MACsec の暗号化設定

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、https://cfnng.cisco.com/に進みます。Cisco.com のアカウントは必要ありません。

MACsec 暗号化について

この章では、Catalyst スイッチで Media Access Control Security（MACsec）暗号化を設定する方法について説明します。MACsec は 2 台の MACsec 対応デバイス間のパケットの認証と暗号化の IEEE 802.1AE 規格です。また、スイッチは、Cisco 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）および Security Association Protocol（SAP）キー交換を使用して MACsec リンク層スイッチ間セキュリティをサポートします。リンク層セキュリティはスイッチ間のパケット認証とスイッチ間の MACsec 暗号化の両方を含みます（暗号化は任意です）。

（注） MACsec は NPE または LAN ベース イメージを実行しているスイッチではサポートされません。

Cisco TrustSec MACsec リンク層スイッチ間セキュリティは、スイッチ上のすべてのダウンリンク ポートで実行できます。

表 *1:* スイッチ ポートの *MACsec* サポート

インターフェイス（Interface）	接続	MACsec のサポート
他のスイッチに接続されたスイッチポート	スイッチからスイッチへ	Cisco TrustSec NDAC MACsec

Cisco TrustSec と Cisco SAP はスイッチ間のリンクにのみ使用され、PC や IP フォンなどのエンドホストに接続されたスイッチ ポートではサポートされません。Cisco NDAC および SAP は、コンパクトなスイッチがワイヤリング クローゼットの外側にセキュリティを拡張するために使用する、ネットワーク エッジ アクセス トポロジ（NEAT）と相互排他的です。

Media Access Control Security と MACsec Key Agreement

802.1AE で定義された MACsec では、暗号化キー入力のためにアウトオブバンド方式を使用することによって、有線ネットワーク上で MAC レイヤの暗号化を実現します。MACsec Key Agreement（MKA）プロトコルでは、必要なセッション キーを提供し、必要な暗号化キーを管理します。MKA と MACsec は、802.1x 拡張認証プロトコル（EAP-TLS）または事前共有キー（PSK）フレームワークを使用した認証に成功した後に実装されます。

MACsec を使用するスイッチでは、MKA ピアに関連付けられたポリシーに応じて、MACsec フレームまたは非 MACsec フレームを許可します。MACsec フレームは暗号化され、整合性チェック値（ICV）で保護されます。スイッチは MKA ピアからフレームを受信すると、MKA によって提供されたセッション キーを使用してこれらのフレームを暗号化し、正しい ICV を計算します。スイッチはこの ICV をフレーム内の ICV と比較します。一致しない場合は、フレームが破棄されます。また、スイッチは現在のセッション キーを使用して、ICV を暗号化し、セキュアなポート（セキュアな MAC サービスを MKA ピアに提供するために使用されるアクセス ポイント）を介して送信されたフレームに追加します。

MKA プロトコルは、基礎となる MACsec プロトコルで使用される暗号キーを管理します。MKA の基本的な要件は 802.1x-REV で定義されています。MKA プロトコルでは 802.1x を拡張し、相互認証の確認によってピアを検出し、MACsec 秘密キーを共有してピアで交換されるデータを保護できます。

EAP フレームワークでは、新しく定義された EAP-over-LAN（EAPOL）パケットとして MKA を実装します。EAP 認証では、データ交換で両方のパートナーで共有されるマスター セッション キー（MSK）を生成します。EAP セッション ID を入力すると、セキュアな接続アソシエーション キー名（CKN）が生成されます。スイッチは、アップリンクおよびダウンリンクの両

方のオーセンティケータとして機能します。また、ダウンリンクのキー サーバーとして機能します。これによってランダムなセキュア アソシエーション キー（SAK）が生成され、クライアント パートナーに送信されます。クライアントはキー サーバーではなく、単一の MKA エンティティであるキー サーバーとだけ対話できます。キーの派生と生成の後で、スイッチは定期的にトランスポートをパートナーに送信します。デフォルトの間隔は 2 秒間です。

EAPOL プロトコル データ ユニット（PDU）のパケット本体は、MACsec Key Agreement PDU（MKPDU）と呼ばれます。MKA セッションと参加者は、MKA ライフタイム（6 秒間）が経過しても参加者から MKPDU を受信していない場合に削除されます。たとえば、MKA ピアが接続を解除した場合、スイッチ上の参加者は MKA ピアから最後の MKPDU を受信した後、6 秒間が経過するまで MKA の動作を継続します。

（注） MKPDU の整合性チェック値（ICV）インジケータはオプションです。トラフィックが暗号化されている場合、ICV はオプションではありません。

EAPoL 通知は、キー関連情報のタイプの使用を示します。通知は、サプリカントとオーセンティケータの機能を通知するために使用できます。各側の機能に基づいて、キー関連情報の最大公分母を使用できます。

Cisco IOS XE Fuji 16.8.1a よりも前のリリースでは、MKA と SAP で should-secure がサポートされていました。should-secure を有効にすると、ピアが MACsec に設定されている場合はデータトラフィックが暗号化され、それ以外の場合はクリアテキストで送信されます。Cisco IOS XE Fuji 16.8.1a 以降、入力と出力の両方で must-secure のサポートが有効になります。MKA および SAP では、Must-secure がサポートされています。must-secure を有効にすると、EAPoL トラフィックのみが暗号化されません。他のトラフィックは暗号化されます。暗号化されないパケットはドロップされます。

（注） デフォルトでは、Must-secure モードが有効になっています。

MKA ポリシー

インターフェイスで MKA を有効にするには、定義された MKA ポリシーをインターフェイスに適用する必要があります。MKA ポリシーを削除すると、そのインターフェイス上で MKA がディセーブルになります。次のオプションを設定可能です。

- 16 ASCII 文字未満のポリシー名。
- 物理インターフェイスごとの 0 バイト、30 バイト、または 50 バイトの機密保持（暗号化）オフセット。
- 再送保護。許可される順序外のフレームの数によって定義される MACsec ウィンドウ サイズを設定できます。この値は MACsec でセキュリティ アソシエーションをインストールする際に使用されます。値 0 は、フレームが正しい順序で許可されることを意味します。

仮想ポート

仮想ポートは、1 つの物理ポート上の複数のセキュアな接続アソシエーションに使用します。各接続アソシエーション（ペア）は仮想ポートを表します。1つの物理ポートにつき、仮想ポートは最大 2 つです。2 つの仮想ポートのうち、1 つだけをデータ VLAN の一部とすることができます。もう1つは、音声VLANに対してパケットを外部的にタグ付けする必要があります。同じポートで同じ VLAN 内のセキュアなセッションとセキュアでないセッションを同時にホストすることはできません。この制限のため、802.1x マルチ認証モードはサポートされません。

この制限の例外は、マルチホスト モードで最初の MACsec サプリカントが正常に認証され、スイッチに接続されたハブに接続される場合です。ハブに接続された非MACsecホストでは、マルチホストモードであるため、認証なしでトラフィックを送信できます。最初にクライアントが成功した後、他のクライアントでは認証が必要ないため、マルチホストモードの使用は推奨しません。

仮想ポートは、接続アソシエーションの任意のIDを表し、MKAプロトコル外では意味を持ちません。仮想ポートは個々の論理ポート ID に対応します。仮想ポートの有効なポート ID は 0x0002 ～ 0xFFFF です。各仮想ポートは、16 ビットのポート ID に連結された物理インターフェイスの MAC アドレスに基づいて、一意のセキュア チャネル ID（SCI）を受け取ります。

MACsec およびスタッキング

MACsec を実行している（Catalyst 3560cx）スイッチ スタックマスターは、MACsec をサポートしているメンバースイッチ上のポートを示すコンフィギュレーション ファイルを維持します。スタック マスターは、次に示す機能を実行します。

- セキュアなチャネルとセキュアなアソシエーションの作成および削除を処理します。
- スタック メンバーにセキュアなアソシエーション サービス要求を送信します。
- ローカル ポートまたはリモート ポートからのパケット番号とリプレイ ウィンドウ情報を処理し、キー管理プロトコルを通知します。
- オプションがグローバルに設定されたMACsec初期化要求を、スタックに追加される新しいスイッチに送信します。
- ポート単位の設定をメンバー スイッチに送信します。

メンバー スイッチは、次の機能を実行します。

- スタック マスターからの MACsec 初期化要求を処理します。
- スタック マスターから送信された MACsec サービス要求を処理します。
- スタック マスターにローカル ポートに関する情報を送信します。

スタックマスターの切り替えの場合、すべてのセキュアなセッションがダウンし、再確立されます。認証マネージャはセキュアなセッションを認識し、これらのセッションのティアダウンを開始します。

（注） スイッチ間接続に 1G SFP モジュールを使用している場合、MACsec のオーバーヘッドを確実にするため、システム MTU を 1550 バイトに変更します。

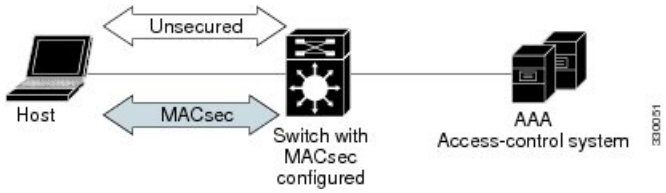
MACsec、MKA、および 802.1x ホスト モード

MACsec と MKA プロトコルは、802.1x シングルホスト モード、、またはマルチドメイン認証（MDA）モードで使用できます。マルチ認証モードはサポートされません。

シングルホスト モード

次の図に、MKA を使用して、MACsec で 1 つの EAP 認証済みセッションをセキュアにする方法を示します。

図 *1:* セキュアなデータ セッションでのシングルホスト モードの *MACsec*



MKA 統計情報

一部の MKA カウンタはグローバルに集約され、その他のカウンタはグローバルとセッション単位の両方で更新されます。また、MKA セッションのステータスに関する情報も取得できます。

次に、**show mka statistics** コマンドの出力例を示します。

```
SWitch# show mka statistics
MKA Global Statistics
=====================
MKA Session Totals
Secured..................... 32
Reauthentication Attempts.. 31

Deleted (Secured)..... 1
Keepalive Timeouts..... 0

CA Statistics
Pairwise CAKs Derived..... 32
Pairwise CAK Rekeys..... 31
Group CAKs Generated..... 0
Group CAKs Received..... 0

SA Statistics
SAKs Generated..... 32
SAKs Rekeyed..... 31
SAKs Received..... 0
SAK Responses Received..... 32


MKPDU Statistics
```

```
MKPDUs Validated & Rx...... 580
"Distributed SAK"..... 0
"Distributed CAK"..... 0
MKPDUs Transmitted......... 597
"Distributed SAK"..... 32
"Distributed CAK"..... 0

MKA Error Counter Totals
========================

Bring-up Failures.................. 0
Reauthentication Failures.......... 0

SAK Failures

SAK Generation.................. 0
Hash Key Generation............. 0
SAK Encryption/Wrap............. 0
SAK Decryption/Unwrap........... 0


CA Failures

Group CAK Generation............ 0
Group CAK Encryption/Wrap....... 0
Group CAK Decryption/Unwrap..... 0
Pairwise CAK Derivation......... 0
CKN Derivation.................. 0
ICK Derivation.................. 0
KEK Derivation.................. 0
Invalid Peer MACsec Capability.. 2

MACsec Failures

Rx SC Creation.................. 0
Tx SC Creation.................. 0
Rx SA Installation.............. 0
Tx SA Installation.............. 0

MKPDU Failures

MKPDU Tx........................ 0
MKPDU Rx Validation............. 0
MKPDU Rx Bad Peer MN............ 0
MKPDU Rx Non-recent Peerlist MN.. 0
```

EAP-TLS を使用した MACsec MKA に関する情報

MACsec MKA はスイッチ間リンクでサポートされます。Extensible Authentication Protocol（EAP-TLS）による IEE 802.1X ポートベース認証を使用して、デバイスのアップリンク ポート間で MACsec MKA を設定できます。EAP-TLS は相互認証を許可し、MSK（マスター セッション キー）を取得します。そのキーから、MKA 操作用の接続アソシエーション キー（CAK）が取得されます。デバイスの証明書は、AAA サーバーへの認証用に、EAP-TLS を使用して伝送されます。

EAP-TLS を使用した MACsec MKA の前提条件

- 認証局（CA）サーバーがネットワークに設定されていることを確認します。
- CA 証明書を生成します。
- Cisco Identity Services Engine（ISE）リリース 2.0 が設定されていることを確認します。

- 両方の参加デバイス（CA サーバーと Cisco Identity Services Engine（ISE））が Network Time Protocol（NTP）を使用して同期されていることを確認します。時間がすべてのデバイスで同期されていないと、証明書は検証されません。
- 802.1x 認証と AAA がデバイスに設定されていることを確認します。

EAP-TLS を使用した MACsec MKA の制限事項

- MKA は、ポート チャネルではサポートされていません。
- Cisco Catalyst 3560-CX スイッチは、EtherChannel での MACSec MKA 設定をサポートしていません。
- MKA は、高可用性とローカル認証ではサポートされていません。
- MKA と EAPTLS は、無差別 PVLAN プライマリポートではサポートされません。
- EAP-TLS を使用して MACsec MKA を設定している間、MACsec セキュアチャネル暗号化カウンタは最初のキー再生成の前に増加しません。

Cisco TrustSec の概要

次の表に、TrustSec がイネーブルになった Cisco スイッチで実装される TrustSec 機能を示します。継続的な TrustSec の General Availability リリースによって、サポートされるスイッチの数および各スイッチでサポートされる TrustSec 機能の数は増加しています。

Cisco TrustSec の機能	説明
802.1AE タギング（MACSec）	IEEE 802.1AE に基づくワイヤレート ホップ単位レイヤ 2 暗号化のプロトコル。 MACSec 対応デバイス間において、パケットは送信デバイスからの出力で暗号化され、受信デバイスへの入力で復号化されます。デバイス内では平文です。 この機能は、TrustSec ハードウェア対応デバイス間だけで利用できます。
エンドポイントアドミッション コントロール（EAC）	EAC は、TrustSec ドメインに接続しているエンドポイント ユーザーまたはデバイスの認証プロセスです。通常、EAC はアクセス レベル スイッチで実行されます。EAC プロセスの認証および許可に成功すると、ユーザーまたはデバイスに対してセキュリティ グループ タグが割り当てられます。現在、EAC は 802.1X、MAC 認証バイパス（MAB）、および Web 認証プロキシ（WebAuth）とすることができます。

Cisco TrustSec の機能	説明
ネットワーク デバイス アドミッション コントロール（NDAC）	NDAC は、TrustSec ドメイン内の各ネットワーク デバイスがピア デバイスのクレデンシャルおよび信頼性を確認できる認証プロセスです。NDAC は、IEEE 802.1X ポート ベースの認証に基づく認証フレームワークを利用し、EAP 方式として EAP-FAST を使用します。NDAC プロセスの認証および許可に成功すると、IEEE 802.1AE 暗号化のセキュリティ アソシエーション プロトコル ネゴシエーションとなります。
セキュリティ アソシエーション プロトコル（SAP）	NDAC 認証のあと、セキュリティ アソシエーション プロトコル（SAP）は、その後の TrustSec ピア間の MACSec リンク暗号化のキーおよび暗号スイートについて、自動的にネゴシエーションを行います。SAP は IEEE 802.11i で定義されます。
セキュリティ グループ タグ（SGT）	SGT は、TrustSec ドメイン内の送信元のセキュリティ分類を示す 16 ビットの単一ラベルです。イーサネット フレームまたは IP パケットに追加されます。
SGT 交換プロトコル（SXP）	Security Group Tag Exchange Protocol（SXP）。SXP を使用すると、TrustSec にハードウェアで対応していないデバイスが Cisco Identity Services Engine（ISE）または Cisco Secure アクセス コントロール システム（ACS）から認証されたユーザーとデバイスの SGT 属性を受信できます。デバイスは、次にセキュリティ グループ アクセス コントロール リスト（SGACL）強制のために、送信元トラフィックをタグ付けする TrustSec にハードウェアで対応しているデバイスに、sourceIP-to-SGT バインディングを転送できます。

リンクの両端で 802.1AE MACsec をサポートしている場合、SAP ネゴシエーションが実行されます。サプリカントとオーセンティケータの間で EAPOL-Key が交換され、暗号スイートのネゴシエーション、セキュリティ パラメータの交換、およびキーの管理が実行されます。これらの作業が正常に完了すると、セキュリティ アソシエーション（SA）が確立します。

ソフトウェア バージョンとライセンスおよびリンク ハードウェア サポートに応じて、SAP ネゴシエーションは次の動作モードの 1 つを使用できます。

- Galois Counter Mode（GCM）：認証と暗号化
- GCM authentication（GMAC）：GCM 認証、暗号化なし

- No Encapsulation：カプセル化なし（クリア テキスト）
- null：カプセル化、認証または暗号化なし

MKA および MACsec の設定

MACsec MKA のデフォルト設定

MACsec はディセーブルです。MKA ポリシーは設定されていません。

MKA ポリシーの設定

手順の概要

1. **configure terminal**
2. **mka policy** *policy name*
3. **confidentiality-offset** オフセット値
4. **replay-protection window-size** *frames*
5. **end**
6. **show mka policy**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**mka policy** *policy name*	MKA ポリシーを指定し、MKA ポリシー コンフィギュレーション モードを開始します。ポリシー名の長さは最大で 16 文字です。
ステップ 3	**confidentiality-offset** オフセット値	各物理インターフェイスに機密性（暗号化）オフセットを設定します。 （注） オフセット値は、0、30、または 50 を指定できます。クライアントで Anyconnect を使用している場合は、オフセット 0 を使用することをお勧めします。
ステップ 4	**replay-protection window-size** *frames*	再送保護をイネーブルにして、ウィンドウ サイズをフレームの数で設定します。範囲は 0 ～ 4294967295 です。デフォルトのウィンドウ サイズは 0 です。

	コマンドまたはアクション	目的
		ウィンドウサイズに 0 を入力することと、 **no replay-protection command** を入力することとは異なります。ウィンドウサイズを 0 に設定すると、厳密なフレーム順序でリプレイ保護が使用されます。**no replay-protection** を入力すると、MACsec 再送保護が無効になります。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show mka policy**	入力内容を確認します。

例

次に、MKA ポリシー *relay-policy* を設定する例を示します。

```
Switch(config)# mka policy replay-policy
Switch(config-mka-policy)# confidentiality-offset 0
Switch(config-mka-policy)# replay-protection window-size 300
Switch(config-mka-policy)# end
```

インターフェイスでの MACsec の設定

音声用に 1 つの MACsec セッションとデータ用に 1 つの MACsec セッションが存在するインターフェイスで MACsec を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface***interface-id*
4. **switchport access vlan***vlan-id*
5. **switchport mode access**
6. **macsec**
7. **authentication event linksec fail action authorize vlan** *vlan-id*
8. **authentication host-mode multi-domain**
9. **authentication linksec policy must-secure**
10. **authentication port-control auto**
11. **authentication periodic**
12. **authentication timer reauthenticate**
13. **authentication violation protect**
14. **mka policy** *policy name*
15. **dot1x pae authenticator**
16. **spanning-tree portfast**
17. **end**

18. **show authentication session interface** *interface-id*
19. **show authentication session interface** *interface-id* details
20. **show macsec interface** *interface-id*
21. **show mka sessions**
22. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： スイッチ> **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： スイッチ# **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	**interface***interface-id*	MACsecインターフェイスを指定し、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。インターフェイスは物理インターフェイスでなければなりません。
ステップ 4	**switchport access vlan***vlan-id*	このポートのアクセス VLAN を設定します。
ステップ 5	**switchport mode access**	インターフェイスをアクセス ポートとして設定します。
ステップ 6	**macsec**	インターフェイスで 802.1ae MACsec をイネーブルにします。
ステップ 7	**authentication event linksec fail action authorize vlan** *vlan-id*	（任意）認証の試行に失敗した後で、ポート上の制限付き VLAN を許可することによって、ユーザー証明書が認識されない認証リンク セキュリティの問題をスイッチが処理することを指定します。
ステップ 8	**authentication host-mode multi-domain**	ホストと音声デバイスの両方が、802.1x で許可されたポート上で認証されるように、ポート上の認証マネージャ モードを設定します。設定されていない場合、デフォルトのホストモードはシングルです。
ステップ 9	**authentication linksec policy must-secure**	LinkSecセキュリティ ポリシーを設定して、ピアを利用できる場合に、MACsec でセッションをセキュアにします。設定されていない場合、デフォルト値は *should secure* です。

	コマンドまたはアクション	目的
ステップ 10	**authentication port-control auto**	ポート上で 802.1x 認証をイネーブルにします。スイッチとクライアント間の認証交換に基づいてポートが許可ステートまたは無許可ステートに変わります。
ステップ 11	**authentication periodic**	このポートの再認証を有効または無効にします。
ステップ 12	**authentication timer reauthenticate**	1 ～ 65535 の値を入力します。サーバから再認証タイムアウト値を取得します。
ステップ 13	**authentication violation protect**	新しいデバイスがポートに接続された場合、または最大数のデバイスがポートに接続されたあとに新しいデバイスがそのポートに接続された場合に、予期しない着信 MAC アドレスを破棄するようポートを設定します。設定されていない場合、デフォルトではポートをシャット ダウンします。
ステップ 14	**mka policy** *policy name*	既存の MKA プロトコル ポリシーをインターフェイスに適用し、インターフェイス上で MKA をイネーブルにします。（**mka policy** グローバル コンフィギュレーション コマンドを入力して）MKA ポリシーが設定されていない場合、**mka default-policy** インターフェイス コンフィギュレーション コマンドを入力して、MKA のデフォルトのポリシーをインターフェイスに適用する必要があります。
ステップ 15	**dot1x pae authenticator**	ポートを 802.1x ポート アクセス エンティティ（PAE）オーセンティケータとして設定します。
ステップ 16	**spanning-tree portfast**	関連するすべての VLAN 内の特定のインターフェイスで、スパニングツリー Port Fast をイネーブルにします。Port Fast 機能がイネーブルの場合、インターフェイスはブロッキング ステートからフォワーディング ステートに直接移行します。その際に、中間のスパニングツリー ステートは変わりません。
ステップ 17	**end** 例： `スイッチ(config)# end`	特権 EXEC モードに戻ります。
ステップ 18	**show authentication session interface** *interface-id*	許可されたセッションのセキュリティ ステータスを確認します。
ステップ 19	**show authentication session interface** *interface-id* details	承認されたセッションのセキュリティ ステータスの詳細を確認します。

	コマンドまたはアクション	目的
ステップ 20	**show macsec interface** *interface-id*	インターフェイスの MacSec ステータスを確認します。
ステップ 21	**show mka sessions**	確立された mka セッションを確認します。
ステップ 22	**copy running-config startup-config** 例： スイッチ# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

PSK を使用した MACsec MKA の設定

手順の概要

1. **configure terminal**
2. **key chain** *key-chain-name* **macsec**
3. **key** *hex-string*
4. **key-string** *{ [0|6|7] pwd-string | pwd-string}*
5. **lifetime local** [*start timestamp {hh::mm::ss | day | month | year}*] [**duration** *seconds* | *end timestamp {hh::mm::ss | day | month | year}*]
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**key chain** *key-chain-name* **macsec**	キー チェーンを設定して、キー チェーン 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	**key** *hex-string*	キーチェーン内の各キーの固有識別子を設定し、キーチェーンのキー コンフィギュレーション モードを開始します。 （注） 128 ビット暗号の場合は、32 文字の 16 進数キー文字列を使用します。
ステップ 4	**key-string** *{ [0|6|7] pwd-string	pwd-string}*	キー文字列のパスワードを設定します。16進数の文字のみを入力する必要があります。

	コマンドまたはアクション	目的
ステップ 5	**lifetime local** [*start timestamp {hh::mm::ss	day	month	year}*] [**duration** *seconds*	*end timestamp {hh::mm::ss	day	month	year}*]	事前共有キーの有効期間を設定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。

例

次に例を示します。

```
Switch(config)# Key chain keychain1 macsec
Switch(config-key-chain)# key 1000
Switch(config-keychain-key)# cryptographic-algorithm gcm-aes-128
Switch(config-keychain-key)# key-string 12345678901234567890123456789012
Switch(config-keychain-key)# lifetime local 12:12:00 July 28 2016 12:19:00
July 28 2016
Switch(config-keychain-key)# end
```

PSK を使用した、インターフェイスでの MACsec MKA の設定

手順の概要

1. **configure terminal**
2. **interface** *interface-id*
3. **macsec network-link**
4. **mka policy** *policy-name*
5. **mka pre-shared-key key-chain** *key-chain name*
6. **macsec replay-protection window-size** *frame number*
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**interface** *interface-id*	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	**macsec network-link**	インターフェイス上で MACsec をイネーブルにします。
ステップ 4	**mka policy** *policy-name*	MKA ポリシーを設定します。
ステップ 5	**mka pre-shared-key key-chain** *key-chain name*	MKA 事前共有キーのキーチェーン名を設定します。

	コマンドまたはアクション	目的
		（注） MKA 事前共有キーは、物理インターフェイスまたはサブインターフェイスで設定できますが、両方で設定することはできません。
ステップ 6	**macsec replay-protection window-size** *frame number*	リプレイ保護の MACsec ウィンドウ サイズを設定します。
ステップ 7	**end**	特権 EXEC モードに戻ります。

例

次に例を示します。

```
Switch(config)# interface GigabitEthernet 0/0/0
Switch(config-if)# mka policy mka_policy
Switch(config-if)# mka pre-shared-key key-chain key-chain-name
Switch(config-if)# macsec replay-protection window-size 10
Switch(config-if)# end
```

次のタスク

セッションの実行中に MKA PSK が設定されたインターフェイスで MKA ポリシーを変更することは推奨されません。ただし、変更が必要な場合は、次のようにポリシーを再設定する必要があります。

1. **no macsec network-link** コマンドを使用して、各参加ノードの macsec network-link 設定を削除し、既存のセッションを無効にします。
2. **mka policy policy-name** コマンドを使用して、各参加ノードのインターフェイスで MKA ポリシーを設定します。
3. **macsec network-link** コマンドを使用して、各参加ノードで新しいセッションを有効にします。

EAP-TLS を使用した MACsec MKA の設定

ポイントツーポイント リンクで MKA による MACsec を設定するには、次のタスクを実行します。

- 証明書登録の設定
  - キー ペアの生成
  - SCEP 登録の設定

- 証明書の手動設定

- 認証ポリシーの設定
- EAP-TLS プロファイルおよび IEEE 802.1x クレデンシャルの設定
- インターフェイスでの EAP-TLS を使用した MKA MACsec の設定

リモート認証

キー ペアの生成

手順

	コマンドまたはアクション	目的
ステップ 1	**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	**crypto key generate rsa label** *label-name* **general-keys modulus** *size*	署名および暗号化用に RSA キーペアを作成します。 label キーワードを使用すると、各キーペアにラベルを割り当てることもできます。このラベルは、キーペアを使用するトラストポイントによって参照されます。ラベルを割り当てなかった場合、キーペアには <Default-RSA-Key> というラベルが自動的に付けられます。 追加のキーワードを使用しない場合、このコマンドは汎用 RSA キー ペアを 1 つ生成します。係数が指定されていない場合は、デフォルトのキー係数である 1024 が使用されます。その他の係数サイズを指定するには、modulus キーワードを使用します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show authentication session interface** *interface-id*	許可されたセッションのセキュリティ ステータスを確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

SCEP による登録の設定

Simple Certificate Enrollment Protocol（SCEP）は、HTTP を使用して認証局（CA）または登録局（RA）と通信する、シスコが開発した登録プロトコルです。SCEP は、要求および証明書の送受信用に最も一般的に使用される方式です。

手順

	コマンドまたはアクション	目的
ステップ 1	**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	**crypto pki trustpoint** *server name*	トラストポイントおよび設定された名前を宣言して、CA トラストポイント 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	**enrollment url** *url name pem*	デバイスが証明書要求を送信する CA の URL を指定します。 URL 内の IPv6 アドレスは括弧で囲む必要があります。たとえば、http:// [2001:DB8:1:1::1]:80 です。 pem キーワードは、証明書要求に Privacy Enhanced Mail（PEM）の境界を追加します。
ステップ 4	**rsakeypair** *label*	証明書に関連付けるキー ペアを指定します。 （注） **rsakeypair** 名は、信頼ポイント名と一致している必要があります。
ステップ 5	**serial-number none**	**none** キーワードは、証明書要求にシリアル番号が含まれないことを指定します。
ステップ 6	**ip-address none**	**none** キーワードは、証明書要求に IP アドレスが含まれないことを指定します。
ステップ 7	**revocation-check crl**	ピアの証明書が取り消されていないことを確認する方法として CRL を指定します。
ステップ 8	**auto-enroll** *percent* **regenerate**	自動登録をイネーブルにします。これにより、クライアントはCAから自動的にロールオーバー証明書を要求できます。 自動登録がイネーブルでない場合、証明書の失効時にクライアントを手動で PKI に再登録する必要があります。 デフォルトでは、デバイスのドメイン ネーム システム（DNS）名だけが証明書に含められます。 現行の証明書の有効期間が指定のパーセンテージに達したときに、新しい証明書が要求されるように指定するには、percent 引数を使用します。

	コマンドまたはアクション	目的
		名前付きのキーがすでに存在する場合でも、証明書の新しいキーを生成するには、regenerate キーワードを使用します。 ロールオーバー中のキー ペアがエクスポート可能な場合、新しいキーペアもエクスポート可能です。次のコメントがトラストポイントコンフィギュレーションに表示され、キー ペアがエクスポート可能かどうかが示されます。「! RSA key pair associated with trustpoint is exportable.」 新しいキー ペアは、セキュリティ上の問題に対処するために生成することを推奨します。
ステップ 9	**crypto pki authenticate** *name*	CA 証明書を取得して、認証します。
ステップ 10	**exit**	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 11	**show crypto pki certificate** *trustpoint name*	信頼ポイントの証明書に関する情報を表示します。

登録の手動設定

CA が SCEP をサポートしない場合、またはルータと CA 間のネットワーク接続が不可能な場合。手動での証明書登録を設定するには、次の作業を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**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	**crypto pki trustpoint** *server name*	トラストポイントおよび設定された名前を宣言して、CA トラストポイント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	**enrollment url** *url name pem*	デバイスが証明書要求を送信する CA の URL を指定します。 URL 内の IPv6 アドレスは括弧で囲む必要があります。たとえば、http:// [2001:DB8:1:1::1]:80 です。 pem キーワードは、証明書要求に Privacy Enhanced Mail（PEM）の境界を追加します。
ステップ 4	**rsakeypair** *label*	証明書に関連付けるキー ペアを指定します。

	コマンドまたはアクション	目的
ステップ 5	**serial-number none**	**none** キーワードは、証明書要求にシリアル番号が含まれないことを指定します。
ステップ 6	**ip-address none**	**none** キーワードは、証明書要求に IP アドレスが含まれないことを指定します。
ステップ 7	**revocation-check crl**	ピアの証明書が取り消されていないことを確認する方法として CRL を指定します。
ステップ 8	**exit**	グローバル コンフィギュレーション モードから抜けます。
ステップ 9	**crypto pki authenticate** *name*	CA 証明書を取得して、認証します。
ステップ 10	**crypto pki enroll** *name*	証明書要求を生成し、証明書サーバーにコピーおよびペーストするために要求を表示します。 プロンプトが表示されたら、登録情報を入力します。たとえば、証明書要求にデバイスの FQDN および IP アドレスを含めるかどうかを指定します。 コンソール端末に対して証明書要求を表示するかについても選択できます。 必要に応じて、Base 64 符号化証明書を PEM ヘッダーを付けて、または付けずに表示します。
ステップ 11	**crypto pki import** *name* **certificate**	許可された証明書を取得するコンソール端末で、TFTP によって証明書をインポートします。 デバイスは、拡張子が「.req」から「.crt」に変更されたことを除いて、要求の送信に使用した同じファイル名を使用して、許可された証明書を TFTP によって取得しようと試みます。用途キー証明書の場合、拡張子「-sign.crt」および「-encr.crt」が使用されます。 デバイスは、受信したファイルを解析して証明書を検証し、証明書をスイッチの内部証明書データベースに挿入します。 （注） 一部の CA は、証明書要求の用途キー情報を無視し、汎用目的の証明書を発行します。ご使用の CA が証明書要求の用途キー情報を無視する場合は、汎用目的の証明書だけをインポートしてください。ルータは、生成される 2 つのキー ペアのいずれも使用しません。

	コマンドまたはアクション	目的
ステップ 12	**exit**	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 13	**show crypto pki certificate** *trustpoint name*	信頼ポイントの証明書に関する情報を表示します。
ステップ 14	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

802.1x 認証の有効化と AAA の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**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**	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	**aaa new-model**	AAA をイネーブルにします。
ステップ 4	**dot1x system-auth-control**	デバイス上で 802.1X を有効にします。
ステップ 5	**radius server** *name*	RADIUS サーバの設定の名前を Protected Access Credential（PAC）のプロビジョニング用に指定し、RADIUS サーバ設定モードを開始します。
ステップ 6	**address** *ip-address* **auth-port** *port-number* **acct-port** *port-number*	RADIUSサーバーのアカウンティングおよび認証パラメータの IPv4 アドレスを設定します。
ステップ 7	**automate-tester username** *username*	RADIUS サーバーの自動テスト機能を有効にします。 このようにすると、デバイスは RADIUS サーバーにテスト認証メッセージを定期的に送信し、サーバーからの RADIUS 応答を待機します。成功メッセージは必須ではありません。認証失敗であっても、サーバーが稼働していることを示しているため問題ありません。
ステップ 8	**key** *string*	デバイスと RADIUS サーバーとの間におけるすべての RADIUS 通信用の認証および暗号キーを指定します。

	コマンドまたはアクション	目的
ステップ 9	**radius-server deadtime** *minutes*	いくつかのサーバーが使用不能になったときの RADIUS サーバーの応答時間を短くし、使用不能になったサーバーがすぐにスキップされるようにします。
ステップ 10	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 11	**aaa group server radius** *group-name*	異なる RADIUS サーバー ホストを別々のリストと方式にグループ化し、サーバー グループ コンフィギュレーション モードを開始します。
ステップ 12	**server** *name*	RADIUS サーバー名を割り当てます。
ステップ 13	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 14	**aaa authentication dot1x default group** *group-name*	IEEE 802.1x 用にデフォルトの認証サーバー グループを設定します。
ステップ 15	**aaa authorization network default group** *group-name*	ネットワーク認証のデフォルト グループを設定します。

EAP-TLS プロファイルと 802.1x クレデンシャルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**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**	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	**eap profile** *profile-name*	EAP プロファイルを設定し、EAP プロファイル 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	**method tls**	デバイスで EAP-TLS 方式を有効にします。
ステップ 5	**pki-trustpoint** *name*	デフォルトの PKI トラストポイントを設定します。
ステップ 6	**exit**	グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 7	**dot1x credentials** *profile-name*	802.1x クレデンシャルプロファイルを設定し、dot1x クレデンシャル コンフィギュレーション モードを開始します。
ステップ 8	**username** *username*	認証ユーザー ID を設定します。
ステップ 9	**pki-trustpoint** *name*	デフォルトの PKI トラストポイントを設定します。
ステップ 10	**end**	特権 EXEC モードに戻ります。

インターフェイスでの 802.1x MACsec MKA 設定の適用

EAP-TLS を使用して MACsec MKA をインターフェイスに適用するには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**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	**interface** *interface-id*	MACsec インターフェイスを指定し、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。インターフェイスは物理インターフェイスでなければなりません。
ステップ 3	**macsec network-link**	インターフェイス上で MACsec をイネーブルにします。
ステップ 4	**authentication periodic**	このポートの再認証をイネーブルにします。
ステップ 5	**authentication timer reauthenticate interval**	再認証間隔を設定します。
ステップ 6	**access-session host-mode multi-domain**	ホストにインターフェイスへのアクセスを許可します。
ステップ 7	**access-session closed**	インターフェイスへの事前認証アクセスを防止します。
ステップ 8	**access-session port-control auto**	ポートの認可状態を設定します。
ステップ 9	**dot1x pae both**	ポートを 802.1X ポート アクセス エンティティ（PAE）のサプリカントおよびオーセンティケータとして設定します。
ステップ 10	**dot1x credentials profile**	802.1x クレデンシャルプロファイルをインターフェイスに割り当てます。

	コマンドまたはアクション	目的
ステップ 11	**dot1x supplicant eap profile** *name*	EAP-TLS プロファイルをインターフェイスに割り当てます。
ステップ 12	**service-policy type control subscriber** *control-policy name*	インターフェイスに加入者制御ポリシーを適用します。
ステップ 13	**exit**	特権 EXEC モードに戻ります。
ステップ 14	**show macsec interface**	インターフェイスの MACsec の詳細を表示します。
ステップ 15	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ローカル認証

ローカル認証を使用した EAP クレデンシャルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**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**	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	**aaa new-model**	AAA をイネーブルにします。
ステップ 4	**aaa local authentication default authorization default**	デフォルトのローカル認証およびデフォルトのローカル認証方法を設定します。
ステップ 5	**aaa authentication dot1x default local**	IEEE 802.1x 用にデフォルトのローカル ユーザー名認証リストを設定します。
ステップ 6	**aaa authorization network default local**	ローカル ユーザーの認可方式リストを設定します。
ステップ 7	**aaa authorization credential-download default local**	ローカル クレデンシャルの使用に関する認可方式リストを設定します。
ステップ 8	**exit**	特権 EXEC モードに戻ります。

ローカル EAP-TLS 認証と認証プロファイルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**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**	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	**aaa new-model**	AAA をイネーブルにします。
ステップ 4	**dot1x credentials** *profile-name*	dot1x クレデンシャル プロファイルを設定し、dot1x クレデンシャル 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	**username** *name* **password** *password*	認証のユーザー ID およびパスワードを設定します。
ステップ 6	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**aaa attribute list** *list-name*	（任意）AAA 属性リスト定義を設定し、属性リスト コンフィギュレーション モードを開始します。
ステップ 8	**aaa attribute type linksec-policy must-secure**	（任意）AAA 属性タイプを指定します。
ステップ 9	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**username** *name* **aaa attribute list** *name*	（任意）ユーザー ID に AAA 属性リストを指定します。
ステップ 11	**end**	特権 EXEC モードに戻ります。

SCEP による登録の設定

Simple Certificate Enrollment Protocol（SCEP）は、HTTP を使用して認証局（CA）または登録局（RA）と通信する、シスコが開発した登録プロトコルです。SCEP は、要求および証明書の送受信用に最も一般的に使用される方式です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable**	特権 EXEC モードを有効にします。

	コマンドまたはアクション	目的
		• 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**	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	**crypto pki trustpoint** *server name*	トラストポイントおよび設定された名前を宣言して、CA トラストポイント 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	**enrollment url** *url name pem*	デバイスが証明書要求を送信する CA の URL を指定します。 URL 内の IPv6 アドレスは括弧で囲む必要があります。たとえば、http:// [2001:DB8:1:1::1]:80 です。 pem キーワードは、証明書要求に Privacy Enhanced Mail（PEM）の境界を追加します。
ステップ 5	**rsakeypair** *label*	証明書に関連付けるキー ペアを指定します。 （注） **rsakeypair** 名は、信頼ポイント名と一致している必要があります。
ステップ 6	**serial-number none**	**none** キーワードは、証明書要求にシリアル番号が含まれないことを指定します。
ステップ 7	**ip-address none**	**none** キーワードは、証明書要求に IP アドレスが含まれないことを指定します。
ステップ 8	**revocation-check crl**	ピアの証明書が取り消されていないことを確認する方法として CRL を指定します。
ステップ 9	**auto-enroll** *percent* **regenerate**	自動登録をイネーブルにします。これにより、クライアントはCAから自動的にロールオーバー証明書を要求できます。 自動登録がイネーブルでない場合、証明書の失効時にクライアントを手動で PKI に再登録する必要があります。 デフォルトでは、デバイスのドメイン ネーム システム（DNS）名だけが証明書に含められます。 現行の証明書の有効期間が指定のパーセンテージに達したときに、新しい証明書が要求されるように指定するには、percent 引数を使用します。

	コマンドまたはアクション	目的
		名前付きのキーがすでに存在する場合でも、証明書の新しいキーを生成するには、regenerate キーワードを使用します。 ロールオーバー中のキー ペアがエクスポート可能な場合、新しいキーペアもエクスポート可能です。次のコメントがトラストポイントコンフィギュレーションに表示され、キー ペアがエクスポート可能かどうかが示されます。「! RSA key pair associated with trustpoint is exportable.」 新しいキー ペアは、セキュリティ上の問題に対処するために生成することを推奨します。
ステップ 10	**crypto pki authenticate** *name*	CA 証明書を取得して、認証します。
ステップ 11	**exit**	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 crypto pki certificate** *trustpoint name*	信頼ポイントの証明書に関する情報を表示します。

登録の手動設定

CA が SCEP をサポートしない場合、またはルータと CA 間のネットワーク接続が不可能な場合。手動での証明書登録を設定するには、次の作業を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**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**	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	**crypto pki trustpoint** *server name*	トラストポイントおよび設定された名前を宣言して、CA トラストポイント 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	**enrollment url** *url name pem*	デバイスが証明書要求を送信する CA の URL を指定します。 URL 内の IPv6 アドレスは括弧で囲む必要があります。たとえば、http:// [2001:DB8:1:1::1]:80 です。

	コマンドまたはアクション	目的
		pem キーワードは、証明書要求に Privacy Enhanced Mail（PEM）の境界を追加します。
ステップ 5	**rsakeypair** *label*	証明書に関連付けるキー ペアを指定します。
ステップ 6	**serial-number none**	**none** キーワードは、証明書要求にシリアル番号が含まれないことを指定します。
ステップ 7	**ip-address none**	**none** キーワードは、証明書要求に IP アドレスが含まれないことを指定します。
ステップ 8	**revocation-check crl**	ピアの証明書が取り消されていないことを確認する方法として CRL を指定します。
ステップ 9	**exit**	グローバル コンフィギュレーション モードから抜けます。
ステップ 10	**crypto pki authenticate** *name*	CA 証明書を取得して、認証します。
ステップ 11	**crypto pki enroll** *name*	証明書要求を生成し、証明書サーバーにコピーおよびペーストするために要求を表示します。 プロンプトが表示されたら、登録情報を入力します。たとえば、証明書要求にデバイスの FQDN および IP アドレスを含めるかどうかを指定します。 コンソール端末に対して証明書要求を表示するかについても選択できます。 必要に応じて、Base 64 符号化証明書を PEM ヘッダーを付けて、または付けずに表示します。
ステップ 12	**crypto pki import** *name* **certificate**	許可された証明書を取得するコンソール端末で、TFTP によって証明書をインポートします。 デバイスは、拡張子が「.req」から「.crt」に変更されたことを除いて、要求の送信に使用した同じファイル名を使用して、許可された証明書を TFTP によって取得しようと試みます。用途キー証明書の場合、拡張子「-sign.crt」および「-encr.crt」が使用されます。 デバイスは、受信したファイルを解析して証明書を検証し、証明書をスイッチの内部証明書データベースに挿入します。

	コマンドまたはアクション	目的
		（注） 一部の CA は、証明書要求の用途キー情報を無視し、汎用目的の証明書を発行します。ご使用の CA が証明書要求の用途キー情報を無視する場合は、汎用目的の証明書だけをインポートしてください。ルータは、生成される 2 つのキー ペアのいずれも使用しません。
ステップ 13	**exit**	グローバル コンフィギュレーション モードから抜けます。
ステップ 14	**show crypto pki certificate** *trustpoint name*	信頼ポイントの証明書に関する情報を表示します。
ステップ 15	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

EAP-TLS プロファイルと 802.1x クレデンシャルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**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**	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	**eap profile** *profile-name*	EAP プロファイルを設定し、EAP プロファイル 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	**method tls**	デバイスで EAP-TLS 方式を有効にします。
ステップ 5	**pki-trustpoint** *name*	デフォルトの PKI トラストポイントを設定します。
ステップ 6	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**dot1x credentials** *profile-name*	802.1x クレデンシャル プロファイルを設定し、dot1x クレデンシャル コンフィギュレーション モードを開始します。
ステップ 8	**username** *username*	認証ユーザー ID を設定します。
ステップ 9	**pki-trustpoint** *name*	デフォルトの PKI トラストポイントを設定します。

	コマンドまたはアクション	目的
ステップ 10	**end**	特権 EXEC モードに戻ります。

インターフェイスでの 802.1x MKA MACsec 設定の適用

EAP-TLS を使用して MKA MACsec をインターフェイスに適用するには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**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**	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	**interface** *interface-id*	MACsecインターフェイスを指定し、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。インターフェイスは物理インターフェイスでなければなりません。
ステップ 4	**macsec**	インターフェイス上で MACsec をイネーブルにします。
ステップ 5	**authentication periodic**	このポートの再認証をイネーブルにします。
ステップ 6	**authentication timer reauthenticate interval**	再認証間隔を設定します。
ステップ 7	**access-session host-mode multi-domain**	ホストにインターフェイスへのアクセスを許可します。
ステップ 8	**access-session closed**	インターフェイスへの事前認証アクセスを防止します。
ステップ 9	**access-session port-control auto**	ポートの認可状態を設定します。
ステップ 10	**dot1x pae both**	ポートを 802.1X ポート アクセス エンティティ（PAE）のサプリカントおよびオーセンティケータとして設定します。
ステップ 11	**dot1x credentials profile**	802.1x クレデンシャルプロファイルをインターフェイスに割り当てます。
ステップ 12	**dot1x authenticator eap profile** *name*	EAP-TLS オーセンティケータ プロファイルをインターフェイスに割り当てます。

	コマンドまたはアクション	目的
ステップ 13	**dot1x supplicant eap profile** *name*	EAP-TLSサプリカントプロファイルをインターフェイスに割り当てます。
ステップ 14	**service-policy type control subscriber** *control-policy name*	インターフェイスに加入者制御ポリシーを適用します。
ステップ 15	**exit**	特権 EXEC モードに戻ります。
ステップ 16	**show macsec interface**	インターフェイスのMACsecの詳細を表示します。
ステップ 17	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

EAP-TLS を使用した MACsec MKA の確認

EAP-TLS を使用して MACsec MKA の設定を確認するには、次のように **show** コマンドを使用します。以下に、**show** コマンドの出力例を示します。

show mka sessions コマンドは、アクティブな MACsec Key Agreement（MKA）プロトコルのセッションの概要を表示します。

```
Device# show mka sessions

  Total MKA Sessions....... 1
      Secured Sessions... 1
      Pending Sessions... 0

==============================================================================================
Interface      Local-TxSCI         Policy-Name      Inherited         Key-Server

Port-ID        Peer-RxSCI          MACsec-Peers     Status            CKN

==============================================================================================
Te0/1/3        74a2.e625.4413/0013 *DEFAULT POLICY* NO                YES

19             74a2.e625.4c22/0012 1                Secured
10000000000000000000000000000000000000000000000000000000000000000000
```

show macsec status interface *interface-id* は、指定されたインターフェイスの MACsec ステータス情報を表示します。

```
Device# show macsec status interface te0/1/2

  Capabilities:
  Ciphers Supported:        GCM-AES-128 GCM-AES-256
  Cipher:                   GCM-AES-128
  Confidentiality Offset:   0
  Replay Window:            64
  Delay Protect Enable:     FALSE
  Access Control:           must-secure
```

```
Transmit SC:
  SCI:                      74A2E6254C220012
  Transmitting:             TRUE
Transmit SA:
  Next PN:                  412
  Delay Protect AN/nextPN:  99/0

Receive SC:
  SCI:                      74A2E62544130013
  Receiving:                TRUE
Receive SA:
  Next PN:                  64
  AN:                       0
  Delay Protect AN/LPN:     0/0
```

show access-session interface *interface-id* **details** は、指定されたインターフェイスのアクセス セッションに関する詳細情報を表示します。

```
Device# show access-session interface te1/0/1 details
```

```
   Interface:  TenGigabitEthernet1/0/1
             IIF-ID:  0x17298FCD
         MAC Address:  f8a5.c592.13e4
        IPv6 Address:  Unknown
        IPv4 Address:  Unknown
           User-Name:  DOT1XCRED
              Status:  Authorized
              Domain:  DATA
      Oper host mode:  multi-host
    Oper control dir:  both
     Session timeout:  N/A
   Common Session ID:  000000000000000BB72E8AFA
     Acct Session ID:  Unknown
              Handle:  0xc3000001
      Current Policy:  MUSTS_1


Local Policies:
 Security Policy:  Must Secure
      Security Status:  Link Secured

Server Policies:


Method status list:
       Method           State
     dot1xSup           Authc Success
        dot1x           Authc Success
```

Cisco TrustSec MACsec の設定

スイッチの Cisco TrustSec クレデンシャルの設定

Cisco TrustSec 機能をイネーブルにするには、他の TrustSec 設定で使用するスイッチで Cisco TrustSec クレデンシャルを作成する必要があります。Cisco TrustSec クレデンシャルを設定するには、特権 EXEC モードで次の手順を行います。

手順の概要

1. **cts credentials id** *device-id* **password** *cts-password*
2. **show cts credentials**
3. **copy running-config startup-config**

手順の詳細

	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** *cts-password* 例： `Switch# cts credentials id trustsec password mypassword`	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 クレデンシャルを指定します。 • **id** *device-id*：スイッチの Cisco TrustSec デバイス ID 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。 • **password** *cts-password*：デバイスの Cisco TrustSec パスワードを指定します。
ステップ 2	**show cts credentials** 例： `Switch# show cts credentials`	（任意）スイッチで設定された Cisco TrustSec クレデンシャルを表示します。
ステップ 3	**copy running-config startup-config** 例： `スイッチ# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

例

Cisco TrustSec クレデンシャルを削除するには、**clear cts credentials** 特権 EXEC コマンドを入力します。

次に、Cisco TrustSec クレデンシャルを作成する例を示します。

```
Switch# cts credentials id trustsec password mypassword
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.

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

次のタスク

Cisco TrustSec MACsec 認証を設定する前に、Cisco TrustSec シードおよび非シード デバイスを設定する必要があります。802.1x モードでは、アクセス コントロール システム（ACS）に最も近い少なくとも 1 台のシード デバイスを設定する必要があります。『Cisco TrustSec Configuration Guide』の次のセクションを参照してください。
http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/ident-conn_config.html

802.1X モードでの Cisco TrustSec スイッチ間のリンク セキュリティの設定

始める前に

別の Cisco TrustSec デバイスに接続されているインターフェイス上で Cisco TrustSec リンク層スイッチ間セキュリティをイネーブルにします。インターフェイス上で 802.1X モードの Cisco TrustSec を設定する場合は、次の注意事項に従ってください。

- 802.1x モードを使用するには、各デバイスでグローバルに 802.1x をイネーブルにする必要があります。802.1x の詳細については、「IEEE 802.1x ポートベースの認証の設定」の章を参照してください。
- SAP 動作モードとして GCM を選択すると、シスコの MACsec 暗号化ソフトウェア ライセンスが必要です。MACsec は、Catalyst 3560cx の汎用 IP Base ライセンスと IP サービス ライセンスでサポートされます。これは NPE ライセンスまたは LAN ベース サービス イメージではサポートされません。

  必要なライセンスなしで GCM を選択した場合、インターフェイスはリンク ダウン状態になります。

特権 EXEC モードから 802.1x で Cisco TrustSec のスイッチ間のリンク層セキュリティを設定する手順は、次のとおりです。

手順の概要

1. **configure terminal**
2. **interface** *interface-id*
3. **cts dot1x**
4. **sap mode-list***mode1* [*mode2* [*mode3* [*mode4*]]]
5. **no propagate sgt**
6. **exit**
7. **end**

8. **show cts interface** [*interface-id* | **brief** | **summary**]
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# 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	**interface** *interface-id* 例： `Switch(config)# interface tengigabitethernet 1/1/2`	（注） 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	**cts dot1x** 例： `Switch(config-if)# cts dot1x`	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	**sap mode-list***mode1* [*mode2* [*mode3* [*mode4*]]] 例： `Switch(config-if-cts-dot1x)# sap mode-list gcm-encrypt null no-encap`	（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。優先する順序で許容されるモードを入力します。 *mode* の選択肢は次のとおりです。 • **gcm-encrypt**：認証および暗号化 （注） ソフトウェア ライセンスが MACsec 暗号化をサポートする場合、MACsec の認証と暗号化にこのモードを選択します。 • **gmac**：認証、暗号化なし • **no-encap**：カプセル化なし • **null**：カプセル化、認証または暗号化なし （注） インターフェイスでデータ 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。SGT はサポートされません。 （注） CLI ヘルプには表示されますが、timer reauthentication および propagate sgt キーワードはサポートされません。

	コマンドまたはアクション	目的
ステップ 5	**no propagate sgt** 例： `Switch(config-if-cts-dot1x)# no propagate sgt`	スイッチ（Catalyst 3560cx）は SGT のタギングをサポートしていません。このコマンドは、CTS リンクでの SGT タグの伝達を無効にします。トラフィックが CTS リンクを適切に流れるには、ピア スイッチでも「no propagate sgt」が設定されていることが必須です。
ステップ 6	**exit** 例： `Switch(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 7	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show cts interface** [*interface-id* | **brief** I**summary**]	（任意）TrustSec 関連のインターフェイス特性を表示して、設定を確認します。
ステップ 9	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

例

次に、優先 SAP モードとして GCM を使用して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例を示します。

```
Switch# configure terminal
Switch(config)# interface tengigabitethernet 1/1/2
Switch(config-if)# cts dot1x
Switch(config-if-cts-dot1x)# sap mode-list gcm-encrypt null no-encap
Switch(config-if-cts-dot1x)# no propagate sgt
Switch(config-if-cts-dot1x)# exit
Switch(config-if)# end
```

手動モードでの Cisco TrustSec スイッチ間リンク セキュリティの設定

始める前に

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。

- SAP 動作モードとして GCM を選択すると、シスコの MACsec 暗号化ソフトウェア ライセンスが必要です。必要なライセンスなしで GCM を選択した場合、インターフェイスはリンク ダウン状態になります。
- これらの保護レベルは、SAP の Pairwise Master Key（sap pmk）を設定する場合にサポートされます。
  - SAP が設定されていない：保護は行われません。
  - **sap mode-list gcm-encrypt gmac no-encap**：保護が望ましいが必須ではない。
  - **sap mode-list gcm-encrypt gmac**：機密性が推奨され、整合性が必須。保護はサプリカントの設定に応じてサプリカントによって選択されます。
  - **sap mode-list gmac**：整合性のみ。
  - **sap mode-list gcm-encrypt**：機密性が必須。
  - **sap mode-list gmac gcm-encrypt**：整合性が必須であり推奨される。機密性は任意。

別の Cisco TrustSec デバイスへのインターフェイスで Cisco TrustSec を手動で設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **interface** *interface-id*
3. **cts manual**
4. **sap pmk** *key* [**mode-list** *mode1* [*mode2* [*mode3* [*mode4*]]]]
5. **no propagate sgt**
6. **exit**
7. **end**
8. **show cts interface** [*interface-id* | **brief** | **summary**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# 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	**interface** *interface-id* 例： `Switch(config)# interface tengigabitethernet 1/1/2`	（注） 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	**cts manual** 例：	Cisco TrustSec 手動コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Switch(config-if)# cts manual`	
ステップ 4	**sap pmk** *key* [**mode-list** *mode1* [*mode2* [*mode3* [*mode4*]]]] 例： `Switch(config-if-cts-manual)# sap pmk 1234abcdef mode-list gcm-encrypt null no-encap`	（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 動作モードのオプションは次のとおりです。 • **gcm-encrypt**：認証および暗号化 （注） ソフトウェア ライセンスが MACsec 暗号化をサポートする場合、MACsec の認証と暗号化にこのモードを選択します。 • **gmac**：認証、暗号化なし • **no-encap**：カプセル化なし • **null**：カプセル化、認証または暗号化なし （注） インターフェイスでデータ 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。SGT はサポートされません。
ステップ 5	**no propagate sgt** 例： `Switch(config-if-cts-manual)# no propagate sgt`	ピアが SGT を処理できない場合、このコマンドの **no** 形式を使用します。**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 6	**exit** 例： `Switch(config-if-cts-manual)# 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 7	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show cts interface** [*interface-id* | **brief** | **summary**]	（任意）TrustSec 関連のインターフェイス特性を表示して、設定を確認します。

例

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。

```
Switch# configure terminal
Switch(config)# interface tengigabitethernet 1/1/2
Switch(config-if)# cts manual
Switch(config-if-cts-manual)# sap pmk 1234abcdef mode-list gcm-encrypt null no-encap
Switch(config-if-cts-manual)# no propagate sgt
Switch(config-if-cts-manual)# exit
Switch(config-if)# end
```

MACsec 暗号化の設定例

例：インターフェイスでの MACsec の設定

インターフェイスでの MACsec の設定

```
スイッチ(config)# interface GigabitEthernet1/0/25
スイッチ(config-if)# switchport access vlan 10
スイッチ(config-if)# switchport mode access
スイッチ(config-if)# macsec
スイッチ(config-if)# authentication event linksec fail action authorize vlan
 2
スイッチ(config-if)# authentication host-mode multi-domain
スイッチ(config-if)# authentication linksec policy must-secure
スイッチ(config-if)# authentication port-control auto
スイッチ(config-if)# authentication periodic
スイッチ(config-if)# authentication timer reauthenticate
スイッチ(config-if)# authentication violation protect
スイッチ(config-if)# mka policy replay-policy
スイッチ(config-if)# dot1x pae authenticator
スイッチ(config-if)# spanning-tree portfast
スイッチ(config-if)# end
スイッチ# show authentication session interface gigabitethernet1/0/5

Interface MAC Address Method Domain Status Fg Session ID
---------------------------------------------------------------------------
Gi1/0/5 88f0.7788.9205 dot1x VOICE Auth 1E0000010000001300030B0F
Gi1/0/5 000c.2923.6ff1 dot1x DATA  Auth 1E0000010000001400030D80


Key to Session Events Blocked Status Flags:

A - Applying Policy (multi-line status for details)
D - Awaiting Deletion
F - Final Removal in progress
I - Awaiting IIF ID allocation
N - Waiting for AAA to come up
P - Pushed Session
R - Removing User Profile (multi-line status for details)
U - Applying User Profile (multi-line status for details)
```

```
X - Unknown Blocker

Runnable methods list:
Handle Priority Name
7 5 dot1x
21 10 mab

19 15 webauth
```

スイッチ# **show authentication session interface gigabitethernet1/0/5 details**

```
Interface: GigabitEthernet1/0/5
MAC Address: 88f0.7788.9205
IPv6 Address: Unknown
IPv4 Address: Unknown
User-Name: CP-9971-SEP88F077889205
Status: Authorized
Domain: VOICE
Oper host mode: multi-domain
Oper control dir: both
Session timeout: N/A
Common Session ID: 1E000001000000001300030B0F
Acct Session ID: Unknown
Handle: 0xC0000006
Current Policy: POLICY_Gi1/0/5

Local Policies:
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
Security Policy: Should Secure
Security Status: Link Unsecure

Server Policies:

Method status list:

Method State

dot1x Authc Success

----------------------------------------
Interface: GigabitEthernet1/0/5
MAC Address: 000c.2923.6ff1
IPv6 Address: Unknown
IPv4 Address: 172.30.30.50
User-Name: dataMustSecure
Status: Authorized
Domain: DATA
Oper host mode: multi-domain
Oper control dir: both
Session timeout: N/A
Common Session ID: 1E000001000000001400030D80
Acct Session ID: Unknown
Handle: 0x22000007
Current Policy: POLICY_Gi1/0/5

Local Policies:
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
Security Policy: Should Secure

Security Status: Link Secured

Server Policies:

Method status list:
```

```
Method State

dot1x Authc Success

スイッチ#
スイッチ# show  macsec interface gigabitethernet1/0/5
MACsec is enabled
Replay protect : enabled
Replay window : 0
Include SCI : yes
Use ES Enable : no
Use SCB Enable : no
Admin Pt2Pt MAC : forceTrue(1)
Pt2Pt MAC Operational : no
Cipher : GCM-AES-128
Confidentiality Offset : 0

Capabilities
Identifier :
Name :
ICV length : 16
Data length change supported: yes
Max. Rx SA : 8
Max. Tx SA : 8
Max. Rx SC : 4
Max. Tx SC : 4
Validate Frames : strict
PN threshold notification support : Yes
Ciphers supported : GCM-AES-128

Transmit Secure Channels
SCI : 547C69B687850002
SC state : inUse(1)
Elapsed time : 16:36:44
Start time : 7w0d
Current AN: 0
Previous AN: -
Next PN: 0
SA State: inUse(1)
Confidentiality : no
SAK Unchanged : no
SA Create time : 00:09:21
SA Start time : 7w0d
SC Statistics
Auth-only Pkts : 0
Auth-only Bytes : 0
Encrypt Pkts : 52960
Encrypt Bytes : 0
SA Statistics
Auth-only Pkts : 0
Encrypt Pkts : 52960

Port Statistics

Receive Secure Channels
SCI : 000C29236FF10000
SC state : inUse(1)
Elapsed time : 16:36:44
Start time : 7w0d
Current AN: 0
Previous AN: -
Next PN: 0
RX SA Count: 0
SA State: inUse(1)
```

```
SAK Unchanged : no
SA Create time : 00:09:19
SA Start time : 7w0d
SC Statistics
Notvalid pkts 0
Invalid pkts 0
Valid pkts 9914
Valid bytes 0
Late pkts 0
Uncheck pkts 0
Delay pkts 0
UnusedSA pkts 0
NousingSA pkts 0
Decrypt bytes 0
SA Statistics
Notvalid pkts 0
Invalid pkts 0
Valid pkts 9914
UnusedSA pkts 0
NousingSA pkts 0

Port Statistics

Switch#
```

EAP-TLS を使用した MACsec MKA の設定例

例:：証明書の登録

```
Configure Crypto PKI Trustpoint:
  crypto pki trustpoint POLESTAR-IOS-CA
   enrollment terminal
   subject-name CN=ASR1000x1@polestar.com, C=IN, ST=KA, OU=ENG,O=Polestar
   revocation-check none
   rsakeypair mkaioscarsa
   storage nvram:
  !
Manual Installation of Root CA certificate:
 crypto pki authenticate POLESTAR-IOS-CA
```

例：802.1x 認証の有効化と AAA の設定

```
aaa new-model
dot1x system-auth-control
radius server ISE
 address ipv4 <ISE ipv4 address> auth-port 1645 acct-port 1646
 automate-tester username dummy
 key dummy123
 radius-server deadtime 2
!
aaa group server radius ISEGRP
 server name ISE
!
```

```
aaa authentication dot1x default group ISEGRP
aaa authorization network default group ISEGRP
```

例：EAP-TLS プロファイルと 802.1x クレデンシャルの設定

```
eap profile EAPTLS-PROF-IOSCA
 method tls
 pki-trustpoint POLESTAR-IOS-CA
!

dot1x credentials EAPTLSCRED-IOSCA
 username asr1000@polestar.company.com
 pki-trustpoint POLESTAR-IOS-CA
!
```

例：インターフェイスでの 802.1 X、PKI、および MACsec の設定の適用

```
interface TenGigabitEthernet0/1
 macsec network-link
 authentication periodic
 authentication timer reauthenticate <reauthentication interval>
 access-session host-mode multi-host
 access-session closed
 access-session port-control auto
 dot1x pae both
 dot1x credentials EAPTLSCRED-IOSCA
 dot1x supplicant eap profile EAPTLS-PROF-IOSCA
 service-policy type control subscriber DOT1X_POLICY_RADIUS
```

Cisco TrustSec スイッチ間リンク セキュリティの設定例

次に、Cisco TrustSec スイッチ間のセキュリティのためにシードおよび非シード デバイスに必要な設定を示します。リンク セキュリティ用に AAA および RADIUS を設定する必要があります。この例では、ACS-1 から ACS-3 は任意のサーバー名、cts-radius は Cisco TrustSec サーバーです。

シード デバイスの設定

```
Switch(config)# aaa new-model
Switch(config)# radius server ACS-1
Switch(config-radius-server)# address ipv4 10.5.120.12 auth-port 1812 acct-port
 1813
Switch(config-radius-server)# pac key cisco123
Switch(config-radius-server)# exit
Switch(config)# radius server ACS-2
Switch(config-radius-server)# address ipv4 10.5.120.14 auth-port 1812 acct-port
 1813
Switch(config-radius-server)# pac key cisco123
Switch(config-radius-server)# exit
Switch(config)# radius server ACS-3
```

```
Switch(config-radius-server)# address ipv4 10.5.120.15 auth-port 1812 acct-port
 1813
Switch(config-radius-server)# pac key cisco123
Switch(config-radius-server)# exit
Switch(config)# aaa group server radius cts-radius
Switch(config-sg-radius)# server name ACS-1
Switch(config-sg-radius)# server name ACS-2
Switch(config-sg-radius)# server name ACS-3
Switch(config-sg-radius)# exit
Switch(config)# aaa authentication login default none
Switch(config)# aaa authentication dot1x default group cts-radius
Switch(config)# aaa authorization network cts-radius group cts-radius
Switch(config)# aaa session-id common
Switch(config)# cts authorization list cts-radius
Switch(config)# dot1x system-auth-control

Switch(config)# interface gi1/1/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# cts dot1x
Switch(config-if-cts-dot1x)# sap mode-list gcm-encrypt gmac
Switch(config-if-cts-dot1x)# no propagate sgt
Switch(config-if-cts-dot1x)# exit
Switch(config-if)# exit

Switch(config)# interface gi1/1/4
Switch(config-if)# switchport mode trunk
Switch(config-if)# cts manual
Switch(config-if-cts-manual)# sap pmk 033445AABBCCDDEEFF mode-list gcm-encrypt
 gmac
Switch(config-if-cts-manual)# no propagate sgt
Switch(config-if-cts-manual)# exit
Switch(config-if)# exit

Switch(config)# radius-server vsa send authentication
Switch(config)# exit
Switch# cts credentials id cts-36 password trustsec123
```

非シード デバイス

```
Switch(config)# aaa new-model
Switch(config)# aaa session-id common
Switch(config)# dot1x system-auth-control

Switch(config)# interface gi1/1/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# shutdown
Switch(config-if)# cts dot1x
Switch(config-if-cts-dot1x)#sap mode-list gcm-encrypt gmac
Switch(config-if-cts-dot1x)#exit
Switch(config-if)#exit

Switch(config)# interface gi1/1/4
Switch(config-if)# switchport mode trunk
Switch(config-if)# shutdown
Switch(config-if)# cts manual
```

```
Switch(config-if-cts-manual)# sap pmk 033445AABBCCDDEEFF mode-list gcm-encrypt
 gmac
Switch(config-if-cts-manual)# no propagate sgt
Switch(config-if-cts-manual)# exit
Switch(config-if)# exit

Switch(config)# radius-server vsa send authentication
Switch(config)# end
Switch# cts credentials id cts-72 password trustsec123
```

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