削除するには、このコマンドの **no** 形式を使用します。

cts sxp default password {*password* | **7** *encrypted-password*}

no cts sxp default password

構文の説明

password	テキスト パスワードをクリアします。パスワードには英数字を使用します。大文字と小文字が区別され、最大長は 32 文字です。
7 *encrypted password*	暗号化パスワードを指定します。最大長は 32 文字です。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.1(3)	暗号化パスワードの使用を可能にするため、**7** オプションが追加されました。
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、デバイスのデフォルト SXP パスワードを設定する例を示します。

```
switch# configure terminal
switch(config)# cts sxp default password Cisco654
```

次に、デフォルト SXP パスワードを削除する例を示します。

```
switch# configure terminal
switch(config)# no cts sxp default password
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts sxp	Cisco TrustSec SXP 設定情報を表示します。

cts sxp default source-ip

デバイスのデフォルト SGT Exchange Protocol（SXP）送信元 IPv4 アドレスを設定するには、**cts sxp default source-ip** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

cts sxp default source-ip *ipv4-address*

no cts sxp default source-ip *ipv4-address*

構文の説明

ipv4-address	デバイスのデフォルト SXP IPv4 アドレス

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

Cisco TrustSec では、IPv4 アドレッシングだけを使用できます。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、デバイスのデフォルト SXP 送信元 IP アドレスを設定する例を示します。

```
switch# configure terminal
switch(config)# cts sxp default source-ip 10.10.3.3
```

次に、デフォルト SXP 送信元 IP アドレスを削除する例を示します。

```
switch# configure terminal
switch(config)# no cts sxp default source-ip
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts sxp	Cisco TrustSec SXP 設定情報を表示します。

cts sxp enable

デバイス上の SGT Exchange Protocol（SXP）ピアをイネーブルにするには、**cts sxp enable** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

cts sxp enable

no cts sxp enable

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、SXP をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# cts sxp enable
```

次に、SXP をディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# no cts sxp enable
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts sxp	Cisco TrustSec SXP 設定情報を表示します。

cts sxp reconcile-period

SGT Exchange Protocol（SXP）復帰期間タイマーを設定するには、**cts sxp reconcile-period** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

cts sxp reconcile-period *seconds*

no cts sxp reconcile-period

構文の説明

seconds	秒数。範囲は 0 ～ 64000 です。

デフォルト

60 秒（1 分）

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

ピアが SXP 接続を終了すると、内部ホールドダウン タイマーが開始されます。内部ホールドダウン タイマーが終了する前にピアが再接続すると、SXP 復帰期間タイマーが開始されます。SXP 復帰期間タイマーがアクティブな間、Cisco NX-OS ソフトウェアは前回の接続で学習した SGT マッピング エントリを保持し、無効なエントリを削除します。

（注） SXP 復帰期間を 0 秒に設定すると、タイマーがディセーブルになり、前回の接続のすべてのエントリが削除されます。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、SXP 復帰期間を設定する例を示します。

```
switch# configure terminal
switch(config)# cts sxp reconcile-period 120
```

次に、SXP 復帰期間をデフォルト値に戻す例を示します。

```
switch# configure terminal
switch(config)# no cts sxp reconcile-period
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts sxp connection	Cisco TrustSec SXP 設定情報を表示します。

cts sxp retry-period

SGT Exchange Protocol（SXP）リトライ期間タイマーを設定するには、**cts sxp retry-period** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

cts sxp retry-period *seconds*

no cts sxp retry-period

構文の説明

seconds	秒数。範囲は 0 ～ 64000 です。

デフォルト

120 秒（2 分）

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

SXP リトライ期間によって、Cisco NX-OS ソフトウェアが SXP 接続を再試行する頻度が決まります。SXP 接続が正常に確立されなかった場合、Cisco NX-OS ソフトウェアは SXP リトライ期間タイマーの終了後に、新たな接続の確立を試行します。

（注） SXP リトライ期間を 0 秒に設定すると、タイマーがディセーブルになり、再試行は実行されません。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、SXP リトライ期間を設定する例を示します。

```
switch# configure terminal
switch(config)# cts sxp retry-period 120
```

次に、SXP リトライ期間をデフォルト値に戻す例を示します。

```
switch# configure terminal
switch(config)# no cts sxp retry-period
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts sxp connection	Cisco TrustSec SXP ピア接続情報を表示します。