

# FireSIGHT 시스템의 LDAP 인증 객체 컨피그레이션

## 목차

[소개](#)

[LDAP 인증 객체 구성](#)

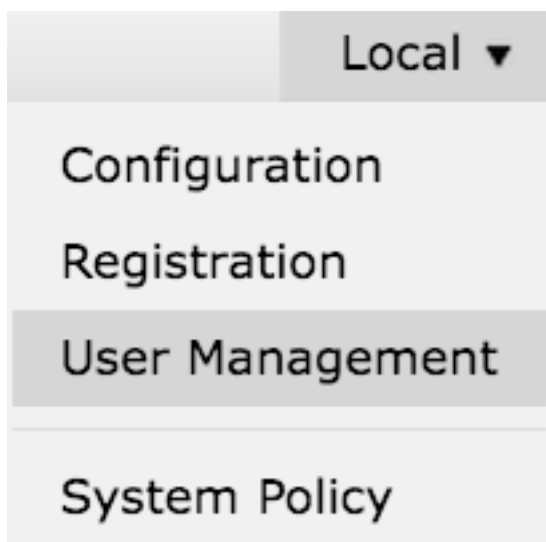
[관련 설명서](#)

## 소개

Authentication Objects(인증 객체)는 외부 인증 서버에 대한 서버 프로파일로서 해당 서버에 대한 연결 설정 및 인증 필터 설정을 포함합니다. FireSIGHT Management Center에서 인증 객체를 생성, 관리, 삭제할 수 있습니다. 이 문서에서는 FireSIGHT 시스템에서 LDAP 인증 객체를 구성하는 방법에 대해 설명합니다.

## LDAP 인증 객체 구성

1. FireSIGHT Management Center의 웹 사용자 인터페이스에 로그인합니다.
2. 시스템 > 로컬 > 사용자 관리로 이동합니다.



Login Authentication(로그인 인증) 탭을 선택합니다.



Create Authentication Object(인증 개체 생성)를 클릭합니다.



3. 인증 방법 및 서버 유형을 선택합니다.

- 인증 방법: LDAP
- 이름: <인증 개체 이름>
- 서버 유형: MS Active Directory

참고: 별표(\*)로 표시된 필드는 필수 항목입니다.

A screenshot of a web-based configuration form titled "Authentication Object" in red text. The form has a light gray background. It contains four rows of labels on the left and corresponding input fields on the right. The first row is "Authentication Method" with a dropdown menu showing "LDAP". The second row is "Name \*" with an empty text input field. The third row is "Description" with an empty text input field. The fourth row is "Server Type" with a dropdown menu showing "MS Active Directory".

4. 기본 및 백업 서버 호스트 이름 또는 IP 주소를 지정합니다. 백업 서버는 선택 사항입니다. 그러나 동일한 도메인 내의 모든 도메인 컨트롤러를 백업 서버로 사용할 수 있습니다.

참고: LDAP 포트는 기본적으로 포트 389이지만, LDAP 서버가 수신하는 비표준 포트 번호를 사용할 수 있습니다.

5. 아래와 같이 LDAP 관련 매개변수를 지정합니다.

팁: LDAP 관련 매개변수를 구성하기 전에 사용자, 그룹 및 OU 특성을 식별해야 합니다. 인증 객체 [컨피그레이션](#)을 위한 Active Directory LDAP 객체 속성을 식별하려면 이 문서를 읽으십시오.

- 기본 DN - 도메인 또는 특정 OU DN
- Base Filter - 사용자가 속한 그룹 DN입니다.
- 사용자 이름 - DC의 가장 계정
- 암호: <암호>
- 암호 확인: <암호>

고급 옵션:

- 암호화: SSL, TLS 또는 None
- SSL 인증서 업로드 경로: CA 인증 업로드(선택 사항)
- 사용자 이름 템플릿: %s
- 시간 초과(초): 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)

AD의 Domain Security Policy Setting(도메인 보안 정책 설정)에서 LDAP 서버 서명 요구 사항이 Require Signing(서명 필요)으로 설정된 경우 SSL 또는 TLS를 사용해야 합니다.

### LDAP 서버 서명 요구 사항

- **None:** 서버와 바인딩하기 위해 데이터 서명이 필요하지 않습니다. 클라이언트가 데이터 서명을 요청하면 서버에서 이를 지원합니다.
- **서명 필요:** TLS\SSL을 사용하지 않는 경우 LDAP 데이터 서명 옵션을 협상해야 합니다.

**참고:** LDAPS에는 클라이언트측 또는 CA 인증서(CA 인증서)가 필요하지 않습니다. 그러나 CA 인증서가 인증 객체에 업로드되는 보안 수준이 더 높습니다.

### 6. 속성 매핑 지정

- **UI 액세스 특성:** 계정 이름
- **셸 액세스 특성:** 계정 이름

**Attribute Mapping**

UI Access Attribute \*

Shell Access Attribute \*

**팁:** 테스트 출력에서 지원되지 않는 사용자 메시지가 나타나면 **UI Access Attribute(UI 액세스 특성)**를 **userPrincipalName**으로 변경하고 **User Name(사용자 이름) 템플릿**이 **%s(으)**로 설정되어 있는지 확인하십시오.

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. 그룹 제어 액세스 역할 구성

ldp.exe에서 각 그룹을 찾아 아래에 표시된 대로 해당 그룹 DN을 인증 객체에 복사합니다.

- <그룹 이름> 그룹 DN: <그룹 dn>
- 그룹 구성원 특성: 항상 멤버

예:

- 관리자 그룹 DN: CN=DC 관리자,CN=보안 그룹,DC=VirtualLab,DC=로컬
- 그룹 구성원 특성: 멤버

AD 보안 그룹은 member 속성 뒤에 **member** 사용자의 DN이 옵니다. number preceding member 특성은 멤버 사용자 수를 나타냅니다.

```
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. 셸 액세스 필터에 대한 기본 필터와 동일 을 선택하거나 단계 5에 표시된 대로 memberOf 특성을 지정합니다.

셸 액세스 필터: (memberOf=<그룹 DN>)

예를 들어

셸 액세스 필터: (memberOf=CN=셸 사용자,CN=보안 그룹,DC=VirtualLab,DC=로컬)

9. 인증 객체를 저장하고 테스트를 수행합니다. 테스트 결과는 다음과 같습니다.



## 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. 인증 객체가 테스트를 통과하면 시스템 정책에서 객체를 활성화하고 어플라이언스에 정책을 다시 적용합니다.

## 관련 설명서

- [인증 객체 구성을 위한 Active Directory LDAP 객체 속성 식별](#)