

# FireSIGHT システムでの LDAP 認証オブジェクトの設定

## 目次

[はじめに](#)

[LDAP認証 オブジェクトの設定](#)

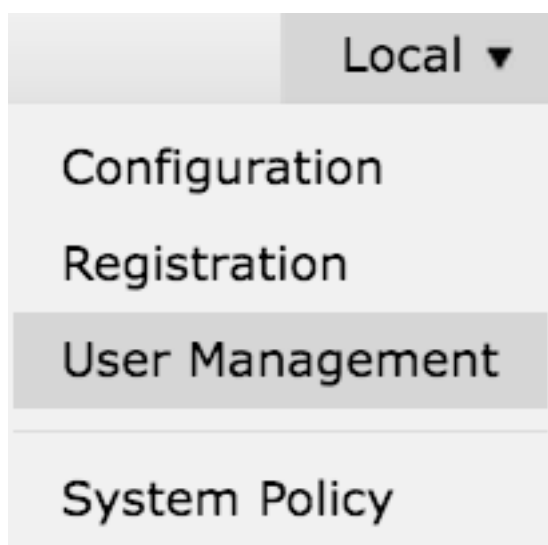
[関連資料](#)

## 概要

認証オブジェクトは外部認証サーバのためのサーバプロファイルで、それらのサーバの接続 設定 および認証フィルターの設定が含まれています。 FireSIGHT Management Center の認証オブジェクトを作成し、管理し、削除できます。この資料に FireSIGHT システムの LDAP認証 オブジェクトを設定する方法を記述されています。

## LDAP認証 オブジェクトの設定

1. FireSIGHT Management Center の Web ユーザ ユーザー・ インターフェースにログインして下さい。
2. システム > ローカル > ユーザマネージメントへのナビゲート。



ログイン認証タブを選択して下さい。



認証オブジェクトを『Create』をクリックして下さい。

## Create Authentication Object

3. 認証方式およびサーバタイプを選択して下さい。

- [Authentication Method] : LDAP
- [Name] : <Authentication オブジェクト Name>
- Server Type : MS アクティブ ディレクトリ

注: アスタリスクがついているフィールドが ( \* ) 必要となります。

### Authentication Object

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

4. プライマリ および バックアップ サーバ ホスト名か IP アドレスを規定して下さい。バックアップサーバはオプションです。ただし、同じドメイン内のどのドメインコントローラでもバックアップサーバと使用することができます。

注: LDAP ポートがポート 389 へデフォルトであるが、LDAPサーバが受信している標準外ポート番号を使用できます。

5. 下記に示されているように LDAP 仕様パラメータを規定して下さい:

ヒント : ユーザ、グループおよび OU 属性は LDAP 仕様パラメータを設定する前に識別する必要があります。認証 オブジェクト設定用のアクティブ ディレクトリ LDAP オブジェクト属性を識別するために[この資料](#)を読んで下さい。

- ベース DN -ドメインか仕様 OU DN
- 基礎フィルタ-ユーザがメンバーのことグループ DN。
- ユーザネーム- DC のための偽装アカウント
- password : <password>
- Confirm Password : <password>

詳細オプション:

- Encryption ( 暗号化 ) : SSL、TLS またはどれも
- SSL 証明書アップロードパス: CA 認証をアップロードして下さい ( オプションの )
- ユーザネーム テンプレート: %s
- タイムアウト ( 秒 ) : 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)

AD のドメイン セキュリティポリシー設定では、要件に設定される場合 SSL が TLS 署名する署名を必要とするために LDAPサーバが使用される。

### LDAPサーバ署名要件

- **None** : サーバによって結合 するためにデータ署名が必要となりません。 署名する Client 要求データがサーバそれをサポートすれば。
- **require 署名**: TLS \ SSL が使用されなければ、LDAP データ署名オプションはネゴシエートする必要があります。

注: クライアント側がか CA 認証 ( CA CERT ) は LDAPS に必要となりません。 ただし、それは認証 オブジェクトに CA 証明書の余分セキュリティレベル アップロードされます。

### 6. 属性マッピングを規定して下さい

- **UI アクセス属性**: sAMAccountName
- **シェル アクセス属性**: sAMAccountName

#### Attribute Mapping

UI Access Attribute \*

Shell Access Attribute \*

ヒント : テスト出力のサポートされていないユーザ メッセージが表示する場合、UI アクセス属性を userPrincipalName に変更し、ユーザネームが %s. にテンプレート設定されることを確かめて下さい

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

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. 群制御アクセスロールを設定して下さい

ldp.exe で各グループにコピーしまグループ DN を下記に示されているように認証 オブジェクトに対応します:

- <Group Name> グループ DN: <group dn>
- グループ メンバー属性: メンバーは常にあるはずです

例:

- 管理者グループ DN: CN=DC admin、CN=Security グループ、DC=VirtualLab、DC=local
- グループ メンバー属性: メンバー

AD セキュリティグループはメンバーの属性をメンバー ユーザの DN に先行させてもらいます。数先行するメンバー属性はメンバー ユーザの数を示します。

```
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. 同じを基礎フィルタとシェル アクセス フィルタ用に選択するか、またはステップ 5.に示すように memberOf 属性を規定して下さい。

シェル アクセス フィルタ: ( memberOf=<group DN> )

例として、

シェル アクセス フィルタ: memberOf=CN=Shell CN=Security DC=VirtualLabDC=local

9. 認証 オブジェクトを保存し、テストを行って下さい。下記にのように正常なテスト結果見え:



## 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. 認証 オブジェクトがテストに合格したら、システム ポリシーのオブジェクトを有効にし、アプライアンスにポリシーを再適用して下さい。

## 関連資料

- [認証オブジェクトに関する Active Directory LDAP オブジェクト属性の識別の設定](#)