セキュリティ証明書を管理する

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/ja-jp/active-iq-unified-manager-918/config/task_view_https_security_certificate_ocf.html on November 13, 2026. Always check docs.netapp.com for the latest.

目次

セキュリティ証明書を管理する . . . 1
- Active IQ Unified Manager でHTTPSセキュリティ証明書を表示する . . . 1
- Active IQ Unified Manager で HTTPS 証明書署名要求をダウンロードする . . . 1
- CA署名付きHTTPS証明書をActive IQ Unified Managerにインストールする . . . 1
  - 証明書チェーンの例 . . . 2
- Active IQ Unified Manager で外部ツールを使用して生成された HTTPS 証明書について . . . 3
  - ECキー ペアを含む証明書のロード形式 . . . 3
  - RSAキー ペアを含む証明書のロード形式 . . . 3
  - 外部で生成された証明書のアップロード チェック . . . 4
- 証明書管理のページの説明 . . . 5
  - Active IQ Unified Manager の HTTPS 証明書ページについて . . . 5
  - Active IQ Unified Manager の「HTTPS証明書の再生成」ダイアログボックス . . . 6

セキュリティ証明書を管理する

Active IQ Unified Manager でHTTPSセキュリティ証明書を表示する

HTTPS証明書の詳細をブラウザで取得した証明書と比較して、Unified Managerに対するブラウザの暗号化された接続が妨害されていないことを確認できます。

開始する前に

オペレータ、アプリケーション管理者、またはストレージ管理者のロールが必要です。

証明書を表示すると、再生成された証明書の内容を検証したり、Unified Managerへのアクセスに使用できるSubject Alt Name（SAN）を確認したりできます。

手順

1. 左側のナビゲーションペインで、**General** > **HTTPS Certificate** をクリックします。

   HTTPS証明書がページの上部に表示されます。

セキュリティ証明書について、[HTTPS 証明書]ページの情報よりも詳しい情報を表示する必要がある場合は、ブラウザで接続証明書を表示します。

Active IQ Unified Manager で HTTPS 証明書署名要求をダウンロードする

認証局にファイルを送信して署名を求めるために、現在のHTTPSセキュリティ証明書の証明書署名要求をダウンロードできます。CA署名証明書は、中間者攻撃を阻止するのに役立ち、自己署名証明書よりも強力なセキュリティ保護を実現します。

開始する前に

アプリケーション管理者のロールが必要です。

手順

1. 左側のナビゲーションペインで、**General** > **HTTPS Certificate** をクリックします。
2. 「HTTPS証明書署名要求をダウンロード」をクリックしてください。
3. `<hostname>.csr`ファイルを保存します。

認証局にファイルを送信して署名を求め、署名済み証明書をインストールできます。

CA署名付きHTTPS証明書をActive IQ Unified Managerにインストールする

認証局から署名を受けて返されたセキュリティ証明書を、アップロードしてインストールすることができます。アップロードしてインストールするファイルは、既存の自己署

名証明書の署名済みバージョンである必要があります。CA署名証明書は、中間者攻撃の阻止に役立ち、自己署名証明書よりも強力なセキュリティ保護を実現します。

*What .始める前に

次の操作を完了しておきます。

- 証明書署名要求ファイルをダウンロードし、認証局の署名を受けます。
- 証明書チェーンをPEM形式で保存します。
- すべての証明書（Unified Managerサーバ証明書からルート署名証明書まで。存在する中間証明書もすべて含む）をチェーンに組み込みます。

アプリケーション管理者のロールが必要です。

CSRを作成した証明書の有効期間が397日より長い場合、CAは証明書に署名して返信する前に有効期間を397日に短縮します。

手順

1. 左側のナビゲーションペインで、**General** > **HTTPS Certificate** をクリックします。
2. 「HTTPS証明書のインストール」をクリックします。
3. 表示されたダイアログボックスで、「ファイルを選択...」をクリックして、アップロードするファイルを選択します。
4. ファイルを選択し、*インストール*をクリックしてファイルをインストールしてください。

   詳細については、"外部ツールを使用して生成されたHTTPS証明書のインストール"を参照してください。

証明書チェーンの例

証明書チェーン ファイルの内容の例を次に示します。

```
-----BEGIN CERTIFICATE-----
<*Server certificate*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#1 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#2 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Root signing certificate*>
-----END CERTIFICATE-----
```

Active IQ Unified Manager で外部ツールを使用して生成された HTTPS 証明書について

自己署名またはCA署名の証明書に加え、OpenSSL、BoringSSL、LetsEncryptなどの外部ツールを使用して生成された証明書をインストールできます。

これらの証明書は外部で生成された公開鍵と秘密鍵のペアであるため、証明書チェーンとともに秘密鍵も読み込む必要があります。使用可能な鍵ペアアルゴリズムは「RSA」と「EC」です。「HTTPS証明書のインストール」オプションは、「HTTPS証明書」ページの「一般」セクションにあります。アップロードするファイルは、以下の入力形式である必要があります。

1. Active IQ Unified Managerホストに属するサーバの秘密鍵
2. 秘密鍵と一致するサーバの証明書
3. 上記の証明書への署名に使用された、ルートまでのCAの証明書

ECキー ペアを含む証明書のロード形式

許可されている曲線は「prime256v1」と「secp384r1」です。外部で生成されたECペアを含む証明書のサンプル：

```
 -----BEGIN EC PRIVATE KEY-----
<EC private key of Server>
-----END EC PRIVATE KEY-----
```

```
 -----BEGIN CERTIFICATE-----
 <Server certificate>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #1 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #2 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Root signing certificate>
 -----END CERTIFICATE-----
```

RSAキー ペアを含む証明書のロード形式

ホスト証明書に属する RSA 鍵ペアに許可される鍵サイズは 2048、3072、および 4096 です。外部で生成された **RSA** 鍵ペア を持つ証明書：

```
-----BEGIN RSA PRIVATE KEY-----
```

```
<RSA private key of Server>
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
<Server certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate #1 (if present)>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate #2 (if present)>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Root signing certificate>
-----END CERTIFICATE-----
```

証明書をアップロードしたら、Active IQ Unified Managerインスタンスを再起動して変更を反映する必要があります。

外部で生成された証明書のアップロード チェック

外部ツールを使用して生成された証明書をアップロードすると、システムでいくつかのチェックが実行されます。チェックに1つでも失敗すると、証明書は拒否されます。また、製品内のCSRから生成された証明書、および外部ツールを使用して生成された証明書の検証も実施されます。

- 入力で指定された秘密鍵が入力で指定されたホスト証明書と照合して検証されます。
- ホスト証明書の共通名（CN）がホストのFQDNと照合してチェックされます。
- ホスト証明書の共通名（CN）を空または空白にしたり、ローカル ホストに設定したりすることはできません。
- 証明書の有効期間の開始日を将来の日付にしたり、有効期限を過去の日付にしたりすることはできません。
- 中間CAまたはCAが存在する場合、証明書有効期間の開始日を将来の日付にしたり、有効期限を過去の日付にしたりすることはできません。

入力で指定する秘密鍵は暗号化しないでください。暗号化された秘密鍵はシステムで拒否されます。

例1

```
----BEGIN ENCRYPTED PRIVATE KEY-----
<Encrypted private key>
-----END ENCRYPTED PRIVATE KEY-----
```

例2

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END RSA PRIVATE KEY-----
```

例3

```
-----BEGIN EC PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END EC PRIVATE KEY-----
```

証明書のインストールが失敗した場合は、ナレッジベース（KB）の記事を参照してください：https://kb.netapp.com/mgmt/AIQUM/AIQUM_fails_to_install_externally_generated_certificate["ActiveIQ Unified Manager が外部で生成された証明書のインストールに失敗する"^]

証明書管理のページの説明

Active IQ Unified Manager の HTTPS 証明書ページについて

[HTTPS 証明書]ページでは、現在のセキュリティ証明書の表示、証明書署名要求のダウンロード、新しい自己署名HTTPS証明書の生成、新しいHTTPS証明書のインストールを行うことができます。

新しい自己署名HTTPS証明書を生成していない場合は、インストール時に生成された証明書がこのページに表示されます。

コマンド ボタン

各コマンド ボタンを使用して次の処理を実行できます。

- **HTTPS**証明書署名要求をダウンロード

  現在インストールされているHTTPS証明書の認証要求をダウンロードします。署名のために認証局に提供できるように、ブラウザで<hostname>.csrファイルを保存するよう求められます。

- **HTTPS**証明書をインストールする

  認証局の署名を受けて返されたセキュリティ証明書を、アップロードしてインストールすることができます。新しい証明書は、管理サーバを再起動すると有効になります。

- **HTTPS**証明書を再生成する

  新しい自己署名HTTPS証明書を生成して現在のセキュリティ証明書と置き換えることができます。新しい証明書は、Unified Managerを再起動すると有効になります。

Active IQ Unified Manager の「HTTPS証明書の再生成」ダイアログボックス

[HTTPS 証明書の再生成]ダイアログ ボックスでは、セキュリティ情報をカスタマイズし、その情報を使用して新しいHTTPS証明書を生成することができます。

このページには現在の証明書の情報が表示されます。

「Regenerate Using Current Certificate Attributes」と「Update the Current Certificate Attributes」を選択すると、現在の情報を使用して証明書を再生成するか、新しい情報を使用して証明書を生成することができます。

- コモンネーム

  必須。保護する対象の完全修飾ドメイン名（FQDN）。

  Unified Managerの高可用性構成では、仮想IPアドレスを使用します。

- メール

  任意。組織の連絡先のEメール アドレス。証明書の管理者またはIT部門のEメール アドレスが一般的です。

- 会社

  任意。通常は会社の法人名。

- 部門

  任意。社内の部署の名前。

- 市区町村

  任意。会社の所在地の市区町村。

- 状態

  任意。会社の所在地の都道府県。

- 国

  任意。会社の所在地の国。通常はISOの2文字の国コードです。

- 別名

  必須。このサーバにアクセスするために既存のローカルホストやその他のネットワーク アドレスに加えて使用できる、プライマリ ドメイン以外の追加の名前。別名はそれぞれカンマで区切ります。

  証明書の「代替名」フィールドからローカル識別情報を削除する場合は、「ローカル識別情報を除外する（例：localhost）」チェックボックスを選択してください。このチェックボックスを選択すると、代替名フィールドにはフィールドに入力した内容のみが使用されます。空欄のままにした場合、作成される証明書には「代替名」フィールドは一切含まれません。

- 鍵サイズ（鍵アルゴリズム：**RSA**）

  鍵アルゴリズムはRSAに設定されています。鍵のサイズ：2048、3072、4096ビットのいずれかを選択できます。デフォルトの鍵サイズは2048ビットに設定されています。

- 有効期間

  デフォルトの有効期間は397日です。以前のバージョンからアップグレードした場合は、以前の証明書の有効期間がそのまま表示される可能性があります。

詳細については、"HTTPS証明書の生成"を参照してください。

著作権に関する情報

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、http://www.netapp.com/TMに記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。