

Configuratie van LDAP verificatieobject op FireSIGHT-systeem

Inhoud

[Inleiding](#)

[Configuratie van een LDAP-verificatieobject](#)

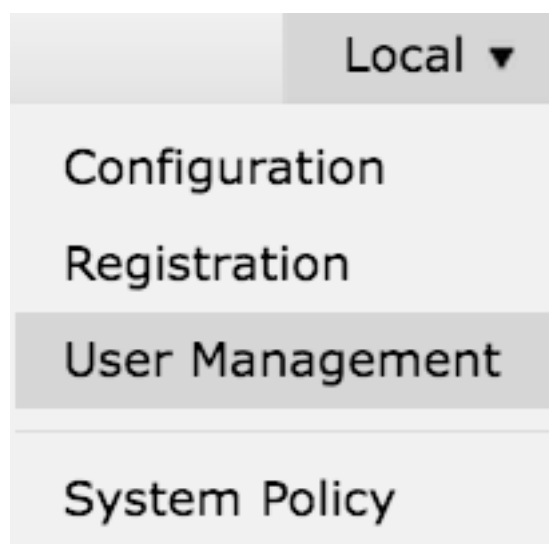
[Verwante document](#)

Inleiding

Verificatieobjecten zijn serverprofielen voor externe verificatieservers, die verbindinginstellingen en de filterinstellingen voor deze servers bevatten. U kunt verificatieobjecten op een FireSIGHT Management Center maken, beheren en verwijderen. In dit document wordt beschreven hoe u de LDAP-verificatieobject op FireSIGHT-systeem kunt configureren.

Configuratie van een LDAP-verificatieobject

1. Meld u aan bij de webgebruikersinterface van het FireSIGHT Management Center.
2. Navigeer naar **stelsel > Lokaal > gebruikersbeheer**.



Selecteer het tabblad **Login-verificatie**.



Klik op **Verificatieobject maken**.

Create Authentication Object

3. Selecteer een **verificatiemethode** en een **servertype**.

- **Verificatiemethode** : LDAP
- **Name**: <naam van verificatieobject>
- **Type server**: MS Active Directory

Opmerking: Velden met sterretjes (*) zijn vereist.

Authentication Object

Authentication Method	LDAP
Name *	<input type="text"/>
Description	<input type="text"/>
Server Type	MS Active Directory

4. Specificeer de hostnaam van de server en het IP-adres. Een back-upserver is optioneel. Elke Domain Controller binnen hetzelfde domein kan echter worden gebruikt als een reserveserver.

Opmerking: Hoewel de LDAP poort standaard op poort **389 staat**, kunt u een niet-standaard poortnummer gebruiken dat de LDAP server aanstuurt.

5. Specificeer de **LDAP-specifieke parameters** zoals hieronder wordt weergegeven:

Tip: De gebruikers-, groep- en OU-eigenschappen moeten worden geïdentificeerd voordat u de **LDAP-specifieke parameters** gaat configureren. Lees [dit document](#) om de eigenschappen van het actieve lidaf-object van de map te identificeren voor de configuratie van het verificatieobject.

- **Base DN** - Domain of Specific OU ISDN
- **Base Filter** - de groep DNA waarvan de gebruikers lid zijn.
- **Gebruikersnaam** - Imitatie-rekening voor DC
- **Wachtwoord**: <wachtwoord>
- **Wachtwoord bevestigen**: <wachtwoord>

Geavanceerde opties:

- **Encryptie**: SSL, TLS of geen
- **SSL-certificaatuploadpad**: Upload de CA-certificering (optioneel)
- **Sjabloon voor gebruikersnaam**: %s
- **Time-out (seconden)**: 30

LDAP-Specific Parameters

Base DN * ex. dc=sourcefire,dc=com

Base Filter ex. (cn=jsmith), (&(cn=jsmith)((cn=bsmith)(cn=csmith*)))

User Name * ex. cn=jsmith,dc=sourcefire,dc=com

Password *

Confirm Password *

Show Advanced Options ▼

Encryption SSL TLS None

SSL Certificate Upload Path ex. PEM Format (base64 encoded version of DER)

User Name Template ex. cn=%s,dc=sourcefire,dc=com

Timeout (Seconds)

In de Domain Security Policy Setting van de AD, indien de **LDAP server Signing-eis** is ingesteld, moet er SSL of TLS worden gebruikt.

Vereisten voor signalering van LDAP-server

- **None:** Het ondertekenen van gegevens is niet vereist om zich aan een server te binden. Als de client gegevens gebaren vraagt, ondersteunt de server het.
- **Meld:** Tenzij het TLS\SSL wordt gebruikt, moet de LDAP-gegevenssignaaloptie worden onderhandeld.

Opmerking: Voor LDAPS is geen client- of CA-certificaat (CA-cert) vereist. Het zou echter een extra beveiligingsniveau van CA cert zijn geüpload naar het verificatieobject.

6. Toewijzing van kenmerken specificeren

- **UI-toegangskarakter:** AMAaccountNaam
- **Shell-toegangskarakter:** AMAaccountNaam

Attribute Mapping

UI Access Attribute *

Shell Access Attribute *

Tip: Als u in de testuitvoer een bericht van niet-ondersteunde gebruikers tegenkomt, wijzigt u het **UI-toegangskarakter** in naam van gebruiker en zorgt u ervoor dat de gebruikersnaamsjabloon is ingesteld op %s.

Unsupported Admin Users

The following administrator shell access users (3) were found with this filter but are invalid because their format is not supported for this appliance:

secadmin1, secadmin2, secadmin3

Unsupported Users

The following users (3) were found with this filter but are invalid because their format is not supported for this appliance:

secadmin1, secadmin2, secadmin3

*Required Field

7. Groepsgecontroleerde toegangsrollen instellen

Op **ldp.exe**, bladert u naar elke groepen en kopieert u de betreffende groep DN naar het verificatieobject zoals hieronder wordt getoond:

- **<groepsnaam> groep DN: <groep den>**
- **Kenmerk groepslid:** moet altijd **lid** zijn

Voorbeeld:

- **Administrator Group DN:** CN=DC Admins, CN=Security Groepen, DC=VirtualLab,DC=Local
- **Kenmerk groepslid:** lid

Een AD-beveiligingsgroep heeft een eigenschap van **lid**, gevolgd door de DN-gebruikers van leden. Het nummer dat aan **de** eigenschap voorafgaat geeft het aantal aangesloten gebruikers aan.

```
3> member: CN=secadmin3,CN=Users,DC=VirtualLab,DC=local; CN=secadmin2,CN=Users,DC=VirtualLab,DC=local; CN=secadmin1,CN=Users,DC=VirtualLab,DC=local;
```

8. Selecteer **Zelfde als basisfilter** voor Shell Access Filter, of specificeer **lidOf** eigenschap zoals aangegeven in stap 5.

Shell-toegangsfiler: (lid van=<groep DN>)

Bijvoorbeeld:

Shell-toegangsfiler: (lid van=CN=Shell gebruikers, CN=Security Groepen, DC=VirtualLab,DC=local)

9. Sla de verificatieobject op en voer een test uit. Hieronder ziet een succesvol testresultaat eruit:



Info



Administrator Shell Test:

3 administrator shell access users were found with this filter.

See Test Output for details.



Info



User Test:

3 users were found with this filter.

See Test Output for details.



Success



Test Complete: You may enter a test user name to further verify your Base Filter parameter.

Admin Users

The following administrator shell access users (3) were found with this filter:

secadmin1, secadmin2, secadmin3

Users

The following users (3) were found with this filter:

secadmin1, secadmin2, secadmin3

*Required Field

Save

Test

Cancel

10. Nadat de verificatieobject de test heeft doorlopen, stelt u het object in het systeembeleid in en past u het beleid opnieuw op uw apparaat toe.

Verwante document

- [Identificeer actieve Directory LDAP Objectkenmerken voor verificatie Objectconfiguratie](#)