Gérer les certificats de sécurité

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/fr-fr/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.

Sommaire

Gérer les certificats de sécurité . . . 1
- Consultez le certificat de sécurité HTTPS dans Active IQ Unified Manager . . . 1
- Téléchargez une demande de signature de certificat HTTPS dans Active IQ Unified Manager . . . 1
- Installez un certificat HTTPS signé par une autorité de certification dans Active IQ Unified Manager . . . 2
  - Exemple de chaîne de certificats . . . 2
- Découvrez les certificats HTTPS générés à l'aide d'outils externes dans Active IQ Unified Manager Unified Manager . . . 3
  - Format pour charger un certificat avec une paire de clés EC . . . 3
  - Format pour charger un certificat avec une paire de clés RSA . . . 4
  - Vérifications lors du chargement de certificats générés en externe . . . 4
- Descriptions des pages pour la gestion des certificats . . . 5
  - Découvrez la page relative au certificat HTTPS dans Active IQ Unified Manager . . . 5
  - Boîte de dialogue « Régénérer un certificat HTTPS » dans Active IQ Unified Manager . . . 6

Gérer les certificats de sécurité

Consultez le certificat de sécurité HTTPS dans Active IQ Unified Manager

Vous pouvez comparer les détails du certificat HTTPS au certificat récupéré dans votre navigateur pour vous assurer que la connexion chiffrée de votre navigateur à Unified Manager n'est pas interceptée.

Avant de commencer

Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.

L'affichage du certificat vous permet de vérifier le contenu d'un certificat régénéré ou d'afficher les noms alternatifs du sujet (SAN) à partir desquels vous pouvez accéder à Unified Manager.

Étape

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Certificat HTTPS**.

   Le certificat HTTPS est affiché en haut de la page

Si vous souhaitez consulter des informations plus détaillées sur le certificat de sécurité que celles affichées sur la page du certificat HTTPS, vous pouvez visualiser le certificat de connexion dans votre navigateur.

Téléchargez une demande de signature de certificat HTTPS dans Active IQ Unified Manager

Vous pouvez télécharger une demande de signature de certificat pour le certificat de sécurité HTTPS actuel afin de fournir le fichier à une autorité de certification pour qu'elle le signe. Un certificat signé par une autorité de certification contribue à prévenir les attaques de l'homme du milieu et offre une meilleure protection de sécurité qu'un certificat autosigné.

Avant de commencer

Vous devez posséder le rôle d'administrateur d'application.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Certificat HTTPS**.
2. Cliquez sur **Télécharger la demande de signature de certificat HTTPS**.
3. Enregistrez le `<hostname>.csr` fichier.

Vous pouvez soumettre le fichier à une autorité de certification pour qu'elle le signe, puis installer le certificat signé.

Installez un certificat HTTPS signé par une autorité de certification dans Active IQ Unified Manager

Vous pouvez téléverser et installer un certificat de sécurité après qu'une autorité de certification l'a signé et renvoyé. Le fichier que vous téléversez et installez doit être une version signée du certificat auto-signé existant. Un certificat signé par une autorité de certification aide à prévenir les attaques de type man-in-the-middle et offre une meilleure protection de sécurité qu'un certificat auto-signé.

*Quoi .Avant de commencer

Vous devez avoir effectué les actions suivantes :

- Téléchargement du fichier de demande de signature de certificat et signature par une autorité de certification
- Chaîne de certificats enregistrée au format PEM
- Inclure tous les certificats de la chaîne, du certificat de serveur Unified Manager au certificat de signature racine, y compris tous les certificats intermédiaires présents

Vous devez posséder le rôle d'administrateur d'application.

Si la durée de validité du certificat pour lequel une CSR a été créée est supérieure à 397 jours, elle sera ramenée à 397 jours par la CA avant de signer et de renvoyer le certificat

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Certificat HTTPS**.
2. Cliquez sur **Installer le certificat HTTPS**.
3. Dans la boîte de dialogue qui s'affiche, cliquez sur **Choisir un fichier…** pour localiser le fichier à télécharger.
4. Sélectionnez le fichier, puis cliquez sur **Installer** pour l'installer.

   Pour plus d'informations, consultez "Installation d'un certificat HTTPS généré à l'aide d'outils externes".

Exemple de chaîne de certificats

L'exemple suivant montre à quoi peut ressembler un fichier de chaîne de certificats :

```
-----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-----
```

Découvrez les certificats HTTPS générés à l'aide d'outils externes dans Active IQ Unified Manager Unified Manager

Vous pouvez installer des certificats auto-signés ou signés par une autorité de certification et générés à l'aide d'un outil externe comme OpenSSL, BoringSSL, LetsEncrypt.

Vous devez charger la clé privée avec la chaîne de certificats, car ces certificats sont des paires de clés publique/privée générées en externe. Les algorithmes de paires de clés autorisés sont "RSA" et "EC". L'option **Installer le certificat HTTPS** est disponible sur la page Certificats HTTPS, dans la section Général. Le fichier que vous téléchargez doit respecter le format d'entrée suivant.

1. Clé privée du serveur appartenant à l'hôte Active IQ Unified Manager
2. Certificat du serveur correspondant à la clé privée
3. Certificats des autorités de certification (AC) en ordre inverse jusqu'à la racine, utilisés pour signer le certificat ci-dessus

Format pour charger un certificat avec une paire de clés EC

Les courbes autorisées sont « `prime256v1` » et « `secp384r1` ». Exemple de certificat avec une paire EC générée en externe :

```
 -----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-----
```

Format pour charger un certificat avec une paire de clés RSA

Les tailles de clé autorisées pour la paire de clés RSA appartenant au certificat hôte sont 2048, 3072 et 4096. certificat avec une paire de clés RSA générée en externe :

```
-----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-----
```

Une fois le certificat téléchargé, vous devez redémarrer l'instance Active IQ Unified Manager pour que les modifications soient prises en compte.

Vérifications lors du chargement de certificats générés en externe

Le système effectue des vérifications lors du chargement d'un certificat généré à l'aide d'outils externes. Si l'une de ces vérifications échoue, le certificat est rejeté. Des validations sont également incluses pour les certificats générés à partir de la CSR au sein du produit et pour les certificats générés à l'aide d'outils externes.

- La clé privée fournie en entrée est validée par rapport au certificat de l'hôte fourni en entrée.
- Le nom commun (CN) du certificat de l'hôte est comparé au nom de domaine complet (FQDN) de l'hôte.
- Le nom commun (CN) du certificat de l'hôte ne doit pas être vide ou blanc et ne doit pas être défini sur localhost.
- La date de début de validité ne doit pas être dans le futur et la date d'expiration de validité du certificat ne doit pas être dans le passé.
- Si une autorité de certification intermédiaire ou une autorité de certification existe, la date de début de validité du certificat ne doit pas être dans le futur et la date d'expiration de validité ne doit pas être dans le passé.

La clé privée fournie en entrée ne doit pas être chiffrée. Si des clés privées sont chiffrées, elles sont rejetées par le système.

Exemple 1

```
----BEGIN ENCRYPTED PRIVATE KEY-----
```

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

Exemple 2

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

Exemple 3

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

Si l'installation du certificat échoue, consultez l'article de la base de connaissances (KB) : "ActiveIQ Unified Manager ne parvient pas à installer un certificat généré en externe"

Descriptions des pages pour la gestion des certificats

Découvrez la page relative au certificat HTTPS dans Active IQ Unified Manager

La page Certificat HTTPS vous permet de consulter le certificat de sécurité actuel, de télécharger une demande de signature de certificat, de générer un nouveau certificat HTTPS auto-signé ou d'installer un nouveau certificat HTTPS.

Si vous n'avez pas généré de nouveau certificat HTTPS auto-signé, le certificat qui apparaît sur cette page est celui qui a été généré lors de l'installation.

Boutons de commande

Les boutons de commande vous permettent d'effectuer les opérations suivantes :

- **Télécharger la demande de signature de certificat HTTPS**

  Télécharge une demande de certification pour le certificat HTTPS actuellement installé. Votre navigateur vous invite à enregistrer le fichier <hostname>.csr afin que vous puissiez fournir le fichier à une autorité de certification pour signature.

- **Installer le certificat HTTPS**

  Permet de télécharger et d'installer un certificat de sécurité après sa signature et son renvoi par une autorité de certification. Le nouveau certificat prend effet après le redémarrage du serveur d'administration.

- **Régénérer le certificat HTTPS**

Permet de générer un nouveau certificat HTTPS auto-signé, qui remplace le certificat de sécurité actuel. Le nouveau certificat prend effet après le redémarrage d'Unified Manager.

Boîte de dialogue « Régénérer un certificat HTTPS » dans Active IQ Unified Manager

La boîte de dialogue « Régénérer le certificat HTTPS » vous permet de personnaliser les informations de sécurité, puis de générer un nouveau certificat HTTPS avec ces informations.

Les informations relatives au certificat actuel figurent sur cette page.

Les options « `Regenerate Using Current Certificate Attributes` » et « `Update the Current Certificate Attributes` » vous permettent de régénérer le certificat avec les informations actuelles ou de générer un certificat avec de nouvelles informations.

- **Nom commun**

  Obligatoire. Le nom de domaine complet (FQDN) que vous souhaitez sécuriser.

  Dans les configurations à haute disponibilité d'Unified Manager, utilisez l'adresse IP virtuelle.

- **E-mail**

  Facultatif. Une adresse électronique pour contacter votre organisation ; généralement l'adresse électronique de l'administrateur du certificat ou du service informatique.

- **Entreprise**

  Facultatif. Généralement, la dénomination sociale de votre entreprise.

- **Département**

  Facultatif. Le nom du département au sein de votre entreprise.

- **Ville**

  Facultatif. La ville où se situe votre entreprise.

- **État**

  Facultatif. Indiquez, en toutes lettres, l'État ou la province où se situe votre entreprise.

- **Pays**

  Facultatif. Le pays où est située votre entreprise. Il s'agit généralement du code ISO à deux lettres du pays.

- **Autres noms**

  Obligatoire. Noms de domaine supplémentaires, non principaux, pouvant être utilisés pour accéder à ce serveur en plus de localhost existant ou d'autres adresses réseau. Séparez chaque nom alternatif par une virgule.

  Cochez la case « Exclure les informations d'identification locales (par exemple localhost) » si vous

souhaitez supprimer les informations d'identification locales du champ « Autres noms » du certificat. Lorsque cette case est cochée, seules les informations que vous saisissez dans le champ sont utilisées dans le champ « Autres noms ». Si le champ est laissé vide, le certificat obtenu ne comportera aucun champ « Autres noms ».

- **TAILLE DE LA CLÉ (ALGORITHME DE CLÉ: RSA)**

  L'algorithme de clé est défini sur RSA. Vous pouvez sélectionner l'une des tailles de clé suivantes : 2048, 3072 ou 4096 bits. La taille de clé par défaut est définie sur 2048 bits.

- **PÉRIODE DE VALIDITÉ**

  La période de validité par défaut est de 397 jours. Si vous avez effectué une mise à niveau depuis une version précédente, il est possible que la validité du certificat précédent reste inchangée.

Pour plus d'informations, consultez "Génération de certificats HTTPS".

Informations sur le copyright

Copyright © 2026 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site http://www.netapp.com/TM sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.