Konfiguration des LDAP-Authentifizierungsobjekts auf dem FireSIGHT-System

Inhalt

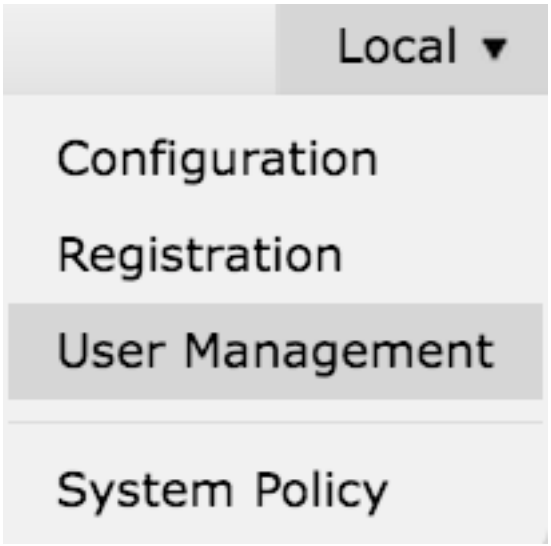
Einführung

Authentifizierungsobjekte sind Serverprofile für externe Authentifizierungsserver, die Verbindungseinstellungen und Authentifizierungsfiltereinstellungen für diese Server enthalten. Sie können Authentifizierungsobjekte in einem FireSIGHT Management Center erstellen, verwalten und löschen. In diesem Dokument wird beschrieben, wie das LDAP-Authentifizierungsobjekt auf FireSIGHT System konfiguriert wird.

Konfiguration eines LDAP-Authentifizierungsobjekts

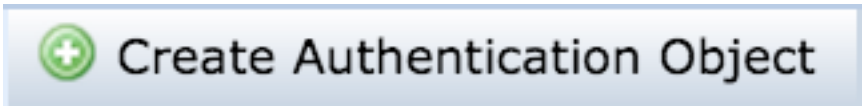
1. Melden Sie sich bei der Web-Benutzeroberfläche des FireSIGHT Management Center an.

2. Navigieren Sie zu **System > Local > User Management**.



Wählen Sie die Registerkarte **Anmeldenauthentifizierung** aus.

Klicken Sie auf **Authentifizierungsobjekt erstellen**.



3. Wählen Sie eine **Authentifizierungsmethode** und einen **Servertyp aus**.

- **Authentifizierungsmethode**: LDAP
- **Name**: *<Name des Authentifizierungsobjekts>*
- **Server-Typ**: MS Active Directory

Hinweis: Mit Sternchen (*) gekennzeichnete Felder sind Pflichtfelder.

4. Geben Sie den Host-Namen oder die IP-Adresse des primären und des Backup-Servers an. Ein Backup-Server ist optional. Jedoch kann jeder Domänencontroller in derselben Domäne als Backup-Server verwendet werden.

Hinweis: Obwohl der LDAP-Port standardmäßig Port **389** ist, können Sie eine nicht standardmäßige Portnummer verwenden, die vom LDAP-Server überwacht wird.

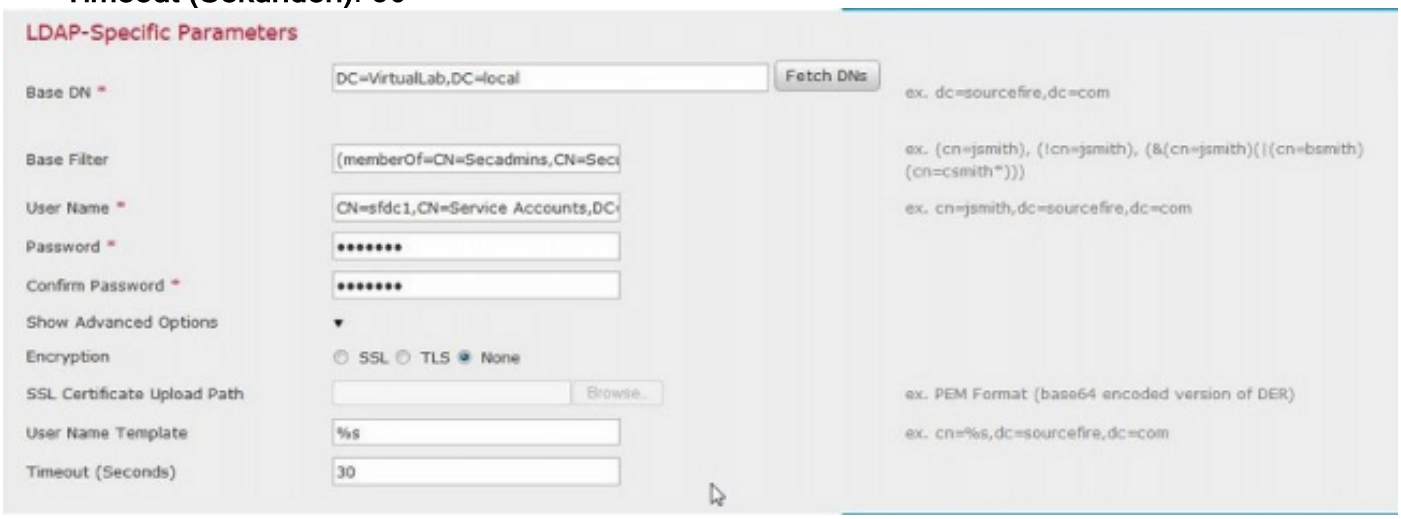
5. Geben Sie die **LDAP-spezifischen Parameter** wie folgt an:

Tipp: Das Benutzer-, Gruppen- und OU-Attribut sollte vor der Konfiguration der **LDAP-spezifischen Parameter** identifiziert werden. Lesen Sie dieses Dokument, um Active Directory-LDAP-Objektattribute für die Konfiguration von Authentifizierungsobjekten zu identifizieren.

- **Base DN** - Domänen- oder spezifischer OU-DN
- **Base Filter**: Die Gruppen-DN, der Benutzer angehören.
- Benutzername - Identitätskonto für das Rechenzentrum
- **Kennwort**: *<Kennwort>*
- **Kennwort bestätigen**: *<Kennwort>*

Erweiterte Optionen:

- **Verschlüsselung**: SSL, TLS oder Keine
- **Pfad zum Hochladen von SSL-Zertifikaten**: Zertifizierungsstelle hochladen (optional)
- **Vorlage für Benutzernamen**: %s
- **Timeout (Sekunden)**: 30



Wenn in der Domänensicherheitsrichtlinieneinstellung des AD die **LDAP-Serversignaturanforderung Signierung** auf **Signierung** erforderlich **festgelegt** ist, muss SSL oder TLS verwendet werden.

LDAP-Serversignaturanforderung

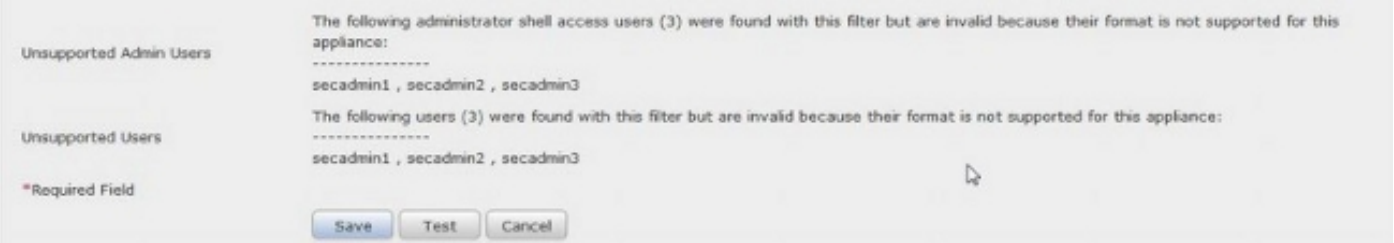
- **Keine:** Für die Bindung an den Server ist keine Datensignierung erforderlich. Wenn der Client die Signierung von Daten anfordert, wird diese vom Server unterstützt.
- **Signierung erforderlich**: Wenn TLS\SSL nicht verwendet wird, muss die LDAP-Datensignierungsoption ausgehandelt werden.

  Hinweis: Für LDAPS ist kein clientseitiges oder CA-Zertifikat (CA cert) erforderlich. Dies wäre jedoch eine zusätzliche Sicherheitsstufe, bei der CA-Zertifikate in das Authentifizierungsobjekt hochgeladen werden.

6. Attributzuordnung festlegen

- **UI-Zugriffsattribut**: sAMAccountName
- **Shell-Zugriffsattribut**: sAMAccountName

Tipp: Wenn in der Testausgabe **die** Meldung **Nicht unterstützte Benutzer** angezeigt wird, ändern Sie das **UI Access Attribute** in **userPrincipalName**, und stellen Sie sicher, dass die **Vorlage User Name** auf **%s** festgelegt ist.



7. Konfigurieren **von Gruppen-gesteuerten Zugriffsrollen**

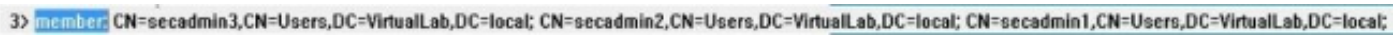
Durchsuchen Sie auf **ldp.exe** die einzelnen Gruppen, und kopieren Sie die entsprechende Gruppen-DN in das Authentifizierungsobjekt, wie unten gezeigt:

- **<Gruppenname> Gruppen-DN: <Gruppennummer>**
- **Gruppenmitgliedsattribut**: sollte immer **Mitglied** sein

Beispiel:

- **Administratorgruppen-DN:** CN=DC-Administratoren,CN=Security Groups,DC=VirtualLab,DC=local
- **Gruppenmitgliedsattribut**: Mitglied

Eine AD-Sicherheitsgruppe verfügt über ein Attribut des **Mitglieds**, gefolgt von dem DN der Member-Benutzer. Das numerische vorangegangene **Member**-Attribut gibt die Anzahl der Member-Benutzer an.



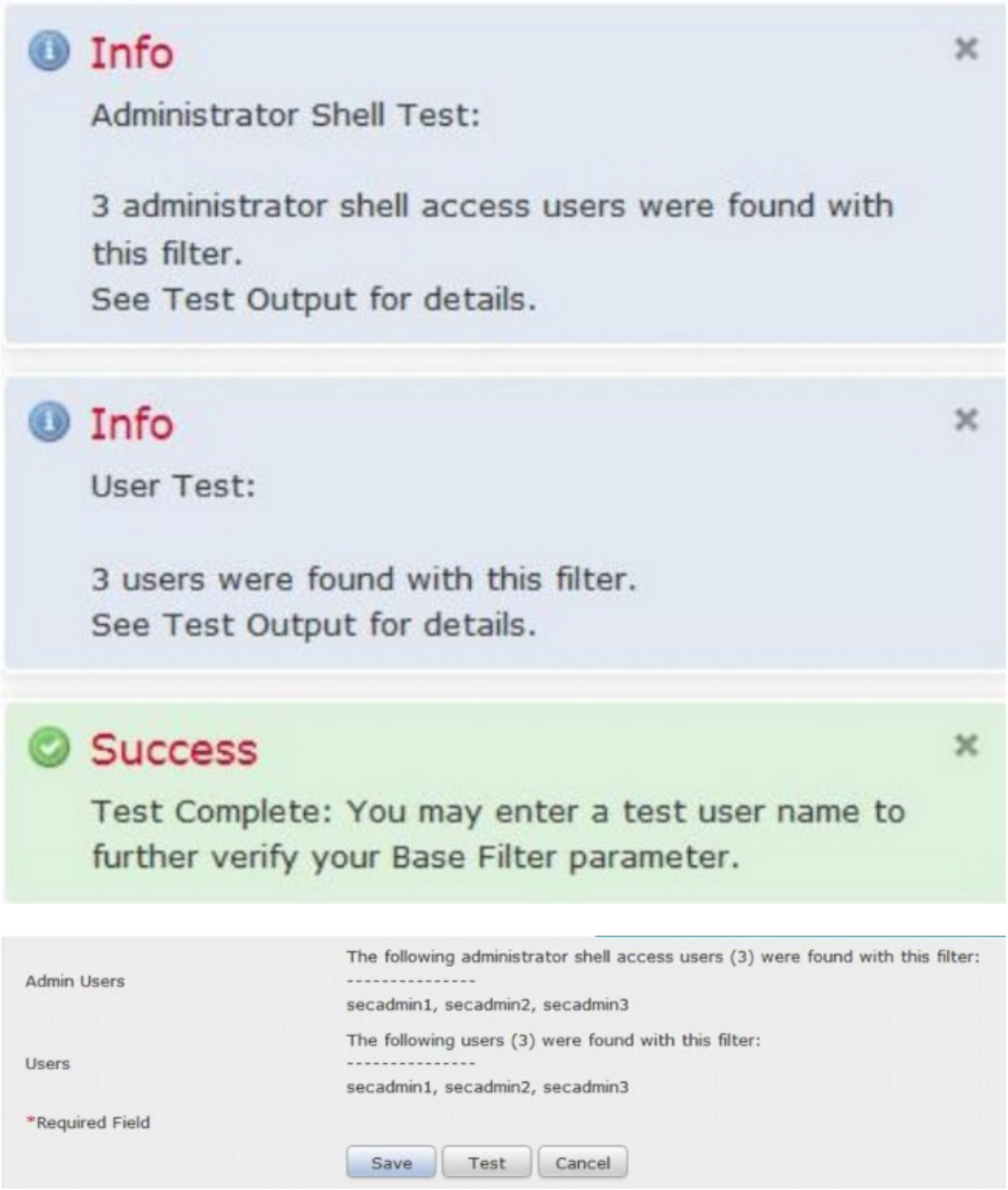
8. Wählen Sie **Identischer Basisfilter** für Shell Access Filter, oder geben Sie das memberOf-Attribut wie in Schritt 5 beschrieben an.

Shell-Zugriffsfilter: (memberOf=<group DN>)

Beispiel:

Shell-Zugriffsfilter: (memberOf=CN=Shell-Benutzer,CN=Security Groups,DC=VirtualLab,DC=local)

9. Speichern Sie das Authentifizierungsobjekt, und führen Sie einen Test aus. Ein erfolgreiches Testergebnis sieht wie folgt aus:



10. Wenn das Authentifizierungsobjekt den Test besteht, aktivieren Sie das Objekt in der Systemrichtlinie, und wenden Sie die Richtlinie erneut auf die Appliance an.

Verwandtes Dokument

- Identifizieren von Active Directory-LDAP-Objektattributen für die Konfiguration von

Authentifizierungsobjekten