

在FireSIGHT系統上配置LDAP身份驗證對象

目錄

[簡介](#)

[LDAP身份驗證對象的配置](#)

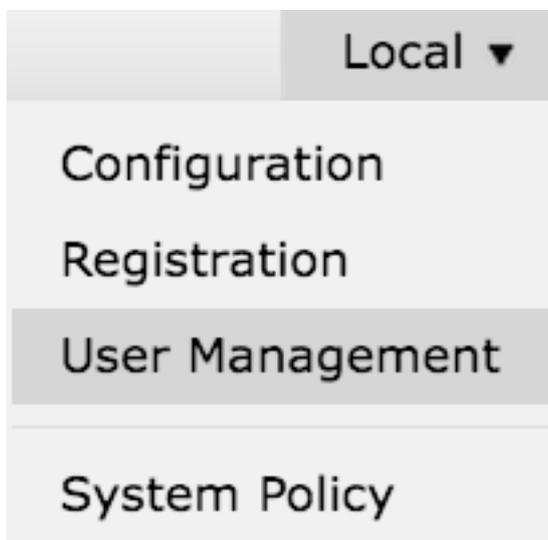
[相關檔案](#)

簡介

身份驗證對象是外部身份驗證伺服器的伺服器配置檔案，包含這些伺服器的連線設定和身份驗證過濾器設定。您可以在FireSIGHT管理中心上建立、管理和刪除身份驗證對象。本文檔介紹如何在FireSIGHT系統上配置LDAP身份驗證對象。

LDAP身份驗證對象的配置

1. 登入FireSIGHT管理中心的Web使用者介面。
2. 定位至系統>本地>使用者管理。



選擇Login Authentication選項卡。



按一下Create Authentication Object。

Create Authentication Object

3. 選擇 Authentication Method 和 Server Type。

- 驗證方法:LDAP
- 名稱:<身份驗證對象名稱>
- 伺服器型別:MS Active Directory

附註：標有星號(*)的欄位為必填欄位。

Authentication Object

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

4. 指定主伺服器和備份伺服器主機名或IP地址。備份伺服器是可選的。但是，同一域中的任何域控制器都可以用作備份伺服器。

附註：儘管LDAP埠預設為埠389，但您可以使用LDAP伺服器偵聽的非標準埠號。

5. 按以下所示指定LDAP特定引數：

提示：在配置LDAP特定引數之前應標識使用者、組和OU屬性。請閱讀[本文檔](#)，確定用於身份驗證對象配置的Active Directory LDAP對象屬性。

- 基本DN — 網域或特定OU DN
- Base Filter — 使用者所屬的組DN。
- 使用者名 - DC的模擬帳戶
- 密碼:<password>
- 確認密碼:<password>

高級選項：

- 加密:SSL、TLS或無
- SSL憑證上傳路徑:上傳CA認證 (可選)
- 使用者名稱模板:%s
- 超時 (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「域安全策略設定」中，如果LDAP伺服器簽名要求設定為**需要簽名**，則必須使用SSL或TLS。

LDAP伺服器簽名要求

- **無**:不需要資料簽名即可與伺服器繫結。如果客戶端請求資料簽名，伺服器將支援它。
- **需要簽名**:除非使用TLS\SSL，否則必須協商LDAP資料簽名選項。

附註：LDAPS不需要客戶端或CA證書 (CA證書)。但是，如果將CA證書上傳到身份驗證對象，則會有額外的安全級別。

6.指定屬性對映

- **UI訪問屬性**:sAMAccountName
- **外殼訪問屬性**:sAMAccountName

Attribute Mapping

UI Access Attribute *

Shell Access Attribute *

提示：如果在測試輸出中遇到不受支援的使用者消息，請將**UI Access Attribute**更改為**userPrincipalName**，並確保**User Name template**設定為**%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.配置組控制的訪問角色

在ldp.exe上，瀏覽到每個組，並將相應的組DN複製到身份驗證對象，如下所示：

- <Group Name>組DN:<group dn>
- 組成員屬性:應始終為成員

範例：

- 管理員組DN:CN=DC管理員，CN=安全組，DC=虛擬實驗室，DC=本地
- 組成員屬性:成員

AD安全組的屬性為**member**，後跟成員使用者的DN。**member**屬性前的number表示成員使用者的數量。

```
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.選擇**Same as Base Filter for Shell Access Filter**，或指定**memberOf**屬性（如步驟5所示）。

外殼訪問過濾器：(memberOf=<group DN>)

例如，

外殼訪問過濾器：(memberOf=CN=Shell使用者，CN=安全組，DC=虛擬實驗室，DC=本地)

9.儲存身份驗證對象並執行測試。成功的測試結果如下所示：



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. 身份驗證對象通過測試後，在「系統策略」中啟用該對象，並將策略重新應用到裝置。

相關檔案

- [確定身份驗證對象配置的Active Directory LDAP對象屬性](#)