# 証明書ベースの MACsec 暗号化

証明書ベースの MACsec 暗号化機能は、Extensible Authentication Protocol – Transport Layer Security（EAP-TLS）による802.1X ポートベース認証を使用して、MACsec 暗号化が必要なルータ ポートの証明書を伝送します。EAP-TLS メカニズムを使用して相互認証を実行し、プライマリセッションキーを取得します。このキーから、MACsec Key Agreement（MKA）プロトコル用の接続アソシエーションキー（CAK）が導出されます。

証明書ベースの MACsec 暗号化は、リモート認証またはローカル認証のいずれかを使用して実行されます。



# 証明書ベース MACsec 暗号化の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

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、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1:* 証明書ベース *MACsec* 暗号化の機能情報

| 機能名 | リリース | 機能情報 |
|---|---|---|
| 証明書ベースの MACsec 暗号化 | Cisco IOS XE Everest リリース 16.6.1 | 証明書ベースの MACsec 暗号化機能は、MACsec 暗号化が必要なルータポートの証明書を伝送するために、拡張認証プロトコルを使用した 802.1 x ポートベースの認証を使用します。 Transport Layer Security (eap-tls) を使用します。EAP-TLS メカニズムを使用して相互認証を実行し、プライマリセッションキーを取得します。このキーから、MACsec Key Agreement（MKA）プロトコル用の接続アソシエーションキー（CAK）が導出されます。 |

# 証明書ベース MACsec 暗号化の前提条件

- 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。『*Cisco Identity Services Engine* リリース *2.3* 管理者ガイド』を参照してください。
- 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。

# 証明書ベース MACsec 暗号化の制約事項

- MKA は、ポート チャネルではサポートされていません。
- MKA のハイ アベイラビリティはサポートされません。
- サブインターフェイスでの証明書ベースの MACsec 暗号化はサポートされていません。

# 証明書ベース MACsec 暗号化に関する情報

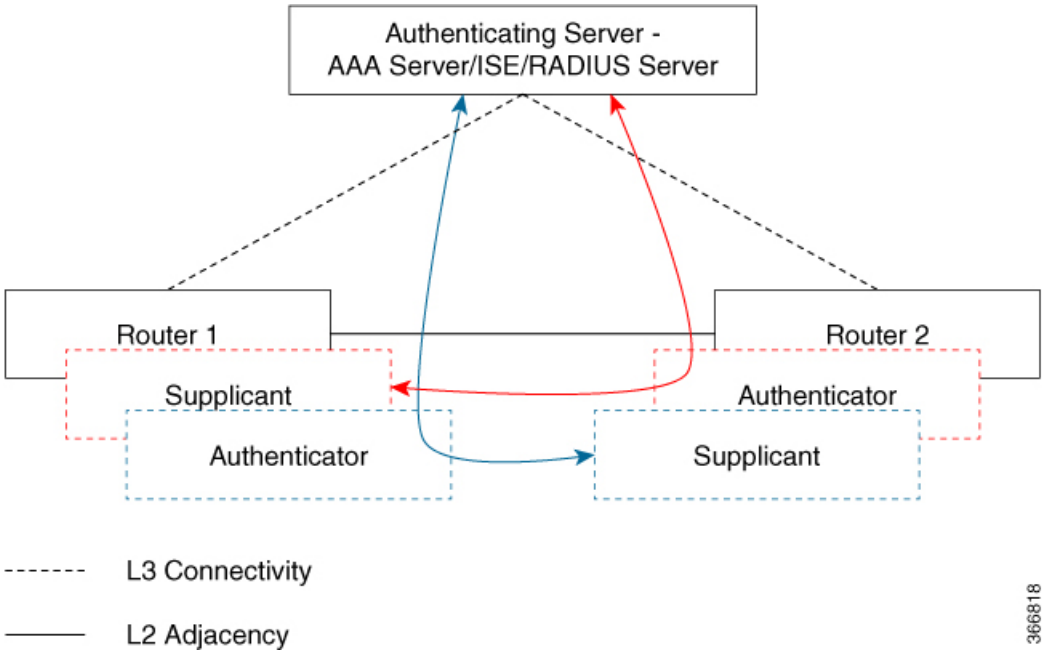
MKA MACsec は、ルータ間のリンクでサポートされています。Extensible Authentication Protocol（EAP-TLS）による IEE 802.1X ポートベース認証を使用して、デバイスのポート間の MKA MACsec を設定できます。EAP-TLS は相互認証を許可し、プライマリセッションキーを取得します。そのキーから、MKA プロトコル用の接続アソシエーションキー（CAK）が取得されます。デバイスの証明書は、AAA サーバーへの認証用に、EAP-TLS を使用して伝送されます。

# リモート認証を使用した証明書ベース MACsec 暗号化のコール フロー

サプリカントは、ネットワークへアクセスしようとする未承認デバイスです。オーセンティケータは、サプリカントの認証ステータスに基づいて、ネットワークへの物理アクセスを制御するデバイスです。

次の図に示すように、デバイスは直接接続されています。ルータは、ポート上で EAP サプリカントとオーセンティケータの両方として機能します。

次の図は、ルータ上の 2 つの EAP コール フロー（個別の EAP セッション ID を持つ）を示しています。赤色のフローは、ルータ 1 をサプリカントとして、ルータ 2 をオーセンティケータとして示しています。青のフローはその逆を示しています。




インターフェイスが 802.1 x の両方のロールとして設定されている場合、ルータの認証マネージャは、サプリカントとオーセンティケータのロールを使用して 2 つの EAP セッション（個別の EAP セッション ID を持つ青色と赤色のセッション）フローを持つセッションを作成し、両方のロールがリモート認証サーバー（AAA サーバー/ISE/RADIUS）を使用した EAP-TLS 相互認証をトリガします。

相互認証後、認証サーバーとしてより大きいMACアドレスを持ち、オーセンティケータ ロールを持つルータに対応するフローの MSK が選択されて CAK を導出します。

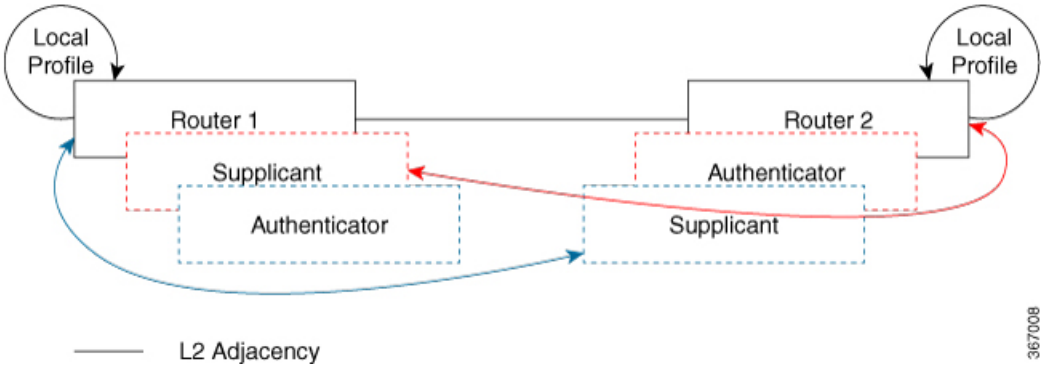
上の図では、ルータ 1 の MAC アドレスがルータ 2 より小さい場合、EAP セッション（青色のフロー）から取得したプライマリセッションキー（PSK）がMKAのEAP-PSKとして使用されます（ルータ 1 はオーセンティケータとして、ルータ 2 はサプリカントとして機能します）。これにより、ルータ1がMKA キーサーバーとして機能し、ルータ2が非キーサーバーとして機能することが保証されます。

ルータ 2 の MAC アドレスがルータ 1 の MAC アドレスよりも小さい場合は、EAP セッションから取得された PSK（赤色のフロー）が（両方のルータにより）MKA の EAP-PSK として使用され、CAK が導出されます。

# ローカル認証を使用した証明書ベース MACsec 暗号化のコール フロー

次の図に示すように、デバイスは直接接続されています。ルータは、ポート上で EAP サプリカントとオーセンティケータの両方として機能します。

次の図は、ルータ上の 2 つの EAP コール フロー（個別の EAP セッション ID を持つ）を示しています。赤色のフローは、ルータ 1 をサプリカントとして、ルータ 2 をオーセンティケータとして示しています。青のフローはその逆を示しています。




インターフェイスが 802.1 x の両方のロールとして設定されている場合、ルータの認証マネージャは、サプリカントとオーセンティケータのロールを使用して 2 つの EAP セッション（個別の EAP セッション ID を持つ青色と赤色のセッション）フローを持つセッションを作成し、両方のロールがローカル認証サーバーを使用した EAP-TLS 相互認証をトリガします。

相互認証後、認証サーバーとしてより大きい MAC アドレスを持ち、オーセンティケーターロールを持つルータに対応するフローの PSK が選択されて CAK を導出します。

上の図では、ルータ 1 の MAC アドレスがルータ 2 より小さい場合、EAP セッション（青色のフロー）から取得したプライマリセッションキー（PSK）が MKA の EAP-PSK として使用されます（ルータ 1 はオーセンティケータとして、ルータ 2 はサプリカントとして機能します）。これにより、ルータ1が MKA キーサーバーとして機能し、ルータ2が非キーサーバーとして機能することが保証されます。

ルータ 2 の MAC アドレスがルータ 1 の MAC アドレスよりも小さい場合は、EAP セッションから取得された PSK（赤色のフロー）が（両方のルータにより）MKA の EAP-PSK として使用され、CAK が導出されます。

# リモート認証を使用した証明書ベース MACsec 暗号化の設定

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

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。<br>• 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 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。<br>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。<br>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 4 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 5 | **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 6 | **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 | **enable** | 特権 EXEC モードを有効にします。<br>• 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。<br>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。<br>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。<br>（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。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | 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。<br>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。<br>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。<br>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。<br>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.」<br>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。<br>• 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。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| 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。<br>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。<br>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。<br>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。<br>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。<br>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。<br>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 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | 合、拡張子「-sign.crt」および「-encr.crt」が使用されます。<br>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。<br>（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。 |

# 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。<br>• 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。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| 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。<br>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。 |
| 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。<br>• パスワードを入力します（要求された場合）。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| 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。 |
| 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。<br>• 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。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| 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 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 13 | **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 14 | **exit** | 特権 EXEC モードに戻ります。 |
| ステップ 15 | **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 16 | **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。 |

# ローカル認証を使用した証明書ベース MACsec 暗号化の設定

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。

# 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。<br>• 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。<br>• 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。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| 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。<br>• 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。<br>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。<br>（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。<br>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。<br>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。<br>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。<br>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。<br>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.」<br>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。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| 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。<br>• 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。<br>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。<br>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。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| 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。<br>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。<br>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。<br>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。<br>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。<br>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。<br>（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。<br>• 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。 |
| 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。<br>• 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。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| 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。 |
| 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。 |

# 証明書ベース MACsec 暗号化の確認

証明書ベースの MACsec 暗号化の設定を確認するには、次の **show** コマンドを使用します。次に、 **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
```

# 証明書ベース MACsec 暗号化の設定例

## 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 802.1X、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
```

# その他の参考資料

### 関連資料

| 関連項目 | マニュアル タイトル |
|---|---|
| セキュリティ コマンド | • 『Security Command Reference: Commands A to C』<br>• 『Security Command Reference: Commands D to L』<br>• 『Security Command Reference: Commands M to R』<br>• 『Security Command Reference: Commands S to Z』 |

### 標準および RFC

| 標準/RFC | タイトル |
|---|---|
| IEEE 802.1AE-2006 | *Media Access Control*（*MAC*）セキュリティ |
| IEEE 802.1X-2010 | ポート ベースのネットワーク アクセス コントロール |
| IEEE 802.1AEbw-2013 | *Media Access Control*（*MAC*）セキュリティ（IEEE 802.1AE-2006 の修正）：Extended Packet Numbering（XPN） |
| IEEE 802.1Xbx-2014 | ポートベースのネットワーク アクセス コントロール（IEEE 802.1 x-2010 の修正） |
| RFC 4493 | *AES-CMAC* アルゴリズム |

### シスコのテクニカル サポート

| 説明 | リンク |
|---|---|
| 右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。 | http://www.cisco.com/cisco/web/support/index.html |

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。