CHAPTER 7

Cisco TrustSec コマンドの概要

Cisco TrustSec 特権 EXEC コマンド	
cts change-password	AAA サーバのパスワード変更を開始します
cts credentials	キーストアに CTS デバイス ID およびパスワードを挿入します。
cts refresh	環境、ピアと RBACL ポリシーをリフレッシュします。
cts rekey	CTS SAP キーを再生成します
Cisco TrustSec グローバル コンフィギュレーション コマンド	
cts authorization list	CTS のグローバルな認証の設定を設定します。
cts cache	DRAM および NVRAM への TrustSec 許可および環境データ情報のキャッシュをイネーブルにします。
cts manual	CTS のキーストアの動作を定義します
cts policy layer3	CTS レイヤ 3 トランスポート ゲートウェイ インターフェイスのトラフィック ポリシーおよび例外ポリシーを指定します。
cts role-based	SGT への IP アドレス、L3 インターフェイス、VRF のマッピング。CTS のキャッシュおよび SGACL 強制をイネーブルにします。
cts server	RADIUS サーバのリストの設定を設定します。
cts sgt	ローカル デバイスのセキュリティ グループ タグを設定します。
cts sxp	TCP での SGT 交換を設定します。
CTS Flexible Netflow コマンド	
match flow cts	

CTS インターフェイス コンフィギュレーション コマンド

cts dot1x	CTS dot1x インターフェイス コンフィギュレーション モードを開始します（config-if-cts-dot1x）。
cts layer3	トラフィック ポリシーおよび例外ポリシーをイネーブルにし、CTS のレイヤ 3 トランスポート ゲートウェイ インターフェイスに適用します。
cts manual	（config-if）CTS パラメータのフィードのローカル コンフィギュレーションを指定します
platform cts	TrustSec 出力または入力のリフレクタをイネーブルにします。

CTS dot1x サブモード コマンド

default（cts dot1x インターフェイス コンフィギュレーション サブモード）	CTS dot1x コマンドのデフォルトを復元します。
propagate（cts dot1x サブモード）	dot1x モードの SGT 伝搬をイネーブルまたはディセーブルにします。
sap（cts dot1x インターフェイス サブモード）	dot1x モードの CTS SAP を設定します。
timer（cts do1x インターフェイス サブモード）	CTS のタイマーを設定します。

CTS 手動インターフェイス コンフィギュレーション サブモード コマンド

default（cts 手動インターフェイス コンフィギュレーション サブモード）	CTS 手動モードのデフォルト コンフィギュレーション復元します。
policy（cts 手動インターフェイス コンフィギュレーション サブモード）	手動モードの CTS ポリシーを設定します
propagate（cts 手動インターフェイス コンフィギュレーション サブモード）	手動モードの CTS SGT 伝搬を設定します
sap（cts 手動インターフェイス サブモード）	手動モードの CTS SAP を設定します。

Cisco TrustSec クリア コマンド

clear cts cache	TrustSec キャッシュ ファイルをタイプごとまたはファイル名ごとにクリアするか、すべてのキャッシュ ファイルをクリアします。
clear cts counter	単一 TrustSec インターフェイスまたはすべてのインターフェイスのカウンタをクリアします
clear cts credentials	すべての PAC を含むすべての CTS クレデンシャルをクリアします。
clear cts environment-data	キャッシュからの TrustSec 環境データをクリアします。
clear cts macsec	指定されたインターフェイスの MACsec カウンタをクリアします。
clear cts pac	キーストアから 1 つまたはすべての PAC をクリアします。
clear cts role-based counters	SGT および DGT のロールベース アクセス コントロール強制の統計情報を表示します。

clear cts server	指定された認証サーバを削除します。
Cisco TrustSec Show コマンド	
show cts authorization entries	認可エントリを表示します。
show cts credentials	CTS 認証に使用するクレデンシャルを表示します。
show cts environment-data	CTS 環境データを表示します。
show cts interface	インターフェイスごとの CTS ステートおよび統計情報を表示します。
show cts macsec	インターフェイス単位の暗号 ASIC のパケットカウンタを表示します。
show cts pacs	キーストアの PAC の A-ID および PAC 情報を表示します。
show cts policy peer	TrustSec ピアのピア認可ポリシーを表示します。
show cts policy layer3	CTS レイヤ 3 トランスポートで使用されるトラフィック ポリシーおよび例外ポリシーを表示します。
show cts provisioning	未処理の CTS のプロビジョニング ジョブが表示されます
show cts role-based sgt-map	IP アドレスとセキュリティ グループ タグのマッピングを表示します。
show cts role-based counters	SGT および DGT のロールベース アクセス コントロール強制の統計情報を表示します。
show cts role-based sgt-map	IP と SGT のバインディング、許可リスト、および Netflow 統計情報を表示します。
show cts server-list	AAA サーバとロード バランシング設定のリストを表示します。
show cts sxp	CTS SXP プロトコル情報を表示します。
show platform cts reflector	インターフェイスごとの CTS のリフレクタのステータスを表示します。
エンドポイント アドミッション コントロール（EAC）を設定するコマンド	
aaa accounting	
aaa authorization	
aaa authentication	
order	
priority	
event	
periodic	
timer	
host-mode	
authorization	
accounting	
radius-server host	
authentication port-control	

debug コマンド	
debug authentication event	
debug authentication feature	
debug cts aaa	
debug cts authentication events	
debug cts authorization	
debug cts authorization events	
debug cts authorization rbacl	
debug cts authorization snmp	
debug cts cache	
debug cts coa events	
debug cts dp errors	
debug cts dp info	
debug cts dp packets	
debug cts environment-data	
debug cts environment-data events	
debug cts error	
debug cts fips	
debug cts ha	
debug cts ha core	
debug cts ha infra	
debug cts ifc	
debug cts ifc cache	
debug cts ifc events	
debug cts ifc snmp	
debug cts layer3-trustsec	
debug cts provisioning	
debug cts provisioning event	
debug cts provisioning pak	
debug cts relay event	
debug cts relay pak	
debug cts sap events	
debug cts sap packets	
debug cts sap pakdump	
debug cts server-list	
debug cts states	
debug cts sxp	
debug cts sxp conn	
debug cts sxp error	
debug cts sxp internal	

debug cts sxp mdb	
debug cts sxp message	
debug dot.1x	
debug epm	
debug event	
debug mab	
debug radius	
debug rbm api	
debug rbm cli	
debug rbm bindings	
debug rbm dp errors	
debug rbm dp events	
debug rbm dp packets	
debug rbm platform	
debug rbm policy	

cts authorization list

TrustSec シード デバイスで使用する AAA サーバのリストを指定するには、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** 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 の AAA サーバ グループを指定します。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2 (33) SXI3	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

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。

例

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。

```
Router# cts credentials id Switch1 password Cisco123
Router# configure terminal
Router(config)# aaa new-model
Router(config)# aaa authentication dot1x default group radius
Router(config)# aaa authorization network MLIST group radius
Router(config)# cts authorization list MLIST
Router(config)# aaa accounting dot1x default start-stop group radius
Router(config)# radius-server host 10.20.3.1 auth-port 1812 acct-port 1813 pac key
AbCe1234
Router(config)# radius-server vsa send authentication
Router(config)# dot1x system-auth-control
Router(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 cache

DRAM および NVRAM への TrustSec 認可および環境データ情報のキャッシングをイネーブルにするには、**cts cache** グローバル コンフィギュレーション コマンドを使用します。キャッシングをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
[no] cts cache {
     enable |
     nv-storage {bootflash: [dir] | disk0: [dir] | disk1: [dir] | sup-bootflash: [image]}
}
```

構文の説明

enable	CTS のキャッシュ サポートをイネーブルにします
nv-storage	DRAM キャッシュ更新が不揮発性ストレージに書き込まれるようにし、ネットワーク デバイスの起動時に nv ストレージから DRAM キャッシュが初期入力されるようにします。
bootflash: *dir*	nv ストレージの位置としてブートフラッシュ ディレクトリを指定します。
disk0: *dir*	nv ストレージの位置としてディスク 0 ディレクトリを指定します。
disk1: *dir*	nv ストレージの位置としてディスク 1 ディレクトリを指定します。
sup-bootflash: *image*	nv ストレージの位置としてスーパーバイザ ブートフラッシュのディレクトリを指定します。

デフォルト

デフォルトはキャッシュはディセーブルです。

コマンド モード

グローバル コンフィギュレーション（config）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(33) SXI	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。
12.2(50) SY	PMK キャッシュのサポートは、Catalyst 6500 シリーズ スイッチに追加されます。

使用上のガイドライン

cts cache コマンドは認証、許可、および環境データ情報の DRAM へのキャッシュをイネーブルにします。キャッシングは、認証および認可によって取得された情報のメンテナンスおよび再使用のためです。キーストアはデバイス自身のクレデンシャル（パスワード、証明書、PAC）のセキュアなストレージを、ソフトウェアまたは専用のハードウェア コンポーネントで提供します。専用のハードウェア キーストアがない場合、ソフトウェア エミュレーション キーストアは DRAM および NVRAM を使用して作成されます。

Cisco TrustSec では、各デバイスが信頼できる AAA サーバ（Cisco Secure ACS 5.1 以降）を使用して各自のネイバーを認証および認可してから、TrustSec ネットワークへのアクセスが承認されるように要求することで、ネットワーク デバイスのセキュア クラウドを作成します。認証および認可が完了すると、情報はしばらくの間有効です。キャッシングがイネーブルになっている場合、その情報は再利用できるため、ネットワーク デバイスは ACS に接続しなくてもリンクを起動できるため、リブート時に

CTS クラウドが素早く形成でき、ネットワークのアベイラビリティが向上して、ACS の負荷が低減します。キャッシングは揮発性メモリ（情報はリブート時に消える）または不揮発性メモリ（情報はリブート後も存続）に保存できます。

例

次に、キャッシュ サポートをイネーブルにする例を示します。

```
Router# config t
Router(config)# cts cache nv-storage disk0:
Router(config)# cts cache enable
```

関連コマンド

コマンド	説明
clear cts cache	キーストアの内容をクリアします。
show cts keystore	キーストアの内容を表示します。
cts rekey	
cts credentials	

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 サーバの識別ストリングを指定します
key	プロビジョニングに使用する RADIUS キーを指定します
source	要求パケットの送信元アドレスのインターフェイスを指定します
interface_list	表示されたリストあたりのインターフェイス タイプおよび ID パラメータを指定します。

デフォルト

このコマンドにはデフォルトはありません。

コマンド モード

特権 EXEC（#）

サポートされるユーザ ロール

Administrator

コマンドの種類

次のコマンド構文を使用します

コマンド履歴

リリース	変更点
12.2(50) SY	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

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。

（注） **cts change-password** は、Cisco Secure ACS の 5.1 以降のバージョンでサポートされています。

デュアル スーパーバイザ シャーシの Catalyst 6500 では、2 つめのスーパーバイザのラインカードを挿入するときに、ハードウェア ベースのキーストアを手動で同期する必要があります。パスワード変更プロセスにより、アクティブおよびスタンバイ スーパーバイザに、同じデバイス パスワードが設定される場合があります。

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。クレデンシャルを削除するには、**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。

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

Administrator

コマンド履歴

リリース	変更点
12.2(33) SXI	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

TrustSec ネットワーク デバイス アドミッション コントロール（NDAC）認証で使用する場合、**cts credentials** コマンドは、EAP-FAST を使用して別の Cisco TrustSec デバイスと認証を行う際に、このスイッチが使用する Cisco TrustSec デバイス ID およびパスワードを指定します。CTS のクレデンシャル情報は startup-config ではなくキーストアに保存されているため、CTS のクレデンシャル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 CTS 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。これらのクレデンシャルは、キーストアで保存され、running-config を保存する必要性がなくなります。CTS 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） CTS 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。

例

次に、CTS デバイス ID を himalaya、パスワードを cisco に設定する例を示します。

```
Router# cts credentials id himalaya password cisco
```

```
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、CTS バイス ID を atlas、パスワードを cisco123 に変更する例を示します。

```
Router# cts credentials id atlas pacssword cisco123
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、CTS デバイス ID およびパスワード ステートを表示する例を示します。

```
Router# show cts credentials
CTS password is defined in keystore, device-id = atlas
```

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 dot1x

CTS dot1x 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-dot1x）を開始してインターフェイスの TrustSec 再認証タイマーを設定するには、**cts dot1x** コマンドを使用します。インターフェイス タイマーをディセーブルにするには、このコマンドの **no** 形式を使用します。

[**no**] **cts dot1x**

構文の説明　このコマンドには、引数またはキーワードはありません。

デフォルト　インターフェイスの CTS dot1x コンフィギュレーションはデフォルトではディセーブルです。

コマンド モード　インターフェイス コンフィギュレーション（config-if）

サポートされるユーザ ロール　Administrator

コマンド履歴

リリース	変更点
12.2 (33) SXI3	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン　TrustSec dot1x 再認証タイマーを設定する前に、インターフェイス コンフィギュレーション モードからインターフェイスからの dot1x をグローバルに設定します。CTS dot1x の設定は、TrustSec EAC プロセスではなく TrustSec NDAC を制御します。

例　次の例では、Catalyst 6500 シリーズ スイッチは最初に dot1x インターフェイス コンフィギュレーション モードをイネーブルにせずに CTS コンフィギュレーション モードを開始します。

```
Router(config-if)# cts dot1x
Warning: Global dot1x is not configured, CTS will not run until dot1x is enabled
. (Gi3/1)

Router(config-if-cts-dot1x)# ?
CTS dot1x configuration commands:
  default  Set a command to its defaults
  exit     Exit from CTS dot1x sub mode
  no       Negate a command or set its defaults
  timer    CTS timer configuration
```

関連コマンド

コマンド	説明
default timer reauthentication（cts インターフェイス）	CTS dot1x 再認証タイマーをデフォルト値にリセットします。
timer reauthentication（cts インターフェイス）	CTS dot1x 再認証タイマーを設定します。
show cts interface	CTS インターフェイスのステータスおよび設定を表示します。
show dotx interface	IEEE 802.1x の設定と統計情報を表示します。

default timer reauthentication（cts インターフェイス）

CTS dot1x 認証タイマーをデフォルト値にリセットするには、CTS インターフェイス コンフィギュレーション モードで **default timer reauthentication** コマンドを使用します。

default timer reauthentication

構文の説明

timer reauthentication	CTS 認証タイマーをデフォルト値に設定します。

デフォルト

3600 秒

コマンド モード

CTS インターフェイス コンフィギュレーション（config-if-cts-dot1x）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(33) SXI	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

CTS 再認証タイマーのデフォルト値はグローバルな dot1x 再認証のデフォルト（3600 秒）です。このタイマーが満了すると、デバイスは、CTS のネットワークに再認証します（NDAC）。

例

次に、グローバル デフォルト値に CTS 再認証タイマーをリセットする例を示します。

```
Router # configure terminal
Router(config)# interface gigabitEthernet 3/1
Router(config-if)# cts dot1x
Router(config-if-cts-dot1x)# default timer reauthentication
```

関連コマンド

コマンド	説明
cts dot1x	CTS dot1x インターフェイス コンフィギュレーション モードを開始します（config-if-cts-dot1x）。
timer reauthentication（cts インターフェイス）	CTS 再認証タイマーを設定します。
show cts interface	CTS インターフェイスのステータスおよび設定を表示します。
show dotx interface	IEEE 802.1x の設定と統計情報を表示します。

timer reauthentication（cts インターフェイス）

再認証タイマーを設定するには、CTS インターフェイス コンフィギュレーション モードで **timer reauthentication** コマンドを使用します。タイマーをディセーブルにするには、このコマンドの **no** 形式を使用します。

[**no**] **timer reauthentication** *seconds*

構文の説明

reauthentication *seconds*	再認証タイマーを設定します。

デフォルト

なし

コマンド モード

CTS インターフェイス コンフィギュレーション（config-if-cts-dot1x）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(33) SXI	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドは、TrustSec 再認証タイマーを設定します。このタイマーが満了すると、デバイスは、CTS のネットワークに再認証します（NDAC）。

例

次に、再認証タイマーを 44 秒に設定する例を示します。

```
Router(config-if-cts-dot1x)# timer reauthentication 44
```

関連コマンド

コマンド	説明
cts dot1x	CTS dot1x インターフェイス コンフィギュレーション モードを開始します（config-if-cts-dot1x）。
default timer reauthentication（cts インターフェイス）	CTS dot1x 再認証タイマーをデフォルト値にリセットします。
show cts interface	CTS インターフェイスのステータスおよび設定を表示します。
show dotx interface	IEEE 802.1x の設定と統計情報を表示します。

cts layer3

CTS レイヤ 3 トランスポート ゲートウェイ インターフェイスをイネーブルに設定し、例外ポリシーとトラフィック ポリシーを適用するには、**cts layer 3** インターフェイス コンフィギュレーション コマンドを使用します。

cts layer3 {**ipv4** | **ipv6**} {**policy** | **trustsec forwarding**}

構文の説明

ipv4 | **ipv6**	IPv4 または IPv6 のいずれかを指定します
policy	ゲートウェイ インターフェイスにトラフィック ポリシーおよび例外ポリシーを適用します。
trustsec forwarding	ゲートウェイ インターフェイスの CTS レイヤ 3 トランスポートをイネーブルにします。

デフォルト

デフォルトでは CTS レイヤ 3 トランスポートは有効になっていません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(50) SY	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

いずれのトラフィック コマンドおよび例外コマンドを CTS レイヤ 3 ゲートウェイに適用するかを指定するには、**cts policy layer3** グローバル コンフィギュレーション コマンドを使用します。CTS レイヤ 3 ゲートウェイ インターフェイスをイネーブルにして、トラフィック ポリシーおよび例外ポリシーを適用するには、**cts layer3** インターフェイス コンフィギュレーション コマンドを使用します。トラフィック ポリシーおよび例外ポリシーの詳細については、cts policy layer3 を参照してください。

例

次に、CTS レイヤ 3 トランスポート ゲートウェイ インターフェイスをイネーブルにする例を示します。

```
Router# config t
Router(config)# interface gigabitEthernet 6/1
Router(config-if)# cts layer3 ipv4 trustsec forwarding
Router(config-if)# cts layer3 ipv4 trustsec
Router(config-if)# cts layer3 ipv4 policy
```

関連コマンド

コマンド	説明
cts policy layer3	CTS レイヤ 3 トランスポートのトラフィック ポリシーおよび例外ポリシーを指定します。
show cts policy layer3	CTS レイヤ 3 トランスポート コンフィギュレーションで使用されるトラフィック ポリシーおよび例外ポリシーの名前を表示します。

cts manual

TrustSec 手動インターフェイス コンフィギュレーション サブモードを開始するには、**cts manual** インターフェイス コンフィギュレーション コマンドを使用します。

cts manual

構文の説明　このコマンドの構文はありません

デフォルト　このコマンドにはデフォルトはありません。

コマンド モード　インターフェイス コンフィギュレーション（config-if）

サポートされるユーザ ロール　Administrator

コマンド履歴

リリース	変更点
12.2(50) SY	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

リンクにポリシーおよびセキュリティ アソシエーション プロトコル（SAP）を設定する TrustSec 手動インターフェイス コンフィギュレーション サブモードを開始するには、**cts manual** インターフェイス コンフィギュレーション コマンドを使用します。**sap** または **policy** サブ コマンドが設定されていない場合、TrustSec にインターフェイスが設定されていないように見えます。

CTS 手動モードが設定された場合、802.1X 認証はリンクで実行されません。ポリシーを定義し、リンクに適用するには、**policy** サブコマンドを使用します。デフォルトは no policy です。MACsec リンク間暗号化を設定するには、SAP ネゴシエーション パラメータを定義する必要があります。デフォルトは no SAP です。同じ SAP PMK をリンクの両端で設定する必要があります（つまり、共有秘密）。

例

次に、CTS 手動モードを開始する例を示します。

```
router# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
router(config)# interface giga 2/1
router(config-if)# cts manual
router(config-if-cts-manual)# ?
CTS manual configuration commands:
  default    Set a command to its defaults
  exit       Exit from CTS manual sub mode
  no         Negate a command or set its defaults
  policy     CTS policy for manual mode
  propagate  CTS SGT Propagation configuration for manual mode
  sap        CTS SAP configuration for manual mode
```

関連コマンド

コマンド	説明
policy（cts 手動インターフェイス コンフィギュレーション サブモード）	
sap（cts 手動インターフェイス サブモード）	
show cts interface	

cts policy layer3

Cisco Secure ACS が使用できない場合、システムで CTS レイヤ 3 トランスポート用にトラフィック ポリシーと例外ポリシーを指定するには、**cts policy layer3** グローバル コンフィギュレーション コマンドを使用します。

[**no**] **cts policy layer3 ipv4** {[**exception** *access_list*] | [**traffic** *access_list*]}

[**no**] **cts policy layer3 ipv6** {[**exception** *access_list*] | [**traffic** *access_list*]}

構文の説明

ipv4 exception *access_list*	（任意）IPv4 L3 のトラフィック ポリシーに例外を定義する定義済みの ACL を指定します。
ipv4 traffic *access_list*	IPv4 TrustSec をイネーブルにしたサブネットおよびゲートウェイをリストした定義済みの ACL を指定します。
ipv6 exception *access_list*	（任意）IPv6 L3 のトラフィック ポリシーに例外を定義する定義済みの ACL を指定します。
ipv6 traffic *access_list*	IPv6 TrustSec をイネーブルにしたサブネットおよびゲートウェイをリストした定義済みの ACL を指定します

デフォルト

デフォルトは no policy 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）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(50) SY	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

CTS レイヤ 3 トランスポート機能は、TrustSec をイネーブルにしたネットワーク セグメントからのレイヤ 2 SGT タグ付きトラフィックが、アプリケーションにより非 TrustSec ネットワーク セグメントを経由して転送され、指定した CTS レイヤ 3 ゲートウェイでレイヤ 3 カプセル化が解除されるようにできます。トラフィック ポリシーは、すべての TrustSec をイネーブルにしたサブネットおよびこれに対応するゲートウェイ アドレスをリストしたアクセス リストです。例外ポリシーは、CTS レイヤ 3 トランスポートのカプセル化を適用しないトラフィックをリストするアクセス リストです。たとえば、ポリシーの取得に使用される RADIUS パケットは、クリアで送信する必要があります。

トラフィック ポリシーおよび例外ポリシーは、**cts policy layer3 {ipv4 | ipv6} traffic** *access_list* and the **cts policy layer3 {ipv4 | ipv6} exception** *access_list* グローバル コンフィギュレーション コマンドで指定します。CTS L3 ゲートウェイ インターフェイスにトラフィック ポリシーおよび例外ポリシーを適用するには、**cts layer3 {ipv4 | ipv6} policy** インターフェイス コンフィギュレーション コマンドを使用します。CTS L3 ゲートウェイ インターフェイスをイネーブルにするには、**cts layer3 {ipv4 | ipv6} trustsec forwarding** インターフェイス コンフィギュレーション コマンドを使用します。

次のような使用上のガイドラインおよび制限を考慮して Cisco TrustSec レイヤ 3 SGT トランスポートを設定します。

- Cisco TrustSec レイヤ 3 SGT トランスポート機能はハードウェア暗号化をサポートするポートだけで設定できます。
- Cisco TrustSec レイヤ 3 SGT トランスポートのトラフィック ポリシーおよび例外ポリシーには次の制限があります。
  - ポリシーは、IP 拡張または IP 名前付き拡張 ACL として設定する必要があります。
  - ポリシーには **deny** エントリを含めることはできません。
  - 同じ ACE がトラフィック ポリシーおよび例外ポリシーの両方に存在する場合は、例外ポリシーが優先されます。Cisco TrustSec レイヤ 3 カプセル化は、その ACE に一致するパケットで実行されます。
- トラフィック ポリシーおよび例外ポリシーは認証サーバからダウンロード（ご使用の Cisco IOS Release でサポートされている場合）するか、または **ip access-list global** コンフィギュレーション コマンドを使用して、デバイスに手動で設定できます。ポリシーは次のルールに基づいて適用されます。
  - トラフィック ポリシーまたは例外ポリシーが認証サーバからダウンロードされる場合、手動で設定されたトラフィック ポリシーまたは例外ポリシーよりも優先されます。
  - 認証サーバが使用できず、トラフィック ポリシー、および例外ポリシーの両方を手動で設定すると、手動で設定されたポリシーが使用されます。
  - 認証サーバが使用できず、トラフィック ポリシーを例外ポリシーなしで設定すると、例外ポリシーは適用されません。Cisco TrustSec レイヤ 3 カプセル化がトラフィック ポリシーに基づいてインターフェイスに適用されます。
  - 認証サーバが使用できず、トラフィック ポリシーが手動で設定されていない場合は、Cisco TrustSec レイヤ 3 カプセル化がインターフェイスで実行されません。

例

次に、リモート Cisco TrustSec ドメインにレイヤ 3 SGT トランスポートを設定する例を示します。

```
Router# configure terminal
Router(config)# ip access-list extended traffic-list
Router(config-ext-nacl)# permit ip any 10.1.1.0 0.0.0.255
Router(config-ext-nacl)# exit
Router(config)# ip access-list extended exception-list
Router(config-ext-nacl)# permit ip any 10.2.2.0 0.0.0.255
Router(config-ext-nacl)# exit
Router(config)# cts policy layer3 ipv4 traffic traffic-sgt
Router(config)# cts policy layer3 ipv4 exception exception-list
Router(config)# interface gi2/1
Router(config-if)# cts layer3 trustsec ipv4 forwarding
Router(config-if)# shutdown
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# exit
```

関連コマンド

コマンド	説明
cts layer3	トラフィック ポリシーおよび例外ポリシーをイネーブルにし、CTS のレイヤ 3 トランスポート ゲートウェイ インターフェイスに適用します。
show cts policy layer3	CTS レイヤ 3 トランスポートで使用されるトラフィック ポリシーおよび例外ポリシーを表示します。

cts refresh

すべてまたは特定の CTS ピアの TrustSec ピア認可ポリシーをリフレッシュするか、認証サーバによりスイッチ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 environment-data

cts refresh policy {**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。すべてのピア ポリシーを更新するには、ID を指定しないで Enter を押します。
sgt *sgt_number*	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。すべてのセキュリティ グループ タグ ポリシーをリフレッシュするには、SGT 番号を指定せずに Enter を押します。
default	デフォルトの SGACL ポリシーをリフレッシュします。
unknown	未知の SGACL ポリシーをリフレッシュします。

デフォルト

なし

コマンド モード

特権 EXEC（#）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(33) SXI	このコマンドは、Catalyst 6500 シリーズ スイッチで **cts policy refresh** として追加されました。
12.2(50) SY	このコマンドは、Catalyst 6500 シリーズ スイッチで **cts refresh policy** に変更されました。**sgt**、**default**、および **unknown** キーワードが追加されました。

使用上のガイドライン

すべての TrustSec ピアのピア認可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 はピア認可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。

例

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

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

次に、すべてのピアの TrustSec ピア認可ポリシーを表示する例を示します。

```
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
cts refresh	
clear cts policy	CTS ポリシーをすべてクリアするか、ピア ID または SGT により単独でクリアします。
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 Pairwise Master Key を再生成するには、**cts rekey** 特権 EXEC コマンドを使用します。

構文の説明

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

デフォルト

デフォルト値はありません。

コマンド モード

特権 EXEC（#）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(50) SY	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。
IOS-XE 3.3.0 SG	このコマンドが、Catalyst 4500 シリーズ スイッチに追加されました。
IOS 15.0(1) SE	このコマンドが、Catalyst 3000 シリーズ スイッチに追加されました。

使用上のガイドライン

SAP の Pairwise Master Key（PMK）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** CTS 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。

例

次の例では、指定したインターフェイスの PMK を再生成します。

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

関連コマンド

コマンド	説明
sap（cts 手動インターフェイス サブモード）	
show cts	

cts role-based

SGT のインポジション、TrustSec NetFlow パラメータと SGACL 強制を手動で設定するには、**cts role-based** グローバル コンフィギュレーション コマンドを使用します。コンフィギュレーションを削除するには、コマンドの **no** 形式を使用します。

[**no**] **cts role-based enforcement** [**vlan-list** {*vlan-ids* | **all**}]

[**no**] **cts role-based** {**ip** | **ipv6**} **flow monitor fnf-ubm dropped**

[**no**] **cts role-based ipv6-copy**

[**no**] **cts role-based l2-vrf** *instance_name* **vlan-list** *vlan-ids* [**all**]

[**no**] **cts role-based permissions default** {*access-list* | **ipv4** | **ipv6**} *access-list access-list . . .*

[**no**] **cts role-based permissions from** {*sgt* | **unknown to** {*sgt* | **unknown**}} {*access-list* | **ipv4** | **ipv6**} *access-list , access-list, . . .*

[**no**] **cts role-based sgt-caching vlan-list {***vlan_ids* | **all}**

[**no**] **cts role-based sgt-caching with-enforcement**

[**no**] **cts role-based sgt-map** {i*pv4_netaddress* | *ipv6_netaddress*} | **sgt** *sgt_number*

[**no**] **cts role-based sgt-map** {i*pv4_netaddress/prefix* | *ipv6_netaddress/prefix*} | **sgt** *sgt_number*

[**no**] **cts role-based sgt-map host** {i*pv4_hostaddress* | *ipv6_hostaddress* | **sgt** *sgt_number*

[**no**] **cts role-based sgt-map vrf** *instance_name* {*ip4_netaddress* | *ipv6_netaddress* | **host** {*ip4_address* | *ip6_address*}] **sgt** *sgt_number*

[**no**] **cts role-based sgt-map interface** interface_type *slot*/*port* {**security-group** | **sgt**} *sgt_number*

[**no**] **cts role-based sgt-map vlan-list [***vlan_ids*| **all]** *slot*/*port* **sgt** *sgt_number*

構文の説明

l2-vrf *instance_name*	（任意）レイヤ 2 VRF インスタンス名を指定します。
enforcement	すべてのレイヤ 3 CTS インターフェイスのローカル デバイスの SGACL 強制をイネーブルにします。
interface interface_type	指定 SGT はこの論理または物理レイヤ 3 インターフェイスからのトラフィックにマッピングされます。
vlan-list *vlan-ids*	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。
all	（任意）すべての VLAN ID を指定します。
with-enforcement	SGACL 強制がイネーブルの SGT キャッシングをイネーブルにします。
sgt-map *ipv4_netaddress* | *ipv6_netaddress*	（任意）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。
sgt-map *ipv4_netaddress/prefix* | *ipv6_netaddress/prefix*	（任意）SGT が、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マッピングされるように指定します。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。*（0 ～ 128）*

sgt-map host *ipv4_hostaddress* | *ipv6_hostaddress*	指定したホスト IP アドレスと指定した SGT をバインドします。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。
sgt *sgt_number*	（0 ～ 65,535）。セキュリティ グループ タグ（SGT）番号を指定します。
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。

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

Administrator

コマンド履歴

リリース	変更点
12.2 (33) SXI3	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。
12.2 (50) SG7	このコマンドが、Catalyst 4000 シリーズ スイッチに追加されました。
12.2 (53) SE2	このコマンドが、Catalyst 3750(E)、3560(E)、および 3750(X) シリーズ スイッチに追加されました（**vrf** または IPv6 サポートなし）。
12.2(50) SY	次のキーワードは、Catalyst 6500 シリーズ スイッチに追加されました。 • [no] cts role-based enforcement • [no] cts role-based ip flow monitor user-defined-monitor dropped • [no] cts role-based ipv6 flow monitor user-defined-monitor dropped • [no] cts role-based ipv6 copy • [no] cts role-based permissions
15.0(0) SY	次のキーワードは、Catalyst 6500 シリーズ スイッチに追加されました。 • [no] cts role-based sgt-map interface • [no] cts role-based sgt-map vlan-list

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 ARP インスペクション、DHCP スヌーピング、ホスト トラッキングがスイッチで使用できない場合、**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
- レイヤ 3 物理または論理インターフェイス

単一のホスト アドレスと SGT のバインディング

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 アドレスが一致した場合に、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 強制用にスイッチ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。

ネットワークまたはサブネットワーク アドレスと SGT のバインディング

cts role-based sgt-map *ipv4_netaddress* **|** *ipv6_netaddress* および **cts role-based sgt-map** *ipv4_subnetaddress/prefix* **|** *ipv6_subnetaddress/prefix* コマンドは、指定したネットワーク アドレス範囲内のパケットに、指定した 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。

VRF と SGT のバインディング

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。VRF コンテキストの設定はこのマニュアルの範囲外です。**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。

VLAN と SGT のマッピング

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、スイッチ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。

レイヤ 3 インターフェイス マッピング（L3IF）

cts role-based sgt-map interface コマンドは、指定したレイヤ 3 論理インターフェイスをセキュリティ グループの名前または SGT にバインドします。セキュリティ グループの名前に SGT をマッピングするセキュリティ グループ情報テーブルは、TrustSec 環境データと一緒に認証サーバからダウンロードされます。**cts role-based sgt-map interface security-group** コマンドは、セキュリティ グループの名前のテーブルが使用できない場合は拒否されます。

セキュリティ グループのテーブルが初めてダウンロードされるか更新されるたびに、すべての L3IF マッピングは再処理されます。指定されたインターフェイスを経由する出力パスを持つすべてのネットワーク プレフィックスに対して、IP-SGT バインディングが追加、更新、または削除されます。

バインディング送信元プライオリティ

TrustSec は完全優先方式で、マスター バインディング データベースの IP-SGT バインディング ソース間の競合を解決します。たとえば、SGT も **policy** {**dynamic identity** *peer-name* | **static sgt** *tag*} cts interface コマンドでインターフェイスに適用される場合があります（アイデンティティ ポート マッピング）。現在の優先順位の適用順序は、最小から最大まで、次のとおりです。

1. VLAN：VLAN-SGT マッピングが設定された VLAN 上のスヌーピングされた ARP パケットから学習されたバインディング。
2. CLI：**cts role-based sgt-map** グローバル コンフィギュレーション コマンドの IP-SGT 形式を使用して設定されたアドレス バインディング。

3. レイヤ 3 インターフェイス：（L3IF）一貫した L3IF-SGT マッピングやアイデンティティ ポート マッピングを使用する 1 つ以上のインターフェイスを通るパスを持つ FIB 転送エントリが原因で追加されたバインディング。
4. SXP：SXP ピアから学習されたバインディング。
5. IP_ARP：タグ付けされた ARP パケットが CTS 対応リンクで受信されたときに学習されたバインディング。
6. LOCAL：EPM とデバイス トラッキングによって学習された認証済みホストのバインディング。このタイプのバインディングには、L2 [I]PM が設定されたポートの ARP スヌーピングによって学習された個々のホストも含まれます。
7. INTERNAL：ローカルで設定された IP アドレスとデバイス独自の SGT 間のバインディング。

L2 VRF の割り当て

[**no**] **cts role-based l2-vrf vrf-name vlan-list** {**vlan-list** | **all**} グローバル コンフィギュレーション コマンドでは、**vlan-list** 引数には単一の VLAN ID、カンマで区切った VLAN ID のリスト、またはハイフンで区切った VLAN ID の範囲を指定できます。

キーワード **all** 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。キーワード **all** 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 に複数回実行する場合、入力される連続した各コマンドは、指定された VRF に指定された 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 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。

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 アドレスの設定が解除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。

ロールベースの強制

システムの CTS をイネーブルにしたレイヤ 3 インターフェイスの SGACL 強制をグローバルにイネーブルまたはディセーブルにするには、[**no**] **cts role-based enforcement** コマンドを使用します。

（注）　CTS の CLI コマンドの説明に表示されるロールベース アクセス コントロールおよびロールベース ACL は、Cisco TrustSec マニュアルのセキュリティ グループ アクセス コントロール リスト（SGACL）に相当します。

VLAN 強制

SVI インターフェイス上でのレイヤ 2 スイッチド パケットと L3 スイッチド パケットに対する SGACL 強制をイネーブルまたはディセーブルにするには、[**no**] **cts role-based enforcement vlan-list** {*vlan-ids* | **all**} コマンドを使用します。

vlan-ids 引数には単一の VLAN ID、VLAN ID リスト、または VLAN ID 範囲を指定できます。複数のエントリはハイフン「-」またはカンマ「,」で区切ります。

キーワード **all** は、プラットフォームによってサポートされている VLAN の全範囲と同等です（たとえば、Catalyst 6500 VLAN 範囲は 1 ～ 4094 です）。複数のコマンドを発行すると、付加的な効果があります。SGACL が指定されたすべてのリストのすべての VLAN に適用されます。キーワード **all** は、不揮発性生成（NVGEN）プロセスで保持されません。

（注） デフォルトでは、SGACL 強制は VLAN でイネーブルではありません。VLAN の SGACL 強制をイネーブルにするためには、**cts role-based enforcement vlan-list** コマンドを発行する必要があります。

（注） ロールベース アクセス コントロール（RBAC）が強制されている VLAN で SVI がアクティブである場合、RBAC はその VLAN 内のレイヤ 2 およびレイヤ 3 の両方のスイッチド パケットに対して強制されます。レイヤ 3 スイッチングは SVI を使用しない VLAN 内では使用できないため、SVI を使用しない場合、RBAC はレイヤ 2 スイッチド パケットのみに対して強制されます。

Flexible NetFlow

標準の 5 タプル フロー オブジェクトを使用してフロー レコードに SGT および DGT フロー オブジェクトが設定されている場合、Flexible NetFlow は、SGACL 強制によってドロップされたパケットに対応できます

flow record および **flow exporter** グローバル コンフィギュレーション　コマンドを使用してフロー レコードおよびフロー エクスポータを設定してから、それらを **flow monitor** コマンドを使用してフロー モニタに追加します。**show flow** show コマンドを使用して設定を確認します。

SGACL のドロップされたパケットだけを収集するには、**[no] cts role-based** {**ip** | **ipv6**} **flow monitor dropped** グローバル コンフィギュレーション コマンドを使用します。

Flexible NetFlow の概要および設定の詳細については、次のマニュアルを参照してください。

『Getting Started with Configuring Cisco IOS Flexible NetFlow』

http://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/get_start_cfg_fnflow.html

『Cisco IOS Flexible Netflow Configuration Guide, Release 15.0SY』

http://www.cisco.com/en/US/docs/ios-xml/ios/fnetflow/configuration/15-0sy/fnf-15-0sy-book.html

例

次の例では、Catalyst 4500 シリーズ スイッチが、ホスト IP アドレス 10.1.2.1 を SGT 3 に、10.1.2.2 を SGT 4 にバインドしてから、**show** コマンドで確認します。これらのバインディングは、SXP によって SGACL 強制のスイッチに転送されます。

```
cat4k# (config)# cts role-based sgt-map host 10.1.2.1 sgt 3
cat4k(config)#cts role-based sgt-map host 10.1.2.2 sgt 4

cat4k# show cts role-based sgt-map all
Active IP-SGT Bindings Information

IP Address    SGT  Source
============================================
10.1.2.1       3   CLI
10.1.2.2       4   CLI

IP-SGT Active Bindings Summary
============================================
Total number of CLI      bindings = 2
Total number of active   bindings = 2
```

次の例では、Catalyst 6500 シリーズで、VLAN 57、および 89 ～ 101 を VRF l2ipv4 に割り当てます。VRF は **vrf** グローバル コンフィギュレーション コマンドで作成済みです。

```
Cat6k(config)# cts role-based l2-vrf l2ipv4 vlan-list 57, 89-101
```

関連コマンド

コマンド	説明
cts sxp	ネットワーク デバイスに SXP を設定します。
cts sgt	ローカル デバイスのセキュリティ グループ タグを設定します。
show cts role-based sgt-map	ロールベース アクセス コントロール情報を表示します

cts server

RADIUS サーバ グループのロード バランシングを設定するには、グローバル コンフィギュレーション モードで **cts server** コマンドを使用します。ロード バランシングをディセーブルにするには、このコマンドの **no** 形式を使用します。

[**no**] **cts server deadtime** *timer_secs*

[**no**] **cts server key-wrap enable**

[**no**] **cts server load-balance method least-outstanding** [**batch-size** *transactions*] [**ignore-preferred-server**]

[**no**] **cts server test** {*ip4_address* | **all**} {**deadtime** *seconds* | **enable** | **idle-time** *minutes*}

構文の説明

deadtime *timer_secs*	いったん停止中としてマークされたグループ内のサーバを、どのくらいの期間、サービス用に選択してはいけないかを指定します。デフォルトは 20 秒です。指定できる範囲は 1 ～ 864000 です。
load-balance method least-outstanding	Cisco TrustSec プライベート サーバ グループに RADIUS ロード バランシングをイネーブルにし、最も未処理のトランザクションが少ないサーバを選択します。デフォルトでは、ロード バランシングは適用されません。
batch-size *transactions*	（任意）バッチごとに割り当てられるトランザクションの数。デフォルトの *transactions* は 25 です。 **（注）** バッチ サイズがスループットと CPU の負荷に影響する場合があります。デフォルト バッチ サイズの 25 の使用を推奨します。これは、CPU の負荷に悪影響を及ぼさない、高スループットに最適化されているためです。
ignore-preferred-server	（任意）セッション全体を通じて同じサーバを使用しないようにスイッチに指示します。
test {*ip4_address* | **all** {**deadtime** *seconds* | **enable** | **idle-time** *minutes* } }	指定された RADIUS サーバまたはダイナミック サーバ リスト内のすべてのサーバに対してサーバ存続性テストを設定します。デフォルトでは、テストはすべてのサーバに対してイネーブルになっています。デフォルトの **deadtime** は 20 秒です。指定できる範囲は 1 ～ 864000 秒です。デフォルトの **idle-time** は 60 秒で、範囲は 1 ～ 14400 秒です。
key-wrap enable	TrustSec の RADIUS サーバ通信に対して、AES キー ラップの暗号化をイネーブルにします。

デフォルト

Deadtime	20 秒
Batch-size	25 トランザクション
test idle-time	60 秒

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　Administrator

コマンド履歴

リリース	変更点
12.2(33) SXI	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。
12.2(50) SY	**key-wrap** キーワードは、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

スイッチを FIPS モードで稼働させる場合は、**key-wrap** キーワードを使用します。

RADIUS サーバ ロード バランシングの情報は次の URL で入手できます。

http://www.cisco.com/en/US/docs/ios/12_2sb/feature/guide/sbrdldbl.html

例

次に、サーバ設定を設定して Cisco TrustSec サーバ リストを表示する例を示します。

```
Router# configure terminal
Router(config)# cts server load-balance method least-outstanding batch-size 50
ignore-preferred-server
Router(config)# cts server test all deadtime 20
Router(config)# cts server test all enable
Router(config)# cts server test 10.15.20.102 idle-time 120
Router(config)# exit

Router# show cts server-list
CTS Server Radius Load Balance = ENABLED
  Method     = least-outstanding
  Batch size = 50
  Ignore preferred server
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: 10.15.20.102, port 1812, A-ID  87B3503255C4384485BB808DC24C6F55
                Status = ALIVE
                auto-test = TRUE, idle-time = 120 mins, deadtime = 20 secs
Installed list: SL1-1E6E6AE57D4E2A9B320D1844C68BA291, 3 server(s):
 *Server: 10.15.20.102, port 1812, A-ID  87B3503255C4384485BB808DC24C6F55
                Status = ALIVE
                auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
 *Server: 10.15.20.101, port 1812, A-ID 255C438487B3503485BBC6F55808DC24
                Status = ALIVE
                auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
Installed list: SL2-1E6E6AE57D4E2A9B320D1844C68BA293, 3 server(s):
 *Server: 10.0.0.1, port 1812, A-ID 04758B1F05D8C1439F27F9509E07CFB6.
                Status = ALIVE
                auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
 *Server: 10.0.0.2, port 1812, A-ID 04758B1F05D8C1439F27F9509E07CFB6.
                Status = DEAD
                auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
```

関連コマンド

コマンド	説明
show cts server-list	AAA サーバとロード バランシング設定のリストを表示します。

cts sgt

手動でネットワーク デバイスにセキュリティ グループ タグ（SGT）番号を割り当てるには、グローバル コンフィギュレーション モードで **cts sgt** コマンドを使用します。タグを削除するには、コマンドの **no** 形式を使用します。

[**no**] **cts sgt** *tag-number*

構文の説明

tag-number	デバイスから送信されるパケットの SGT を設定します。*tag* 引数は 10 進表記です。指定できる範囲は 1 ～ 65533 です。

デフォルト

SGT 番号が割り当てられません。

コマンド モード

グローバル コンフィギュレーション（config）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2 (33) SXI3	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。
12.2 (50) SG7	このコマンドが、Catalyst 4000 シリーズ スイッチに追加されました。
12.2 (53) SE2	このコマンドが Catalyst 3750(E) および 3560(E) シリーズ スイッチに追加されました。
12.2 (53) SE2	このコマンドが、Catalyst 3750(X) シリーズ スイッチに追加されました。

使用上のガイドライン

通常の Cisco TrustSec 動作では、認証サーバがデバイスから発信されるパケット用に、そのデバイスに SGT を割り当てます。認証サーバにアクセスできない場合は、使用する SGT を手動で設定できますが、認証サーバから割り当てられた SGT のほうが、手動で割り当てた SGT よりも優先されます。

例

次に、ネットワーク デバイスの SGT を手動で設定する例を示します。

```
Router# configure terminal
Router(config)# cts sgt 1234
Router(config)# exit
```

関連コマンド

コマンド	説明
show cts environment-data	CTS 環境データを表示します。

cts sxp

ネットワーク デバイスに SXP を設定するには、**cts sxp** グローバル コンフィギュレーション コマンドを使用します。このコマンドは、SXP をイネーブルにし、SXP パスワード、ピアのスピーカーとリスナー関係および復帰期間を決定します。また、バインディング変更のログのオン / オフを切り替えます。SXP コンフィギュレーションをディセーブルにするには、このコマンドの **no** 形式を使用します。

[**no**] **cts sxp connection peer** *ip4_address* **password** {**default | none**} **mode** {**local | peer**} [**speaker | listener**] [**vrf** *vrf_name*]

[**no**] **cts sxp connection peer** *ip4_address* **source** *ip4_address* **password** {**default | none**} **mode** {**local | peer**} [**speaker | listener**] [**vrf** *vrf_name*]

[**no**] **cts sxp default password** {**0** *unencrypted_pwd* | **6** *encrypted_key* | **7** *encrypted_key* | *cleartext_pwd* }

[**no**] **cts sxp default source-ip** *ip4_address*

[**no**] **cts sxp enable**

[**no**] **cts sxp log binding-changes**

[**no**] **cts sxp mapping network-map** *bindings*

[**no**] **cts sxp reconciliation period** *seconds*

[**no**] **cts sxp retry period** *seconds*

構文の説明

connection peer *ip4_address*	ピア SXP アドレスを指定します。
password {default | none}	次のオプションを使用して、SXP がピア接続で使用するパスワードを指定します。 • **default**：**cts sxp default password** コマンドを使用して設定したデフォルトの SXP パスワードを使用します。 • **none**：パスワードを使用しません。 パスワードの最大長は 32 文字です。
mode {local | peer}	リモート ピア デバイスのロールを指定します。 • **local**：指定モードはローカル デバイスを示します。 • **peer**：指定モードはピア デバイスを示します。
network-map *bindings*	0 ～ 65535。IP-SGT タギングおよびエクスポートのサブネットを拡張する場合は許可される、SGT にバインディングできるサブネット ホスト アドレスの最大数。拡張なしにするには 0 を入力します。
speaker | listener	**speaker**：デフォルト。このデバイスが接続の際にスピーカーになります。 **listener**：このデバイスが接続の際にリスナーになります。
vrf *vrf_name*	（任意）ピアの VRF を指定します。デフォルトはデフォルト VRF です。

default password **0** *unencrypted_pwd* | **6** *encrypted_key* | **7** *encrypted_key* | *cleartext_pwd*	SXP のデフォルト パスワードを設定します。クリア テキスト パスワード（**0** またはオプションなしを使用）または暗号化パスワード（**6** または **7** オプションを使用）を入力できます。パスワードの最大長は 32 文字です。
source-ip *ip4_address*	（任意）送信元デバイスの IPv4 アドレスを指定します。アドレスが指定されていない場合、接続は、デフォルトの送信元アドレス（設定されている場合）、またはポートのアドレスを使用します。
enable	Cisco TrustSec で SGT 交換プロトコル over TCP（SXP）イネーブルにします。
log binding-changes	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。デフォルトはオフです。
reconciliation period *seconds*	SXP 復帰タイマーを変更します。範囲は 0 ～ 64000 です。デフォルトは 120 秒（2 分）です。
retry period *seconds*	SXP リトライ タイマーを変更します。範囲は 0 ～ 64000 です。デフォルト値は 120 秒（2 分）です。

デフォルト

sxp	デフォルトでディセーブル
log binging-changes	off
password	none
reconciliation period	120 秒
retry period	60 秒
source-ip	デフォルトの送信元 IP アドレス（設定されている場合）またはポート アドレス
VRF	デフォルトの VRF 名

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

Administrator

コマンド履歴

リリース	変更点
12.2 (33) SXI3	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。
12.2 (50) SG7	このコマンドが、Catalyst 4000 シリーズ スイッチに追加されました。
12.2 (53) SE2	このコマンドは、Catalyst 3750(E) および 3560(E) シリーズ スイッチに追加されました（**log binding-changes** キーワードなし）。
12.2 (53) SE2	このコマンドは、Catalyst 3750(X) シリーズ スイッチに追加されました（**log binding-changes** キーワードなし）。
12.2 (50) SY	**mapping** キーワードが追加されました。

使用上のガイドライン

ピアへの 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** キーワードは任意です。VRF 名が指定されていない、または VRF 名が「default」という名前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。

SXP 接続パスワードのデフォルト設定は **none** です。SXP 接続は IP アドレスごとに設定されるため、複数のピアを持つデバイスは、できるだけ多くの SXP 接続を持つことができます。**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デフォルト SXP パスワードを設定します。SXP パスワードは、**0 | 7 | 6** *encrypted_key* 暗号化タイプ オプションを使用してクリア テキストまたは暗号化したものを使用します。デフォルトはタイプ 0（クリア テキスト）です。暗号化タイプが 6 または 7 である場合、暗号化の password 引数は、有効なタイプ 6 またはタイプ 7 の暗号テキストである必要があります。SXP パスワードを削除するには、**no cts sxp default password** コマンドを使用します。

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、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。SXP 接続は 3 台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

再試行タイマー

再試行タイマーは、少なくとも 1 つの 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 SXP 接続が試行されます。このタイマー値を設定するには、**cts sxp retry period** コマンドを使用します。デフォルト値は 120 秒です。指定できる範囲は 0 ～ 64000 秒です。ゼロの値は、再試行が発生しなくなります。

削除のホールドダウン タイマー

削除のホールドダウン タイマー値は設定できず、120 秒に設定されています。このタイマーは、SXP リスナー接続がダウンするとトリガーされます。ダウンした接続から学習した IP-SGT マッピングは、このタイマーが期限切れになると削除されます。削除のホールドダウン タイマーが期限切れになる前にダウンした接続が復元された場合、復帰タイマーが開始されます。

復帰タイマー

ピアが SXP 接続を終了すると、内部の削除のホールドダウン タイマーが開始されます。削除のホールドダウン タイマーが終了する前にピアが再接続すると、SXP 復帰タイマーが開始されます。SXP 復帰期間タイマーがアクティブな間、Cisco TrustSec 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。デフォルト値は 120 秒（2 分）です。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。このタイマーを設定するには、**cts sxp reconciliation period** コマンドを使用します。

例

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

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

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

```
SwitchB# configure terminal
```

```
SwitchB(config)# cts sxp enable
SwitchB(config)# cts sxp default password Cisco123
SwitchB(config)# cts sxp default source-ip 10.20.2.2
SwitchB(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
show cts sxp	すべての SXP 設定のステータスを表示します。

clear cts cache

TrustSec 認可をクリアし、**clear cts counter** 特権 EXEC コマンドを使用します。

clear cts cache authorization-policies [**peer** | **sgt**]

clear cts cache environment-data

clear cts cache filename *file*

clear cts cache interface-controller [**type** *slot*/*port*]

構文の説明

authorization-policies [peer | sgt]	すべてのキャッシュされた SGT およびピア認可ポリシーをクリアします。
environment-data	環境データ キャッシュ ファイルをクリアします。
filename *file*	クリアするキャッシュ ファイルのファイル名を指定します。
interface-controller type *slot*/*port*	クリアするインターフェイス コントローラ キャッシュを指定します。

デフォルト

なし

コマンド モード

特権 EXEC（#）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(33) SXI	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。
12.2(50) SY	**interface-controller** キーワードは、Catalyst 6500 シリーズ スイッチで導入されました。

例

次に、キャッシュから環境データを削除する例を示します。

```
Router# clear cts cache environment-data
Router#
```

（注） ピアの認可および SGT ポリシーのクリアは、SGACL を強制できる TrustSec デバイスだけに関連します。

関連コマンド

コマンド	説明
cts cache	DRAM および NVRAM への TrustSec 許可および環境データ情報のキャッシュをイネーブルにします

clear cts counter

指定したインターフェイスの TrustSec 統計情報をクリアするには、**clear cts counter** 特権 EXEC コマンドを使用します。

clear cts counter [**type** *slot/port*]

構文の説明

type *slot/port*	（任意）クリアするインターフェイスのインターフェイスタイプ、スロット、およびポートを指定します。

デフォルト

なし

コマンド モード

特権 EXEC（#）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(33) SXI	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

clear cts counter コマンドは、選択したインターフェイスに固有の CTS カウンタをクリアします。インターフェイスが指定されていない場合、すべての TrustSec インターフェイスのすべての TrustSec カウンタがクリアされます。

例

次に、GigabitEthernet インターフェイス 3/1 の CTS 統計情報をクリアしてから、**show cts interface** コマンドを使用して確認する例を示します（**show** コマンド出力のフラグメントを表示）。

```
Router# clear cts counter gigabitEthernet3/1
Router# show cts interface  gigabitEthernet3/1
Global Dot1x feature is Disabled
Interface GigabitEthernet3/1:
<snip>

    Statistics:
        authc success:              0
        authc reject:               0
        authc failure:              0
        authc no response:          0
        authc logoff:               0
        authz success:              0
        authz fail:                 0
        port auth fail:             0
<snip>
```

関連コマンド

コマンド	説明
show cts interface	CTS インターフェイスのステータスおよび設定を表示します。

clear cts credentials

TrustSec デバイス ID およびパスワードを削除するには、特権 EXEC モードで **clear cts credentials** コマンドを使用します。

clear cts credentials

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

なし

コマンド モード

特権 EXEC（#）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(33) SXI	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

例

```
Router# clear cts credentials
Router# clear cts environment-data
Router# show cts environment-data
CTS Environment Data
====================
Current state = START
Last status = Cleared
Environment data is empty
State Machine is running
Retry_timer (60 secs) is running
```

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。

clear cts environment-data

キャッシュから TrustSec 環境データを消去するには、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

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

なし

コマンド モード

特権 EXEC（#）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(33) SXI	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

例

次に、キャッシュから環境データをクリアする例を示します。

```
Router# clear cts environment-data
```

関連コマンド

コマンド	説明
show cts environment-data	CTS 環境データを表示します。

clear cts macsec

指定されたインターフェイスの MACsec カウンタをクリアするには、**clear cts macsec counters** コマンドを使用します。

clear cts macsec counters interface type *slot*/*port*

構文の説明

interface type *slot*/*port*	インターフェイスを指定します。

コマンド モード

特権 EXEC

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(50) SY	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

例

次の例では、Catalyst 6500 シリーズ スイッチの gigabitEthernet インターフェイス カウンタをクリアします。

```
Router# clear cts macsec counters interface gigabitEthernet 6/2
```

関連コマンド

コマンド	説明
show cts macsec	
show cts interface	

clear cts pac

キーストアから TrustSec Protected Access Credential（PAC）情報をクリアするには、特権 EXEC モードで **clear cts pac** コマンドを使用します。

clear cts pac {**A-ID** *hexstring* | **all**}

構文の説明

A-ID *hexstring*	キーストアから削除する PAC のオーセンティケータ ID（A-ID）を指定します。
all	デバイスのすべての PAC を削除するように指定します。

デフォルト

なし

コマンド モード

特権 EXEC（#）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(33) SXI	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

例

次のコマンドは、キーストアのすべての PAC をクリアします。

```
Router# clear cts pac all
```

関連コマンド

コマンド	説明
show cts pacs	キーストアの PAC の A-ID および PAC 情報を表示します。
show cts keystore	キーストアの内容を表示します。

clear cts policy

TrustSec ピアのピア認可ポリシーを削除するには、特権 EXEC モードで **clear cts policy** コマンドを使用します。

clear cts policy {**peer** [*peer_id*] | **sgt** [*sgt*]}

構文の説明

peer *peer_id*	TrustSec ピア デバイスのピア ID を指定します。
sgt *sgt*	TrustSec ピア デバイスのセキュリティ グループ タグ（SGT）を、16 進数で指定します。

デフォルト

なし

コマンド モード

特権 EXEC（#）

サポートされるユーザ ロール

Administrator

コマンド デフォルト

リリース	変更点
12.2(33) SXI	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

すべての TrustSec ピアのピア認可ポリシーをクリアするには、ピア ID を指定しないで **clear cts policy peer** コマンドを使用します。TrustSec ピアのセキュリティ グループ タグをクリアするには、**clear cts policy sgt** コマンドを使用します。確認するには、**show cts policy peer** コマンドを使用します。

例

次の例では、ピア ID が atlas2 の TrustSec ピアのピア認可ポリシーをクリアします。

```
Router# clear cts policy peer atlas2
Delete all peer policies? [confirm] y
Router#
```

関連コマンド

コマンド	説明
cts refresh	ピア認可ポリシーを強制的にリフレッシュします。
show cts policy peer	TrustSec ピアのピア認可ポリシーを表示します。

clear cts role-based counters

セキュリティ グループ ACL 統計カウンタをリセットするには、EXEC モードまたは特権 EXEC モードで **clear cts role-basedcounters** コマンドを使用します。

clear cts role-based counters default [**ipv4** | **ipv6**]

clear cts role-based counters from {*sgt_num* | **unknown**} [**ipv4** | **ipv6** | **to** {*sgt_num* | **unknown**} [**ipv4** | **ipv6**]]

clear cts role-based counters to {*sgt_num* | **unknown**} [**ipv4** | **ipv6** | **]**

clear cts role-based counters [**ipv4** | **ipv6**]

構文の説明

default	デフォルト ポリシー カウンタ
from	送信元セキュリティ グループを指定します
ipv4	IP バージョン 4 ネットワークでセキュリティ グループを指定します
ipv6	IP バージョン 6 ネットワークでセキュリティ グループを指定します
to	宛先セキュリティ グループを指定します
sgt_num	（0 ～ 65533）セキュリティ グループ タグ番号を指定します
unknown	すべての送信元グループを指定します

コマンド モード

EXEC（>）、特権 EXEC（#）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(50) SY	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

指定したスコープのセキュリティ グループ ACL（SGACL）強制カウンタをクリアするには、**clear cts role-based counters** コマンドを使用します。**show cts role-based counters** は、最後に clear コマンドが発行されてから蓄積された統計情報を、例 7-1 に示されているような表形式で表示します。

例 7-1　show role-based カウンタからの表形式の SGACL 出力

```
router# show cts role-based counters
Role-based counters
From    To      SW-Denied       HW-Denied       SW-Permitted    HW_Permitted
2       5       129               89762               421       7564328
3       5        37              123456              1325      12345678
3       7         0               65432               325       2345678
```

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** および句、**to** キーワードの両方が省略された場合は、許可マトリクス全体のカウンタがクリアされます。

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クリアします。

ipv4 および **ipv6** のいずれも指定しない場合、コマンドは IPv4 カウンタだけをクリアします。

例

次の例では、IPv4 トラフィックの SGACL 強制の統計情報をコンパイルしているすべてのロールベース カウンタをクリアします。

```
router# clear cts role-based counters ipv4
```

関連コマンド

clear cts server

CTS の AAA サーバ リストからサーバを削除するには、**clear cts server** コマンドを使用します。

clear cts server *ip_address*

構文の説明

ip_address	サーバ リストから削除する AAA サーバの IPv4 アドレス。

コマンド モード

特権 EXEC（#）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(33) SXI	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドは、**cts authorization list** グローバル コンフィギュレーション コマンドで設定された CTS AAA サーバのリスト、または CTS のオーセンティケータのピアによりプロビジョニングされた AAA サーバ リストから、サーバを削除します。

例

次の例は、CTS の AAA サーバ リストから AAA サーバ 10.10.10.1 を削除します。

```
router# clear cts server 1.1.1.1
```

関連コマンド

コマンド	説明
show cts server-list	
cts server	

default（cts dot1x インターフェイス コンフィギュレーション サブモード）

任意の **cts dot1x** コンフィギュレーションをデフォルト値に復元するには、CTS dot1x インターフェイス コンフィギュレーション サブモードで **default** コマンドを使用します。

default propagate sgt

default sap

default timer reauthentication

構文の説明

propagate sgt	propagate sgt をイネーブルにしたデフォルトに復元します。
sap	デフォルトの **sap modelist gcm-encrypt null** に復元します。
timer	dot1x 再認証時間が 86,400 秒のデフォルトに復元します。

デフォルト

このコマンドにはデフォルトはありません。

コマンド モード

CTS dot1x インターフェイス コンフィギュレーション サブモード（config-if-cts-dot1x）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(50) SY	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

例

次に、SGT 伝搬を再イネーブル化する例を示します。

```
router# config t
router(config)# interface gigabit 6/1
router(config-if)# cts dot1x
router(config-if-cts-dot1x)# default propagate sgt
```

関連コマンド

コマンド	説明
propagate（cts dot1x サブモード）	dot1x モードの SGT 伝搬をイネーブルまたはディセーブルにします。
sap（cts dot1x インターフェイス サブモード）	dot1x モードの CTS SAP を設定します。
timer（cts do1x インターフェイス サブモード）	CTS のタイマーを設定します。

default（cts 手動インターフェイス コンフィギュレーション サブモード）

任意の **cts manual** コンフィギュレーションをデフォルト値に復元するには、CTS 手動インターフェイス コンフィギュレーション サブモードで **default** コマンドを使用します。

default policy dynamic identity

default policy static sgt

default propagate sgt

default sap

構文の説明

dynamic identity	ピア ポリシーを AAA サーバからダウンロードするデフォルトに復元します。
policy static sgt	デフォルトの no policy に復元します。つまり、SGT は入力トラフィックに適用されません。
policy propagate sgt	SGT の伝播のモードを On に指定します。
sap	デフォルト SAP 値を指定します。（GCM-Encrypt、null）

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 サブモード（config-if-cts-manual）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(50) SY	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

CTS の手動インターフェイス コンフィギュレーション サブモード パラメータをデフォルト値に戻すには、**default** サブコマンドを使用します。

例

次に、Catalyst 6500 シリーズ スイッチの CTS イネーブルにされたインターフェイスのデフォルトのダイナミック ポリシーと、SGT 伝播ポリシーを復元する例を示します。

```
router# config t
router(config)# interface gigbitEthernet 6/1
router(config-if)# cts manual
router(config-if-cts-manual)# default policy dynamic identity
router(config-if-cts-manual)# default propagate sgt
```

関連コマンド

コマンド	説明
policy（cts 手動インターフェイス コンフィギュレーション サブモード）	手動モードの CTS ポリシーを設定します
sap（cts 手動インターフェイス サブモード）	手動モードの CTS SAP を設定します。

match flow cts

Flexible NetFlow フロー レコードに、Cisco TrustSec フロー オブジェクトを追加するには、**match flow cts** レコード コンフィギュレーション コマンドを使用します。

[**no**] **match flow cts destination group-tag**

[**no**] **match flow cts source group-tag**

構文の説明

destination group-tag	Cisco TrustSec セキュリティ グループ タグ（SGT）の宛先フィールドを照合します
source group-tag	Cisco TrustSec セキュリティ グループ タグ（SGT）の送信元フィールドを照合します

デフォルト

このコマンドにはデフォルトはありません。

コマンド モード

Flexible NetFlow レコード コンフィギュレーション（config-flow-record）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(50) SY	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

標準の 5 タプル フロー オブジェクトを使用してフロー レコードに SGT および DGT フロー オブジェクトが設定されている場合、Flexible NetFlow は、SGACL 強制によってドロップされたパケットに対応できます

flow record および **flow exporter** グローバル コンフィギュレーション コマンドを使用してフロー レコードおよびフロー エクスポータを設定してから、それらを **flow monitor** コマンドを使用してフロー モニタに追加します。**show flow** show コマンドを使用して設定を確認します。

SGACL のドロップされたパケットだけを収集するには、**[no] cts role-based** {**ip** | **ipv6**} **flow monitor dropped** グローバル コンフィギュレーション コマンドを使用します。

Flexible NetFlow の概要および設定の詳細については、次のマニュアルを参照してください。

『Getting Started with Configuring Cisco IOS Flexible NetFlow』

http://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/get_start_cfg_fnflow.html

『Catalyst 6500 Release 12.2SY Software Configuration Guide』

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SY/configuration/guide/netflow_hw_support.html

例

次に、IPv4 フロー レコード（5 タプル、方向、SGT、SGT）を設定する例を示します。

```
router(config)# flow record cts-record-ipv4
router(config-flow-record)# match ipv4 protocol
```

```
router(config-flow-record)# match ipv4 source address
router(config-flow-record)# match ipv4 destination address
router(config-flow-record)# match transport source-port
router(config-flow-record)# match transport destination-port
router(config-flow-record)# match flow direction
router(config-flow-record)# match flow cts source group-tag
router(config-flow-record)# match flow cts destination group-tag
router(config-flow-record)# collect counter packets
```

関連コマンド

コマンド	説明
show flow monitor	Flexible NetFlow フロー モニタのステータスおよび統計情報を表示します
cts role-based	Flexible NetFlow では、このコマンドには、すべてのレイヤ 3 インターフェイスにフロー モニタを接続して、SGACL によってドロップされるトラフィックの統計情報を収集するように設定するオプションがあります。

platform cts

TrustSec 出力または入力のリフレクタをイネーブルにするには、**platform cts** グローバル コンフィギュレーション コマンドを使用します。リフレクタをディセーブルにするには、コマンドの **no** 形式を入力します。

[**no**] **platform cts** {**egress** | **ingress**}

構文の説明

egress	イネーブルまたはディセーブルにされる出力 TrustSec リフレクタを指定します。
ingress	イネーブルまたはディセーブルにされる入力 TrustSec リフレクタを指定します。

デフォルト

デフォルトは、no ingress または egress reflector 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）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(50) SY	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

例

次の例では、Catalyst 6500 スイッチで CTS 入力リフレクタをイネーブル化します。

```
switch(config)# platform cts egress
```

次の例では、Catalyst 6500 スイッチで CTS 入力リフレクタをディセーブル化します。

```
switch(config)# no platform cts egress
```

関連コマンド

コマンド	説明
show platform cts reflector	Cisco TrustSec リフレクタ モードのステータスを表示します。

policy（cts 手動インターフェイス コンフィギュレーション サブモード）

手動で設定された TrustSec リンクにポリシーを適用するには、**policy** インターフェイス手動サブモード コマンドを使用します。ポリシーを削除するには、コマンドの **no** 形式を使用します。

[**no**] **policy dynamic identity** *peer_deviceID*

[**no**] **policy static sgt** *sgt_number* [**trusted**]

構文の説明

dynamic	認証サーバからポリシーを取得します。
identity *peer_deviceID*	認証サーバのポリシー データベースの、ピアに適用されるポリシーに関連付けられたピア デバイス名またはシンボリック名。
static	リンクの着信トラフィックに SGT ポリシーを指定します。
sgt *sgt_number*	ピアからの着信トラフィックに適用するセキュリティ グループ タグ番号。
trusted	コマンドで SGT が指定されたインターフェイスの入力トラフィックでは、SGT を上書きしてはいけないことを示します。デフォルトは untrusted です。

デフォルト

デフォルトは no policy です。

コマンド モード

CTS インターフェイスの手動サブモード（config-if-cts-manual）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(50) SY	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

TrustSec リンクを手動で設定する場合はポリシーを適用するには、**policy** コマンドを使用します。デフォルトは **no policy** で、すべてのトラフィックを SGT を適用しないで通過させます。**sap** CTS 手動モード サブコマンドはまた、TrustSec リンクをアップするように設定する必要があります。

選択した SAP モードで SGT を挿入可能にし、すべての着信パケットが SGT を伝送していない場合、タギング ポリシーは次のとおりです。

- **policy static** コマンドが設定されている場合､パケットには **policy static** コマンドで設定した SGT がタグ付けされます。
- **policy dynamic** コマンドが設定されている場合、パケットはタグ付けされません。

選択した SAP モードで SGT を挿入可能にし、着信パケットが SGT を伝送している場合、タギング ポリシーは次のとおりです。

- **policy static** コマンドが **trusted** キーワードを指定せずに設定されている場合、SGT は **policy static** コマンドで設定した SGT に置き換えられます。

- **policy static** コマンドが **trusted** キーワードを使用して設定されている場合、SGT は変更されません。
- **policy dynamic** コマンドが設定されていて、認証サーバからダウンロードされた認可ポリシーがパケットの送信元が信頼できないことを示している場合、SGT はダウンロードしたポリシーで指定されている SGT に置き換えられます。

  認可ポリシーは、ピアの SGT、ピアの SGT 割り当ての信頼状態、関連するピア SGT の RBACL、およびインターフェイス ACL を指定できます。
- **policy dynamic** コマンドが設定されていて、ダウンロードされた認可ポリシーがパケットの送信元が信頼できることを示している場合、SGT は変更されません。

静的に設定された SGT については RBACL は適用されませんが、従来のインターフェイス ACL は、必要に応じてトラフィック フィルタリング用に個別に設定できます。

例

次の例では、タグ付け済みのトラフィックを除き、ピアからの着信トラフィックに SGT 3 を適用します（Cisco Secure ACS サーバと通信していないインターフェイス）。

```
Router# configure terminal
Router(config)# interface gi2/1
Router(config-if)# cts manual
Router(config-if-cts-manual)# sap pmk 1234abcdef mode-list gcm null no-encap
Router(config-if-cts-manual)# policy static sgt 3 trusted
Router(config-if-cts-manual)# exit
Router(config-if)# shutdown
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# exit

Router# show cts interface GigabitEthernet 2/1
Global Dot1x feature is Enabled
Interface GigabitEthernet2/1:
    CTS is enabled, mode:    MANUAL
    IFC state:               OPEN
    Authentication Status:   NOT APPLICABLE
        Peer identity:       "unknown"
        Peer's advertised capabilities: "sap"
    Authorization Status:    SUCCEEDED
        Peer SGT:            3
        Peer SGT assignment: Trusted
    SAP Status:              SUCCEEDED
        Version:             1
        Configured pairwise ciphers:
            gcm-encrypt
            null

        Replay protection:      enabled
        Replay protection mode: STRICT

        Selected cipher:        gcm-encrypt

    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:                1
sap fail:                   0
authz success:              5
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
```

関連コマンド

コマンド	説明
show cts interface	インターフェイスごとの TrustSec 設定の統計情報を表示します。
default（cts 手動インターフェイス コンフィギュレーション サブモード）	CTS 手動モードのデフォルト コンフィギュレーション復元します。
policy（cts 手動インターフェイス コンフィギュレーション サブモード）	手動モードの CTS ポリシーを設定します。
sap（cts 手動インターフェイス サブモード）	手動モードの CTS SAP を設定します。

propagate（cts dot1x サブモード）

Cisco TrustSec インターフェイスで SGT 伝播をイネーブルまたはディセーブルにするには、CTS dot1x インターフェイス コンフィギュレーション サブモードで propagate sgt コマンドを使用します。

[**no**] **propagate sgt**

構文の説明

sgt	CTS SGT 伝搬を指定します。

デフォルト

SGT 伝播は、CTS dot1x および CTS 手動インターフェイス コンフィギュレーション サブモードでデフォルトでイネーブルになっています。

コマンド モード

CTS Dot1x インターフェイス コンフィギュレーション サブモード（config-if-cts-dot1x）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(50) SY	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

SGT の伝播（SGT タグ カプセル化）は、CTS dot1x および CTS 手動インターフェイス コンフィギュレーション サブモードの両方でデフォルトでイネーブルになっています。TrustSec 対応ポートはレイヤ 2 MACsec および SGT カプセル化をサポートできます。SGT のタグとデータの送信のためにピアと最もセキュアなモードをネゴシエートします。MACsec はスイッチおよびサーバが使用する 802.1AE 規格ベースのリンク間プロトコルです。ピアは MACsec をサポートできますが、SGT カプセル化はサポートできません。このような場合、**no propagate sgt** CTS Dot1x 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、このレイヤ 2 SGT 伝播をディセーブルにしておくことをお勧めします。

SGT の伝播を再度イネーブルにするには **propagate sgt** コマンドを入力します。SGT の伝播の状態を確認するには、**show cts interface** コマンドを使用します。ディセーブル ステートだけが不揮発生成（NVGEN）に保存されます。

例

次の例は、TrustSec 対応インターフェイスで SGT 伝播をディセーブル化します。

```
router(config) interface gigabit 6/1
router(config-if) cts dot1x
router(config-if-cts-dot1x)# no propagate sgt

router# show cts interface gigabit 6/1
Global Dot1x feature is Enabled
Interface GigabitEthernet6/1:
    CTS is enabled, mode:    DOT1X
    IFC state:               INIT

<snip> . . .

SAP Status:              UNKNOWN
```

```
Configured pairwise ciphers:
    gcm-encrypt
    null

        Replay protection:      enabled
        Replay protection mode: STRICT

        Selected cipher:

    Propagate SGT:           Disabled
<snip> . . .
```

関連コマンド

コマンド	説明
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。
sap（cts dot1x インターフェイス サブモード）	dot1x モードの CTS SAP を設定します。
timer（cts do1x インターフェイス サブモード）	CTS のタイマーを設定します。

propagate（cts 手動インターフェイス コンフィギュレーション サブモード）

セキュリティ グループ タグをインターフェイス上で伝播するインターフェイスの機能をイネーブルまたはディセーブルにするには、**cts propagate** cts インターフェイス手動設定サブモード コマンドを使用します。

[**no**] **propagate sgt**

構文の説明

sgt	セキュリティ グループ タグを指定します

デフォルト

デフォルトは、SGT を伝播することです。

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 サブモード（config-if-cts-manual）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(50) SY	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

セキュリティ グループ タグの伝播は、CTS dot1x および CTS 手動モードの両方でデフォルトでイネーブルです。SGT 処理をディセーブルにするには、**no propagate sgt** コマンドを入力します。再度イネーブルにするには、**propagate sgt** を入力します。不揮発生成（NVGEN）プロセスを呼び出す CLI コマンドを発行した場合、**no propagate sgt** ステートだけが保存されます（たとえば、**copy system running-config**）。

TrustSec 対応インターフェイスは MACsec（レイヤ 2 802.1AE のセキュリティ）および SGT タギングをサポートできます。TrustSec 対応インターフェイスがピアと最もセキュアなモードをネゴシエートしようとします。ピアは、MACsec 対応ですが、SGT を処理できないことがあります。手動 CTS インターフェイス コンフィギュレーションでは、MACsec 機能のみを設定している場合、CTS 対応インターフェイスで SGT 伝播をディセーブルにします。

例

次に、手動で設定した TrustSec 対応インターフェイスで SGT タギングをディセーブル化する例を示します。

```
router(config-if)# cts manual
router(config-if-cts-manual)# sap pmk FFFE
router(config-if-cts-manual)# no propagate sgt
router(config-if-cts-manual)# exit
router(config-if)# exit
router(config)# exit
router# show running-config
. . .
interface GigabitEthernet6/2
 ip address 172.16.4.12 255.255.255.0
cts manual
```

```
  no propagate sgt
  sap pmk 00000000000000000000000000000000000000000000000000000000000000000FFFE
. . .
```

関連コマンド

コマンド	説明
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。
show running-config	現在のシステム設定を表示します。

sap（cts dot1x インターフェイス サブモード）

2 個のインターフェイス間のリンク暗号化をネゴシエーションするために、セキュリティ アソシエーション プロトコル（SAP）の認証および暗号化モード選択するには、**sap mode-list** コマンドを使用します。modelist 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。

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

構文の説明

mode-list	アドバタイズされた SAP 認証および暗号化モードをリストします（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

デフォルト

デフォルトの暗号化は、**sap modelist gcm-encrypt null** です。ピア インターフェイスが dot1x、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 dot1x インターフェイス サブモード（config-if-cts-dot1x）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(50) SY	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。
IOS-XE 3.3.0 SG	このコマンドが、Catalyst 4500 シリーズ スイッチに追加されました。
IOS 15.0(1) SE	このコマンドが、Catalyst 3000 シリーズ スイッチに追加されました。

使用上のガイドライン

Dot1x 認証中に使用する認証および暗号化方式を指定するには、**sap 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 802.11i IEEE 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。

Dot1x 認証後に SAP 交換が開始される前に、両側（サプリカントとオーセンティケータ）で Cisco Secure Access Control Server（Cisco Secure ACS）から Pairwise Master Key（PMK）とピアのポートの MAC アドレスを受信しています。802.1X 認証が不可能である場合、CTS 手動コンフィギュレーション モードで、SAP および PMK を 2 個のインターフェイス間で手動で設定できます。

デバイスが CTS-Aware 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 modelist no-encap** コマンドを使用してカプセル化を拒否します。

期間が Cisco Secure ACS から使用できない場合は、**timer reauthentication** コマンドを使用して CTS リンクに適用する再認証期間を設定します。デフォルトの再認証期間は 86,400 秒です。

（注）　TrustSec NDAC および SAP はスイッチ間リンクでスイッチングだけでサポートされているため、dot1x はマルチホスト モードで設定する必要があります。オーセンティケータ PAE は **dot1x system-auth-control** がグローバルにイネーブルになっている場合のみ開始されます。

例

次に、SAP が CTS カプセル化の使用を GCM 暗号化と、または第 2 の選択肢として null-cipher とネゴシエートするが、ピアがハードウェアで CTS カプセル化をサポートしない場合は CTS カプセル化を受け入れることができない例を示します。

```
Router(config-if-cts-dot1x)# sap modelist gcm-encrypt  null  no-encap
```

関連コマンド

コマンド	説明
propagate（cts dot1x サブモード）	dot1x モードの SGT 伝搬をイネーブルまたはディセーブルにします。
sap（cts dot1x インターフェイス サブモード）	dot1x モードの CTS SAP を設定します。
timer（cts do1x インターフェイス サブモード）	CTS のタイマーを設定します。

sap（cts 手動インターフェイス サブモード）

2 個のインターフェイス間で MACsec のリンク暗号化のネゴシエーションを行うために、Pairwise Master Key（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。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。

[**no**] **sap pmk** *hex_value* [**modelist** {**gcm-encrypt** | **gmac** | **no-encap** | **null**} [**gcm-encrypt** | **gmac** | **no-encap** | **null**] . . .]

構文の説明

pmk *hex_value*	16 進数データの PMK（先頭の 0x は付けません。偶数の 16 進数文字を入力し、最後の文字に 0 をプレフィックスします）
modelist	アドバタイズド モードのリスト（最高から最低に優先順位付け）
gcm-encrypt	GCM 認証、GCM 暗号化を指定します
gmac	GCM 認証を指定し、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

デフォルト

デフォルトの暗号化は、**sap modelist gcm-encrypt null** です。ピア インターフェイスが dot1x、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 サブモード（config-if-cts-manual）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(50) SY	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

セキュリティ アソシエーション プロトコル（SAP）は 802.11i IEEE 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。TrustSec 設定では、キーは 2 個のインターフェイス間での MACsec のリンク間暗号化に使用されます。

802.1X 認証が不可能である場合、SAP、および Pairwise Master Key（PMK）を **sap pmk** コマンドで 2 個のインターフェイス間に手動で設定できます。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。

例

次に、ギガビット イーサネット インターフェイスの SAP 設定の例を示します。

```
router(config)# interface gigabitEthernet 2/1
router(config-if)# cts manual
router(config-if-cts-manual)# sap pmk FFFEE mode-list gcm-encrypt
```

関連コマンド

コマンド	説明
default（cts 手動インターフェイス コンフィギュレーション サブモード）	CTS 手動モードのデフォルト コンフィギュレーション復元します。
policy（cts 手動インターフェイス コンフィギュレーション サブモード）	手動モードの CTS ポリシーを設定します
propagate（cts 手動インターフェイス コンフィギュレーション サブモード）	手動モードの CTS SGT 伝搬を設定します
show cts interface	インターフェイスごとの TrustSec 設定の統計情報を表示します。

show cts

Cisco TrustSec に関連するステートおよび統計情報を表示するには、**show cts** 特権 EXEC コマンドを使用します。

show cts [

authorization entries |

credentials |

environment-data

interface {type *slot*/*port* **| vlan** *vlan_number* **|**

keystore |

macsec counters interface type *slot*/*port* [**delta**] |

pacs |

policy layer3 [**ipv4** | **ipv6**] |

policy peer *peer_id* |

provisioning |

role-based counters . . . |

role-based flow . . . |

role-based permissions . . . |

role-based sgt-map . . . |

server-list |

sxp connections . . . |

sxp sgt-map . . . |

構文の説明

authorization	認可エントリを表示します。
credentials	CTS 認証に使用するクレデンシャルを表示します。
environment-data	CTS 環境データを表示します。
interface	CTS インターフェイスのステータスと設定を表示します。
keystore	キーストアの情報を表示します。
macsec	MACSec カウンタ情報を表示します。
pacs	キーストアの PAC の A-ID および PAC 情報を表示します。
policy	CTS ポリシーを表示します。
provisioning	未処理の CTS のプロビジョニング ジョブを表示します。
role-based	ロールベース アクセス コントロール情報（SGACL 情報）を表示します。
server-list	CTS のサーバ リストを表示します。
sxp	CTS SXP プロトコル情報を表示します。

デフォルト

なし

コマンド モード　EXEC（>）、特権 EXEC（#）

サポートされるユーザ ロール　Administrator

コマンド履歴

リリース	変更点
12.2(33) SXI	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。
12.2(50) SY	次のキーワードは、Catalyst 6500 シリーズ スイッチに追加されました。

例　次に、キーワードを使用しないで入力した **show cts** の例を示します。

```
Router# show cts
Global Dot1x feature: Enabled
CTS device identity: "dcas1"
CTS caching support: disabled

Number of CTS interfaces in DOT1X mode:  19,    MANUAL mode: 5
Number of CTS interfaces in LAYER3 TrustSec mode: 0

Number of CTS interfaces in corresponding IFC state
  INIT            state:  19
  AUTHENTICATING  state:  0
  AUTHORIZING     state:  0
  SAP_NEGOTIATING state:  0
  OPEN            state:  5
  HELD            state:  0
  DISCONNECTING   state:  0
  INVALID         state:  0

CTS events statistics:
  authentication success: 14
  authentication reject : 19
  authentication failure: 0
  authentication logoff : 1
  authentication no resp: 0
  authorization success : 19
  authorization failure : 3
  sap success           : 12
  sap failure           : 0
  port auth failure     : 0
```

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 authorization entries

TrustSec NDAC 認証エントリを表示するには、EXEC モードまたは特権 EXEC モードで **show cts authorization entries** コマンドを使用します。

show cts authorization entries

構文の説明　このコマンドには、引数またはキーワードはありません。

デフォルト　なし

コマンド モード　EXEC（>）、特権 EXEC（#）

サポートされるユーザ ロール　Administrator

コマンド履歴

リリース	変更点
12.2(33) SXI	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

例　次の例では、Catalyst 6500 スイッチからの **show** コマンドの出力です。

```
router# show cts authorization entries
Authorization Entries Info
 Peer-name                = annapurna
Peer-SGT                 = 7-1F05D8C1
Entry State              = COMPLETE
Entry last refresh       = 01:19:37 UTC Sat Dec 8 2007
Session queuesize        = 1
  Interface:       Gi2/3
  status:          SUCCEEDED
Peer policy last refresh = 01:19:37 UTC Sat Dec 8 2007
SGT policy last refresh = 01:19:37 UTC Sat Dec 8 2007
Peer policy refresh time = 2000
Policy expires in     0:00:28:26 (dd:hr:mm:sec)
Policy refreshes in  0:00:28:26 (dd:hr:mm:sec)
Retry_timer                  = not running
Cache data applied           = NONE
Entry status                 = SUCCEEDED

Peer-name = Unknown-0000
Peer-SGT = 0-AD23BDF78
Entry State = COMPLETE
Entry last refresh       = 01:30:37 UTC Sat Dec 8 2007
session queuesize = 0
Peer policy last refresh = 01:30:37 UTC Sat Dec 8 2007
SGT policy last refresh = 01:30:37 UTC Sat Dec 8 2007
Peer policy refresh time = 0
SGT policy refresh time = 2000
Policy expires in    0:00:29:27 (dd:hr:mm:sec)
Policy refreshes in 0:00:29:27 (dd:hr:mm:sec)
Retry_timer                  = not running
Cache data applied      = NONE
```

```
Entry status                 = SUCCEEDED

Peer-name = Unknown-FFFF
Peer-SGT = FFFF-ABC876234
Entry State = COMPLETE
Entry last refresh       = 01:30:37 UTC Sat Dec 8 2007
session queuesize = 0
Peer policy last refresh = 00:20:37 UTC Sat Dec 8 2007
SGT policy last refresh = 01:30:37 UTC Sat Dec 8 2007
Peer policy refresh time = 0
SGT policy refresh time = 2000
Policy expires in    0:00:29:27 (dd:hr:mm:sec)
Policy refreshes in 0:00:29:27 (dd:hr:mm:sec)
Retry_timer                  = not running
Cache data applied       = NONE
Entry status                  = SUCCEEDED
```

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 credentials

TrustSec 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。

デフォルト

なし

コマンド モード

EXEC（>）、特権 EXEC（#）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(33) SXI	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

例

```
Router# 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

TrustSec 環境データを表示するには、EXEC モードまたは特権 EXEC モードで **show cts environment-data** コマンドを使用します。

show cts environment-data

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。

デフォルト

なし

コマンド モード

EXEC（>）、特権 EXEC（#）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(33) SXI	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

例

次の例は、Cisco Catalyst 6500 シリーズ スイッチの環境データを表示します。

```
Router# show cts environment-data
CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
  SGT tag = 11-ea7f3097b64bc9f8
Server List Info:
Preferred list, 0 server(s):
Installed list: SL1-15A25AC3633E7F074FF7E0B45861DF15, 1 server(s):
 *Server: 43.1.1.3, port 1812, A-ID 05181D8147015544BC20F0119BE8717E
          Status = ALIVE
          auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
  Multicast Group Addresses:
Multicast Group SGT Table:
  Name = mcg_table_2-4ff532e525a3efe4
  Multicast SGT:
Transport type = CTS_TRANSPORT_IP_UDP
Environment Data Lifetime = 2000 secs
Last update time = 21:43:28 UTC Mon Aug 27 2007
Data loaded from cache = FALSE
Refresh timer is running
State Machine is running
```

関連コマンド

コマンド	説明
clear cts environment-data	キャッシュからの TrustSec 環境データをクリアします。

show cts interface

TrustSec 設定の統計情報を表示するには、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 [**type** *slot*/*port*] | [**brief**] | [**summary**]

構文の説明

type *slot*/*port*	（任意）インターフェイス タイプ、スロット番号、およびポート番号を指定します。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。
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。

デフォルト

なし

コマンド モード

EXEC（>）、特権 EXEC（#）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(33) SXI	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

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、キーワードなしで **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）。

```
Router# show cts interface
Global Dot1x feature is Enabled
Interface GigabitEthernet4/1:
    CTS is enabled, mode:    DOT1X
    IFC state:               OPEN
    Authentication Status:   SUCCEEDED
        Peer identity:       "r1"
        Peer is:             CTS capable
        802.1X role:         Authenticator
        Reauth period configured:       0 (locally not configured)
        Reauth period per policy:       3000 (server configured)
        Reauth period applied to link:  3000 (server configured)
    Authorization Status:    SUCCEEDED
        Peer SGT:            0
        Peer SGT assignment: Untrusted
    SAP Status:              NOT APPLICABLE
```

```
        Configured pairwise ciphers:
            gcm-encrypt
            null

        Replay protection:      enabled
        Replay protection mode: OUT-OF-ORDER
        SPI range:              (256, 1023)
        Pairwise Master Session Key:
             27C2DF9D 7C686B03 C930D003 95F83737
             6AC0276C 8160FE3C 0C33EF9A C01FCBAC

        Selected cipher:
        Current receive SPI:    0
        Current transmit SPI:   0
        Current Transient Session Key:
             27C2DF9D 7C686B03 C930D003 95F83737
             6AC0276C 8160FE3C 0C33EF9A C01FCBAC

        Current Offset:
             27C2DF9D 7C686B03 C930D003 95F83737
             6AC0276C 8160FE3C 0C33EF9A C01FCBAC

    Statistics:
        authc success:              1
        authc reject:               18
        authc failure:              0
        authc no response:          0
        authc logoff:               0
        sap success:                0
        sap fail:                   0
        authz success:              1
        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

Dot1x Info for GigabitEthernet4/1
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = MULTI_HOST
ReAuthentication          = Enabled
QuietPeriod               = 60
ServerTimeout             = 30
SuppTimeout               = 30
ReAuthPeriod              = 3000 (Locally configured)
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
```

次に、**brief** キーワードを使用した出力例を表示します。

```
Router# show cts interface brief
Global Dot1x feature is Enabled
Interface GigabitEthernet4/1:
    CTS is enabled, mode:    DOT1X
    IFC state:               OPEN
    Authentication Status:   SUCCEEDED
        Peer identity:       "r1"
        Peer is:             CTS capable
        802.1X role:         Authenticator
        Reauth period configured:       0 (locally not configured)
        Reauth period per policy:       3000 (server configured)
        Reauth period applied to link:  3000 (server configured)
    Authorization Status:    SUCCEEDED
        Peer SGT:            0
        Peer SGT assignment: Untrusted
    SAP Status:              NOT APPLICABLE

Dot1x Info for GigabitEthernet4/1
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = MULTI_HOST
ReAuthentication          = Enabled
QuietPeriod               = 60
ServerTimeout             = 30
SuppTimeout               = 30
ReAuthPeriod              = 3000 (Locally configured)
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
```

次に、**summary** キーワードを使用した出力例を表示します。

```
Router# show cts interface summary
Interface  Mode    IFC-state dot1x-role peer-id    IFC-cache  Dot1x
------------------------------------------------------------------------
Gi4/1      DOT1X   OPEN      Authent    r1         invalid    enabled
```

関連コマンド

コマンド	説明
cts sxp	ネットワーク デバイスに SXP を設定します。

show cts macsec

CTS リンク間暗号化に関連するインターフェイスごとに暗号 ASIC のパケット カウンタを表示するには、**show cts macsec** コマンドを使用します。

show cts macsec counters interface interface_type *slot*/*port* [**delta**]

構文の説明

interface interface_type *slot*/*port*	CTS MACsec インターフェイスを指定します。
delta	最後にクリアされた時点以降のカウンタ値を表示します。

コマンド モード

EXEC（>）、特権 EXEC（#）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(50) SY	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドは、インターフェイス単位の暗号 ASIC のパケット カウンタを表示します。セキュリティ アソシエーション（SA）がインストールされている場合（NDAC または **sap** cts インターフェイス do1x または手動サブコマンドを介して）、アクティブな SA カウンタが表示されます。一度に 1 つの SA しかアクティブになりません。SA のサポートされる値は 1 と 2. です。delta キーワードにより、**clear cts macsec counters interface** コマンドが発行された時点以降のカウンタ値がリストされます。

例

次の例では、Catalyst 6500 シリーズ スイッチ上で手動で設定された CTS アップリンク インターフェイスの MACsec カウンタを表示します。

```
router# show cts macsec counters interface gigabitEthernet 6/2
CTS Security Statistic Counters:
                    rxL2UntaggedPkts = 0
                       rxL2NotagPkts = 0
                     rxL2SCMissPkts = 0
                       rxL2CTRLPkts = 0
                       rxL3CTRLPkts = 0
                    rxL3UnknownSAPkts = 0
                       rxL2BadTagPkts = 0
                     txL2UntaggedPkts = 0
                       txL2CtrlPkts = 0
                       txL3CtrlPkts = 0
                      txL3UnknownSA = 0
GENERIC Counters:
                      CRCAlignErrors = 0
                      UndersizedPkts = 0
                       OversizedPkts = 0
                       FragmentPkts = 0
                            Jabbers = 0
                         Collisions = 0
                           InErrors = 0
                          OutErrors = 0
                        ifInDiscards = 0
```

```
                  ifInUnknownProtos = 0
                      ifOutDiscards = 0
  dot1dDelayExceededDiscards = 0
                              txCRC = 0
                         linkChange = 0
```

関連コマンド

コマンド	説明
show cts interface	
sap（cts dot1x インターフェイス サブモード）	
sap（cts 手動インターフェイス サブモード）	

show cts pacs

Protected Access Credential（PAC）を表示するには、EXEC モードまたは特権 EXEC モードで **show cts pacs** コマンドを使用します。

show cts pacs

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。

デフォルト

なし

コマンド モード

EXEC（>）、特権 EXEC（#）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(33) SXI	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

NDAC オーセンティケータを識別し、NDAC の完了を確認するには、このコマンドを使用します。

例

次に、atlas という名前のデバイスによって acs1 のオーセンティケータ ID（A-ID–Info）を使用して Cisco ACS から受け取った Protected Access Credential（PAC）を表示する例を示します。

```
Router# show cts pacs
  AID: 1100E046659D4275B644BF946EFA49CD
  PAC-Info:
    PAC-type = Cisco Trustsec
    AID: 1100E046659D4275B644BF946EFA49CD
    I-ID: atlas
    A-ID-Info: acs1
    Credential Lifetime: 13:59:27 PDT Jun 5 2010
  PAC-Opaque: 000200B000030001000400101100E046659D4275B644BF946EFA49CD0006009400
0301008285A14CB259CA096487096D68D5F34D000000014C09A6AA00093A808ACA80B39EB656AF0B
CA91F3564DF540447A11F9ECDFA4AEC3A193769B80066832495B8C40F6B5B46B685A68411B7DF049
A32F2B03F89ECF948AC4BB85CF855CA186BEF8E2A8C69A7C0BE1BDF6EC27D826896A31821A7BA523
C8BD90072CB8A8D0334F004D4B627D33001B0519D41738F7EDDF3A
  Refresh timer is set for 00:01:24
```

関連コマンド

コマンド	説明
clear cts pac	キーストアから 1 つまたはすべての PAC をクリアします。
cts sxp	ネットワーク デバイスに SXP を設定します。

show cts policy layer3

CTS レイヤ 3 トランスポート コンフィギュレーションに使用されるトラフィック ポリシーおよび例外ポリシーの名前を表示するには、EXEC モードまたは特権 EXEC モードで **show cts policy layer3** コマンドを使用します。

show cts policy layer3 {**ipv4** | **ipv6**}

構文の説明

ipv4	IPv4 ポリシーを指定します。
ipv6	IPv6 ポリシーを指定します

デフォルト

なし

コマンド モード

EXEC（>）、特権 EXEC（#）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(50) SY	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

トラフィックまたは例外ポリシーは、ローカルで設定されるか、Cisco Secure ACS から取得されます。CTS レイヤ 3 トランスポート機能の詳細については、「cts policy layer3」を参照してください。

例

次に、**show cts policy3** のコマンドの出力を表示します。

```
router# show cts policy layer3 ipv4
No CTS L3 IPV4 policy received from ACS
Local CTS L3 IPv4 exception policy name  : cts-exceptions-local
Local CTS L3 IPv4 traffic policy name     : cts-traffic-local
Current CTS L3 IPv4 exception policy name: cts-exceptions-local
Current CTS L3 IPv4 traffic policy name   : cts-traffic-local
```

関連コマンド

コマンド	説明
cts policy layer3	CTS レイヤ 3 トランスポートのトラフィック ポリシーおよび例外ポリシーを指定します。
cts layer3	トラフィック ポリシーおよび例外ポリシーをイネーブルにし、CTS のレイヤ 3 トランスポート ゲートウェイ インターフェイスに適用します。

show cts policy peer

TrustSec ピアのピア認可ポリシーのデータを表示するには、EXEC モードまたは特権 EXEC モードで **show cts policy peer** コマンドを使用します。

show cts policy peer

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。

デフォルト　なし

コマンド モード　EXEC（>）、特権 EXEC（#）

サポートされるユーザ ロール　Administrator

コマンド履歴

リリース	変更点
12.2(33) SXI	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

例　次に、すべてのピアの TrustSec ピア認可ポリシーを表示する例を示します。

```
VSS-1# show cts policy peer
CTS Peer Policy
===============
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
```

出力フィールド	説明
Peer name	ローカル デバイスが接続されたピアの CTS デバイス ID。
Peer SGT	ピアのセキュリティ グループ タグ。
Trusted Peer	TRUE：ローカル デバイスはこのピアから送信される SGT タグが付けられたパケットを信頼します。 FALSE：デバイスはこのピアから送信される SGT タグが付けられたパケットを信頼しません。
Peer Policy Lifetime	リフレッシュされるまでの、ポリシーが有効な時間の長さ。
Peer Last update time	このポリシーが最後にリフレッシュされた時刻
Policy expires in (dd:hr:mm:sec)	このピア ポリシーはこの時間が経過すると期限切れになります

出力フィールド	説明
Policy refreshes in 0:00:01:51 (dd:hr:mm:sec)	このピア ポリシーはこの時間が経過するとリフレッシュされます
Cache data applied = NONE	このポリシーはキャッシュから入力されませんでした。つまり、ACS から取得されました

関連コマンド

コマンド	説明
cts refresh	ピア認可ポリシーを強制的にリフレッシュします。
clear cts policy	TrustSec ピアのピア認可ポリシーをクリアします。

show cts provisioning

待機中の RADIUS サーバ CTS プロビジョニング ジョブを表示するには、EXEC モードまたは特権 EXEC モードで **show cts provisioning** コマンドを使用します。

show cts provisioning

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。

デフォルト

なし

コマンド モード

EXEC（>）、特権 EXEC（#）

サポートされるユーザ ロール

Administrator

コマンド履歴

使用上のガイドライン

Protected Access Credential Provisioning（PAC-provisioning）ジョブ用のキューを表示するには、このコマンドを使用します。PAC が期限切れになるか、またはデバイスが再設定されたときに再プロビジョニングが発生します。

例

次の出力では、CTS のプロビジョニング ドライバが PAC プロビジョニングを再試行している AAA サーバのリストを表示します。

```
router# show cts provisioning
A-ID: 0b2d160f3e4dcf4394262a7f99ea8f63
   Server 41.16.19.201, using existing PAC
      Req-ID EB210008: callback func 418A8990, context 290F14D0
A-ID: Unknown
   Server 41.16.19.203, using shared secret
      Req-ID 49520002: callback func 40540CF0, context AE000007
```

関連コマンド

コマンド	説明
show cts pacs	キーストアの PAC の A-ID および PAC 情報を表示します。
radius-server host	デバイス認証用に RADIUS サーバを指定します。

show cts role-based counters

セキュリティ グループ ACL 強制の統計情報を表示するには、**show cts role-based** カウンタの show コマンドを使用します。カウンタをクリアするには、**clear cts role-based counters** コマンドを使用します。

show cts role-based counters

show cts role-based counters default [**ipv4** | **ipv6**]

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

show cts role-based counters to {*sgt_num* | **unknown**} [**ipv4** | **ipv6** | **]**

show cts role-based counters [**ipv4** | **ipv6**]

構文の説明

default	デフォルト ポリシー カウンタ
from	送信元セキュリティ グループを指定します
ipv4	IP バージョン 4 ネットワークでセキュリティ グループを指定します
ipv6	IP バージョン 6 ネットワークでセキュリティ グループを指定します
to	宛先セキュリティ グループを指定します
sgt_num	（0 ～ 65533）セキュリティ グループ タグ番号を指定します
unknown	すべての送信元グループを指定します

コマンド モード

EXEC（>）、特権 EXEC（#）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(50) SY	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

セキュリティ グループ ACL（SGACL）強制の統計情報を表示するには、**show cts role-based counters** コマンドを使用します。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** 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。

例

次の例は、IPv4 および IPv6 イベントのすべての強制の統計情報を表示します。

```
router# show cts role-based counters
Role-based counters
From    To      SW-Denied       HW-Denied       SW-Permitted    HW_Permitted
2       5       129                 89762               421      7564328
```

```
3        5          37                123456                1325      12345678
3        7           0                 65432                 325       2345678
```

関連コマンド

コマンド	説明
clear cts role-based counters	セキュリティ グループ ACL 統計情報カウンタをリセットします。
cts role-based	手動で送信元 IP アドレスをホストまたは VRF 上のセキュリティ グループ タグ（SGT）にマッピングし、SGACL 強制をイネーブルにします。

show cts role-based sgt-map

SXP 送信元 IP と SGT のバインディング テーブル（IP-SGT バインディング）を表示するには、EXEC モードまたは特権 EXEC モードで **show cts role-based sgt-map** コマンドを使用します。

show cts role-based sgt-map {*ipv4_dec* | *ipv4_cidr* | *ipv6_hex* | *ipv6_cidr* | **all** [**ipv4** | **ipv6**] | **host** {*ipv4_decimal* | *ipv6_dec*} | **summary** [**ipv4** | **ipv6**] |

vrf *instance_name* {*ipv4_dec* | *ipv4_cidr* | *ipv6_dec* | *ipv6_cidr* | **all** {**ipv4** | **ipv6**} | **host** {*ipv4_decimal* | *ipv6_dec*} |**summary** {**ipv4** | **ipv6**} }

構文の説明

ipv4_dec	ドット付き 10 進数表記で IPv4 アドレスを指定します。 例（208.77.188.166）
ipv4_cidr	Classless Inter-Domain Routing（CIDR）で IPv4 アドレス範囲を指定します。たとえば、35.0.0.0/8 では、/8 は最上位 8 ビットがネットワークを識別し、最下位 24 ビットがホストを識別することを表します。
ipv6_hex	コロンで区切られた 16 進数の IP Version 6 アドレスを指定します。 たとえば、2001:db8:85a3::8a2e:370:7334 です。
ipv6_cidr	16 進数の CIDR 表記で IPv6 アドレスの範囲を指定します。
host *ipv4_decimal* | *ipv6_hex*	特定の IPv4 または IPv6 ホストのマッピングを指定します。IPv4 にはドット付き 10 進数、IPv6 にはコロン 16 進数を使用します。
all	表示されるすべてのマッピングを指定します。
summary ipv4 | **ipv6**	IPv4 または IPv6 マッピングの概要。キーワードを指定しない場合、IPv4 と IPv6 の両方を表示します。
vrf *instance_name*	マッピング用の VPN ルーティング/転送インスタンスを指定します。

デフォルト

なし

コマンド モード

EXEC（>）、特権 EXEC（#）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2 (33) SXI3	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。
12.2 (50) SG7	このコマンドが Catalyst 4000 シリーズ スイッチに追加されました（**vrf** キーワードなし）。
12.2 (53) SE2	このコマンドは、Catalyst 3750(E) および 3560(E) シリーズ スイッチに追加されました（**vrf** キーワードなし）。
12.2 (53) SE2	このコマンドが Catalyst 3750(X) シリーズ スイッチに追加されました（**vrf** キーワードなし）。

使用上のガイドライン

SXP が適切なセキュリティ グループ タグ（SGT）に送信元 IP アドレスを正しくバインドしていることを確認するには、このコマンドを使用します。VRF のレポートは、特権 EXEC モードからだけ使用できます。

例

次の例は、IP アドレスおよび SGT の送信元名のバインディングを表示します。

```
Router# show cts role-based sgt-map all
Active IP-SGT Bindings Information

IP Address    SGT Source
============================================
1.1.1.1       7   INTERNAL
10.252.10.1   7   INTERNAL
10.252.10.10  3   LOCAL
10.252.100.1  7   INTERNAL
172.26.208.31 7   INTERNAL

IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 1
Total number of INTERNAL bindings = 4
Total number of active   bindings = 5
```

関連コマンド

コマンド	説明
cts role-based	手動でセキュリティ グループ タグ（SGT）に送信元 IP アドレスをマッピングします。
cts sxp	ネットワーク デバイスに SXP を設定します。
show cts sxp	CTS SXP プロトコル情報を表示します

show cts server-list

TrustSec シードおよび非シード デバイスで利用可能な RADIUS サーバのリストを表示するには、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、コマンドまたはキーワードはありません。

デフォルト

なし

コマンド モード

EXEC（>）、特権 EXEC（#）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(33) SXI	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

例

次の例は、TrustSec RADIUS サーバ リストを表示します。

```
Router> 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
cts server	CTS のサーバ リストの設定を表示します。

show cts sxp

SXP 接続または SourceIP-to-SGT マッピング情報を表示するには、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** | **sgt-map**} [**brief** | **vrf** *instance_name*]

構文の説明

connections	CTS SXP 接続情報を表示します。
sgt-map	SXP 経由で受信した IP-SGT マッピングを表示します。
brief	（任意）SXP 情報の省略形を表示します。
vrf *instance_name*	（任意）指定された VRF インスタンス名の SXP 情報を表示します。

デフォルト

なし

コマンド モード

EXEC（>）、特権 EXEC（#）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(33) SXI	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。
12.2 (50) SG7	このコマンドが、Catalyst 4000 シリーズ スイッチに追加されました
12.2 (53) SE2	このコマンドが Catalyst 3750(E) および 3560(E) シリーズ スイッチに追加されました。
12.2 (53) SE2	このコマンドが、Catalyst 3750(X) シリーズ スイッチに追加されました。

使用上のガイドライン

ネットワーク デバイスの SXP 設定のステータスを表示するには、**cts sxp connections** のコマンドを使用します。現在の SourceIP-to-SGT のマッピング データベースを表示するには、**cts sxp sgt-map** コマンドを使用します。

例

次の例では、Catalyst 6500 シリーズ スイッチのデフォルト SXP の設定を表示します。

```
Router# show cts sxp connections
 SXP              : Disabled
 Default Password : Not Set
 Default Source IP: Not Set
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is not running
There are no SXP Connections.
```

次に、**brief** キーワードを使用して Catalyst 6500 スイッチの SXP 接続を表示する例を示します。

```
Router# 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
------------------------------------------------------------------------------
2.2.2.1          2.2.2.2          On                0:00:02:14 (dd:hr:mm:sec)
3.3.3.1          3.3.3.2          On                0:00:02:14 (dd:hr:mm:sec)

Total num of SXP Connections = 2
```

次の例では、Catalyst 6500 シリーズ スイッチの SXP 接続を表示します。

```
Router# 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          : 2.2.2.1
Source IP        : 2.2.2.2
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          : 3.3.3.1
Source IP        : 3.3.3.2
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
```

次の例は、SXP スピーカーへの接続が切断された SXP リスナーからの出力を表示します。SourceIP-to-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。

```
Router# 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          : 2.2.2.1
Source IP        : 2.2.2.2
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          : 3.3.3.1
Source IP        : 3.3.3.2
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
```

次の例は、SXP を介して学習された現在の SourceIP-to-SGT マッピング データベースを表示します。

```
router# show cts sxp sgt-map
IP-SGT Mappings as follows:
IPv4,SGT: <2.2.2.1 , 7>
source  : SXP;
Peer IP : 2.2.2.1;
Ins Num : 1;
IPv4,SGT: <2.2.2.1 , 7>
source  : SXP;
Peer IP : 3.3.3.1;
Ins Num : 1;
Status  : Active;
IPv4,SGT: <3.3.3.1 , 7>
source  : SXP;
Peer IP : 2.2.2.1;
Ins Num : 1;
```

次の例は、**brief** キーワードを使用して現在の SourceIP-to-SGT マッピング データベースを表示します。

```
Router# show cts sxp sgt-map brief
IP-SGT Mappings as follows:
IPv4,SGT: <2.2.2.1 , 7>
IPv4,SGT: <3.3.3.1 , 7>
IPv4,SGT: <4.4.4.1 , 7>
IPv4,SGT: <43.13.21.41 , 7>
```

関連コマンド

コマンド	説明
cts sxp	ネットワーク デバイスに SXP を設定します。

show cts keystore

ソフトウェアまたはハードウェア暗号化キーストアの内容を表示するには、EXEC モードまたは特権 EXEC モードで **show cts keystore** コマンドを使用します。

show cts keystore

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。

デフォルト　なし

コマンド モード　EXEC（>）、特権 EXEC（#）

サポートされるユーザ ロール　Administrator

コマンド履歴

リリース	変更点
12.2(33) SXI	このコマンドが **show cts keystore** として Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン　このコマンドは、キーストアに保存されているすべてのレコードを示します。保存された秘密は表示されません。

例　次の例は、Catalyst 6500 ソフトウェア エミュレート キーストアの内容を表示します。

```
Router# show cts keystore
No hardware keystore present, using software emulation.
Keystore contains the following records (S=Simple Secret, P=PAC, R=RSA):

Index  Type  Name
-----  ----  ----
    0     P  05181D8147015544BC20F0119BE8717E
    1     S  CTS-password
```

次の例は、Catalyst 6500 ハードウェア キーストアの内容を表示します。

```
Router# show cts keystore
CTS keystore firmware version 2.0.
Keystore contains the following records (S=Simple Secret, P=PAC, R=RSA):

Index  Type  Name
-----  ----  ----
    0     S  CTS-passwordFOX094901KW
    1     P  74656D706F72617279

Hardware Keystore error counters:
       FW Panics = 0
       FW Resets = 0
       RX FIFO underruns = 12
       RX timeouts = 0
```

```
RX bad checksums = 0
RX bad fragment lengths = 0
Corruption Detected in keystore = 0
```

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。
cts sxp	ネットワーク デバイスに SXP を設定します。

show platform cts reflector

特定のインターフェイスの Cisco TrustSec リフレクタ モード（Ingress、Egress、Pure、No CTS）のステータスを表示するには、**show platform cts reflector** コマンドを使用します。

show platformcts reflector interface type *slot*/*port*

構文の説明

interface type *slot*/*port*	ステータスを表示するインターフェイス タイプ、スロット、およびポートを指定します。

コマンド モード

特権 EXEC（#）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(50) SY	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

関連コマンド

コマンド	説明
platform cts	TrustSec 出力または入力のリフレクタをイネーブルにします。

timer（cts do1x インターフェイス サブモード）

dot1x 認証タイマーを設定するには、タイマーの認証の CTS dot1x インターフェイス コンフィギュレーション コマンドを使用します。dot1x 再認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

[no] timer reauthentication *seconds*

構文の説明

reauthentication *seconds*	（0 ～ 2147483）秒単位のタイマー。dot1x 再認証をディセーブルにするには、0 を入力します。

デフォルト

デフォルトの期間は 86,400 秒（24 時間）です。

コマンド モード

CTS dot1x インターフェイス コンフィギュレーション サブモード（config-if-cts-dot1x）

サポートされるユーザ ロール

Administrator

コマンド履歴

リリース	変更点
12.2(33) SXI	このコマンドが、Catalyst 6500 シリーズ スイッチに追加されました。

使用上のガイドライン

認証サーバが期間を指定していない場合は、**timer reauthentication** コマンドを使用して dot1x 再認証期間を設定します。再認証期間が指定されていない場合、デフォルトの期間は 86,400 秒です。dot1x 再認証をディセーブルにするには、このコマンドの **no** 形式を使用するか、または 0 秒の期間を指定します。デフォルト値に戻すには、**default timer reauthentication** コマンドを使用します。

例

次の例では、802.1X 再認証期間を 48 時間（172,800 秒）に設定します。

```
router# config t
router(config)# interface gigabitEthernet 6/1
router(config-if)# cts dot1x
router(config-if-cts-dot1x)# timer reauthentication 172800
```

関連コマンド

コマンド	説明
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。
sap（cts dot1x インターフェイス サブモード）	dot1x モードの CTS SAP を設定します。
propagate（cts dot1x サブモード）	dot1x モードの SGT 伝搬をイネーブルまたはディセーブルにします。