Configuration de l'objet d'authentification LDAP sur le système FireSIGHT

Contenu

[Introduction](#)
[Configuration d'un objet d'authentification LDAP](#)
[Documents connexes](#)

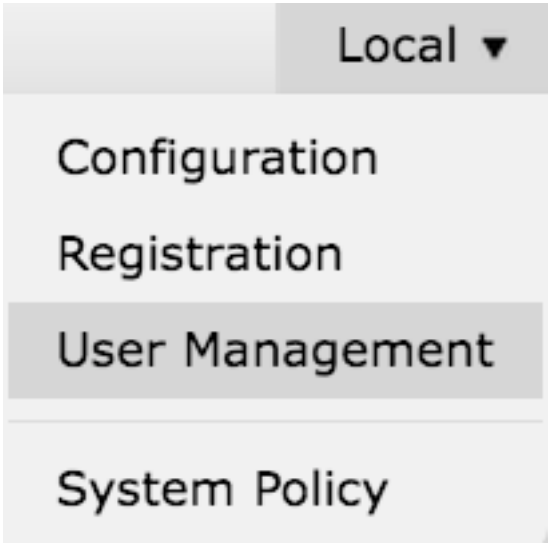
Introduction

Les objets d'authentification sont des profils de serveur pour les serveurs d'authentification externes, qui contiennent les paramètres de connexion et les paramètres de filtre d'authentification pour ces serveurs. Vous pouvez créer, gérer et supprimer des objets d'authentification dans FireSIGHT Management Center. Ce document décrit comment configurer l'objet d'authentification LDAP sur le système FireSIGHT.

Configuration d'un objet d'authentification LDAP

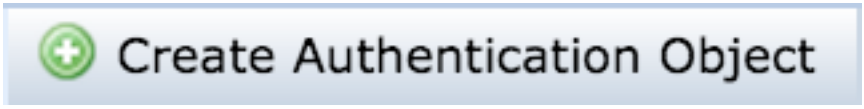
1. Connectez-vous à l'interface utilisateur Web de FireSIGHT Management Center.

2. Accédez à **System > Local > User Management**.



Sélectionnez l'onglet **Authentification de connexion**.

Cliquez sur **Create Authentication Object**.



3. Sélectionnez une **méthode d'authentification** et un **type de serveur**.

- **Méthode d'authentification** : LDAP
- **Name :** *<Nom d'objet d'authentification>*
- **Type de serveur** : MS Active Directory

Note: Les champs marqués d'un astérisque (*) sont obligatoires.

4. Spécifiez le nom d'hôte ou l'adresse IP du serveur principal et du serveur de sauvegarde. Un serveur de sauvegarde est facultatif. Cependant, tout contrôleur de domaine du même domaine peut être utilisé comme serveur de sauvegarde.

Note: Bien que le port LDAP soit par défaut le port **389**, vous pouvez utiliser un numéro de port non standard sur lequel le serveur LDAP écoute.

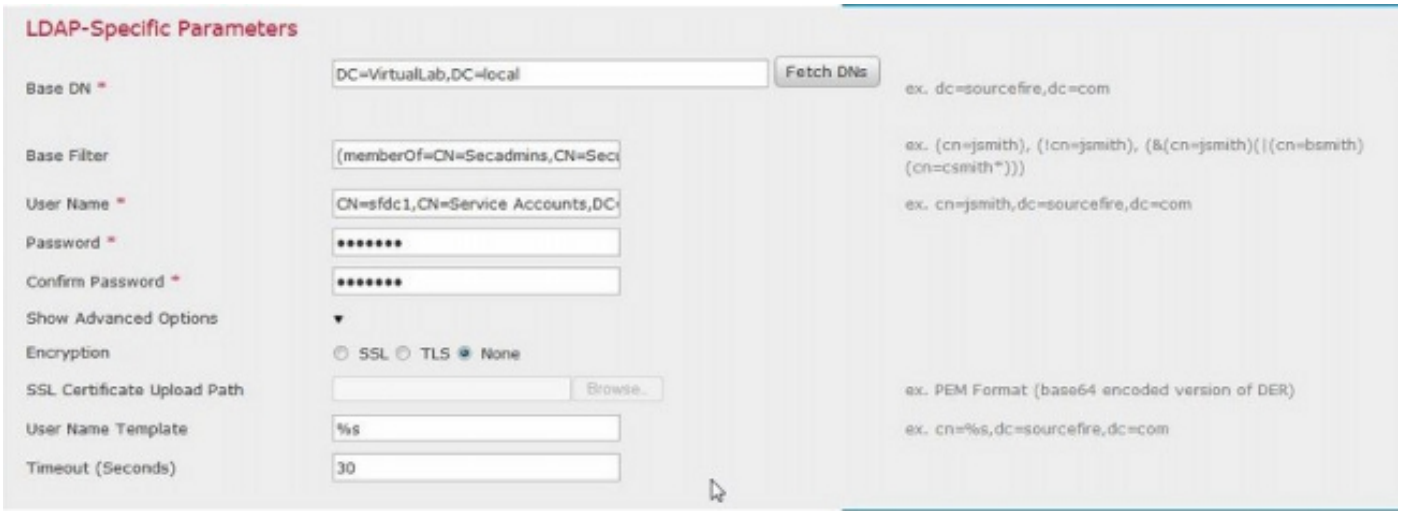
5. Spécifiez les **paramètres spécifiques à LDAP** comme indiqué ci-dessous :

Astuce : Les attributs d'utilisateur, de groupe et d'unité d'organisation doivent être identifiés avant de configurer **les paramètres spécifiques à LDAP**. Lisez ce document pour identifier les attributs d'objet LDAP Active Directory pour la configuration d'objet d'authentification.

- **DN de base** - DN de domaine ou d'unité d'organisation spécifique
- **Filtre de base** - DN du groupe dont les utilisateurs sont membres.
- **Nom d'utilisateur** - Compte d'emprunt d'identité pour le contrôleur de domaine
- **Mot de passe** : *<mot de passe>*
- **Confirm Password**: *<mot de passe>*

Options avancées :

- **Chiffrement** : SSL, TLS ou Aucun
- **Chemin de téléchargement du certificat SSL** : Télécharger la certification CA (facultatif)
- **Modèle de nom d'utilisateur** : %s
- **Délai (secondes)** : 30



Dans le paramètre de stratégie de sécurité de domaine de AD, si l'**exigence de signature du serveur LDAP** est définie sur **Exiger la signature**, SSL ou TLS doit être utilisé.

Serveur LDAP requis pour la signature

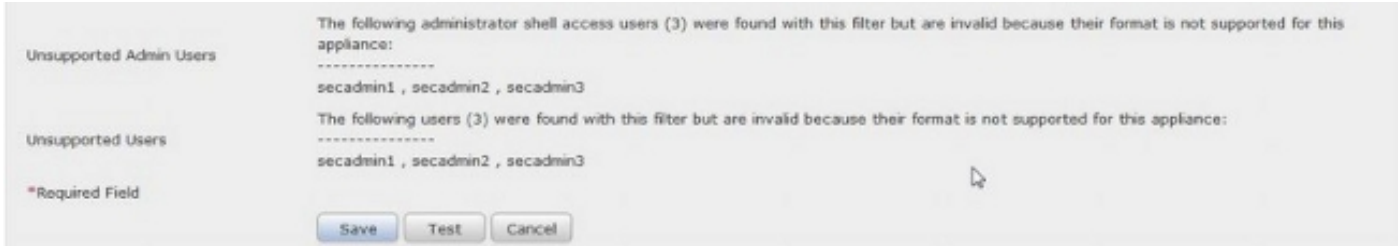
- **Aucune:** La signature des données n'est pas nécessaire pour établir une liaison avec le serveur. Si le client demande la signature des données, le serveur la prend en charge.
- **Exiger la signature** : À moins que TLS\SSL ne soit utilisé, l'option de signature des données LDAP doit être négociée.

  Note: Le côté client ou le certificat CA (certificat CA) n'est pas requis pour LDAPS. Cependant, il s'agirait d'un niveau de sécurité supplémentaire lorsque le certificat CA est téléchargé vers l'objet d'authentification.

6. Spécifiez le mappage d'attribut

- **Attribut d'accès UI** : sAMAccountName
- **Attribut d'accès shell** : sAMAccountName

Astuce : Si vous rencontrez un message Utilisateurs non pris en charge dans le résultat du test, remplacez l'**attribut d'accès à l'interface utilisateur** par **userPrincipalName** et vérifiez que le **modèle Nom d'utilisateur** est défini sur **%s**.



7. Configurer les **rôles d'accès contrôlé par groupe**

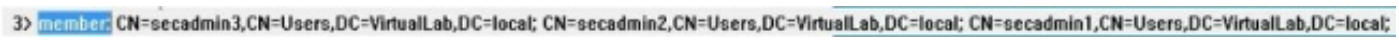
Sur **ldp.exe**, accédez à chaque groupe et copiez le DN du groupe correspondant dans l'objet Authentication comme indiqué ci-dessous :

- **<Nom du groupe> DN du groupe : <nom de groupe>**
- **Attribut de membre du groupe** : doit toujours être **membre**

Exemple :

- **DN du groupe administrateur :** CN=Administrateurs DC,CN=Groupes de sécurité,DC=VirtualLab,DC=Local
- **Attribut de membre du groupe** : membre

Un groupe de sécurité Active Directory a un attribut de **membre** suivi du DN des utilisateurs membres. L'attribut de **membre** number previous indique le nombre d'utilisateurs membres.



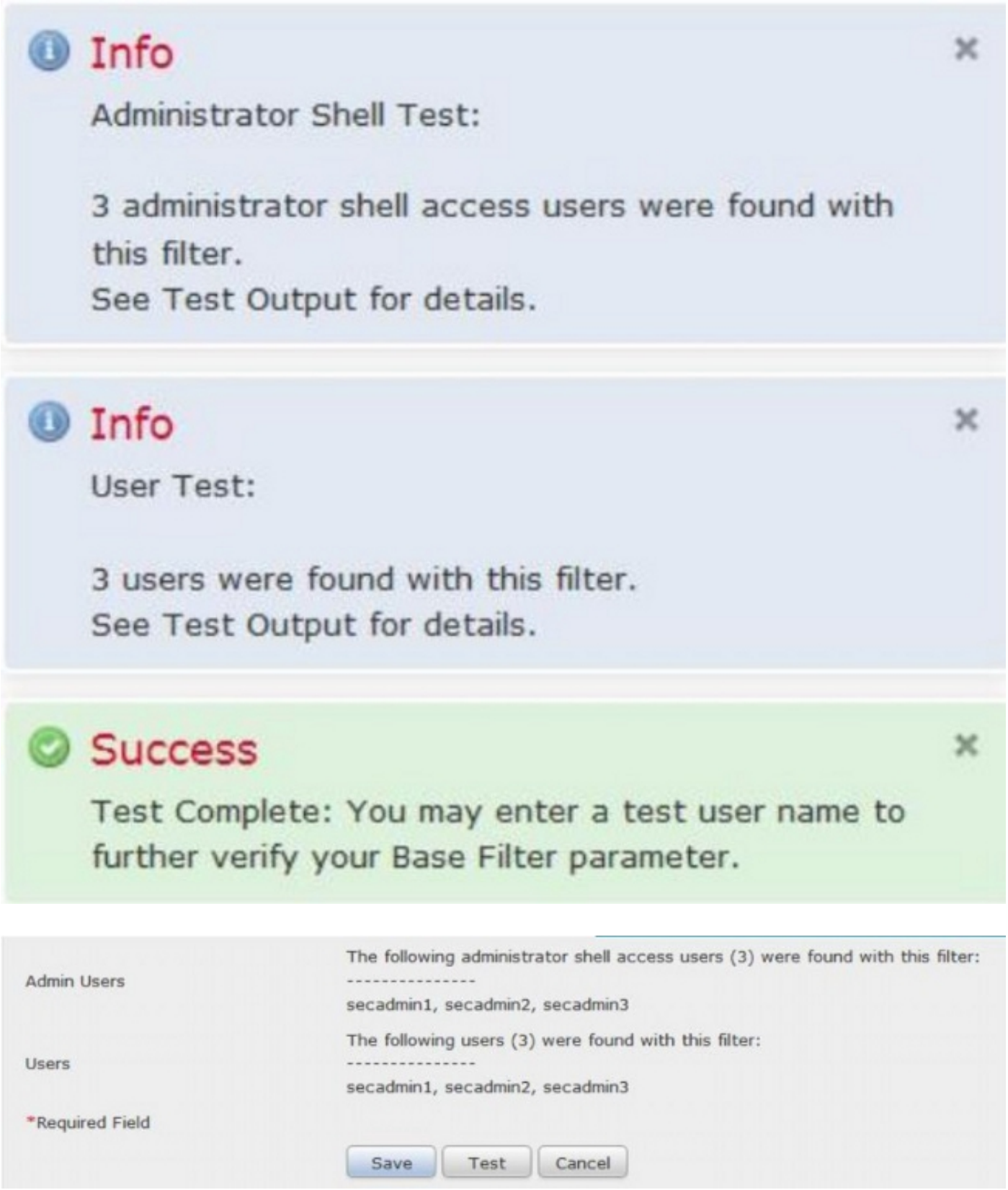
8. Sélectionnez **Identique au filtre de base** pour le filtre d'accès au shell ou spécifiez l'attribut memberOf comme indiqué à l'étape 5.

Filtre d'accès shell : (memberOf=<nom distinctif du groupe>)

Par exemple,

Filtre d'accès shell : (memberOf=CN=Utilisateurs Shell,CN=Groupes de sécurité,DC=VirtualLab,DC=local)

9. Enregistrez l'objet d'authentification et effectuez un test. Un résultat de test réussi ressemble à ceci :



10. Une fois que l'objet d'authentification a réussi le test, activez-le dans la stratégie système et réappliquez la stratégie à votre appliance.

Documents connexes

- Identifier les attributs d'objet LDAP Active Directory pour la configuration des objets

d'authentification