



HTTPS アクセス

この章は、次の項で構成されています。

- [概要 \(1 ページ\)](#)
- [カスタム証明書の設定のガイドライン \(1 ページ\)](#)
- [SSL 暗号設定を変更する \(2 ページ\)](#)
- [GUI を使用した Cisco ACI HTTPS アクセス用カスタム証明書の設定 \(3 ページ\)](#)
- [GUI を使用したデフォルトの SSL プロトコルおよび Diffie-Hellman キー交換の構成 \(7 ページ\)](#)
- [NX-OS CLI を使用した証明書ベースの認証の有効化 \(8 ページ\)](#)
- [SSL 暗号について \(8 ページ\)](#)

概要

この記事は、Cisco ACI を使用する際の HTTPS アクセスのカスタム証明書を設定する方法の例を示します。

カスタム証明書の設定のガイドライン

- Cisco Application Policy Infrastructure Controller (APIC) で証明書署名要求 (CSR) を生成するために使用される秘密キーのエクスポートはサポートされていません。証明書の CSR を生成するために使用された秘密キーを共有することにより、「Subject Alternative Name (SAN)」フィールドのワイルドカード（「*cisco.com」など）を介して複数のサーバで同じ証明書を使用する場合は、秘密キーを Cisco Application Centric Infrastructure (ACI) ファブリックの外部に配置し、Cisco ACI ファブリックにインポートします。
- 証明書署名要求 (CSR) を生成する前に、公開中間証明書とルート CA 証明書をダウンロードしてインストールする必要があります。ルート CA 証明書は技術的には CSR を生成するために必要ではありませんが、シスコでは、対象とする CA 機関と CSR への署名に使用される実物の間の不一致を防ぐために、CSR を生成する前にルート CA 証明書が必要です。Cisco APIC は、送信された証明書が設定された CA によって署名されていることを確認します。

- 更新された証明書の生成に同じ公開キーと秘密キーを使用するには、次のガイドラインを満たす必要があります。
 - 元の CSR にはキー リング内の秘密キーとペアになる公開キーが含まれているため、元の CSR を維持する必要があります。
 - Cisco APIC で公開キーと秘密キーを再使用する場合は、元の証明書に使用されたものと同じ CSR を更新された証明書に再送信する必要があります。
 - 更新された証明書に同じ公開キーと秘密キーを使用する場合は、元のキーリングを削除しないでください。キーリングを削除すると、CSR で使用されている関連秘密キーが自動的に削除されます。
- Cisco ACI マルチサイト、VCPlugin、VRA、および SCVMM は、証明書ベースの認証ではサポートされません。
- Cisco APIC クラスタごとに 1 つの SSL 証明書のみが許可されます。
- 以降のリリースからリリース 4.0(1) にダウングレードする前に、証明書ベースの認証を無効にする必要があります。
- 証明書ベースの認証セッションを終了するには、ログアウトして CAC カードを削除する必要があります。
- Cisco APIC に設定されたカスタム証明書は、リーフ スイッチとスパイン スイッチに展開されます。ファブリック ノードに接続するために使用される URL または DN が **[サブジェクト (Subject)]** または **[サブジェクト代替名 (Subject Alternative Name)]** フィールド内にある場合、ファブリック ノードは証明書でカバーされます。
- Cisco APIC GUI は、最大サイズが 4k バイトの証明書を受け入れることができます。
- HTTPS アクセスに使用している自己署名 SSL 証明書の有効期限が切れると、証明書は自動的に更新されます。

SSL 暗号設定を変更する

SSL 暗号は、有効化、無効化、または完全に削除できます。必要な暗号設定に応じて、必要な正確な組み合わせを理解する必要があります。暗号が残らない方法で暗号を無効化および有効化することは設定ミスであり、NGINX の検証に失敗します。

NGINX は OpenSSL 暗号リスト形式を使用します。形式については、OpenSSL Web サイトにアクセスしてください。

Cisco APIC SSL 設定オプションを暗号リスト形式化にマッピングする

暗号を有効にすると、その暗号が NGINX 構成ファイルに書き込まれます。暗号を無効にすると、その暗号が NGINX 構成ファイルに前に感嘆符 (!) を付けて書き込まれます。たとえば、

「EEDCH」を無効にすると、「!EEDCH」と書き込まれます。暗号を削除すると、その暗号が NGINX 構成ファイルに暗号がまったく書き込まれなくなります。



(注) OpenSSL 暗号リスト形式のドキュメントには次のように記載されています。「(!) が使用されている場合、暗号はリストから完全に削除されます。削除された暗号は、明示的に指定されていても、リストに再び表示されることはありません」これにより、暗号の「有効」状態に関係なく、「無効」に設定された暗号を参照する組み合わせ暗号が削除される可能性があります。

例：「EEDCH」を無効にし、「EECDH+aRSA+SHA384」を有効にします。これにより、次が NGINX 構成ファイルに書き込まれます：「!EEDCH:EECDH+aRSA+SHA384」。「!EEDCH」は、「EECDH+aRSA+SHA384」が追加されないようにします。これにより、暗号が使用されないことで NGINX 検証に失敗するため、NGINX の更新（カスタム HTTPS 証明書の適用など）が成功しなくなります。

Cisco APIC SSL 設定を変更する前の暗号リスト形式のテスト

Cisco Application Policy Infrastructure Controller (APIC) に暗号の変更を加える前に、`openssl ciphers -V 'cipher_list'` コマンドを使用して、計画した暗号の組み合わせの結果を検証し、暗号出力が目的の結果と一致することを確認します。

例：

```
apic# openssl ciphers -V 'EECDH+aRSA+SHA256:EECDH+aRSA+SHA384'
0xC0,0x27 - ECDHE-RSA-AES128-SHA256 TLSv1.2 Kx=EC DH Au=RSA Enc=AES (128)
Mac=SHA256
0xC0,0x28 - ECDHE-RSA-AES256-SHA384 TLSv1.2 Kx=EC DH Au=RSA Enc=AES (256)
Mac=SHA384
```

テストした暗号リストがエラーまたは「暗号が一致しません」という結果になった場合は、この設定を Cisco APIC に適用しないでください。これを行うと、Cisco APIC GUI にアクセスできなくなったり、カスタム証明書アプリケーションが壊れたりするなど、NGINX の問題が発生する可能性があります。

例：

```
apic# openssl ciphers -V '!EECDH:EECDH+aRSA+SHA256:EECDH+aRSA+SHA384'
Error in cipher list
132809172158128:error:1410D0B9:SSL routines:SSL_CTX_set_cipher_list:no cipher
match:ssl_lib.c:1383:
```

GUI を使用した Cisco ACI HTTPS アクセス用カスタム証明書の設定



注意 ダウンタイムの可能性があるため、メンテナンス時間中にのみこのタスクを実行してください。

ダウンタイムは外部ユーザまたはシステムからの Cisco Application Policy Infrastructure Controller (APIC) APIC クラスタおよびスイッチへのアクセスには影響しますが、Cisco APIC とスイッチの接続には影響しませスイッチで実行されている NGINX プロセスのため、外部接続にも影響が及びますが、ファブリックのデータプレーンには影響ありません。Cisco APIC、設定、管理、トラブルシューティングなどへのアクセスは影響を受けることになります。Cisco APIC およびスイッチで実行されている NGINX Web サーバーは、この操作中に再起動されます。

始める前に

適切な認証局を作成できるように、信頼できる証明書を取得する機関を決定します。

手順

-
- ステップ 1** メニュー バーで、**[Admin] > [AAA]** の順にクリックします。
- ステップ 2** **[ナビゲーション (Navigation)]** ペインで、**[セキュリティ (Security)]** を選択します。
- ステップ 3** 作業ペインで、**[認証局 (Certificate Authorities)] > [アクション (Actions)] > [認証局の作成 (Create Certificate Authority)]** の順に選択します。
- ステップ 4** **[認証局の作成 (Create Certificate Authority)]** 画面で、**[Name (名前)]** フィールドに、認証局の名前を入力します。
- ステップ 5** (オプション) 認証局の **[説明 (Description)]** を入力します。
- ステップ 6** **[証明書チェーン (Certificate Chain)]** フィールドで、Cisco APIC の証明書署名要求 (CSR) に署名する認証局の中間証明書とルート証明書をコピーします。
- 証明書は、Base64 エンコード X.509 CER (Cisco Emergency Responder) フォーマットである必要があります。中間証明書はルート CA 証明書の前に配置されます。次の例のようになります。
- ```
-----BEGIN CERTIFICATE-----
<Intermediate Certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Root CA Certificate>
-----END CERTIFICATE-----
```
- ステップ 7** **[保存 (Save)]** をクリックします。
- ステップ 8** 作業ペインで、**[キーリング (Key Rings)] > [アクション (Actions)] > [キーリングの作成 (Create Key Ring)]** の順に選択します。
- キーリングを使用すると、以下を管理できます。
1. 秘密キー (外部デバイスからインポートされた、または Cisco APIC で内部的に生成されたもの)。
  2. 秘密キーによって生成された CSR。
  3. CSR を通じて署名された証明書。
- ステップ 9** **[Create Key Ring]** ダイアログボックスで、**[Name]** フィールドに、名前を入力します。
- ステップ 10** (オプション) キーリングの **[説明 (Description)]** を入力します。

- ステップ 11** [認証局 (Certificate Authority)] フィールドで、[認証局の選択 (Select Certificate Authority)] をクリックし、以前に作成した認証局を選択するか、[認証局の作成 (Create Certificate Authority)] を選択します。
- ステップ 12** [秘密キー (Private Key)] フィールドで必要なラジオボタンを選択します。  
次のオプションがあります。
1. 新しいキーの生成 (Generate New Key)
  2. 既存キーのインポート (Import Existing Key.)
- ステップ 13** 秘密キーを入力します。このオプションは、[秘密キー (Private Key)] の [既存キーのインポート (Import Existing Key)] オプションを選択した場合にのみ表示されます。
- ステップ 14** [秘密キー (Private Key)] フィールドで [新しいキーの生成 (Generate New Key)] オプションを選択した場合は、[キー タイプ (Key Type)] で必要なラジオ ボタンを選択します。  
選択できる基準は、次のとおりです。
1. [RSA] (Rivest、Shamir、および Adelman)
  2. [ECC] (楕円曲線暗号)。ECDSA (楕円曲線デジタル署名アルゴリズム) とも呼ばれます。
- ステップ 15** キーリングで Cisco APIC を使用して CSR を生成する場合は、その内容を [証明書 (Certificate)] フィールドに追加しないでください。前の手順で Cisco APIC を使用せずに秘密キーおよび CSR を生成していて、CA によって署名された証明書がある場合は、その内容を [証明書 (Certificate)] フィールドに追加します。
- ステップ 16** 暗号に必要なキー強度を選択します。このオプションは、[秘密キー (Secret Key)] で [新しいキーの生成 (Generate New Key)] オプションを選択した場合にのみ表示されます。RSA の場合は [モジュラス (Modulus)] ドロップダウンリストで、ECC [キー タイプ (Key Type)] の場合は [ECC カーブ (ECC Curve)] ラジオ ボタンで選択します。
- a) [キー タイプ (Key Type)] で [RSA] を選択した場合は、[モジュラス (Modulus)] ドロップダウンリストからモジュラス値を選択します。
  - b) [キー タイプ (Key Type)] で [ECC] を選択した場合は、[ECC 曲線 (ECC Curve)] ラジオ ボタンのリストから適切な曲線を選択します。
- ステップ 17** [保存 (Save)] ([キーリングの作成 (Create Key Ring)] 画面) をクリックします。
- ステップ 18** [作業 (Work)] ペインで、[キーリング (Key Rings)] > [キーリング名] を選択します (または、必要なキーリングの行をダブルクリックします)。
- 署名付き証明書と秘密キーを入力していない場合は、[作業 (Work)] ペインの [キーリング (Key Rings)] 領域で、作成されたキーリングの [管理状態 (Admin State)] に [開始 (Started)] と表示され、CSR が生成されるのを待ちます。手順 19 に進みます。
- 署名付き証明書と秘密キーの両方を入力した場合は、[キーリング (Key Rings)] 領域に、作成されたキーリングの [管理状態 (Admin State)] が [完了 (Completed)] と表示されます。手順 22 に進みます。
- (注)  
キーリングは削除しないでください。キーリングを削除すると、CSR で使用されている関連秘密キーが自動的に削除されます。

展開ボタンをクリックすると、新しい画面に選択したキーリングが表示されます。

**ステップ 19** [証明書要求 (Certificate Request)] ペインで、[証明書要求の作成 (Create Certificate Request)] をクリックします。

[証明書要求 (Certificate Request)] ウィンドウが表示されます。

a) [サブジェクト (Subject)] フィールドに、CSR の共通名 ([CN]) を入力します。

ワイルドカードを使用して Cisco APIC の完全修飾ドメイン名 (FQDN) を入力することもできますが、新しいタイプの証明書では、識別可能な証明書の名前を入力し、[代替サブジェクト名 (Alternate Subject Name)] フィールド ([SAN] フィールド) にすべての Cisco APIC の FQDN を入力することを推奨します (多くの最新のブラウザは、[SAN] フィールドに FQDN が入力されていることを想定しています)。

b) [代替サブジェクト名 (Alternate Subject Name)] フィールドに、「DNS:apic1.example.com, DNS:apic2.example.com, DNS:apic3.example.com」や「DNS:\*example.com」など、すべての Cisco APIC の FQDN を入力します。。

または、SAN を IP アドレスと一致させる場合は、Cisco APIC の IP アドレスを次の形式で入力します。

IP:192.168.2.1

このフィールドには、DNS 名、IPv4 アドレス、またはその両方を組み合わせて使用できます。IPv6 アドレスはサポートされていません。

c) [地域 (Locality)] フィールドに、組織の市または町を入力します。

d) [州 (State)] フィールドに、組織が所在する州を入力します。

e) [国 (Country)] フィールドに、組織の所在地の国を表す 2 文字の ISO コードを入力します。

f) [組織名 (Organization Name)] を入力し、[組織単位名 (Organization Unit Name)] に単位を入力します。

g) 組織の連絡担当者の [電子メール (Email)] アドレスを入力します。

h) [パスワード (Password)] に入力し、[パスワードの確認 (Confirm Password)] フィールドにもう一度入力します。

i) [OK] をクリックします。

**ステップ 20** [証明書要求の設定 (Certificate Request Settings)] ペインに、上で入力した情報が表示されます (手順 19)。

**ステップ 21** [作業 (Work)] ペインで、[キーリング (Key Rings)] > [キーリング名] を選択します (または、必要なキーリングの行をダブルクリックします)。

新しい画面に選択したキーリングが表示されます。

(注)

キーリングに示されている認証局によって署名されていない CSR、または MS-DOS 形式の行末を持つ CSR は受け入れられません。エラーメッセージが表示されたら、MS-DOS の行末を削除して解決します。

キーが正常に確認されて、[作業 (Work)] ペインの [管理状態 (Admin State)] が [完了済み (Completed)] に変わり、HTTP ポリシーで使用できるようになります。

- ステップ 22 メニューバーで、[ファブリック (Fabric)] > [ファブリック ポリシー (Fabric Policies)] を選択します。
- ステップ 23 [ナビゲーション (Navigation)] ペインで、[ポリシー (Policies)] > [ポッド (Pod)] > [管理アクセス (Management Access)] > [デフォルト (default)] をクリックします。
- ステップ 24 [Work] ペインの [Admin Key Ring] ドロップダウン リストで目的のキー リングを選択します。
- ステップ 25 (オプション) 証明書ベースの認証では、[Client Certificate TP] ドロップダウン リストで、以前に作成したローカル ユーザ ポリシーを選択し、[Client Certificate Authentication state] の [Enabled] をクリックします。
- ステップ 26 [Submit] をクリックします。  
すべての Web サーバーがリスタートし、証明書がアクティブになり、デフォルト以外のキーリングは HTTPS アクセスに関連付けられます。

### 次のタスク

証明書の失効日には注意し、期限切れになる前に必要な措置を取ってください。更新された証明書に同じキー ペアを保持するには、CSR を保持します。CSR にはキーリング内の秘密キーとペアになる公開キーが含まれています。証明書が期限切れになる前に、同じ CSR を再送信してください。削除したり、新しいキーリングを作成したりしないでください。キーリングを削除すると、Cisco APIC に保存されている秘密キーが削除されます。

## GUI を使用したデフォルトの SSL プロトコルおよび Diffie-Hellman キー交換の構成

この手順では、デフォルトの SSL プロトコルと Diffie-Hellman キー交換を構成します。これらのパラメータは、組織のセキュリティポリシーと、使用するアプリケーションのニーズに基づいて構成する必要があります。

### 手順

- ステップ 1 メニューバーで、[ファブリック (Fabric)] > [ファブリック ポリシー (Fabric Policies)] を選択します。
- ステップ 2 [ナビゲーション (Navigation)] ペインで、[ポリシー (Policies)] > [ポッド (Pod)] > [管理アクセス (Management Access)] > [デフォルト (default)] を選択します。
- ステップ 3 [作業 (Work)] ペインで、[HTTPS] セクションを見つけます。
- a) [SSL プロトコル (SSL Protocols)] の場合、ネットワークで許可されているトランスポート層セキュリティ (TLS) のバージョンのチェックボックスをオンにします。ネットワークで許可されていない TLS バージョンについては、ボックスをオフのままにします。
  - b) 6.0(1) リリースでは、[DH パラメータ (DH Param)] で、必要なキーサイズ (ビット単位) を選択します。

いずれかのキーサイズを選択すると、楕円曲線 Diffie-Hellman (ECDH) キー交換に加えて、標準の Diffie-Hellman (DH) キー交換が有効になり、選択したビット数が DH キー交換で使用されます。[な

し（**None**）]を選択した場合には、楕円曲線 ECDH キー交換のみが使用されます。いずれの場合も、ECDH は常に 256 ビットを使用します。

6.0(2)リリース以降、DH パラメータは、クライアントとの通信ハンドシェイク中に動的に決定されます。キーサイズを手動で選択する必要はなくなりました。

c) [Submit] をクリックします。

## NX-OS CLI を使用した証明書ベースの認証の有効化

### 手順

証明書ベースの認証を有効にするには、次の手順を実行します。

例：

```
To enable CAC for https access:
configure terminal
 comm-policy default
 https
 client-cert-ca <ca name>
 client-cert-state-enable
To disable:
configure terminal
 comm-policy default
 https
 no client-cert-state-enable
 no client-cert-ca
```

## SSL 暗号について

Cisco Application Centric Infrastructure (ACI) Representational State Transfer (REST) アプリケーションプログラミングインターフェイス (API) は、ソリューションがデビューした日から、HTTPS/SSL/TLS サポートがますます厳しくなる最近のバージョンへと進化を遂げました。このドキュメントは、Cisco ACI REST API での HTTPS、SSL、および TLS サポートの進化について説明し、クライアントが REST API を安全に利用するために必要なものに関するガイドを顧客に提供することを目的としています。

HTTPS は、Secure Socket Layers (SSL) または Transport Layer Security (TLS) のいずれかを利用して、HTTP セッションの安全な接続を形成するプロトコルです。SSL または TLS は、クライアントと HTTP サーバ間のトラフィックを暗号化するために使用されます。さらに、HTTPS をサポートするサーバには、サーバの信頼性を検証するためにクライアントが通常使用できる証明書があります。これは、サーバで認証するクライアントの反対です。この場合、サーバは「私は server\_xyz です。それを証明する証明書はここにあります」と言っていま



す。その後、クライアントはその証明書を利用して、サーバーが「server\_xyz」であることを確認できます。

SSL/TLS には、SSL または TLS プロトコルの固有のセキュリティだけでなく、各プロトコルで使用可能なサポートされている暗号化方式も関係する、他の重要な側面があります。SSL は、SSLv1、SSLv2、SSLv3 の 3 回の反復を経て、現在ではすべて安全ではないと見なされています。TLS は、TLSv1、TLSv1.1、および TLSv1.2 の 3 つの反復を経ており、そのうち TLSv1.1 と TLSv1.2 のみが「安全」と見なされています。理想的には、クライアントは利用可能な最高の TLS バージョンを利用し、サーバーは TLSv1.1 と TLSv1.2 のみをサポートする必要があります。ただし、ほとんどのサーバは、古いクライアントに対して TLSv1 を保持する必要があります。

ほぼすべての最新のブラウザで、TLSv1.1 と TLSv1.2 の両方をサポートしています。ただし、HTTPS を使用するクライアントはブラウザではない場合があります。クライアントは、Web サーバーと通信し、HTTPS/TLS をネゴシエートする必要がある Java アプリケーションまたは Python スクリプトである場合があります。このような状況では、何をどこでサポートするかという問題がより重要になります。

## CLI を使用してサポートされている SSL 暗号を判別する

### 始める前に

このセクションでは、CLI を使用して、サポートされている SSL 暗号を判別する方法について説明します。

### 手順

**ステップ 1** 次に示されているように、OpenSSL 環境でサポートされている暗号を取得します。

例：  

```
openssl ciphers 'ALL:NULL'
```

**ステップ 2** 次に示されているように、sed またはその他のツールを使用して暗号を分離します。

例：  

```
openssl ciphers 'ALL:NULL' | sed -e 's/:/\n/g'
```

**ステップ 3** 次のように、暗号をループし、APIC をポーリングして、サポートされている暗号を確認します。

例：  

```
openssl s_client -cipher '<some cipher to test>' -connect <apic ipaddress>:<ssl port, usually 443>
```

次の暗号の例を参照してください。

例：  

```
openssl s_client -cipher 'ECDHE-ECDSA-AES128-GCM-SHA256' -connect 10.1.1.14:443
```

(注)

応答に `CONNECTED` が含まれている場合、その暗号はサポートされています。

---

## 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。