디바이스 사용자 계정

매니지드 디바이스는 CLI 액세스에 대한 기본 관리자 계정을 포함합니다. 이 장에서는 맞춤형 사용자 계정을 생성하는 방법을 설명합니다. 매니지드 디바이스에 사용자 계정으로 로그인하는 방법에 대한 자세한 내용은 Firepower System에 로그인에서 확인할 수 있습니다.

디바이스 사용자 계정 정보

매니지드 디바이스에서 맞춤형 사용자 계정을 내부 사용자로 추가할 수 있으며, FTD의 경우 LDAP 또는 RADIUS 서버에 외부 사용자로 추가할 수 있습니다. 매니지드 디바이스 각각은 별도 사용자 계정을 유지 관리합니다. 예를 들어 사용자를 FMC에 추가하는 경우, 해당 사용자만 FMC에 액세스할 수 있습니다. 해당 사용자 이름을 사용해 매니지드 디바이스에 직접 로그인할 수 없습니다. 매니지드 디바이스에서 사용자를 별도로 추가해야 합니다.

내부 및 외부 사용자

매니지드 디바이스는 두 가지 유형의 사용자를 지원합니다.

- 내부 사용자—디바이스는 사용자 인증을 위해 로컬 데이터베이스를 검사합니다. 내부 사용자에 대한 자세한 내용은 CLI에서 내부 사용자 추가, 3 페이지을 참조하십시오. FTD, NGIPSv 및 ASA FirePOWER는 내부 사용자를 지원합니다.
- 외부 사용자(FTD만 해당) - 사용자가 로컬 데이터베이스에 없는 경우, 시스템이 외부 LDAP 또는 RADIUS 인증 서버에 쿼리합니다. 외부 사용자에 대 한 자세한 내용은 FTD에 대한 외부 인증 구성, 5 페이지을 참조하십시오. FTD만 외부 사용자를 지원합니다.

CLI 액세스

Firepower 디바이스는 Linux에서 실행되는 Firepower CLI를 포함합니다. CLI를 사용하여 디바이스에서 내부 사용자를 생성할 수 있습니다. FMC를 통해 FTD 디바이스에서 외부 사용자를 설정할 수 있습니다. 관리 UI에 대한 자세한 내용은 Firepower System 유저 인터페이스을 참조하십시오.

⚠

주의 CLI 설정 레벨 액세스 권한이 있는 사용자는 **expert** 명령을 사용하여 Linux 셸에 액세스하고 Linux 셸에서 `sudoers` 권한을 얻을 수 있으며, 따라서 보안 위험이 발생할 수 있습니다. 시스템 보안을 위해 다음을 적극 권장합니다.

- TAC 감독하에 있거나 Firepower 사용자 설명서에서 명시적으로 지시한 경우에만 Linux 셸을 사용하십시오.
- CLI 액세스 권한이 있는 사용자 목록을 적절하게 제한해야 합니다.
- CLI 액세스 권한을 부여하는 경우, 구성 레벨 액세스로 사용자 목록을 제한합니다.
- Linux 셸에서 바로 사용자를 추가하지 마십시오. 이 장에서 설명하는 절차만 사용해야 합니다.
- Cisco TAC가 지시하거나 Firepower 사용자 설명서에서 명시적으로 지시하지 않는 한, CLI 전문가 모드를 이용하여 Firepower 디바이스에 액세스해서는 안 됩니다.

CLI 사용자 역할

매지니드 디바이스의 경우, CLI에서의 명령에 대한 사용자 액세스는 할당하는 역할에 따라 달라집니다.

None

ㅈ사용자는 명령줄에서 디바이스에 로그인할 수 없습니다.

Config(컨피그레이션**)**

사용자는 구성 명령을 비롯하여 모든 명령에 액세스할 수 있습니다. 사용자에게 이 액세스 수준을 할당할 때는 각별히 주의하십시오.

기본

사용자는 비구성 명령에만 액세스할 수 있습니다. 내부 사용자 및 FTD 외부 RADIUS 사용자만 기본 역할을 지원합니다.

디바이스의 사용자 계정에 대한 요구 사항 및 사전 요건

모델 지원

- FTD내부 및 외부 사용자
- ASA FirePOWER내부 사용자

- NGIPSv내부 사용자

지원되는 도메인

모든

사용자 역할

외부 사용자 구성- 관리자 FMC 사용자

내부 사용자 구성-CLI 사용자 구성

디바이스 사용자 계정을 위한 지침 및 제한 사항

기본값

모든 디바이스는 로컬 사용자 어카운트로 관리자 사용자를 포함합니다. 관리자 사용자는 삭제할 수 없습니다. 기본 초기 비밀번호는 **Admin123**입니다. 시스템은 초기화 프로세스 중에 비밀번호를 변경하게 합니다. 시스템 초기화에 관한 자세한 내용은 모델에 맞는 시작 가이드를 참조하십시오.

CLI에서 내부 사용자 추가

CLI를 사용하여 FTD, ASA FirePOWER 및 NGIPSv 디바이스에서 내부 사용자를 생성합니다.

프로시저

단계 **1** Config(구성) 권한이 있는 계정을 사용하여 디바이스 CLI에 로그인합니다.

관리자 사용자 어카운트가 필수 권한을 갖고 있지만, Config(구성) 권한이 있는 모든 어카운트에도 작동합니다. SSH 세션 또는 콘솔 포트를 사용할 수 있습니다.

특정 FTD 모델의 경우, 콘솔 포트는 사용자를 FXOS CLI에 연결합니다. FTD CLI로 이동하려면 **connect ftd** 명령을 사용하십시오.

단계 **2** 사용자 계정을 생성합니다.

configure user add *username* {**basic** | **config**}

- *username(*사용자 이름*)* - 사용자 이름을 설정합니다. 사용자 이름은 다음과 같은 Linux 기준을 준수해야 합니다.
  - 최대 32개의 영숫자 문자와 하이픈(-) 및 밑줄(_)
  - 모두 소문자
  - 하이픈(-)으로 시작할 수 없으며, 숫자만으로 구성할 수 없고, 마침표(.), 단가 기호(@) 또는 슬래시(/)를 포함할 수 없음

- **basic**- 사용자에게 기본 액세스 권한을 제공합니다. 이 역할은 사용자가 구성 명령을 입력하는 것을 허용하지 않습니다.
- **config**- 사용자에게 컨피그레이션 액세스 권한을 제공합니다. 이 역할은 사용자에게 모든 명령에 대한 전체 관리자 권한을 제공합니다.

예제:

다음 예에서는 Config(구성) 액세스 권한이 있는 johncrichton이라는 이름의 사용자 어카운트를 추가합니다. 입력하고 있으므로 비밀번호가 표시되지 않습니다.

```
> configure user add johncrichton config
Enter new password for user johncrichton: newpassword
Confirm new password for user johncrichton: newpassword
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
johncrichton      1001  Local Config  Enabled    No  Never  N/A  Dis   No   5
```

참고 **configure password** 명령을 사용하여 비밀번호를 변경할 수 있다고 사용자에게 알려줍니다.

단계 **3** (선택 사항) 보안 요건을 충족하도록 어카운트의 특성을 조정합니다.

다음 명령을 사용하여 기본 어카운트 동작을 변경할 수 있습니다.

- **configure user aging** *username max_days warn_days*

  사용자 비밀번호의 만료일을 설정합니다. 비밀번호가 유효한 최대 일수를 지정한 후 며칠 전부터 사용자에게 다가오는 만료일에 대해 경고할지 일수를 지정합니다. 두 값 모두 1~9999 범위이지만, 경고 일수는 최대 일수보다 작아야 합니다. 어카운트를 생성할 때 비밀번호 만료일이 없습니다.

- **configure user forcereset** *username*

  사용자가 다음 로그인 시 강제로 비밀번호를 변경하게 합니다.

- **configure user maxfailedlogins** *username number*

  어카운트를 잠그기 전에 허용되는 연속 실패 로그인의 최대 수를 1~9999 범위로 설정합니다. 계정의 잠금을 해제하려면 **configure user unlock** 명령을 사용하십시오. 새 어카운트에 대한 기본값은 로그인 5회 연속 실패입니다.

- **configure user minpasswdlen** *username number*

  최소 비밀번호 길이를 1~127 범위로 설정합니다.

- **configure user strengthcheck** *username* {**enable** | **disable**}

  비밀번호 강도 검사를 활성화하거나 비활성화합니다. 이 경우 비밀번호를 변경할 때 사용자는 특정 비밀번호 기준을 충족해야 합니다. 사용자의 암호가 만료되거나 **configure user forcereset** 명령을 사용하는 경우, 이 요건은 사용자가 다음번 로그인할 때 자동으로 활성화됩니다.

단계 **4** 필요 시 사용자 어카운트를 관리합니다.

사용자가 자신의 어카운트를 잠글 수 있게 하거나, 어카운트를 제거하거나 다른 문제를 해결해야 합니다. 시스템에서 사용자 어카운트를 관리하려면 다음 명령을 사용합니다.

- **configure user access** *username* {**basic** | **config**}

  사용자 어카운트에 대한 권한을 변경합니다.

- **configure user delete** *username*

  지정된 어카운트를 삭제합니다.

- **configure user disable** *username*

  지정된 어카운트를 삭제하지 않고 비활성화합니다. 사용자는 어카운트를 활성화할 때까지 로그인할 수 없습니다.

- **configure user enable** *username*

  지정된 어카운트를 활성화합니다.

- **configure user password** *username*

  지정된 사용자에 대한 비밀번호를 변경합니다. 사용자는 일반적으로 **configure password** 명령을 사용하여 자신의 암호를 변경해야 합니다.

- **configure user unlock** *username*

  연속 실패 로그인 시도의 최대 횟수를 초과하므로 잠겨 있는 사용자 어카운트의 잠금을 해제합니다.

FTD에 대한 외부 인증 구성

FTD 디바이스에 대한 외부 인증을 활성화하려면 하나 이상의 외부 인증 개체를 추가해야 합니다.

FTD 외부 인증 정보

FTD 사용자에 대해 외부 인증을 사용하도록 설정하면 FTD는 외부 인증 개체에 지정된 LDAP 또는 RADIUS 서버를 사용하여 사용자 자격 증명을 확인합니다.

외부 인증 개체는 FMC 및 FTD 디바이스가 사용할 수 있습니다. 다양한 어플라이언스/디바이스 유형 간에 동일한 개체를 공유하거나 별도 개체를 생성할 수 있습니다. FTD의 경우, 디바이스에 구축하는 플랫폼 설정에서 하나의 외부 인증 개체만 활성화할 수 있습니다.

참고 시간 제한 범위는 FTD와 FMC가 다르므로 개체를 공유할 때는 FTD의 더 적은 시간 제한 범위(LDAP의 경우 1~30초, RADIUS의 경우 1~300초)를 초과하지 않아야 합니다. 시간 초과 값을 더 높은 값으로 설정하면 FTD 외부 인증 설정이 작동하지 않습니다.

참고 FTD 가상 디바이스에서 외부 인증은 지원되지 않습니다.

외부 인증 개체에서 필드 하위 집합만 FTD SSH 액세스에 사용됩니다. 다른 필드를 입력하는 경우, 해당 필드는 무시됩니다. 이 개체를 다른 디바이스 유형에 사용하는 경우, 해당 필드가 사용됩니다.

LDAP 사용자는 항상 Config(구성) 권한을 갖습니다. RADIUS 사용자는 Config(구성) 또는 Basic(기본) 사용자로 정의할 수 있습니다.

RADIUS 서버(Service-Type(서비스 유형) 속성)에서 사용자를 정의하거나 외부 인증 개체에서 사용자 목록을 미리 정의할 수 있습니다. LDAP의 경우, 필터를 지정하여 LDAP 서버의 CLI 사용자와 매칭할 수 있습니다.

참고 Linux 셸 액세스 권한이 있는 사용자는 루트 권한을 얻을 수 있으며, 따라서 보안 위험이 발생할 수 있습니다. 다음을 확인하십시오.

- Linux 셸 액세스 권한이 있는 사용자 목록 제한
- Linux 셸 사용자를 생성 금지

LDAP 정보

LDAP(Lightweight Directory Access Protocol)를 사용하면 중앙의 한 위치에 개체(예: 사용자 크리덴셜)를 조직하는 네트워크에서 디렉토리를 설정할 수 있습니다. 그러면 여러 애플리케이션에서 이 크리덴셜 및 크리덴셜 설명에 사용된 정보에 액세스할 수 있습니다. 사용자 크리덴셜을 변경해야 하는 경우, 한 곳에서 변경할 수 있습니다.

Microsoft는 Active Directory 서버가 2020년에 LDAP 바인딩 및 LDAP 서명을 시행할 것이라고 발표했습니다. Microsoft는 이러한 설정을 기본 설정으로 사용할 때 Microsoft Windows에 권한 상승 취약점이 존재하여 MITM(man-in-the-middle) 공격자가 Windows LDAP 서버에 인증 요청을 성공적으로 전달할 수 있기 때문에 이러한 요구 사항을 적용하고 있습니다. 자세한 내용은 Microwoft 지원 사이트에서 2020 LDAP 채널 바인딩 및 Windows용 LDAP 서명 요구 사항을 참조하십시오.

아직 수행하지 않은 경우 TLS/SSL 암호화를 사용하여 Active Directory 서버에서 인증을 시작하는 것이 좋습니다.

RADIUS 정보

RADIUS(Remote Authentication Dial In User Service)는 네트워크 리소스에 대한 사용자 액세스의 인증, 권한 부여, 어카운팅에 사용되는 인증 프로토콜입니다. RFC 2865를 준수하는 모든 RADIUS 서버에 대해 인증 개체를 생성할 수 있습니다.

Firepower 디바이스는 SecurID 토큰 사용을 지원합니다. SecurID를 사용하여 서버에서 인증을 구성하는 경우, 해당 서버에서 인증된 사용자는 SecurID PIN 끝에 SecurID 토큰을 추가하고 이를 로그인 비밀번호로 사용합니다. SecurID를 지원하기 위해 Firepower 디바이스에서 추가로 구성할 사항은 없습니다.

FTD에 대한 LDAP 외부 인증 개체 추가

FTD 관리를 위해서 외부 사용자를 지원할 수 있도록 LDAP 서버를 추가합니다.

다중 도메인 구축에서 외부 인증 개체는 생성된 도메인에서만 사용할 수 있습니다.

외부 인증 객체 공유

외부 LDAP 개체는 FMC 및 FTD 디바이스가 사용할 수 있습니다. FMC 및 디바이스 간에 동일한 개체를 공유하거나 별도 개체를 생성할 수 있습니다.

참고 LDAP의 경우 FTD와 FMC의 시간 제한 범위가 다르므로 개체를 공유하는 경우 FTD의 더 작은 시간 제한 범위(1 ~ 30초)를 초과하지 않아야 합니다. 시간 초과 값을 더 높은 값으로 설정하면 FTD에 대한 구축이 실패합니다.

FTD 지원되는 필드

LDAP 개체에서 필드 하위 집합만 FTD SSH 액세스에 사용됩니다. 다른 필드를 입력하는 경우, 해당 필드는 무시됩니다. 이 개체를 FMC에 사용하는 경우, 해당 필드가 사용됩니다. 이 절차는 FTD에 대한 지원되는 필드만 적용합니다. 다른 필드는 FMC에 대한 LDAP 외부 인증 개체 추가 섹션을 참조하십시오.

사용자 이름

사용자 이름은 Linux에서 유효한 사용자 이름이어야 하며 소문자로 된 영숫자에 마침표(.) 또는 하이픈(-)을 사용해야 합니다. at 기호(@) 및 사선(/) 등 다른 특수 문자는 지원되지 않습니다. 외부 인증에 대한 관리자 사용자를 추가할 수 없습니다. 외부 사용자만 외부 인증 객체의 일부로 FMC에서 추가할 수 있습니다. CLI에서는 추가할 수 없습니다. 내부 사용자는 FMC가 아닌 CLI에서만 추가할 수 있습니다.

내부 사용자에 대해 **configure user add** 명령을 사용하여 동일한 사용자 이름을 구성한 경우, FTD가 우선 내부 사용자에 대해 비밀번호를 확인하고 실패한 경우 LDAP 서버를 확인합니다. 참고로 외부 사용자와 이름이 같은 내부 사용자를 나중에 추가할 수 없습니다. 기존 내부 사용자만 지원됩니다.

권한 레벨

LDAP 사용자는 항상 Config(구성) 권한을 갖습니다.

시작하기 전에

해당 장치에서 도메인 이름 조회를 위해 DNS 서버를 지정해야 합니다. 이 절차에서 IP 주소는 지정하고 LDAP 서버에 대한 호스트 이름은 지정하지 않더라도, LDAP 서버는 인증을 위한 URI를 반환할 수 있으며 여기에는 호스트 이름이 포함됩니다. 호스트 이름을 지정하려면 DNS 조회가 필요합니다. CLI에서 디바이스 관리 인터페이스 수정를 참조하고 DNS 서버를 추가합니다.

프로시저

단계 **1** **System(**시스템**)** > **Users(**사용자**)**을 선택합니다.

단계 **2** **External Authentication(**외부 인증**)** 탭을 클릭합니다.

단계 **3** **Add External Authentication Object(**외부 인증 개체 추가**)**를 클릭합니다.

단계 **4** **Authentication Method(**인증 방법**)**을 **LDAP**로 설정합니다.

단계 **5** **Name(**이름**)**과 **Description(**설명**)**(선택 사항)을 입력합니다.

단계 **6** 드롭다운 목록에서 **Server Type(**서버 유형**)**을 선택합니다.

단계 **7** **Primary Server(**기본 서버**)**에 **Host Name/IP Address(**호스트 이름**/IP** 주소**)**를 입력합니다.

TLS 또는 SSL을 통한 연결에 인증서를 사용하는 경우 인증서의 호스트 이름이 이 필드에 사용된 호스트 이름과 일치해야 합니다. 또한 IPv6 주소는 암호화된 연결이 지원되지 않습니다.

단계 **8** (선택 사항) **Port(**포트**)**를 기본값에서 변경합니다.

단계 **9** (선택 사항) **Backup Server(**백업 서버**)** 파라미터를 입력합니다.

단계 **10** **LDAP-Specific Parameters(LDAP** 전용 파라미터**)**를 입력합니다.

a) 액세스를 원하는 LDAP 디렉터리에 대해 **Base DNs(**기본 **DN)**를 입력합니다. 예를 들어, 예시 회사의 보안 조직에서 이름을 인증하려면 `ou=security,dc=example,dc=com`을 입력합니다. 아니면 **Fetch DN(DN** 가져오기**)**을 클릭하고, 드롭다운 목록에서 적절한 기본 고유 이름을 선택합니다.

b) (선택 사항) **Base Filter(**기본 필터**)**를 입력합니다. 예를 들어 디렉토리 트리의 사용자 개체에 `physicalDeliveryOfficeName` 속성이 있고 a뉴욕 사무실의 사용자는 그 속성 값이 `NewYork`인 경우 뉴욕 사무실의 사용자만 가져오려면 `(physicalDeliveryOfficeName=NewYork)`이라고 입력합니다.

c) LDAP 서버를 검색하기에 크리덴셜이 충분한 사용자의 경우, **User Name(**사용자 이름**)**을 입력합니다. 예를 들어 OpenLDAP 서버에 연결하려는 경우, 해당 사용자 개체에 `uid` 속성이 있으며 예시 회사 보안 부서 관리자 개체의 `uid`값이 `NetworkAdmin`이라면 `uid=NetworkAdmin,ou=security,dc=example,dc=com`과 같이 입력할 수 있습니다.

d) **Password(**비밀번호**)** 및 **Confirm Password(**비밀번호 확인**)** 필드에 사용자 비밀번호를 입력합니다.

e) (선택 사항) **Show Advanced Options(**고급 옵션 표시**)**를 클릭하고 다음 고급 옵션을 구성합니다.

- **Encryption(**암호화**)- None (**해당 없음**)**, **TLS**또는 **SSL**을 클릭 합니다.

  포트를 지정한 다음 암호화 방식을 변경할 경우, 그 방법에 대해서는 포트가 기본값으로 재설정됩니다. **None(**해당 없음**)** 또는 **TLS**인 경우, 포트는 기본값인 389로 재설정됩니다. SSL 암호화를 선택할 경우 포트는 636로 재설정됩니다.

- **SSL Certificate Upload Path(SSL** 인증서 업로드 경로**)**—SSL 또는 TLS 암호화인 경우, **Choose File(**파일 선택**)**을 클릭하여 인증서를 선택해야 합니다.

  이전에 업로드한 인증서를 대체하려는 경우, 새 인증서를 업로드하고 구성을 디바이스에 다시 적용하여 새 인증서로 복사합니다.

  참고 TLS 암호화는 모든 플랫폼에서 인증서가 필요합니다. SSL의 경우, FTD도 인증서가 필요합니다. 다른 플랫폼의 경우, SSL은 인증서가 필요하지 않습니다. 그러나 항상 끼어들기 공격을 방지하기 위해 SSL에 대한 인증서를 업로드하는 것이 좋습니다.

- (사용되지 않음) **User Name Template(**사용자 이름 템플릿**)** - FTD에서 사용되지 않습니다.

- **Timeout(**시간 초과**)**—백업 연결로 전환하기 전 시간(초)을 1과 30 사이로 입력합니다. 기본값은 30입니다.

  참고 시간 제한 범위는 FTD와 FMC에 따라 다르므로 개체를 공유하는 경우 FTD의 더 작은 시간 제한 범위 (1 ~ 30초)를 초과하지 않아야 합니다. 시간 초과 값을 더 높은 값으로 설정하면 FTD LDAP 구성이 작동하지 않습니다.

단계 **11** (선택 사항) 사용자 고유 유형 이외의 쉘(shell) 액세스 속성을 사용하려는 경우 **CLI Access Attribute(CLI** 액세스 속성**)**를 입력합니다. 예를 들어 Microsoft Active Directory Server에서 `sAMAccountName` 쉘 액세스 속성을 사용하여 쉘 액세스 사용자를 가져오려면 `sAMAccountName`을 **CLI Access Attribute(CLI** 액세스 속성**)** 필드에 입력합니다.

단계 **12** **CLI Access Filter(CLI** 액세스 필터**)**를 설정합니다.

다음 방법 중 하나를 선택합니다.

- 인증 설정을 구성할 때 지정한 것과 동일한 필터를 사용하려면 **Same as Base Filter(**기본 필터와 동일**)**를 선택합니다.
- 속성 값에 따라 관리자 사용자 엔트리를 검색하려면 속성 이름, 비교 연산자, 필터로 사용할 속성 값을 괄호로 묶어 입력합니다. 예를 들어 모든 네트워크 관리자에게 `manager` 속성이 있고 그 값이 `shell`이라면 `(manager=shell)`이라는 기본 필터를 설정할 수 있습니다.

사용자 이름은 다음과 같은 Linux 기준을 준수해야 합니다.

- 최대 32개의 영숫자 문자와 하이픈(-) 및 밑줄(_)
- 모두 소문자
- 하이픈(-)으로 시작할 수 없으며, 숫자만으로 구성할 수 없고, 마침표(.), 단가 기호(@) 또는 슬래시(/)를 포함할 수 없음

참고 내부 사용자에 대해 동일한 사용자 이름을 구성한 경우, FTD가 우선 내부 사용자에 대해 비밀번호를 확인하고 실패한 경우 LDAP 서버를 확인합니다. 참고로 외부 사용자와 이름이 같은 내부 사용자를 나중에 추가할 수 없습니다. 기존 내부 사용자만 지원됩니다.

단계 **13** **Save(**저장**)**를 클릭합니다.

단계 **14** 이 서버의 사용을 활성화합니다. SSH에 대한 외부 인증 설정의 내용을 참조하십시오.

단계 **15** LDAP 서버에서 사용자를 나중에 추가 또는 삭제한다면, 사용자 목록을 새로 고침하고 매니지드 디바이스에 대한 Platform Settings(플랫폼 설정)를 재구축해야 합니다.

a) 각 LDAP 서버 옆에 새로 로침( )를 클릭합니다.

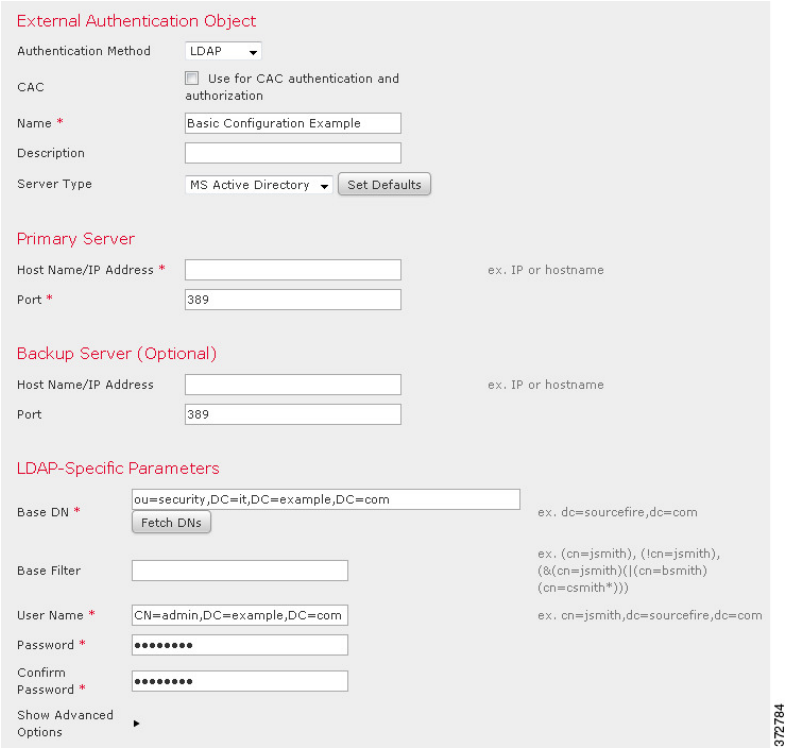
사용자 목록을 변경하는 경우, 디바이스에 대한 구성 변경을 구축하라는 메시지가 표시됩니다.

b) 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

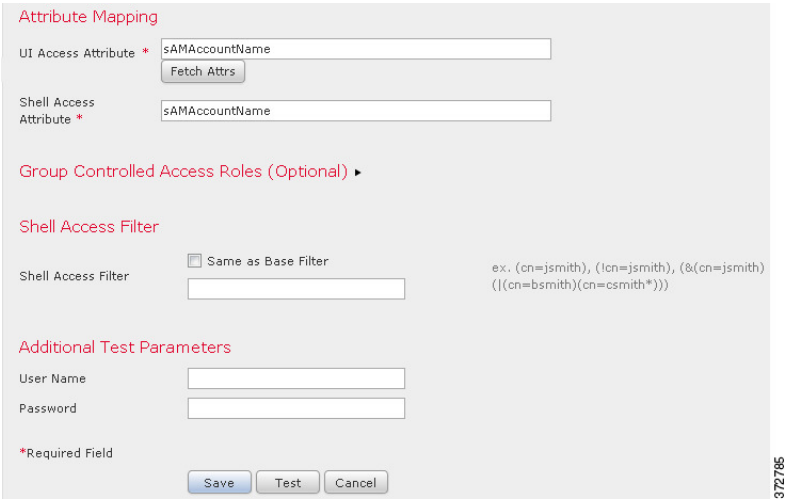
예

기본 예시

다음 그림은 Microsoft Active Directory Server를 위한 LDAP 로그인 인증 개체의 기본 구성입니다. 여기서 LDAP 서버의 IP 주소는 10.11.3.4입니다. 이 연결은 포트 389을 액세스에 사용합니다.



이 예는 예시 회사의 정보 기술 도메인에 있는 보안 조직에 대해 `OU=security,DC=it,DC=example,DC=com`이라는 기본 DN을 사용하는 연결을 보여줍니다.

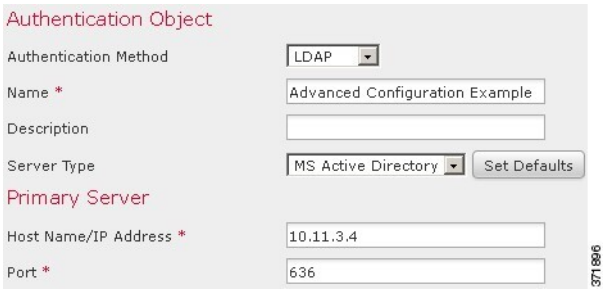


또한 Shell Access Attribute(셸 액세스 속성)가 `sAMAccountName`이면 사용자가 FTD에 로그인할 때 디렉토리의 모든 개체에 대해 각 `sAMAccountName` 속성을 검사하여 매칭하는지 확인합니다.

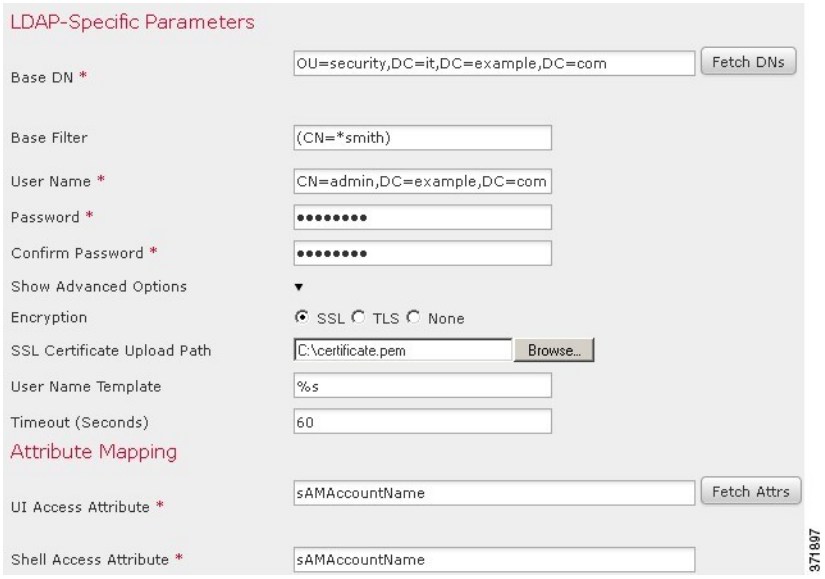
이 서버에는 기본 필터가 적용되지 않으므로 FTD에서는 기본 DN이 나타내는 디렉토리의 모든 개체에 대해 속성을 검사합니다. 기본 기간(또는 LDAP 서버에 설정된 시간 초과 기간)이 경과하면 서버와의 연결이 시간 초과됩니다.

고급 예시

이 예에서는 Microsoft Active Directory Server에 대한 LDAP 로그인 인증 개체의 고급 구성을 보여줍니다. 여기서 LDAP 서버의 IP 주소는 10.11.3.4입니다. 이 연결은 포트 636을 액세스에 사용합니다.



이 예는 예시 회사의 정보 기술 도메인에 있는 보안 조직에 대해 `OU=security,DC=it,DC=example,DC=com`이라는 기본 DN을 사용하는 연결을 보여줍니다. 그러나 이 서버는 기본 필터 `(cn=*smith)`가 있습니다. 이 필터는 CN이 `smith`로 끝나는 사용자만 서버에서 가져오도록 제한합니다.



서버와의 연결은 SSL로 암호화되고 `certificate.pem`이라는 인증서가 연결에 사용됩니다. 또한 **Timeout(**시간 초과**)** 설정 때문에 60초가 지나면 서버와의 연결이 시간 초과됩니다.

이 서버는 Microsoft Active Directory Server이므로 `sAMAccountName` 속성을 사용해 사용자 이름을 저장하며 `uid` 속성을 사용하지 않습니다.

또한 Shell Access Attribute(셸 액세스 속성)가 `sAMAccountName`이면 사용자가 FTD에 로그인할 때 디렉토리의 모든 개체에 대해 각 `sAMAccountName` 속성을 검사하여 매칭하는지 확인합니다.

다음 예에서 셸 액세스 필터는 기본 필터와 동일하게 설정됩니다.

FTD에 대한 RADIUS 외부 인증 개체 추가

FTD에 대한 RADIUS 서버를 추가하고 외부 사용자를 지원합니다.

다중 도메인 구축에서 외부 인증 개체는 생성된 도메인에서만 사용할 수 있습니다.

외부 인증 객체 공유

FMC 및 디바이스 간에 동일한 개체를 공유하거나 별도 개체를 생성할 수 있습니다. FTD에서는 RADIUS 서버에서 사용자를 정의하는 것을 지원하지만, FMC에서는 외부 인증 객체에 사용자 목록을 미리 정의해야 합니다. FTD에 대해 사전 정의된 목록 방법을 사용하도록 선택할 수 있지만, RADIUS 서버에서 사용자를 정의하려면 FTD 및 FMC에 대해 별도의 개체를 만들어야 합니다.

참고 시간 제한 범위는 FTD와 FMC에서 서로 다르므로 개체를 공유하는 경우 FTD의 더 작은 시간 제한 범위(1 ~ 300초)를 초과하지 않아야 합니다. 시간 초과 값을 더 높은 값으로 설정하면 FTD RADIUS 구성이 작동하지 않습니다.

FTD 지원되는 필드

RADIUS 개체에서 필드 하위 집합만 FTD SSH 액세스에 사용됩니다. 다른 필드를 입력하는 경우, 해당 필드는 무시됩니다. 이 개체를 FMC에 사용하는 경우 해당 필드가 사용됩니다. 이 절차는 FTD에 대한 지원되는 필드만 적용합니다. 다른 필드는 FMC에 대한 RADIUS 외부 인증 개체 추가 섹션을 참조하십시오.

사용자 이름

외부 인증에 대한 관리자 사용자를 추가할 수 없습니다. 외부 사용자만 외부 인증 객체의 일부로 FMC에서 추가할 수 있습니다. CLI에서는 추가할 수 없습니다. 내부 사용자는 FMC가 아닌 CLI에서만 추가할 수 있습니다.

내부 사용자에 대해 **configure user add** 명령을 사용하여 동일한 사용자 이름을 구성한 경우, FTD가 우선 내부 사용자에 대해 비밀번호를 확인하고 실패한 경우 RADIUS 서버를 확인합니다. 참고로 외부 사용자와 이름이 같은 내부 사용자를 나중에 추가할 수 없습니다. 기존 내부 사용자만 지원됩니다. RADIUS 서버에 정의된 사용자의 경우 권한 수준을 모든 내부 사용자와 동일하게 설정해야 합니다. 그렇지 않으면 외부 사용자 비밀번호를 사용하여 로그인할 수 없습니다.

프로시저

단계 **1** Service-Type 속성을 사용하여 RADIUS 서버에서 사용자를 정의합니다.

다음은 Service-Type 속성에 대해 지원되는 값입니다.

- Administrator(관리자) (6) - CLI에 대한 Config 액세스 권한을 제공합니다. 이러한 사용자는 CLI에서 모든 명령을 사용할 수 있습니다.
- NAS Prompt(NAS 프롬프트) (7) 또는 6 이외의 모든 레벨 - CLI에 대한 기본 액세스 권한을 제공합니다. 이러한 사용자는 모니터링 및 문제 해결을 위해 **show** 명령 같은 읽기 전용 명령을 사용할 수 있습니다.

이름은 다음과 같은 Linux 기준을 준수하는 사용자 이름이어야 합니다.

- 최대 32개의 영숫자 문자와 하이픈(-) 및 밑줄(_)
- 모두 소문자
- 하이픈(-)으로 시작할 수 없으며, 숫자만으로 구성할 수 없고, 마침표(.), 단가 기호(@) 또는 슬래시(/)를 포함할 수 없음

또는 외부 인증 객체에서 사용자를 미리 정의할 수 있습니다(단계 12, 14 페이지 단계 참조). FTD 및 에FMC 동일한 RADIUS 서버를 사용하는 한편 Service-Type(서비스-유형) 속성 방법을 FTD에 사용한다면, 동일한 RADIUS 서버를 식별하는 두 개의 외부 인증 개체를 생성합니다. 한 개체는 사전 정의된 **CLI Access Filter(CLI** 액세스 필터**)** 사용자(FMC에 사용)를 포함하며, 나머지 한 개체는 **CLI Access Filter(CLI** 액세스 필터**)**를 공란으로 둡니다(FTD에 사용).

단계 **2** FMC에서 **System(**시스템**)** > **Users(**사용자**)**를 선택합니다.

단계 **3** **External Authentication(**외부 인증**)**을 클릭합니다.

단계 **4** **Add External Authentication Object(**외부 인증 개체 추가**)**를 클릭합니다.

단계 **5** **Authentication Method(**인증 방법**)**을 **RADIUS**로 설정합니다.

단계 **6** **Name(**이름**)**과 **Description(**설명**)**(선택 사항)을 입력합니다.

단계 **7** **Primary Server(**기본 서버**)**에 **Host Name/IP Address(**호스트 이름**/IP** 주소**)**를 입력합니다.

참고 TLS 또는 SSL을 통한 연결에 인증서를 사용하는 경우 인증서의 호스트 이름이 이 필드에 사용된 호스트 이름과 일치해야 합니다. 또한 IPv6 주소는 암호화된 연결이 지원되지 않습니다.

단계 **8** (선택 사항) **Port(**포트**)**를 기본값에서 변경합니다.

단계 **9** **RADIUS Secret Key(RADIUS** 비밀 키**)**를 입력합니다.

단계 **10** (선택 사항) **Backup Server(**백업 서버**)** 파라미터를 입력합니다.

단계 **11** (선택 사항) **RADIUS-Specific Parameters(RADUIS** 특정 파라미터**)**를 입력합니다.

a) **Timeout(**시간 초과**)**을 초 단위로(1부터 300까지) 입력하고 기본 서버를 다시 시도합니다. 기본값은 30입니다.

참고 시간 제한 범위는 FTD와 FMC에서 서로 다르므로 개체를 공유하는 경우 FTD의 더 작은 시간 제한 범위(1 ~ 300초)를 초과하지 않아야 합니다. 시간 초과 값을 더 높은 값으로 설정하면 FTD RADIUS 컨피그레이션이 작동하지 않습니다.

b) **Retries(**재시도**)**를 입력하고 백업 서버로 이동합니다. 기본값은 3입니다.

단계 **12** (선택 사항) RADIUS 정의 사용자(단계 1, 13 페이지 단계 참조)를 사용하는 대신 **CLI Access Filter(CLI** 액세스 필터**)** 영역 **Administrator CLI Access User List(**관리자 **CLI** 액세스 사용자 목록**)** 필드에 CLI 액세스 권한이 있어야 하는 사용자 이름을 쉼표로 구분하여 입력합니다. 예를 들어, **`jchrichton, aerynsun, rygel`**을 입력합니다.

FTD에 **CLI Access Filter(CLI** 액세스 필터**)** 방법을 사용하여 FTD 및 다른 플랫폼 유형과 동일한 외부 인증 개체를 사용할 수 있습니다.

참고 RADIUS에서 정의한 사용자를 사용하려는 경우, **CLI Access Filter(CLI** 액세스 필터**)** 를 공란으로 두어야 합니다.

이러한 사용자 이름은 RADIUS 서버의 사용자 이름과 일치해야 합니다. 이름은 다음과 같은 Linux 기준을 준수하는 사용자 이름이어야 합니다.

- 최대 32개의 영숫자 문자와 하이픈(-) 및 밑줄(_)
- 모두 소문자
- 하이픈(-)으로 시작할 수 없으며, 숫자만으로 구성할 수 없고, 마침표(.), 단가 기호(@) 또는 슬래시(/)를 포함할 수 없음

단계 **13** (선택 사항) **Test(**테스트**)**를 클릭해 RADIUS 서버와 FMC 연결을 테스트합니다.

이 기능은 RADIUS 서버와 의 연결만 테스트합니다. 매니지드 디바이스와 RADIUS 서버의 연결을 테스트하는 기능은 없습니다.FMC

단계 **14** (선택 사항) **Additional Test Parameters(**추가 테스트 파라미터**)**를 입력하고 인증 가능한 사용자의 크리덴셜을 테스트할 수 있습니다. **User Name(**사용자 이름**)** 및 **Passowrd(**비밀번호**)**를 입력한 다음 **Test(**테스트**)**를 클릭합니다.

팁 테스트 사용자의 이름이나 비밀번호를 잘못 입력할 경우 서버 구성이 맞더라도 테스트는 실패합니다. 서버 구성이 올바른지 확인하려면 먼저 **Test(**테스트**)**를 클릭합니다. 여기서 **Additional Test Parameters(**추가 테스트 파라미터**)** 필드에는 사용자 정보를 입력할 필요가 없습니다. 테스트가 성공하면 사용자 이름과 비밀번호를 입력하고 특정 사용자로 테스트하십시오.

예제**:**

예를 들어 예시 회사의 `JSmith` 사용자 크리덴셜을 가져올 수 있는지 테스트하려면 `JSmith`를 입력하고 올바른 비밀번호를 입력합니다.

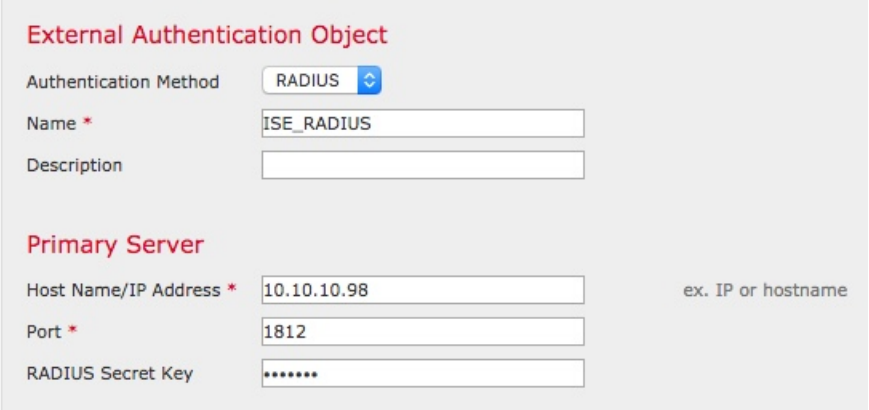
단계 **15** **Save(**저장**)**를 클릭합니다.

단계 **16** 이 서버의 사용을 활성화합니다. SSH에 대한 외부 인증 설정의 내용을 참조하십시오.

예

단순한 사용자 역할 할당

다음 그림은 포트 1812에서 IP 주소 10.10.10.98을 사용하여 Cisco ISE(Identity Services Engine)를 실행하는 서버를 위한 RADIUS 로그인 인증 개체의 예를 보여 줍니다. 정의된 백업 서버가 없습니다.



다음 예는 RADIUS 관련 매개변수를 보여 줍니다. 여기에는 시간 초과(30초) 및 Firepower System이 백업 서버에 연결을 시도하기 전 실패한 재시도 횟수(있는 경우)가 포함됩니다.

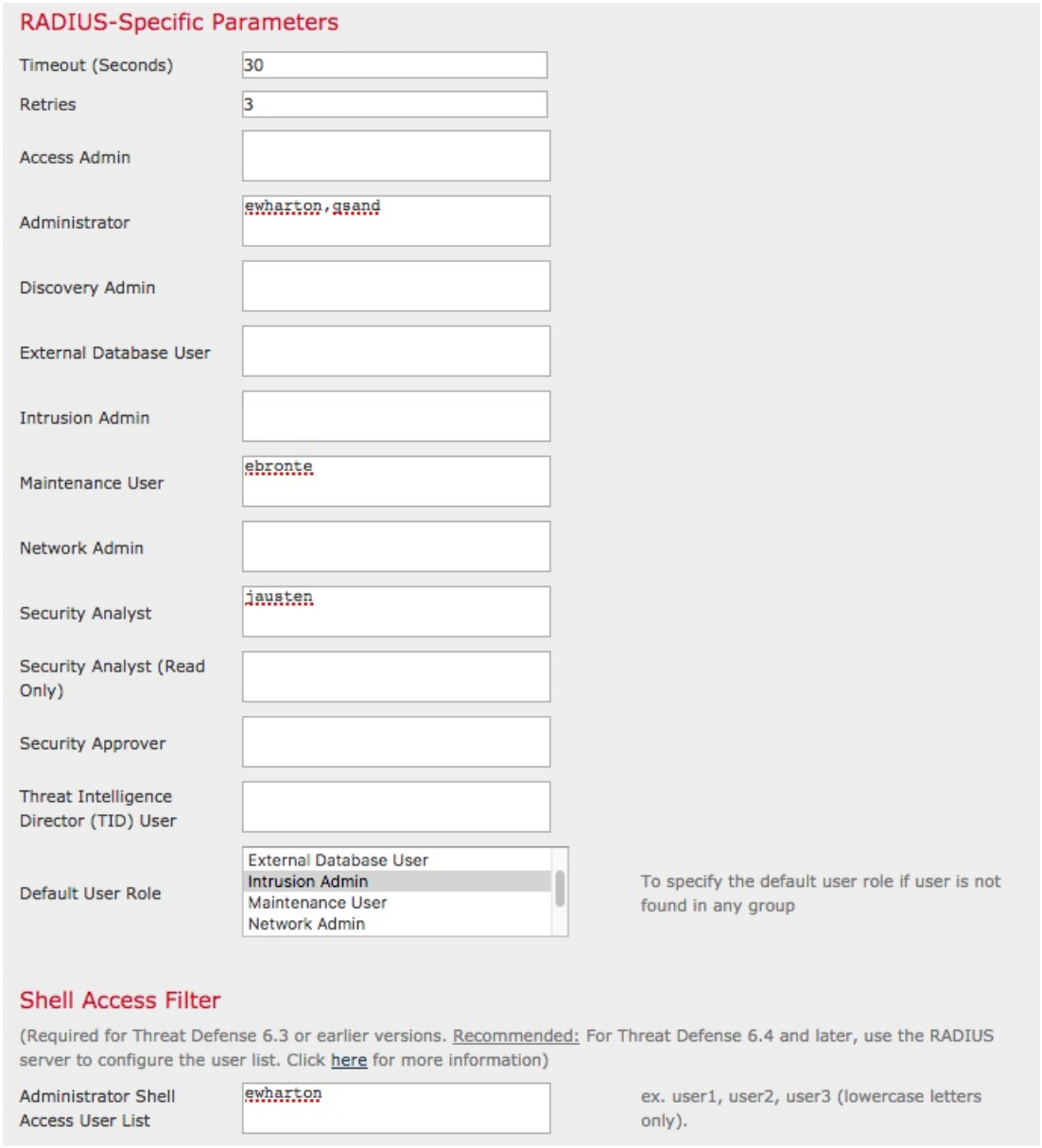
이 예에서는 RADIUS 사용자 역할 구성의 주요 측면을 보여줍니다.

사용자 `ewharton` 및 `gsand`에게 웹 인터페이스 Administrator(관리자) 액세스 권한이 주어집니다.

사용자 `cbronte`에게 웹 인터페이스 Maintenance User(유지 보수 사용자) 액세스 권한이 주어집니다.

사용자 `jausten`에게 웹 인터페이스 Security Analyst(보안 분석가) 액세스 권한이 주어집니다.

사용자 `ewharton`은 CLI 계정을 사용하여 디바이스에 로그인할 수 있습니다.



다음 그림은 이 예시에서의 역할 구성을 나타냅니다.

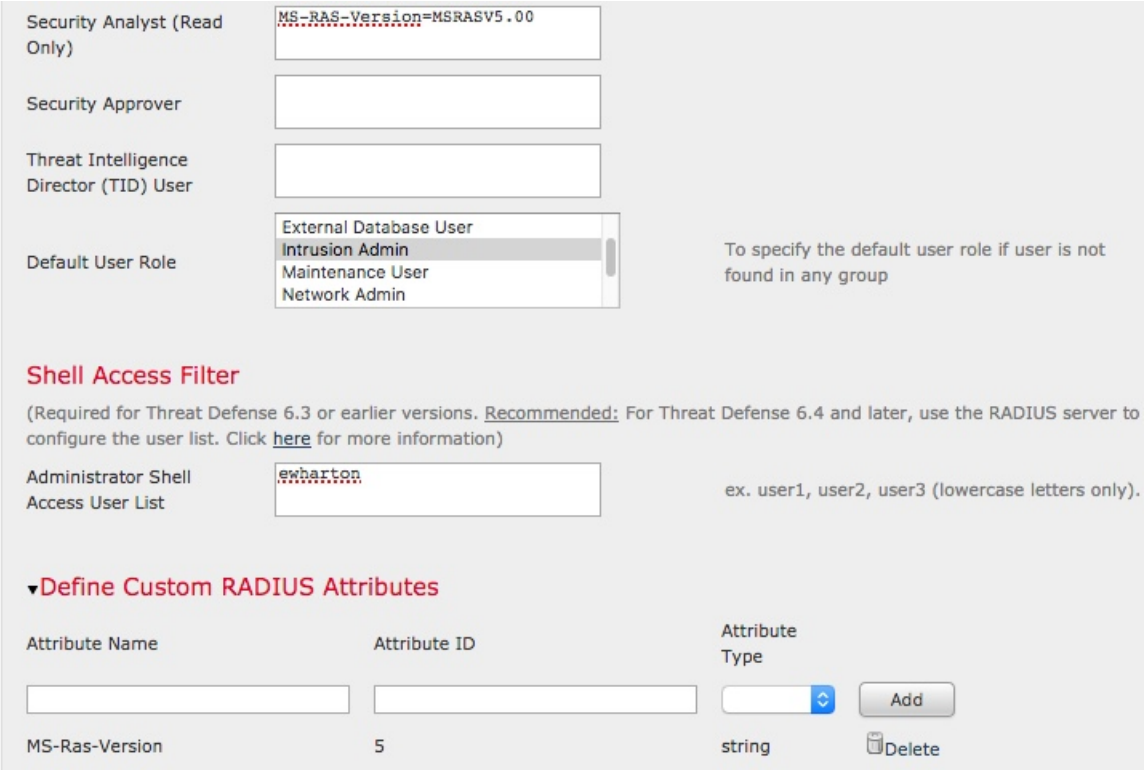
속성-값 쌍을 매칭하는 사용자의 역할

속성-값 쌍을 사용하여 특정 사용자 역할을 갖는 사용자를 식별할 수 있습니다. 사용하는 속성이 맞춤형 속성일 경우 해당 맞춤형 속성을 정의해야 합니다.

다음 그림은 이전의 예와 동일한 ISE 서버를 위한 샘플 RADIUS 로그인 인증 개체에 포함된 역할 설정 및 맞춤형 속성 정의를 보여 줍니다.

그러나 여기서는 Microsoft 원격 액세스 서버가 사용 중이므로 `MS-RAS-Version` 맞춤형 속성 한 명 이상의 사용자에게 반환됩니다. 참고로 `MS-RAS-Version` 맞춤형 속성은 문자열입니다. 이 예에서는 Microsoft v. 5.00 원격 액세스 서버를 통해 RADIUS로 로그인하는 모든 사용자

가 Security Analyst(Read Only)(보안 분석가(읽기 전용)) 역할을 받아야 하므로 속성-값 쌍 `MS-RAS-Version= MSRASV5.00`을 **Security Analyst(Read Only)(**보안 분석가**(**읽기 전용**))** 필드에 입력합니다.



FTD 디바이스 사용자에 대한 외부 인증 활성화

Firepower Threat Defense Platform Settings(Firepower Threat Defense 플랫폼 설정)에서 External Authentication(외부 인증)을 활성화한 후 해당 설정을 매니지드 디바이스에 구축합니다. 자세한 내용은 SSH에 대한 외부 인증 설정를 참조하십시오.

LDAP 인증 연결 문제 해결

LDAP 인증 개체를 생성하는 경우, 선택한 서버와의 연결에 실패하거나 원하는 사용자 목록을 가져오지 않는다면 개체의 설정을 조정할 수 있습니다.

연결 테스트 결과 연결에 실패할 경우, 다음 방법으로 구성 문제를 해결해보십시오.

- 웹 인터페이스 화면 상단 및 테스트 출력에 표시된 메시지를 참조하여 개체의 어느 영역에서 문제를 일으키는지 확인합니다.
- 개체에 사용한 사용자 이름과 비밀번호가 올바른지 확인합니다.

  - 사용자가 기본 DN에 나타난 디렉토리로 이동할 권한이 있는지 확인하기 위해 서드파티 LDAP 브라우저를 사용하여 LDAP 서버에 연결해봅니다.
  - 사용자 이름이 LDAP 서버의 디렉토리 정보 트리에서 고유한지 확인합니다.
  - 테스트 출력에 LDAP 바인드 오류 49가 있을 경우 해당 사용자에 대한 사용자 바인딩이 실패한 것입니다. 서드파티 애플리케이션을 통해 서버 인증을 시도하여 해당 연결에서도 바인딩이 실패하는지 확인합니다.

- 서버를 정확하게 식별했는지 확인합니다.
  - 서버 IP 주소 또는 호스트 이름이 정확한지 확인합니다.
  - 로컬 어플라이언스에서 연결할 인증 서버까지 TCP/IP 액세스 권한이 있는지 확인합니다.
  - 서버에 대한 액세스가 방화벽에 의해 차단되지 않고 개체에 구성한 포트가 열려 있는지 확인합니다.
  - TLS 또는 SSL을 통한 연결에 인증서를 사용하는 경우 인증서의 호스트 이름이 서버에 사용된 호스트 이름과 일치해야 합니다.
  - CLI 액세스를 인증하는 경우, 서버 연결에 IPv6 주소를 사용하지 않았는지 확인합니다.
  - 서버 유형 기본값을 사용한 경우 정확한 서버 유형인지 확인하고 **Set Defaults(**기본값 설정**)**를 다시 클릭하여 기본값을 재설정합니다.
- 기본 DN을 입력한 경우 **Fetch DNs(DN** 가져오기**)**를 클릭하여 서버에서 사용 가능한 모든 기본 DN을 가져오고 그 목록에서 이름을 선택합니다.
- 필터, 액세스 특성 또는 고급 설정을 사용하는 경우 각각이 올바르고 제대로 입력되었는지 확인합니다.
- 필터, 액세스 특성 또는 고급 설정을 사용하는 경우 각 설정을 제거하고 그 설정 없이 개체를 테스트해봅니다.
- 기본 필터 또는 셸 액세스 필터를 사용하는 경우, 필터가 괄호로 묶여 있고 올바른 비교 연산자를 사용하고 있는지 확인합니다. 묶인 괄호를 포함하여 최대 450자까지 입력할 수 있습니다.
- 더 제한적인 기본 필터를 테스트하려면 사용자의 기본 DN으로 설정하여 그 사용자만 검색해봅니다.
- 암호화 연결을 사용하는 경우:
  - 인증서에 있는 LDAP 서버의 이름이 연결에 사용하는 호스트 이름과 매칭되는지 확인합니다.
  - 암호화 서버 연결에 IPv6 주소를 사용하지 않았는지 확인합니다.
- 테스트 사용자를 사용하는 경우 사용자 이름과 비밀번호가 제대로 입력되었는지 확인합니다.
- 테스트 사용자를 사용하는 경우 사용자 크리덴셜을 제거하고 개체를 테스트합니다.
- LDAP 서버에 연결하고 다음 구문을 사용하여 사용 중인 쿼리를 테스트합니다.

```
ldapsearch -x -b 'base_distinguished_name'
-h LDAPserver_ip_address -p port -v -D
'user_distinguished_name' -W 'base_filter'
```

예를 들어 `myrtle.example.com`의 보안 도메인에 연결하기 위해 `domainadmin@myrtle.example.com` 사용자와 (`cn=*`) 기본 필터를 사용하는 경우, 다음 구문으로 연결을 테스트할 수 있습니다.

```
ldapsearch -x -b 'CN=security,DC=myrtle,DC=example,DC=com'
-h myrtle.example.com -p 389 -v -D
'domainadmin@myrtle.example.com' -W '(cn=*)'
```

연결 테스트에 성공했지만 플랫폼 설정 정책을 적용한 후 인증이 되지 않을 경우, 디바이스에 적용되는 플랫폼 설정 정책에서 인증 및 사용할 개체가 모두 활성화되었는지 확인합니다.

성공적으로 연결했지만 연결에서 검색되는 사용자 목록을 조정하려는 경우, 기본 필터 또는 셸 액세스 필터를 추가하거나 변경할 수 있습니다. 또는 더 제한적이거나 덜 제한적인 기본 DN을 사용할 수 있습니다.

디바이스용 사용자 계정 기록

기능	버전	세부 사항
RADUIS 서버에 정의된 FTD 사용자에 대한 Service-Type(서비스 유형) 속성을 지원합니다.	6.4	FTD CLI 사용자의 RADIUS 인증의 경우, RADIUS 외부 인증 개체에서 사용자 이름을 사전 정의하고 해당 목록과 RADIUS 서버에 정의된 사용자 이름을 수동으로 매칭시켜야 했었습니다. 이제 Service-Type(서비스 유형) 속성을 사용하여 RADIUS 서버의 CLI 사용자를 정의하고 Basic(기본) 및 Config(구성) 사용자 역할을 정의할 수 있습니다. 이 방법을 사용하려면 외부 인증 개체에서 셸 액세스 필터를 공란으로 두어야 합니다. 신규/수정된 화면: **System(**시스템**)** > **Users(**사용자**)** > **External Authentication(**외부 인증**)** > **Add External Authentication Object(**외부 인증 개체 추가**)** > 셸 액세스 필터 **(Shell Access Filter)** 지원되는 플랫폼: FTD

기능	버전	세부 사항
FTD SSH 액세스를 위한 외부 인증	6.2.3	이제 FTD LDAP 또는 RADIUS를 사용하여 SSH 액세스를 위한 외부 인증을 구성할 수 있습니다. 신규/수정된 화면: **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)** > **External Authentication(**외부 인증**)** 지원되는 플랫폼: FTD