CHAPTER 3

アイデンティティ、接続および SGT の設定

ここでは、次の内容について説明します。

Cisco TrustSec シード デバイスのクレデンシャル、AAA 設定

認証サーバに直接接続されているか、または接続は間接でも TrustSec ドメインを開始する最初のデバイスである Cisco TrustSec 対応デバイスは、シード デバイスと呼ばれます。他の Cisco TrustSec ネットワーク デバイスは非シード デバイスです。

Cisco TrustSec ドメインを開始できるように、シード スイッチで NDAC および AAA をイネーブルにするには、次の手順を実行します。

リリース	機能の履歴
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）。

	コマンド	目的
ステップ 1	`Router# cts credentials id device-id password password`	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。*device-id* 引数は、最大 32 文字で大文字と小文字を区別します。
ステップ 2	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	`Router(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 4	`Router(config)# aaa authentication dot1x default group radius`	RADIUS として 802.1X ポート ベース認証方式を指定します。
ステップ 5	`Router(config)# aaa authorization network mlist group radius`	ネットワーク関連のすべてのサービス要求に対して RADIUS 認証を使用するようにスイッチを設定します。 • *mlist*：Cisco TrustSec AAA サーバ グループ。
ステップ 6	`Router(config)# cts authorization list mlist`	Cisco TrustSec の AAA サーバ グループを指定します。非シード デバイスはオーセンティケータからサーバ リストを取得します。
ステップ 7	`Router(config)# aaa accounting dot1x default start-stop group radius`	RADIUS を使用して 802.1X アカウンティングをイネーブルにします。
ステップ 8	`Router(config)# radius-server host ip-addr auth-port 1812 acct-port 1813 pac key secret`	RADIUS 認証サーバのホスト アドレス、サービス ポートおよび暗号キーを指定します。 • *ip-addr*：認証サーバの IP アドレス。 • *secret*：認証サーバによって共有される暗号キー。
ステップ 9	`Router(config)# radius-server vsa send authentication`	認証段階でスイッチによって生成される RADIUS Access-Request 内のベンダー固有属性（VSA）を認識して使用するようにスイッチを設定します。
ステップ 10	`Router(config)# dot1x system-auth-control`	802.1x ポートベースの認証をグローバルにイネーブルにします。
ステップ 11	`Router(config)# exit`	コンフィギュレーション モードを終了します。

（注）　Cisco Secure ACS でスイッチの Cisco TrustSec クレデンシャルを設定する必要があります（『*Configuration Guide for the Cisco Secure ACS*』を参照）。

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

```
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
```

Cisco TrustSec 非シード デバイスのクレデンシャル、AAA 設定

リリース	機能の履歴
12.2(33) SXI3	この機能が、Catalyst 6500 シリーズ スイッチに追加されました。
IOS-XE 3.3.0 SG	この機能が、Catalyst 4000 シリーズ スイッチに追加されました。
15.0(1)SE	この機能が、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。

Cisco TrustSec ドメインに参加できるように、非シード スイッチで NDAC および AAA をイネーブルにするには、次の手順を実行します。

	コマンド	目的
ステップ 1	`Router# cts credentials id device-id password password`	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。*device-id* 引数は、最大 32 文字で大文字と小文字を区別します。
ステップ 2	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	`Router(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 4	`Router(config)# aaa authentication dot1x default group radius`	RADIUS として 802.1X ポート ベース認証方式を指定します。
ステップ 5	`Router(config)# aaa authorization network mlist group radius`	ネットワーク関連のすべてのサービス要求に対して RADIUS 認証を使用するようにスイッチを設定します。 • *mlist*：Cisco TrustSec の AAA サーバ グループを指定します。
ステップ 6	`Router(config)# aaa accounting dot1x default start-stop group radius`	RADIUS を使用して 802.1X アカウンティングをイネーブルにします。
ステップ 7	`Router(config)# radius-server vsa send authentication`	認証段階でスイッチによって生成される RADIUS Access-Request 内のベンダー固有属性（VSA）を認識して使用するようにスイッチを設定します。
ステップ 8	`Router(config)# dot1x system-auth-control`	802.1x ポートベースの認証をグローバルにイネーブルにします。
ステップ 9	`Router(config)# exit`	コンフィギュレーション モードを終了します。

（注）　Cisco Secure ACS でスイッチの Cisco TrustSec クレデンシャルを設定する必要があります（『*Configuration Guide for the Cisco Secure ACS*』を参照）。

次に、非シード デバイスに Cisco TrustSec の AAA を設定する例を示します。

```
Router# cts credentials id Switch2 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)# aaa accounting dot1x default start-stop group radius
Router(config)# radius-server vsa send authentication
Router(config)# dot1x system-auth-control
Router(config)# exit
```

アップリンク ポートでの 802.1X モードの Cisco TrustSec 認証のイネーブル化

リリース	機能の履歴
12.2(33) SXI3	この機能が、Catalyst 6500 シリーズ スイッチに追加されました。
IOS-XE 3.3.0 SG	この機能が、Catalyst 4000 シリーズ スイッチに追加されました。
15.0(1)SE	この機能が、Catalyst 3750(X) シリーズ スイッチに追加されました。

別の Cisco TrustSec デバイスに接続する各インターフェイスで Cisco TrustSec 認証をイネーブルにする必要があります。別の Cisco TrustSec デバイスにアップリンク インターフェイス上で 802.1X を使用して Cisco TrustSec 認証を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# interface` *type slot/port*	アップリンク インターフェイスのインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	`Router(config-if)# cts dot1x`	アップリンク インターフェイスを NDAC 認証を実行するように設定します。
ステップ 4	`Router(config-if-cts-dot1x)# [no] sap mode-list` *mode1* [*mode2* [*mode3* [*mode4*]]]	（任意）インターフェイスに SAP 動作モードを設定します。インターフェイスは相互に受け入れ可能なモード用のピアとネゴシエートします。優先順位で許容されるモードをリストします。*mode* の選択肢は次のとおりです。 • **gcm**：認証および暗号化 • **gmac**：認証あり、暗号化なし • **no-encap**：カプセル化なし • **null**：カプセル化あり、認証なし、暗号化なし **（注）** インターフェイスで SGT 挿入またはデータ リンク暗号化を使用できない場合は、デフォルトおよび唯一使用可能な SAP 動作モードは **no-encap** です。
ステップ 5	`Router(config-if-cts-dot1x)# [no] timer reauthentication` *seconds*	（任意）認証サーバが期間を指定しなかった場合、再認証期間を使用するように設定します。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 86400 秒です。

	コマンド	目的
ステップ 6	`Router(config-if-cts-dot1x)# [no] propagate sgt`	（任意）このコマンドの **no** 形式は、ピアが SGT を処理できない場合に使用されます。**no propagate sgt** コマンドを使用すると、インターフェイスからピアに SGT が送信されなくなります。
ステップ 7	`Router(config-if-cts-dot1x)# exit`	Cisco TrustSec 802.1X インターフェイス コンフィギュレーション モードを終了します。
ステップ 8	`Router(config-if)# shutdown`	インターフェイスをディセーブルにします。
ステップ 9	`Router(config-if)# no shutdown`	インターフェイスをイネーブルにして、インターフェイスの Cisco TrustSec 認証をイネーブルにします。
ステップ 10	`Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。

この例では、優先 SAP モードとして GCM を使用しているインターフェイス上で、802.1X モードで Cisco TrustSec 認証をイネーブルにする方法を示します。認証サーバは、再認証タイマーを提供していません。

```
Router# configure terminal
Router(config)# interface gi2/1
Router(config-if)# cts dot1x
Router(config-if-cts-dot1x)# sap mode-list gcm null no-encap
Router(config-if-cts-dot1x)# timer reauthentication 43200
Router(config-if-cts-dot1x)# exit
Router(config-if)# shutdown
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# exit
```

アップリンク ポートでの手動モードによる Cisco TrustSec 認証の設定

リリース	機能の履歴
IOS 12.2(50) SY	この機能が、Catalyst 6500 シリーズ スイッチに追加されました。
IOS-XE 3.3.0 SG	この機能が、Catalyst 4000 シリーズ スイッチに追加されました。
IOS 15.0(1) SE	この機能が、Catalyst 3750(X) シリーズ スイッチに追加されました。

スイッチが認証サーバにアクセスできない場合、または 802.1X 認証が必要でない場合には、インターフェイスで Cisco TrustSec を手動で設定できます。接続の両側のインターフェイスに手動で設定する必要があります。

別の Cisco TrustSec デバイスにアップリンク インターフェイス上で手動で Cisco TrustSec を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# interface` *type slot/port*	アップリンク インターフェイスのインターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	`Router(config-if)# cts manual`	Cisco TrustSec 手動コンフィギュレーション モードを開始します。
ステップ 4	`Router(config-if-cts-manual)# [no] sap pmk key [mode-list mode1 [mode2 [mode3 [mode4]]]]`	（任意）SAP の Pairwise Master Key（PMK）と動作モードを設定します。Cisco TrustSec の手動モードでは、SAP はデフォルトでディセーブルになっています。 • *key*：文字数が偶数個で最大 32 文字の 16 進値。 SAP 動作の *mode* オプションは次のとおりです。 • **gcm**：認証および暗号化 • **gmac**：認証あり、暗号化なし • **no-encap**：カプセル化なし • **null**：カプセル化あり、認証または暗号化なし **（注）** インターフェイスで SGT 挿入またはデータリンク暗号化を使用できない場合は、デフォルトおよび唯一使用可能な SAP 動作モードは **no-encap** です。
ステップ 5	`Router(config-if-cts-manual)# [no] policy dynamic identity peer-name`	（任意）ピアのアイデンティティに基づいた認可サーバからの認可ポリシーの動的ダウンロードを許可するようにアイデンティティ ポート マッピング（IPM）を設定します。この作業の次に記載されている追加の使用上の注意を参照してください。 • *peer-name*：ピア デバイスの Cisco TrustSec デバイス ID。ピア名では、大文字と小文字が区別されます。 **（注）** Cisco TrustSec クレデンシャルが設定されていることを確認します（「Cisco TrustSec シード デバイスのクレデンシャル、AAA 設定」（P.3-1）を参照）。
	`Router(config-if-cts-manual)# [no] policy static sgt tag [trusted]`	（任意）スタティック許可ポリシーを設定します。この作業の次に記載されている追加の使用上の注意を参照してください。 • *tag*：10 進表記の SGT。指定できる範囲は 1 ～ 65533 です。 • **trusted**：この SGT を使用するインターフェイスの入力トラフィックのタグを上書きしてはいけないことを示します。
ステップ 6	`Router(config-if-cts-manual)# [no] propagate sgt`	（任意）このコマンドの **no** 形式は、ピアが SGT を処理できない場合に使用されます。**no propagate sgt** コマンドを使用すると、インターフェイスからピアに SGT が送信されなくなります。
ステップ 7	`Router(config-if-cts-manual)# exit`	Cisco TrustSec 手動インターフェイス コンフィギュレーション モードを終了します。
ステップ 8	`Router(config-if)# shutdown`	インターフェイスをディセーブルにします。

	コマンド	目的
ステップ 9	`Router(config-if)# no shutdown`	インターフェイスをイネーブルにして、インターフェイスの Cisco TrustSec 認証をイネーブルにします。
ステップ 10	`Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。

アイデンティティ ポート マッピング（IPM）は、そのポートに着信するすべてのトラフィックに対して、単一の SGT が適用されるように、物理ポートを設定します。この SGT は、新しいバインディングが取得されるまで、そのポートから発信されるすべての IP トラフィックに適用されます。IPM は次のように設定されます。

- CTS 手動インターフェイス コンフィギュレーション モードで **policy static sgt** *tag* コマンドを使用
- CTS 手動インターフェイス コンフィギュレーション モードで **policy dynamic identity** *peer-name* コマンドを使用。Cisco ACS または Cisco ISE 設定では、*peer-name* は non-trusted に指定されています。

IPM は、次のポートでサポートされます。

- ルーテッド ポート
- アクセス モードのスイッチ ポート
- トランク モードのスイッチ ポート

インターフェイスの Cisco TrustSec を手動で設定する場合は、次のような使用上の注意事項、および制約事項を考慮してください。

- SAP パラメータが定義されていない場合、Cisco TrustSec カプセル化または暗号化は行われません。
- 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。
  - **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。

次に、インターフェイスに Cisco TrustSec 認証を手動モードで設定する例を示します。

```
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)# exit
```

```
Router(config-if)# shutdown
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# exit
```

インターフェイスの SAP キーの再生成

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。SAP キー リフレッシュは通常、ネットワーク イベントおよび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。

機能	履歴
12.2(50) SY	この機能が、Catalyst 6500 シリーズ スイッチに追加されました。
IOS-XE 3.3.0 SG	この機能が、Catalyst 4000 シリーズ スイッチに追加されました。
15.0(1)SE	この機能が、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。

	コマンド	目的
ステップ 1	`Router# cts rekey interface int slot/port`	MACsec リンクで SAP キーの再ネゴシエーションを強制します。

Cisco TrustSec インターフェイス設定の確認

TrustSec-relate MLS インターフェイスの設定を表示するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# show cts interface [interface type slot/port | brief | summary]`	TrustSec-related インターフェイス コンフィギュレーションを表示します。

次に、TrustSec-related インターフェイス コンフィギュレーションを表示する例を示します。

```
Router# show cts interface interface gi3/3

Global Dot1x feature is Enabled
Interface GigabitEthernet3/3:
    CTS is enabled, mode:    DOT1X
    IFC state:               OPEN
    Authentication Status:   SUCCEEDED
        Peer identity:       "sanjose"
        Peer's advertised capabilities: ""
        802.1X role:         Supplicant
        Reauth period applied to link:  Not applicable to Supplicant role
    Authorization Status:    SUCCEEDED
        Peer SGT:            11
        Peer SGT assignment: Trusted
    SAP Status:              NOT APPLICABLE
        Configured pairwise ciphers:
            gcm-encrypt
            null

        Replay protection:      enabled
```

```
        Replay protection mode: OUT-OF-ORDER

        Selected cipher:

    Cache Info:
        Expiration            : 23:32:40 PDT Jun 22 2009
        Cache applied to link : NONE
        Expiration            : 23:32:40 PDT Jun 22 2009

    Statistics:
        authc success:              1
        authc reject:               0
        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

Dot1x Info for GigabitEthernet3/1
-----------------------------------
PAE                       = SUPPLICANT
StartPeriod               = 30
AuthPeriod                = 30
HeldPeriod                = 60
MaxStart                  = 3
Credentials profile       = CTS-ID-profile
EAP profile               = CTS-EAP-profile
Dot1x Info for GigabitEthernet3/1
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = FORCE_AUTHORIZED
ControlDirection          = Both
HostMode                  = SINGLE_HOST
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 55
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
```

デバイス SGT の手動設定

リリース	機能の履歴
12.2(50) SY	この機能が、Catalyst 6500 シリーズ スイッチに追加されました。

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。

デバイスの SGT を手動で設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# cts sgt tag`	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。
ステップ 3	`Router(config)# exit`	コンフィギュレーション モードを終了します。

次に、デバイス 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
```

IP-Address-to-SGT マッピングの手動設定

リリース	機能の履歴
12.2(50) SY	この機能が、Catalyst 6500 シリーズ スイッチに追加されました。
15.0(0)SY	SXPv3 が Catalyst 6500 スイッチに追加されました。 次のキーワードが、Catalyst 6500 シリーズ スイッチの **cts role-based sgt-map** コマンドに追加されました。 • *ipv4-address/prefix* • *ipv6-address/prefix* • **interface**

この項では、SGT と送信元 IP アドレスのマッピングについて説明します。

- 「サブネットと SGT のマッピング」（P.3-10）
- 「VLAN と SGT のマッピング」（P.3-15）
- 「レイヤ 3 論理インターフェイスと SGT のマッピング（L3IF-SGT マッピング）」（P.3-19）

cts インターフェイス手動モードでのアイデンティティ ポート マッピングについては、次の項を参照してください。

- 「アップリンク ポートでの手動モードによる Cisco TrustSec 認証の設定」（P.3-5）

サブネットと SGT のマッピング

サブネットと SGT のマッピングは、指定したサブネット内のすべてのホスト アドレスに SGT をバインドします。TrustSec は着信パケットの送信元 IP アドレスが指定したサブネットに属する場合そのパケットに SGT を適用します。サブネットおよび SGT は、**cts role-based sgt-map** *net_address*/*prefix* **sgt** *sgt_number* 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 CLI で指定されます。単一のホストは、このコマンドでマップされる可能性があります。

IPv4 ネットワークでは、SXPv3 以降のバージョンは SXPv3 ピアからサブネットの *net_address*/*prefix* ストリングを受信し、解析できます。以前の SXP バージョンは SXP リスナー ピアへエクスポートする前にサブネット プレフィックスをホストのバインディングのセットに変換します。

たとえば、IPv4 サブネット 198.1.1.0 /29 は次のように拡張されます（ホスト アドレスの 3 ビットのみ）。

- ホスト アドレス 198.1.1.1 ～ 198.1.1.7：タグ付けされ SXP ピアに伝播されます。
- ネットワーク、およびブロードキャスト アドレス 198.1.1.0 および 198.1.1.8：タグ付けされず、伝播しません。

SXPv3 がエクスポートできるサブネット バインディング数は制限するには、**cts sxp mapping network-map** 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。

サブネット バインディングはスタティックで、アクティブ ホストの学習はありません。これらは SGT インポジションおよび SGACL の強制にローカルで使用できます。サブネットと SGT のマッピングによってタグ付けされたパケットは、レイヤ 2 またはレイヤ 3 TrustSec リンクに伝播できます。

IPv6 ネットワークの場合、SXPv3 は SXPv2 または SXPv1 ピアにサブネット バインディングをエクスポートできません。

サブネットと SGT のマッピングの機能履歴

機能名	リリース	機能情報
サブネットと SGT のマッピング	15.0 (1) SY	このコマンドのサポートが Catalyst 6500 シリーズ スイッチの SXPv3 で導入されました。関連する CLI は以前のリリースで表示されています。

デフォルト設定値

この機能には、デフォルト設定はありません。

サブネットと SGT のマッピングの設定

ここでは、次の内容について説明します。

- 「サブネットと SGT マッピング設定の確認」（P.3-13）
- 「サブネットと SGT のマッピングの設定」（P.3-11）

制約事項

- /31 プレフィックスの IPv4 サブ ネットワークを拡張できません。
- サブネット ホスト アドレスは、**network-map** *bindings* パラメータが、指定したサブネットのサブネット ホストの合計数よりも小さいか、*bindings* が 0 の場合、SGT にバインドできません。
- SXP スピーカーおよびリスナーが SXPv3 以降のバージョンを実行している場合のみ、IPv6 拡張および伝播が実行されます。

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** switch# config t switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[**no**] **cts sxp mapping network-map** *bindings* **Example:** switch(config)# cts sxp mapping network-map 10000	サブネットと SGT のマッピングのホスト数の制限を設定します。*bindings* 引数は、SGT にバインドされ、SXP リスナーにエクスポートできるサブネット IP ホストの最大数を指定します。 • *bindings*：（0 ～ 65,535）デフォルトは 0（実行される拡張なし）
ステップ 3	[**no**] **cts role-based sgt-map** *ipv4_address/prefix* **sgt** *number* **Example:** switch(config)# cts role-based sgt-map 10.10.10.10/29 sgt 1234	（IPv4）CIDR 表記でサブネットを指定します。サブネットと SGT のマッピング設定を取り消すには、このコマンドの **no** 形式を使用します。ステップ 2 で指定するバインディングの数は、サブネット上のホスト アドレスの数以上である必要があります（ネットワーク、およびブロードキャスト アドレスを除く）。**sgt** *number* キーワードは、指定したサブネットの各ホスト アドレスにバインドするセキュリティ グループ タグを指定します。 • *ipv4_address*：ドット付き 10 進表記で IPv4 ネットワーク アドレスを指定します。 • *prefix*：（0 ～ 30）。ネットワーク アドレスのビット数を指定します。 • **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。
ステップ 4	[**no**] **cts role-based sgt-map** *ipv6_address::prefix* **sgt** *number* **Example:** switch(config)# cts role-based sgt-map 2020::/64 sgt 1234	（IPv6）コロン 16 進表記でサブネットを指定します。サブネットと SGT のマッピング設定を取り消すには、このコマンドの **no** 形式を使用します。 ステップ 2 で指定するバインディングの数は、サブネット上のホスト アドレスの数以上である必要があります（ネットワーク、およびブロードキャスト アドレスを除く）。**sgt** *number* キーワードは、指定したサブネットの各ホスト アドレスにバインドするセキュリティ グループ タグを指定します。 • *ipv6_address*：コロン 16 進表記で IPv6 ネットワーク アドレスを指定します。 • *prefix*：（0 ～ 128）。ネットワーク アドレスのビット数を指定します。 • **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。

	コマンド	目的
ステップ 5	**exit** **Example:** switch(config)# exit switch#	グローバル コンフィギュレーション モードを終了します。
ステップ 6	**show running-config** | include *search_string* **Example:** switch# show running-config | include sgt 1234 switch# show running-config | include network-map	実行コンフィギュレーションに **cts role-based sgt-map** および **cts sxp mapping network-map** コマンドがあることを確認します。
ステップ 7	**copy running-config startup-config** **Example:** switch# copy running-config startup-config	実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

サブネットと SGT マッピング設定の確認

サブネットと SGT のマッピング設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show cts sxp connections	SXP スピーカーとリスナーの接続と、動作ステータスを表示します。
show cts sxp sgt-map	SXP リスナーにエクスポートした IP と SGT のバインディングを表示します。
show running-config	サブネットと SGT のコンフィギュレーション コマンドが実行コンフィギュレーション ファイル内にあることを確認します。

これらのコマンド出力に含まれるフィールドの詳細については、第 7 章「Cisco TrustSec コマンドの概要」を参照してください。

サブネットと SGT のマッピングの設定例

次に、SXPv3 を実行している 2 台の Catalyst 6500 シリーズ スイッチ（Switch1 と Switch2）間で IPv4 のサブネットと SGT のマッピングを設定する例を示します。

ステップ 1　Switch1（1.1.1.1）とスイッチ 2（2.2.2.2）間の SXP スピーカー / リスナー ピアリングを設定します。

```
Switch1# config t
Switch1(config)# cts sxp enable
```

```
Switch1(config)# cts sxp default source-ip 1.1.1.1
Switch1(config)# cts sxp default password 1syzygy1
Switch1(config)# cts sxp connection peer 2.2.2.2 password default mode local speaker
```

ステップ 2　Switch1 の SXP リスナーとしてスイッチ 2 を設定します。

```
Switch2(config)# cts sxp enable
Switch2(config)# cts sxp default source-ip 2.2.2.2
Switch2(config)# cts sxp default password 1syzygy1
Switch2(config)# cts sxp connection peer 1.1.1.1 password default mode local listener
```

ステップ 3　Switch2 で、SXP 接続が動作していることを確認してください。

```
Switch2# show cts sxp connections brief | include 1.1.1.1
     1.1.1.1          2.2.2.2          On               3:22:23:18 (dd:hr:mm:sec)
```

ステップ 4　サブネットワークを Switch1 に拡張されるように設定します。

```
Switch1(config)# cts sxp mapping network-map 10000
Switch1(config)# cts role-based sgt-map 10.10.10.0/30 sgt 101
Switch1(config)# cts role-based sgt-map 11.11.11.0/29 sgt 11111
Switch1(config)# cts role-based sgt-map 192.168.1.0/28 sgt 65000
```

ステップ 5　Switch2 で、Switch1 からのサブネットと SGT の拡張を確認します。ここには、10.10.10.0/30 サブネットワーク用の拡張が 2 個、11.11.11.0/29 サブネットワーク用の拡張が 6 個、192.168.1.0/28 サブネットワーク用の拡張が 14 個存在する必要があります。

```
Switch2# show cts sxp sgt-map brief | include 101|11111|65000
    IPv4,SGT: <10.10.10.1 , 101>
    IPv4,SGT: <10.10.10.2 , 101>
    IPv4,SGT: <11.11.11.1 , 11111>
    IPv4,SGT: <11.11.11.2 , 11111>
    IPv4,SGT: <11.11.11.3 , 11111>
    IPv4,SGT: <11.11.11.4 , 11111>
    IPv4,SGT: <11.11.11.5 , 11111>
    IPv4,SGT: <11.11.11.6 , 11111>
    IPv4,SGT: <192.168.1.1 , 65000>
    IPv4,SGT: <192.168.1.2 , 65000>
    IPv4,SGT: <192.168.1.3 , 65000>
    IPv4,SGT: <192.168.1.4 , 65000>
    IPv4,SGT: <192.168.1.5 , 65000>
    IPv4,SGT: <192.168.1.6 , 65000>
    IPv4,SGT: <192.168.1.7 , 65000>
    IPv4,SGT: <192.168.1.8 , 65000>
    IPv4,SGT: <192.168.1.9 , 65000>
    IPv4,SGT: <192.168.1.10 , 65000>
    IPv4,SGT: <192.168.1.11 , 65000>
    IPv4,SGT: <192.168.1.12 , 65000>
    IPv4,SGT: <192.168.1.13 , 65000>
    IPv4,SGT: <192.168.1.14 , 65000>
```

ステップ 6　Switch1 拡張数を確認します。

```
Switch1# show cts sxp sgt-map

    IP-SGT Mappings expanded:22
    There are no IP-SGT Mappings
```

ステップ 7　設定をスイッチ 1 およびスイッチ 2 に保存し、グローバル コンフィギュレーション モードを終了します。

```
Switch1(config)# copy running-config startup-config
Switch1(config)# exit
Switch2(config)# copy running-config startup-config
```

```
Switch2(config)# exit
```

VLAN と SGT のマッピング

VLAN と SGT のマッピング機能にでは、指定された VLAN からのパケットに SGT をバインドします。これは、次のような点で、レガシーネットワークからの TrustSec 対応ネットワークへの移行を簡素化します。

- レガシーのスイッチ、ワイヤレス コントローラ、アクセス ポイント、VPN などの、TrustSec 対応ではないが VLAN 対応のデバイスをサポートします。
- データセンターのサーバ セグメンテーションなどの、VLAN および VLAN ACL がネットワークを分割するトポロジに対する下位互換性を提供します。

VLAN と SGT のバインディングは **cts role-based sgt-map vlan-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ます。

TrustSec 対応スイッチ上で、スイッチ仮想インターフェイス（SVI）であるゲートウェイが VLAN に割り当てられており、そのスイッチで IP デバイス トラッキングがイネーブルになっている場合、TrustSec は、SVI サブネットにマッピングされている VLAN 上のすべてのアクティブなホストに対して IP と SGT のバインディングを作成できます。

アクティブ VLAN のホストの IP-SGT バインディングは SXP リスナーにエクスポートされます。マッピングされた各 VLAN のバインディングは VRF に関連付けられた IP-to-SGT テーブルに挿入されます。VLAN は SVI または **cts role-based l2-vrf** cts グローバル コンフィギュレーション コマンドでマッピングされます。

VLAN と SGT のバインディングの優先順位は最も低く、SXP または CLI ホスト コンフィギュレーションなどのその他のソースからのバインディングが受信された場合は、無視されます。バインディング優先順位は「バインディング送信元プライオリティ」（P.3-21）に記載しています。

VLAN と SGT のマッピングの機能履歴

表 3-1　VLAN と SGT のマッピングの機能履歴

機能名	リリース	機能情報
VLAN と SGT のマッピング	15.0 (1) SY	このコマンドのサポートが Catalyst 6500 シリーズ スイッチの SXPv3 で導入されました。関連する CLI は以前のリリースで表示されています。

デフォルト設定値

デフォルト設定はありません。

VLAN と SGT のマッピングの設定

ここでは、次の内容について説明します。

- 「VLAN-SGT マッピングを設定するためのタスク フロー」（P.3-16）

VLAN-SGT マッピングを設定するためのタスク フロー

- 着信 VLAN で同じ VLAN_ID で TrustSec スイッチ上に VLAN を作成します。
- エンドポイントのクライアントに対して、デフォルトのゲートウェイになるように TrustSec スイッチの VLAN に SVI を作成します。
- VLAN トラフィックに SGT を適用するように TrustSec スイッチを設定します。
- TrustSec スイッチで IP デバイス トラッキングをイネーブルにします。
- VLAN と SGT のマッピングが TrustSec スイッチで発生することを確認します。

手順の詳細

	コマンド	目的
ステップ 1	**config t** **Example:** TS_switchswitch# config t TS_switchswitch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan** ***vlan_id*** **Example:** TS_switch(config)# vlan 100 TS_switch(config-vlan)#	TrustSec 対応ゲートウェイ スイッチに VLAN 100 を作成し、VLAN コンフィギュレーション サブモードを開始します。
ステップ 3	[**no**] **shutdown** **Example:** TS_switch(config-vlan)# **no shutdown**	VLAN 100 をプロビジョニングします。
ステップ 4	**exit** **Example:** TS_switch(config-vlan)# exit TS_switch(config)#	VLAN コンフィギュレーション モードを終了してグローバル コンフィギュレーション モードを開始します。
ステップ 5	**interface** type *slot/port* **Example:** TS_switch(config)# interface vlan 100 TS_switch(config-if)#	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。
ステップ 6	**ip address** *slot/port* **Example:** TS_switch(config-if)# ip address 10.1.1.2 255.0.0.0	VLAN 100 のスイッチ仮想インターフェイス（SVI）を設定します。
ステップ 7	[**no**] **shutdown** **Example:** TS_switch(config-if)# **no shutdown**	SVI をイネーブルにします。
ステップ 8	**exit** **Example:** TS_switch(config-if)# exit TS_switch(config)#	VLAN インターフェイス コンフィギュレーション モードを終了してグローバル コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 9	**cts role-based sgt-map vlan-list** *vlan_id* **sgt** *sgt_number* **Example:** TS_switch(config)# cts role-based sgt-map vlan-list 100 sgt 10	指定した SGT を指定した VLAN を割り当てます。
ステップ 10	**ip device tracking probe** [**count** *count* | **delay** *seconds* | **interval** *length*] **Example:** TS-switch(config)# **ip device tracking**	IP デバイス トラッキングをイネーブルにします。アクティブ ホストが検出されると、スイッチは IP デバイス トラッキング テーブルに次のエントリを追加します。 • ホストの IP アドレス • ホストの MAC アドレス • ホストの VLAN • スイッチがホストを検出したインターフェイス • ホスト ステート（アクティブまたは非アクティブ） IP デバイス トラッキング テーブルに追加されたホストは、定期的な ARP プローブによって監視されます。応答が得られなかったホストがテーブルから削除されます。
ステップ 11	**exit** **Example:** TS_switch(config)# exit TS_switch#	グローバル コンフィギュレーション モードを終了します。
ステップ 12	**show cts role-based sgt-map** {*ipv4_netaddr* | *ipv4_netaddr/prefix* | *ipv6_netaddr*| *ipv6_netaddr/prefix* | **all** [**ipv4** | **ipv6**] | host {*ipv4__addr* | *ipv6_addr*} | **summary** [**ipv4** | **ipv6**] **Example:** TS_switch# cts role-based sgt-map all	（任意）VLAN と SGT のマッピングを表示します。
ステップ 13	**show ip device tracking {all|interface|ip|mac}** **Example:** TS_switch# show ip device tracking all	（任意）IP デバイス トラッキングの動作ステータスを確認します。
ステップ 14	**copy running-config startup-config** **Example:** TS_switch# copy running-config startup-config	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

VLAN と SGT のマッピングの確認

VLAN と SGT の設定情報を表示するには、次の show コマンドを使用します。

コマンド	目的
show ip device tracking	VLAN のアクティブ ホストの IP アドレスを識別する IP デバイスのトラッキングのステータスを表示します。
show cts role-based sgt-map	IP アドレスと SGT のバインディングを表示します。

これらのコマンドの出力フィールドの詳細については、第 7 章「Cisco TrustSec コマンドの概要」または『Cisco IOS 15.0SY Security and VPN Command Reference』を参照してください。

アクセス リンクを介した 1 つのホストに対する VLAN と SGT のマッピングの設定例

次の例では、単一のホストは、アクセス スイッチ上の VLAN 100 に接続します。アクセス スイッチから Catalyst 6500 シリーズ TrustSec ソフトウェア対応スイッチにアクセス モードのリンクがあります。TrustSec スイッチのスイッチ仮想インターフェイスは VLAN 100 のエンドポイントのデフォルト ゲートウェイになります（IP アドレス 10.1.1.1）。TrustSec スイッチは VLAN 100 からのパケットにセキュリティ グループ タグ（SGT）10 を適用します。

ステップ 1　アクセス スイッチ上に VLAN 100 を作成します。

```
access_switch# config t
access_switch(config)# vlan 100
access_switch(config-vlan)# no shutdown
access_switch(config-vlan)# exit
access_switch(config)#
```

ステップ 2　アクセス リンクとして TrustSec スイッチのインターフェイスを設定します。エンドポイントのアクセス ポートの設定は、この例では省略されます。

```
access_switch(config)# interface gigabitEthernet 6/3
access_switch(config-if)# switchport
access_switch(config-if)# switchport mode access
access_switch(config-if)# switchport access vlan 100
```

ステップ 3　TrustSec スイッチに VLAN 100 を作成します。

```
TS_switch(config)# vlan 100
TS_switch(config-vlan)# no shutdown
TS_switch(config-vlan)# end
TS_switch#
```

ステップ 4　着信 VLAN 100 のゲートウェイとして SVI を作成します。

```
TS_switch(config)# interface vlan 100
TS_switch(config-if)# ip address 10.1.1.2 255.0.0.0
TS_switch(config-if)# no shutdown
TS_switch(config-if)# end
TS_switch(config)#
```

ステップ 5　VLAN 100 のホストにセキュリティ グループ タグ（SGT）10 を割り当てます。

```
TS_switch(config)# cts role-based sgt-map vlan 100 sgt 10
```

ステップ 6　TrustSec スイッチで IP デバイス トラッキングをイネーブルにします。それが動作していることを確認します。

```
TS_switch(config)# ip device tracking
TS_switch# show ip device tracking all

IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 100
--------------------------------------------------------------------
  IP Address     MAC Address   Vlan  Interface              STATE
--------------------------------------------------------------------
Total number interfaces enabled: 1
Vlan100
```

ステップ 7　（任意）エンドポイントからデフォルト ゲートウェイを ping します（この例では、ホスト IP アドレス 10.1.1.1）。SGT 10 が VLAN 100 のホストにマッピングされていることを確認します。

```
TS_switch# show cts role-based sgt-map all

Active IP-SGT Bindings Information

IP Address              SGT     Source
============================================

10.1.1.1                10      VLAN

IP-SGT Active Bindings Summary
============================================
Total number of VLAN     bindings = 1
Total number of CLI      bindings = 0
Total number of active   bindings = 1
```

レイヤ 3 論理インターフェイスと SGT のマッピング（L3IF-SGT マッピング）

L3IF-SGT マッピングは、基盤となる物理インターフェイスに関係なく、次のレイヤ 3 インターフェイスのトラフィックに直接 SGT をマッピングできます:

- ルーテッド ポート
- SVI（VLAN インターフェイス）
- レイヤ 2 ポートのレイヤ 3 サブインターフェイス
- トンネル インターフェイス

（SGT アソシエーションが Cisco ISE または Cisco ACS アクセス サーバから動的に取得される）特定の SGT 番号またはセキュリティ グループ名を指定するには、**cts role-based sgt-map interface** 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。

アイデンティティ ポート マッピング（cts インターフェイス手動サブ モード コンフィギュレーション）および L3IF-SGT が異なる IP と SGT のバインディングを必要とする場合、IPM が優先されます。IP と SGT のバインディングのその他の競合は、「バインディング送信元プライオリティ」（P.3-21）にリストされている優先順位に従って解決されます。

L3IF-SGT マッピングの機能履歴

機能名	リリース	機能情報
L3IF と SGT のマッピング	15.0 (1) SY	このコマンドのサポートが Catalyst 6500 シリーズ スイッチに追加されました。

デフォルト設定

デフォルト設定はありません。

L3IF と SGT のマッピングの設定

手順の詳細

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# cts role-based sgt-map interface` type *slot*/*port* [**security-group** *name* | **sgt** *number*] `Router(config)# cts role-based sgt-map interface gigabitEthernet 1/1 sgt 77`	SGT は指定されたインターフェイスへの入力トラフィックに適用されます。 • **interface** type *slot*/*port* : 使用可能なインターフェイスのリストを表示します。 • **security-group** *name* : SGT ペアリングに対するセキュリティ グループ名は Cisco ISE または Cisco ACS で設定されています。 • **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。
ステップ 3	`Router(config)# exit`	コンフィギュレーション モードを終了します。
ステップ 4	`Router# show cts role-based sgt-map all`	入力トラフィックに指定された SGT がタグ付けされたことを確認します。

L3IF と SGT のマッピングの確認

L3IF と SGT の設定情報を表示するには、次の show コマンドを使用します。

コマンド	目的
show cts role-based sgt-map all	すべての IP アドレスと SGT のバインディングを表示します。

入力ポートでの L3IF と SGT のマッピングの設定例

次の例では、Catalyst 6500 シリーズ スイッチ ラインカードのレイヤ 3 インターフェイスで、すべての入力トラフィックに SGT 3 がタグ付けされるように設定します。接続されたサブネットのプレフィックスがすでにわかっています。

ステップ 1　インターフェイスを設定します。

```
Switch# config t
Switch(config)# interface gigabitEthernet 6/3 sgt 3
Switch(config)# exit
```

ステップ 2　インターフェイスに着信するトラフィックが適切にタグ付けされることを確認します。

```
Router# show cts role-based sgt-map all
IP Address              SGT     Source
============================================
15.1.1.15               4       INTERNAL
17.1.1.0/24             3       L3IF
21.1.1.2                4       INTERNAL
31.1.1.0/24             3       L3IF
31.1.1.2                4       INTERNAL
43.1.1.0/24             3       L3IF
49.1.1.0/24             3       L3IF
50.1.1.0/24             3       L3IF
50.1.1.2                4       INTERNAL
51.1.1.1                4       INTERNAL
52.1.1.0/24             3       L3IF
81.1.1.1                5       CLI
102.1.1.1               4       INTERNAL
105.1.1.1               3       L3IF
111.1.1.1               4       INTERNAL

IP-SGT Active Bindings Summary
============================================
Total number of CLI      bindings = 1
Total number of L3IF     bindings = 7
Total number of INTERNAL bindings = 7
Total number of active   bindings = 15
```

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 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 は **policy** {**dynamic identity** *peer-name* | **static sgt** *tag*} CTS 手動インターフェイス モード コマンド（アイデンティティ ポート マッピング）を使用してインターフェイスに適用されます。現在の優先順位の適用順序は、最も小さい（1）から最高（7）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。

追加認証サーバ関連のパラメータの設定

スイッチと Cisco TrustSec サーバ間の相互対話を設定するには、次の作業を 1 つまたは複数行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Router(config)# [no] cts server deadtime seconds`	（任意）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。
ステップ 3	`Router(config)# [no] cts server load-balance method least-outstanding [batch-size transactions] [ignore-preferred-server]`	（任意）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。 デフォルトの *transactions* は 25 です。 **ignore-preferred-server** キーワードは、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。
ステップ 4	`Router(config)# [no] cts server test {server-IP-address | all} {deadtime seconds | enable | idle-time seconds}`	（任意）指定された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 **idle-time** は 60 秒で、範囲は 1 ～ 14400 です。
ステップ 5	`Router(config)# exit`	コンフィギュレーション モードを終了します。
ステップ 6	`Router# show cts server-list`	Cisco TrustSec サーバのリストのステータスおよび設定の詳細を表示します。

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
```

認証サーバでの新規または交換パスワードの自動設定

リリース	機能の履歴
12.2(50) SY	この機能が、Catalyst 6500 シリーズ スイッチに追加されました。
IOS-XE 3.3.0 SG	この機能が、Catalyst 4000 シリーズ スイッチに追加されました。
15.0(1) SE	この機能が、Catalyst 3750(X) シリーズ スイッチに追加されました。

スイッチと認証サーバ間のパスワードを手動で設定する方法の代替方法として、スイッチからパスワード ネゴシエーションを開始できます。パスワード ネゴシエーションを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Router# **cts change-password server** *ip-address port* {**key** *secret* | **a-id** *a-id*}	スイッチと認証サーバ間のパスワード ネゴシエーションを開始します。 • *ip-address*：認証サーバの IP アドレス。 • *port*：認証サーバの UDP ポート。 • **key** *secret*：認証サーバの RADIUS 共有秘密。 • **a-id** *a-id*：認証サーバに関連付けられた A-ID。