

# LDAP认证对象的配置在FireSIGHT系统的

## 目录

[简介](#)

[LDAP认证对象的配置](#)

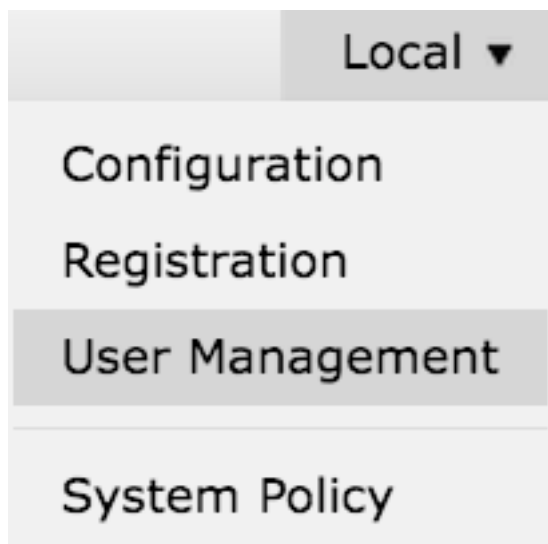
[相关文档](#)

## 简介

验证对象是外部验证服务器的服务器配置文件，包含连接设置和验证过滤器设置那些服务器的。您能创建，管理和删除在FireSIGHT管理中心的验证对象。本文描述如何配置在FireSIGHT系统的LDAP认证对象。

## LDAP认证对象的配置

1. 登陆对FireSIGHT管理中心的网页用户界面。
2. 导航对系统>本地>用户管理。



选择**登录认证**选项卡。



单击**创建验证对象**。

## Create Authentication Object

### 3. 选择认证方法和服务器类型。

- 认证方法：LDAP
- 名称：<Authentication对象Name>
- 服务器类型:MS活动目录

注意：菲尔茨标记用星号(\*)要求。

### Authentication Object

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

### 4. 指定主要和备份服务器主机名或IP地址。备份服务器可选。然而，在同一个域内的所有域控制器可以使用作为备份服务器。

注意：虽然LDAP端口是默认到端口389，您能使用LDAP服务器侦听的非标准端口号。

### 5. 指定LDAP特定参数如下所示：

提示：应该在配置LDAP特定参数之前识别用户、组和OU属性。读[本文](#)识别活动目录LDAP验证对象配置的对象属性。

- 根据DN -域或特定OU DN
- 基本过滤器-组DN用户是成员。
- 用户名- DC的模拟帐户
- 密码：<password>
- 确认密码：<password>

高级选项:

- 加密：SSL，TLS或者无
- SSL证书加载路径：上传CA证明(可选)
- 用户名模板：%s
- 超时(秒):30

**LDAP-Specific Parameters**

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

Base Filter  ex. (cn=jsmith), (|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)

在AD的域安全策略设置，如果LDAP服务器签署的需求设置要求签字，必须使用SSL或TLS。

### LDAP服务器签署的需求

- 无：数据签字没有要求为了用服务器绑定。如果签字的客户端要求数据，服务器支持它。
- **require签字**：除非使用TLS \ SSL，必须协商LDAP数据签署的选项。

**注意**：客户端或CA证书(CA cert)没有为LDAP要求。然而，它是一个额外的安全级别CA cert上传对验证对象。

### 6. 指定属性映射

- **UI访问属性**：sAMAccountName
- **Shell访问属性**：sAMAccountName

**Attribute Mapping**

UI Access Attribute \*

Shell Access Attribute \*

**提示**：如果在测验输出中遇到不支持的用户消息，请更改UI访问属性对userPrincipalName并且确保用户名模板设置为%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. 配置组被控制的访问角色

在ldp.exe给每组并且复制对应组DN于验证对象如下所示：

- <group name>组DN : <group dn>
- 组成员属性 : 应该总是成员

示例 :

- 管理员组DN : CN=DC admins , CN=Security组 , DC=VirtualLab , DC=local
- 组成员属性 : 成员

AD安全组安排成员属性跟随由成员用户DN。编号之前的成员属性指示成员用户数量。

```
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. 选择同Shell访问过滤器的基本过滤器一样或者如步骤5.所示指定memberOf属性。

**Shell访问过滤器** : (memberOf=<group DN>)

作为示例 ,

**Shell访问过滤器** : (memberOf=CN=Shell CN=Security DC=VirtualLab DC=local)

9. 保存验证对象并且执行测验。成功的测试检验结果看起来象如下 :



## 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. 一旦验证对象通过测验，请启用在系统策略的对象并且重新应用策略到您的设备。

## 相关文档

- [识别活动目录LDAP验证对象配置的对象属性](#)