Gérer les paramètres d'authentification SAML

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/concept_manage_saml_authentication_settings_um.html on November 13, 2026. Always check docs.netapp.com for the latest.

Sommaire

Gérer les paramètres d’authentification SAML . . . 1
- Activer l’authentification SAML dans Active IQ Unified Manager . . . 1
- Utilisez un fournisseur d’identité dans Active IQ Unified Manager . . . 1
  - Normes de chiffrement prises en charge . . . 1
  - Fournisseurs d’identité validés . . . 1
  - Exigences de configuration d’ADFS . . . 1
  - Autres exigences de configuration . . . 2
- Activer l’authentification SAML dans Active IQ Unified Manager . . . 2
- Modifier le fournisseur d’identité d’authentification SAML dans Active IQ Unified Manager . . . 3
- Mettez à jour les paramètres d’authentification SAML après une modification du certificat de sécurité d’Active IQ Unified Manager. . . . 4
- Désactiver l’authentification SAML dans Active IQ Unified Manager . . . 5
- Désactivez l’authentification SAML depuis la console de maintenance Active IQ Unified Manager . . . 6
- Utilisez la page d’authentification SAML dans Active IQ Unified Manager . . . 7

Gérer les paramètres d’authentification SAML

Activer l’authentification SAML dans Active IQ Unified Manager

Une fois les paramètres d’authentification à distance configurés, vous pouvez activer l’authentification SAML (Security Assertion Markup Language) afin que les utilisateurs distants soient authentifiés par un fournisseur d’identité sécurisé (IdP) avant de pouvoir accéder à l’interface utilisateur Web Unified Manager.

Notez que seuls les utilisateurs distants auront accès à l’interface utilisateur graphique de Unified Manager après l’activation de l’authentification SAML. Les utilisateurs locaux et les utilisateurs de maintenance ne pourront pas accéder à l’interface utilisateur. Cette configuration n’affecte pas les utilisateurs qui accèdent à la console de maintenance.

Utilisez un fournisseur d’identité dans Active IQ Unified Manager

Lors de la configuration d’Unified Manager pour utiliser un fournisseur d’identité (IdP) afin d’effectuer l’authentification SAML pour tous les utilisateurs distants, vous devez connaître certains paramètres de configuration requis pour que la connexion à Unified Manager réussisse.

Vous devez saisir l’URI et les métadonnées d’Unified Manager dans le serveur IdP. Vous pouvez copier ces informations depuis la page Unified ManagerSAML Authentication. Unified Manager est considéré comme le fournisseur de services (SP) dans la norme SAML (Security Assertion Markup Language).

Normes de chiffrement prises en charge

- Norme de chiffrement avancée (AES) : AES-128 et AES-256
- Algorithme de hachage sécurisé (SHA) : SHA-1 et SHA-256

Fournisseurs d’identité validés

- Shibboleth
- Services de fédération Active Directory (ADFS)

Exigences de configuration d’ADFS

- Vous devez définir trois règles de revendication dans l’ordre suivant, nécessaires pour que Unified Manager puisse analyser les réponses SAML ADFS pour cette entrée d’approbation de partie de confiance.

Règle de revendication	Valeur
SAM-account-name	ID de nom
SAM-account-name	urn:oid:0.9.2342.19200300.100.1.1

Règle de revendication	Valeur
Groupes de jetons — Nom non qualifié	urn:oid:1.3.6.1.4.1.5923.1.5.1.1

- Vous devez définir la méthode d'authentification sur "Forms Authentication", sinon les utilisateurs risquent de recevoir une erreur lors de leur déconnexion de Unified Manager. Procédez comme suit :
  a. Ouvrez la Console de gestion ADFS.
  b. Cliquez sur le dossier « Stratégies d'authentification » dans l'arborescence de gauche.
  c. Dans Actions à droite, cliquez sur Modifier la stratégie d'authentification principale globale.
  d. Définissez la méthode d'authentification Intranet sur « `Forms Authentication` » au lieu de la valeur par défaut « `Windows Authentication` ».
- Dans certains cas, la connexion via l'IdP est refusée lorsque le certificat de sécurité d'Unified Manager est signé par une autorité de certification. Deux solutions permettent de résoudre ce problème :
  - Suivez les instructions indiquées dans le lien pour désactiver la vérification de révocation sur le serveur ADFS pour le certificat d'autorité de certification chaîné associé à la partie de confiance :

    "Désactiver la vérification de révocation par approbation de partie de confiance"

  - Le serveur d'autorité de certification doit résider sur le serveur ADFS pour signer la demande de certificat du serveur Unified Manager.

Autres exigences de configuration

- Le décalage horaire d'Unified Manager est fixé à 5 minutes. La différence de temps entre le serveur IdP et le serveur Unified Manager ne peut donc pas dépasser 5 minutes, sinon l'authentification échouera.

Activer l'authentification SAML dans Active IQ Unified Manager

Vous pouvez activer l'authentification SAML (Security Assertion Markup Language) afin qu'un fournisseur d'identité sécurisé (IdP) authentifie les utilisateurs distants avant qu'ils puissent accéder à l'interface utilisateur web de Unified Manager.

Avant de commencer

- Vous devez avoir configuré l'authentification à distance et vérifié son bon fonctionnement.
- Vous devez avoir créé au moins un utilisateur distant ou un groupe distant avec le rôle Application Administrator.
- Le fournisseur d'identité (IdP) doit être pris en charge par Unified Manager et doit être configuré.
- Vous devez disposer de l'URL et des métadonnées de l'IdP.
- Vous devez avoir accès au serveur IdP.

Une fois que vous avez activé l'authentification SAML depuis Unified Manager, les utilisateurs ne peuvent pas accéder à l'interface utilisateur graphique tant que le fournisseur d'identité (IdP) n'a pas été configuré avec les informations sur l'hôte du serveur Unified Manager. Vous devez donc être prêt à effectuer les deux parties de la connexion avant de commencer le processus de configuration. Le fournisseur d'identité peut être configuré avant ou après la configuration de Unified Manager.

Seuls les utilisateurs distants auront accès à l'interface graphique de Unified Manager après l'activation de

l'authentification SAML. Les utilisateurs locaux et les utilisateurs de maintenance ne pourront pas accéder à l'interface utilisateur. Cette configuration n'affecte pas les utilisateurs qui accèdent à la console de maintenance, aux commandes Unified Manager ou aux ZAPIs.

Unified Manager redémarre automatiquement une fois la configuration SAML terminée sur cette page.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Authentification SAML**.
2. Cochez la case **Activer l'authentification SAML**.

   Les champs nécessaires à la configuration de la connexion IdP sont affichés.

3. Saisissez l'URI IdP et les métadonnées IdP requises pour connecter le serveur Unified Manager au serveur IdP.

   Si le serveur IdP est accessible directement depuis le serveur Unified Manager, vous pouvez cliquer sur le bouton **Récupérer les métadonnées IdP** après avoir saisi l'URI IdP pour renseigner automatiquement le champ Métadonnées IdP.

4. Copiez l'URI des métadonnées de l'hôte Unified Manager ou enregistrez les métadonnées de l'hôte dans un fichier texte XML.

   Vous pouvez configurer le serveur IdP avec ces informations dès maintenant.

5. Cliquez sur **Enregistrer**.

   Une boîte de dialogue s'affiche pour confirmer que vous souhaitez terminer la configuration et redémarrer Unified Manager.

6. Cliquez sur **Confirmer et se déconnecter** ; Unified Manager redémarre.

La prochaine fois que des utilisateurs distants autorisés tenteront d'accéder à l'interface graphique de Unified Manager, ils saisiront leurs identifiants sur la page de connexion IdP au lieu de la page de connexion de Unified Manager.

Si ce n'est pas déjà fait, accédez à votre IdP et saisissez l'URI du serveur Unified Manager ainsi que les métadonnées pour terminer la configuration.

Lorsque vous utilisez ADFS comme fournisseur d'identité, l'interface graphique de Unified Manager ne tient pas compte du délai d'expiration de ADFS et continue de fonctionner jusqu'à ce que le délai d'expiration de la session Unified Manager soit atteint. Vous pouvez modifier le délai d'expiration de la session de l'interface graphique en cliquant sur **General** > **Feature Settings** > **Inactivity Timeout**.

Modifier le fournisseur d'identité d'authentification SAML dans Active IQ Unified Manager

Vous pouvez modifier le fournisseur d'identité (IdP) utilisé par Unified Manager pour authentifier les utilisateurs distants.

Avant de commencer

- Vous devez disposer de l'URL et des métadonnées de l'IdP.
- Vous devez avoir accès à l'IdP.

Le nouvel IdP peut être configuré avant ou après la configuration d'Unified Manager.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Authentification SAML**.
2. Saisissez le nouvel URI IdP et les métadonnées IdP requises pour connecter le serveur Unified Manager à l'IdP.

   Si l'IdP est accessible directement depuis le serveur Unified Manager, vous pouvez cliquer sur le bouton **Fetch IdP Metadata** après avoir saisi l'URL de l'IdP pour renseigner automatiquement le champ IdP Metadata.

3. Copiez l'URI des métadonnées d'Unified Manager, ou enregistrez les métadonnées dans un fichier texte XML.
4. Cliquez sur **Enregistrer la configuration**.

   Une boîte de dialogue s'affiche pour confirmer que vous souhaitez modifier la configuration.

5. Cliquez sur **OK**.

Accédez au nouvel IdP et saisissez l'URI du serveur Unified Manager ainsi que les métadonnées pour terminer la configuration.

La prochaine fois que des utilisateurs distants autorisés tenteront d'accéder à l'interface graphique de Unified Manager, ils saisiront leurs identifiants sur la nouvelle page de connexion IdP au lieu de l'ancienne page de connexion IdP.

Mettez à jour les paramètres d'authentification SAML après une modification du certificat de sécurité d'Active IQ Unified Manager.

Toute modification du certificat de sécurité HTTPS installé sur le serveur Unified Manager nécessite la mise à jour des paramètres de configuration de l'authentification SAML. Le certificat est mis à jour si vous renommez le système hôte, lui attribuez une nouvelle adresse IP ou modifiez manuellement son certificat de sécurité.

Après la modification du certificat de sécurité et le redémarrage du serveur Unified Manager, l'authentification SAML ne fonctionnera plus et les utilisateurs ne pourront pas accéder à l'interface graphique de Unified Manager. Vous devez mettre à jour les paramètres d'authentification SAML sur le serveur IdP et sur le serveur Unified Manager pour rétablir l'accès à l'interface utilisateur.

Étapes

1. Connectez-vous à la console de maintenance.
2. Dans le **Main Menu**, saisissez le numéro correspondant à l'option **Disable SAML authentication**.

   Un message s'affiche pour confirmer que vous souhaitez désactiver l'authentification SAML et redémarrer Unified Manager.

3. Lancez l'interface utilisateur Unified Manager à l'aide du FQDN ou de l'adresse IP mis à jour, acceptez le certificat de serveur mis à jour dans votre navigateur et connectez-vous à l'aide des identifiants de l'utilisateur de maintenance.
4. Dans la page **Setup/Authentication**, sélectionnez l'onglet **SAML Authentication** et configurez la connexion IdP.
5. Copiez l'URI des métadonnées de l'hôte Unified Manager ou enregistrez les métadonnées de l'hôte dans un fichier texte XML.
6. Cliquez sur **Enregistrer**.

   Une boîte de dialogue s'affiche pour confirmer que vous souhaitez terminer la configuration et redémarrer Unified Manager.

7. Cliquez sur **Confirmer et se déconnecter** ; Unified Manager redémarre.
8. Accédez à votre serveur IdP et saisissez l'URI du serveur Unified Manager ainsi que les métadonnées pour terminer la configuration.

fournisseur d'identité	Étapes de configuration
ADFS	a. Supprimez l'entrée d'approbation de partie de confiance existante dans l'interface graphique de gestion ADFS. b. Ajoutez une nouvelle entrée d'approbation de partie de confiance à l'aide de celle du serveur Unified Manager mis à jour `saml_sp_metadata.xml`. c. Définissez les trois règles de revendication requises pour que Unified Manager puisse analyser les réponses SAML ADFS pour cette entrée d'approbation de partie de confiance. d. Redémarrez le service ADFS sous Windows.
Shibboleth	a. Mettez à jour le nouveau nom de domaine complet (FQDN) du serveur Unified Manager dans les fichiers `attribute-filter.xml` et `relying-party.xml`. b. Redémarrez le serveur web Apache Tomcat et attendez que le port 8005 devienne disponible.

9. Connectez-vous à Unified Manager et vérifiez que l'authentification SAML fonctionne comme prévu via votre IdP.

Désactiver l'authentification SAML dans Active IQ Unified Manager

Vous pouvez désactiver l'authentification SAML lorsque vous souhaitez cesser d'authentifier les utilisateurs distants via un fournisseur d'identité sécurisé (IdP) avant qu'ils puissent se connecter à l'interface utilisateur web de Unified Manager. Lorsque l'authentification SAML est désactivée, les fournisseurs de services d'annuaire configurés, tels qu'Active Directory ou LDAP, assurent l'authentification de connexion.

Une fois l'authentification SAML désactivée, les utilisateurs locaux et les utilisateurs de maintenance pourront accéder à l'interface utilisateur graphique en plus des utilisateurs distants configurés.

Vous pouvez également désactiver l'authentification SAML à l'aide de la console de maintenance de Unified Manager si vous n'avez pas accès à l'interface utilisateur graphique.

Unified Manager redémarre automatiquement après la désactivation de l'authentification SAML.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Authentification SAML**.
2. Décochez la case **Activer l'authentification SAML**.
3. Cliquez sur **Enregistrer**.

   Une boîte de dialogue s'affiche pour confirmer que vous souhaitez terminer la configuration et redémarrer Unified Manager.

4. Cliquez sur **Confirmer et se déconnecter** ; Unified Manager redémarre.

La prochaine fois que les utilisateurs distants tenteront d'accéder à l'interface graphique de Unified Manager, ils saisiront leurs identifiants sur la page de connexion de Unified Manager au lieu de la page de connexion IdP.

Accédez à votre IdP et supprimez l'URI et les métadonnées du serveur Unified Manager.

Désactivez l'authentification SAML depuis la console de maintenance Active IQ Unified Manager

Il peut être nécessaire de désactiver l'authentification SAML depuis la console de maintenance lorsqu'il n'est pas possible d'accéder à l'interface graphique de Unified Manager. Cela peut se produire en cas de mauvaise configuration ou si l'IdP n'est pas accessible.

Avant de commencer

Vous devez avoir accès à la console de maintenance en tant qu'utilisateur de maintenance.

Lorsque l'authentification SAML est désactivée, les fournisseurs de services d'annuaire configurés, tels qu'Active Directory ou LDAP, assurent l'authentification de connexion. Les utilisateurs locaux et les utilisateurs de maintenance pourront accéder à l'interface utilisateur graphique, en plus des utilisateurs distants configurés.

Vous pouvez également désactiver l'authentification SAML depuis la page Setup/Authentication de l'interface utilisateur.

Unified Manager redémarre automatiquement après la désactivation de l'authentification SAML.

Étapes

1. Connectez-vous à la console de maintenance.
2. Dans le **Main Menu**, saisissez le numéro correspondant à l'option **Disable SAML authentication**.

   Un message s'affiche pour confirmer que vous souhaitez désactiver l'authentification SAML et redémarrer

Unified Manager.

3. Tapez **y**, puis appuyez sur Entrée, et Unified Manager redémarre.

La prochaine fois que les utilisateurs distants tenteront d'accéder à l'interface graphique de Unified Manager, ils saisiront leurs identifiants sur la page de connexion de Unified Manager au lieu de la page de connexion IdP.

Si nécessaire, accédez à votre IdP et supprimez l'URL et les métadonnées du serveur Unified Manager.

Utilisez la page d'authentification SAML dans Active IQ Unified Manager

Vous pouvez utiliser la page d'authentification SAML pour configurer Unified Manager afin d'authentifier les utilisateurs distants à l'aide de SAML via un fournisseur d'identité sécurisé (IdP) avant qu'ils puissent se connecter à l'interface utilisateur web d'Unified Manager.

- Vous devez disposer du rôle d'administrateur d'application pour créer ou modifier la configuration SAML.
- Vous devez avoir configuré l'authentification à distance.
- Vous devez avoir configuré au moins un utilisateur distant ou un groupe distant.

Une fois l'authentification à distance et les utilisateurs distants configurés, vous pouvez cocher la case « Activer l'authentification SAML » pour activer l'authentification à l'aide d'un fournisseur d'identité sécurisé.

- **URI du fournisseur d'identité**

  L'URI permettant d'accéder à l'IdP depuis le serveur Unified Manager. Des exemples d'URI sont fournis ci-dessous.

  Exemple d'URI ADFS :

  ```
  https://win2016-dc.ntap2016.local/federationmetadata/2007-
  06/federationmetadata.xml
  ```

  Exemple d'URI Shibboleth:

  ```
  https://centos7.ntap2016.local/idp/shibboleth
  ```

- **Métadonnées du fournisseur d'identité**

  Les métadonnées du fournisseur d'identité au format XML.

  Si l'URL IdP est accessible depuis le serveur Unified Manager, vous pouvez cliquer sur le bouton **Fetch IdP Metadata** pour renseigner ce champ.

- **Système hôte (FQDN)**

  Le nom de domaine complet (FQDN) du système hôte d'Unified Manager, tel que défini lors de l'installation. Vous pouvez modifier cette valeur si nécessaire.

- **URI de l'hôte**

L’URI permettant d’accéder au système hôte Unified Manager depuis l’IdP.

- **Métadonnées de l’hôte**

  Les métadonnées du système hôte au format XML.

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.