Configuration of LDAP Authentication Object on FireSIGHT System

Document ID: 118738

Contributed by Nazmul Rajib and Binyam Demissie, Cisco TAC Engineers.

Jan 05, 2015

Contents

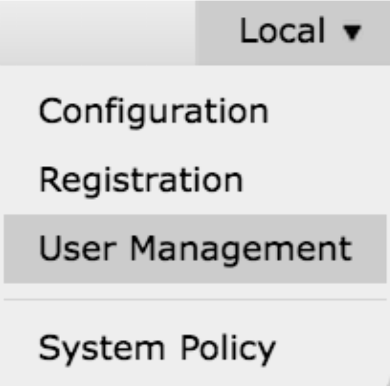
Introduction

Authentication Objects are server profiles for external authentication servers, containing connection settings and authentication filter settings for those servers. You can create, manage, and delete Authentication Objects on a FireSIGHT Management Center. This document describes how to configure LDAP Authentication Object on FireSIGHT System.

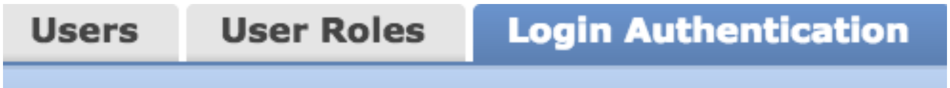
Configuration of an LDAP Authentication Object

1. Login to the web user interface of the FireSIGHT Management Center.

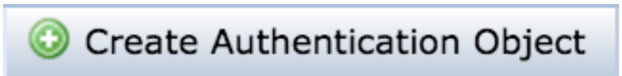
2. Navigate to ***System*** > ***Local*** > ***User Management***.



Select the ***Login Authentication*** tab.



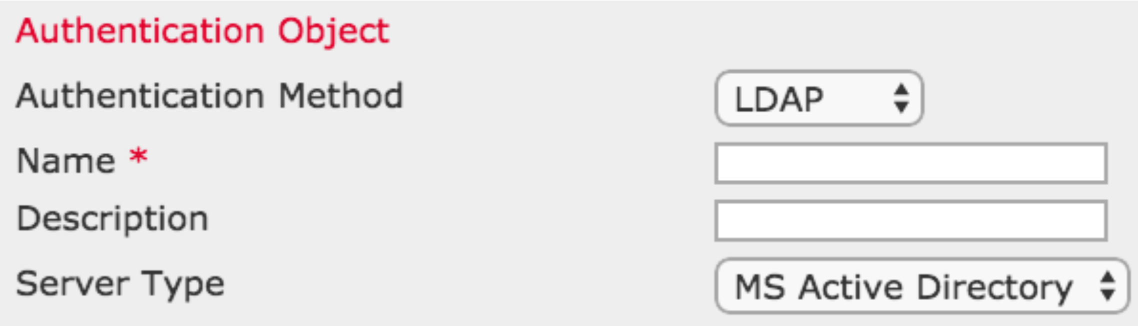
Click on ***Create Authentication Object***.



3. Select an ***Authentication Method*** and a ***Server Type***.

- ***Authentication Method*** : LDAP
- ***Name***: *<Authentication Object Name>*
- ***Server Type***: MS Active Directory

Note: Fields marked with asterisks (*) are required.



Authentication Object

Authentication Method LDAP

Name *

Description

Server Type MS Active Directory

4. Specify the Primary and Backup Server Host Name or IP Address. A Backup Server is optional. However, any Domain Controller within the same domain can be used as a backup server.

Note: Although the LDAP port is default to port ***389***, you can use a non−standard port number that the LDAP server is listening on.

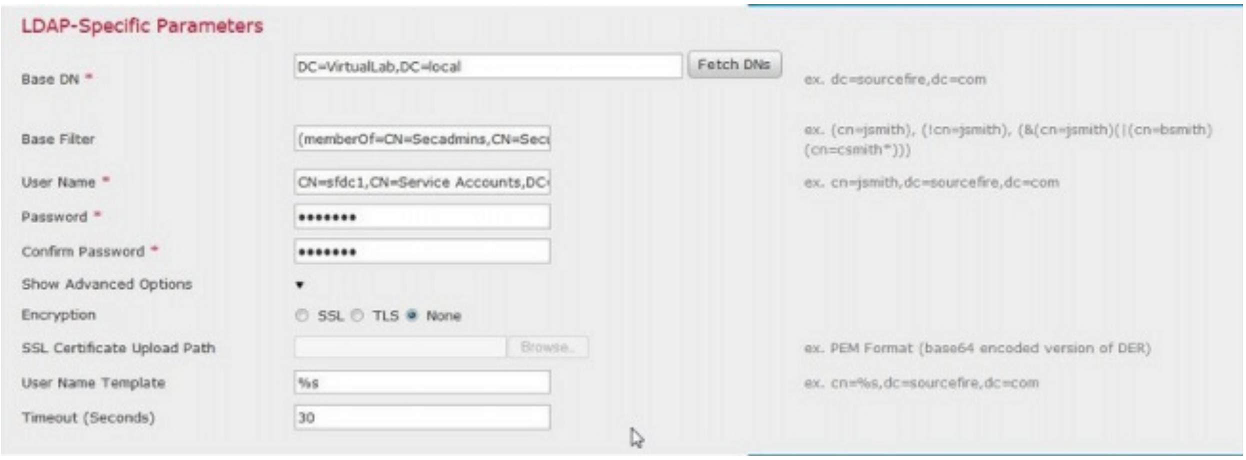
5. Specify the ***LDAP−Specific Parameters*** as shown below:

Tip: The user, group, and OU attributes should be identified prior to configuring ***LDAP−Specific Parameters***. Read this document to identify Active Directory LDAP object attributes for authentication object configuration.

- ***Base DN*** − Domain or Specific OU DN
- ***Base Filter*** − The group DN that users are member of.
- ***User Name*** − Impersonation account for the DC
- ***Password***: *<password>*
- ***Confirm Password***: *<password>*

Advanced Options:

- ***Encryption***: SSL, TLS or None
- ***SSL Certificate Upload Path***: Upload the CA certification (Optional)
- ***User Name Template***: %s
- ***Timeout (Seconds)*** : 30



LDAP-Specific Parameters

Base DN *	DC=VirtualLab,DC=local	ex. dc=sourcefire,dc=com
Base Filter	(memberOf=CN=Secadmins,CN=Secu	ex. (cn=jsmith), (!cn=jsmith), (&(cn=jsmith)(|(cn=bsmith)(cn=csmith*)))
User Name *	CN=sfdc1,CN=Service Accounts,DC=	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	%s	ex. cn=%s,dc=sourcefire,dc=com
Timeout (Seconds)	30	

In the Domain Security Policy Setting of the AD, if ***LDAP server Signing requirement*** is set to ***Require Signing***, SSL or TLS must be used.

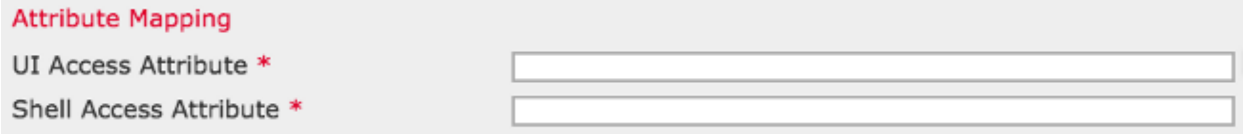
LDAP server Signing requirement

- ***None:*** Data signing is not required in order to bind with server. If the client requests data signing, the server supports it.
- ***Require signing***: Unless TLS\SSL is being used, the LDAP data signing option must be negotiated.

Note: Client side or CA certificate (CA cert) is not required for LDAPS. However, it would be an extra level of security of CA cert is uploaded to the Authentication Object.

6. Specify Attribute Mapping

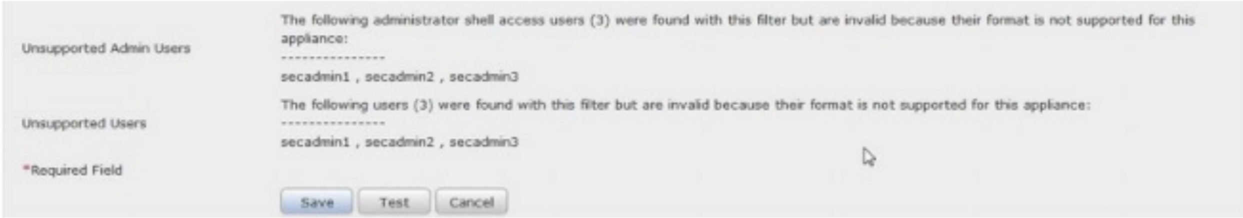
- ***UI Access Attribute***: sAMAccountName
- ***Shell Access Attribute***: sAMAccountName



Attribute Mapping

UI Access Attribute *	
Shell Access Attribute *	

Tip: If you encounter ***Unsupported Users*** message in the test output, change the ***UI Access Attribute*** to ***userPrincipalName*** and make sure ***User Name template*** is set to ***%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. Configure ***Group Controlled Access Roles***

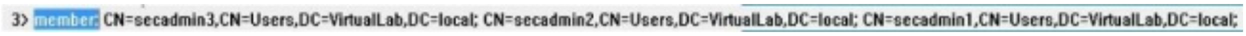
On ***ldp.exe***, browse to each groups and copy the corresponding group DN to the Authentication Object as shown below:

- ***<Group Name> Group DN: <group dn>***
- ***Group Member Attribute***: should always be ***member***

Example:

- ***Administrator Group DN:*** CN=DC admins,CN=Security Groups,DC=VirtualLab,DC=local
- ***Group Member Attribute***: member

An AD security group has an attribute of ***member*** followed by the DN of member users. The number preceding ***member*** attribute indicates the number of member users.



```
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;
```

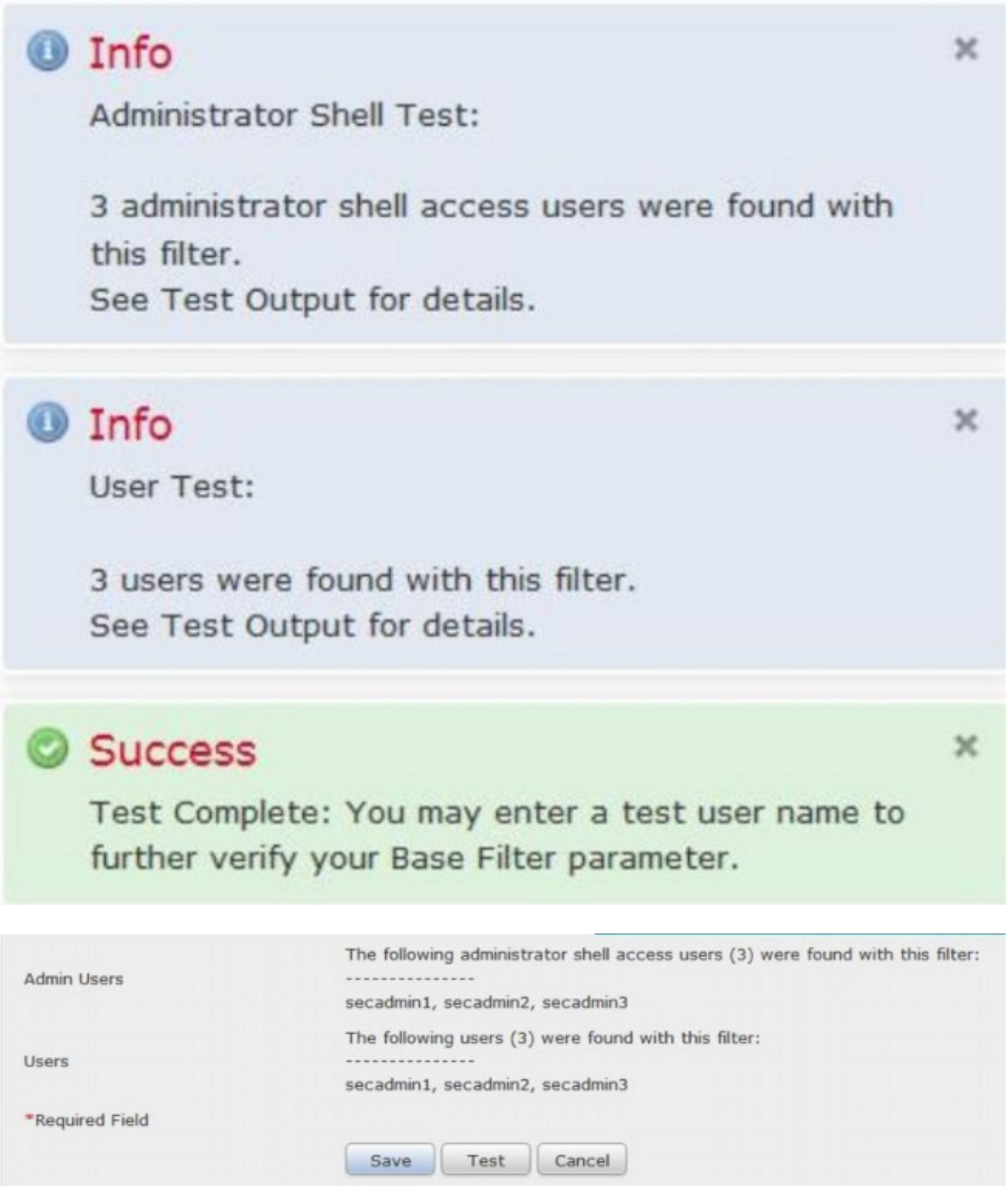
8. Select ***Same as Base Filter*** for Shell Access Filter, or specify memberOf attribute as indicated in step 5.

Shell Access Filter: (memberOf=<group DN>)

As example,

Shell Access Filter: (memberOf=CN=Shell users,CN=Security Groups,DC=VirtualLab,DC=local)

9. Save the Authentication Object and perform a test. A successful test result looks like below:



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

10. Once the Authentication Object passes the test, enable the object in the System Policy and reapply the policy to your appliance.

Related Document

- Identify Active Directory LDAP Object Attributes for Authentication Object Configuration

Updated: Jan 05, 2015 Document ID: 118738