



NXAPI 証明書

Cisco NX-OS スイッチを NX-API HTTPS モードで機能させるには、SSL 証明書が必要です。SSL 証明書を生成し、CA によってそれに署名することができます。証明書は、スイッチ コンソールで CLI コマンドを使用して手動でインストールすること、または Cisco Nexus ダッシュボード ファブリック コントローラ を使用してスイッチにインストールすることができます。

Cisco Nexus ダッシュボード ファブリック コントローラ では、NX-API 証明書を Nexus ダッシュボード ファブリック コントローラ にアップロードするための Web UI フレームワークを提供しています。後で、Nexus ダッシュボード ファブリック コントローラ によって管理されるスイッチに証明書をインストールできます。



(注) この機能は、Cisco NXOS バージョン 9.2(3)以降で動作するスイッチでサポートされます。

- [証明書の生成と管理 \(1 ページ\)](#)

証明書の生成と管理

データセンター管理者は、スイッチごとに ASCII (base64) エンコードの証明書を生成します。この証明書は、次の 2 つのファイルで構成されます。

- 秘密キーを含む .key ファイル
- 証明書を含む .crt/.cer/.pem ファイル

Cisco Nexus ダッシュボード ファブリック コントローラ は、組み込みキー ファイル、つまり .crt/.cer/.pem ファイルを含む単一の証明書ファイルもサポートします。これには、.key ファイルの内容も含めることができます。

Nexus ダッシュボード ファブリック コントローラ は、バイナリ エンコードされた証明書はサポートしていません。つまり、.der 拡張子の証明書はサポートされません。キー ファイルは、暗号化用のパスワードで保護できます。Cisco Nexus ダッシュボード ファブリック コントローラ は暗号化を義務付けていません。ただし、これは Nexus ダッシュボード ファブリック

コントローラに保存されるため、キーファイルを暗号化することをお勧めします。NexusダッシュボードファブリックコントローラはAES暗号化をサポートしています。

CA署名付き証明書または自己署名証明書のいずれかを選択することができます。Cisco Nexusダッシュボードファブリックコントローラは署名を義務付けていません。ただし、セキュリティガイドラインでは、CA署名付き証明書を使用することを推奨しています。

複数のスイッチ用に複数の証明書を生成して、Nexusダッシュボードファブリックコントローラにアップロードすることができます。証明書に適したスイッチを選択できるように、証明書に適切な名前を付けてください。

1つの証明書と対応するキーファイルをアップロードすることも、複数の証明書とキーファイルを一括アップロードすることもできます。アップロードが完了したら、スイッチにインストールする前に、アップロードリストを確認することができます。組み込みキーファイルを含む証明書ファイルがアップロードされた場合、Nexusダッシュボードファブリックコントローラは自動的にキーを取得します。

証明書とキーファイルは同じファイル名である必要があります。たとえば、証明書ファイル名がmycert.pemの場合、キーファイル名はmycert.keyである必要があります。証明書とキーペアのファイル名が同じでない場合、Nexusダッシュボードファブリックコントローラはスイッチに証明書をインストールできません。

Cisco Nexusダッシュボードファブリックコントローラでは、スイッチに証明書を一括インストールできます。一括インストールでは同じパスワードが使用されるため、すべての暗号化キーは同じパスワードで暗号化する必要があります。キーのパスワードが異なる場合、証明書を一括モードでインストールすることはできません。一括モードインストールでは、暗号化されたキー証明書と暗号化されていないキー証明書を一緒にインストールできますが、すべての暗号化キーは同じパスワードを持つ必要があります。

スイッチに新しい証明書をインストールすると、既存の証明書が新しい証明書に置き換えられます。

同じ証明書を複数のスイッチにインストールすることができます。ただし、一括アップロード機能は使用できません。



- (注) Nexusダッシュボードファブリックコントローラは、提供される証明書またはオプションが有効であることを要求しません。この規則に従うかどうかは、ユーザーとスイッチの要件次第です。たとえば、スイッチ1のための証明書が生成されても、それがスイッチ2にインストールされた場合、Nexusダッシュボードファブリックコントローラは証明書の適用を強制しません。スイッチは、証明書のパラメータに基づいて証明書を受け入れるか、拒否するかを選択できます。

Cisco NexusダッシュボードファブリックコントローラによるNX-API証明書の検証

リリース12.0.1a以降、Cisco Nexusダッシュボードファブリックコントローラはスイッチによって提供されるNX-API証明書を検証する機能をサポートしています。Cisco Nexusダッシュボードファブリックコントローラが行うNX-APIリクエストにはSSL接続が必要です。ス

スイッチはSSLサーバーのように動作し、SSLネゴシエーションの一部としてサーバー証明書を提供します。対応するCA証明書が提供されている場合、Cisco Nexusダッシュボードファブリックコントローラはそれを確認できます。



- (注) デフォルトでは、NX-API 証明書の検証は有効にされていません。これは、データセンター内のすべてのスイッチにCA署名付き証明書がインストールされている必要があり、Cisco Nexusダッシュボードファブリックコントローラには対応するすべてのCA証明書が供給されるためです。

Cisco NexusダッシュボードファブリックコントローラのNX-API証明書管理には、同じ対象を管理するためのスイッチ証明書とCA証明書という2つの機能があります。

スイッチ証明書

証明書のアップロード

証明書をNexusダッシュボードファブリックコントローラにアップロードするには、次の手順を実行します。

1. **[証明書のアップロード (Upload Certificate)]** をクリックして、適切な証明書ファイルをアップロードします。
2. ローカルディレクトリを参照し、Nexusダッシュボードファブリックコントローラにアップロードする必要がある証明書キーペアを選択します。

拡張子が .cer/.crt/.pem および .key の証明書を個別に選択できます。

Cisco Nexusダッシュボードファブリックコントローラでは、埋め込みキーファイルを含む単一の証明書ファイルをアップロードすることもできます。キーファイルはアップロード後に自動的に取得されます。

3. **[アップロード (Upload)]** をクリックし、選択したファイルをNexusダッシュボードファブリックコントローラにアップロードします。

ファイルのアップロードに成功すると、そのことを知らせるメッセージが表示されます。アップロードされた証明書がテーブルに一覧表示されます。

テーブルには、ステータスが **UPLOADED** と表示されます。証明書がキーファイルなしでアップロードされた場合、ステータスは **KEY_MISSING** と表示されます。

スイッチの割り当てと証明書のインストール

Cisco Nexusダッシュボードファブリックコントローラ Web UIを使用してスイッチに証明書をインストールするには、次の手順を実行します。

1. 1つまたは複数の証明書のチェックボックスをオンにします。

2. **[アクション (Actions)]** ドロップダウンリストから、**[スイッチの割り当てとインストール (Assign Switch & Install)]** を選択します。
3. **[NX API 証明書クレデンシャル (NX API Certificate Credentials)]** フィールドに、証明書の生成時にキーを暗号化するために使用したパスワードを入力します。

[パスワード (Password)] フィールドは必須ですが、キーがパスワードを使用して暗号化されていない場合は、任意のランダムな文字列を入力できます（たとえば `test`、`install` など）。暗号化されていないファイルの場合、パスワードは使用されませんが、一括モードであるため、ランダムな文字列を入力する必要があります。



- (注) 1回の一括インストールで、暗号化されていないキーと暗号化されたキーおよび証明書をインストールできます。ただし、暗号化キーに使用するキーパスワードを指定する必要があります。

4. 証明書ごとに、**[割り当て (Assign)]** の矢印をクリックし、証明書に関連付けるスイッチを選択します。
5. **[証明書のインストール (Install Certificates)]** をクリックして、それぞれのスイッチにすべての証明書をインストールします。

証明書のリンク解除と削除

証明書をスイッチにインストールすると、NexusダッシュボードファブリックコントローラはNexusダッシュボードファブリックコントローラから証明書をアンインストールできません。ただし、スイッチにはいつでも新しい証明書をインストールできます。スイッチにインストールされていない証明書は削除できます。スイッチにインストールされている証明書を削除するには、スイッチから証明書のリンクを解除してから、Nexusダッシュボードファブリックコントローラから削除する必要があります。



- (注) スイッチから証明書のリンクを解除しても、スイッチの証明書は削除されません。証明書はまだスイッチに存在します。Cisco Nexusダッシュボードファブリックコントローラはスイッチの証明書を削除できません。

Nexusダッシュボードファブリックコントローラリポジトリから証明書を削除するには、次の手順を実行します。

1. 削除する必要がある証明書を選択します。
2. **[アクション (Actions)]** ドロップダウンリストから、**[リンク解除 (Unlink)]** を選択します。確認メッセージが表示されます。
3. **[OK]** をクリックして、選択した証明書をスイッチからリンク解除します。

ステータス カラムには [UPLOADED] と表示されます。[Switch] カラムには [NOT_INSTALLED] と表示されます。

4. [Switch] から、現在リンク解除されている証明書を選択します。
5. [アクション (Actions)] ドロップダウン リストから、[削除 (Delete)] を選択します。
証明書は Nexus ダッシュボード ファブリック コントローラ から削除されます。

CA 証明書

証明書のアップロード

証明書を Nexus ダッシュボード ファブリック コントローラ にアップロードするには、次の手順を実行します。

1. [証明書のアップロード (Upload Certificate)] をクリックして、適切なライセンス ファイルをアップロードします。
2. ローカルディレクトリを参照し、Nexus ダッシュボード ファブリック コントローラ にアップロードする証明書とキーのペアを選択します。

ファイル拡張子が .cer/.crt/.pem ファイル拡張子をもつ証明書を個別に選択できます。



(注) CA 証明書は公開証明書であり、キーは含まれません。また、この操作にはキーは必要ありません。これは、スイッチが提供する NX-API 証明書を確認するために Cisco Nexus ダッシュボード ファブリック コントローラ が必要とする証明書です。つまり、CA 証明書は Cisco Nexus ダッシュボード ファブリック コントローラ によってのみ使用され、スイッチにインストールされることはありません。

3. [アップロード (Upload)] をクリックし、選択したファイルを Nexus ダッシュボード ファブリック コントローラ にアップロードします。

ファイルのアップロードに成功すると、そのことを知らせるメッセージが表示されます。アップロードされた証明書がテーブルに一覧表示されます。

スイッチの割り当てと証明書のインストール

これらの CA 証明書は Cisco Nexus ダッシュボード ファブリック コントローラ によってのみ使用され、スイッチにインストールされることはありません。

証明書のリンク解除と削除

CA 証明書はスイッチにインストールされないため、リンク解除する必要はありません。

CA 証明書は、特定の CA に新しい証明書を持ち込む必要があるため、削除できます。

[アクション (Actions)] ドロップダウンリストから、[削除 (Delete)] を選択します。証明書は Nexus ダッシュボード ファブリック コントローラ から削除されます。

NX-API 証明書検証の有効化

NX-API 証明書の検証は、[CA 証明書] ページのトグル ボタンを使用して有効にできます。ただし、これは、Cisco Nexus ダッシュボード ファブリック コントローラ が管理するすべてのスイッチに CA 署名付き証明書がインストールされ、対応する CA ルート証明書 (1つ以上) が Cisco Nexus ダッシュボード ファブリック コントローラ にアップロードされた後にのみ行う必要があります。これを有効にすると、Cisco Nexus ダッシュボード ファブリック コントローラ SSL クライアントはスイッチによって提供される証明書の検証を開始します。検証に失敗すると、NX-API コールも失敗します。



- (注)
- NX-API 証明書の検証は、スイッチごとに適用できません。all または none のいずれかです。したがって、すべてのスイッチに対応する CA 署名付き証明書がインストールされている場合にのみ、検証を有効にすることが重要です。
 - また、すべての CA 証明書が Cisco Nexus ダッシュボード ファブリック コントローラ にインストールされている必要があります。
 - 検証の問題が原因で特定のスイッチで NX-API コールが失敗した場合は、トグル ボタンを使用して適用を無効にできます。すべての結果は、以前の状態に戻ります。
 - 上記の点から、メンテナンス期間中に適用を有効にする必要があります。

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。