アイデンティティ、接続および SGT の設定

アイデンティティと接続の設定

このモジュールでは、次の機能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
- Cisco TrustSec 非シード デバイスのクレデンシャル、AAA 設定
- アップリンクポートでの 802.1X モードの Cisco TrustSec 認証と Macsec
- アップリンクポートでの手動モードの Cisco TrustSec と MACsec
- インターフェイスの SAP キーの再生成

アイデンティティと接続の設定方法

このセクションでは、アイデンティティと接続の設定方法を説明します。

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。

（注）

- Cisco Identity Services Engine（Cisco ISE）または Cisco Secure Access Control Server（Cisco ACS）にも、デバイスの Cisco TrustSec クレデンシャルを設定する必要があります。
- **cts authorization list** コマンドは、Cisco Identity Services Engine（ISE）から Cisco TrustSec 環境データと SGACL ポリシーをダウンロードするように設定する必要があります。

Cisco TrustSec ドメインを開始できるように、シードデバイスで NDAC および AAA を有効にするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**cts credentials id** *device-id* **password** *password* 例： `Device# cts credentials id device1 password Cisco123`	EAP-FAST を使用して他の Cisco TrustSec デバイスで認証するときにこのデバイスが使用する Cisco TrustSec デバイス ID およびパスワードを指定します。*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	**enable** 例： `Device# enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 3	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 4	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 5	**aaa authentication dot1x default group radius** 例： `Device(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 6	**aaa authorization network** *mlist* **group radius** 例： `Device(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デバイスを設定します。 • *mlist*：Cisco TrustSec AAA サーバ グループ。

	コマンドまたはアクション	目的
ステップ 7	**cts authorization list** *mlist* 例： `Device(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 8	**aaa accounting dot1x default start-stop group radius** 例： `Device(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 9	**radius-server host** *ip-addr* **auth-port 1812 acct-port 1813 pac key** *secret* 例： `Device(config)# radius-server host 10.20.3.1 auth-port 1812 acct-port 1813 pac key AbCe1234`	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 10	**radius-server vsa send authentication** 例： `Device(config)# radius-server vsa send authentication`	認証段階でデバイス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デバイスを設定します。
ステップ 11	**dot1x system-auth-control** 例： `Device(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 12	**exit** 例： `Device(config)# exit`	設定モードを終了します。

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

（注） Cisco Identity Services Engine または Cisco Secure ACS にも、デバイスの Cisco TrustSec クレデンシャルを設定する必要があります。

Cisco TrustSec ドメインに参加できるように、非シードデバイスで 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。

手順

	コマンドまたはアクション	目的
ステップ 1	**cts credentials id** *device-id* **password** *password* 例： `Device# 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デバイスが使用する Cisco TrustSec デバイス ID およびパスワードを指定します。*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	**enable** 例： `Device# enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 3	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 4	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 5	**aaa authentication dot1x default group radius** 例： `Device(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 6	**aaa authorization network** *mlist* **group radius** 例： `Device(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デバイスを設定します。 • *mlist*：Cisco TrustSec の AAA サーバグループを指定します。
ステップ 7	**aaa accounting dot1x default start-stop group radius** 例： `Device(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	**radius-server vsa send authentication** 例： `Device(config)# radius-server vsa send authentication`	認証段階でデバイス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デバイスを設定します。

	コマンドまたはアクション	目的
ステップ 9	**dot1x system-auth-control** 例： `Device(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 10	**exit** 例： `Device(config)# exit`	設定モードを終了します。

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。

手順

	コマンドまたはアクション	目的
ステップ 1	**cts rekey interface** *type slot/port* 例： `Device# cts rekey int gig 1/1`	MACsec リンクで SAP キーの再ネゴシエーションを強制します。

追加認証サーバ関連のパラメータの設定

デバイスと 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。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**cts server deadtime** *seconds* 例： `Device(config)# cts server deadtime 20`	（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

	コマンドまたはアクション	目的
		です。指定できる範囲は 1 ～ 864000 です。
ステップ 4	**cts server load-balance method least-outstanding** [**batch-size** *transactions*] [**ignore-preferred-server**] 例： `Device(config)# cts server load-balance method least-outstanding batch-size 50 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デバイスに指示します。
ステップ 5	**cts server test** {*server-IP-address* | **all**} { **deadtime** *seconds* | **enable** | **idle-time** *seconds* } 例： `Device(config)# cts server test 10.15.20.102 idle-time 120`	（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 6	**exit** 例： `Device(config)# exit`	設定モードを終了します。
ステップ 7	**show cts server-list** 例： `Device# 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。

例：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。

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。

```
Device# configure terminal
Device(config)# cts server load-balance method least-outstanding batch-size 50
ignore-preferred-server
Device(config)# cts server test all deadtime 20
Device(config)# cts server test all enable
Device(config)# exit
Device#show cts server-list
CTS Server Radius Load Balance = ENABLED
    Method    = least-outstandin
```

```
    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 sec
```

Cisco TrustSec インターフェイス設定の確認

Cisco TrustSec 関連のインターフェイスの設定を表示するには、次のコマンドを使用します。 **show cts interface**

```
Device# show cts interface gigabitethernet 1/1/1

Global Dot1x feature is Disabled
Interface GigabitEthernet1/1/1:
    CTS is enabled, mode:    MANUAL
    IFC state:               OPEN
    Interface Active for 00:54:01.936
    Authentication Status:   NOT APPLICABLE
        Peer identity:       "unknown"
        Peer's advertised capabilities: "sap"
    Authorization Status:    SUCCEEDED
        Peer SGT:            18
        Peer SGT assignment: Trusted
    SAP Status:              SUCCEEDED
        Version:             2
        Configured pairwise ciphers:
            gcm-encrypt

        Replay protection:      enabled
        Replay protection mode: STRICT

        Selected cipher:        gcm-encrypt

    Propagate SGT:           Enabled
    Cache Info:
        Expiration            : N/A
        Cache applied to link : NONE

    Statistics:
```

```
        authc success:              0
        authc reject:               0
        authc failure:              0
        authc no response:          0
        authc logoff:               0
        sap success:                3
        sap fail:                   0
        authz success:              4
        authz fail:                 0
        port auth fail:             0

    L3 IPM:   disabled.
```

アイデンティティ、接続、および SGT の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

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

リリース	機能	機能情報
Cisco IOS XE Fuji 16.9.2	アイデンティティ、接続および SGT	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 Cisco 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 Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。