



証明書

- [CA 署名済み証明書の保持, on page 1](#)
- [SAN Windows/Linux の証明書管理, on page 2](#)
- [SAN OVA/ISO の証明書管理 \(10 ページ\)](#)

CA 署名済み証明書の保持

アップグレード後に CA 署名付き SSL 証明書を保持する必要がある場合は、次の手順を実行します。

3 ノードフェデレーションセットアップを構成し、外部 CA 証明書を適用する場合は、次の手順を実行します。

1. フェデレーションの DCNM サーバを停止します。
 - Windows の場合 : C:\Program Files\cisco 各 Systems\dcm\dcnm\bin に移動します。StopLANSANServer.bat をダブルクリックして、サービスを停止します。
 - Linux の場合 : /root へのログオンします。/root/Stop_DCNM_Servers コマンドを使用して、サービスを停止します。
2. プライマリ サーバの CA 証明書を生成し、同じ CA 証明書を 3 つのセカンダリ サーバに適用します。
3. 最初にプライマリ サーバを起動し、次にフェデレーションでセカンダリ サーバを起動します。

キーストアのパスワードまたはエイリアスを変更する場合は、次の場所にある **standalone-san** ドキュメントで更新する必要があることに注意してください。

```
< DCNM_install_root >  
\dcm\wildfly-14.0.1.Final\standalone\configuration\standalone-san.xml
```

keystore タグとエイリアスのパスワードを更新します。

```
<keystore key-password>="<<storepass-pwd>> key-alias="updated-key-alias"
keystore-password="updated-password"
path="<DCNM_install_root>\dcm\wildfly-14.0.1.Final\standalone\configuration\fmserver.jks">
```



Note <<storepass-pwd>> は、DCNM サーバのインストール時に生成されるパスワード文字列です。この文字列は <install_dir>/dcm/fm/conf/serverstore.properties ディレクトリにあります。storepass-pwd の dcnm.fmserver.token 値を取得します。

Procedure

ステップ 1 次の場所から署名付き証明書をバックアップします。

- Windows の場合 :
`<DCNM_install_root>\dcm\wildfly-14.0.1.Final\standalone\configuration\fmserver.jks`
- Linux の場合 :
`<DCNM_install_root>/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks`

ステップ 2 Cisco DCNM リリース 11.5(1) にアップグレードします。

ステップ 3 アップグレード後、Cisco DCNM のアップグレードされたバージョンと同じ場所に証明書をコピーします。

Note [ステップ 1, on page 2](#) に記載されているのと同じ場所に証明書をロードする必要があります。

ステップ 4 DCNM サービスを再起動します。

SAN Windows/Linux の証明書管理

ここでは、Cisco DCNM で証明書を設定する 3 つの方法について説明します。

キーストアのパスワードまたはエイリアスを変更する場合は、次の場所にある **standalone-san** ドキュメントで更新する必要があることに注意してください。

```
< DCNM_install_root >
\dcm\wildfly-14.0.1.Final\standalone\configuration\standalone-san.xml
```

keystore タグのパスワードと **key-alias** タグのエイリアスを次のように更新します。

```
<keystore key-password>="<<storepass-pwd>> key-alias="updated-key-alias"
keystore-password="updated-password"
path="<DCNM_install_root>\dcm\wildfly-14.0.1.Final\standalone\configuration\fmserver.jks">
```



Note <<storepass-pwd>>は、DCNM サーバのインストール時に生成されるパスワード文字列です。この文字列は <install dir>/dcm/fm/conf/serverstore.properties ディレクトリにあります。storepass-pwd の dcm.fmserver.token 値を取得します。

ここでは、次の内容について説明します。

自己署名 SSL 証明書の使用

Procedure

ステップ 1 DCNM サービスを停止します。

ステップ 2 次の場所にあるキーストアの名前を変更します

```
< DCNM_install_root >  
\dcm\wildfly-14.0.1.Final\standalone\configuration\fmserver.jks
```

～

```
< DCNM_install_root >  
\dcm\wildfly-14.0.1.Final\standalone\configuration\fmserver.jks.old
```

ステップ 3 コマンドプロンプトから <DCNM install root>\dcm\java\jre1.8\bin\ に移動します。

```
<DCNM install root>\dcm\java\jdk11\bin\
```

ステップ 4 次のコマンドを使用して、自己署名証明書を生成します。

```
keytool -genkey -trustcacerts -keyalg RSA -sigalg SHA256withRSA -alias sme -keystore  
<DCNM_install_root>\dcm\wildfly-10.1.0.Final\standalone\configuration\fmserver.jks -storepass  
<<storepass-pwd>> -validity 360 -keysize 2048
```

Note <<storepass-pwd>>は、DCNM サーバのインストール時に生成されるパスワード文字列です。この文字列は <install dir>/dcm/fm/conf/serverstore.properties ディレクトリにあります。storepass-pwd の dcm.fmserver.token 値を取得します。

ステップ 5 DCNM サービスを開始します。

Windows でキーツールを使用して証明書要求が生成される場合 SSL 証明書を使用する

Procedure

ステップ 1 DCNM サービスを停止します。

ステップ 2 次の場所にあるキーストアの名前を変更します

```
< DCNM_install_root >
\dcm\wildfly-14.0.1.Final\standalone\configuration\fmserver.jks
~
```

```
< DCNM_install_root >
\dcm\wildfly-14.0.1.Final\standalone\configuration\fmserver.jks.old
```

ステップ 3 コマンドプロンプトから <DCNM install root>\dcm\java\jre1.8\bin\ に移動します。
<DCNM install root>\dcm\java\jdk11\bin\

ステップ 4 次のコマンドを使用して、DCNM キーストアで公開秘密キーペアを生成します。

```
keytool -genkey -keyalg RSA -sigalg SHA256withRSA -alias sme -keystore
"<DCNM_install_root>\dcm\wildfly-14.0.1.Final\standalone\configuration\fmserver.jks" -storepass
<<storepass-pwd>> -validity 360 -keysize 2048
```

Note <<storepass-pwd>> は、DCNM サーバのインストール時に生成されるパスワード文字列です。この文字列は <install dir>/dcm/fm/conf/serverstore.properties ディレクトリにあります。
storepass-pwd の dcm.fmserver.token 値を取得します。

ステップ 5 [ステップ 4, on page 4](#) で生成された公開キーから証明書署名要求 (CSR) を生成します。

```
keytool -certreq -alias sme -file dcm.csr -keystore "<DCNM install
root>\dcm\wildfly-14.0.1.Final\standalone\configuration\fmserver.jks" -storepass <<storepass-pwd>>
```

Note <<storepass-pwd>> は、DCNM サーバのインストール時に生成されるパスワード文字列です。この文字列は <install dir>/dcm/fm/conf/serverstore.properties ディレクトリにあります。
storepass-pwd の dcm.fmserver.token 値を取得します。

Note dcm csr ファイルは、/usr/local/cisco/dcm/java/jdk11/bin にあるキーツールディレクトリに作成されます。

ステップ 6 CSR を CA に送信し、Base-64 形式で署名付き証明書チェーンをダウンロードします。これにより、.p7b ファイルが作成されます。

CA は、証明書と署名証明書を PKCS 7 形式 (.p7b ファイル) または PEM (.pem) ファイルの証明書チェーンとして提供することがあります。CA が提供した PKCS7 形式の場合は、[ステップ 7, on page 5](#) に移動して PEM 形式に変換します。CA が PEM 形式を提供した場合は、[ステップ 8, on page 5](#) に進みます。

ステップ 7 Openssl を使用して、PKCS 7 証明書チェーンを X509 証明書チェーンに変換します。

```
openssl pkcs7 -print_certs -in cert-chain.p7b -out cert-chain.pem
```

Note 上記のコマンドで、ユーザーが cert-chain.p7b の正しい場所への絶対パスまたは相対パスのいずれかを提供していることを確認します。

ステップ 8 次の手順に従って、最初に中間証明書をインポートし、次に root 証明書をインポートし、署名付き証明書を最後にインポートします。

```
keytool -importcert -trustcacerts -file cert-chain.pem -keystore  
"<DCNM_install_root>\dcm\wildfly-14.0.1.Final\standalone\configuration\fmserver.jks" -storepass  
<<storepass-pwd>> -alias sme
```

Note <<storepass-pwd>> は、DCNM サーバのインストール時に生成されるパスワード文字列です。この文字列は <install dir>/dcm/fm/conf/serverstore.properties ディレクトリにあります。storepass-pwd の dcm.fmserver.token 値を取得します。

Note 上記のコマンドで、ユーザーが cert-chain.pem ファイルの正しい場所への絶対パスまたは相対パスのいずれかを提供していることを確認します。

ステップ 9 プライマリ サーバから次のコマンドを使用して、フェデレーション セットアップの各サーバのストアを作成します。

```
keytool -importkeystore -srckeystore  
/usr/local/cisco/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks -srckeypass  
<<storepass-pwd of primary>> -srcstorepass <<storepass-pwd of primary>> -srcstoretype JKS  
-destkeystore /usr/local/cisco/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver2.jks  
-destkeypass <<storepass-pwd-of-federation-server>> -deststorepass  
<<storepass-pwd-of-federation-server>> -deststoretype JKS -alias sme
```

Note <<storepass-pwd>> は、DCNM サーバのインストール時に生成されるパスワード文字列です。この文字列は <install dir>/dcm/fm/conf/serverstore.properties ディレクトリにあります。storepass-pwd の dcm.fmserver.token 値を取得します。

ステップ 10 新しい fmserver2.jks をフェデレーション サーバにフェデレーション サーバの /usr/local/cisco/dcm/wildfly-14.0.1.Final/standalone/configuration ディレクトリに fmserver.jks として送ります。

ステップ 11 フェデレーション設定のすべてのサーバで、ステップ [ステップ 9, on page 5](#) と [ステップ 10, on page 5](#) を繰り返します。

ステップ 12 DCNM サービスを開始します。

フェデレーション設定で、プライマリ サーバ、2 番目のサーバ、3 番目のサーバを順番に起動します。

ステップ 13 SAN クライアントの起動を有効にするために、フェデレーション設定の 2 番目と 3 番目のサーバの両方に /usr/local/cisco/dcm/fm/lib/fm/fmtrust.jks にある server1 の fmtrust.jks をコピーします。

詳細な手順については、[SAN クライアントおよびデバイス マネージャの起動](#) を参照してください。

Linux でキーツールを使用して証明書要求が生成されたときに SSL 証明書を使用する

Procedure

ステップ 1 `appmgr stop dcnm` コマンドを使用して、DCNM サービスまたは DCNM アプリケーションを停止します。

ステップ 2 次の場所にあるキーストアの名前を変更します。

```
< DCNM_install_root
>/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks
```

目的

```
< DCNM_install_root
>/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks.old
```

ステップ 3 コマンドプロンプトから、適切なフォルダに移動します。

```
<DCNM install root>/dcm/java/jdk11/bin/
```

ステップ 4 次のコマンドを使用して、DCNM キーストアで公開秘密キーペアを生成します。

```
./keytool -genkey -keyalg RSA -sigalg SHA256withRSA -alias sme -keystore
<DCNM_install_root>/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks -storepass
<<storepass-pwd>> -validity 360 -keysize 2048
```

Note <<storepass-pwd>> は、DCNM サーバのインストール時に生成されるパスワード文字列です。この文字列は <install dir>/dcm/fm/conf/serverstore.properties ディレクトリにあります。storepass-pwd の `dcnm.fmserver.token` 値を取得します。

ステップ 5 [ステップ 4, on page 6](#) で生成されている公開キーから、証明書署名要求 (CSR) を生成します。

```
./keytool -certreq -alias sme -file dcnm.csr -keystore "<DCNM install
root>/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks" -storepass <<storepass-pwd>>
```

Note <<storepass-pwd>> は、DCNM サーバのインストール時に生成されるパスワード文字列です。この文字列は <install dir>/dcm/fm/conf/serverstore.properties ディレクトリにあります。storepass-pwd の `dcnm.fmserver.token` 値を取得します。

Note `dcnm csr` ファイルは、`/usr/local/cisco/dcm/java/jdk11/bin` にあるキーツールディレクトリに作成されます。

- ステップ 6** CSR を CA に送信し、Base-64 形式で署名付き証明書チェーンをダウンロードします。これにより、.p7b ファイルが作成されます。
- CA は、証明書と署名証明書を PKCS 7 形式 (.p7b ファイル) または PEM (.pem) ファイルの証明書チェーンとして提供することがあります。PKCS 7 形式で CA が証明書チェーンを提供した場合は、[ステップ 7, on page 7](#) に移動して PEM 形式に変換します。PEM 形式で CA が証明書チェーンを提供した場合、[ステップ 8, on page 7](#) に移動します。
- ステップ 7** OpenSSL を使用して、PKCS 7 証明書チェーンを X509 証明書チェーンに変換します。
- ```
openssl pkcs7 -print_certs -in cert-chain.p7b -out cert-chain.pem
```
- Note** 上記のコマンドで、ユーザーが cert-chain.p7b の正しい場所への絶対パスまたは相対パスのいずれかを提供していることを確認します。
- ステップ 8** 次の手順に従って、最初に中間証明書をインポートし、次に root 証明書をインポートし、署名付き証明書を最後にインポートします。
- ```
./keytool -importcert -trustcacerts -file cert-chain.pem -keystore  
<DCNM_install_root>/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks -storepass  
<<storepass-pwd>> -alias sme
```
- Note** <<storepass-pwd>> は、DCNM サーバのインストール時に生成されるパスワード文字列です。この文字列は <install_dir>/dcm/fm/conf/serverstore.properties ディレクトリにあります。**storepass-pwd** の **dcnm.fmserver.token** 値を取得します。
- Note** 上記のコマンドで、ユーザーが cert-chain.pem ファイルの正しい場所への絶対パスまたは相対パスのいずれかを提供していることを確認します。
- ステップ 9** プライマリ サーバから次のコマンドを使用して、フェデレーションセットアップで各サーバのストアを作成します。
- ```
keytool -importkeystore -srckeystore
/usr/local/cisco/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks -srckeypass
<<storepass-pwd of primary>> -srcstorepass <<storepass-pwd of primary>> -srcstoretype JKS
-destkeystore /usr/local/cisco/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver2.jks
-destkeypass <<storepass-pwd-of-federation-server>> -deststorepass
<<storepass-pwd-of-federation-server>> -deststoretype JKS -alias sme
```
- ステップ 10** 新しい fmserver2.jks をフェデレーション サーバにフェデレーション サーバの `/usr/local/cisco/dcm/wildfly-14.0.1.Final/standalone/configuration` ディレクトリに **fmserver.jks** として送ります。
- ステップ 11** フェデレーション設定のすべてのサーバで、[ステップ 9, on page 7](#) と [ステップ 10, on page 7](#) を繰り返します。
- ステップ 12** SAN クライアントの起動を有効にするために、フェデレーション設定の 2 番目と 3 番目のサーバの両方に `/usr/local/cisco/dcm/fm/lib/fm/fmtrust.jks` にある server1 の **fmtrust.jks** をコピーします。
- 詳細な手順については、[SAN クライアントおよびデバイス マネージャの起動](#) を参照してください。

ステップ 13 DCNM サービスを開始します。

フェデレーション設定で、プライマリ サーバ、2 番目のサーバ、3 番目のサーバを順番に起動します。

## Linux で OpenSSL を使用して証明書要求が生成される場合 SSL 証明書を使用する

Open SSL を使用して生成された証明書要求を使用して Cisco DCNM で SSL 証明書を設定するには、次の手順を実行します。

### Procedure

ステップ 1 **appmgr stop dcnm** コマンドを使用して、DCNM サービスまたは DCNM アプリケーションを停止します。

ステップ 2 次の場所にあるキーストアの名前を変更します。

```
< DCNM_install_root
>/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks
~
```

```
< DCNM_install_root
>/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks.old
```

ステップ 3 コマンドプロンプトから `<DCNM install root>/dcm/java/jdk11/bin/` に移動します。

ステップ 4 OpenSSL を使用して RSA 秘密キーを生成します。

```
openssl genrsa -out dcnm.key 2048
```

ステップ 5 次のコマンドを使用して、自己署名証明書 (CSR) を生成します。

```
openssl req -new -key dcnm.key -sha256 -out dcnm.csr
```

ステップ 6 CSR を証明書認定機関に送信し、Base-64 形式で署名付き証明書チェーンをダウンロードします。これにより、**.p7b** ファイルが作成されます。

CA は、証明書と署名証明書を PKCS 7 形式 (.p7b ファイル) または PEM (.pem) ファイルの証明書チェーンとして提供することがあります。CA が PKCS 7 形式を提供している場合は、[ステップ 7, on page 8](#) に移動して PEM 形式に変換します。CA が PEM 形式を提供している場合は、[ステップ 8, on page 8](#) に進みます。

ステップ 7 PKCS 7 証明書チェーンを X509 証明書チェーンに変換します。

```
openssl pkcs7 -print_certs -in cert-chain.p7b -out cert-chain.pem
```

ステップ 8 X509 証明書チェーンと秘密キーを PKCS 12 形式に変換します。

```
openssl pkcs12 -export -in cert-chain.pem -inkey dcnm.key -out dcnm.p12 -password pass
<<storepass-kwd>> -name sme
```



**Note** <<storepass-pwd>>は、DCNM サーバのインストール時に生成されるパスワード文字列です。この文字列は <install dir>/dcm/fm/conf/serverstore.properties ディレクトリにあります。**storepass-pwd** の **dcm.fmserver.token** 値を取得します。

**Note** 上記のコマンドで **dcm.key** および **dcm.p12** ファイルの正しい場所に、ユーザーが絶対パスまたは相対パスのどちらかを提供するようにします。

**ステップ 9** 中間証明書、root 証明書、および署名付き証明書を同じ順序でインポートします。

```
./keytool -importkeystore -srckeystore dcm.p12 -srcstoretype PKCS12 -destkeystore <DCNM_install_root>/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks -deststoretype JKS -alias sme -srcstorepass <<storepass-pwd>> -deststorepass <<storepass-pwd>>
```

**Note** <<storepass-pwd>>は、DCNM サーバのインストール時に生成されるパスワード文字列です。この文字列は <install dir>/dcm/fm/conf/serverstore.properties ディレクトリにあります。**storepass-pwd** の **dcm.fmserver.token** 値を取得します。

**Note** 上記のコマンドで、**cert-chain.pem**、**dcm.key**、および **dcm.p12** の正しい場所に対して絶対パスまたは相対パスを提供していることを確認します。

**ステップ 10** プライマリ サーバから次のコマンドを使用して、フェデレーションセットアップで各サーバのストアを作成します。

```
keytool -importkeystore -srckeystore /usr/local/cisco/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks -srckeypass <<storepass-pwd of primary>> -srcstorepass <<storepass-pwd of primary>> -srcstoretype JKS -destkeystore /usr/local/cisco/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver2.jks -destkeypass <<storepass-pwd-of-federation-server>> -deststorepass <<storepass-pwd-of-federation-server>> -deststoretype JKS -alias sme
```

**ステップ 11** 新しい **fmserver2.jks** をフェデレーションサーバにフェデレーションサーバの **/usr/local/cisco/dcm/wildfly-14.0.1.Final/standalone/configuration** ディレクトリに **fmserver.jks** として送ります。

**ステップ 12** フェデレーション設定のすべてのサーバで、ステップ [ステップ 10, on page 9](#) と [ステップ 11, on page 9](#) を繰り返します。

**ステップ 13** DCNM サービスを開始します。

フェデレーション設定で、プライマリサーバ、2番目のサーバ、3番目のサーバを順番に起動します。

**ステップ 14** SAN クライアントの起動を有効にするために、フェデレーション設定の2番目と3番目のサーバの両方に **/usr/local/cisco/dcm/fm/lib/fm/fmtrust.jks** にある **server1** の **fmtrust.jks** をコピーします。

詳細な手順については、[SAN クライアントおよびデバイス マネージャの起動](#) を参照してください。

## SAN OVA/ISO の証明書管理



(注) このセクションでは、DCNM OVA/ISO の展開にのみ適用されます。

リリース 11.2(1) 以降、Cisco DCNM では新しい方法と新しい CLI で、システム上で証明書のインストール、アップグレード後の復元、検証が可能です。



(注) リリース 11.3(1) 以降では、証明書の管理に **sysadmin** ロールを使用する必要があります。

Cisco DCNM は、次の 2 つの証明書を保存します。

- 自己署名証明書 (Cisco DCNM サーバとさまざまなアプリケーション間の内部通信用)
- Web UI などの外部世界と通信するための CA (認証局) 署名付き証明書。



(注) CA 署名付き証明書をインストールするまで、Cisco DCNM は外部ネットワークと通信するため自己署名証明書を保持します。

## 証明書管理のベスト プラクティス

Cisco DCNM での証明書管理のガイドラインとベスト プラクティスを次に示します。

- Cisco DCNM は、証明書を表示、インストール、復元、およびエクスポートまたはインポートするための CLI ベースのユーティリティを提供します。これらの CLI は SSH コンソールから使用でき、**sysadmin** ユーザーのみがこれらのタスクを実行できます。
- Cisco DCNM をインストールするとき、デフォルトで自己署名付き証明書がインストールされています。この証明書は、外部との通信に使用されます。Cisco DCNM のインストール後に、CA 署名付き証明書をシステムにインストールする必要があります。
- CN (共通名) を使用して Cisco DCNM で CSR を生成します。CN として VIP FQDN (仮想 IP アドレス FQDN) を指定して、CA 署名付き証明書をインストールします。FQDN は、Cisco DCNM Web UI にアクセスするために使用される管理サブネット VIP (eth0 の VIP) インターフェイスの完全修飾ドメイン名です。
- Cisco DCNM をアップグレードする前に CA 署名付き証明書がインストールされている場合は、Cisco DCNM をアップグレードした後に、CA 署名付き証明書を復元する必要があります。



- (注) インラインアップグレードまたはバックアップと復元を実行する場合は、証明書のバックアップを取得する必要はありません。

## インストールされた証明書の表示

次のコマンドを使用して、インストールされた証明書の詳細を表示できます。

### appmgr afw show-cert-details

**appmgr afw show-cert-details** コマンドの次のサンプル出力では、**CERTIFICATE 1** は外部ネットワークおよび Web ブラウザに提供されている証明書を示します。**CEERTIFICATE 2** は内部で使用されている証明書を示します。

```
dcnm# appmgr afw show-cert-details
```

```
****CERTIFICATE 1****
[Certificate available to web gateway. This certificate is offered to webclients]:
-----Web gateway certificate-----
Certificate:
 Data:
 Version: 3 (0x2)
 Serial Number: 4202 (0x106a)
 Signature Algorithm: sha256WithRSAEncryption
 Issuer: C=IN, ST=KA, L=BGL, O=xyz, OU=ABC, CN=<FQDN/IP>
 Validity
 Not Before: Jun 4 13:55:25 2019 GMT
 Not After : Jun 3 13:55:25 2020 GMT
 Subject: C=IN, ST=KA9, L=BGL9, O=XYZ123, OU=ABC123, CN=<FQDN/IP>
 Subject Public Key Info:
 Public Key Algorithm: rsaEncryption
 Public-Key: (2048 bit)
 Modulus:
 00:bb:52:1e:7f:24:d7:2e:24:62:5a:83:cc:e4:88:
-----Certificate output is truncated to first 15 lines-----

****CERTIFICATE 2****
[Certificate available in keystore(jks). CA signed certificate is installed here till
DCNM version 11.1.x]
If you have upgraded from DCNM version 11.1.x to later version please see installation
guide to restore
CA signed certificate to upgraded version.
-----Keystore certificate-----
alias = sme, storepass = <<storepass-pwd>>
Alias name: sme
Creation date: Oct 14, 2018
Entry type: PrivateKeyEntry
Certificate chain length: 2
Certificate[1]:
Owner: CN=localhost, OU=Data Center, O=Cisco Systems Inc, L=San Jose, ST=CA, C=US
Issuer: CN=dcnmca, OU=Data Center, O=Cisco Systems Inc, L=San Jose, ST=CA, C=US
Serial number: 62044620
Valid from: Sun Oct 14 20:39:39 PDT 2018 until: Fri Oct 13 20:39:39 PDT 2023
Certificate fingerprints:
 MD5: E5:F8:AD:17:4D:43:2A:C9:EE:35:5F:BE:D8:22:7D:9C
 SHA1: 38:66:F1:CD:10:61:27:E7:43:85:10:41:3D:A3:4B:5C:C9:CC:17:5E
 SHA256:
E0:87:D8:34:71:18:FE:8C:AB:18:0B:D7:85:B1:91:A8:4B:75:A3:91:BA:90:83:46:72:87:FE:FE:FE:04:F0:E1
```

```
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 2048-bit RSA key
-----Certificate output is truncated to first 15 lines-----
dcnm#
```



- (注) <<storepass-pwd>> は、DCNM サーバのインストール時に生成されるパスワード文字列です。この文字列は <install dir>/dcm/fm/conf/serverstore.properties ディレクトリにあります。storepass-pwd の dcnm.fmserver.token 値を取得します。

インストール後、Web UI は **CERTIFICATE 1** を参照します。**CERTIFICATE 1** が利用できない場合、次のコマンドを使用して、すべてのアプリケーションを停止し再起動する必要があります。



- (注) Cisco DCNM で同じ一連のコマンドに従い、このシナリオをトラブルシューティングするようにしてください。

Cisco DCNM スタンドアロンアプライアンスで、次のコマンドを実行して、すべてのアプリケーションを停止および開始し、**CERTIFICATE 1** をトラブルシューティングします。

```
dcnm# appmgr stop all /* stop all the applications running on Cisco DCNM */
dcnm# appmgr start all /* start all the applications running on Cisco DCNM */
```

## CA 署名付き証明書のインストール

標準のセキュリティ慣行として CA 署名付き証明書をインストールすることをお勧めします。CA 署名付き証明書が認識され、ブラウザによって検証されます。CA 署名付き証明書を手動で検証することもできます。



- (注) 認証局は、企業の署名機関でもかまいません。

## Cisco DCNM スタンドアロン セットアップで CA 署名済み証明書をインストールする

Cisco DCNM に CA 署名付き証明書をインストールするには、次の手順を実行します。

### Procedure

**ステップ 1** SSH 端末を経由して DCNM サーバにログオンします。

**ステップ 2** `appmgr afw gen-csr` コマンドを使用して、CISCO DCNM サーバで CSR を生成します。

**Note** CSR は Cisco DCNM に固有のものであり、対応する CSR 署名付き証明書のみが所定の Cisco DCNM にインストールされている必要があります。

```

dcnm# appmgr afw gen-csr
Generating CSR....
..
...

Country Name (2 letter code) [XX]:US
State or Province Name (full name) []:CA
Locality Name (eg, city) [Default City]:San Jose
Organization Name (eg, company) [Default Company Ltd]:Cisco
Organizational Unit Name (eg, section) []:DCBG
Common Name (eg, your name or your server's hostname) []:dcnmhost.cisco.com
Email Address []:dcnm@cisco.com

Please enter the following 'extra' attributes to be sent with your certificate request
A challenge password []: /* This field is not mandatory */
An optional company name []: /* This field is not mandatory */
...

CSR ファイル dcnmweb.csr が /var/tmp/ ディレクトリに作成されます。

***** CA certificate installation not completed yet. Please do followings. *****
CSR is generated and placed at /var/tmp/dcnmweb.csr.
Please download or copy the content to your certificate signing server.

```

**ステップ 3** この CSR を証明書署名サーバに送信します。

**Note** CA 署名サーバは、組織に対してローカルです。

**ステップ 4** 認証局によって署名された証明書を取得します。

認証局 (CA) は、プライマリ、中間 (Issuing/Subordinate) 証明書、およびルート証明書の 3 つの証明書を返します。3 つの証明書すべてを `one.pem` ファイルに結合し、DCNM にインポートします。

**ステップ 5** 新しい CA 署名付き証明書を Cisco DCNM サーバにコピーします。

証明書が Cisco DCNM サーバの `/var/tmp` ディレクトリにあることを確認します。

**ステップ 6** 次のコマンドを使用して、Cisco DCNM に CA 署名付き証明書をインストールします。

**Note** 以下に示すように、同じ順序で次のコマンドを実行することを推奨します。

```

dcnm# appmgr stop all /* Stop all applications running on Cisco DCNM
dcnm# appmgr afw install-CA-signed-cert <CA-signed certificate directory>
/* CA-signed certificate with full or relative path */
Making the signed certificate available to web gateway....

CA signed certificate CA-signed-cert.pem is installed. Please start all applications as
followings:
On standalone setup execute: 'appmgr start all'

```

**ステップ 7** `appmgr start all` コマンドを使用して、Cisco DCNM で新しい証明書ですべてのアプリケーションを再起動します。

```
dcnm# appmgr start all
```

**ステップ 8** `appmgr afw show-cert-details` コマンドを使用して、新しくインストールした CA 署名証明書を確認します。

システムは、CA 証明書を用意しており、ブラウザで確認できます。

**Note** CSR は Cisco DCNM に固有のものであり、対応する CSR 署名付き証明書のみが所定の Cisco DCNM にインストールされている必要があります。

## アップグレード後に証明書を復元する

このメカニズムは、インラインアップグレードプロセスのみを使用した Cisco DCNM アップグレード手順に適用されます。この手順は、同じバージョンの Cisco DCNM アプライアンスでのデータのバックアップと復元には必要ありません。

証明書の復元は破壊的なメカニズムであることに注意してください。アプリケーションを停止して再起動する必要があります。復元は、アップグレードされたシステムが安定している際のみ実行する必要があります。つまり、Cisco DCNM Web UI にログインできる必要があります。Cisco DCNM ネイティブ HA セットアップでは、アクティブ ノードとスタンバイ ノードの両方でピア関係が確立されている必要があります。



(注) 証明書は、次の状況でのみ復元する必要があります。

- アップグレード前に CA 署名付き証明書がシステムにインストールされている場合。
- 11.2(1) より前のバージョンからバージョン 11.2(1) 以降にアップグレードしている場合。

Cisco DCNM をアップグレードした後は、復元する前に **CERTIFICATE 1** が CA 署名付き証明書であるか必ず証明書を確認する必要があります。それ以外の場合は、証明書を復元する必要があります。

次のサンプル出力に示すように、**appmgr afw show-cert-details** を使用して証明書を確認します。

```
dcnm# appmgr afw show-cert-details
****CERTIFICATE 1****
[Certificate available to web gateway. This certificate is offered to webclients]:
-----Web gateway certificate-----
Certificate:
 Data:
 Version: 3 (0x2)
 Serial Number: 1575924977762797464 (0x15decf6aec378798)
 Signature Algorithm: sha256WithRSAEncryption
 Issuer: C=US, ST=CA, L=San Jose, O=Enterprise CA inc, OU=Data Center,
 CN=dcnm1.ca.com
 Validity
 Not Before: Dec 9 20:56:17 2019 GMT
 Not After : Dec 9 20:56:17 2024 GMT
 Subject: C=US, ST=CA, L=San Jose, O= Enterprise CA inc, OU=Data Center,
 CN=dcnm1.ca.com
 Subject Public Key Info:
 Public Key Algorithm: rsaEncryption
 Public-Key: (2048 bit)
 Modulus:
 00:cf:6e:cd:c6:a9:30:08:df:92:98:38:49:9c:2a:
-----Certificate output is truncated to first 15 lines-----
```

```
****CERTIFICATE 2****
[Certificate available in keystore(jks). CA signed certificate is installed here till
DCNM version 11.1.x]
If you have upgraded from DCNM version 11.1.x to later version please see installation
guide to restore
CA signed certificate to upgraded version.
-----Keystore certificate-----
Alias name: sme
Creation date: Oct 14, 2018
Entry type: PrivateKeyEntry
Certificate chain length: 2
Certificate[1]:
Owner: CN=localhost, OU=Data Center, O=Cisco Systems Inc, L=San Jose, ST=CA, C=US
Issuer: CN=dcnmca, OU=Data Center, O=Cisco Systems Inc, L=San Jose, ST=CA, C=US
Serial number: 62044620
Valid from: Sun Oct 14 20:39:39 PDT 2018 until: Fri Oct 13 20:39:39 PDT 2023
Certificate fingerprints:
 SHA1: 38:66:F1:CD:10:61:27:E7:43:85:10:41:3D:A3:4B:5C:C9:CC:17:5E
 SHA256:
E0:87:D8:34:71:18:FE:8C:AB:18:0B:D7:85:B1:91:A8:4B:75:A3:91:BA:90:83:46:72:87:FE:FE:FE:04:F0:E1
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 3
-----Certificate output is truncated to first 15 lines-----
dcnm#
```

## アップグレード後に Cisco DCNM スタンドアロン セットアップで証明書を復元する

Cisco DCNM スタンドアロン展開をリリース にアップグレードした後に証明書を復元するには、次の手順を実行します。

### Procedure

- ステップ 1 Note** リリース にアップグレードすると、CA 署名付き証明書のバックアップが作成されます。
- Cisco DCNM スタンドアロンアプライアンスが正常にアップグレードされたら、SSH を使用して DCNM サーバにログインします。
- ステップ 2** 次のコマンドを使用して、すべてのアプリケーションを停止します。
- ```
appmgr stop all
```
- ステップ 3** 次のコマンドを使用して、証明書を復元します。

```
appmgr afw restore-CA-signed-cert
```

ステップ 4 [はい (yes)] と入力し、以前インストールした証明書を復元することを確認します。

ステップ 5 次のコマンドを使用して、すべてのアプリケーションを開始します。

```
appmgr start all
```

ステップ 6 **appmgr afw show-cert-details** コマンドを使用して、新しくインストールした CA 署名証明書を

確認します。

システムは、CA 証明書を用意しており、ブラウザで確認できます。

以前にインストールされた CA 署名付き証明書の回復と復元

CA 署名付き証明書のインストール、復元、管理は、サードパーティの署名サーバが関係しているため、時間がかかるプロセスです。これにより、誤った証明書をインストールすることとなるミスが生じる場合があります。このようなシナリオでは、最新のインストールまたはアップグレードの前にインストールされた証明書を復元することをお勧めします。

以前にインストールされた CA 署名付き証明書を回復して復元するには、次の手順を実行します。

手順

ステップ 1 SSH 端末を経由して DCNM サーバにログオンします。

ステップ 2 /var/lib/dcnm/afw/apigateway/ ディレクトリに移動します。

```
dcnm# cd /var/lib/dcnm/afw/apigateway/
dcnm# ls -ltr /* View the contents of the folder
total 128
-rw----- 1 root root 1844 Nov 18 13:14 dcnmweb.key.2019-11-20T132939-08:00
-rw-r--r-- 1 root root 1532 Nov 18 13:14 dcnmweb.crt.2019-11-20T132939-08:00
-rw----- 1 root root 1844 Nov 20 10:15 dcnmweb.key.2019-11-20T132950-08:00
-rw-r--r-- 1 root root 1532 Nov 20 10:15 dcnmweb.crt.2019-11-20T132950-08:00
-rw----- 1 root root 1844 Dec 22 13:59 dcnmweb.key
-rw-r--r-- 1 root root 1532 Dec 22 13:59 dcnmweb.crt
.
..
...
```

dcnmweb と **dcnmweb** は、現在、システムにインストールされているキーと証明書ファイルです。同様のファイル名は、タイムスタンプサフィックスを使用して、最近のアップグレードまたは復元の前にインストールされているキーと証明書のペアを識別するのに役立ちます。

ステップ 3 **appmgr stop all** コマンドを使用して、Cisco DCNM 上で実行されているすべてのアプリケーションを停止します。

ステップ 4 **dcnmweb.key** および **dcnmweb.crt** ファイルのバックアップをとります。

ステップ 5 復元する古いキーと証明書のペアを特定します。

ステップ 6 キーと証明書のペアを **dcnmweb.key** および **dcnmweb.crt** として (タイムスタンプ サフィックスなしで) コピーします。

ステップ 7 **appmgr start all** コマンドを使用して、Cisco DCNM 上で実行されているすべてのアプリケーションを開始します。

ステップ 8 **appmgr afw show-cert-details** コマンドを使用して、証明書の詳細を確認します。CERTIFICATE 1 は CA 署名付き証明書です。

- (注) CA 署名付き証明書が Cisco DCNM Web UI に表示されない場合、または DCNM サーバがエラーメッセージを送信した場合は、システムを再起動する必要があります。

インストールした証明書の確認



`appmgr afw show-cert-details` コマンドを使用してインストールした証明書を確認でき、Web ブラウザによって証明書が有効か否か確認します。Cisco DCNM はすべての標準ブラウザ (Chrome、IE、Safari、Firefox) をサポートします。しかし、各ブラウザでは証明書情報が異なって表示されます。

ブラウザのプロバイダ Web サイトで、ブラウザの固有情報を参照することをお勧めします。

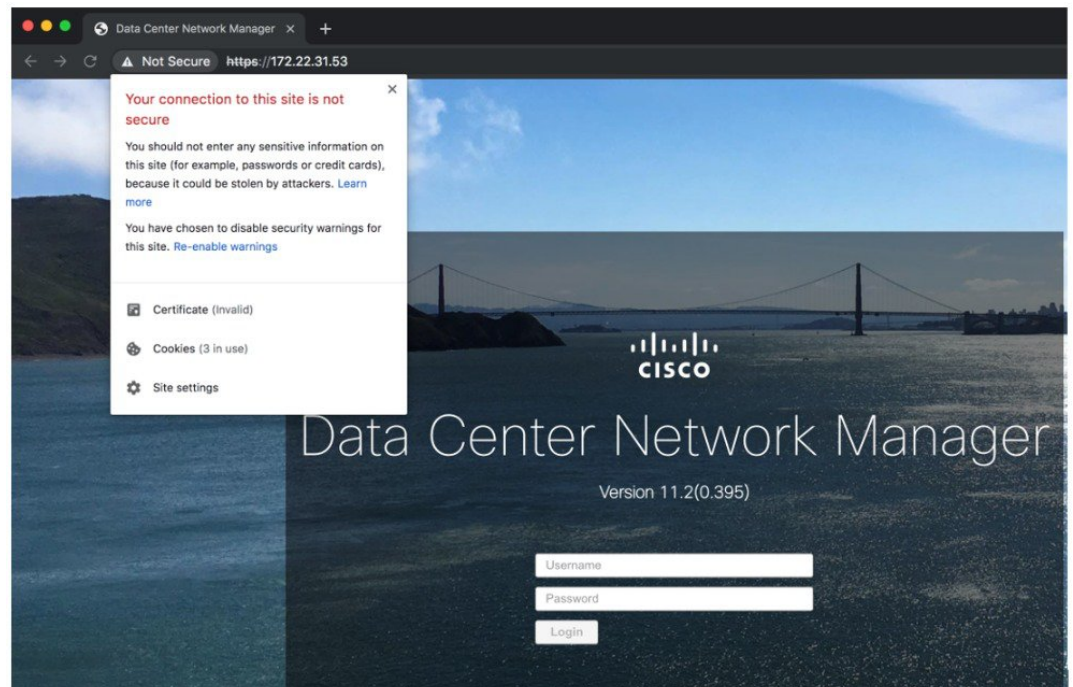
次のスニペットは、証明書を確認するための Chrome ブラウザバージョン 74.0.3729.169 の例です。

1. URL `https://<dcnm-ip-address>` または `https://<FQDN>` をブラウザのアドレスバーに入力します。

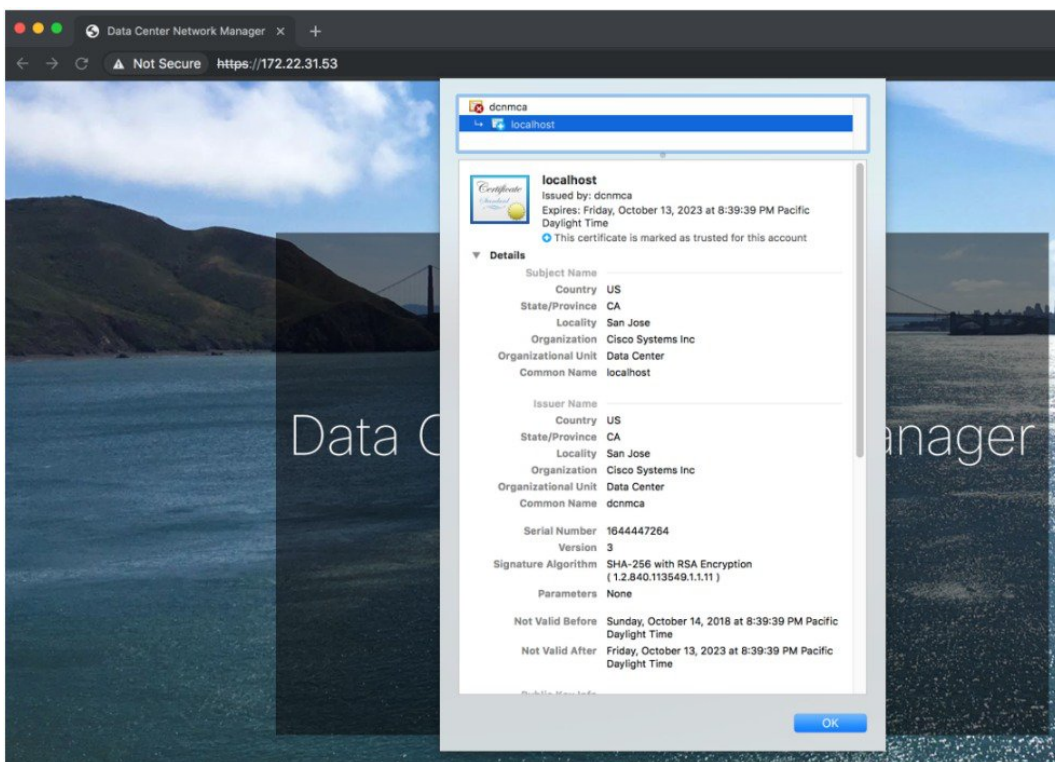
Return キーを押します。

2. 証明書の種類に基づき、URL フィールドの左側のアイコンにロックアイコン [] またはアラートアイコン [] が表示されます。

アイコンをクリックします。



3. カードで、[証明書 (Certificate)] フィールドをクリックします。
証明書の情報が示されます。



表示されている情報は、`appmgr afw show-cert-details` を使用して証明書の詳細を確認したときに、証明書 1 に表示されている詳細と一致している必要があります。

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。