TrustSec コマンド

- address（CTS） （3 ページ）
- clear cts environment-data （5 ページ）
- clear cts policy-server statistics （6 ページ）
- content-type json （7 ページ）
- cts authorization list （8 ページ）
- cts change-password （10 ページ）
- cts credentials （11 ページ）
- cts environment-data enable （13 ページ）
- cts policy-server device-id （14 ページ）
- cts policy-server name （15 ページ）
- cts policy-server order random （16 ページ）
- cts policy-server username （17 ページ）
- cts refresh （19 ページ）
- cts rekey （21 ページ）
- cts role-based enforcement （22 ページ）
- cts role-based l2-vrf （24 ページ）
- cts role-based monitor （26 ページ）
- cts role-based permissions （28 ページ）
- cts role-based sgt-caching （30 ページ）
- cts role-based sgt-map （31 ページ）
- cts sxp connection peer （34 ページ）
- cts sxp default password （37 ページ）
- cts sxp default source-ip （39 ページ）
- cts sxp filter-enable （41 ページ）
- cts sxp filter-group （42 ページ）
- cts sxp filter-list （44 ページ）
- cts sxp log binding-changes （46 ページ）
- cts sxp reconciliation period （47 ページ）
- cts sxp retry period （48 ページ）

- debug cts environment-data （49 ページ）
- debug cts policy-server （51 ページ）
- port（CTS） （52 ページ）
- propagate sgt (cts manual) （53 ページ）
- retransmit（CTS） （55 ページ）
- sap mode-list (cts manual) （56 ページ）
- show cts credentials （58 ページ）
- show cts environment-data （59 ページ）
- show cts interface （60 ページ）
- show cts policy-server （63 ページ）
- show cts role-based counters （66 ページ）
- show cts role-based permissions （68 ページ）
- show cts server-list （70 ページ）
- show cts sxp （72 ページ）
- show platform hardware fed switch active fwd-asic resource tcam utilization （75 ページ）
- show platform hardware fed switch active sgacl resource usage （77 ページ）
- show platform software classification switch active F0 class-group-manager class-group client acl all （78 ページ）
- show platform software cts forwarding-manager switch active F0 port （79 ページ）
- show platform software cts forwarding-manager switch active F0 （83 ページ）
- show platform software cts forwarding-manager switch active F0 permissions （84 ページ）
- show platform software fed switch active acl counters hardware | inc SGACL （86 ページ）
- show platform software fed switch active acl usage （87 ページ）
- show platform software fed switch active ifm mappings （88 ページ）
- show platform software fed switch active ip route （92 ページ）
- show platform software fed switch active sgacl detail （94 ページ）
- show platform software fed switch active sgacl port （95 ページ）
- show platform software fed switch active sgacl vlan （97 ページ）
- show platform software status control-processor brief （98 ページ）
- show monitor capture <name> buffer （99 ページ）
- timeout（CTS） （100 ページ）
- tls server-trustpoint （101 ページ）

address（CTS）

Cisco TrustSec ポリシーサーバのアドレスを設定するには、ポリシーサーバ コンフィギュレーション モードで **address** コマンドを使用します。ポリシーサーバのアドレスを削除するには、このコマンドの **no** 形式を使用します。

address {**domain-name** *name* | **ipv4** *policy-server-address* | **ipv6** *policy-server-address*}
no address {**domain-name** | **ipv4** | **ipv6**}

構文の説明

domain-name *name*	ポリシーサーバのドメイン名を指定します。
ipv4 *policy-server-address*	ポリシーサーバの IP アドレスを指定します。
ipv6	ポリシーサーバの IPv6 アドレスを指定します。

コマンド デフォルト

ポリシーサーバのアドレスは設定されていません。

コマンド モード

ポリシーサーバ コンフィギュレーション（config-policy-server）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

使用上のガイドライン

ポリシーサーバ コンフィギュレーション モードを開始するには、ポリシーサーバ名を設定します。

例

次に、ポリシーサーバのドメイン名を設定する例を示します。

```
Device# enable
Device# configure terminal
Device(config)# policy-server name ise_server_2
Device(config-policy-server)# address domain-name ISE_domain
```

次に、ポリシーサーバの IP アドレスを設定する例を示します。

```
Device# enable
Device# configure terminal
Device(config)# cts policy-server name ise_server_2
Device(config-policy-server)# address ipv4 10.1.1.1
```

関連コマンド

コマンド	説明
cts policy-server name	ポリシーサーバの名前を設定し、ポリシーサーバ コンフィギュレーション モードを開始します。

clear cts environment-data

Cisco TrustSec の環境データをクリアするには、特権 EXEC モードで **clear cts environment-data** コマンドを使用します。

clear cts environment-data

このコマンドには引数またはキーワードはありません。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

例

次に、環境データをクリアする例を示します。

```
Device# enable
Device# clear cts environment-data
```

関連コマンド

コマンド	説明
cts environment-data enable	環境データのダウンロードを有効にします。
debug cts environment-data	Cisco TrustSec 環境データ操作のデバッグを有効にします。
show cts environment-data	Cisco TrustSec の環境データ情報を表示します。

clear cts policy-server statistics

Cisco TrustSec ポリシーサーバの統計情報をクリアするには、特権 EXEC モードで **clear cts policy-server statistics** コマンドを使用します。

clear cts policy-server statistics {**active** | **all**}

構文の説明

active	アクティブなすべてのポリシーサーバの統計情報をクリアします。
all	すべてのポリシーサーバの統計情報をクリアします。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

例

次に、すべてのポリシーサーバの統計情報をクリアする例を示します。

```
Device# enable
Device# clear cts policy-server statistics all
```

関連コマンド

コマンド	説明
cts policy-server name	Cisco TrustSec ポリシーサーバを設定し、ポリシーサーバ コンフィギュレーション モードを開始します。

content-type json

JavaScript Object Notation（JSON）をコンテンツタイプとして有効にするには、ポリシーサーバ コンフィギュレーション モードで **content-type json** コマンドを使用します。このコンテンツタイプを削除するには、このコマンドの **no** 形式を使用します。

content-type json
no content-type json

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

JSON コンテンツタイプが有効になっています。

コマンド モード

ポリシーサーバ コンフィギュレーション（config-policy-server）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

使用上のガイドライン

JSON は、Cisco Identity Services Engine（ISE）からセキュリティ グループ アクセス コントロール リスト（SGACL）および環境データをダウンロードするためのコンテンツタイプとして使用されます。

例

次に、JSON コンテンツタイプを有効にする例を示します。

```
Device# enable
Device# configure terminal
Device(config)# policy-server name ise_server_2
Device(config-policy-server)# content-type json
```

関連コマンド

コマンド	説明
cts policy-server name	ポリシーサーバの名前を設定し、ポリシーサーバ コンフィギュレーション モードを開始します。

cts authorization list

TrustSec シードデバイスで使用する認証、許可、およびアカウンティング（AAA）サーバのリストを指定するには、Cisco TrustSec シードデバイスでグローバル コンフィギュレーション モードで **cts authorization list** コマンドを使用します。認証中にリストの使用を停止するには、このコマンドの **no** 形式を使用します。

cts authorization list *server_list*

no cts authorization list *server_list*

構文の説明

server_list	Cisco TrustSec AAA サーバグループ。

コマンド 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（config）

サポートされるユーザロール

管理者（Administrator）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、シードデバイスだけです。非シードデバイスは、TrustSec 環境データのコンポーネントとして TrustSec オーセンティケータのピアからの TrustSec AAA サーバリストを取得します。

次の例は、TrustSec シードデバイスの AAA コンフィギュレーションを表示します。

```
Device# cts credentials id Device1 password Cisco123
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication dot1x default group radius
Device(config)# aaa authorization network MLIST group radius
Device(config)# cts authorization list MLIST
Device(config)# aaa accounting dot1x default start-stop group radius
Device(config)# radius-server host 10.20.3.1 auth-port 1812 acct-port 1813 pac key
AbCe1234
Device(config)# radius-server vsa send authentication
Device(config)# dot1x system-auth-control
Device(config)# exit
```

関連コマンド

コマンド	説明
show cts server-list	RADIUS サーバ設定を表示します。

cts change-password

ローカルデバイスと認証サーバの間でパスワードを変更するには、**cts change-password** 特権 EXEC コマンドを使用します。

cts change-password server *ipv4_address udp_port* {**a-id** *hex_string* | **key** *radius_key* }[**source** *interface_list*]

構文の説明

server	認証サーバを指定します。
ipv4_address	認証サーバの IP アドレス。
udp_port	認証サーバの UDP ポート。
a-id *hex_string*	ACS サーバの識別文字列を指定します。
key	プロビジョニングに使用する RADIUS キーを指定します。
source *interface_list*	（任意）表示されるリストに従って、要求パケットの送信元アドレスのインターフェイスタイプとその識別パラメータを指定します。

コマンド 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

管理者（Administrator）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン

cts change-password コマンドにより、管理者は認証サーバを再設定しなくても、ローカルデバイスと Cisco Secure ACS 認証サーバ間で使用されるパスワードを変更することができます。

次に、スイッチと Cisco Secure ACS の間で Cisco TrustSec パスワードを変更する例を示します。

```
Device# cts change-password server 192.168.2.2 88 a-id ffef
```

cts credentials

ネットワークデバイスの TrustSec ID およびパスワードを指定するには、特権 EXEC モードで **cts credentials** コマンドを使用します。ログイン情報を削除するには、**clear cts credentials** コマンドを使用します。

cts credentials id *cts_id* **password** *cts_pwd*

構文の説明

credentials id *cts_id*	EAP-FAST を使用して他の Cisco TrustSec デバイスで認証するときにこのデバイスが使用する Cisco TrustSec デバイス ID を指定します。*cts-id* 変数は、最大 32 文字で大文字と小文字を区別します。
password *cts_pwd*	EAP-FAST を使用して他の Cisco TrustSec デバイスで認証するときにこのデバイスが使用するパスワードを指定します。

コマンド 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

管理者（Administrator）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン

重要 **cts credentials** コマンドは、特権 EXEC モードでのみ設定する必要があります。グローバル コンフィギュレーション（config）モードを使用して **cts credentials** コマンドを設定することはできません。

cts credentials コマンドは、EAP-FAST を使用して他の Cisco TrustSec デバイスで認証するときにこのデバイスが使用する Cisco TrustSec デバイス ID およびパスワードを指定します。Cisco TrustSec のログイン情報はスタートアップ コンフィギュレーションではなくキーストアに保存されているため、Cisco TrustSec のログイン情報の状態取得は不揮発性生成（NVGEN）プロセスでは実行されません。デバイスは、Cisco Secure Access Control Server（ACS）から Cisco TrustSec アイデンティティを割り当てられるか、ACS から要求されたときに新しいパスワードを自動生成するようにできます。これらのログイン情報は、キーストアで保存され、実行コンフィギュレーションを保存する必要性がなくなります。Cisco TrustSec デバイス ID を表示するには、**show cts credentials** コマンドを使用します。保存されたパスワードは表示されません。

デバイス ID またはパスワードを変更するには、コマンドを再入力します。キーストアをクリアするには、**clear cts credentials** コマンドを使用します。

（注） Cisco TrustSec デバイス ID が変更された場合、Protected Access Credential（PAC）は古いデバイス ID に関連付けられており、新しいアイデンティティに対しては有効でないため、すべての PAC はキーストアから消去されます。

次に、Cisco TrustSec デバイス ID およびパスワードを設定する例を示します。

```
Device# cts credentials id cts1 password password1
CTS device ID and password have been inserted in the local keystore. Please make sure
that
the same ID and password are configured in the server database.
```

次に、Cisco TrustSec デバイス ID を cts_new、パスワードを password123 に変更する例を示します。

```
Device# cts credentials id cts_new pacssword password123
A different device ID is being configured.
This may disrupt connectivity on your CTS links.
Are you sure you want to change the Device ID? [confirm] y

TS device ID and password have been inserted in the local keystore. Please make sure
that
the same ID and password are configured in the server database.
```

次に、Cisco TrustSec デバイス ID およびパスワードの状態を表示する例を示します。

```
Device# show cts credentials

CTS password is defined in keystore, device-id = cts_new
```

関連コマンド

コマンド	説明
clear cts credentials	Cisco TrustSec デバイス ID とパスワードをクリアします。
show cts credentials	現在の Cisco TrustSec デバイス ID およびパスワードの状態を表示します。
show cts keystore	ハードウェアおよびソフトウェアのキーストアの内容を表示します。

cts environment-data enable

REST アプリケーション プログラミング インターフェイス（API）による環境データのダウンロードを有効にするには、グローバル コンフィギュレーション モードで **cts environment-data enable** コマンドを使用します。環境データのダウンロードを無効にするには、このコマンドの **no** 形式を使用します。

cts environment-data enable
no cts environment-data enable

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

環境データのダウンロードは有効になっていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

使用上のガイドライン

cts environment-data enable コマンドと **cts authorization list** コマンドを一緒に使用することはできません。**cts authorization list** コマンドでは、RADIUS による環境データのダウンロードが有効になります。

cts authorization list コマンドを使用して RADIUS ベースの設定を試行したときに **cts environment-data enable** コマンドがすでに設定されていると、コンソールに次のエラーメッセージが表示されます。

```
Error: 'cts policy-server or cts environment-data' related configs are enabled.
Disable http-based configs, to enable 'cts authorization'
```

例

次に、環境データのダウンロードを有効にする例を示します。

```
Device# enable
Device# configure terminal
Device(config)# cts environment-data enable
```

関連コマンド

コマンド	説明
clear cts environment-data	環境データをクリアします。
debug cts environment-data	Cisco TrustSec 環境データ操作のデバッグを有効にします。
show cts environment-data	Cisco TrustSec の環境データ情報を表示します。

cts policy-server device-id

ポリシーサーバのデバイス ID を設定するには、グローバル コンフィギュレーション モードで **cts policy-server device-id** コマンドを使用します。ポリシーサーバのデバイス ID を削除するには、このコマンドの **no** 形式を使用します。

cts policy-server device-id *device-ID*
no cts policy-server device-id *device-ID*

構文の説明

device-ID	Cisco TrustSec デバイスのデバイス ID。

コマンド デフォルト

デバイス ID は設定されていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

使用上のガイドライン

デバイス ID は、Cisco Identity Services Engine（ISE）でネットワーク アクセス デバイス（NAD）を追加するために使用したものと同じである必要があります。この ID は、Cisco ISE に環境データ要求を送信するために使用されます。

例

次に、ポリシーサーバのデバイス ID を設定する例を示します。

```
Device# enable
Device# configure terminal
Device(config)# cts policy-server device-id server1
```

関連コマンド

コマンド	説明
cts policy-server name	Cisco TrustSec ポリシーサーバを設定し、ポリシーサーバ コンフィギュレーション モードを開始します。

cts policy-server name

Cisco TrustSec ポリシーサーバを設定し、ポリシーサーバ コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **cts policy-server name** コマンドを使用します。ポリシーサーバを削除するには、このコマンドの **no** 形式を使用します。

cts policy-server name *server-name*
no cts policy-server name *server-name*

構文の説明

server-name	ポリシーサーバ名。

コマンド デフォルト

ポリシーサーバは設定されていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

使用上のガイドライン

ポリシーサーバ名にはすべての文字を使用できます。ポリシーサーバ名を設定すると、コンフィギュレーション モードがポリシーサーバ コンフィギュレーションに切り替わります。このモードで、ポリシーサーバのその他の詳細を設定できます。

例

次に、ポリシーサーバ名を設定する例を示します。

```
Device# enable
Device# configure terminal
Device(config)# cts policy-server name ISE1
Device(config-policy-server)#
```

関連コマンド

コマンド	説明
show cts policy-server	ポリシーサーバ情報を表示します。

cts policy-server order random

サーバ選択ロジックをランダム方式に変更するには、グローバル コンフィギュレーション モードで **cts policy-server order random** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

cts policy-server order random
no cts policy-server order random

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトは順序どおりの選択です。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

使用上のガイドライン

デバイスで複数の HTTP ポリシーサーバが設定されている場合、常に最初に設定されたサーバが選択されると、1 つの Cisco Identity Services Engine（ISE）インスタンスが過負荷になる可能性があります。この状況を回避するには、各デバイスでランダムにサーバを選択します。ランダムな番号がデバイスによって生成され、この番号に基づいてサーバが選択されます。デバイスごとにランダムな番号を生成するには、デバイスの一意のボード ID と Cisco TrustSec プロセス ID を使用して乱数ジェネレータを初期化します。

サーバ選択ロジックをランダム方式に変更するには、**cts policy-server order random** コマンドを使用します。このコマンドが選択されていない場合、デフォルトの順序どおりの選択が使用されます。

順序どおりの選択では、サーバが設定された順序（パブリックサーバリスト）またはダウンロードされた順序（プライベートサーバリスト）で選択されます。サーバが選択されると、そのサーバがデッド状態としてマークされるまで使用され、その後にリストの次のサーバが選択されます。

例

次に、サーバ選択ロジックを変更する例を示します。

```
Device# enable
Device# configure terminal
Device(config)# cts policy-server order random
```

関連コマンド

コマンド	説明
cts policy-server name	Cisco TrustSec ポリシーサーバを設定し、ポリシーサーバ コンフィギュレーション モードを開始します。

cts policy-server username

ポリシーサーバのユーザ名を設定するには、グローバル コンフィギュレーション モードで **cts policy-server username** コマンドを使用します。ポリシーサーバのユーザ名を削除するには、このコマンドの **no** 形式を使用します。

cts policy-server username *username***password** {**0** | **6** | **7** *password* }*password*
no cts policy-server username

構文の説明

username	REST アプリケーション プログラミング インターフェイス（API）にアクセスするためのユーザ名。
password	ユーザの認証で使用するパスワードを指定します。
0	暗号化されていないパスワードを指定します。
6	暗号化パスワードを指定します。
7	非表示のパスワードを指定します。
password	暗号化または非暗号化パスワード。

コマンド デフォルト

ユーザログイン情報は設定されていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

使用上のガイドライン

デバイスで設定する前に、Cisco Identity Services Engine（ISE）でユーザ名とパスワードを REST API アクセス用のログイン情報として設定しておく必要があります。詳細については、「Cisco TrustSec Policies Configuration」の章の「TrustSec HTTP Servers」セクションを参照してください。

例

次に、ポリシーサーバのログイン情報を設定する例を示します。

```
Device# enable
Device# configure terminal
```

```
Device(config)# policy-server username user1 password 0 ise-password
```

関連コマンド

コマンド	説明
cts policy-server name	ポリシーサーバの名前を設定し、ポリシーサーバ コンフィギュレーション モードを開始します。

cts refresh

すべてまたは特定の Cisco TrustSec ピアの TrustSec ピア認証ポリシーをリフレッシュするか、認証サーバによりデバイスにダウンロードされた SGACL ポリシーをリフレッシュするには、特権 EXEC モードで **cts refresh** コマンドを使用します。

cts refresh {**peer** [*peer_id*] | **sgt** [*sgt_number* | **default** | **unknown**]}

構文の説明

environment-data	環境データをリフレッシュします。
peer *Peer-ID*	（任意）peer-idが指定される場合、指定されたピア接続に関連するポリシーだけがリフレッシュされます。
sgt *sgt_number*	（任意）認証サーバからのSGACLポリシーの即時リフレッシュを実行します。 SGT 番号が指定されている場合、その SGT に関連するポリシーだけがリフレッシュされます。
default	（任意）デフォルトの SGACL ポリシーをリフレッシュします。
unknown	（任意）未知の SGACL ポリシーをリフレッシュします。

コマンド 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

管理者（Administrator）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン

すべての TrustSec ピアのピア認証ポリシーをリフレッシュするには、ピア ID を指定しないで **cts policy refresh** を入力します。

ピア認可ポリシーはEAP-FAST NDAC 認証の成功の最後に Cisco ACS から最初にダウンロードされます。Cisco ACS はピア認証ポリシーを更新するように設定されていますが、**cts policy refresh** コマンドにより、Cisco ACS タイマーが期限切れになる前にポリシーの即時更新を強制できます。このコマンドは、セキュリティ グループ タグ（SGT）を適用でき、セキュリティ グループ アクセス コントロール リスト（SGACL）を強制できる TrustSec デバイスだけに関連します。

次に、すべてのピアの TrustSec ピア認証ポリシーをリフレッシュする例を示します。

```
Device# cts policy refresh
Policy refresh in progress
```

次に、すべてのピアの TrustSec ピア認証ポリシーを表示する出力例を示します。

```
VSS-1# show cts policy peer

CTS Peer Policy
===============
device-id of the peer that this local device is connected to
Peer name: VSS-2T-1
Peer SGT: 1-02
Trusted Peer: TRUE
Peer Policy Lifetime = 120 secs
Peer Last update time = 12:19:09 UTC Wed Nov 18 2009
Policy expires in 0:00:01:51 (dd:hr:mm:sec)
Policy refreshes in 0:00:01:51 (dd:hr:mm:sec)
Cache data applied = NONE
```

関連コマンド

コマンド	説明
clear cts policy	Cisco TrustSec ポリシーをすべてクリアするか、ピア ID または SGT によりクリアします。
show cts policy peer	すべてまたは特定の TrustSec ピアのピア認可ポリシーが表示されます。

cts rekey

セキュリティ アソシエーション プロトコル（SAP）で使用するペアワイズマスターキーを再生成するには、**cts rekey** 特権 EXEC コマンドを使用します。

cts rekey interface type *slot/port*

構文の説明

interface type *slot/port*	SAP キーを再生成する Cisco TrustSec インターフェイスを指定します。

コマンド 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

管理者（Administrator）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン

SAP のペアワイズマスターキー（PMK）のリフレッシュは通常、ネットワークイベントおよび dot1X 認証に関連する設定不可能な内部タイマーの組み合わせによりトリガーされ、自動的に行われます。暗号キーを手動で更新する機能は、多くの場合、ネットワーク アドミニストレーションのセキュリティ要件の一部です。手動で PMK のリフレッシュを強制するには、**cts rekey** コマンドを使用します。

TrustSec は、dot1X 認証でスイッチ間のリンク間暗号化を作成する必要のない手動コンフィギュレーション モードをサポートします。この場合、PMK は、**sap pmk** Cisco TrustSec 手動インターフェイス コンフィギュレーション コマンドを使用してリンクの両端のデバイスで手動で設定されます。

次に、指定したインターフェイス上で PMK を再生成する例を示します。

```
Device# cts rekey interface gigabitEthernet 2/1
```

関連コマンド

コマンド	説明
sap mode-list (cts manual)	手動モードの Cisco TrustSec SAP を設定します。

cts role-based enforcement

Cisco TrustSec を使用したロールベースのアクセス制御をグローバルおよび特定のレイヤ 3 インターフェイスで有効にするには、グローバル コンフィギュレーション モードおよびインターフェイス コンフィギュレーション モードで **cts role-based enforcement** コマンドをそれぞれ使用します。ロールベースのアクセス制御のインターフェイスレベルでの適用を無効にするには、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

このコマンドにはキーワードまたは引数はありません。

コマンド デフォルト

ロールベースのアクセス制御のインターフェイスレベルでの適用はグローバルに無効になっています。

コマンド モード

グローバル コンフィギュレーション（config）

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン

グローバル コンフィギュレーション モードで **cts role-based enforcement** コマンドを使用すると、ロールベースのアクセス制御がグローバルに有効になります。ロールベースのアクセス制御がグローバルに有効になると、デバイスのすべてのレイヤ3インターフェイスで自動的に有効になります。特定のレイヤ3インターフェイスでロールベースのアクセス制御を無効にするには、インターフェイス コンフィギュレーション モードでこのコマンドの **no** 形式を使用します。インターフェイス コンフィギュレーション モードで **cts role-based enforcement** コマンドを使用すると、特定のレイヤ3インターフェイスでロールベースのアクセス制御の適用が可能になります。

属性ベースのアクセス制御リストでは、ネットワークデバイスの Cisco TrustSec アクセス制御を整理して管理します。セキュリティ グループ アクセス コントロール リスト（SGACL）は、セキュリティグループタグ（SGT）の値に基づいてアクセスをフィルタ処理するためのレイヤ 3/4 アクセス制御リストです。通常、フィルタ処理は Cisco TrustSec ドメインの出力ポートで実行されます。ロールベースのアクセス制御リスト（RBACL）と SGACL という用語は同じ意味で使用され、どちらも属性ベースのアクセス制御（ABAC）ポリシーモデルで使用されるトポロジに依存しない ACL を示します。

次に、ギガビットイーサネットインターフェイスでロールベースのアクセス制御を有効にする例を示します。

```
Device> enable
```

```
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/3
Device(config-if)# cts role-based enforcement
Device(config-if)# end
```

cts role-based l2-vrf

レイヤ 2 VLAN の Virtual Routing and Forwarding（VRF）インスタンスを選択するには、グローバル コンフィギュレーション モードで **cts role-based l2-vrf** コマンドを使用します。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 role-based l2-vrf *vrf-name* **vlan-list** {**all** *vlan-ID*} [**,**] [**-**]
no cts role-based l2-vrf *vrf-name* **vlan-list** {**all** *vlan-ID*} [**,**] [**-**]

構文の説明

vrf-name	VRF インスタンスの名前。
vlan-list	VRF インスタンスに割り当てられる VLAN のリストを指定します。
all	すべての VLAN を指定します。
vlan-ID	VLAN ID。有効な値は 1 ～ 4094 です。
,	（任意）別の VLAN をカンマで区切って指定します。
-	（任意）VLAN の範囲をハイフンで区切って指定します。

コマンド デフォルト

VRF インスタンスは選択されていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン

vlan-list 引数には単一の VLAN ID、カンマで区切られた VLAN ID のリスト、またはハイフンで区切られた VLAN ID の範囲を指定できます。

all キーワードは、ネットワークデバイスによってサポートされている VLAN の全範囲と同等です。**all** キーワードは、不揮発性生成（NVGEN）プロセスで保持されません。

cts role-based l2-vrf コマンドが同じ VRF に複数回実行される場合、入力される連続した各コマンドは、指定された VRF に VLAN ID を追加します。

cts role-based l2-vrf コマンドで設定された VRF 割り当ては、VLAN がレイヤ 2 VLAN として維持されている間はアクティブです。VRF の割り当てがアクティブな間に、学習した IP-SGT バインディングも VRF と IP プロトコルバージョンに関連付けられた転送情報ベース（FIB）テーブルに追加されます。VLAN のスイッチ仮想インターフェイス（SVI）がアクティブになると、VRF から VLAN への割り当てが非アクティブになり、VLAN で学習されたすべてのバインディングが SVI の VRF に関連付けられた FIB テーブルに移動されます。

SVI インターフェイスを設定するには **interface vlan** コマンドを使用し、VRF インスタンスをインターフェイスに関連付けるには **vrf forwarding** コマンドを使用します。

VRF から VLAN への割り当ては、割り当てが非アクティブになっても保持されます。SVI が削除された、または SVI の IP アドレスの変更された場合に再アクティブ化されます。再アクティブ化された場合、IP-SGT バインディングは、SVI の FIB に関連付けられた FIB テーブルから、**cts role-based l2-vrf** コマンドによって割り当てられた VRF に関連付けられた FIB テーブルに戻されます。

次に、VRF インスタンスに割り当てられる VLAN のリストを選択する例を示します。

```
Device(config)# cts role-based l2-vrf vrf1 vlan-list 20
```

次に、SVI インターフェイスを設定し、VRF インスタンスを関連付ける例を示します。

```
Device(config)# interface vlan 101
Device(config-if)# vrf forwarding vrf1
```

関連コマンド

コマンド	説明
interface vlan	VLAN インターフェイスを設定します。
vrf forwarding	VRF インスタンスまたは仮想ネットワークをインターフェイスまたはサブインターフェイスに関連付けます。
show cts role-based permissions	SGACL の権限リストを表示します。

cts role-based monitor

ロールベース（セキュリティグループ）アクセスリストモニタリングを有効にするには、グローバル コンフィギュレーション モードで **cts role-based monitor** コマンドを使用します。ロールベース アクセス リスト モニタリ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 monitor {**all** | **permissions** {**default** [**ipv4** | **ipv6**] | **from** {*sgt* | **unknown**} **to** {*sgt* | **unknown**} [**ipv4** | **ipv6**]}}
no cts role-based monitor {**all** | **permissions** {**default** [**ipv4** | **ipv6**] | **from** {*sgt* | **unknown**} **to** {*sgt* | **unknown**} [**ipv4** | **ipv6**]}}

構文の説明

all	すべての宛先タグへのすべての送信元タグの権限をモニタします。
permissions	1 つの送信元タグから 1 つの宛先タグへの権限をモニタします。
default	デフォルトの権限リストをモニタします。
ipv4	（任意）IPv4 プロトコルを指定します。
ipv6	（任意）IPv6 プロトコルを指定します。
from	フィルタリングされるトラフィックの送信元グループタグを指定します。
sgt	セキュリティグループタグ（SGT）有効値は 2 ～ 65519 です。
unknown	未知の送信元または宛先グループタグ（DST）を指定します。

コマンド デフォルト

ロールベース アクセス コントロール モニタリングは有効になっていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン

グローバルモニタモードを有効にするには、**cts role-based monitor all** コマンドを使用します。**cts role-based monitor all** コマンドが設定されている場合、**show cts role-based permissions** コマンドの出力には、設定されているすべてのポリシーのモニタモードが true と表示されます。

次に、送信元タグから宛先タグへの SGACL モニタを設定する例を示します。

```
Device(config)# cts role-based monitor permissions from 10 to 11
```

関連コマンド

コマンド	説明
show cts role-based permissions	SGACL の権限リストを表示します。

cts role-based permissions

1 つの送信元グループから 1 つの宛先グループへの権限を有効にするには、グローバル コンフィギュレーション モードで **cts role-based permissions** コマンドを使用します。権限を削除するには、このコマンドの **no** 形式を使用します。

cts role-based permissions {**default** | **from** {*sgt* | **unknown**}**to** {*sgt* | **unknown**}} {*rbacl-name* | **ipv4** | **ipv6**}
no cts role-based permissions {**default** | **from** {*sgt* | **unknown**}**to** {*sgt* | **unknown**}} {*rbacl-name* | **ipv4** | **ipv6**}

構文の説明

default	デフォルトの権限リストを指定します。セキュリティ グループ アクセス コントロール リスト（SGACL）権限が静的または動的に設定されていないすべてのセル（SGT ペア）は、デフォルトのカテゴリに属します。
from	フィルタリングされるトラフィックの送信元グループ タグを指定します。
sgt	セキュリティグループタグ（SGT）有効値は 2 ～ 65519 です。
unknown	未知の送信元または宛先グループタグを指定します。
rbacl-name	ロールベース アクセス コントロール リスト（RBACL）または SGACL の名前。この設定では最大 16 の SGACL を指定できます。
ipv4	IPv4 プロトコルを指定します。
ipv6	IPv6 プロトコルを指定します。

コマンド デフォルト

1 つの送信元グループから 1 つの宛先グループへの権限は有効になっていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン

特定の送信元グループタグ（SGT）、宛先グループタグ（DGT）ペアの SGACL のリストを定義したり、置き換えたり、削除したりするには、**cts role-based permissions** コマンドを使用します。このポリシーは、同じ DGT または SGT に対するダイナミックなポリシーがないかぎり有効です。

cts role-based permissions default コマンドでは、同じ DGT に対するダイナミックなポリシーがないかぎり、デフォルトポリシーの SGACL のリストを定義したり、置き換えたり、削除したりすることができます。

次に、宛先グループの権限を有効にする例を示します。

```
Device(config)# cts role-based permissions from 6 to 6 mon_2
```

関連コマンド

コマンド	説明
show cts role-based permissions	SGACL の権限リストを表示します。

cts role-based sgt-caching

セキュリティグループタグ（SGT）キャッシングをグローバルに有効にするには、グローバルコンフィギュレーションモードで**cts role-based sgt-caching** コマンドを使用します。SGT キャッシ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-caching [**vlan-list** {*vlan-id* | **all**}]
no cts role-based sgt-caching [**vlan-list** {*vlan-id* | **all**}]

構文の説明

vlan-list *vlan-id*	（任意）VLAN ID を指定します。各 VLAN ID はカンマで区切られ、ID の範囲はハイフンで指定されます。有効な値は1 ～ 4094 です。
all	（任意）すべての VLAN を選択します。

コマンド デフォルト

SGT キャッシングは設定されていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン

VLAN で SGT キャッシングを有効にするには、**cts role-based sgt-caching** コマンドと **cts role-based sgt-caching vlan-list** コマンドの両方を設定する必要があります。

例

次に、VLAN で SGT キャッシングを有効にする例を示します。

```
Device# configure terminal
Device(config)# cts role-based sgt-caching
Device(config)# cts role-based sgt-caching vlan-list 4
```

cts role-based sgt-map

ホストまたは VRF のいずれかで送信元 IP アドレスをセキュリティグループタグ（SGT）に手動でマッピングするには、グローバル コンフィギュレーション モードで **cts role-based sgt-map** コマンドを使用します。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-map
{*ipv4_netaddress* | *ipv6_netaddress* | *ipv4_netaddress/prefix* | *ipv6_netaddress/prefix*} **sgt** *sgt-number*
cts role-based sgt-map host {*ipv4_hostaddress* | *ipv6_hostaddress*} **sgt** *sgt-number*
cts role-based sgt-map vlan-list [*vlan_ids* | **all**] **sgt** *sgt-number*
cts role-based sgt-map vrf *instance_name*
{*ipv4_netaddress* | *ipv6_netaddress* | *ipv4_netaddress/prefix* | *ipv6_netaddress/prefix* | **host**
{*ipv4_hostaddress* | *ipv6_hostaddress*}} **sgt** *sgt-number*
no cts role-based sgt-map

構文の説明

ipv4_netaddress | **ipv6_netaddress**	SGT に関連付けるネットワークを指定します。IPv4 アドレスをドット付き 10 進数表記で、IPv6 をコロン 16 進数表記で入力します。
ipv4_netaddress/prefix | **ipv6_netaddress/prefix**	指定したサブネットアドレス（IPv4 または IPv6）のすべてのホストに SGT をマッピングします。IPv4 はドット付き 10 進数 CIDR 表記で、IPv6 はコロン 16 進数表記で指定されます。
host {*ipv4_hostaddress* | *ipv6_hostaddress*}	指定したホスト IP アドレスを SGT とバインドします。IPv4 アドレスをドット付き 10 進数表記で、IPv6 をコロン 16 進数表記で入力します。
vlan-list {*vlan_ids* | **all**}	VLAN ID を指定します。 • （任意）*vlan_ids*：各 VLAN ID はカンマで区切られ、ID の範囲はハイフンで指定されます。 • （任意）**all**：すべての VLAN ID を指定します。
vrf *instance_name*	以前デバイスで作成した VRF インスタンスを指定します。
sgt *sgt-number*	SGT 番号（0 ～ 65,535）を指定します。

コマンド 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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン

自動的に SGT を送信元 IP アドレスにマッピングするための、Cisco Identity Services Engine、Cisco Secure ACS、ダイナミックアドレス解決プロトコル（ARP）インスペクション、動的ホスト制御プロトコル（DHCP）スヌーピング、ホストトラッキングが使用できない場合、**cts role-based sgt-map** コマンドを使用して SGT を次の内容にマッピングできます。

- 単一ホストの IPv4 または IPv6 アドレス
- IPv4 または IPv6 ネットワークまたはサブネットワーク上のすべてのホスト
- VRF
- 単一または複数の VLAN

cts role-based sgt-map コマンドは、指定されたネットワークアドレス範囲内のパケットに、指定された SGT をバインドします。

SXP は指定されたネットワークまたはサブネットワーク内のすべての可能な個別 IP-SGT バインディングの包括的な拡張をエクスポートします。IPv6 バインディングとサブネット バインディングは SXP バージョン 2 以降の SXP リスナー ピアだけにエクスポートされます。拡張には、個別に認識されたホストバインディングや、ネストされたサブネットバインディングに対して SXP から設定または学習されたホストバインディングは含まれません。

cts role-based sgt-map host コマンドは、IP 送信元アドレスが指定ホストアドレスで一致した場合に、この着信パケットに指定 SGT をバインドします。この IP-SGT バインディングは優先順位が最も低く、他の送信元から動的に検出されたその他のバインディング（SXP またはローカルで認証済みホストなど）が存在する場合は無視されます。バインディングは、SGT インポジションおよび SGACL 強制用にデバイス上でローカルに使用されます。このバインディングが指定したホスト IP アドレスに認識される唯一のバインディングである場合、これが SXP ピアにエクスポートされます。

vrf キーワードは、以前に vrf definition グローバル コンフィギュレーション コマンドで定義された仮想ルーティングおよびフォワーディングテーブルを指定します。**cts role-based sgt-map vrf** グローバル コンフィギュレーション コマンドで指定された IP-SGT バインディングは、指定された VRF と、入力された IP アドレスのタイプによって示される IP プロトコルのバージョンに関連付けられた IP-SGT のテーブルに入力されます。

cts role-based sgt-map vlan-list コマンドは、SGT を指定された VLAN または VLAN のセットにバインドします。キーワード **all** は、デバイスでサポートされている VLAN の全範囲と同じで、不揮発性生成（NVGEN）プロセスで保持されません。指定 SGT は指定した VLAN のいずれかで受信した着信パケットにバインドされます。システムでは、DHCP/ARP スヌーピング（別名 IP デバイストラッキング）などの検出方式を使用して、このコマンドによってマッピングされた VLAN のいずれかでアクティブなホストを検出します。また、各 VLAN の SVI に関連付けられたサブネットを指定された SGT にマッピングすることもできます。SXP は、バインディングのタイプに応じて、結果のバインディングをエクスポートします。

例

次に、送信元 IP アドレスを SGT に手動でマッピングする例を示します。

```
Device(config)# cts role-based sgt-map 10.10.1.1 sgt 77
```

次の例では、デバイスでホスト IP アドレス 10.1.2.1 を SGT 3 にバインドし、10.1.2.2 を SGT 4 にバインドしています。これらのバインディングは、SXP によって SGACL 強制のデバイスに転送されます。

```
Device(config)# cts role-based sgt-map host 10.1.2.1 sgt 3
Device(config)# cts role-based sgt-map host 10.1.2.2 sgt 4
```

関連コマンド

コマンド	説明
show cts role-based sgt-map	ロールベースのアクセス制御の情報を表示します。

cts sxp connection peer

Cisco TrustSec セキュリティグループタグ交換プロトコルのピアの IP アドレスを入力し、ピア接続にパスワードを使用するかどうかを指定し、リスナーまたはスピーカーデバイスのグローバルなホールド時間を指定し、接続が双方向であるかどうかを指定するには、グローバル コンフィギュレーション モードで **cts sxp connection peer** コマンドを使用します。これらのピア接続の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 sxp connection peer *ipv4-address* {**source** | **password**} {**default** | **none**} **mode** {**local** | **peer**} [[[**listener** | **speaker**] [**hold-time** *minimum-time maximum-time* | **vrf** *vrf-name*]] | **both** [**vrf** *vrf-name*]]
cts sxp connection peer *ipv4-address* {**source** | **password**} {**default** | **none**} **mode** {**local** | **peer**} [[[**listener** | **speaker**] [**hold-time** *minimum-time maximum-time* | **vrf** *vrf-name*]] | **both** [**vrf** *vrf-name*]]

構文の説明

ipv4-address	SXP ピアの IPv4 アドレス。
source	送信元の IPv4 アドレスを指定します。
password	ピア接続に SXP パスワードを使用するように指定します。
default	デフォルトの SXP パスワードを使用するように指定します。
none	パスワードを使用しないように指定します。
mode	ローカルまたはピアのいずれかの SXP 接続モードを指定します。
local	SXP 接続モードでローカルデバイスを参照するように指定します。
peer	SXP 接続モードでピアデバイスを参照するように指定します。
listener	（任意）デバイスを接続のリスナーとして指定します。
speaker	（任意）デバイスを接続のスピーカーとして指定します。
hold-time *minimum-time maximum-time*	（任意）デバイスのホールド時間を秒単位で指定します。最小時間と最大時間の範囲は 0 ～ 65535 です。 *maximum-time* の値は、キーワード **peer speaker** および **local listener** を使用する場合のみ必要です。それ以外の場合は、*minimum-time* の値のみが必要です。 （注） 最小時間と最大時間の両方が必要な場合、*maximum-time* の値を *minimum-time* の値以上にする必要があります。
vrf *vrf-name*	（任意）ピアに対する Virtual Routing and Forwarding（VRF）インスタンス名を指定します。

both	（任意）デバイスを双方向 SXP 接続のスピーカーとリスナーの両方として指定します。

コマンド デフォルト

CTS-SXP ピア IP アドレスは設定されておらず、ピア接続に CTS-SXP ピアパスワードは使用されません。

CTS-SXP 接続パスワードのデフォルトの設定は **none** です。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン

ピアへの CTS-SXP 接続が **cts sxp connection peer** コマンドを使用して設定された場合、接続モードだけを変更できます。**vrf** キーワードはオプションです。VRF 名が指定されていない、または VRF 名が **default** キーワードで指定されている場合、接続はデフォルトルーティングまたはフォワーディングドメインで設定されます。

hold-time *maximum-period* の値は、キーワード **peer speaker** および **local listener** を使用する場合のみ必要です。それ以外の場合は、**hold-time** *minimum-period* の値のみが必要です。

（注） *maximum-period* 値は、*minimum-period* 値よりも大きいか等しくする必要があります。

双方向 SXP 接続を設定するには、**both** キーワードを使用します。双方向 SXP の設定をサポートすることで、ピアはスピーカーとリスナーのどちらとしても動作し、単一の接続を使用する双方向の SXP バインドを伝播できるようになります。

例

次に、CTS-SXP をイネーブルにし、Device_A（スピーカー）で Device_B（リスナー）への SXP ピア接続を設定する例を示します。

```
Device_A> enable
Device_A# configure terminal
Device_A#(config)# cts sxp enable
Device_A#(config)# cts sxp default password Cisco123
Device_A#(config)# cts sxp default source-ip 10.10.1.1
Device_A#(config)# cts sxp connection peer 10.20.2.2 password default mode local speaker
```

次に、Device_B（リスナー）で Device_A（スピーカー）への CTS-SXP ピア接続を設定する例を示します。

```
Device_B> enable
Device_B# configure terminal
Device_B(config)# cts sxp enable
Device_B(config)# cts sxp default password Cisco123
```

```
Device_B(config)# cts sxp default source-ip 10.20.2.2
Device_B(config)# cts sxp connection peer 10.10.1.1 password default mode local listener
```

SXP 接続のピアと送信元の両方の IP アドレスを設定することもできます。**cts sxp connection** コマンドで送信元 IP アドレスを指定すると、デフォルト値が上書きされます。

```
Device_A(config)# cts sxp connection peer 51.51.51.1 source 51.51.51.2 password none
mode local speaker
```

```
Device_B(config)# cts sxp connection peer 51.51.51.2 source 51.51.51.1 password none
mode local listener
```

次の例は、双方向 CTS-SXP を有効化し、Device_A 上の SXP ピア接続が Device_B に接続するよう設定する方法を示します。

```
Device_A> enable
Device_A# configure terminal
Device_A#(config)# cts sxp enable
Device_A#(config)# cts sxp default password Cisco123
Device_A#(config)# cts sxp default source-ip 10.10.1.1
Device_A#(config)# cts sxp connection peer 10.20.2.2 password default mode local both
```

関連コマンド

コマンド	説明
cts sxp default password	Cisco TrustSec SXP のデフォルトパスワードを設定します。
cts sxp default source-ip	Cisco TrustSec SXP の送信元 IPv4 アドレスを設定します。
cts sxp enable	デバイスで Cisco TrustSec SXP を有効にします。
cts sxp log	IP と SGT のバインディングの変更のロギングを有効にします。
cts sxp reconciliation	Cisco TrustSec SXP の復帰期間を変更します。
cts sxp retry	Cisco TrustSec SXP の再試行期間タイマーを変更します。
cts sxp speaker hold-time	Cisco TrustSec SGT SXPv4 ネットワークにおけるスピーカーデバイスのグローバルなホールド時間を設定します。
cts sxp listener hold-time	Cisco TrustSec SGT SXPv4 ネットワークにおけるリスナーデバイスのグローバルなホールド時間を設定します。
show cts sxp	Cisco TrustSec SXP のすべての設定のステータスを表示します。

cts sxp default password

Cisco TrustSec セキュリティグループタグ（SGT）交換プロトコル（CTS-SXP）のデフォルトパスワードを指定するには、グローバル コンフィギュレーション モードで **cts sxp default password** コマンドを使用します。CTS-SXP のデフォルトパスワードを削除するには、このコマンドの **no** 形式を使用します。

cts sxp default password {**0** *unencrypted-pwd* | **6** *encrypted-key* | **7** *encrypted-keycleartext-pwd*}
no cts sxp default password {**0** *unencrypted-pwd* | **6** *encrypted-key* | **7** *encrypted-keycleartext-pwd*}

構文の説明

0 *unencrypted-pwd*	暗号化されていない CTS-SXP デフォルトパスワードが続くことを指定します。パスワードの最大長は 32 文字です。
6 *encrypted-key*	タイプ 6 暗号化パスワードを CTS SXP デフォルトパスワードとして使用することを指定します。パスワードの最大長は 32 文字です。
7 *encrypted-key*	タイプ 7 暗号化パスワードを CTS SXP デフォルトパスワードとして使用することを指定します。パスワードの最大長は 32 文字です。
cleartext-pwd	クリアテキストの CTS-SXP デフォルトパスワードを指定します。パスワードの最大長は 32 文字です。

コマンド デフォルト

タイプ **0**（クリアテキスト）

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン

cts sxp default password コマンドは、デバイスに設定されているすべての SXP 接続に任意で使用する CTS-SXP デフォルトパスワードを設定します。CTS-SXP パスワードは、クリアテキストまたは **0**、**7**、**6** 暗号化タイプキーワードを使用して暗号化したものを使用します。暗号化タイプが 0 の場合は、暗号化されていないクリアテキストパスワードが続きます。

例

次に、CTS-SXP をイネーブルにし、Device_A（スピーカー）で Device_B（リスナー）への SXP ピア接続を設定する例を示します。

```
Device_A# configure terminal
Device_A#(config)# cts sxp enable
Device_A#(config)# cts sxp default password Cisco123
Device_A#(config)# cts sxp default source-ip 10.10.1.1
Device_A#(config)# cts sxp connection peer 10.20.2.2 password default mode local speaker
```

次に、Device_B（リスナー）で Device_A（スピーカー）への CTS-SXP ピア接続を設定する例を示します。

```
Device_B# configure terminal
Device_B(config)# cts sxp enable
Device_B(config)# cts sxp default password Cisco123
Device_B(config)# cts sxp default source-ip 10.20.2.2
Device_B(config)# cts sxp connection peer 10.10.1.1 password default mode local listener
```

関連コマンド

コマンド	説明
cts sxp connection peer	CTS-SXP ピアの IP アドレスを入力し、ピア接続にパスワードを使用するかどうかを指定します。
cts sxp default source-ip	CTS-SXP の送信元 IPv4 アドレスを設定します。
cts sxp enable	デバイスで CTS-SXP を有効にします。
cts sxp log	IP と SGT のバインディングの変更のロギングを有効にします。
cts sxp reconciliation	CTS-SXP の復帰期間を変更します。
cts sxp retry	CTS-SXP の再試行期間タイマーを変更します。
show cts sxp	SXP のすべての設定のステータスを表示します。

cts sxp default source-ip

Cisco TrustSec セキュリティグループタグ（SGT）交換プロトコル（CTS-SXP）の送信元 IPv4 アドレスを設定するには、グローバル コンフィギュレーション モードで **cts sxp default source-ip** コマンドを使用します。CTS-SXP のデフォルトの送信元 IP アドレスを削除するには、このコマンドの **no** 形式を使用します。

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

構文の説明

ip-address	CTS-SXP のデフォルトの送信元 IPv4 アドレス。

コマンド デフォルト

CTS-SXP の送信元 IP アドレスは設定されていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン

cts sxp default source-ip コマンドは、送信元 IP アドレスが指定されていない場合に、CTS-SXP が新規の TCP 接続すべてに使用するデフォルトの送信元 IP アドレスを設定します。既存の TCP 接続は、このコマンドが入力されても影響を受けません。CTS-SXP 接続は 3 つのタイマーによって制御されます。

- 再試行タイマー
- 削除のホールドダウン タイマー
- 復帰タイマー

例

次に、CTS-SXP をイネーブルにし、Device_A（スピーカー）で Device_B（リスナー）への SXP ピア接続を設定する例を示します。

```
Device_A# configure terminal
Device_A#(config)# cts sxp enable
Device_A#(config)# cts sxp default password Cisco123
Device_A#(config)# cts sxp default source-ip 10.10.1.1
Device_A#(config)# cts sxp connection peer 10.20.2.2 password default mode local speaker
```

次に、Device_B（リスナー）で Device_A（スピーカー）への CTS-SXP ピア接続を設定する例を示します。

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

```
Device_B(config)# cts sxp default password Cisco123
Device_B(config)# cts sxp default source-ip 10.20.2.2
Device_B(config)# cts sxp connection peer 10.10.1.1 password default mode local listener
```

関連コマンド

コマンド	説明
cts sxp connectionpeer	CTS-SXP ピアの IP アドレスを入力し、ピア接続にパスワードを使用するかどうかを指定します。
cts sxp default password	CTS-SXP のデフォルト パスワードを設定します。
cts sxp enable	デバイスで CTS-SXP を有効にします。
cts sxp log	IP と SGT のバインディングの変更のロギングを有効にします。
cts sxp reconciliation	CTS-SXP の復帰期間を変更します。
cts sxp retry	CTS-SXP の再試行期間タイマーを変更します。
show cts sxp	SXP のすべての設定のステータスを表示します。

cts sxp filter-enable

フィルタリストおよびフィルタグループの作成後にフィルタリングを有効にするには、グローバル コンフィギュレーション モードで **cts sxp filter-enable** コマンドを使用します。フィルタリングを無効にするには、このコマンドの **no** 形式を使用します。

cts sxp filter-enable
no cts sxp filter-enable

構文の説明

このコマンドにはキーワードまたは引数はありません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、フィルタリングを有効または無効にするためにいつでも使用できます。設定したフィルタリストとフィルタグループは、フィルタリングを有効にした後にのみフィルタリングの実装に使用できます。フィルタアクションでは、フィルタリングを有効にした後に交換されたバインディングのみがフィルタリングされます。フィルタリングを有効にする前に交換されたバインディングに対しては効果はありません。

例

```
Device(config)# cts sxp filter-enable
```

関連コマンド

コマンド	説明
cts sxp filter-list	IP プレフィックス、SGT、またはその両方の組み合わせに基づいて IP-SGT バインディングをフィルタリングするための SXP フィルタリストを作成します。
cts sxp filter-group	一連のピアをグループ化してフィルタリストを適用するためのフィルタグループを作成します。
show cts sxp filter-group	設定されているフィルタグループに関する情報を表示します。
show cts sxp filter-list	設定されているフィルタリストに関する情報を表示します。
debug cts sxp filter events	フィルタリストおよびフィルタグループの作成、削除、更新に関連するイベントをログに記録します。

cts sxp filter-group

一連のピアをグループ化してフィルタリストを適用するためのフィルタグループを作成するには、グローバル コンフィギュレーション モードで **cts sxp filter-group** コマンドを使用します。フィルタグループを削除するには、このコマンドの **no** 形式を使用します。

cts sxp filter-group {**listener** | **speaker**} {*filter-group-name* | **global** *filter-list-name*}
no cts sxp filter-group {**listener** | **speaker**} {*filter-group-name* | **global** *filter-list-name*}

構文の説明

listener	一連のリスナーのフィルタグループを作成します。
speaker	一連のスピーカーのフィルタグループを作成します。
global	デバイスのすべてのスピーカーまたはリスナーをグループ化します。
filter-group-name	フィルタグループの名前。
filter-list-name	フィルタ リストの名前。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン

このコマンドを発行すると、デバイスがフィルタ グループ コンフィギュレーション モードになります。このモードで、グループ化するデバイスを指定し、フィルタグループにフィルタリストを適用できます。

デバイスまたはピアをグループに追加するためのコマンドの形式は次のとおりです。

peer ipv4 *peer-IP*

1 つのコマンドで 1 つのピアを追加できます。ピアをさらに追加するには、必要な回数だけコマンドを繰り返します。

フィルタリストをグループに適用するためのコマンドの形式は次のとおりです。

filter *filter-list-name*

グローバルリスナーおよびグローバルスピーカーのフィルタグループオプションではピアリストは指定できません。この場合、フィルタはすべての SXP 接続に適用されます。

グローバルなフィルタグループとピアベースのフィルタグループの両方が適用されている場合、グローバルフィルタが優先されます。グローバルリスナーまたはグローバルスピーカーのいずれかのフィルタグループのみが設定されている場合、その方向でのみグローバルフィルタ

リングが優先されます。もう一方の方向については、ピアベースのフィルタグループが実装されます。

例

次に、**group_1** というリスナーグループを作成し、そのグループにピアとフィルタリストを割り当てる例を示します。

```
Device# configure terminal
Device(config)# cts sxp filter-group listener group_1
Device(config-filter-group)# filter filter_1
Device(config-filter-group)# peer ipv4 10.0.0.1
Device(config-filter-group)# peer ipv4 10.10.10.1
```

次に、**group_2** というグローバルリスナーグループを作成する例を示します。

```
Device# configure terminal
Device(config)# cts sxp filter-group listener global group_2
```

関連コマンド

コマンド	説明
cts sxp filter-list	IP プレフィックス、SGT、またはその両方の組み合わせに基づいて IP-SGT バインディングをフィルタリングするための SXP フィルタリストを作成します。
cts sxp filter-enable	フィルタリングを有効にします。
show cts sxp filter-group	設定されているフィルタグループに関する情報を表示します。
show cts sxp filter-list	設定されているフィルタリストに関する情報を表示します。
debug cts sxp filter events	フィルタリストおよびフィルタグループの作成、削除、更新に関連するイベントをログに記録します。

cts sxp filter-list

IP-SGTバインディングをフィルタリングするための一連のフィルタルールを保持するSXPフィルタリストを作成するには、グローバル コンフィギュレーション モードで **cts sxp filter-list** コマンドを使用します。フィルタリストを削除するには、このコマンドの**no**形式を使用します。

cts sxp filter-list *filter-list-name*
no cts sxp filter-list *filter-list-name*

構文の説明

filter-list-name	フィルタリストの名前。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン

このコマンドを発行すると、デバイスがフィルタ リスト コンフィギュレーション モードになります。このモードで、フィルタリストのルールを指定できます。

フィルタルールは、SGT、IP プレフィックス、または SGT と IP プレフィックスの両方の組み合わせに基づいて設定できます。

グループにルールを追加するためのコマンドの形式は次のとおりです。

sequence-number **action(permit/deny) filter-type(ipv4/ipv6/sgt)** *value/values*

たとえば、SGT 値が 20 である SGT-IP バインディングを許可するルールは次のようになります。

```
30 permit sgt 20
```

シーケンス番号はオプションです。シーケンス番号を指定しない場合は、システムによって生成されます。シーケンス番号は、最後に使用/設定されたシーケンス番号から自動的に 10 ずつ増分されます。2 つの既存のルールの間のシーケンス番号を指定することによって新しいルールを挿入できます。

有効な SGT 値の範囲は 2 ～ 65519 です。1 つのルールに複数の SGT 値を指定するには、スペースを使用して値を区切ります。1 つのルールに最大 8 つの SGT 値を指定できます。

SGT と IP プレフィックスを組み合わせたルールでは、ルールの両方の部分にバインディングの一致がある場合、ルールの 2 つ目の部分で指定されたアクションが優先されます。たとえば、次のルールでは、IP プレフィックス 10.0.0.1 の SGT 値が 20 の場合、ルールの最初の部分でバインディングが許可されても、対応するバインディングが拒否されます。

```
Device(config-filter-list)# 10 permit sgt 30 20 deny 10.0.0.1/24
```

同様に、次のルールでは、IP プレフィックス 10.0.0.1 の SGT が 20 で最初のアクションではバインディングが許可されなくても、SGT 値 20 のバインディングが許可されます。

```
Device(config-filter-list)# 10 deny 10.0.0.1/24 permit sgt 30 20
```

例

次に、フィルタリストを作成していくつかのルールを追加する例を示します。

```
Device# configure terminal
Device(config)# cts sxp filter-list filter_1
Device (config-filter-list)# 10 deny ipv4 10.0.0.1/24 permit sgt 100
Device(config-filter-list)# 20 permit sgt 60 61 62 63
```

関連コマンド

コマンド	説明
cts sxp filter-enable	SXP の IP プレフィックスおよび SGT ベースのフィルタリングを有効にします。
cts sxp filter-group	一連のピアをグループ化してフィルタリストを適用するためのフィルタグループを作成します。
show cts sxp filter-group	設定されているフィルタグループに関する情報を表示します。
show cts sxp filter-list	設定されているフィルタリストに関する情報を表示します。
debug cts sxp filter events	フィルタリストおよびフィルタグループの作成、削除、更新に関連するイベントをログに記録します。

cts sxp log binding-changes

IP と Cisco TrustSec セキュリティグループタグ（SGT）交換プロトコル（CTS-SXP）のバインディングの変更のロギングを有効にするには、グローバル コンフィギュレーション モードで **cts sxp log binding-changes** コマンドを使用します。ロギングを無効にするには、このコマンドの **no** 形式を使用します。

cts sxp log binding-changes
no cts sxp log binding-changes

コマンド デフォルト

ロギングは無効になっています。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン

cts sxp log binding-changes コマンドを使用すると、IP と SGT のバインディングの変更のロギングが有効になります。IP アドレスと SGT のバインディングに追加、削除、変更が発生するたびに SXP の syslog（sev 5 syslog）が生成されます。これらの変更は SXP 接続で学習されて伝播されます。

関連コマンド

コマンド	説明
cts sxp connectionpeer	CTS-SXP ピアの IP アドレスを入力し、ピア接続にパスワードを使用するかどうかを指定します。
cts sxp default password	CTS-SXP のデフォルト パスワードを設定します。
cts sxp default source-ip	CTS-SXP の送信元 IPv4 アドレスを設定します。
cts sxp enable	デバイスで CTS-SXP を有効にします。
cts sxp reconciliation	CTS-SXP の復帰期間を変更します。
cts sxp retry	CTS-SXP の再試行期間タイマーを変更します。
show cts sxp	すべての SXP 設定のステータスを表示します。

cts sxp reconciliation period

Cisco TrustSec セキュリティグループタグ（SGT）交換プロトコル（CTS-SXP）の復帰期間を変更するには、グローバル コンフィギュレーション モードで **cts sxp reconciliation period** コマンドを使用します。CTS-SXP の復帰期間をデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

cts sxp reconciliation period *seconds*
no cts sxp reconciliation period *seconds*

構文の説明

seconds	CTS-SXP 復帰タイマー（秒）。範囲は 0 ～ 64000 です。デフォルトは 120 です。

コマンド 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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン

ピアが CTS-SXP 接続を終了すると、内部の削除ホールドダウンタイマーが開始されます。削除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、CTS-SXP 復帰タイマーが開始されます。CTS-SXP 復帰期間タイマーがアクティブな間、CTS-SXP 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。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。

関連コマンド

コマンド	説明
cts sxp connection peer	CTS-SXP ピアの IP アドレスを入力し、ピア接続にパスワードを使用するかどうかを指定します。
cts sxp default password	CTS-SXP のデフォルト パスワードを設定します。
cts sxp default source-ip	CTS-SXP の送信元 IPv4 アドレスを設定します。
cts sxp enable	デバイスで CTS-SXP を有効にします。
cts sxp log	IP と SGT のバインディングの変更のロギングをオンにします。
cts sxp retry	CTS-SXP の再試行期間タイマーを変更します。
show cts sxp	CTS-SXP のすべての設定のステータスを表示します。

cts sxp retry period

Cisco TrustSec セキュリティグループタグ（SGT）交換プロトコル（CTS-SXP）の再試行期間タイマーを変更するには、グローバル コンフィギュレーション モードで **cts sxp retry period** コマンドを使用します。CTS-SXP の再試行期間タイマーをデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

cts sxpretry period *seconds*
no cts sxpretry period *seconds*

構文の説明

seconds	CTS-SXP 再試行タイマー（秒）。範囲は 0 ～ 64000 です。デフォルトは 120 です。

コマンド 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（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン

再試行タイマーは、少なくとも 1 つの CTS-SXP 接続が稼働していない場合にトリガーされます。このタイマーの期限が切れると新しい CTS-SXP 接続が試行されます。ゼロの値は、再試行が発生しなくなります。

関連コマンド

コマンド	説明
cts sxp connectionpeer	CTS-SXP ピアの IP アドレスを入力し、ピア接続にパスワードを使用するかどうかを指定します。
cts sxp default password	CTS-SXP のデフォルト パスワードを設定します。
cts sxp default source-ip	CTS-SXP の送信元 IPv4 アドレスを設定します。
cts sxp enable	デバイスで CTS-SXP を有効にします。
cts sxp log	IP と SGT のバインディングの変更のロギングを有効にします。
cts sxp reconciliation	CTS-SXP の復帰期間を変更します。
show cts sxp	CTS-SXP のすべての設定のステータスを表示します。

debug cts environment-data

Cisco TrustSec 環境データ操作のデバッグを有効にするには、特権 EXEC モードで **debug cts environment-data** コマンドを使用します。環境データ操作のデバッグを停止するには、このコマンドの **no** 形式を使用します。

debug cts environment-data [**aaa** | **all** | **default-epg** | **default-sg** | **events** | **platform** | **sg-epg**]
no debug cts environment-data [**aaa** | **all** | **default-epg** | **default-sg** | **events** | **platform** | **sg-epg**]

構文の説明

aaa	（任意）認証、許可、およびアカウンティング（AAA）メッセージのデバッグを指定します。
all	（任意）すべての環境データメッセージのデバッグを指定します。
default-epg	（任意）デフォルトエンドポイントグループ（EPG）メッセージのデバッグを指定します。
default-sg	（任意）デフォルト サーバ グループ メッセージのデバッグを指定します。
events	（任意）環境データイベントのデバッグを指定します。
platform	（任意）セキュリティグループタグ（SGT）EPG プラットフォームメッセージのデバッグを指定します。
sg-epg	（任意）SP-EPG マッピングのデバッグを指定します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

例

次に、環境データイベントのデバッグを有効にする例を示します。

```
Device# enable
Device# debug cts environment-data events
```

関連コマンド

コマンド	説明
cts environment-data enable	環境データのダウンロードを有効にします。
clear cts environment-data	環境データをクリアします。
show cts environment-data	Cisco TrustSec の環境データ情報を表示します。

debug cts policy-server

Cisco TrustSec ポリシーサーバのデバッグをイネーブルにするには、特権 EXEC モードで **debug cts policy-server** コマンドを使用します。

debug cts policy-server {**all** | {**http** | **json**} {**all** | **error** | **events**}}

構文の説明

all	ポリシーサーバのすべてのデバッグをイネーブルにします。
http	HTTP クライアントのデバッグをイネーブルにします。
json	JSON パーサーのデバッグをイネーブルにします。
error	HTTP エラーのデバッグをイネーブルにします。
events	HTTP イベントのデバッグをイネーブルにします。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

例

次に、HTTP クライアントエラーのデバッグをイネーブルにする例を示します。

```
Device# enable
Device# debug cts policy-server http error
```

関連コマンド

コマンド	説明
cts policy-server name	ポリシーサーバの名前を設定し、ポリシーサーバ コンフィギュレーション モードを開始します。
show cts policy-server	Cisco TrustSec ポリシーサーバの情報を表示します。

port（CTS）

ポリシーサーバのポートを設定するには、ポリシーサーバ コンフィギュレーション モードで **port** コマンドを使用します。ポリシーサーバのポートを削除するには、このコマンドの **no** 形式を使用します。

port *port-number*
no port

構文の説明

port-number	ポリシーサーバのポート番号。有効な値は 1025 ～ 65535 です。

コマンド デフォルト

デフォルトポートは 9063 です。

コマンド モード

ポリシーサーバ コンフィギュレーション（config-policy-server）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

使用上のガイドライン

外部 RESTful サービス（ERS）ポートとしてサポートされるのは 9063 のみです。

例

次に、ポリシーサーバのポートを設定する例を示します。

```
Device# enable
Device# configure terminal
Device(config)# policy-server name ise_server_2
Device(config-policy-server)# port 9063
```

関連コマンド

コマンド	説明
cts policy-server name	ポリシーサーバの名前を設定し、ポリシーサーバ コンフィギュレーション モードを開始します。

propagate sgt (cts manual)

Cisco TrustSec Security（CTS）インターフェイスでレイヤ2のセキュリティグループタグ（SGT）伝達を有効にするには、インターフェイス コンフィギュレーション モードで **propagate sgt** コマンドを使用します。SGT 伝達を無効にするには、このコマンドの **no** 形式を使用します。

propagate sgt

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。

コマンド デフォルト

SGT 処理の伝達が有効になっています。

コマンド モード

CTS 手動インターフェイス コンフィギュレーション モード（config-if-cts-manual）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン

SGT 処理の伝達によって、CTS 対応のインターフェイスは L2 SGT タグに基づいて CTS メタデータ（CMD）を受信および送信できます。ピアデバイスが SGT を受信できず、その結果、SGT タグを L2 ヘッダーに配置できない状況で、インターフェイスの SGT 伝達を無効にするには **no propagate sgt** コマンドを使用します。

例

次に、手動で設定された TrustSec 対応のインターフェイスで SGT 伝達を無効にする例を示します。

```
Device# configure terminal
Device(config)# interface gigabitethernet 0
Device(config-if)# cts manual
Device(config-if-cts-manual)# no propagate sgt
```

次に、ギガビット イーサネット インターフェイス 0 で SGT 伝達が無効になっている例を示します。

```
Device#show cts interface brief
Global Dot1x feature is Disabled
Interface GigabitEthernet0:
    CTS is enabled, mode:    MANUAL
    IFC state:               OPEN
    Authentication Status:   NOT APPLICABLE
        Peer identity:       "unknown"
        Peer's advertised capabilities: ""
    Authorization Status:    NOT APPLICABLE
    SAP Status:              NOT APPLICABLE
    Propagate SGT:           Disabled
    Cache Info:
        Cache applied to link : NONE
```

関連コマンド

コマンド	説明
cts manual	CTS のインターフェイスを有効にします。
show cts interface	インターフェイスごとの Cisco TrustSec ステートおよび統計情報を表示します。

retransmit（CTS）

サーバからの最大リトライ回数を設定するには、ポリシーサーバ コンフィギュレーション モードで **retransmit** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

retransmit *number-of-retries*
no retransmit

構文の説明

number-of-retries	リトライの最大数。有効な値は 0 ～ 5 です。

コマンド デフォルト

デフォルトは 4 です。

コマンド モード

ポリシーサーバ コンフィギュレーション（config-policy-server）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

例

次に、最大リトライ回数を変更する例を示します。

```
Device# enable
Device# configure terminal
Device(config)# policy-server name ise_server_2
Device(config-policy-server)# retransmit 3
```

関連コマンド

コマンド	説明
cts policy-server name	ポリシーサーバの名前を設定し、ポリシーサーバ コンフィギュレーション モードを開始します。

sap mode-list (cts manual)

2 個のインターフェイスの間のリンク暗号化をネゴシエートするために使用される Security Association Protocol（SAP）の認証と暗号化モード（最高から最低に優先順位付けされた）を選択するには、CTS dot1x インターフェイス コンフィギュレーション モードで **sap mode-list** コマンドを使用します。モードリストを削除してデフォルトに戻すには、このコマンドの **no** 形式を使用します。

2 個のインターフェイス間で MACsec のリンク暗号化をネゴシエートするために、ペアワイズ マスターキー（PMK）と Security Association Protocol（SAP）の認証および暗号化モードを手動で指定するには、**sap mode-list** コマンドを使用します。設定を無効にするには、このコマンドの **no** 形式を使用します。

sap pmk mode-list {**gcm-encrypt** | **gmac** | **no-encap** | **null**} [**gcm-encrypt** | **gmac** | **no-encap** | **null**]
no sap pmk mode-list {**gcm-encrypt** | **gmac** | **no-encap** | **null**} [**gcm-encrypt** | **gmac** | **no-encap** | **null**]

構文の説明

pmk *hex_value*	16 進数データ PMK を指定します（先行する 0x なし。偶数の16 進数文字を入力する。そうでない場合は、最後の文字に 0 のプレフィックスが付加される）。
mode-list	アドバタイズされたモードのリストを指定します（最高から最低に優先順位付け）。
gcm-encrypt	GMAC 認証、GCM 暗号化を指定します。
gmac	GMAC 認証だけを指定し、暗号化を指定しません。
no-encap	カプセル化を指定しません。
null	カプセル化あり、認証なし、暗号化なしを指定します。

コマンド デフォルト

デフォルトのカプセル化は **sap pmk mode-list gcm-encrypt null** です。ピア インターフェイスが 802.1AE MACsec または 802.REV レイヤ 2 リンク暗号化をサポートしない場合、デフォルトの暗号化は **null** です。

コマンド モード

CTS 手動インターフェイス コンフィギュレーション（config-if-cts-manual）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン

認証と暗号化方式を指定するには、**sap pmk mode-list** コマンドを使用します。

セキュリティアソシエーションプロトコル（SAP）は802.11iIEEEプロトコルのドラフトバージョンに基づいた暗号キーの取得および交換プロトコルです。SAPはMACsecをサポートするインターフェイス間の 802.1AE リンク間暗号化（MACsec）を確立および管理するために使用します。

SAP およびペアワイズマスターキー（PMK）は、**sap pmk mode-list** コマンドを使用して、2 個のインターフェイス間に手動で設定することもできます。802.1X 認証を使用する場合、両方（サプリカントおよびオーセンティケータ）が Cisco Secure Access Control Server からピアのポートの PMK および MAC アドレスを受信します。

デバイスがCTS対応ソフトウェアを実行していて、ハードウェアがCTS非対応である場合は、**sap mode-list no-encap** コマンドを使用してカプセル化を拒否します。

例

次に、ギガビット イーサネット インターフェイスで SAP を設定する例を示します。

```
Device# configure terminal
Device(config)# interface gigabitethernet 2/1
DeviceD(config-if)# cts manual
Device(config-if-cts-manual)# sap pmk FFFEE mode-list gcm-encrypt
```

関連コマンド

コマンド	説明
cts manual	CTS のインターフェイスを有効にします。
propagate sgt (cts manual)	Cisco TrustSec Security（CTS）インターフェイスのレイヤ 2 でのセキュリティ グループ タグ（SGT）の伝達を有効にします。
show cts interface	Cisco TrustSec インターフェイス設定の統計情報を表示します。

show cts credentials

Cisco TrustSec（CTS）デバイス ID を表示するには、EXEC モードまたは特権 EXEC モードで **show cts credentials** コマンドを使用します。

show cts credentials

構文の説明

このコマンドには、コマンドまたはキーワードはありません。

コマンド モード

特権 EXEC（#）ユーザ EXEC（>）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

例

次に、出力例を示します。

```
Device# show cts credentials

CTS password is defined in keystore, device-id = r4
```

関連コマンド

コマンド	説明
cts credentials	TrustSec ID およびパスワードを指定します。

show cts environment-data

Cisco TrustSec の環境データ情報を表示するには、特権 EXEC モードで **show cts environment-data** コマンドを使用します。

show cts environment-data

このコマンドには、引数およびキーワードはありません。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

例

次に、**show cts environment-data** コマンドの出力例を示します。

```
Device# enable
Device# show cts environment-data

TS Environment Data
====================
Current state = START
Last status = Failed
Environment data is empty
State Machine is running
Retry_timer (60 secs) is running
```

出力フィールドの意味は自明です。

関連コマンド

コマンド	説明
cts environment-data enable	環境データのダウンロードを有効にします。
clear cts environment-data	環境データをクリアします。
debug cts environment-data	Cisco TrustSec 環境データ操作のデバッグを有効にします。

show cts interface

インターフェイスの Cisco TrustSec（CTS）設定の統計を表示するには、EXEC モードまたは特権 EXEC モードで **show cts interface** コマンドを使用します。

show cts interface [**GigabitEthernet** *port* | **Vlan** *number* | **brief** | **summary**]

構文の説明

port	（任意）ギガビットイーサネットインターフェイス番号。このインターフェイスの冗長ステータス出力が返されます。
number	（任意）VLAN インターフェイス番号（1 ～ 4095）。
brief	（任意）すべての CTS インターフェイスの短縮ステータスを表示します。
summary	（任意）インターフェイスごとに、すべての CTS インターフェイスのサマリーを、4 個または 5 個のキー ステータス フィールドを持つ表形式で表示します。

コマンド デフォルト

なし

コマンド モード

EXEC（>） 特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン

すべての CTS インターフェイスの冗長ステータスを表示するには、キーワードを使用せずに **show cts interface** コマンドを使用します。

例

次に、キーワードを使用せずに出力を表示する例を示します（すべての CTS インターフェイスの冗長ステータス）。

```
Device# show cts interface

Global Dot1x feature is Disabled
 Interface GigabitEthernet0/1/0:
     CTS is enabled, mode:    MANUAL
     IFC state:               OPEN
     Interface Active for 00:00:18.232
     Authentication Status:   NOT APPLICABLE
         Peer identity:       "unknown"
         Peer's advertised capabilities: ""
     Authorization Status:    NOT APPLICABLE
     SAP Status:              NOT APPLICABLE
         Configured pairwise ciphers:
             gcm-encrypt
             null

         Replay protection:      enabled
         Replay protection mode: STRICT
```

```
        Selected cipher:

    Propagate SGT:           Enabled
    Cache Info:
        Cache applied to link : NONE

    Statistics:
        authc success:              0
        authc reject:               0
        authc failure:              0
        authc no response:          0
        authc logoff:               0
        sap success:                0
        sap fail:                   0
        authz success:              0
        authz fail:                 0
        port auth fail:             0
        Ingress:
            control frame bypassed: 0
            sap frame bypassed:     0
            esp packets:            0
            unknown sa:             0
            invalid sa:             0
            inverse binding failed: 0
            auth failed:            0
            replay error:           0
        Egress:
            control frame bypassed: 0
            esp packets:            0
            sgt filtered:           0
            sap frame bypassed:     0
            unknown sa dropped:     0
            unknown sa bypassed:    0
```

次に、**brief** キーワードを使用した出力例を示します。

```
Device# show cts interface brief

Global Dot1x feature is Disabled
 Interface GigabitEthernet0/1/0:
     CTS is enabled, mode:    MANUAL
     IFC state:               OPEN
     Interface Active for 00:00:40.386
     Authentication Status:   NOT APPLICABLE
         Peer identity:       "unknown"
         Peer's advertised capabilities: ""
     Authorization Status:    NOT APPLICABLE
     SAP Status:              NOT APPLICABLE
     Propagate SGT:           Enabled
     Cache Info:
         Cache applied to link : NONE
```

関連コマンド

コマンド	説明
cts manual	CTS のインターフェイスを有効にします。
cts sxp enable	ネットワーク デバイスに SXP を設定します。

コマンド	説明
propagate sgt	Cisco TrustSec Security（CTS）インターフェイスのレイヤ 2 でのセキュリティ グループ タグ（SGT）の伝達を有効にします。

show cts policy-server

Cisco TrustSec ポリシーサーバの情報を表示するには、特権 EXEC モードで **show cts policy-server** コマンドを使用します。

show cts policy-server {**details** | **statistics** } {**active** | **all** *name*}

構文の説明

details	ポリシーサーバの詳細を表示します。
statistics	ポリシーサーバの統計を表示します。
active	アクティブなポリシーサーバに関する情報を表示します。
all	すべてのサーバに関する統計情報を表示します。
name	ポリシーサーバ名。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

例

次に、**show cts policy-server details all** コマンドの出力例を示します。

```
Device# enable
Device# show cts policy-server details all

Server Name   : ise_151
Server Status : Inactive
  IPv4 Address     : 10.1.1.1
  IPv4 Address     : 10.2.2.2
  IPv4 Address     : 10.2.2.3
  IPv6 Address     : 2001:db8::1
  IPv6 Address     : 2001:db8::3
  Domain-name      : www.cisco.ise.com
  Trustpoint       : trust_ise_151
  Port-num         : 9063
  Retransmit count : 3
  Timeout          : 15
  App Content type : JSON

Server Name   : ise_150
Server Status : Inactive
  IPv4 Address     : 10.64.69.151
  Trustpoint       : trust_ise_151
  Port-num         : 9063
  Retransmit count : 3
```

```
  Timeout          : 15
  App Content type : JSON
```

次に、**show cts policy-server statistics all** コマンドの出力例を示します。

```
Device# show cts policy-server statistics all

Server Name  : ise_server_1
Server State : ALIVE
  Number of Request sent        : 7
  Number of Request sent fail   : 0
  Number of Response received   : 4
  Number of Response recv fail  : 3
    HTTP 200 OK                 : 4
    HTTP 400 BadReq             : 0
    HTTP 401 UnAuthorized Req   : 0
    HTTP 403 Req Forbidden      : 0
    HTTP 404 NotFound           : 0
    HTTP 408 ReqTimeout         : 0
    HTTP 415 UnSupported Media  : 0
    HTTP 500 ServerErr          : 0
    HTTP 501 Req NoSupport      : 0
    HTTP 503 Service Unavailable: 0
    TCP or TLS handshake error  : 3
    HTTP Other Error            : 0
```

次に、**show cts policy-server statistics** *name* コマンドの出力例を示します。

```
Device# show cts policy-server statistics name ise_server_1

Server Name  : ise_server_1
Server State : ALIVE
  Number of Request sent        : 7
  Number of Request sent fail   : 0
  Number of Response received   : 4
  Number of Response recv fail  : 3
    HTTP 200 OK                 : 4
    HTTP 400 BadReq             : 0
    HTTP 401 UnAuthorized Req   : 0
    HTTP 403 Req Forbidden      : 0
    HTTP 404 NotFound           : 0
    HTTP 408 ReqTimeout         : 0
    HTTP 415 UnSupported Media  : 0
    HTTP 500 ServerErr          : 0
    HTTP 501 Req NoSupport      : 0
    HTTP 503 Service Unavailable: 0
    TCP or TLS handshake error  : 3
    HTTP Other Error            : 0
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

表 *1 : show cts policy-server statistics* のフィールドの説明

フィールド	説明
HTTP 200 OK	クライアント要求が正常に受け入れられました。

フィールド	説明
HTTP 400 BadReq	要求の形式が正しくないか、要求に無効なパラメータが含まれています。
HTTP 401 UnAuthorized Req	リソースにアクセスするための適切なログイン情報（ユーザ名とパスワード）が指定されていません。
HTTP 403 Req Forbidden	クライアント要求がサーバから拒否されました。
HTTP 404 NotFound	URL が無効です。
HTTP 408 ReqTimeout	要求がタイムアウトしました。
HTTP 415 UnSupported Media	サーバで処理できないコンテンツタイプが要求されました。
HTTP 500 ServerErr	内部サーバエラーまたは例外が発生しました。
TCP or TLS handshake error	無効なトラストポイントが原因で、IP に到達できないか Transport Layer Security（TLS）ハンドシェイクに失敗しました。

関連コマンド

コマンド	説明
cts policy-server name	Cisco TrustSec ポリシーサーバを設定し、ポリシーサーバ コンフィギュレーション モードを開始します。
debug cts policy-server	Cisco TrustSec ポリシーサーバのデバッグをイネーブルにします。

show cts role-based counters

セキュリティ グループ アクセス コントロール リスト（ACL）の適用の統計情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show cts role-based counters** コマンドを使用します。

show cts role-based counters [**default** [**ipv4** | **ipv6**]] [{**from** {*sgt-number* | **unknown**}[**ipv4** | **ipv6** | **to** | {*sgt-number* | **unknown**} | [**ipv4** | **ipv6**]]}][**to** {*sgt-number* | **unknown**} [**ipv4** | **ipv6**]] [**ipv4** | **ipv6**]

構文の説明

default	（任意）デフォルトポリシーカウンタに関する情報を表示します。
from	（任意）送信元セキュリティグループに関する情報を表示します。
ipv4	（任意）IPv4 ネットワークのセキュリティグループに関する情報を表示します。
ipv6	（任意）IPv6 ネットワークのセキュリティグループに関する情報を表示します。
to	（任意）宛先セキュリティグループに関する情報を表示します。
sgt-number	（任意）セキュリティグループタグ番号。有効な値は 0 ～ 65533 です。
unknown	（任意）すべての送信元グループに関する情報を表示します。

コマンド モード

ユーザ EXEC (>)

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

使用上のガイドライン

すべてまたは任意の範囲の統計情報をリセットするには、**clear cts role-based counters** コマンドを使用します。

from キーワードで送信元 SGT を、**to** キーワードで宛先 SGT を指定します。**from** および **to** の両方のキーワードを省略すると、すべての統計情報が表示されます。

default キーワードは、デフォルトのユニキャストのポリシー統計情報を表示します。**ipv4** および **ipv6** のいずれのキーワードも指定しない場合、このコマンドは IPv4 カウンタだけを表示します。

Cisco TrustSec モニタモードでは、許可されたトラフィックのカウンタが SW-Permitt ラベルの下に表示され、拒否されたトラフィックのカウンタが SW-Monitor ラベルの下に表示されます。

例

次に、 **show cts role-based counters**

```
Device# show cts role-based counters

Role-based IPv4 counters
From    To      SW-Denied  HW-Denied  SW-Permitt  HW-Permitt  SW-Monitor  HW-Monitor
12      24              0          0           0           0           0           0

12      77              0          0           5           0           0           0
```

下の表に、ディスプレイ内に表示される重要なフィールドのリストを示します。

表 *2 : show cts role-based counters* のフィールドの説明

フィールド	説明
From	送信元セキュリティグループ。
To	宛先セキュリティグループ。
SW-Permitt	許可されたトラフィックのカウンタ。
SW-Monitor	拒否されたトラフィックのカウンタ。

関連コマンド

コマンド	説明
clear role-basedcounters	SGACL 統計カウンタをリセットします。
cts role-based	IP アドレス、レイヤ 3 インターフェイス、および VRF を SGT にマッピングします。Cisco TrustSec キャッシングと SGACL の適用を有効にします。

show cts role-based permissions

ロールベース（セキュリティグループ）アクセスコントロール権限リストを表示するには、特権 EXEC モードで **show cts role-based permissions** コマンドを使用します。

show cts role-based permissions [**default** [**details** | **ipv4 [details]** | **ipv6 [details]**] | **from {** {*sgt* | **unknown** }[**ipv4** | **ipv6** | **to {** {*sgt* | **unknown**}[**details** | **ipv4 [details]** | **ipv6 [details]**]}}] | **ipv4** | **ipv6** | **platform** | **to** {*sgt* | **unknown**}[**ipv4** | **ipv6**]]

構文の説明

default	（任意）デフォルトの権限リストに関する情報を表示します。
details	（任意）アタッチされたアクセス コントロール リスト（ACL）の詳細を表示します。
ipv4	（任意）IPv4 プロトコルに関する情報を表示します。
ipv6	（任意）IPv6 プロトコルに関する情報を表示します。
from	（任意）送信元グループに関する情報を表示します。
sgt	（任意）セキュリティ グループ タグ。有効値は 2 ～ 65519 です。
to	（任意）宛先グループに関する情報を表示します。
unknown	（任意）不明な送信元グループと宛先グループに関する情報を表示します。
platform	（任意）プラットフォームに関する情報を表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、SGACL 権限マトリックスのコンテンツを表示します。送信元セキュリティ グループタグ（SGT）は **from** キーワードを使用して、宛先 SGT は **to** キーワードを使用して指定できます。両方のキーワードを指定すると、単一セルの RBACL が表示されます。列全体は、**to** キーワードを使用した場合にのみ表示されます。行全体は、**from** キーワードを使用した場合に表示されます。権限マトリックス全体は、**from** キーワードと **to** キーワードの両方を省略した場合に表示されます。

コマンド出力は、プライマリ キーの宛先 SGT およびセカンダリ キーの送信元 SGT でソートされます。各セルの SGACL は、設定で定義されているのと同じ順序で、または Cisco Identity Services Engine（ISE）から取得した順序で表示されます。

details キーワードは、 **from** キーワードと **to** キーワードの両方を指定することで、単一のセルが選択された場合に表示されます。**details** キーワードが指定されている場合、単一セルの SGACL のアクセス制御エントリが表示されます。

次に、**show role-based permissions** コマンドの出力例を示します。

```
Device# show cts role-based permissions

IPv4 Role-based permissions default (monitored):
default_sgacl-02
Permit IP-00
IPv4 Role-based permissions from group 305:sgt to group 306:dgt (monitored):
test_reg_tcp_permit-02
RBACL Monitor All for Dynamic Policies : TRUE
RBACL Monitor All for Configured Policies : FALSE
IPv4 Role-based permissions from group 6:SGT_6 to group 6:SGT_6 (configured):
  mon_1
IPv4 Role-based permissions from group 10 to group 11 (configured):
  mon_2
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

関連コマンド

コマンド	説明
cts role-based permissions	送信元グループから宛先グループに対する権限を有効にします。
cts role-based monitor	ロールベースのアクセスリストのモニタリングを有効にします。

show cts server-list

Cisco TrustSec シードおよび非シードデバイスで利用可能な HTTP サーバと RADIUS サーバのリストを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show cts server-list** コマンドを使用します。

show cts server-list

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。

コマンド モード

ユーザ EXEC (>)

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.1.1	このコマンドの出力が変更され、HTTP サーバのアドレスとステータス情報が表示されるようになりました。

使用上のガイドライン

このコマンドは、Cisco TrustSec RADIUS サーバのアドレスとステータス情報を収集するのに使用できます。

Cisco IOS XE Gibraltar 17.1.1 以降のリリースでは、このコマンドの出力に HTTP サーバのアドレスとステータス情報が表示されます。

例

Cisco IOS XE Amsterdam 17.1.1

次の **show cts server-list** コマンドの出力例では、HTTP サーバとそのステータス情報が表示されています。

```
Device> show cts server-list

HTTP Server-list:
Server Name: Http_Server_1
Server Status: DEAD
    IPv4 Address: 10.78.105.148
    IPv6 Address: Not Supported
    Domain-name: http_server_1.ise.com
    Port: 9063


Server Name: Http_Server_2
Server Status: ALIVE
    IPv4 Address: 10.78.105.149
    IPv6 Address: Not Supported
    Domain-name: http_server_2.ise.com
    Status = ALIVE
```

Cisco IOS XE Amsterdam 17.1.1 より前のリリース

次の例では、Cisco TrustSec RADIUS サーバのリストが表示されています。

```
Device> show cts server-list

CTS Server Radius Load Balance = DISABLED
Server Group Deadtime = 20 secs (default)
Global Server Liveness Automated Test Deadtime = 20 secs
Global Server Liveness Automated Test Idle Time = 60 mins
Global Server Liveness Automated Test = ENABLED (default)
Preferred list, 1 server(s):
 *Server: 10.0.1.6, port 1812, A-ID 1100E046659D4275B644BF946EFA49CD
          Status = ALIVE
          auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
Installed list: ACSServerList1-0001, 1 server(s):
 *Server: 101.0.2.61, port 1812, A-ID 1100E046659D4275B644BF946EFA49CD
          Status = ALIVE
          auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
```

関連コマンド

コマンド	説明
address ipv4 (config-radius-server)	PAC プロビジョニングに使用する RADIUS サーバのアカウンティングおよび認証パラメータを設定します。
pac key	PAC 暗号キーを指定します。

show cts sxp

Cisco TrustSec セキュリティグループタグ（SGT）交換プロトコル（CTS-SXP）接続または送信元 IP と SGT のマッピング情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show cts sxp** コマンドを使用します。

show cts sxp {**connections** [**brief** | **vrf** *instance-name*] | **filter-group** [**detailed** | **global** | **listener** | **speaker**] | **filter-list** *filter-list-name* | **sgt-map** [**brief** | **vrf** *instance-name*]} [**brief** | **vrf** *instance-name*]

構文の説明

connections	Cisco TrustSec SXP 接続の情報を表示します。
brief	（任意）SXP 情報の省略形を表示します。
vrf *instance-name*	（任意）指定した Virtual Routing and Forwarding（VRF）インスタンスの SXP 情報を表示します。
filter-group {**detailed** | **global** | **listener** | **speaker** }	（任意）フィルタグループ情報を表示します。
filter-list *filter-list-name*	（任意）フィルタリスト情報を表示します。
sgt-map	（任意）SXP 経由で受信した IP と SGT のマッピングを表示します。

コマンド デフォルト

なし

コマンド モード

ユーザ EXEC（>）特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.2	このコマンドが導入されました。

例

次に、**brief** キーワードを使用して SXP 接続を表示する例を示します。

```
Device# show cts sxp connection brief

 SXP              : Enabled
 Default Password : Set
 Default Source IP: Not Set
Connection retry open period: 10 secs
Reconcile period: 120 secs
Retry open timer is not running
------------------------------------------------------------------------------
Peer_IP          Source_IP        Conn Status       Duration
------------------------------------------------------------------------------
10.10.10.1          10.10.10.2          On               0:00:02:14 (dd:hr:mm:sec)
10.10.2.1          10.10.2.2          On               0:00:02:14 (dd:hr:mm:sec)
```

```
Total num of SXP Connections = 2
```

次に、CTS-SXP 接続を表示する例を示します。

```
Device# show cts sxp connections

 SXP              : Enabled
 Default Password : Set
 Default Source IP: Not Set
Connection retry open period: 10 secs
Reconcile period: 120 secs
Retry open timer is not running
------------------------------------------------
Peer IP          : 10.10.10.1
Source IP        : 10.10.10.2
Set up           : Peer
Conn status      : On
Connection mode  : SXP Listener
Connection inst# : 1
TCP conn fd      : 1
TCP conn password: not set (using default SXP password)
Duration since last state change: 0:00:01:25 (dd:hr:mm:sec)
------------------------------------------------
Peer IP          : 10.10.2.1
Source IP        : 10.10.2.2
Set up           : Peer
Conn status      : On
Connection mode  : SXP Listener
TCP conn fd      : 2
TCP conn password: not set (using default SXP password)
Duration since last state change: 0:00:01:25 (dd:hr:mm:sec)
Total num of SXP Connections = 2
```

次に、デバイスがスピーカーとリスナーの両方である場合に双方向接続のCTS-SXP接続を表示する例を示します。

```
Device# show cts sxp connections

SXP : Enabled
Highest Version Supported: 4
Default Password : Set
Default Source IP: Not Set
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is running
------------------------------------------------
Peer IP : 2.0.0.2
Source IP : 1.0.0.2
Conn status : On (Speaker) :: On (Listener)
Conn version : 4
Local mode : Both
Connection inst# : 1
TCP conn fd : 1(Speaker) 3(Listener)
TCP conn password: default SXP password
Duration since last state change: 1:03:38:03 (dd:hr:mm:sec) :: 0:00:00:46 (dd:hr:mm:sec)
```

次に、SXP スピーカーへの接続が切断された CTS-SXP リスナーからの出力例を示します。送信元 IP と SGT のマッピングは 120 秒（削除のホールドダウンタイマーのデフォルト値）の間保持されます。

```
Device# show cts sxp connections

 SXP              : Enabled
 Default Password : Set
 Default Source IP: Not Set
Connection retry open period: 10 secs
Reconcile period: 120 secs
Retry open timer is not running
------------------------------------------------
Peer IP          : 10.10.10.1
Source IP        : 10.10.10.2
Set up           : Peer
Conn status      : Delete_Hold_Down
Connection mode  : SXP Listener
Connection inst# : 1
TCP conn fd      : -1
TCP conn password: not set (using default SXP password)
Delete hold down timer is running
Duration since last state change: 0:00:00:16 (dd:hr:mm:sec)
------------------------------------------------
Peer IP          : 10.10.2.1
Source IP        : 10.10.2.2
Set up           : Peer
Conn status      : On
Connection inst# : 1
TCP conn fd      : 2
TCP conn password: not set (using default SXP password)
Duration since last state change: 0:00:05:49 (dd:hr:mm:sec)
Total num of SXP Connections = 2
```

関連コマンド

コマンド	説明
cts sxp connection peer	Cisco TrustSec SXP ピアの IP アドレスを入力し、ピア接続にパスワードを使用するかどうかを指定します。
cts sxp default password	Cisco TrustSec SXP のデフォルトパスワードを設定します。
cts sxp default source-ip	Cisco TrustSec SXP の送信元 IPv4 アドレスを設定します。
cts sxp enable	デバイスで Cisco TrustSec SXP を有効にします。
cts sxp log	IP と SGT のバインディングの変更のロギングを有効にします。
cts sxp reconciliation	Cisco TrustSec SXP の復帰期間を変更します。
cts sxp retry	Cisco TrustSec SXP の再試行期間タイマーを変更します。

show platform hardware fed switch active fwd-asic resource tcam utilization

ASIC の CAM 使用率情報を表示するには、特権 EXEC モードで **show platform hardware fed switch active fwd-asic resource tcam utilization** コマンドを使用します。

show platform hardware fed switch active fwd-asic resource tcam utilization [*asic-number*] [*slice-id*]

構文の説明

asic-number	ASIC 番号を表示します。有効な値の範囲は 0 ～ 7 です。
slice-id	スライスごとの使用状況を表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

例

次に、**show platform hardware fed switch active fwd-asic resource tcam utilization** コマンドの出力例を示します。

```
Device# enable
Device# show platform hardware fed switch active fwd-asic resource tcam utilization

CAM Utilization for ASIC  [0]
 Table                  Subtype      Dir      Max     Used    %Used       V4       V6
   MPLS    Other

----------------------------------------------------------------------------------------------

 Mac Address Table      EM           I       32768       25    0.08%        0        0
       0       25
 Mac Address Table      TCAM         I        1024       22    2.15%        0        0
       0       22
 L3 Multicast           EM           I        8192        0    0.00%        0        0
       0        0
 L3 Multicast           TCAM         I         512        9    1.76%        3        6
       0        0
 L2 Multicast           EM           I        8192        0    0.00%        0        0
       0        0
 L2 Multicast           TCAM         I         512       11    2.15%        3        8
       0        0
 IP Route Table         EM           I       24576       14    0.06%       13        0
       1        0
 IP Route Table         TCAM         I        8192       30    0.37%       11       16
       2        1
 QOS ACL                TCAM         IO       5120       85    1.66%       28       38
       0       19
                        TCAM         I                   45    0.88%       15       20
       0       10
```

```
                        TCAM         O                  40    0.78%       13       18
      0        9
Security ACL            TCAM         IO       5120      131    2.56%       26       60
      0       45
                        TCAM         I                  88    1.72%       12       36
      0       40
                        TCAM         O                  43    0.84%       14       24
      0        5
Netflow ACL             TCAM         I         256        6    2.34%        2        2
      0        2
PBR ACL                 TCAM         I        1024       36    3.52%       30        6
      0        0
Netflow ACL             TCAM         O         768        6    0.78%        2        2
      0        2
Flow SPAN ACL           TCAM         IO       1024       13    1.27%        3        6
      0        4
                        TCAM         I                   5    0.49%        1        2
      0        2
                        TCAM         O                   8    0.78%        2        4
      0        2
Control Plane           TCAM         I         512      290   56.64%      138      106
      0       46
Tunnel Termination      TCAM         I         512       22    4.30%        9       13
      0        0
Lisp Inst Mapping       TCAM         I        2048        2    0.10%        0        0
      0        2
Security Association    TCAM         I         256        4    1.56%        2        2
      0        0
CTS Cell Matrix/VPN
Label                   EM           O        8192        0    0.00%        0        0
      0        0
CTS Cell Matrix/VPN
Label                   TCAM         O         512        1    0.20%        0        0
      0        1
Client Table            EM           I        4096        0    0.00%        0        0
      0        0
Client Table            TCAM         I         256        0    0.00%        0        0
      0        0
Input Group LE          TCAM         I        1024        0    0.00%        0        0
      0        0
Output Group LE         TCAM         O        1024        0    0.00%        0        0
      0        0
Macsec SPD              TCAM         I         256        2    0.78%        0        0
      0        2
```

出力フィールドの意味は自明です。

関連コマンド

コマンド	説明
show platform hardware fed switch active fwd-asic resource tcam table	現在の CAM テーブルを表示します。
show platform hardware fed switch active fwd-asic resource tcam usage	現在の CAM の使用状況を表示します。

show platform hardware fed switch active sgacl resource usage

特定用途向け集積回路（ASIC）のセキュリティ グループ アクセス コントロール リスト（SGACL）のリソース情報を表示するには、特権 EXEC モードで **show platform hardware fed switch active sgacl resource usage** コマンドを使用します。

show platform hardware fed switch active sgacl resource usage

構文の説明

usage	SGACL リソースの使用状況を表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

例

次に、**show platform hardware fed switch active sgacl resource usage** コマンドの出力例を示します。

```
Device# enable
Device# show platform hardware fed switch active sgacl resource usage

SGACL RESOURCE DETAILS ASIC :#0
================================
                                                    Percent     Thresholds
Hardware Resource                MAX      Used       Used    Upper     Lower
-------------------------------------------------------------------------------
  CTS Cell Matrix Config    :                                    80        70
  CTS Cell Matrix Entries   :   8192         0          0          Normal
  CTS Cell Overflow Entries :    512         1          0

  Policy Configuration      :                                    80        70
  Policy Entries            :    256         3          1          Normal

  DGT Config                :                                    80        70
  DGT Entries               :   4096         0          0          Normal

  Security ACL Configured   :                                    80        70
  Security ACL Entries      :   5120       131          2          Normal

                                  Total     Percent
      SGACL TCAM Entries           Used      Used
      ------------------------------------------------------------------
      Output PRE SGACL      :        4        12
      Output SGACL          :        0         0
      Output SGACL DEFAULT  :        0         0
.
.
.
Device#
```

出力フィールドの意味は自明です。

show platform software classification switch active F0 class-group-manager class-group client acl all

Ternary Content Addressable Memory（TCAM）エントリの表示に使用される ACL クラスグループ ID を表示するには、特権 EXEC モードで **show platform software classification switch active F0 class-group-manager class-group client acl all** コマンドを使用します。

show platform software classification switch active F0 class-group-manager class-group client acl all

構文の説明

class-group-manager	クラスグループマネージャを表示します。
class-group	クラスグループを表示します。
all	すべてのクラスグループの ACL クラスグループ ID を表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

例

次に、**show platform software classification switch active F0 class-group-manager class-group client acl all** コマンドの出力例を示します。

```
Device#show platform software classification switch active F0 class-group-manager
class-group client acl all

QFP classification class client all group

  class-group [ACL-GRP:273]
  class-group [ACL-GRP:529]
  class-group [ACL-GRP:801]
```

出力フィールドの意味は自明です。

関連コマンド

コマンド	説明
show platform software classification switch active F0 class-group-manager class-group client acl name *class-group name*	指定されたクラスグループの ACL クラスグループ情報を表示します。
show platform software classification switch active F0 class-group-manager class-group client acl *class-group id*	指定されたクラスグループの ACL クラスグループ情報を表示します。

show platform software cts forwarding-manager switch active F0 port

転送マネージャインターフェイスの CTS 情報を表示するには、特権 EXEC モードで **show platform software cts forwarding-manager switch active F0 port** コマンドを使用します。

show platform software cts forwarding-manager switch active F0 port

構文の説明

F0	Embedded Service Processor スロット 0。
port	ポート CTS ステータスを表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

例

次に、**show platform software cts forwarding-manager switch active F0 port** コマンドの出力例を示します。

```
Device#show platform software cts forwarding-manager switch active F0 port

Forwarding Manager Interfaces CTS Information

Name                                ID     CTS Enable  Trusted   Propagate   SGT value
-------------------------------------------------------------------------------------
GigabitEthernet1/0/1                77         0          0          0           0
GigabitEthernet1/0/3                79         0          0          0           0
GigabitEthernet1/0/4                80         0          0          0           0
GigabitEthernet1/0/5                81         0          0          0           0
GigabitEthernet1/0/6                82         0          0          0           0
GigabitEthernet1/0/7                83         0          0          0           0
GigabitEthernet1/0/8                84         0          0          0           0
GigabitEthernet1/0/9                85         0          0          0           0
GigabitEthernet1/0/10               86         0          0          0           0
GigabitEthernet1/0/11               87         0          0          0           0
GigabitEthernet1/0/12               88         0          0          0           0
GigabitEthernet1/0/13               89         0          0          0           0
GigabitEthernet1/0/14               90         0          0          0           0
GigabitEthernet1/0/15               91         0          0          0           0
GigabitEthernet1/0/16               92         0          0          0           0
GigabitEthernet1/0/17               93         0          0          0           0
GigabitEthernet1/0/18               94         0          0          0           0
GigabitEthernet1/0/19               95         0          0          0           0
GigabitEthernet1/0/20               96         0          0          0           0
GigabitEthernet1/0/21               97         0          0          0           0
GigabitEthernet1/0/22               98         0          0          0           0
GigabitEthernet1/0/23               99         0          0          0           0
GigabitEthernet1/0/24              100         0          0          0           0
GigabitEthernet1/0/25              101         0          0          0           0
```

```
GigabitEthernet1/0/26          102         0          0          0          0
GigabitEthernet1/0/27          103         0          0          0          0
GigabitEthernet1/0/28          104         0          0          0          0
GigabitEthernet1/0/29          105         0          0          0          0
GigabitEthernet1/0/30          106         0          0          0          0
GigabitEthernet1/0/31          107         0          0          0          0
GigabitEthernet1/0/32          108         0          0          0          0
GigabitEthernet1/0/33          109         0          0          0          0
GigabitEthernet1/0/34          110         0          0          0          0
GigabitEthernet1/0/35          111         0          0          0          0
GigabitEthernet1/0/36          112         0          0          0          0
GigabitEthernet1/0/37          113         0          0          0          0
GigabitEthernet1/0/38          114         0          0          0          0
GigabitEthernet1/0/39          115         0          0          0          0
GigabitEthernet1/0/40          116         0          0          0          0
GigabitEthernet1/0/41          117         0          0          0          0


Forwarding Manager Interfaces CTS Information

Name                            ID      CTS Enable  Trusted   Propagate   SGT value
-------------------------------------------------------------------------------------
GigabitEthernet1/0/42          118         0          0          0          0
GigabitEthernet1/0/43          119         0          0          0          0
GigabitEthernet1/0/44          120         0          0          0          0
GigabitEthernet1/0/45          121         0          0          0          0
GigabitEthernet1/0/46          122         0          0          0          0
GigabitEthernet1/0/47          123         0          0          0          0
GigabitEthernet1/1/1           125         0          0          0          0
GigabitEthernet1/1/2           126         0          0          0          0
GigabitEthernet1/1/3           127         0          0          0          0
GigabitEthernet1/1/4           128         0          0          0          0
TenGigabitEthernet1/1/1        129         0          0          0          0
TenGigabitEthernet1/1/2        130         0          0          0          0
TenGigabitEthernet1/1/3        131         0          0          0          0
TenGigabitEthernet1/1/4        132         0          0          0          0
TenGigabitEthernet1/1/5        133         0          0          0          0
TenGigabitEthernet1/1/6        134         0          0          0          0
TenGigabitEthernet1/1/7        135         0          0          0          0
TenGigabitEthernet1/1/8        136         0          0          0          0
FortyGigabitEthernet1/1/1      137         0          0          0          0
FortyGigabitEthernet1/1/2      138         0          0          0          0
TwentyFiveGigE1/1/1            139         0          0          0          0
TwentyFiveGigE1/1/2            140         0          0          0          0
AppGigabitEthernet1/0/1        141         0          0          0          0
GigabitEthernet2/0/1           142         1          0          0          0
GigabitEthernet2/0/2           143         0          0          0          0
GigabitEthernet2/0/3           144         0          0          0          0
GigabitEthernet2/0/4           145         0          0          0          0
GigabitEthernet2/0/5           146         0          0          0          0
GigabitEthernet2/0/6           147         0          0          0          0
GigabitEthernet2/0/7           148         0          0          0          0
GigabitEthernet2/0/8           149         0          0          0          0
GigabitEthernet2/0/9           150         0          0          0          0
GigabitEthernet2/0/10          151         0          0          0          0
GigabitEthernet2/0/11          152         0          0          0          0
GigabitEthernet2/0/12          153         0          0          0          0
GigabitEthernet2/0/13          154         0          0          0          0
GigabitEthernet2/0/14          155         0          0          0          0
GigabitEthernet2/0/15          156         0          0          0          0
GigabitEthernet2/0/16          157         0          0          0          0
GigabitEthernet2/0/17          158         0          0          0          0
```

```
Forwarding Manager Interfaces CTS Information

Name                              ID     CTS Enable  Trusted   Propagate   SGT value
-------------------------------------------------------------------------------------
GigabitEthernet2/0/18            159          0          0          0           0
GigabitEthernet2/0/19            160          0          0          0           0
GigabitEthernet2/0/20            161          0          0          0           0
GigabitEthernet2/0/21            162          0          0          0           0
GigabitEthernet2/0/22            163          0          0          0           0
GigabitEthernet2/0/23            164          0          0          0           0
GigabitEthernet2/0/24            165          0          0          0           0
GigabitEthernet2/0/25            166          0          0          0           0
GigabitEthernet2/0/26            167          0          0          0           0
GigabitEthernet2/0/27            168          0          0          0           0
GigabitEthernet2/0/28            169          0          0          0           0
GigabitEthernet2/0/29            170          0          0          0           0
GigabitEthernet2/0/30            171          0          0          0           0
GigabitEthernet2/0/31            172          0          0          0           0
GigabitEthernet2/0/32            173          0          0          0           0
GigabitEthernet2/0/33            174          0          0          0           0
GigabitEthernet2/0/34            175          0          0          0           0
GigabitEthernet2/0/35            176          0          0          0           0
GigabitEthernet2/0/36            177          0          0          0           0
GigabitEthernet2/0/37            178          0          0          0           0
GigabitEthernet2/0/38            179          0          0          0           0
GigabitEthernet2/0/39            180          0          0          0           0
GigabitEthernet2/0/40            181          0          0          0           0
GigabitEthernet2/0/41            182          0          0          0           0
GigabitEthernet2/0/42            183          0          0          0           0
GigabitEthernet2/0/43            184          0          0          0           0
GigabitEthernet2/0/44            185          0          0          0           0
GigabitEthernet2/0/45            186          0          0          0           0
GigabitEthernet2/0/46            187          0          0          0           0
GigabitEthernet2/0/47            188          0          0          0           0
GigabitEthernet2/1/1             190          0          0          0           0
GigabitEthernet2/1/2             191          0          0          0           0
GigabitEthernet2/1/3             192          0          0          0           0
GigabitEthernet2/1/4             193          0          0          0           0
TenGigabitEthernet2/1/1          194          0          0          0           0
TenGigabitEthernet2/1/2          195          0          0          0           0
TenGigabitEthernet2/1/3          196          0          0          0           0
TenGigabitEthernet2/1/4          197          0          0          0           0
TenGigabitEthernet2/1/5          198          0          0          0           0
TenGigabitEthernet2/1/6          199          0          0          0           0


Forwarding Manager Interfaces CTS Information

Name                              ID     CTS Enable  Trusted   Propagate   SGT value
-------------------------------------------------------------------------------------
TenGigabitEthernet2/1/7          200          0          0          0           0
TenGigabitEthernet2/1/8          201          0          0          0           0
FortyGigabitEthernet2/1/1        202          0          0          0           0
FortyGigabitEthernet2/1/2        203          0          0          0           0
TwentyFiveGigE2/1/1              204          0          0          0           0
TwentyFiveGigE2/1/2              205          0          0          0           0
AppGigabitEthernet2/0/1          206          0          0          0           0
GigabitEthernet1/0/2             213          0          0          0           0
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

表 *3 : show platform software cts forwarding-manager switch active F0 port* のフィールドの説明

フィールド	説明
Name	インターフェイスの名前。
ID	インターフェイス ID。
CTS Enable	CTS のステータス。
Trusted	インターフェイスの信頼ステータス。
Propagate	インターフェイスの伝達ステータス。
SGT value	SGT の値。

show platform software cts forwarding-manager switch active F0

セキュリティグループタグ（SGT）バインドテーブルを表示するには、特権 EXEC モードで **show platform software cts forwarding-manager switch active F0** コマンドを使用します。

show platform software cts forwarding-manager switch active F0

構文の説明

F0	Embedded Service Processor スロット 0 を選択します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

例

次に、**show platform software cts forwarding-manager switch active F0** コマンドの出力例を示します。

```
Device#show platform software cts forwarding-manager switch active F0

SGT Binding Table

Number of bindings: 1

2.2.2.2/32
SGT Src: 2
SGT Dst: 2


SGT Binding Table
```

出力フィールドの意味は自明です。

関連コマンド

コマンド	説明
show platform software cts forwarding-manager switch active F0 port	ポート CTS ステータスを表示します。
show platform software cts forwarding-manager switch active F0 permissions	SGACL 権限を表示します。

show platform software cts forwarding-manager switch active F0 permissions

セキュリティ グループ アクセス コントロール リスト（SGACL）の権限を表示するには、特権 EXEC モードで **show platform software cts forwarding-manager switch active F0 permissions** コマンドを使用します。

show platform software cts forwarding-manager switch active F0 permissions

構文の説明

F0	Embedded Service Processor スロット 0 を選択します。
permissions	SGACL 権限を表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

例

次に、**show platform software cts forwarding-manager switch active F0 permissions** コマンドの出力例を示します。

```
Device#show platform software cts forwarding-manager switch active F0 permissions

Forwarding Manager CTS permissions Information

  sgt       dgt     ACL Group Name


   4         2      V4SGACL7100

 65535     65535    V4SGACL8100

 65535     65535    V6SGACL9100
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

表 *4 : show platform software cts forwarding-manager switch active F0 permissions* のフィールドの説明

フィールド	説明
sgt	送信元グループタグ。

dgt	接続先グループタグ。
ACL Group Name	ACL グループの名前。

show platform software fed switch active acl counters hardware | inc SGACL

フォワーディング エンジン ドライバからのカウンタを表示するには、特権 EXEC モードで **show platform software fed switch active acl counters hardware | inc SGACL** コマンドを使用します。

show platform software fed switch active acl counters hardware | inc SGACL

構文の説明

counters	カウンタ情報を表示します。
hardware	ハードウェアカウンタを表示します。
include	指定された文字列に一致する行を含めます。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

例

次に、**show platform software fed switch active acl counters hardware | inc SGACL** コマンドの出力例を示します。

```
Device# show platform software fed switch active acl counters hardware | inc SGACL

Egress IPv4 SGACL Drop           (0x3f000061):           0 frames
Egress IPv6 SGACL Drop           (0x13000062):           0 frames
Egress IPv4 SGACL Test Cell Drop (0xd2000063):           0 frames
Egress IPv6 SGACL Test Cell Drop (0x40000064):           0 frames
Egress IPv4 Pre SGACL Forward    (0x2c000067):           0 frames
```

show platform software fed switch active acl usage

セキュリティグループアクセスコントロールリスト（SGACL）の使用状況を表示するには、特権 EXEC モードで **show platform software fed switch active acl usage** コマンドを使用します。

show platform software fed switch active acl usage

構文の説明

usage	ACLの使用状況を表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

例

次に、**show platform software fed switch active acl usage** コマンドの出力例を示します。

```
Device# show platform software fed switch active acl usage
##########################################################
########                                ##################
#######      Printing Usage Infos       #################
########                                ##################
##########################################################
#####  ACE Software VMR max:196608 used:282
##########################################################
=============================================================================================================
Feature Type            ACL Type        Dir             Name                    Entries
 Used
SGACL                   IPV4            Egress          V4SGACL7100             2

=============================================================================================================
Feature Type            ACL Type        Dir             Name                    Entries
 Used
SGACL_CATCHALL          IPV4            Egress          V4SGACL8100             1

=============================================================================================================
Feature Type            ACL Type        Dir             Name                    Entries
 Used
SGACL_CATCHALL          IPV6            Egress          V6SGACL9100             1

=============================================================================================================
```

出力フィールドの意味は自明です。

show platform software fed switch active ifm mappings

show platform software fed switch active ifm mappings

構文の説明

ifm	インターフェイスマネージャ情報を表示します。
mappings	インターフェイスからハードウェアへのマッピング情報を表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

例

次に、**show platform software fed switch active ifm mappings** コマンドの出力例を示します。

```
Device#show platform software fed switch active ifm mappings

Interface               IF_ID    Inst Asic Core Port SubPort Mac  Cntx LPN  GPN  Type
 Active
GigabitEthernet3/0/1    0xa        1   0    1    0      0      26   6    1    193  NIF
  Y
GigabitEthernet3/0/2    0xb        1   0    1    1      0      6    7    2    194  NIF
  Y
GigabitEthernet3/0/3    0xc        1   0    1    2      0      28   8    3    195  NIF
  Y
GigabitEthernet3/0/4    0xd        1   0    1    3      0      27   9    4    196  NIF
  Y
GigabitEthernet3/0/5    0xe        1   0    1    4      0      30   10   5    197  NIF
  Y
GigabitEthernet3/0/6    0xf        1   0    1    5      0      29   11   6    198  NIF
  Y
GigabitEthernet3/0/7    0x10       1   0    1    6      0      32   12   7    199  NIF
  Y
GigabitEthernet3/0/8    0x11       1   0    1    7      0      31   13   8    200  NIF
  Y
GigabitEthernet3/0/9    0x12       1   0    1    8      0      19   14   9    201  NIF
  Y
GigabitEthernet3/0/10   0x13       1   0    1    9      0      5    15   10   202  NIF
  Y
GigabitEthernet3/0/11   0x14       1   0    1    10     0      21   16   11   203  NIF
  Y
GigabitEthernet3/0/12   0x15       1   0    1    11     0      20   17   12   204  NIF
  Y
GigabitEthernet3/0/13   0x16       1   0    1    12     0      23   18   13   205  NIF
  Y
GigabitEthernet3/0/14   0x17       1   0    1    13     0      22   19   14   206  NIF
  Y
GigabitEthernet3/0/15   0x18       1   0    1    14     0      25   20   15   207  NIF
  Y
GigabitEthernet3/0/16   0x19       1   0    1    15     0      24   21   16   208  NIF
  Y
GigabitEthernet3/0/17   0x1a       1   0    1    16     0      12   22   17   209  NIF
  Y
```

```
GigabitEthernet3/0/18     0x1b       1   0   1    17     0       4    23   18   210  NIF
  Y
GigabitEthernet3/0/19     0x1c       1   0   1    18     0       14   24   19   211  NIF
  Y
GigabitEthernet3/0/20     0x1d       1   0   1    19     0       13   25   20   212  NIF
  Y
GigabitEthernet3/0/21     0x1e       1   0   1    20     0       16   26   21   213  NIF
  Y
GigabitEthernet3/0/22     0x1f       1   0   1    21     0       15   27   22   214  NIF
  Y
GigabitEthernet3/0/23     0x20       1   0   1    22     0       18   28   23   215  NIF
  Y
GigabitEthernet3/0/24     0x21       1   0   1    23     0       17   29   24   216  NIF
  Y
GigabitEthernet3/0/25     0x22       0   0   0    24     0       26   6    25   217  NIF
  Y
GigabitEthernet3/0/26     0x23       0   0   0    25     0       6    7    26   218  NIF
  Y
GigabitEthernet3/0/27     0x24       0   0   0    26     0       28   8    27   219  NIF
  Y
GigabitEthernet3/0/28     0x25       0   0   0    27     0       27   9    28   220  NIF
  Y
GigabitEthernet3/0/29     0x26       0   0   0    28     0       30   10   29   221  NIF
  Y
GigabitEthernet3/0/30     0x27       0   0   0    29     0       29   11   30   222  NIF
  Y
GigabitEthernet3/0/31     0x28       0   0   0    30     0       32   12   31   223  NIF
  Y
GigabitEthernet3/0/32     0x29       0   0   0    31     0       31   13   32   224  NIF
  Y
GigabitEthernet3/0/33     0x2a       0   0   0    32     0       19   14   33   225  NIF
  Y
GigabitEthernet3/0/34     0x2b       0   0   0    33     0       5    15   34   226  NIF
  Y
GigabitEthernet3/0/35     0x2c       0   0   0    34     0       21   16   35   227  NIF
  Y
GigabitEthernet3/0/36     0x2d       0   0   0    35     0       20   17   36   228  NIF
  Y
GigabitEthernet3/0/37     0x2e       0   0   0    36     0       23   18   37   229  NIF
  Y
GigabitEthernet3/0/38     0x2f       0   0   0    37     0       22   19   38   230  NIF
  Y
GigabitEthernet3/0/39     0x30       0   0   0    38     0       25   20   39   231  NIF
  Y
GigabitEthernet3/0/40     0x31       0   0   0    39     0       24   21   40   232  NIF
  Y
GigabitEthernet3/0/41     0x32       0   0   0    40     0       12   22   41   233  NIF
  Y
GigabitEthernet3/0/42     0x33       0   0   0    41     0       4    23   42   234  NIF
  Y
GigabitEthernet3/0/43     0x34       0   0   0    42     0       14   24   43   235  NIF
  Y
GigabitEthernet3/0/44     0x35       0   0   0    43     0       13   25   44   236  NIF
  Y
GigabitEthernet3/0/45     0x36       0   0   0    44     0       16   26   45   237  NIF
  Y
GigabitEthernet3/0/46     0x37       0   0   0    45     0       15   27   46   238  NIF
  Y
GigabitEthernet3/0/47     0x38       0   0   0    46     0       18   28   47   239  NIF
  Y
GigabitEthernet3/0/48     0xd8       0   0   0    47     0       17   29   48   240  NIF
  Y
GigabitEthernet3/1/1      0x3a       1   0   1    48     0       3    4    49   241  NIF
  N
```

```
GigabitEthernet3/1/2      0x3b       1   0   1    49     0      2    5    50   242  NIF
  N
GigabitEthernet3/1/3      0x3c       0   0   0    50     0      3    4    51   243  NIF
  N
GigabitEthernet3/1/4      0x3d       0   0   0    51     0      2    5    52   244  NIF
  N
TenGigabitEthernet3/1/1   0x3e       1   0   1    52     0      3    3    53   245  NIF
  N
TenGigabitEthernet3/1/2   0x3f       1   0   1    53     0      2    2    54   246  NIF
  N
TenGigabitEthernet3/1/3   0x40       1   0   1    54     0      1    1    55   247  NIF
  N
TenGigabitEthernet3/1/4   0x41       1   0   1    55     0      0    0    56   248  NIF
  N
TenGigabitEthernet3/1/5   0x42       0   0   0    56     0      3    3    57   249  NIF
  N
TenGigabitEthernet3/1/6   0x43       0   0   0    57     0      2    2    58   250  NIF
  N
TenGigabitEthernet3/1/7   0x44       0   0   0    58     0      1    1    59   251  NIF
  N
TenGigabitEthernet3/1/8   0x45       0   0   0    59     0      0    0    60   252  NIF
  N
FortyGigabitEthernet3/1/1 0x46       1   0   1    60     0      0    0    61   253  NIF
  N
FortyGigabitEthernet3/1/2 0x47       0   0   0    61     0      0    0    62   254  NIF
  N
TwentyFiveGigE3/1/1       0x48       1   0   1    62     0      0    0    63   255  NIF
  N
TwentyFiveGigE3/1/2       0x49       0   0   0    63     0      0    0    64   256  NIF
  N
AppGigabitEthernet3/0/1   0x4a       1   0   1    24     0     11   30    65   257  NIF
  Y
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

表 *5 : show platform software fed switch active ifm mappings* のフィールドの説明

フィールド	説明
Interface	インターフェイスの名前。
IF_ID	インターフェイス ID。
Inst	インスタンス ID。
Asic	ASIC 番号。
Core	コア番号。
Port	インターフェイスのポート番号。
SubPort	サブポートの数。
MAC	MAC アドレス。
LPN	ASIC 内のローカルポート番号。
GPN	スイッチ内のグローバルシステム番号。

タイプ	インターフェイスのタイプ。
アクティブ	インターフェイスのステータス（アクティブ/非アクティブ）。

show platform software fed switch active ip route

IP ルート情報を表示するには、特権 EXEC モードで **show platform software fed switch active ip route** コマンドを使用します。

show platform software fed switch active ip route

構文の説明

ip	IP コマンドを受け入れます。
route	IPv4転送情報ベース（FIB）の詳細を表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

例

次に、**show platform software fed switch active ip route** コマンドの出力例を示します。

```
Device# show platform software fed switch active ip route
vrf   dest                                          htm            flags   SGT   DGID
MPLS Last-modified            SecsSinceHit
---   ----                                          ---            -----   ---   ----
---- ------------------------ ------------
2     0.0.0.0/0                                     0x78f2fd3488a8 0x0     0     0
    2023/03/14 06:38:18.684            1
2     127.0.0.0/8                                   0x78f2fd351508 0x0     0     0
    2023/03/14 06:38:18.687            1
2     255.255.255.255/32                            0x78f2fd34ebd8 0x0     0     0
    2023/03/14 06:38:18.686            1
2     240.0.0.0/4                                   0x78f2fd350828 0x0     0     0
    2023/03/14 06:38:18.686            1
2     0.0.0.0/32                                    0x78f2fd34cd88 0x0     0     0
    2023/03/14 06:38:18.685            1
2     0.0.0.0/8                                     0x78f2fd350e98 0x0     0     0
    2023/03/14 06:38:18.686            1
0     0.0.0.0/0                                     0x78f2fd345388 0x0     0     0
    2023/03/14 06:39:09.383          352
0     9.24.0.0/32                                   0x78f2fd33e1c8 0x0     0     0
    2023/03/14 06:38:38.930            1
0     9.24.0.1/32                                   0x78f2fd33a5e8 0x0     0     0
    2023/03/14 06:39:09.390            5
0     127.0.0.0/8                                   0x78f2fd3501b8 0x0     0     0
    2023/03/14 06:38:18.686            1
0     255.255.255.255/32                            0x78f2fd34c478 0x0     0     0
    2023/03/14 06:38:18.685            1
0     2.2.2.2/32                                    0x78f2fd3568e8 0x0     2     1
    2023/03/14 06:39:09.383            1
0     9.24.255.255/32                               0x78f2fd344838 0x0     0     0
    2023/03/14 06:38:38.931            1
0     10.64.69.164/32                               0x78f2fd33fac8 0x0     0     0
    2023/03/14 06:39:09.383            1
0     10.77.128.69/32                               0x78f2fd3420a8 0x0     0     0
```

```
    2023/03/14 06:39:09.383           1
0     240.0.0.0/4                                 0x78f2fd34f4d8 0x0     0      0
    2023/03/14 06:38:18.686           1
0     10.106.26.249/32                            0x78f2fd3399a8 0x0     0      0
    2023/03/14 06:39:09.383           1
0     0.0.0.0/32                                  0x78f2fd34a768 0x0     0      0
    2023/03/14 06:38:18.685           1
0     9.24.23.30/32                               0x78f2fd1f2078 0x0     0      0
    2023/03/14 06:38:38.930          24
0     9.24.0.0/16                                 0x78f2fd33af48 0x0     0      0
    2023/03/14 06:38:38.930           1
0     0.0.0.0/8                                   0x78f2fd34fb48 0x0     0      0
    2023/03/14 06:38:18.686           1
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

表 *6 : show platform software fed switch active ip route* のフィールドの説明

フィールド	説明
vrf	VRF ID。
dest	宛先アドレス。
htm	IP ルートのハッシュテーブルマネージャ オブジェクト ポインタ。
SGT	セキュリティグループタグ。
DGID	接続先タグ ID。

show platform software fed switch active sgacl detail

ポリシー情報やカウント情報とともにグローバル適用ステータスを表示するには、特権 EXEC モードで **show platform software fed switch active sgacl detail** コマンドを使用します。

show platform software fed switch active sgacl detail

構文の説明

sgacl	SGACL ハードウェア情報を表示します。
detail	詳細な SGACL 情報を表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

例

次に、**show platform software fed switch active sgacl detail** コマンドの出力例を示します。

```
Device# show platform software fed switch active sgacl detail
Global Enforcement: Off

*Refcnt: for the non-SGACL feature
==================================== DGID Table ====================================
SGT/Refcnt           DGT         DGID         test_cell monitor   permitted      denied
====================================================================================
*/3                    2           1
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

表 *7 : show platform software fed switch active sgacl detail* のフィールドの説明

フィールド	説明
SGT/Refcnt	セキュリティグループのタグ/強化。
DGT	接続先タグ。
DGID	接続先タグ ID。

show platform software fed switch active sgacl port

すべてのインターフェイスのレイヤ2インターフェイス設定項目およびステータスを表示するには、特権 EXEC モードで **show platform software fed switch active sgacl port** コマンドを使用します。

show platform software fed switch active sgacl port

構文の説明

sgacl	セキュリティ グループ アクセス コントロール リスト（SGACL）のハードウェア情報を表示します。
port	ポート構成を指定します。

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

例

次に、**show platform software fed switch active sgacl port** コマンドの出力例を示します。

```
Device# show platform software fed switch active sgacl port

Port             Status     Port-SGT  Trust  Propagate  IngressCache EgressCache
-------------------------------------------------------------------------------
Gi3/0/1        Disabled        0     No      No          No          No
Gi3/0/2        Disabled        0     No      No          No          No
Gi3/0/3        Disabled        0     No      No          No          No
Gi3/0/4        Disabled        0     No      No          No          No
Gi3/0/5        Disabled        0     No      No          No          No
Gi3/0/6        Disabled        0     No      No          No          No
Gi3/0/7        Disabled        0     No      No          No          No
Gi3/0/8        Disabled        0     No      No          No          No
Gi3/0/9        Disabled        0     No      No          No          No
Gi3/0/10       Disabled        0     No      No          No          No
Gi3/0/11       Disabled        0     No      No          No          No
Gi3/0/12       Disabled        0     No      No          No          No
Gi3/0/13       Disabled        0     No      No          No          No
Gi3/0/14       Disabled        0     No      No          No          No
Gi3/0/15       Disabled        0     No      No          No          No
Gi3/0/16       Disabled        0     No      No          No          No
Gi3/0/17       Disabled        0     No      No          No          No
Gi3/0/18       Disabled        0     No      No          No          No
Gi3/0/19       Disabled        0     No      No          No          No
Gi3/0/20       Disabled        0     No      No          No          No
Gi3/0/21       Disabled        0     No      No          No          No
Gi3/0/22       Disabled        0     No      No          No          No
Gi3/0/23       Disabled        0     No      No          No          No
Gi3/0/24       Disabled        0     No      No          No          No
Gi3/0/25       Disabled        0     No      No          No          No
Gi3/0/26       Disabled        0     No      No          No          No
Gi3/0/27       Disabled        0     No      No          No          No
Gi3/0/28       Disabled        0     No      No          No          No
Gi3/0/29       Disabled        0     No      No          No          No
Gi3/0/30       Disabled        0     No      No          No          No
```

```
Gi3/0/31        Disabled        0     No      No          No          No
Gi3/0/32        Disabled        0     No      No          No          No
Gi3/0/33        Disabled        0     No      No          No          No
Gi3/0/34        Disabled        0     No      No          No          No
Gi3/0/35        Disabled        0     No      No          No          No
Gi3/0/36        Disabled        0     No      No          No          No
Gi3/0/37        Disabled        0     No      No          No          No
Gi3/0/38        Disabled        0     No      No          No          No
Gi3/0/39        Disabled        0     No      No          No          No
Gi3/0/40        Disabled        0     No      No          No          No
Gi3/0/41        Disabled        0     No      No          No          No
Gi3/0/42        Disabled        0     No      No          No          No
Gi3/0/43        Disabled        0     No      No          No          No
Gi3/0/44        Disabled        0     No      No          No          No
Gi3/0/45        Disabled        0     No      No          No          No
Gi3/0/46        Disabled        0     No      No          No          No
Gi3/0/47        Disabled        0     No      No          No          No
Gi3/0/48        Disabled        0     No      No          No          No
Gi3/1/1         Disabled        0     No      No          No          No
Gi3/1/2         Disabled        0     No      No          No          No
Gi3/1/3         Disabled        0     No      No          No          No
Gi3/1/4         Disabled        0     No      No          No          No
Te3/1/1         Disabled        0     No      No          No          No
Te3/1/2         Disabled        0     No      No          No          No
Te3/1/3         Disabled        0     No      No          No          No
Te3/1/4         Disabled        0     No      No          No          No
Te3/1/5         Disabled        0     No      No          No          No
Te3/1/6         Disabled        0     No      No          No          No
Te3/1/7         Disabled        0     No      No          No          No
Te3/1/8         Disabled        0     No      No          No          No
Fo3/1/1         Disabled        0     No      No          No          No
Fo3/1/2         Disabled        0     No      No          No          No
Tw3/1/1         Disabled        0     No      No          No          No
Tw3/1/2         Disabled        0     No      No          No          No
Ap3/0/1         Disabled        0     No      No          No          No
```

出力フィールドの意味は自明です。

show platform software fed switch active sgacl vlan

VLAN でのグローバル適用ステータスを表示するには、特権 EXEC モードで **show platform software fed switch active sgacl vlan** コマンドを使用します。

show platform software fed switch active sgacl vlan

構文の説明

sgacl	SGACLハードウェア情報を表示します。
vlan	VLAN 設定を指定します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

例

次に、**show platform software fed switch active sgacl vlan** コマンドの出力例を示します。

```
Device# show platform software fed switch active sgacl vlan

Enforcement enabled:
vlan0
vlan1
vlan2
vlan10
vlan102
vlan192
vlan200
```

show platform software status control-processor brief

CPU とメモリに関する簡潔な情報を表示するには、特権 EXEC モードで **show platform software status control-processor brief** コマンドを使用します。

show platform software status control-processor brief

構文の説明

status	システム ステータスを表示します。
control-processor	制御プロセッサのステータスを表示します。
brief	簡潔にステータスを表示します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

例

次に、**show platform software status control-processor brief** コマンドの出力例を示します。

```
Device# show platform software status control-processor brief

Load Average
 Slot  Status  1-Min  5-Min 15-Min
3-RP0 Healthy   0.03   0.07   0.04

Memory (kB)
 Slot  Status    Total     Used (Pct)     Free (Pct) Committed (Pct)
3-RP0 Healthy  7745656  4178292 (54%)  3567364 (46%)   4755060 (61%)

CPU Utilization
 Slot  CPU   User System   Nice   Idle    IRQ   SIRQ IOwait
3-RP0    0   0.50   0.40   0.00  99.10   0.00   0.00   0.00
         1   0.90   0.50   0.00  98.59   0.00   0.00   0.00
         2   0.40   0.40   0.00  99.20   0.00   0.00   0.00
         3   0.80   0.30   0.00  98.90   0.00   0.00   0.00
         4   0.60   0.30   0.00  99.09   0.00   0.00   0.00
         5   0.70   0.30   0.00  99.00   0.00   0.00   0.00
         6   1.20   0.30   0.00  98.50   0.00   0.00   0.00
         7   0.59   0.39   0.00  99.00   0.00   0.00   0.00
```

出力フィールドの意味は自明です。

show monitor capture <name> buffer

モニターキャプチャバッファまたはキャプチャポイントの内容を表示するには、特権 EXEC モードで **show monitor capture buffer** *name* **buffer** コマンドを使用します。

show monitor capture *name* **buffer**

構文の説明

buffer	指定されたキャプチャバッファの内容を表示します。
name	キャプチャバッファの名前を表します。

コマンド モード

特権 EXEC（#）

コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

次に、**show monitor capture***name***buffer** コマンドの出力例を示します。

```
Device# enable
Device# show monitor capture NewCapture buffer

Starting the packet display ........ Press Ctrl + Shift + 6 to exit

1 0.000000 10.4.1.117 -> 10.5.1.108 ICMP 124 Echo (ping) reply id=0x0008, seq=44279/63404,
 ttl=127
2 0.108862 10.4.1.113 -> 10.5.1.109 ICMP 124 Echo (ping) reply id=0x0008, seq=26717/23912,
 ttl=127
3 0.110106 10.4.1.119 -> 10.5.1.102 ICMP 124 Echo (ping) reply id=0x0008, seq=28341/46446,
 ttl=127
```

出力フィールドの意味は自明です。

timeout（CTS）

応答のタイムアウト（秒数）を設定するには、ポリシーサーバ コンフィギュレーション モードで **timeout** コマンドを使用します。応答のタイムアウトをデフォルトに戻すには、このコマンドの **no** 形式を使用します。

timeout *seconds*
no timeout

構文の説明

seconds	秒単位のタイムアウト値です。有効値は 1 ～ 60 です。

コマンド デフォルト

デフォルトは 5 分です。

コマンド モード

ポリシーサーバ コンフィギュレーション（config-policy-server）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

例

次に、ポリシーサーバのタイムアウトを変更する例を示します。

```
Device# enable
Device# configure terminal
Device(config)# policy-server name ise_server_2
Device(config-policy-server)# timeout 8
```

関連コマンド

コマンド	説明
cts policy-server name	ポリシーサーバの名前を設定し、ポリシーサーバ コンフィギュレーション モードを開始します。

tls server-trustpoint

Transport Layer Security（TLS）のトラストポイントを設定するには、ポリシーサーバ コンフィギュレーション モードで **tls server-trustpoint** コマンドを使用します。TLS 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。

tls server-trustpoint *name*
no tls server-trustpoint

構文の説明

name	トラストポイント名。

コマンド デフォルト

TLS が設定されています。

コマンド モード

ポリシーサーバ コンフィギュレーション（config-policy-server）

コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

使用上のガイドライン

TLS は、Cisco Identity Services Engine（ISE）に接続するためにネットワークデバイスで使用されます。デバイスによる TLS 接続の確立には「Make or Break」のアプローチが使用され、デバイスと Cisco ISE の間に永続的な TLS 接続はありません。TLS 接続が確立された後、その接続を使用して、デバイスから特定の Uniform Resource Locator（URL）に複数の REST API コールを送信できます。すべての REST 要求が処理されると、サーバからの TCP-FIN メッセージによって接続が切断されます。新しい REST API コールを送信するには、サーバとの新しい接続を確立する必要があります。

無効なトラストポイントが設定されている場合、TLS ハンドシェイクは失敗し、サーバが停止中としてマークされます。

例

次に、TLS トラストポイントを設定する例を示します。

```
Device# enable
Device# configure terminal
Device(config)# policy-server name ise_server_2
Device(config-policy-server)# tls server-trustpoint ise_trust
```

関連コマンド

コマンド	説明
cts policy-server name	ポリシーサーバの名前を設定し、ポリシーサーバ コンフィギュレーション モードを開始します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。