FMC의 사용자 계정

FMC에는 웹 및 CLI 액세스에 필요한 기본 관리자 계정이 포함되어 있습니다. 이 장에서는 맞춤형 사용자 계정을 생성하는 방법을 설명합니다. Firepower System에 로그인의 내용을 참조하여 FMC에 사용자 계정으로 로그인하는 방법을 자세히 알아보십시오.

FMC 사용자 계정 정보

FMC에 세 종의 맞춤형 사용자 계정, 즉 LDAP 또는 RADIUS 서버에서 내부 사용자, 외부 사용자로 또는 SAML 2.0 규정 준수 SSO ID 제공자에서 SSO 사용자로 추가할 수 있습니다. FMC은 매니지드 디바이스에서 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, 그리고 SSO 사용자

FMC에서는 다음 3 가지 유형의 사용자를 지원합니다.

- 내부 사용자—FMC는 사용자 인증을 위해 로컬 데이터베이스를 검사합니다. 내부 사용자에 대한 자세한 내용은 내부 사용자 추가, 7 페이지을 참조하십시오.
- 외부 사용자—사용자가 로컬 데이터베이스에 없는 경우, 시스템이 외부 LDAP 또는 RADIUS 인증 서버에 쿼리합니다. 외부 사용자에 대한 자세한 내용은 외부 인증 구성, 9 페이지을 참조하십시오.

- SSO user(SSO 사용자)-계정이 SSO ID 제공자 측에서 구성된 경우 사용자가 FMC 로그인 페이지의 **SSO(Single Sign-On)** 링크를 사용하여 로그인하고 FMC에서는 인증 및 권한 부여를 위해 사용자를 IdP로 리디렉션합니다. SSO 사용자에 대한 자세한 내용은 SAML SSO(Single Sign-On) 구성, 25 페이지을 참조하십시오.

웹 인터페이스 및 CLI 액세스

FMC에는 웹 인터페이스, CLI(콘솔 (시리얼 포트 또는 키보드 및 모니터)에서 액세스하거나 SSH를 사용하여 관리 인터페이스에 액세스할 수 있음) 및 Linux 셸이 있습니다. 관리 UI에 대한 자세한 내용은 Firepower System 유저 인터페이스을 참조하십시오.

FMC 사용자 유형 및 액세스 가능한 UI에 대한 다음 정보를 참조하십시오.

- 관리 사용자 - FMC은 두 개의 서로 다른 내부 관리자 사용자를 지원합니다. 하나는 웹 인터페이스용이며 다른 하나는 CLI 액세스용입니다. 시스템 초기화 프로세스에서 두 관리자 계정의 비밀번호를 동기화하기 때문에 처음에는 두 계정이 동일하지만, 서로 다른 내부 메커니즘을 이용해 추적하며 초기 구성 후에 달라질 수 있습니다. 시스템 초기화에 관한 자세한 내용은 모델에 맞는 시작 가이드를 참조하십시오. (웹 인터페이스 관리자의 암호를 변경하려면 **System(**시스템**)** > **Users(**사용자**)** > **Users(**사용자**)**를 사용합니다. CLI 관리자의 암호를 변경하려면, FMC CLI 명령 **configure password**을 사용합니다.)
- 내부 사용자 - 웹 인터페이스에 추가된 내부 사용자는 웹 인터페이스 액세스만 할 수 있습니다.
- 외부 사용자 - 외부 사용자가 웹 인터페이스에 액세스할 수 있으며, 선택적으로 CLI 액세스를 구성할 수 있습니다.
- SSO 사용자 - SSO 사용자는 웹 인터페이스 액세스만 가능합니다.

⚠

주의 CLI 사용자는 **expert** 명령을 사용하여 Linux 셸에 액세스할 수 있습니다. Cisco TAC가 지시하거나 FMC 설명서에서 명시적으로 지시하지 않는 한, Linux 셸은 사용하지 않는 것이 좋습니다. CLI 사용자는 Linux 셸에서 `sudoers` 권한을 얻을 수 있으며 이로 인해 보안 위험이 발생됩니다. 시스템 보안을 위해 다음을 적극 권장합니다.

- CLI 액세스 권한이 있는 외부 사용자 목록을 적절하게 제한해야 합니다.
- Linux 셸에서 바로 사용자를 추가하지 마십시오. 이 장에서 설명하는 절차만 사용해야 합니다.

사용자 역할

CLI 사용자 역할

FMC의 CLI 외부 사용자는 사용자 역할이 없습니다. CLI 사용자는 사용 가능한 명령을 모두 사용할 수 있습니다.

웹 인터페이스 사용자 역할

사용자 권한은 할당된 사용자 역할을 기반으로 합니다. 예를 들어, 분석가에게 Security Analyst(보안 분석가) 및 Discovery Admin(검색 관리자) 같은 사전 정의된 역할을 부여하고 디바이스를 관리하는 보안 관리자를 위해 Admin(관리자) 역할을 남겨둘 수 있습니다. 조직의 요구 사항에 부합하는 액세스 권한을 가진 맞춤형 사용자 역할을 생성할 수도 있습니다.

FMC는 다음의 사전 정의된 사용자 역할을 포함합니다.

참고 동시 세션 제한을 위해 시스템에서 읽기 전용으로 간주하는 사전 정의된 사용자 역할은 **System(**시스템**)** > **Users(**사용자**)** > **Users(**사용자**)** 및 **System(**시스템**)** > **Users(**사용자**)** > **User Roles(**사용자 역할**)**의 역할 이름에 **(**읽기 전용**)**이라고 표시됩니다. 사용자 역할의 역할 이름에 **(**읽기 전용**)**이라는 표시가 없다면, 시스템은 역할을 읽기/쓰기로 간주합니다. 동시 세션 제한에 대한 자세한 내용은 전역 사용자 구성을 참조하십시오.

액세스 관리자

Policies(정책**)** 메뉴에서 액세스 제어 정책 및 관련된 기능에 대한 액세스를 제공합니다. 액세스 관리자는 정책을 구축할 수 없습니다.

관리자

관리자는 제품의 모든 항목에 액세스할 수 있습니다. 해당 세션은 보안 침해 시 더 심각한 위험을 초래하므로 로그인 세션 시간 초과에서 면제할 수 없습니다.

관리자 역할의 사용은 보안을 위해 필요한 경우로 제한해야 합니다.

검색 관리자

Policies(정책**)** 메뉴에서 네트워크 검색, 애플리케이션 탐지 및 상관 관계 기능에 대한 액세스를 제공합니다. 검색 관리자는 정책을 구축할 수 없습니다.

외부 데이터베이스 사용자**(**읽기 전용**)**

JDBC SSL 연결을 지원하는 애플리케이션을 사용하여 Firepower System 데이터베이스에 대한 읽기 전용 액세스를 제공합니다. 타사 애플리케이션이 Firepower System 어플라이언스를 인증하려면 시스템 설정에서 데이터베이스 액세스를 활성화해야 합니다. 외부 데이터베이스 사용자는 웹 인터페이스에서 **Help(**도움말**)** 메뉴의 온라인 도움말 관련 옵션에만 액세스할 수 있습니다. 이 역할의 기능이 웹 인터페이스와 무관하므로 용이한 지원 및 비밀번호 변경에 대한 액세스만 제공됩니다.

침입 관리자

Policies(정책**)** 및 **Objects(**개체**)** 메뉴에서 모든 침입 정책, 침입 규칙 및 네트워크 분석 정책 기능에 대한 액세스를 제공합니다. 침입 관리자는 정책을 구축할 수 없습니다.

유지 보수 사용자

모니터링 및 유지 보수 기능에 대한 액세스를 제공합니다. 유지 보수 사용자는 **Health(**상태**)** 및 **System(**시스템**)** 메뉴에서 유지 보수 관련 옵션에 액세스할 수 있습니다.

네트워크 관리자

Policies(정책**)** 메뉴에서 액세스 제어, SSL 검사, DNS 정책 및 ID 정책 기능에 대한 액세스를 비롯해 **Devices(**디바이스**)** 메뉴에서 디바이스 구성 기능에 대한 액세스도 제공합니다. 네트워크 관리자는 디바이스에 구성 변경 사항을 구축할 수 있습니다.

보안 분석가

Overview(개요**)**, **Analysis(**분석**)**, **Health(**상태**)** 및 **System(**시스템**)** 메뉴에서 보안 이벤트 분석 기능에 대한 액세스와 상태 이벤트에 대한 읽기 전용 액세스를 제공합니다.

보안 분석가**(**읽기 전용**)**

Overview(개요**)**, **Analysis(**분석**)**, **Health(**상태**)** 및 **System(**시스템**)** 메뉴에서 보안 이벤트 분석 기능과 상태 이벤트 기능에 대한 읽기 전용 액세스를 제공합니다.

이 역할의 사용자는 다음 작업도 수행할 수 있습니다.

- 특정 디바이스에 대한 상태 모니터 페이지에서 문제 해결 파일을 생성하고 다운로드합니다.
- 사용자 기본 설정에서 파일 다운로드 기본 설정을 지정합니다.
- 사용자 기본 설정에서 이벤트 로그 보기의 기본 기간을 설정합니다(**Audit Log Time Window(**감사 로그 시간 기간**)** 제외).

보안 승인자

Policies(정책**)** 메뉴에서 액세스 제어 및 관련된 정책과 네트워크 검색 정책에 대한 제한된 액세스를 제공합니다. 보안 승인자는 이러한 정책을 확인하고 구축할 수 있지만 정책을 변경할 수는 없습니다.

사용자 암호

다음 규칙은 LOM(Lights-Out Management)을 사용하거나 사용하지 않도록 설정한 FMC의 내부 사용자 계정에 대한 비밀번호에 적용됩니다. 외부에서 인증한 계정이나 보안 인증 규정 준수를 활성화한 시스템에서는 다른 비밀번호 요구 사항이 적용됩니다. 자세한 내용은 외부 인증 구성 및 보안 인증 컴플라이언스를 참고하십시오.

FMC 초기 설정에서, 시스템은 관리자 사용자에게 아래 테이블에서 설명하는 LOM 활성화 사용자에 대한 강력한 비밀번호 요구 사항을 준수하는 계정 비밀번호를 설정하도록 요구합니다. 이때 시스템은 웹 인터페이스 관리자와 CLI 액세스 관리자의 비밀번호를 동기화합니다. 초기 구성이 끝나면 웹 인터페이스 관리자는 강력한 비밀번호 요구 사항을 제거할 수 있지만, CLI 액세스 관리자는 강력한 비밀번호 요구사항을 준수해야 합니다.

	LOM 활성화되지 않음	LOM 활성화됨, 관리자 사용자
비밀번호 강도 확인 설정	비밀번호는 다음을 포함해야 합니다. • 최소 8자 또는 관리자가 사용자에 대해 설정한 문자 수 중 더 긴 값 • 반복되는 문자 2개 미만 • 소문자 1개 이상 • 대문자 1개 이상 • 하나 이상의 숫자가 필요합니다. • 특수문자 1개 이상(! @ # * - _ + 등) 시스템은 영어사전에 실린 수많은 단어는 물론 일반적인 비밀번호 해킹 기법으로 쉽게 해독할 수 있는 문자열을 포함하는 특수한 사전을 이용해 비밀번호를 검사합니다.	비밀번호는 다음을 포함해야 합니다. • 8~20개 사이의 문자(MC 1000, MC 2500, MC 4500의 경우 상한은 20자가 아닌 14자입니다.) • 반복되는 문자 2개 미만 • 소문자 1개 이상 • 대문자 1개 이상 • 하나 이상의 숫자가 필요합니다. • 특수문자 1개 이상(! @ # * - _ + 등) 특수 문자 규칙은 물리적 FMC 시리즈에 따라 다릅니다. 아래 마지막 글머리 기호에 나열된 특수 문자만 선택하는 방법을 권장합니다. 비밀번호에는 사용자 이름을 포함하지 마십시오. 시스템은 영어사전에 실린 수많은 단어는 물론 일반적인 비밀번호 해킹 기법으로 쉽게 해독할 수 있는 문자열을 포함하는 특수한 사전을 이용해 비밀번호를 검사합니다.

	LOM 활성화되지 않음	LOM 활성화됨, 관리자 사용자

비밀번호 강도 확인 해제	비밀번호는 관리자가 사용자에 대해 설정한 최소 문자 수 이상을 포함해야 합니다. (자세한 내용은 내부 사용자 추가, 7 페이지를 참조해 주십시오.)	비밀번호는 다음을 포함해야 합니다.
		• 8~20개 사이의 문자(MC 1000, MC 2500, MC 4500의 경우 상한은 20자가 아닌 14자입니다.)
		• 다음 4개 범주 중 3개 이상의 문자:
		  • 대문자
		  • 소문자
		  • 숫자
		  • 특수 문자(! @ # * - _ + 등)
		특수 문자 규칙은 물리적 FMC 시리즈에 따라 다릅니다. 아래 마지막 글머리 기호에 나열된 특수 문자만 선택하는 방법을 권장합니다.
		비밀번호에는 사용자 이름을 포함하지 마십시오.

FMC용 사용자 계정 지침 및 제한 사항

기본값

- FMC는 모든 형태의 액세스에 대해 로컬 사용자 계정으로 관리자 사용자를 포함합니다. 관리자 사용자를 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.
- 기본적으로 다음 설정이 FMC의 모든 사용자 어카운트에 적용됩니다.
  - 비밀번호 재사용에는 제한이 없습니다.
  - 시스템은 성공한 로그인을 추적하지 않습니다.
  - 시스템에서 잘못된 로그인 크리덴셜을 입력한 사용자에 대해 시간이 정해진 임시 잠금을 강제 적용하지 않습니다.
  - 동시에 열 수 있는 읽기 전용 및 읽기/쓰기 세션 수에 대한 사용자 정의 제한은 없습니다.

모든 사용자에 대한 이러한 설정을 시스템 구성으로 변경할 수 있습니다. (**System**(시스템) > **Configuration**(설정) > **User Configuration**(사용자 설정)) 전역 사용자 구성를 참조하십시오.

FMC 사용자 계정 요구 사항 및 사전 요건

모델 지원

FMC

지원되는 도메인

- SSO 구성 - 전역 전용.
- 기타 모든 기능 - 모두.

사용자 역할

- SSO 구성 - 내부 또는 LDAP 또는 RADIUS에 의해 인증된 관리자 역할의 사용자만 SSO를 설정할 수 있습니다.
- 기타 모든 기능 - 관리자 역할의 모든 사용자
- LADP로 CAC(Common Access Card) 인증 구성, 24 페이지에서는 Network Admin(네트워크 관리자) 역할도 지원합니다.

내부 사용자 추가

이 절차에서는 FMC에 대한 사용자 지정 내부 사용자 계정을 추가하는 방법을 설명합니다.

System(시스템**)** > **Users(**사용자**)** > **Users(**사용자**)**에는 사용자가 LDAP 또는 RADIUS 인증을 통해 로그인할 때 수동으로 추가한 내부 사용자와 자동으로 추가된 외부 사용자가 모두 표시됩니다. 외부 사용자의 경우 더 높은 권한이 있는 역할을 할당하면 이 화면에서 사용자 역할을 수정할 수 있지만 비밀번호 설정은 수정할 수 없습니다.

FMC의 다중 도메인 구축에서 사용자는 생성된 도메인에서만 표시될 수 있습니다. 글로벌 도메인에서 사용자를 추가한 다음, 리프 도메인에 사용자 역할을 할당하는 경우 사용자가 리프 도메인에 "속하는" 경우에도 해당 사용자는 추가된 전역 **Users(**사용자**)** 페이지에 계속해서 표시됩니다.

디바이스에서 보안 인증 컴플라이언스 또는 LOM(Lights-Out Management)을 활성화하면 다른 비밀번호 제한이 적용됩니다. 보안 인증 컴플라이언스에 대한 자세한 내용은 보안 인증 컴플라이언스의 내용을 참조하십시오.

리프 도메인에서 사용자를 추가하면 해당 사용자는 글로벌 도메인에서 표시되지 않습니다.

참고 여러 관리자 사용자가 동시에 FMC에서 새 사용자를 생성하지 않도록 하십시오. 사용자 데이터베이스 액세스 충돌로 인해 오류가 발생할 수 있습니다.

프로시저

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

단계 **2** **Create User**(사용자 생성)를 클릭합니다.

단계 **3** **User Name(**사용자 이름**)**을 입력합니다.

사용자 이름은 다음 제한 사항을 준수해야 합니다.

- 최대 32개의 영숫자 문자와 하이픈(-), 밑줄(_) 및 마침표(.).
- 문자는 대문자 또는 소문자일 수 있습니다.
- 하이픈(-), 밑줄(_) 및 마침표(.) 이외의 특수 문자 또는 문장 부호를 포함할 수 없습니다.

단계 **4** **Real Name(**실명**)**: 계정이 속한 사용자 또는 부서를 식별하기 위한 설명 정보를 입력합니다.

단계 **5** **Use External Authentication Method(**외부 인증 방법 사용**)** 확인란은 LDAP 또는 RADIUS를 통해 로그인할 때 자동으로 추가된 사용자를 대상으로 확인됩니다. 외부 사용자를 사전 구성할 필요가 없으므로 이 필드를 무시할 수 있습니다. 외부 사용자의 경우 확인란을 선택 취소하여 이 사용자를 내부 사용자로 되돌릴 수 있습니다.

단계 **6** **Password(**비밀번호**)** 및 **Confirm Password(**비밀번호 확인**)** 필드에 값을 입력합니다.

값은 이 사용자에게 설정한 비밀번호 옵션을 준수해야 합니다.

단계 **7** **Maximum Number of Failed Logins(**최대 실패 로그인 시도 횟수**)**를 설정합니다.

공백 없이 정수를 입력하여 각 사용자가 로그인에 실패한 후 어카운트가 잠길 때까지 로그인을 시도할 수 있는 최대 횟수를 지정합니다. 기본 설정은 5회입니다. **0**을 사용하면 로그인 실패 횟수의 제한이 사라집니다. 관리자 어카운트는 보안 인증 컴플라이언스를 활성화한 경우를 제외하고 실패한 로그인의 최대 수 이후에 잠금에서 제외됩니다.

단계 **8** **Minimum Password Length(**최소 비밀번호 길이**)**를 설정합니다.

공백 없이 정수를 입력하여 사용자 비밀번호의 최소 길이를 글자 수로 지정합니다. 기본 설정은 **8**입니다. 값이 **0**이면 최소 길이 제한이 없습니다.

단계 **9** **Days Until Password Expiration(**비밀번호 만료 시까지의 일수**)**을 설정합니다.

여기에 입력한 일수가 지나면 사용자의 비밀번호가 만료됩니다. 기본 설정은 **0**이며, 이렇게 하면 비밀번호가 만료되지 않습니다. 기본값에서 변경하는 경우, 사용자 목록의 **Password Lifetime(**비밀번호 수명**)** 열에는 각 사용자의 비밀번호에서 남아 있는 일수가 나타납니다.

단계 **10** **Days Before Password Expiration Warning(**비밀번호 만료 경고까지 남은 일수**)**을 설정합니다.

비밀번호가 만료되기 전에 사용자에게 비밀번호를 변경하게 하는 경고 일수를 입력합니다. 기본 설정은 **0**일입니다.

단계 **11** 사용자 **Options(**옵션**)**를 설정합니다.

- **Force Password Reset on Login(**로그인 시 비밀번호 재설정 강제 실행**)** - 사용자가 다음에 로그인할 때 비밀번호를 변경하도록 강제 실행합니다.

- **Check Password Strength(**비밀번호 보안 수준 확인**)** - 강력한 비밀번호가 필요합니다. 비밀번호 강도 확인을 활성화하면, 비밀번호는 사용자 암호, 4 페이지에서 설명하는 강력한 비밀번호 요구 사항을 준수해야 합니다.
- **Exempt from Browser Session Timeout(**브라우저 세션 시간 초과에서 제외**)** - 사용자의 로그인 세션이 비활성화로 인한 종료에서 제외됩니다. 관리자 역할의 사용자는 면제받을 수 없습니다.

단계 **12** **User Role Configuration(**사용자 역할 구성**)** 영역에서 사용자 역할을 할당합니다. 사용자 역할에 대한 자세한 내용은 웹 인터페이스의 사용자 역할 맞춤화, 79 페이지의 내용을 참조하십시오.

외부 사용자의 경우, 사용자 역할이 그룹 구성원 자격(LDAP)을 통해 할당되거나 사용자 속성(RADIUS)을 기반으로 할당되면 최소 액세스 권한을 제거할 수 없습니다. 단, 추가 권한은 할당할 수 있습니다. 사용자 역할이 디바이스에서 설정하는 기본 사용자 역할인 경우, 제한 없이 사용자 어카운트에서 역할을 수정할 수 있습니다. 사용자 역할을 수정하는 경우 **Users(**사용자**)** 탭의 **Authentication Method(**인증 방법**)** 열에 **External - Locally Modified(**외부 - 로컬로 수정됨**)** 상태가 나타납니다.

표시되는 옵션은 디바이스가 단일 도메인 또는 다중 도메인 구축에 있는지 여부에 따라 달라집니다.

- 단일 도메인 - 사용자를 할당할 사용자 역할을 선택합니다.
- 다중 도메인 — 다중 도메인 구축에서 관리자 액세스 권한이 할당된 모든 도메인에서 사용자 계정을 생성할 수 있습니다. 사용자는 각 도메인에서 다른 권한을 가질 수 있습니다. 상위 도메인 및 하위 도메인 모두에서 사용자 역할을 할당할 수 있습니다. 예를 들어 글로벌 도메인에서 사용자에게 읽기 전용 권한을 할당할 수 있지만 하위 도메인에서는 관리자 권한을 할당할 수 있습니다. 다음 단계를 참조하십시오.
  1. **Add Domain(**도메인 추가**)**을 클릭합니다.
  2. **Domain(**도메인**)** 드롭다운 목록에서 도메인을 선택합니다.
  3. 사용자를 할당할 사용자 역할을 선택합니다.
  4. **Save(**저장**)**를 클릭합니다.

단계 **13** (선택 사항, 물리적 FMC의 경우에만 해당됨) 사용자에게 관리자 역할을 할당한 경우, 관리자 옵션이 나타납니다. **Allow Lights-Out Management Access(Lights-Out Management** 액세스 허용**)**를 선택하여 사용자에게 Lights-Out Management 액세스 권한을 부여할 수 있습니다. Lights-Out Management에 대한 자세한 내용은 LOM(Lights-Out Management) 개요의 내용을 참조하십시오.

단계 **14** **Save(**저장**)**를 클릭합니다.

외부 인증 구성

외부 인증을 활성화하려면 하나 이상의 외부 인증 개체를 추가해야 합니다.

외부 인증 정보

외부 인증을 활성화하는 경우, 외부 인증 개체에 지정된 대로 FMC에서 LDAP 또는 RADIUS 서버로 사용자 자격 증명을 확인합니다.

웹 인터페이스 액세스를 위한 여러 외부 인증 개체를 구성할 수 있습니다. 예를 들어 외부 인증 개체가 5개인 경우, 그러한 개체에서 사용자는 웹 인터페이스 액세스를 인증받을 수 있습니다. CLI 액세스는 외부 인증 개체를 하나만 사용할 수 있습니다. 외부 인증 개체를 하나 이상 활성화하는 경우, 사용자는 목록에서 첫 번째 개체로만 인증할 수 있습니다.

외부 인증 개체는 FMC 및 FTD 디바이스가 사용할 수 있습니다. 다양한 어플라이언스/디바이스 유형 간에 동일한 개체를 공유하거나 별도 개체를 생성할 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.

FMC의 경우, 외부 인증 객체를 **System(**시스템**)** > **User(**사용자**)** > **External Authentication(**외부 인증**)** 탭에서 직접 활성화합니다. 이 설정은 FMC 사용에만 영향을 주며 매니지드 디바이스 사용에 대해 이 탭에서 활성화할 필요는 없습니다. FTD 디바이스의 경우, 디바이스에 구축하는 플랫폼 설정에서 외부 인증 객체를 활성화해야 합니다.

웹 인터페이스 사용자는 내부 인증 개체에 있는 CLI 사용자와 별개로 정의됩니다. RADIUS의 CLI 사용자의 경우, 외부 인증 개체의 RADIUS 사용자 이름목록을 사전 구성해야 합니다. LDAP의 경우, 필터를 지정하여 LDAP 서버의 CLI 사용자와 매칭할 수 있습니다.

CAC 인증을 위해 구성된 CLI 액세스를 위한 LDAP 개체를 사용할 수 없습니다.

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 전

달할 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.

FMC에 대한 LDAP 외부 인증 개체 추가

LDAP 서버를 추가하고 디바이스 관리를 위해 외부 사용자를 지원합니다.

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

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. FMC 관리 인터페이스 수정를 참조하고 DNS 서버를 추가합니다.
- CAC 인증과 함께 사용할 LDAP 인증 개체를 구성하는 경우 컴퓨터에 삽입된 AC를 제거해서는 안 됩니다. 사용자 인증서를 활성화한 다음에는 항상 CAC가 삽입된 상태여야 합니다.

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 (선택 사항) CAC 인증 및 권한 부여에 이 인증 개체를 사용하려는 경우 **CAC** 확인란을 선택할 수도 있습니다.

CAC 인증 및 권한 부여를 전부 구성하려면 LADP로 CAC(Common Access Card) 인증 구성, 24 페이지에 있는 절차를 따라야 합니다. 이 개체는 CLI 사용자에게는 사용할 수 없습니다.

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

단계 **7** 드롭다운 목록에서 **Server Type(**서버 유형**)**을 선택합니다.

팁 **Set Defaults(**기본 설정**)**을 클릭하면 디바이스가 **User Name Template(**사용자 이름 템플릿**)**, **UI Access Attribute(UI** 액세스 속성**)**, **CLI Access Attribute(CLI** 액세스 속성**)**, **Group Member Attribute(**그룹 구성원 속성**)** 및 **Group Member URL Attribute(**그룹 구성원 **URL** 속성**)** 필드를 서버 유형의 기본값으로 채웁니다.

단계 **8** **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 **9** (선택 사항) **Port(**포트**)**를 기본값에서 변경합니다.

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

단계 **11** **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.

CAC 인증을 사용하는 경우 활성 사용자 계정만 필터링하려면(비활성화된 사용자 계정 제외) `(!(userAccountControl:1.2.840.113556.1.4.803:=2))`를 입력합니다. 이 기준은 `ldpgrp` 그룹에 속하는 AD 내에서 사용자 계정을 검색하며 `userAccountControl` 속성 값이 `2`(비활성화됨)가 아닙니다.

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. 항상 끼어들기 공격을 방지하기 위해 SSL에 대한 인증서를 업로드하는 것이 좋습니다.

- **User Name Template(**사용자 이름 템플릿**)**— **UI Access Attribute(UI** 액세스 속성**)**에 해당하는 템플릿을 제공합니다. 예를 들어 예시 회사의 보안 조직에서 근무하는 모든 사용자를 인증하기 위해 UI 액세스 속성이 `uid`인 OpenLDP 서버에 연결하는 경우, `uid=%s,ou=security,dc=example,dc=com`를 **User Name Template(**사용자 이름 템플릿**)** 필드에 입력합니다. Microsoft Active Directory 서버에서는 `%s@security.example.com`이라고 입력할 수 있습니다.

  이 필드는 CAC 인증을 위해 필요합니다.

- **Timeout(**시간 초과**)**—백업 연결로 전환하기 전 시간(초)을 1과 1024 사이로 입력합니다. 기본값은 30입니다.

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

단계 **12** (선택 사항) **Attribute Mapping(**속성 매핑**)**을 구성하고 속성에 따라 사용자를 검색합니다.

- **UI Access Attribute(UI** 액세스 속성**)**을 입력하거나 **Fetch Attrs(**속성 가져오기**)**를 클릭하여 사용 가능한 속성 목록을 검색합니다. 예를 들어 Microsoft Active Directory Server의 경우 Active Directory Server 사용자 개체에 `uid` 속성이 없기 때문에 UI Access Attribute(UI 액세스 속성)를 사용하여 사용자를 검색할 수도 있습니다. 그 대신 `userPrincipalName` 속성을 검색할 수 있는데, `userPrincipalName`을 **UI Access Attribute(UI** 액세스 속성**)** 필드에 입력하면 됩니다.

  이 필드는 CAC 인증을 위해 필요합니다.

- 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` CLI 액세스 속성을 사용하여 셸 액세스 사용자를 가져오려면 `sAMAccountName`을 입력합니다.

단계 **13** (선택 사항) **Group Controlled Access Roles(**그룹 제어 액세스 역할**)**를 구성합니다.

액세스 제어 그룹에 역할을 사용하여 사용자의 권한을 구성하지 않는 경우, 사용자는 외부 인증 정책에서 기본적으로 부여된 권한만 갖습니다.

a) (선택 사항) 사용자 역할에 해당하는 필드에 해당 역할이 부여되는 사용자를 포함하는 LDAP 그룹의 DN을 입력합니다.

   참조하는 모든 그룹이 LDAP 서버에 있어야 합니다. 고정 LDAP 그룹 또는 동적 LDAP 그룹을 참조할 수 있습니다. 고정 LDAP 그룹은 특정 사용자를 가리키는 그룹 개체 특성에 의해 멤버십이 결정되며, 동적 LDAP 그룹에서는 사용자 개체 특성에 따라 그룹 사용자를 가져오는 LDAP 검색을 생성하여 멤버십을 결정합니다. 어떤 역할에 대한 그룹 액세스 권한은 그룹의 멤버인 사용자에게만 영향을 미칩니다.

   동적 그룹을 사용하는 경우 LDAP 서버에 구성된 대로 LDAP 쿼리가 사용됩니다. 이런 이유로 Firepower 디바이스는 검색 반복 횟수를 4회로 제한하여 검색 구문 오류로 인한 무한 루프를 방지합니다.

   예제:

Administrator(관리자**)** 필드에 다음과 같이 입력하여 예시 회사의 정보 기술 조직에서 이름을 인증할 수 있습니다.

```
cn=itgroup,ou=groups, dc=example,dc=com
```

b) 지정된 어떤 그룹에도 속하지 않는 사용자에 대해 **Default User Role(**기본 사용자 역할**)**을 선택합니다.

c) 정적 그룹을 사용하는 경우, **Group Member Attribute(**그룹 멤버 속성**)**을 입력합니다.

예제**:**

기본 Security Analyst 액세스에 대한 고정 그룹의 멤버십을 표시하기 위해 `member(멤버)` 속성을 사용하는 경우 `member(멤버)`라고 입력합니다.

d) 동적 그룹을 사용하는 경우, **Group Member URL Attribute(**그룹 멤버 **URL** 속성**)**을 입력합니다.

예제**:**

`memberURL` 속성이 기본 관리자 액세스에 대해 지정한 동적 그룹의 멤버를 가져오는 LDAP 검색을 포함할 경우 `memberURL`이라고 입력합니다.

사용자의 역할을 변경하는 경우, 변경된 외부 인증 개체는 저장/배포하고 **Users(**사용자**)** 화면에서 해당 사용자를 제거해야 합니다. 이 사용자는 다음 로그인 시 자동으로 재추가됩니다.

단계 **14** (선택 사항) CLI 사용자를 허용하도록 **CLI Access Filter(CLI** 액세스 필터**)**를 설정합니다.

CLI 액세스에 대해 LDAP 인증을 하지 않으려면 이 필드를 비워 둡니다. CLI 사용자를 지정하려면 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 **CLI Access Filter(CLI** 액세스 필터**)**에 포함된 사용자와 사용자 이름이 동일한 내부 사용자를 만들지 마십시오. 내부 FMC 사용자만 관리자여야 합니다. **CLI Access Filter(CLI** 액세스 필터**)**에 관리자를 포함하지 마십시오.

단계 **15** (선택 사항) **Test(**테스트**)**를 클릭하고 LDAP 서버와의 연결을 테스트합니다.

테스트 출력에서는 유효한 사용자 이름과 유효하지 않은 사용자 이름을 나열합니다. 사용자 이름은 고유해야 하며 밑줄(_), 마침표(.), 하이픈(-), 영숫자를 포함할 수 있습니다. 1,000명이 넘는 사용자로 서버와의 연결을 테스트할 경우 UI 페이지 크기 제한 때문에 1,000명의 사용자만 반환됩니다. 테스트에 실패하는 경우 LDAP 인증 연결 문제 해결, 84 페이지을 참조하십시오.

단계 **16** (선택 사항) **Additional Test Parameters(**추가 테스트 파라미터**)**를 입력하고 인증 가능한 사용자의 크리덴셜을 테스트할 수도 있습니다. **User Name(**사용자 이름**)** `uid` 및 **Password(**비밀번호**)**를 입력한 다음 **Test(**테스트**)**를 클릭합니다.

Microsoft Active Directory Server에 연결하는 경우 `uid` 대신 UI 액세스 속성을 제공했다면 해당 속성의 값을 사용자 이름으로 사용합니다. 해당 사용자의 정규화된 DN을 지정할 수도 있습니다.

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.

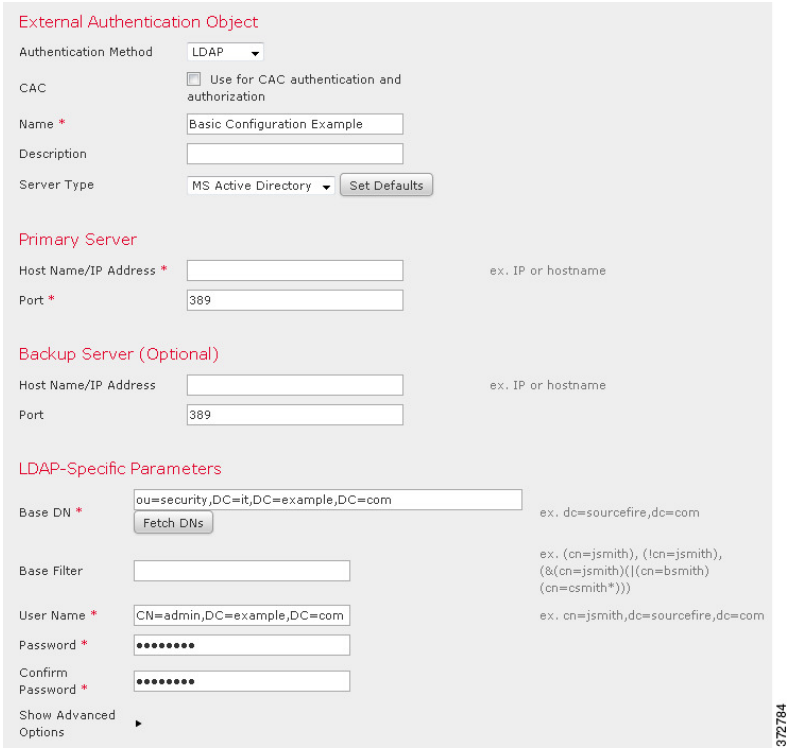
단계 **17** **Save(**저장**)**를 클릭합니다.

단계 **18** 이 서버의 사용을 활성화합니다. FMC 사용자에 대한 외부 인증 활성화, 23 페이지를 참조하십시오.

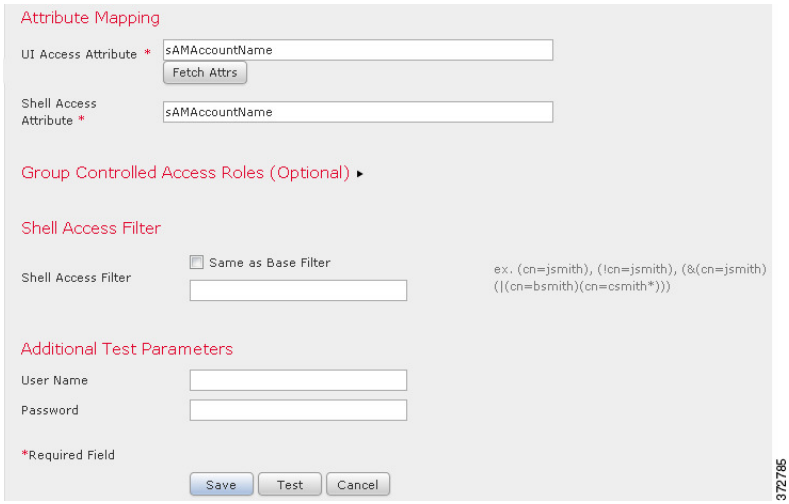
예

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.



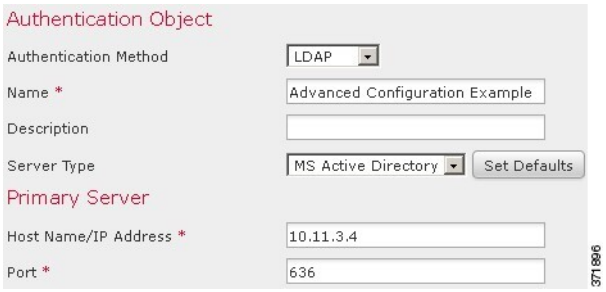
그러나 이 서버는 Microsoft Active Directory Server이므로 `sAMAccountName` 속성을 사용해 사용자 이름을 저장하며 `uid` 속성을 사용하지 않습니다. MS Active Directory Server 유형을 선택하고 **Set Defaults(**기본값 설정**)**을 클릭하면 UI Access Attribute(UI 액세스 속성)이 `sAMAccountName`으로 설정됩니다. 이에 따라 Firepower System에서는 사용자가 Firepower System에 대한 로그인을 시도하는 경우 각 개체에 대해 `sAMAccountName` 속성을 검사하면서 사용자 이름을 매칭합니다.

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

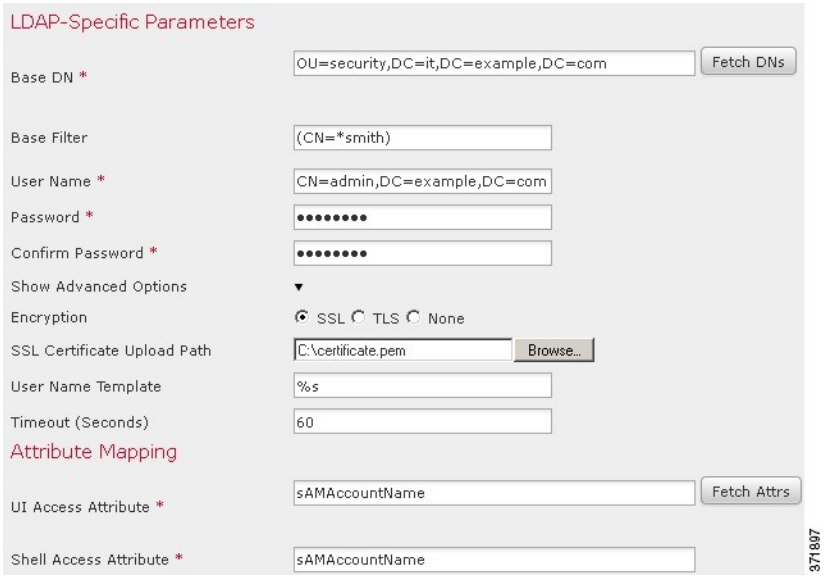
이 서버에는 기본 필터가 적용되지 않으므로 Firepower System에서는 기본 DN이 나타내는 디렉토리의 모든 개체에 대해 특성을 검사합니다. 기본 기간(또는 LDAP 서버에 설정된 시간 초과 기간)이 경과하면 서버와의 연결이 시간 초과됩니다.

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.

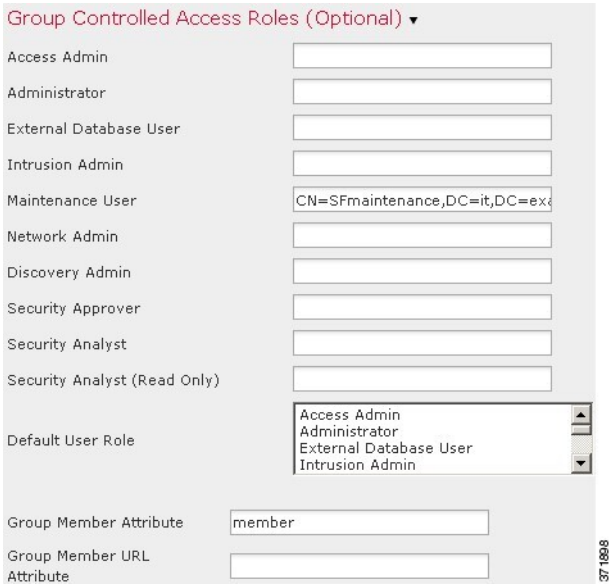


서버와의 연결은 SSL로 암호화되고 `certificate.pem`이라는 인증서가 연결에 사용됩니다. 또한 **Timeout(**시간 초과**)** 설정 때문에 60초가 지나면 서버와의 연결이 시간 초과됩니다.

이 서버는 Microsoft Active Directory Server이므로 `sAMAccountName` 속성을 사용해 사용자 이름을 저장하며 `uid` 속성을 사용하지 않습니다. 구성에 `sAMAccountName`이라는 UI Access Attribute(UI 액세스 속성)가 포함되어 있습니다. 이에 따라 Firepower System에서는 사용자가 Firepower System에 대한 로그인을 시도하는 경우 각 개체에 대해 `sAMAccountName` 속성을 검사하면서 사용자 이름을 매칭합니다.

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

여기에는 그룹 설정도 포함되어 있습니다. `member` 그룹 속성과 `CN=SFmaintenance,DC=it,DC=example,DC=com`이라는 기본 도메인 이름을 갖는 그룹의 모든 멤버에게 Maintenance User(유지 보수 사용자) 역할이 자동으로 지정됩니다.



셸 액세스 필터는 기본 필터와 동일하게 설정되므로, 동일한 사용자가 웹 인터페이스뿐 아니라 CLI를 통해서도 어플라이언스에 액세스할 수 있습니다.

FMC에 대한 RADIUS 외부 인증 개체 추가

RADIUS 서버를 추가하고 디바이스 관리를 위해 외부 사용자를 지원합니다.

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

프로시저

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

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

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

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

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

단계 6 **Primary Server(**기본 서버**)**에 **Host Name/IP Address(**호스트 이름**/IP** 주소**)**를 입력합니다.

단계 7 (선택 사항) **Port(**포트**)**를 기본값에서 변경합니다.

단계 8 **RADIUS Secret Key(RADIUS** 비밀 키**)**를 입력합니다.

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

단계 10 (선택 사항) **RADIUS-Specific Parameters(RADUIS** 특정 파라미터**)**를 입력합니다.

a) **Timeout(**시간 초과**)**을 초 단위(1~1024)로 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.

c) 사용자 역할에 해당하는 필드에 각 사용자의 이름을 입력하거나 해당 역할에 지정될 식별 특성-값 쌍을 입력합니다.

사용자 이름과 속성-값 쌍은 쉼표로 구분합니다.

예제**:**

보안 분석가인 모든 사용자가 `Analyst(분석가)`를 `User-Category(사용자-카테고리)` 속성 값으로 갖는 경우, `User-Category=Analyst`를 **Security Analyst(**보안 분석가 목록**)** 필드에 입력하고 해당 사용자에게 해당 역할을 부여할 수 있습니다.

예제**:**

Administrator(관리자) 역할을 사용자인`jsmith`와 `jdoe`에게 부여하려면 `jsmith, jdoe`를 **Administrator(**관리자**)** 필드에 입력합니다.

예제**:**

Maintenance User(유지 보수 사용자) 역할을 `User-Category(사용자-카테고리)` 값이 `Maintenance(유지 보수)`인 모든 사용자에게 부여하려면 `User-Category=Maintenance`를 **Maintenance User(**유지 보수 사용자**)** 필드에 입력합니다.

d) 지정된 어떤 그룹에도 속하지 않는 사용자에 대해 **Default User Role(**기본 사용자 역할**)**을 선택합니다.

사용자의 역할을 변경하는 경우, 변경된 외부 인증 개체는 저장/배포하고 **Users(**사용자**)** 화면에서 해당 사용자를 제거해야 합니다. 이 사용자는 다음 로그인 시 자동으로 재추가됩니다.

단계 **11** (선택 사항) **Define Custom RADIUS Attributes(**맞춤형 **RADIUS** 속성 정의**)**.

RADIUS 서버가 `/etc/radiusclient`의 `dictionary` 파일에 없는 속성의 값을 반환할 경우, 이러한 속성을 사용하여 해당 속성을 갖는 사용자에 대한 역할을 설정하려면 그러한 속성을 정의해야 합니다. RADIUS 서버에서 사용자 프로파일을 확인하여 사용자에 대해 반환되는 속성을 찾을 수 있습니다.

a) **Attribute Name(**속성 이름**)**을 입력합니다.

속성을 정의할 때 영숫자로 구성된 속성의 이름을 제공합니다. 속성 이름의 단어는 공백이 아닌 대시로 구분해야 합니다.

b) 정수로 **Attribute ID(**속성 **ID)**를 입력합니다.

속성 ID는 정수이며 `etc/radiusclient/dictionary` 파일에 있는 기존 속성 ID와 충돌해서는 안 됩니다.

c) **Attribute Type(**속성 유형**)** 드롭다운 목록에서 선택합니다.

속성의 유형을 문자열, IP 주소, 정수 또는 날짜로 지정합니다.

d) **Add(**추가**)**를 클릭하고 맞춤형 속성을 추가합니다.

RADIUS 인증 개체를 생성하는 경우 해당 개체에 대한 새로운 사전 파일이 `/var/sf/userauth` 디렉토리에 있는 디바이스에 생성됩니다. 추가하는 모든 맞춤형 속성은 사전 파일에 추가됩니다.

예제**:**

RADIUS 서버가 Cisco 라우터가 있는 네트워크에서 사용되는 경우 `Ascend-Assign-IP-Pool` 속성을 사용하여 특정 IP 주소 풀에서 로그인한 모든 사용자에게 특정 역할을 부여할 수 있습니다. `Ascend-Assign-IP-Pool`은 정수 속성으로서 사용자가 로그인할 수 있는 주소 풀을 정의합니다. 여기서 정수는 지정된 IP 주소 풀의 번호를 나타냅니다.

맞춤형 속성을 표시하려면 속성 이름 `Ascend-IP-Pool-Definition`, 속성 ID `218`, 속성 유형 `integer`로 맞춤형 속성을 생성합니다.

그런 다음 `Ascend-Assign-IP-Pool=2`를 **Security Analyst (Read Only)(**보안 분석가**(**읽기 전용**))** 필드에 입력하여 `Ascend-IP-Pool-Definition` 속성의 값이 `2`인 모든 사용자에게 읽기 전용 보안 분석가 권한을 부여할 수 있습니다.

단계 **12** (선택 사항) **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.

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

CLI 액세스에 대해 RADIUS 인증을 하지 않으려면 이 필드를 비워 둡니다.

참고 셸 액세스 필터에 포함된 사용자와 사용자 이름이 동일한 내부 사용자를 모두 제거합니다. FMC에서는 내부 CLI 사용자만 관리자이니, 관리자 외부 사용자를 생성하지 마십시오.

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

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.

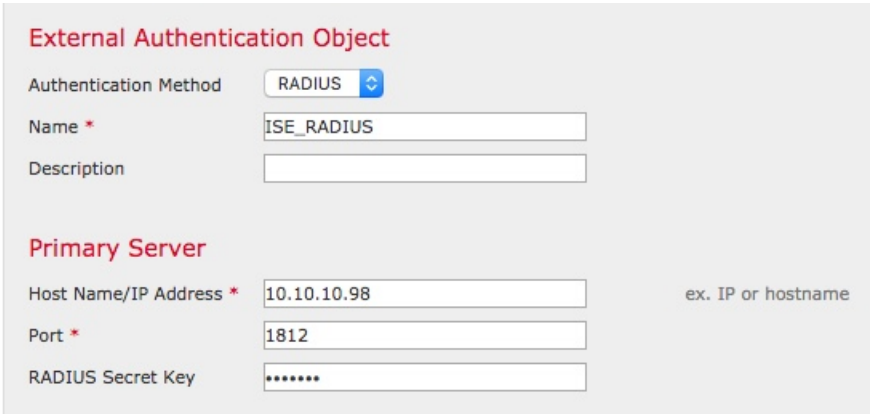
단계 **15** **Save(**저장**)**를 클릭합니다.

단계 **16** 이 서버의 사용을 활성화합니다. FMC 사용자에 대한 외부 인증 활성화, 23 페이지를 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 보여줍니다. 정의된 백업 서버가 없습니다.



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

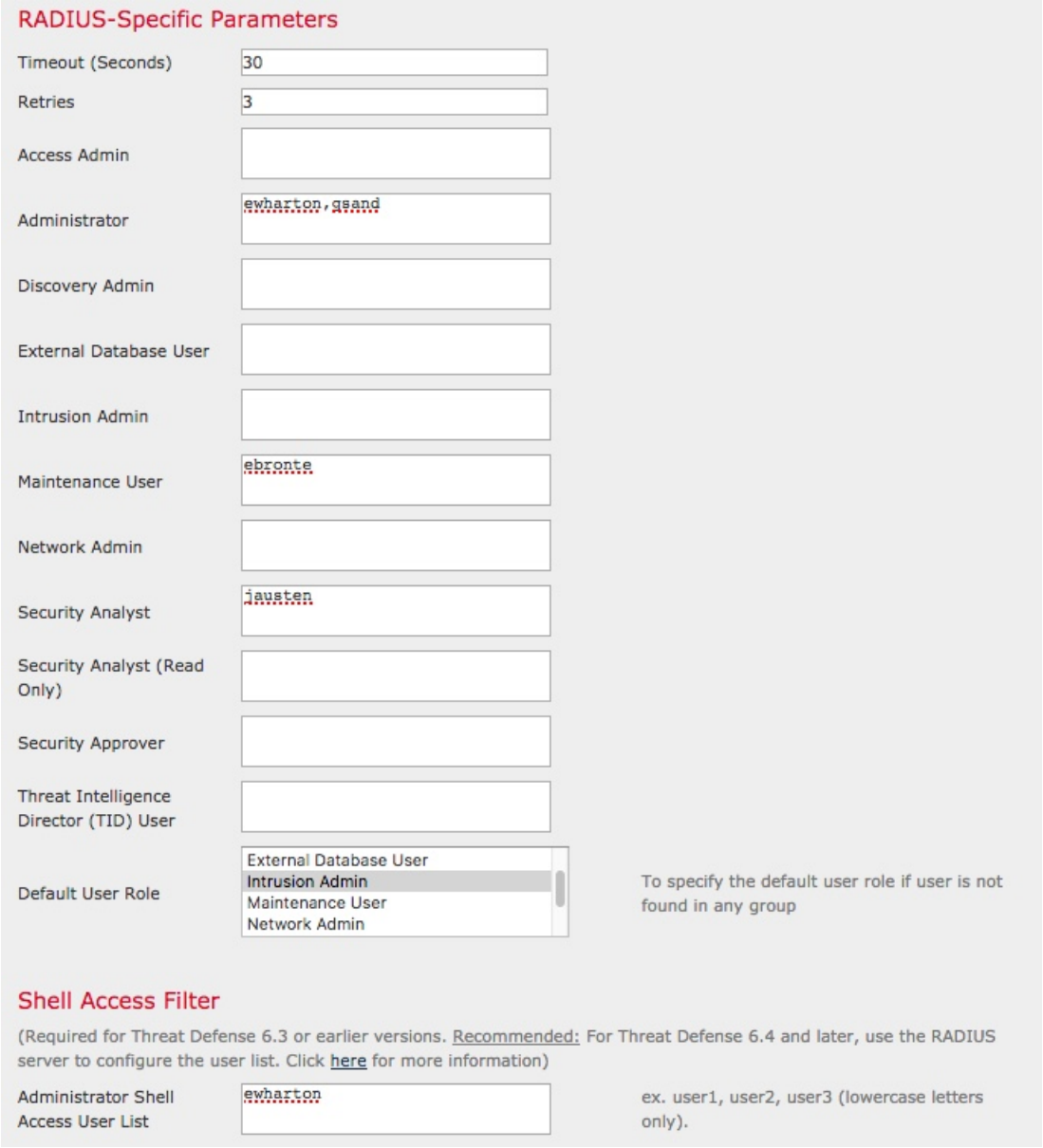
이 예에서는 RADIUS 사용자 역할 구성의 주요 측면을 보여줍니다.

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.



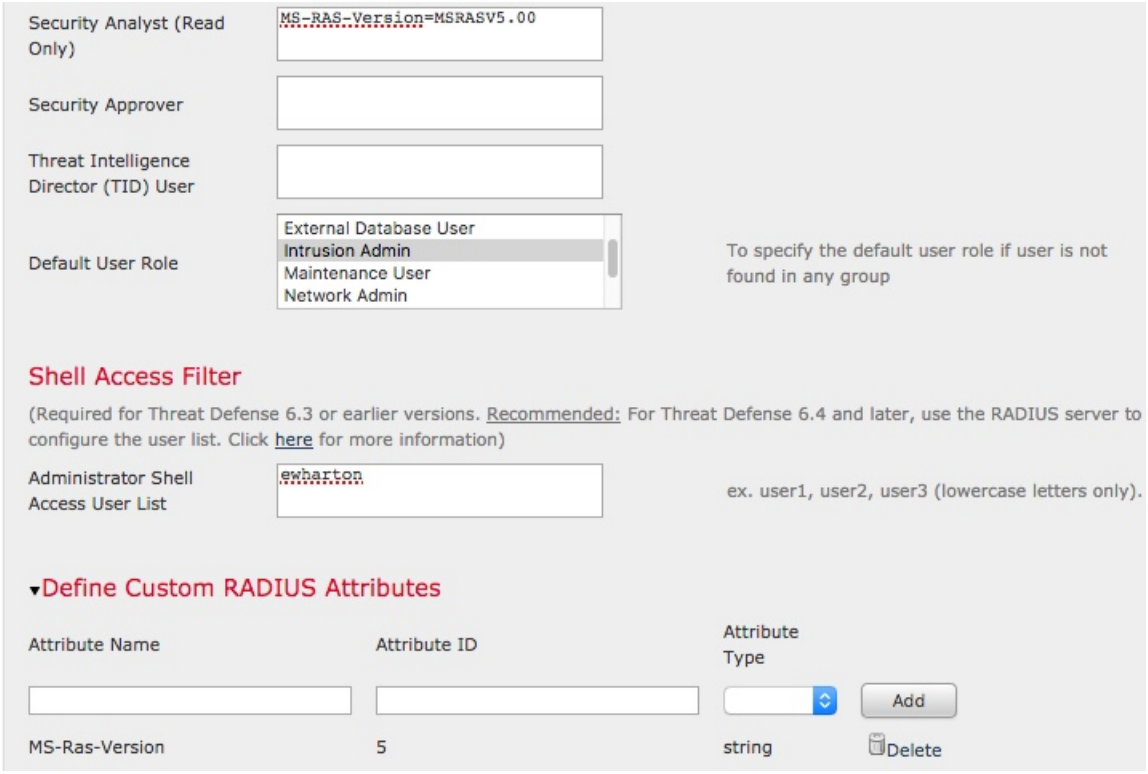
다음 그림은 이 예시에서의 역할 구성을 나타냅니다.

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 보여줍니다.

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 사용자가 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.



FMC 사용자에 대한 외부 인증 활성화

관리 사용자에 대한 외부 인증을 활성화하는 경우, External Authentication(외부 인증) 개체에 지정된 대로 FMC이 LDAP 또는 RADIUS 서버로 사용자 크리덴셜을 확인합니다.

시작하기 전에

FMC에 대한 LDAP 외부 인증 개체 추가, 11 페이지 및 FMC에 대한 RADIUS 외부 인증 개체 추가, 18 페이지에 따라 외부 인증 개체를 1개 이상 추가합니다.

프로시저

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

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

단계 **3** 외부 웹 인터페이스 사용자에 대한 기본 사용자 역할을 설정합니다.

역할이 없는 사용자가 어떤 작업도 수행할 수 없습니다. 외부 인증 개체에 정의된 사용자 역할이 이 기본 사용자 역할보다 우선합니다.

a) **Default User Roles(**기본 사용자 역할**)** 값을 클릭합니다(기본적으로 none(해당 없음) 선택됨).

a) **Default User Role Configuration(**기본 사용자 역할 구성**)** 대화 상자에서 사용하려는 역할(복수 가능)을 선택합니다.

b) **Save(**저장**)**를 클릭합니다.

단계 **4** 사용하려는 각 외부 인증 개체 옆 슬라이더 활성화됨( )를 클릭합니다. 개체를 1개 이상 활성화하는 경우, 사용자가 지정된 순서대로 서버와 비교됩니다. 다음 단계를 참조하고 서버를 재정렬합니다.

셸 인증을 활성화 하는 경우에 셸 액세스 필터를 포함 하는 외부 인증 개체를 활성화 해야 합니다. 또한 CLI 액세스 사용자는 인증 개체가 목록에서 순위가 가장 높은 서버에 대해서만 인증할 수 있습니다.

단계 **5** (선택 사항) 인증 요청이 발생한 경우 서버를 드래그 앤 드롭하고 인증 순서를 변경합니다.

단계 **6** 외부 사용자에 대해 CLI 액세스를 허용하려면, **Shell Authentication(**셸 인증**)** > **Enabled(**활성화**)**를 선택합니다.

첫 번째 외부 인증 개체 이름이 **Enabled(**활성화**)** 옵션 옆에 표시되고 첫 번째 개체만 CLI 액세스에 사용된다고 알립니다.

단계 **7** **Save and Apply(**저장 및 적용**)**를 클릭합니다.

LADP로 CAC(Common Access Card) 인증 구성

조직에서 CAC(Common Access Card)를 사용할 경우, LDAP 인증을 설정하여 웹 인터페이스에 로그인하는 FMC 사용자를 인증할 수 있습니다. CAC 인증으로 사용자는 어플라이언스에 별도의 사용자 이름과 비밀번호를 제공하지 않고 곧바로 로그인할 수 있습니다.

CAC 인증 사용자는 EDIPI(electronic data interchange personal identifier) 번호로 식별됩니다.

24시간 동안 활동이 없는 경우, 디바이스가 CAC 인증 사용자를 **Users(**사용자**)** 탭에서 삭제합니다. 다음에 로그인할 때마다 사용자가 다시 추가되지만, 사용자 역할에 대한 수동 변경사항은 다시 구성해야 합니다.

시작하기 전에

CAC 컨피그레이션 프로세스의 일환으로 사용자 인증서를 활성화하려면 브라우저에 유효한 사용자 인증서(여기서는 CAC를 통해 브라우저에 전달된 인증서)가 반드시 있어야 합니다. CAC 인증 및 권한 부여를 구성하면 네트워크의 사용자는 브라우징 세션 내내 CAC 연결을 유지해야 합니다. 세션 중

에 CAC를 제거하거나 대체할 경우 웹 브라우저는 세션을 종료하며 웹 인터페이스에서 로그아웃됩니다.

프로시저

단계 **1** 조직의 지침대로 CAC를 삽입합니다.

단계 **2** 브라우저에서 **https://***ipaddress_or_hostname*/로 이동합니다. 여기서*ipaddress* 또는 *hostname*은 사용자 디바이스와 일치합니다.

단계 **3** 메시지가 표시되면 1단계에서 삽입한 CAC의 PIN을 입력합니다.

단계 **4** 메시지가 표시되면, 드롭다운 목록에서 적절한 인증서를 선택합니다.

단계 **5** Login(로그인) 페이지의 **Username(**사용자 이름**)** 및 **Password(**비밀번호**)** 필드에서 Administrator(관리자) 권한이 있는 사용자로 로그인합니다. 아직 CAC 크리덴셜을 사용하여 로그인 할 수 없습니다 .

단계 **6** **System** > **Users** > **External Authentication**(시스템 사용자 외부 인증)을 선택합니다.

단계 **7** FMC에 대한 LDAP 외부 인증 개체 추가, 11 페이지의 절차에 따라 CAC 전용 LDAP 인증 개체를 생성합니다. 다음 항목을 구성해야 합니다.

- **CAC** 확인란
- **LDAP-Specific Parameters(LDAP** 관련 매개변수**)** > **Show Advanced Options(**고급 옵션 표시**)** > **User Name Template(**사용자 이름 템플릿**)**
- **Attribute Mapping(**속성 매핑**)** > **UI Access Attribute(UI** 액세스 속성**)**

단계 **8** **Save(**저장**)**를 클릭합니다.

단계 **9** FMC 사용자에 대한 외부 인증 활성화, 23 페이지에 설명된 대로 외부 인증 및 CAC 인증을 활성화합니다.

단계 **10** **System(**시스템**)** > **Configuration(**구성**)**를 선택하고 **HTTPS Certificate(HTTPS** 인증서**)**를 클릭합니다.

단계 **11** 필요하다면 HTTPS 서버 인증서 가져오기에 설명된 절차에 따라 HTTPS 서버 인증서를 가져옵니다.

사용하려는 CAC에서 동일한 CA(인증 기관)이 HTTPS 서버 인증서와 사용자 인증서를 발급해야 합니다.

단계 **12** **HTTPS User Certificate Settings(HTTPS** 사용자 인증서 설정**)**에서 **Enable User Certificates(**사용자 인증서 활성화**)**를 선택합니다. 자세한 내용은 유효한 HTTPS 클라이언트 인증서 필요를 참고하십시오.

단계 **13** CAC 크리덴셜로 Firepower Management Center에 로그인에 따라 디바이스에 로그인합니다.

SAML SSO(Single Sign-On) 구성

조직의 다른 애플리케이션뿐만 아니라 FMC에 로그인하는 사용자에게 인증 및 권한 부여를 제공하는 시스템 인 SSO(Single Sign-On)를 사용하도록 FMC를 구성할 수 있습니다. 이러한 SSO 설정에 참

여하도록 구성된 애플리케이션은 페더레이션 서비스 제공자 애플리케이션이라고 합니다. SSO 사용자는 한 번 로그인하면 동일한 페더레이션의 멤버인 모든 서비스 제공자 애플리케이션에 액세스할 수 있습니다.

SAML SSO(Single Sign-On)

SSO용으로 구성된 FMC는 로그인 페이지에 단일 로그인 링크를 제공합니다. SSO 액세스를 위해 구성된 사용자가 이 링크를 클릭하면 FMC 로그인 페이지에서 사용자 이름과 암호를 제공하지 않고 인증 및 권한 부여를 위해 IdP로 리디렉션됩니다. IdP에서 성공적으로 인증되면 SSO 사용자는 FMC 웹 인터페이스로 다시 리디렉션되고 로그인됩니다.이를 수행하기 위해 FMC와 IdP 간의 모든 통신은 브라우저를 중개자로 사용하여 수행됩니다. 따라서 FMC에서는 ID 제공자에 직접 액세스하기 위해 네트워크 연결이 필요하지 않습니다.

FMC에서는 인증 및 권한 부여를 위해 SAML(Security Assertion Markup Language) 2.0 공개 표준을 준수하는 SSO 제공자를 사용하는 SSO를 지원합니다. FMC 웹 인터페이스는 다음 SSO 제공자에 대한 구성 옵션을 제공합니다.

- Okta
- OneLogin
- Azure
- PingID의 PingOne for Customers 클라우드 솔루션

Note Cisco Secure Sign On SSO 제품은 FMC를 사전 통합된 서비스 제공자로 인식하지 않습니다.

FMC에 대한 SSO 지침

FMC를 SSO 연합 멤버로 설정할 때는 다음 사항에 유의하십시오.

- FMC는 한 번에 하나의 SSO 제공자만 있는 SSO를 지원할 수 있습니다. 예를 들어, SSO용 OneLogin 및 Okta를 모두 사용하도록 FMC를 설정할 수 없습니다.
- FMC고가용성 설정의 FMC는 SSO를 지원할 수 있지만, 다음 사항을 고려해야 합니다.
  - SSO 설정은 고가용성 쌍의 멤버 간에 동기화되지 않습니다. 쌍의 각 멤버에서 SSO를 별도로 설정해야 합니다.
  - 고가용성 쌍의 두 FMC는 모두 SSO에 동일한 IdP를 사용해야 합니다. SSO에 대해 설정된 각 FMC의 IdP에서 서비스 제공자 애플리케이션을 설정해야 합니다.
  - 둘 다 SSO를 지원하도록 설정된 FMC 고가용성 쌍에서는 사용자가 SSO를 사용하여 보조 FMC에 처음으로 액세스하기 전에 먼저 사용자가 SSO를 통해 기본 FMC에 한 번 이상 로그인해야합니다.
  - 고가용성 쌍에서 FMC에 대해 SSO를 설정하는 경우:
    - 기본 FMC에서 SSO를 설정하는 경우, 보조 FMC에서 SSO를 설정할 필요가 없습니다.

- 보조 FMC에서 SSO를 설정하는 경우, 기본 FMC에서도 SSO를 설정해야 합니다. (SSO 사용자는 보조 FMC에 로그인하기 전에 기본 FMC에 한 번 이상 로그인해야 하기 때문입니다.)

- 멀티테넌시를 사용하는 FMC에서 SSO 구성은 전역 도메인 레벨에서만 적용할 수 있으며, 전역 도메인 및 모든 하위 도메인에 적용됩니다.
- 내부 또는 LDAP 또는 RADIUS에 의해 인증된 관리자 역할의 사용자만 SSO를 설정할 수 있습니다.
- FMC는 IdP에서 시작된 SSO를 지원하지 않습니다.
- FMC는 SSO 계정에 대한 CAC 자격 증명을 사용한 로그인을 지원하지 않습니다.
- CC 모드를 사용하는 구축에서는 SSO를 설정하지 마십시오.
- SSO 활동은 Subsystem(하위 시스템) 필드에 Login(로그인) 또는 Logout(로그아웃)이 지정된 FMC 감사 로그에 기록됩니다.

Related Topics

Firepower Management Center 고가용성
도메인 관리
CAC 크리덴셜로 Firepower Management Center에 로그인
보안 인증 컴플라이언스
감사 기록

SSO 사용자 계정

ID 공급자는 사용자 및 그룹 구성을 직접 지원할 수도 있고, Active Directory, RADIUS 또는 LDAP와 같은 다른 사용자 관리 애플리케이션에서 사용자 및 그룹을 가져올 수도 있습니다. 이 문서에서는 IdP 사용자 및 그룹이 이미 설정되어 있다고 가정하고 SSO를 지원하도록 IdP와 작동하도록 FMC를 구성하는 방법을 중점적으로 다룹니다. 다른 사용자 관리 애플리케이션의 사용자 및 그룹을 지원하도록 IdP를 구성하려면 IdP 벤더 설명서를 참조하십시오.

사용자 이름 및 암호를 포함하여 SSO 사용자에 대한 대부분의 계정 특성은 IdP에서 설정됩니다. SSO 계정은 처음 로그인할 때까지 FMC 웹 인터페이스 사용자 페이지에 나타나지 않습니다.

Note FMC에서는 SSO 계정의 사용자 이름과 SAML 로그인 프로세스 중에 IdP가 FMC에 전송하는 NameID 속성이 모두 유효한 이메일 주소여야 합니다. 대부분의 IdP는 자동으로 NameID 속성으로 로그온하려는 사용자의 사용자 이름을 사용하지만, 이 기능이 현재 사용 중인 IdP에도 적용되는지 확인해야 합니다. IdP에서 서비스 제공자 애플리케이션을 설정하고 FMC에 SSO 액세스 권한을 부여할 IdP 사용자 계정을 생성할 때 이 점에 유의하십시오.

SSO 사용자에 대한 다음 계정 특성은 **System(**시스템**)** > **User(**사용자**)** > **Edit User(**사용자 편집**)** 아래의 FMC 웹 인터페이스에서 구성할 수 있습니다.

- 실제 이름
- 브라우저 세션 시간 초과에서 제외

SSO 사용자에 대한 사용자 역할 매핑

기본적으로 FMC에 대한 SSO 액세스 권한이 부여된 모든 사용자에게는 보안 분석가(읽기 전용) 역할이 할당됩니다. 이 기본값을 변경하고 사용자 역할 매핑이 있는 특정 SSO 사용자 또는 그룹에 대해 이 기본값을 재정의할 수 있습니다. FMC SSO 구성을 설정하고 성공적으로 테스트한 후 FMC SSO 사용자가 로그인할 때 할당되는 사용자 역할을 설정하도록 사용자 역할 매핑을 구성할 수 있습니다.

사용자 역할을 매핑하려면 FMC에서 구성 설정을 SSO IdP 애플리케이션의 설정과 조정해야 합니다. 사용자 역할은 사용자 또는 IdP 애플리케이션에 정의된 그룹에 할당할 수 있습니다. 사용자는 그룹의 구성원일 수도 있고 아닐 수도 있으며, 사용자 또는 그룹 정의는 조직 내의 다른 사용자 관리 시스템(예: Active Directory)에서 IdP로 가져오거나 가져올 수 없습니다. 따라서 FMC SSO 사용자 역할 매핑을 효과적으로 구성하려면 SSO 페더레이션이 구성되는 방식과 SSO IdP 애플리케이션에서 사용자, 그룹 및 해당 역할이 할당되는 방식을 숙지해야 합니다. 이 문서에서는 사용자 역할 매핑을 지원하기 위해 IdP와 함께 작동하도록 FMC를 구성하는 방법을 중점적으로 다룹니다. IdP 내에서 사용자 또는 그룹을 생성하거나 사용자 관리 애플리케이션에서 IdP로 사용자 또는 그룹을 가져오려면 IdP 벤더 설명서를 참조하십시오.

사용자 역할 매핑에서 IdP는 FMC 서비스 공급자 애플리케이션에 대한 역할 특성을 유지하며, 해당 FMC에 대한 액세스 권한이 있는 각 사용자 또는 그룹은 역할 특성에 대한 문자열 또는 식으로 구성됩니다(속성 값에 대한 요구 사항은 각 IdP마다 다름). FMC에서 해당 역할 속성의 이름은 SSO 구성의 일부입니다. FMC SSO 구성에는 FMC 사용자 역할 목록에 할당된 식 목록도 포함됩니다. 사용자가 SSO를 사용하여 FMC에 로그인하면 FMC에서는 해당 사용자(또는 구성에 따라 해당 사용자 그룹)의 역할 속성 값을 각 FMC 사용자 역할의 식과 비교합니다. FMC에서는 식이 사용자가 제공한 속성 값과 일치하는 모든 역할을 사용자에게 할당합니다.

Note 개별 권한 또는 그룹 권한에 따라 FMC 역할을 매핑하도록 설정할 수 있지만, 단일 FMC 애플리케이션은 그룹 및 개별 사용자 모두에 대해 역할 매핑을 지원할 수 없습니다.

FMC에서 SSO(Single Sign-On) 활성화

Before you begin

- SAML SSO 관리 애플리케이션에서 FMC에 대한 서비스 제공자 애플리케이션을 구성하고 서비스 제공자 애플리케이션에 사용자 또는 그룹을 할당합니다.
  - Okta용 FMC 서비스 제공자 애플리케이션을 구성하려면 Okta를 위한 FMC 서비스 제공자 애플리케이션 구성, on page 31의 내용을 참조하십시오.
  - OneLogin용 FMC 서비스 제공자 애플리케이션을 구성하려면 OneLogin에 대한 FMC 서비스 제공자 애플리케이션 구성, on page 43의 내용을 참조하십시오.

- Azure 용 FMC 서비스 제공자 애플리케이션을 구성하려면 *Azure*용 *FMC* 서비스 제공자 애플리케이션 구성, 21 페이지를 참조하십시오.
- PingID의 PingOne for Customers 클라우드 솔루션에 대해 FMC 서비스 제공자 애플리케이션을 구성하려면 PingID PingOne for Customers에 대한 FMC 서비스 제공자 애플리케이션 설정, on page 69의 내용을 참조하십시오.
- SAML 2.0 호환 SSO 제공자에 대해 FMC 서비스 제공자 애플리케이션을 구성하려면 SAML 2.0 호환 SSO 제공자에 대한 FMC 서비스 제공자 애플리케이션 구성, on page 74의 내용을 참조하십시오.

Procedure

단계 **1** 시스템 > 사용자 > **SSO(Single Sign-On)**를 선택합니다.

단계 **2** **SSO(Single Sign-On)** 구성 슬라이더를 클릭하여 SSO를 활성화합니다.

단계 **3** **Configure SSO(SSO** 구성**)** 버튼을 클릭합니다.

단계 **4** **Select FMC SAML Provider(FMC SAML** 제공자 선택**)** 대화 상자에서 선택한 SSO IdP 라디오 버튼을 클릭하고 **Next(**다음**)**를 클릭합니다.

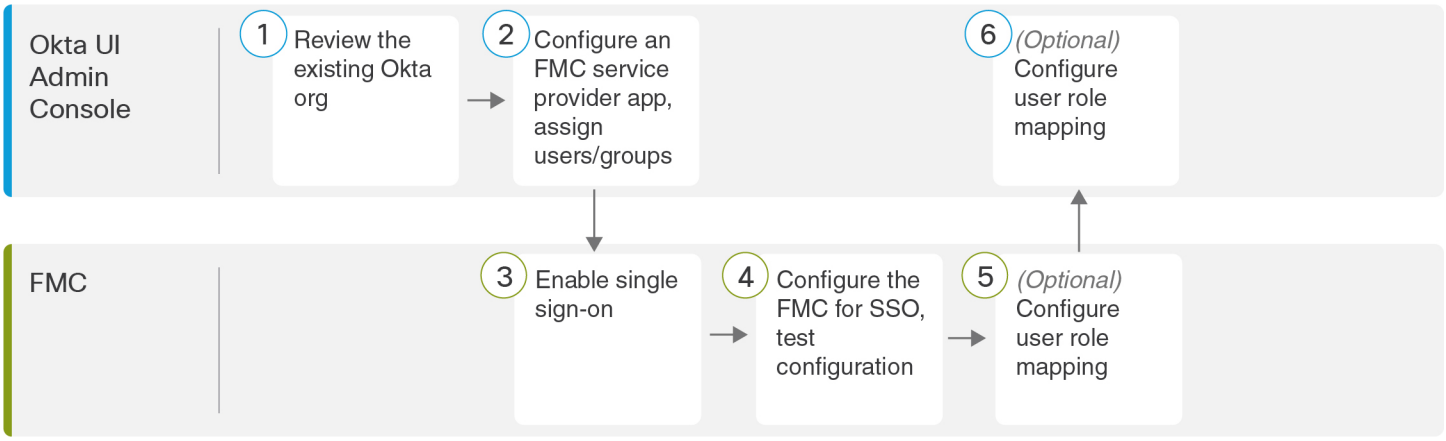
What to do next

선택한 SSO 제공자에 적합한 지침을 진행합니다.

- Okta SSO용 FMC를 구성합니다. Okta SSO용 FMC 구성, on page 32의 내용을 참조하십시오.
- PingID의 PingOne for Customers 클라우드 솔루션을 사용하여 SSO용 FMC를 구성합니다. PingID PingOne for Customers을 사용하여 SSO용 FMC을 구성합니다., on page 71의 내용을 참조하십시오.
- Azure SSO용 FMC를 구성합니다. Azure SSO용 FMC 구성, on page 58의 내용을 참조하십시오.
- OneLogin SSO용 FMC를 구성합니다. OneLogin SSO용 FMC 구성, on page 45의 내용을 참조하십시오.
- SAML 2.0 호환 제공자를 사용하여 SSO용 FMC를 구성합니다. SAML 2.0 호환 SSO 제공자를 사용하여 SSO용 FMC 구성, on page 75의 내용을 참조하십시오.

Okta로 SSO(Single Sign-On) 구성

Okta를 사용하여 SSO를 구성하려면 다음 작업을 참조하십시오.



1	Okta UI 관리 콘솔	Okta 조직 검토, on page 30
2	Okta UI 관리 콘솔	Okta를 위한 FMC 서비스 제공자 애플리케이션 구성, on page 31
3	FMC	FMC에서 SSO(Single Sign-On) 활성화, on page 28
4	FMC	Okta SSO용 FMC 구성, on page 32
5	FMC	Okta에 대한 사용자 역할 매핑 구성 FMC, on page 33
6	Okta UI 관리 콘솔	Okta IdP에서 사용자 역할 매핑 구성, on page 34

Okta 조직 검토

Okta에서는 사용자가 동일한 SSO 계정으로 액세스할 수 있는 모든 페더레이션 디바이스 및 애플리케이션을 포함하는 엔티티를 *org*라고 합니다. Okta 조직에 FMC를 추가하기 전에 해당 구성을 숙지하십시오. 다음 질문을 검토하십시오.

- FMC에 액세스할 수 있는 사용자는 몇 명입니까?
- 사용자가 Okta org 내 그룹 구성원입니까?
- 사용자 및 그룹 정의가 Okta의 기본 설정이거나 Active Directory, RADIUS 또는 LDAP와 같은 사용자 관리 애플리케이션에서 가져온 것입니까?
- FMC에서 SSO를 지원하려면 Okta org에 더 많은 사용자 또는 그룹을 추가해야 합니까?
- 어떤 종류의 사용자 역할을 지정 하시겠습니까? (사용자 역할을 할당하지 않는 경우 FMC가 모든 SSO 사용자에게 구성 가능한 기본 사용자 역할을 자동으로 할당합니다.)
- 필요한 사용자 역할 매핑을 지원하려면 Okta org 내의 사용자 및 그룹을 어떻게 구성해야 합니까?

개별 권한 또는 그룹 권한에 따라 FMC 역할을 매핑하도록 구성할 수 있지만, 단일 FMC 애플리케이션은 그룹 및 개별 사용자 모두에 대해 역할 매핑을 지원할 수 없습니다.

이 문서에서는 Okta Classic UI 관리 콘솔에 대해 잘 알고 있으며 슈퍼 관리자 권한이 필요한 구성 기능을 수행할 수 있는 계정이 있다고 가정합니다. 자세한 내용은 온라인에서 확인 가능한 Okta 문서를 참조하십시오.

Okta를 위한 FMC 서비스 제공자 애플리케이션 구성

Okta Classic UI 관리 콘솔에서 이 지침을 사용하여 Okta 내에 FMC 서비스 공급자 애플리케이션을 생성하고 해당 애플리케이션에 사용자 또는 그룹을 할당합니다. SAML SSO 개념 및 Okta 관리 콘솔에 대해 숙지해야 합니다. 이 문서에서는 모든 기능을 갖춘 SSO 조직을 설정하는 데 필요한 모든 Okta 기능에 대해 설명하지는 않습니다. 예를 들어 사용자 및 그룹을 생성하거나 다른 사용자 관리 애플리케이션에서 사용자 및 그룹 정의를 가져오려면 Okta 문서를 참조하십시오.

Note FMC 애플리케이션에 사용자 그룹을 할당하려는 경우 해당 그룹의 사용자를 개인으로 할당하지 마십시오.

Note FMC는 여러 SSO 특성을 사용하는 역할 매핑을 지원할 수 없습니다. 사용자 역할 매핑 또는 그룹 역할 매핑을 선택하고 사용자 특성을 OneLogin에서 FMC로 전달하도록 단일 속성을 구성해야 합니다.

Before you begin

- SSO 페더레이션 그리고 해당 사용자 및 그룹을 숙지하십시오. Okta 조직 검토, on page 30을 참조하십시오.
- 필요한 경우 Okta 조직에서 사용자 계정 및/또는 그룹을 생성합니다.

  Note FMC에서는 SSO 계정의 사용자 이름과 SAML 로그인 프로세스 중에 IdP가 FMC에 전송하는 NameID 속성이 모두 유효한 이메일 주소여야 합니다. 대부분의 IdP는 자동으로 NameID 속성으로 로그온하려는 사용자의 사용자 이름을 사용하지만, 이 기능이 현재 사용 중인 IdP에도 적용되는지 확인해야 합니다. IdP에서 서비스 제공자 애플리케이션을 설정하고 FMC에 SSO 액세스 권한을 부여할 IdP 사용자 계정을 생성할 때 이 점에 유의하십시오.

- 대상 FMC(`https://ipaddress_or_hostname`)의 로그인 URL을 확인합니다.

  Note 여러 URL(예: 정규화된 도메인 이름 및 IP 주소)로 FMC 웹 인터페이스에 연결할 수 있는 경우, SSO 사용자는 이 작업에서 구성한 로그인 URL을 사용하여 FMC에 일관되게 액세스해야 합니다.

Procedure

단계 **1** Okta Classic UI 관리 콘솔에서 FMC용 서비스 공급자 애플리케이션을 생성합니다. 다음 항목을 선택하여 FMC 애플리케이션을 구성합니다.

- 플랫폼에 대해 **Web(웹)**을 선택합니다.
- **Sign on(로그온)** 방법으로 `SAML 2.0`을 선택합니다.
- **SSO(Single Sign On) URL**을 제공합니다.

  이는 브라우저가 IdP를 대신하여 정보를 전송하는 FMC URL입니다.

  FMC 로그인 URL에 `saml/acs` 문자열을 추가합니다. 예: `https://ExampleFMC/saml/acs`
- **Use this for Recipient URL and Destination URL(수신자 URL 및 대상 URL에 사용)**를 활성화합니다.
- 대상 **URI(SP 엔티티 ID)**를 입력합니다.

  이 이름은 종종 URL로 형식이 지정되는 서비스 제공자(FMC)의 전역 고유 이름입니다.

  FMC 로그인 URL에 `/saml/metadata` 문자열을 추가합니다. 예: `https://ExampleFMC/saml/metadata`
- **Name ID Format(이름 ID 형식)**에서 `Unspecified(지정되지 않음)`를 선택합니다.

단계 **2** (애플리케이션에 그룹을 할당하는 경우엔 선택 사항입니다.) 개별 Okta 사용자를 FMC 애플리케이션에 할당합니다. (FMC 애플리케이션에 그룹을 할당하려는 경우 해당 그룹의 멤버인 사용자를 개인으로 할당하지 마십시오.)

단계 **3** (애플리케이션에 개별 사용자를 할당하는 경우엔 선택 사항입니다.) Okta 그룹을 FMC 애플리케이션에 할당합니다.

단계 **4** (선택 사항) FMC에서 SSO를 보다 쉽게 설정할 수 있도록 FMC 서비스 공급자 애플리케이션용 SAML XML 메타 데이터 파일을 Okta에서 로컬 컴퓨터로 다운로드할 수 있습니다.

What to do next

SSO(Single Sign-On)을 활성화합니다. FMC에서 SSO(Single Sign-On) 활성화, on page 28을 참조하십시오.

Okta SSO용 FMC 구성

FMC 웹 인터페이스에서 다음 지침을 사용하십시오.

시작하기 전에

- Okta Classic UI 관리 콘솔에서 FMC 서비스 제공자 애플리케이션을 생성합니다. Okta를 위한 FMC 서비스 제공자 애플리케이션 구성, on page 31의 내용을 참조하십시오.
- SSO(Single Sign-On)을 활성화합니다. FMC에서 SSO(Single Sign-On) 활성화, on page 28의 내용을 참조하십시오.

Procedure

단계 1 (이 절차는 FMC에서 SSO(Single Sign-On) 활성화, on page 28에서 곧바로 이어집니다.) **Configure Okta Metadata(Okta** 메타데이터 구성**)**에서 두 가지 옵션을 선택할 수 있습니다.

- SSO 구성 정보를 수동으로 입력하려면 다음을 수행합니다.
  a. **Manual Configuration(**수동 구성**)** 라디오 버튼을 클릭합니다.
  b. Okta SSO 서비스 제공자 애플리케이션에서 다음 값을 입력합니다. (Okta Classic UI 관리 콘솔에서 이러한 값을 검색합니다.)
     - **ID** 제공자 **SSO(Single Sign-On) URL**
     - **ID** 제공자 발급자
     - **X.509** 인증서
- Okta에서 생성한 XML 메타데이터 파일을 로컬 컴퓨터에 저장한 경우(Okta를 위한 FMC 서비스 제공자 애플리케이션 구성, on page 31의 4단계) 파일을 FMC에 업로드할 수 있습니다.
  a. **Upload XML File(XML** 파일 업로드**)** 라디오 버튼을 클릭합니다.
  b. 화면의 지침에 따라 로컬 컴퓨터에서 XML 메타데이터 파일을 찾아 선택합니다.

단계 2 **Next(**다음**)**를 클릭합니다.

단계 3 **Verify Metadata(**메타데이터 확인**)** 대화 상자에서 설정 매개변수를 검토하고 **Save(**저장**)**를 클릭합니다.

단계 4 **Test Configuration(**컨피그레이션 테스트**)**을 클릭합니다. 시스템에 오류 메시지가 표시되면 FMC의 SSO 구성과 Okta 서비스 제공자 애플리케이션 구성을 검토하고 오류를 수정한 후 다시 시도하십시오.

단계 5 시스템에서 컨피그레이션 테스트에 성공했다고 보고하면 **Apply(**적용**)**를 클릭합니다.

What to do next

선택적으로 SSO 사용자에 대한 사용자 역할 매핑을 구성할 수 있습니다. Okta에 대한 사용자 역할 매핑 구성 FMC, on page 33의 내용을 참조하십시오. 역할 매핑을 설정하지 않기로 선택하는 경우, 기본적으로 FMC에 로그인하는 모든 SSO 사용자에게 Okta에 대한 사용자 역할 매핑 구성 FMC, on page 33의 4단계에서 설정한 사용자 역할이 할당됩니다.

Okta에 대한 사용자 역할 매핑 구성 FMC

FMC 웹 인터페이스에서 사용자 역할을 설정하는 데 구성할 필드는 선택한 SSO 제공자에 관계없이 동일합니다. 그러나 구성하는 값의 경우, 사용하는 SAML SSO 제공자가 사용자 역할 매핑을 구현하는 방식을 고려해야 합니다.

Before you begin

- Okta 사용자 그룹 매핑 정보를 검토합니다. Okta 조직 검토, on page 30의 내용을 참조하십시오.
- FMC에 대한 SSO 서비스 제공자 애플리케이션을 설정합니다. Okta를 위한 FMC 서비스 제공자 애플리케이션 구성, on page 31의 내용을 참조하십시오.
- FMC에서 SSO(Single Sign-On)를 활성화하고 설정합니다. FMC에서 SSO(Single Sign-On) 활성화, on page 28 및 Okta SSO용 FMC 구성, on page 32의 내용을 참조하십시오.

Procedure

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

단계 **2** **Single Sign-On**(단일 인증) 탭을 클릭합니다.

단계 **3** **Advanced Configuration(Role Mapping)**(고급 구성(역할 매핑))을 펼칩니다.

단계 **4** **Default User Role**(기본 사용자 역할) 드롭다운에서 FMC 사용자 역할을 선택해서 사용자를 기본값으로 할당합니다.

단계 **5** **Group Member Attribute**(그룹 멤버 속성)을 입력합니다. 이 문자열은 사용자 또는 그룹에 대한 사용자 역할을 매핑하는 데 Okta FMC 제공자 애플리케이션에 설정된 속성 이름과 일치해야 합니다. (Okta IdP에서 역할 매핑을 위한 사용자 속성 구성, on page 35의 1단계 또는 Okta IdP에서 역할 매핑을 위한 그룹 속성 구성, on page 36의 1단계 참조)

단계 **6** SSO 사용자에게 할당할 각 FMC 사용자 역할 옆에 정규식을 입력합니다. (FMC는 Golang 및 Perl에서 지원하는 Google의 RE2 정규식 표준의 제한된 버전을 사용합니다.) FMC에서는 이러한 값을 SSO 사용자 정보를 사용하여 IdP가 FMC에 전송하는 사용자 역할 매핑 속성값과 비교합니다. FMC는 사용자에게 일치하는 항목이 발견된 모든 역할의 통합을 허용합니다.

What to do next

- 서비스 제공자 애플리케이션에서 사용자 역할 매핑을 구성합니다. Okta IdP에서 사용자 역할 매핑 구성, on page 34의 내용을 참조하십시오.

Okta IdP에서 사용자 역할 매핑 구성

개별 사용자 권한 또는 그룹 권한에 따라 Okta Classic UI 관리 콘솔에서 SSO 사용자 역할 매핑을 설정할 수 있습니다.

- 개별 사용자 권한에 따라 매핑하려면 Okta IdP에서 역할 매핑을 위한 사용자 속성 구성, on page 35의 내용을 참조하십시오.
- 그룹 권한에 따라 매핑하려면 Okta IdP에서 역할 매핑을 위한 그룹 속성 구성, on page 36의 내용을 참조하십시오.

SSO 사용자가 FMC에 로그인하면 Okta는 Okta IdP에서 설정된 사용자 또는 그룹 역할 속성값을 FMC에 제공합니다. FMC에서는 해당 속성값을 SSO 설정의 각 FMC 사용자 역할에 할당된 정규식과 비교하고, 일치하는 항목이 있는 모든 역할을 사용자에게 부여합니다. (일치 항목이 없으면 FMC는 사용

자에게 설정 가능한 기본 사용자 역할을 부여합니다.) 각 FMC 사용자 역할에 할당하는 식은 Golang 및 Perl에서 지원하는 제한된 버전의 Google RE2 정규식 표준을 준수해야 합니다. FMC는 FMC 사용자 역할 식과의 비교를 위해 동일한 표준을 사용하여 Okta에서 받은 속성값을 정규식으로 처리합니다.

Note 단일 FMC는 그룹 및 개별 사용자 모두에 대해 역할 매핑을 지원할 수 없습니다. FMC 서비스 제공자 애플리케이션에 대해 하나의 매핑 방법을 선택하여 일관되게 사용해야 합니다. 또한 FMC는 Okta에 설정된 FMC 서비스 제공자 애플리케이션당 하나의 그룹 속성 명령문만 사용하여 그룹 역할 매핑을 지원할 수 있습니다. 여러 사용자가 있는 경우, 일반적으로 그룹 기반 롤 매핑은 FMC에 더 효율적입니다. Okta 조직 전체에 설정된 사용자 및 그룹 정의를 고려해야 합니다.

Okta IdP에서 역할 매핑을 위한 사용자 속성 구성

Okta 클래식 UI 관리 콘솔에서 다음 지침을 통해 Okta 기본 사용자 프로파일에 맞춤형 역할 매핑 속성을 추가합니다.

Okta 서비스 제공자 애플리케이션은 다음 두 가지 유형의 사용자 프로파일 중 하나를 사용할 수 있습니다.

- Okta 사용자 프로파일: 모든 맞춤형 속성으로 확장할 수 있습니다.
- 앱 사용자 프로파일: 지원되는 속성에 대해 타사 애플리케이션 또는 디렉토리(예: Active Directory, LDAP 또는 Radius)를 쿼리하여 Okta가 생성하는 사전 정의된 목록의 속성으로만 확장할 수 있습니다.

Okta 조직에서 사용자 프로파일 유형을 사용할 수 있습니다. 설정 방법에 대한 자세한 내용은 Okta 설명서를 참조하십시오. 어떤 사용자 프로파일 유형을 사용하든, FMC와 함께 사용자 역할 매핑을 지원하려면 FMC에 각 사용자의 역할 매핑 식을 전달하도록 프로파일에 맞춤형 속성을 구성해야 합니다.

이 문서에서는 Okta 사용자 프로파일을 통한 역할 매핑에 대해 설명합니다. 앱 프로파일을 사용하여 매핑하려면 맞춤형 속성을 설정하기 위해 조직에서 사용 중인 타사 사용자 관리 애플리케이션에 익숙해야 합니다. 자세한 내용은 Okta 설명서를 참조하십시오.

Before you begin

- Okta를 위한 FMC 서비스 제공자 애플리케이션 구성, on page 31에 설명된 대로 Okta IdP에서 FMC 서비스 제공자 애플리케이션을 설정합니다.
- Okta에 대한 사용자 역할 매핑 구성 FMC, on page 33에 설명된 대로 FMC에서 SSO 사용자 역할 매핑을 설정합니다.

Procedure

단계 **1** 기본 Okta 사용자 프로파일에 새 속성을 추가합니다.

- **Data type(**데이터 유형**)**은 `string`으로 선택합니다.

- Okta IdP가 FMC로 보낼 변수 이름을 제공합니다. 여기에는 사용자 역할 매핑에 일치하는 식이 포함되어 있습니다. 이 변수 이름은 **Group Member Attribute(**그룹 멤버 속성**)**에 대해 FMC SSO 설정에서 입력한 문자열과 일치해야 합니다. (Okta에 대한 사용자 역할 매핑 구성 FMC, on page 33의 5단계 참조)

단계 **2** 이 프로파일을 사용하여 FMC 서비스 제공자 애플리케이션에 할당된 각 사용자에 대해 방금 생성한 사용자 역할 속성에 값을 할당합니다.

식을 사용하여 FMC에서 사용자에게 할당할 역할을 나타냅니다. FMC에서는 이 문자열을 Okta에 대한 사용자 역할 매핑 구성 FMC, on page 33의 6단계에서 각 FMC 사용자 역할에 할당한 식과 비교합니다. (FMC 사용자 역할 식과 비교하기 위해 FMC에서는 Okta에서 수신한 속성값을 Golang 및 Perl에서 지원하는 Google RE2 정규식 표준의 제한된 버전을 준수하는 식으로 처리합니다.)

Okta IdP에서 역할 매핑을 위한 그룹 속성 구성

Okta Classic UI 관리 콘솔에서 다음 지침을 통해 사용자 지정 역할 매핑 그룹 속성을 FMC 서비스 공급자 애플리케이션에 추가하십시오. FMC는 Okta FMC 서비스 제공자 애플리케이션당 하나의 그룹 속성 명령문만 사용하여 그룹 역할 매핑을 지원할 수 있습니다.

Okta 서비스 제공자 애플리케이션은 다음 두 가지 유형의 그룹 중 하나를 사용할 수 있습니다.

- Okta 그룹: 모든 맞춤형 속성으로 확장할 수 있습니다.
- 애플리케이션 그룹: 지원되는 속성에 대해 타사 애플리케이션 또는 디렉토리(예: Active Directory, LDAP 또는 Radius)를 쿼리하여 Okta가 생성하는 사전 정의된 목록의 속성으로만 확장할 수 있습니다.

Okta 조직에서 두 가지 유형의 그룹을 사용할 수 있습니다. 설정 방법에 대한 자세한 내용은 Okta 설명서를 참조하십시오. 어떤 그룹 유형을 사용하든 간에 FMC와 함께 사용자 역할 매핑을 지원하려면 FMC에 그룹에 대한 역할 매핑 식을 전달하기 위한 맞춤형 속성을 설정해야 합니다.

이 문서에서는 Okta 그룹을 사용한 역할 매핑에 대해 설명합니다. 애플리케이션 그룹과 매핑하려면 맞춤형 속성을 설정하기 위해 조직에서 사용 중인 타사 사용자 관리 애플리케이션에 익숙해야 합니다. 자세한 내용은 Okta 설명서를 참조하십시오.

Before you begin

- Okta IdP에서 FMC 서비스 제공자 애플리케이션을 설정합니다. Okta를 위한 FMC 서비스 제공자 애플리케이션 구성, on page 31의 내용을 참조하십시오.
- FMC에서 사용자 역할 매핑을 설정합니다. Okta에 대한 사용자 역할 매핑 구성 FMC, on page 33의 내용을 참조하십시오.

Procedure

FMC 서비스 제공자 애플리케이션에 대한 새 SAML 그룹 속성을 생성합니다.

- **Name(**이름**)**에는 FMC SSO 설정에서 **Group Member Attribute(**그룹 멤버 속성**)**에 대해 입력한 것과 같은 문자열을 사용합니다. (Okta에 대한 사용자 역할 매핑 구성 FMC, on page 33의 5단계 참조)
- **Filter(**필터**)**에서 FMC가 그룹의 멤버에 할당할 역할을 나타내는 식을 지정합니다. Okta는 이 값을 사용자가 멤버인 그룹의 이름과 비교하여 FMC에 일치하는 그룹 이름을 전송합니다. 그다음 FMC는 Okta에 대한 사용자 역할 매핑 구성 FMC, on page 33의 6단계에서 각 FMC 사용자 역할에 할당한 정규식과 해당 그룹 이름을 비교합니다.

Okta 사용자 역할 매핑 예

다음 예에서와 같이 사용자 역할 매핑을 지원하기 위한 FMC의 SSO 설정은 개별 사용자 및 그룹에 대해 동일합니다. 차이점은 Okta의 FMC 서비스 제공자 애플리케이션 설정에 있습니다.

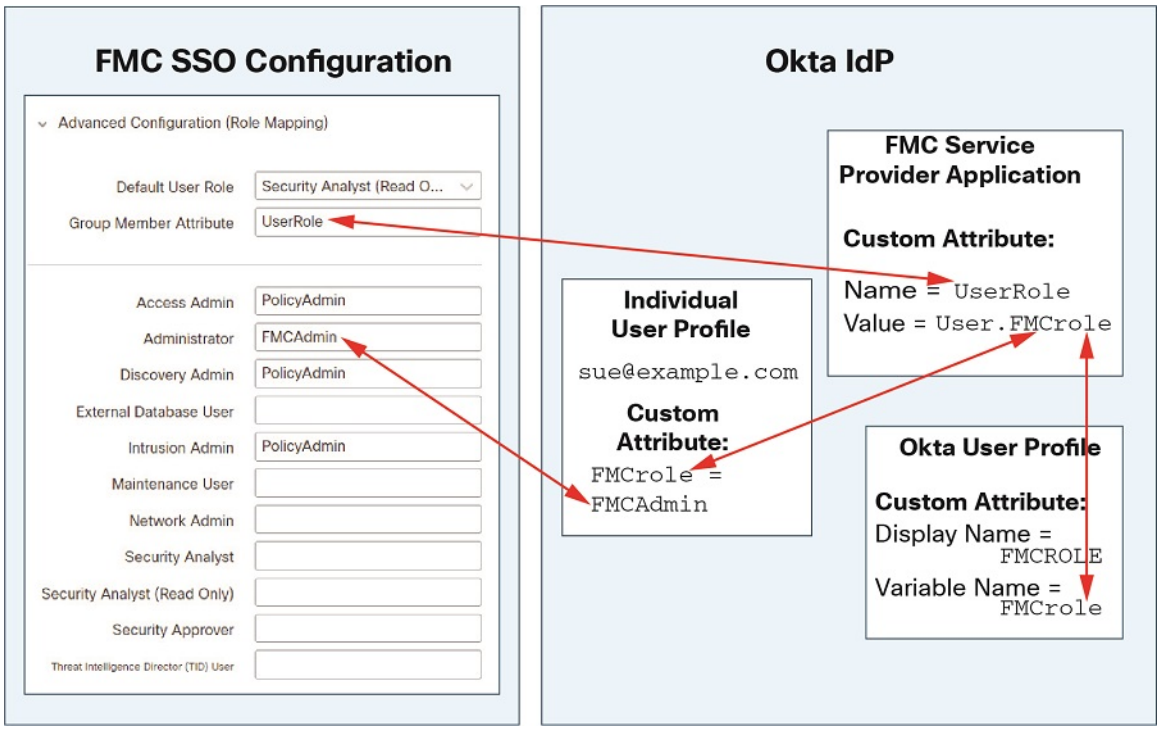
Note 개별 권한 또는 그룹 권한에 따라 FMC 역할을 매핑하도록 설정할 수 있지만, 단일 FMC 애플리케이션은 그룹 및 개별 사용자 모두에 대해 역할 매핑을 지원할 수 없습니다. 또한 FMC는 FMC에 설정된 FMC 서비스 제공자 애플리케이션당 하나의 그룹 속성 명령문만 사용하여 그룹 역할 매핑을 지원할 수 있습니다.

개별 사용자 계정의 Okta 역할 매핑 예제

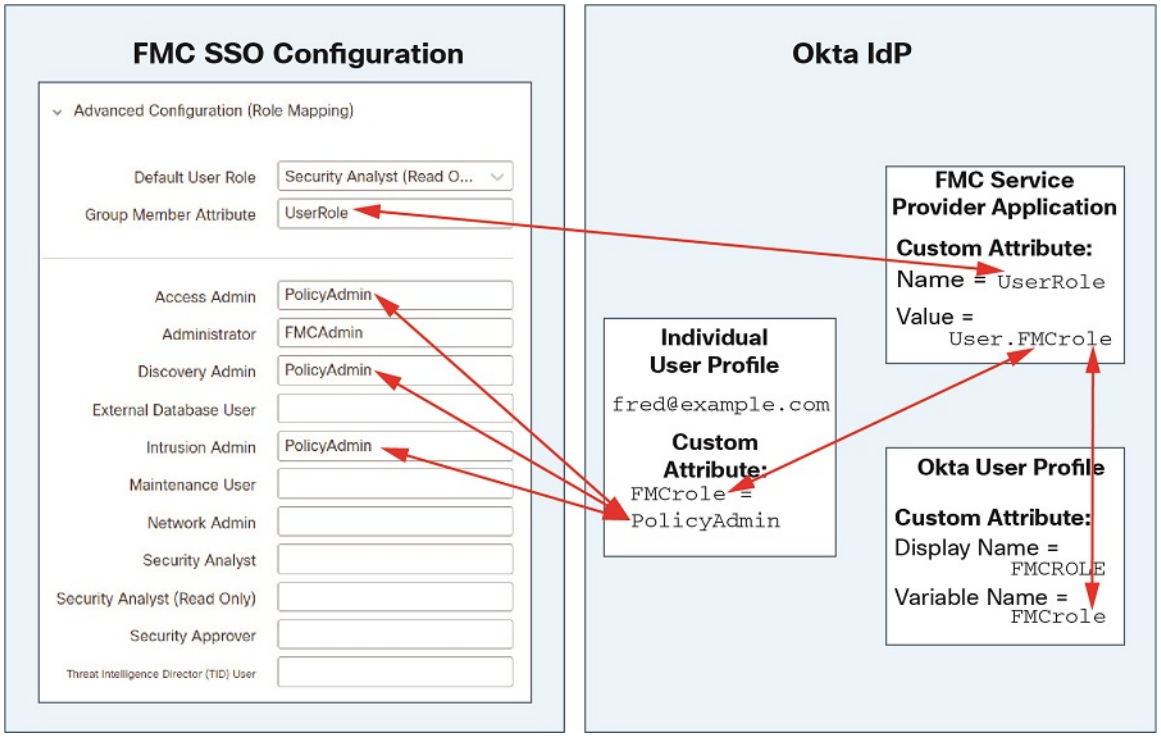
개별 사용자에 대한 역할 매핑에서 Okta FMC 서비스 애플리케이션에는 FMC의 그룹 멤버 속성 이름과 일치하는 이름을 갖는 사용자 지정 속성이 있습니다 (이 예에서는 `UserRole`). Okta의 사용자 프로파일에도 사용자 지정 속성이 있습니다(이 예에서는 `FMCrole`이라는 변수). 애플리케이션 사용자 지정 속성 `UserRole`에 대한 정의는 Okta가 사용자 역할 매핑 정보를 FMC에 전달할 때 해당 사용자에게 할당된 사용자 지정 속성값을 사용하도록 설정합니다.

다음 다이어그램은 FMC 및 Okta 설정의 관련 필드와 값이 개별 어카운트에 대한 사용자 역할 매핑에서 서로 어떻게 대응되는지를 보여줍니다. 각 다이어그램은 FMC 및 Okta UI 관리 콘솔에서 동일한 SSO 설정을 사용하지만, Okta UI 관리 콘솔의 각 사용자에 대한 설정은 FMC에서 서로 다른 방법으로 각 사용자에게 상이한 역할을 할당합니다.

- 이 다이어그램에서 sue@example.com은 `FMCrole` 값 `FMCAdmin`을 사용하며, FMC는 관리자 역할을 할당합니다.



- 이 다이어그램에서 fred@example.com은 `FMCrole` 값 `PolicyAdmin`을 사용하며, FMC는 액세스 관리자, 검색 관리자 및 침입 관리자 역할을 할당합니다.



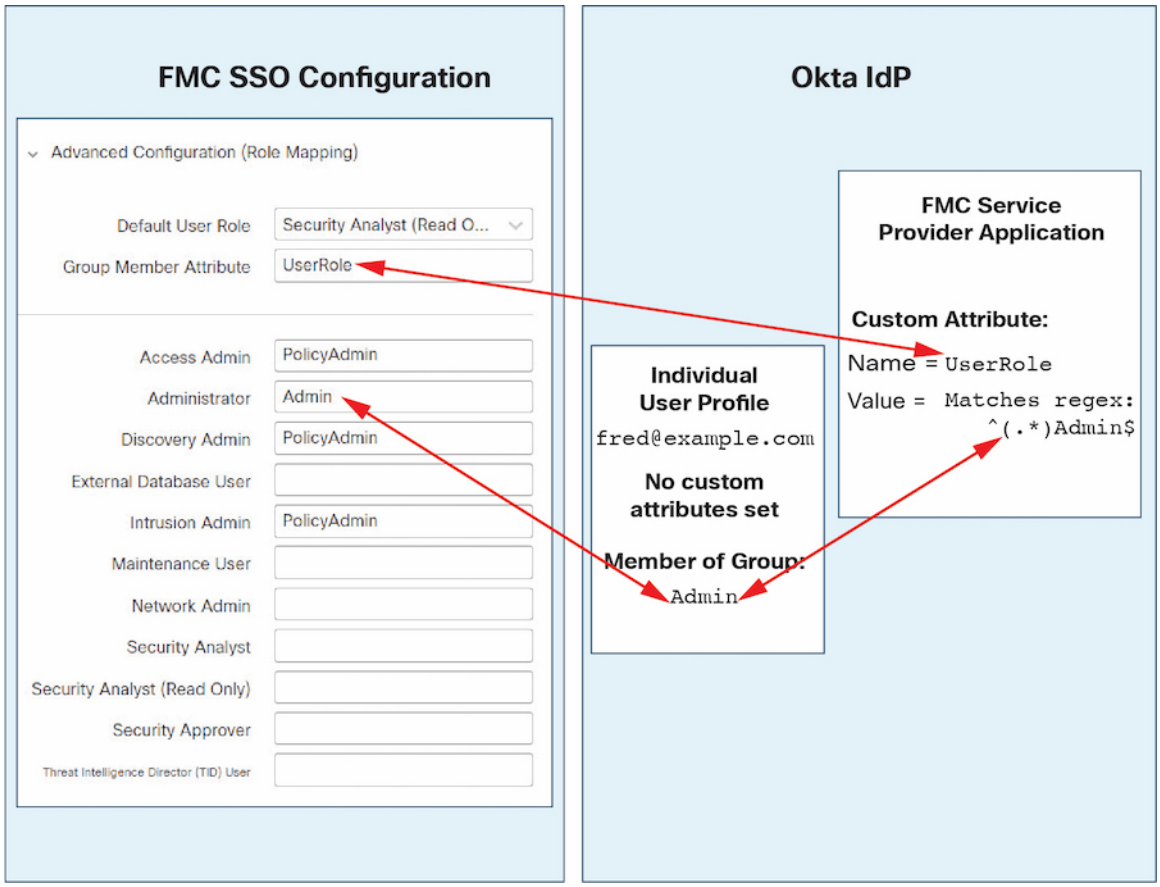
- FMC를 위해 Okta 서비스 애플리케이션에 할당된 다른 사용자에게는 다음 중 하나의 이유로 기본 사용자 역할 보안 분석가(읽기 전용)가 할당됩니다.
  - Okta 사용자 프로파일에서 `FMCrole` 변수에 할당된 값이 없습니다.
  - Okta 사용자 프로필에서 `FMCrole` 변수에 할당된 값이 FMC의 SSO 설정에서 사용자 역할에 대해 구성된 식과 일치하지 않습니다.

그룹에 대한 **Okta** 역할 매핑 예

그룹에 대한 역할 매핑에서 Okta FMC 서비스 애플리케이션에는 FMC의 그룹 멤버 속성의 이름(이 예에서는 `UserRole`)과 일치하는 이름을 갖는 사용자 지정 그룹 속성이 있습니다. Okta는 FMC SSO 로그인 요청을 처리할 때 사용자의 그룹 멤버십을 서비스 FMC 애플리케이션 그룹 속성(이 경우에는 `^(.*)Admin$`)에 할당된 식과 비교합니다. Okta는 그룹 속성과 일치하는 사용자의 그룹 멤버십을 FMC에게 전송합니다. FMC에서는 수신하는 그룹 이름을 각 사용자 역할에 대해 구성한 정규식과 비교하고 그에 따라 사용자 역할을 할당합니다.

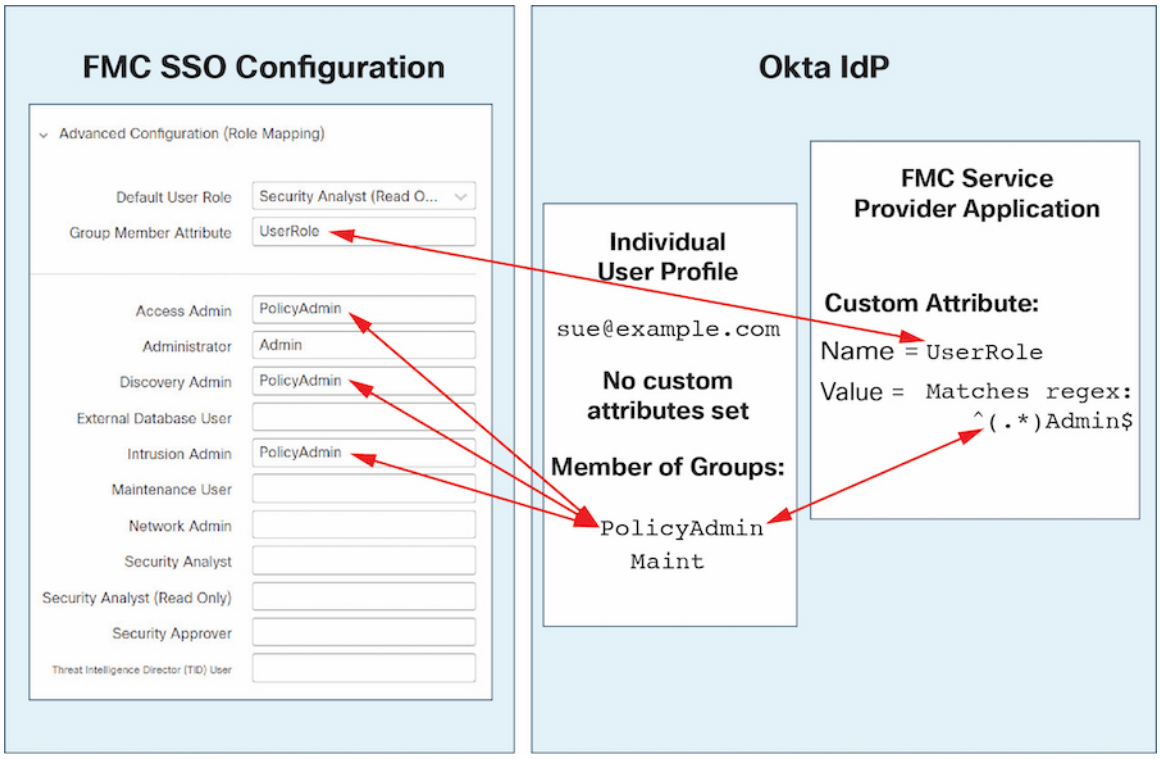
다음 다이어그램은 FMC 및 Okta 구성의 관련 필드와 값이 그룹에 대한 사용자 역할 매핑에서 서로 어떻게 일치하는지를 보여줍니다. 각 다이어그램은 FMC 및 Okta UI 관리 콘솔에서 동일한 SSO 설정을 사용하지만, Okta UI 관리 콘솔의 각 사용자에 대한 설정은 FMC에서 서로 다른 방법으로 각 사용자에게 상이한 역할을 할당합니다.

- 이 다이어그램에서 fred@example.com은 Okta IdP 그룹 `Admin`의 멤버이며 `^ (.*)Admin$` 식과 일치합니다. Okta는 FMC Fred의 `관리자` 그룹 멤버십을 전송하고 FMC는 관리자에게 관리자 역할을 할당합니다.

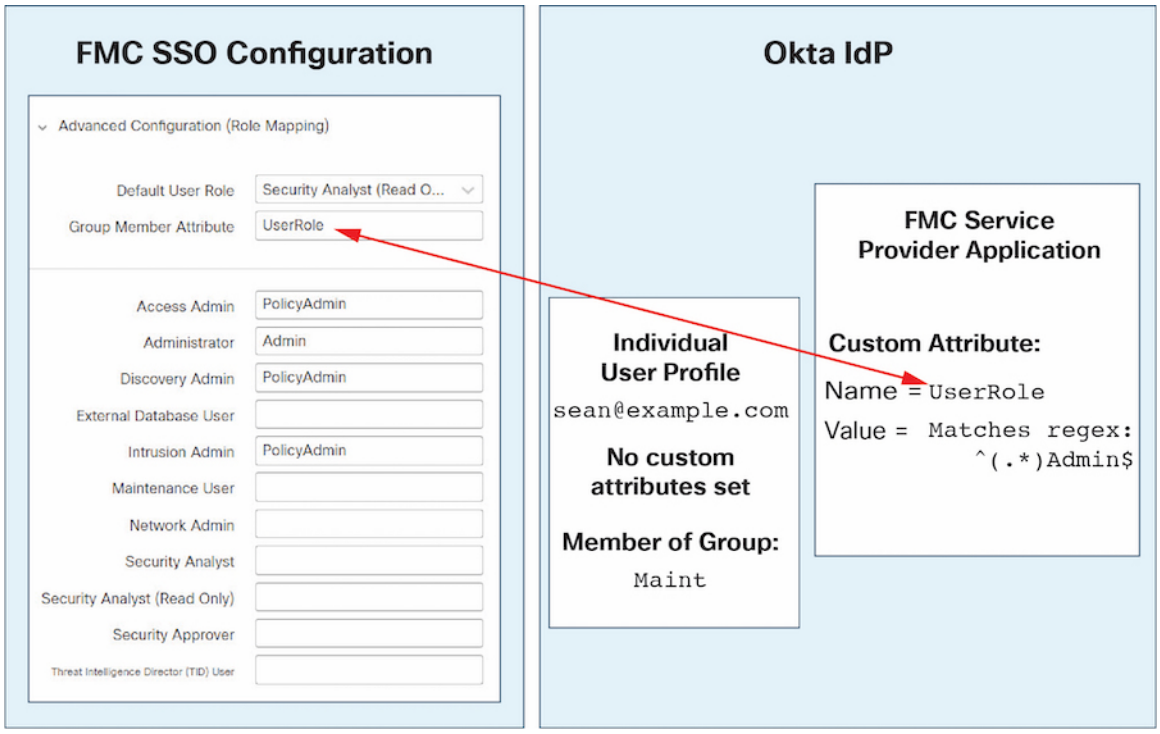


- 이 다이어그램에서 sue@example.com은 `^(.*)Admin$` 식과 일치하는 Okta IdP 그룹 `PolicyAdmin`의 멤버입니다. Okta는 FMC Sue의 `PolicyAdmin` 그룹 멤버십을 전송하고 FMC에서 Access Admin, Discovery Admin 및 Intrusion Admin 역할을 할당합니다.

  Sue는 Okta 그룹 `Maint`의 멤버이지만이 그룹 이름이 Okta FMC 서비스 애플리케이션의 그룹 멤버십 속성에 할당된 식과 일치하지 않으므로 Okta는 Sue의 `Maint` 그룹 멤버십에 대한 정보를 FMC에 전송하지 않습니다. `Maint` 그룹은 FMC가 그녀에게 할당하는 역할에 참여하지 않습니다.



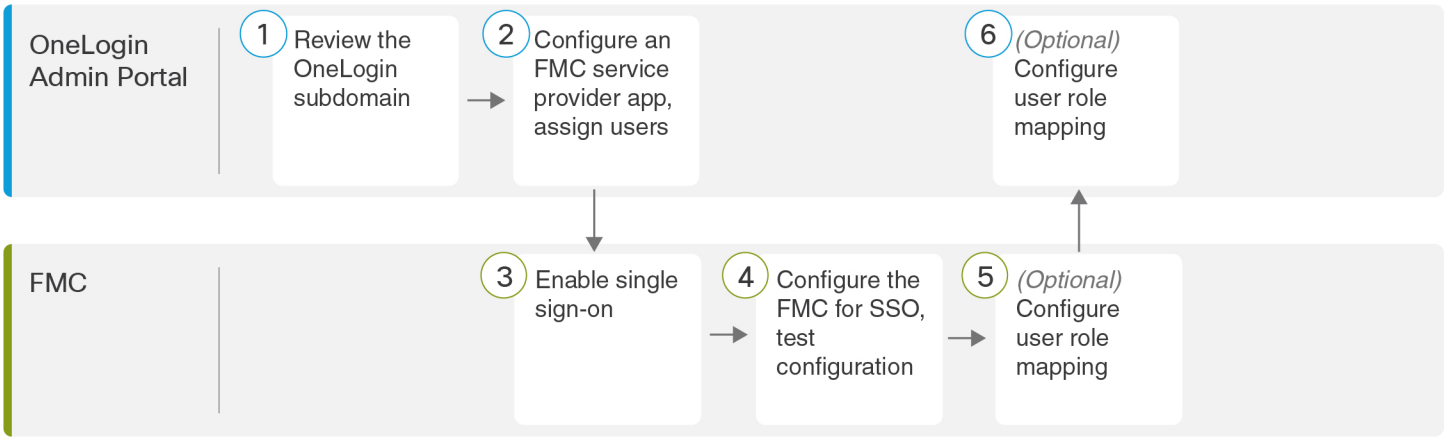
- 이 다이어그램에서 sean@example.com은 Okta IdP 그룹 `Maint`의 멤버입니다. 이 그룹 이름은 `^(.*)Admin$` 식과 일치하지 않습니다. 따라서 sean@example.com이 FMC에 로그인하면 Okta는 `Maint` 그룹 멤버십에 대한 정보를 FMC로 전송하지 않으며, Sean은 유지 보수 사용자 역할이 아닌(보안 분석가(읽기 전용)) 기본 사용자 역할(보안)을 할당 받습니다.



이 다이어그램은 역할 매핑 전략을 설정할 때 사전 계획의 중요성을 보여줍니다. 이 예에서는 `Maint` 그룹의 멤버인 이 FMC에 대한 액세스 권한이 있는 모든 Okta 사용자에게 기본 사용자 역할만 할당할 수 있습니다. FMC는 Okta 서비스 애플리케이션 구성에서 하나의 맞춤형 그룹 특성만 사용하도록 지원합니다. 해당 속성에 할당하는 식과 일치하도록 설정한 그룹 이름은 신중하게 작성해야 합니다. FMC SSO 구성의 사용자 역할 할당 문자열에서 정규식을 사용하여 역할 매핑에 유연성을 추가할 수 있습니다. 각 FMC 사용자 역할에 할당하는 식은 Golang 및 Perl에서 지원하는 제한된 버전의 Google RE2 정규식 표준을 준수해야 합니다.

OneLogin으로 SSO(Single Sign-On) 구성

OneLogin을 사용하여 SSO를 구성하려면 다음 작업을 참조하십시오.



1	FMC	OneLogin 하위 도메인 검토, on page 43
2	FMC	OneLogin에 대한 FMC 서비스 제공자 애플리케이션 구성, on page 43
3	OneLogin 관리 포털	FMC에서 SSO(Single Sign-On) 활성화, on page 28
4	OneLogin 관리 포털	OneLogin SSO용 FMC 구성, on page 45
5	OneLogin 관리 포털	FMC에서 OneLogin 사용자 역할 매핑 구성, on page 46
6	FMC	OneLogin IdP에서 사용자 역할 매핑 구성, on page 47

OneLogin 하위 도메인 검토

OneLogin에서는 사용자가 동일한 SSO 계정으로 액세스할 수 있는 모든 페더레이션 디바이스 및 애플리케이션을 포함하는 엔티티를 하위 도메인이라고 합니다. OneLogin 하위 도메인에 FMC를 추가하기 전에 해당 구성을 숙지하십시오. 다음 질문을 검토하십시오.

- FMC에 액세스할 수 있는 사용자는 몇 명입니까?
- 사용자가 그룹의 OneLogin 하위 도메인 구성원 내에 있습니까?
- Active Directory, Google Apps 또는 LDAP와 같은 서드 파티 디렉터리의 사용자 및 그룹이 OneLogin 하위 도메인과 동기화됩니까?
- FMC에서 SSO를 지원하려면 OneLogin 하위 도메인에 더 많은 사용자 또는 그룹을 추가해야 합니까?
- 어떤 종류의 FMC 사용자 역할을 지정 하시겠습니까? (사용자 역할을 할당하지 않는 경우 FMC가 모든 SSO 사용자에게 구성 가능한 기본 사용자 역할을 자동으로 할당합니다.)
- 필요한 사용자 역할 매핑을 지원하려면 OneLogin 하위 도메인 내의 사용자 및 그룹을 어떻게 구성해야 합니까?

개별 사용자 또는 그룹을 기준으로 매핑할 FMC 역할을 구성할 수 있지만 단일 FMC 애플리케이션이 그룹 및 개별 사용자 모두에 대해 역할 매핑을 지원할 수는 없습니다.

이 문서에서는 사용자가 OneLogin 관리 포털에 대해 잘 알고 있으며 슈퍼 사용자 권한이 있는 계정을 가지고 있다고 가정합니다. 사용자 역할 매핑을 구성하려면 맞춤형 사용자 필드를 지원하는 OneLogin Unlimited 요금제를 구독해야 합니다. 자세한 내용은 온라인에서 사용 가능한 OneLogin 설명서를 참조하십시오.

OneLogin에 대한 FMC 서비스 제공자 애플리케이션 구성

OneLogin 관리 포털에서 이 지침을 사용하여 OneLogin 내에 FMC 서비스 공급자 애플리케이션을 생성하고 해당 애플리케이션에 사용자 또는 그룹을 할당합니다. SAML SSO 개념 및 OneLogin 관리 포

털에 대해 숙지해야 합니다. 이 문서에서는 모든 기능을 갖춘 SSO 조직을 설정하는 데 필요한 모든 OneLogin 기능에 대해 설명하지는 않습니다. 예를 들어 사용자 및 그룹을 생성하거나 다른 사용자 관리 애플리케이션에서 사용자 및 그룹 정의를 가져오려면 OneLogin 문서를 참조하십시오.

Note FMC 애플리케이션에 사용자 그룹을 할당하려는 경우 해당 그룹의 사용자를 개인으로 할당하지 마십시오.

Note FMC는 여러 SSO 특성을 사용하는 역할 매핑을 지원할 수 없습니다. 사용자 역할 매핑 또는 그룹 역할 매핑을 선택하고 사용자 특성을 OneLogin에서 FMC로 전달하도록 단일 속성을 구성해야 합니다.

Before you begin

- OneLogin 하위 도메인과 해당 사용자 및 그룹을 숙지하십시오. OneLogin 하위 도메인 검토, on page 43의 내용을 참조하십시오.
- 필요한 경우 OneLogin 하위 도메인에 사용자 계정을 생성합니다.

  Note FMC에서는 SSO 계정의 사용자 이름과 SAML 로그인 프로세스 중에 IdP가 FMC에 전송하는 NameID 속성이 모두 유효한 이메일 주소여야 합니다. 대부분의 IdP는 자동으로 NameID 속성으로 로그온하려는 사용자의 사용자 이름을 사용하지만, 이 기능이 현재 사용 중인 IdP에도 적용되는지 확인해야 합니다. IdP에서 서비스 제공자 애플리케이션을 설정하고 FMC에 SSO 액세스 권한을 부여할 IdP 사용자 계정을 생성할 때 이 점에 유의하십시오.

- 대상 FMC(`https://ipaddress_or_hostname`)의 로그인 URL을 확인합니다.

  Note 여러 URL로 FMC 웹 인터페이스에 연결할 수 있는 경우 (예: 정규화된 도메인 이름 및 IP 주소) SSO 사용자는 이 작업에서 구성한 로그인 URL을 사용하여 FMC에 일관되게 액세스해야 합니다.

Procedure

단계 **1** **SAML Test Connector (Advanced)**를 기본으로 사용하여 FMC서비스 제공자 애플리케이션을 생성합니다.

단계 **2** 다음 설정으로 애플리케이션을 구성합니다.

- **Audience (Entity ID)(**대상**(**엔티티 **ID))**의 경우, `/saml/metadata` 문자열을 FMC 로그인 URL에 추가합니다. 예: `https://ExampleFMC/saml/metadata`

- **Recipient(**수신자**)**에 대해 FMC 로그인 URL에 `/aml/acs` 문자열을 추가합니다. 예: `https://ExampleFMC/saml/acs`
- **ACS(**소비자**) URL** 검사기의 경우 OneLogin에서 올바른 FMC URL을 사용하고 있는지 확인하는 데 사용하는 식을 입력합니다. ACS URL을 사용하고 다음과 같이 변경하여 간단한 유효성 검사기를 만들 수 있습니다.
  - ACS URL의 시작 부분에 `^`를 추가합니다.
  - ACS URL의 끝에 `$`를 추가합니다.
  - ACS URL 내에서 모든 `/` 및 `?` 앞에 `\`를 삽입합니다.

예를 들어, ACS URL `https://ExampleFMC/saml/acs`의 경우 적절한 URL 유효성 검사기는 `^https:\/\/ExampleFMC\/saml\/acs$`가 됩니다.

- **ACS(**소비자**) URL**의 경우 FMC 로그인 URL에 `/saml/acs` 문자열을 추가합니다. 예: `https://ExampleFMC/saml/acs`
- **Login URL(**로그인 **URL)**의 경우 FMC 로그인 URL에 `/saml/acs` 문자열을 추가합니다. 예: `https://ExampleFMC/saml/acs`
- **SAML Initiator(SAML** 개시자**)**에 대해 `Service Provider(통신 사업자)`를 선택합니다.

단계 **3** OneLogin 사용자를 FMC 사업자 애플리케이션에 할당합니다.

단계 **4** (선택 사항) FMC에서 SSO를 보다 쉽게 설정할 수 있도록 FMC 서비스 공급자 애플리케이션용 SAML XML 메타 데이터를 OneLogin에서 로컬 컴퓨터로 다운로드할 수 있습니다.

What to do next

SSO(Single Sign-On)을 활성화합니다. FMC에서 SSO(Single Sign-On) 활성화, on page 28의 내용을 참조하십시오.

OneLogin SSO용 FMC 구성

FMC 웹 인터페이스에서 다음 지침을 참조하십시오.

Before you begin

- OneLogin 관리 포털에서 FMC 서비스 제공자 애플리케이션을 생성합니다. OneLogin에 대한 FMC 서비스 제공자 애플리케이션 구성, on page 43의 내용을 참조하십시오.
- SSO(Single Sign-On)를 활성화합니다. FMC에서 SSO(Single Sign-On) 활성화, on page 28의 내용을 참조하십시오.

Procedure

단계 **1** 이 단계는 FMC에서 SSO(Single Sign-On) 활성화, on page 28에서 곧바로 이어집니다. **Configure OneLogin Metadata(OneLogin** 메타데이터 설정**)** 대화 상자에서 두 가지 옵션을 선택할 수 있습니다.

- SSO 설정 정보를 수동으로 입력하려면 다음을 수행합니다.
  a. **Manual Configuration(**수동 구성**)** 라디오 버튼을 클릭합니다.
  b. OneLogin 서비스 제공 애플리케이션에서 다음 SSO 설정 값을 입력합니다.
     - **ID** 제공자 **SSO(Single Sign-On) URL**: OneLogin에서 **SAML 2.0** 엔드포인트**(HTTP)**를 입력합니다.
     - **ID** 제공자 발급자: OneLogin의 발급자 **URL**을 입력합니다.
     - **X.509** 인증서: OneLogin에서 **X.509** 인증서를 입력합니다.

- OneLogin에서 생성한 XML 메타데이터 파일을 로컬 컴퓨터에 저장한 경우(OneLogin에 대한 FMC 서비스 제공자 애플리케이션 구성, on page 43의 4단계), 파일을 FMC에 업로드할 수 있습니다.
  a. **Upload XML File(XML** 파일 업로드**)** 라디오 버튼을 클릭합니다.
  b. 화면의 지침에 따라 로컬 컴퓨터에서 XML 메타데이터 파일을 찾아 선택합니다.

단계 **2** **Next(**다음**)**를 클릭합니다.

단계 **3** **Verify Metadata(**메타데이터 확인**)** 대화 상자에서 설정 매개변수를 검토하고 **Save(**저장**)**를 클릭합니다.

단계 **4** **Test Configuration(**설정 테스트**)**을 클릭합니다. 시스템에 오류 메시지가 표시되면 FMC의 SSO 설정과 OneLogin 서비스 제공자 애플리케이션 설정을 검토하고 오류를 수정한 후 다시 시도하십시오.

단계 **5** 시스템에서 설정 테스트에 성공했다고 보고하면 **Apply(**적용**)**를 클릭합니다.

What to do next

선택적으로 SSO 사용자에 대한 사용자 역할 매핑을 구성할 수 있습니다. FMC에서 OneLogin 사용자 역할 매핑 구성, on page 46의 내용을 참조하십시오. 역할 매핑을 설정하지 않기로 선택하는 경우, 기본적으로 FMC에 로그인하는 모든 SSO 사용자에게 FMC에서 OneLogin 사용자 역할 매핑 구성, on page 46의 4단계에서 설정한 사용자 역할이 할당됩니다.

FMC에서 OneLogin 사용자 역할 매핑 구성

FMC 웹 인터페이스에서 사용자 역할 매핑을 구성할 수 있는 필드는 선택한 SSO 제공자와 상관없이 동일합니다. 그러나 구성하는 값의 경우, 사용하는 SAML SSO 제공자가 사용자 역할 매핑을 구현하는 방식을 고려해야 합니다.

Before you begin

- OneLogin 사용자 및 그룹을 검토합니다. OneLogin 하위 도메인 검토, on page 43의 내용을 참조하십시오.
- FMC에 대한 SSO 서비스 제공자 애플리케이션을 구성합니다. OneLogin에 대한 FMC 서비스 제공자 애플리케이션 구성, on page 43를 참조하십시오.
- FMC에서 단일 인증(SSO)을 활성화 및 구성합니다. FMC에서 SSO(Single Sign-On) 활성화, on page 28 그리고 OneLogin에 대한 FMC 서비스 제공자 애플리케이션 구성, on page 43을 참조하십시오.

Procedure

단계 **1** 시스템 > 사용자 > **SSO(Single Sign-On)System(**시스템**)** > **Users(**사용자**)**를 선택합니다.

단계 **2** **Advanced Configuration (Role Mapping)(**고급 설정**(**역할 매핑**))**을 펼칩니다.

단계 **3** **Default User Role(**기본 사용자 역할**)** 드롭다운에서 FMC 사용자 역할을 선택해서 사용자를 기본값으로 할당합니다.

단계 **4** **Group Member Attribute(**그룹 멤버 속성**)**을 입력합니다. 이 문자열은 OneLogin의 FMC 서비스 공급자 애플리케이션에서 역할 매핑에 대해 정의하는 사용자 지정 매개 변수의 필드 이름과 일치해야 합니다. (OneLogin IdP에서 개별 사용자에 대한 사용자 역할 매핑 구성, on page 48의 1단계 또는 OneLogin IdP에서 그룹에 대한 사용자 역할 매핑 구성, on page 49의 1단계 참조)

단계 **5** SSO 사용자에게 할당할 각 FMC 사용자 역할 옆에 정규식을 입력합니다. FMC에서는 이러한 값을 SSO 사용자 정보를 사용하여 IdP가 FMC에 전송하는 사용자 역할 매핑 속성과 비교합니다. FMC는 사용자에게 일치하는 항목이 발견된 모든 역할의 통합을 허용합니다.

What to do next

서비스 제공자 애플리케이션에서 사용자 역할 매핑을 구성합니다. OneLogin IdP에서 사용자 역할 매핑 구성, on page 47의 내용을 참조하십시오.

OneLogin IdP에서 사용자 역할 매핑 구성

개별 권한 또는 그룹 권한을 기반으로 Onelogin 관리 포털에서 SSO 사용자 역할 매핑을 설정할 수 있습니다.

- 개별 사용자 권한에 따라 매핑하려면 OneLogin IdP에서 개별 사용자에 대한 사용자 역할 매핑 구성, on page 48의 내용을 참조하십시오.
- 그룹 권한에 따라 매핑하려면 OneLogin IdP에서 그룹에 대한 사용자 역할 매핑 구성, on page 49의 내용을 참조하십시오.

SSO 사용자가 FMC에 로그인하면 OneLogin은 OneLogin IdP에서 설정된 사용자 정의 사용자 필드에서 사용자 또는 그룹 역할 속성값을 FMC에 제공합니다. FMC에서는 해당 속성값을 SSO 설정의 각 FMC 사용자 역할에 할당된 정규식과 비교하고, 일치하는 항목이 있는 모든 역할을 사용자에게 부여

합니다. (일치 항목이 없으면 FMC는 사용자에게 설정 가능한 기본 사용자 역할을 부여합니다.) 각 FMC 사용자 역할에 할당하는 식은 Golang 및 Perl에서 지원하는 제한된 버전의 Google RE2 정규식 표준을 준수해야 합니다. FMC는 FMC 사용자 역할 식과의 비교를 위해 동일한 표준을 사용하여 OneLogin에서 받은 속성값을 정규식으로 처리합니다.

Note 단일 FMC는 그룹 및 개별 사용자 모두에 대해 역할 매핑을 지원할 수 없습니다. FMC 서비스 제공자 애플리케이션에 대해 하나의 매핑 방법을 선택하여 일관되게 사용해야 합니다. FMC는 OneLogin에 설정된 하나의 맞춤형 사용자 필드만 이용한 역할 매핑을 지원할 수 있습니다. 여러 사용자가 있는 경우, 일반적으로 그룹 기반 역할 매핑은 FMC에 더 효율적입니다. OneLogin 하위 도메인 전체에 설정된 사용자 및 그룹 정의를 고려해야 합니다.

OneLogin IdP에서 개별 사용자에 대한 사용자 역할 매핑 구성

OneLogin 관리 포털을 사용하여 FMC 서비스 제공자 애플리케이션 및 맞춤형 사용자 필드에 대한 맞춤형 파라미터를 생성합니다. 이는 SSO 로그인 프로세스 중에 OneLogin이 사용자 역할 정보를 FMC에 전달할 수 있는 수단을 제공합니다.

Before you begin

- OneLogin 하위 도메인과 해당 사용자 및 그룹을 검토합니다. OneLogin 하위 도메인 검토, on page 43을 참조하십시오.
- OneLogin에서 FMC 서비스 제공자 애플리케이션을 생성하고 구성합니다. OneLogin에 대한 FMC 서비스 제공자 애플리케이션 구성, on page 43의 내용을 참조하십시오.
- FMC에서 OneLogin 사용자 역할 매핑 구성, on page 46에 설명된 대로 SSO 사용자 역할 매핑을 구성합니다.

Procedure

단계 **1** FMC 서비스 제공자 애플리케이션에 대한 맞춤형 매개 변수를 생성합니다.

- **Field Name(**필드 이름**)**의 경우 FMC SSO 설정에서 **Group Member Attribute(**그룹 멤버 속성**)**에 입력한 것과 같은 이름을 사용합니다. FMC에서 OneLogin 사용자 역할 매핑 구성, on page 46의 4단계를 참조합니다.
- **Value(**값**)**에 `FMCUserRole`과 같은 연상 이름을 제공합니다. 이는 이 절차의 2단계에서 구성할 고객 사용자 필드의 이름과 일치해야 합니다.

단계 **2** FMC 액세스 권한이 있는 각 OneLogin 사용자에 대한 사용자 역할 정보를 포함할 맞춤형 사용자 필드를 만듭니다.

- **Name(**이름**)** 필드의 경우 `FMCUserRole`과 같은 연상 이름을 제공합니다. 이는 이 절차의 1단계에 설명된 애플리케이션 맞춤형 매개 변수에 대해 제공된 값과 일치해야 합니다.

- **Short name(**축약 이름**)**의 경우 필드의 축약된 대체 이름을 제공합니다. (이는 OneLogin 프로그래밍 인터페이스에 사용됩니다.)

단계 **3** FMC 서비스 제공자 애플리케이션에 대한 액세스 권한이 있는 각 사용자에 대해 이 절차의 2단계에서 생성한 맞춤형 사용자 필드에 값을 할당합니다.

사용자가 SSO를 사용하여 FMC에 로그인할 때 해당 사용자에 대해 이 필드에 할당하는 값은 FMC이(가) SSO 구성에서 FMC 사용자 역할에 할당한 식과 비교하는 값입니다. (FMC에서 OneLogin 사용자 역할 매핑 구성, on page 46의 5단계 참조)

What to do next

- 다양한 계정에서 SSO를 사용하여 FMC에 로그인하고 사용자에게 예상대로 FMC 사용자 역할이 할당되었는지 확인하여 역할 매핑 체계를 테스트합니다.

OneLogin IdP에서 그룹에 대한 사용자 역할 매핑 구성

OneLogin 관리 포털을 사용하여 FMC 서비스 제공자 애플리케이션 및 맞춤형 사용자 필드에 대한 맞춤형 파라미터를 생성합니다. OneLogin 사용자를 그룹에 할당합니다. 그런 다음 맞춤형 사용자 필드와 사용자 그룹 간에 하나 이상의 매핑을 생성하여 OneLogin이 사용자의 그룹 멤버십을 기반으로 맞춤형 사용자 필드에 값을 할당하도록 합니다. 이는 SSO 로그인 프로세스 중에 OneLogin이 그룹 기반 사용자 역할 정보를 FMC에 전달할 수 있는 수단을 제공합니다.

OneLogin 서비스 제공자 애플리케이션은 다음 두 가지 유형의 그룹 중 하나를 사용할 수 있습니다.

- OneLogin 기본 그룹.
- Active Directory, Google Apps 또는 LDAP와 같은 서드 파티 애플리케이션에 동기화된 그룹입니다.

FMC 그룹 역할 매핑을 위해 그룹 유형 중 하나를 사용할 수 있습니다. 이 문서에서는 OneLogin 그룹을 사용한 역할 매핑에 대해 설명합니다. 서드파티 애플리케이션 그룹을 사용하려면 사용자의 조직에서 사용하고 있는 서드파티 사용자 관리 애플리케이션을 숙지해야 합니다. 자세한 내용은 OneLogin 문서를 참고하십시오.

Before you begin

- OneLogin 하위 도메인과 해당 사용자 및 그룹을 검토합니다. OneLogin 하위 도메인 검토, on page 43을 참조하십시오.
- OneLogin에서 FMC 서비스 제공자 애플리케이션을 생성하고 구성합니다. OneLogin에 대한 FMC 서비스 제공자 애플리케이션 구성, on page 43의 내용을 참조하십시오.
- FMC에서 OneLogin 사용자 역할 매핑 구성, on page 46에 설명된 대로 SSO 사용자 역할 매핑을 구성합니다.

Procedure

단계 **1** FMC 서비스 제공자 애플리케이션에 대한 맞춤형 매개 변수를 생성합니다.

- **Field Name(**필드 이름**)**의 경우 FMC SSO 설정에서 **Group Member Attribute(**그룹 멤버 속성**)**에 입력한 것과 같은 이름을 사용합니다. FMC에서 OneLogin 사용자 역할 매핑 구성, on page 46의 4단계를 참조합니다.
- **Value(**값**)**에 `FMCUserRole`과 같은 연상 이름을 제공합니다. 이는이 절차의 2단계에서 구성할 고객 사용자 필드의 이름과 일치해야 합니다.

단계 **2** FMC 액세스 권한이 있는 각 OneLogin 사용자에 대한 사용자 역할 정보를 포함할 맞춤형 사용자 필드를 만듭니다.

- **Name(**이름**)** 필드의 경우 `FMCUserRole`과 같은 연상 이름을 제공합니다. 이는 이 절차의 1단계에 설명된 애플리케이션 맞춤형 매개 변수에 대해 제공된 값과 일치해야 합니다.
- **Short name(**축약 이름**)**의 경우 필드의 축약된 대체 이름을 제공합니다. (이는 OneLogin 프로그래밍 인터페이스에 사용됩니다.)

단계 **3** 이 절차의 2단계에서 생성한 맞춤형 사용자 필드에 그룹 기반 값을 할당하려면 하나 이상의 사용자 필드 매핑을 만듭니다. 각 OneLogin 사용자 그룹에 올바른 FMC 사용자 역할을 할당하는 데 필요한 수의 매핑을 생성합니다.

- 사용자 그룹 필드와 그룹 이름을 비교하여 매핑에 대해 하나 이상의 조건을 생성합니다.
- 여러 조건을 생성하는 경우 사용자 그룹이 매핑을 수행할 조건 중 하나 또는 모두와 일치해야 하는지 여부를 선택합니다.
- 매핑에 대한 **Action(**동작**)**을 생성해서 이 절차의 2단계에서 생성한 맞춤형 사용자 필드에 값을 할당합니다. **Name(**이름**)** 필드 그리고 사용자가 지정한 조건을 충족하는 모든 사용자에 대해 OneLogin이 맞춤형 사용자 필드에 할당하는 문자열을 제공합니다.

  FMC에서는 이 문자열을 FMC에서 OneLogin 사용자 역할 매핑 구성, on page 46의 5단계에서 각 FMC 사용자 역할에 할당한 식과 비교합니다.
- 변경을 완료하면 모든 매핑을 다시 적용합니다.

What to do next

- 다양한 계정에서 SSO를 사용하여 FMC에 로그인하고 사용자에게 예상대로 FMC 사용자 역할이 할당되었는지 확인하여 역할 매핑 체계를 테스트합니다.

OneLogin 사용자 역할 매핑 예

다음 예에서와 같이 사용자 역할 매핑을 지원하기 위한 FMC의 SSO 설정은 개별 사용자 및 그룹에 대해 동일합니다. 차이점은 OneLogin의 FMC 서비스 제공자 애플리케이션 설정에 있습니다.

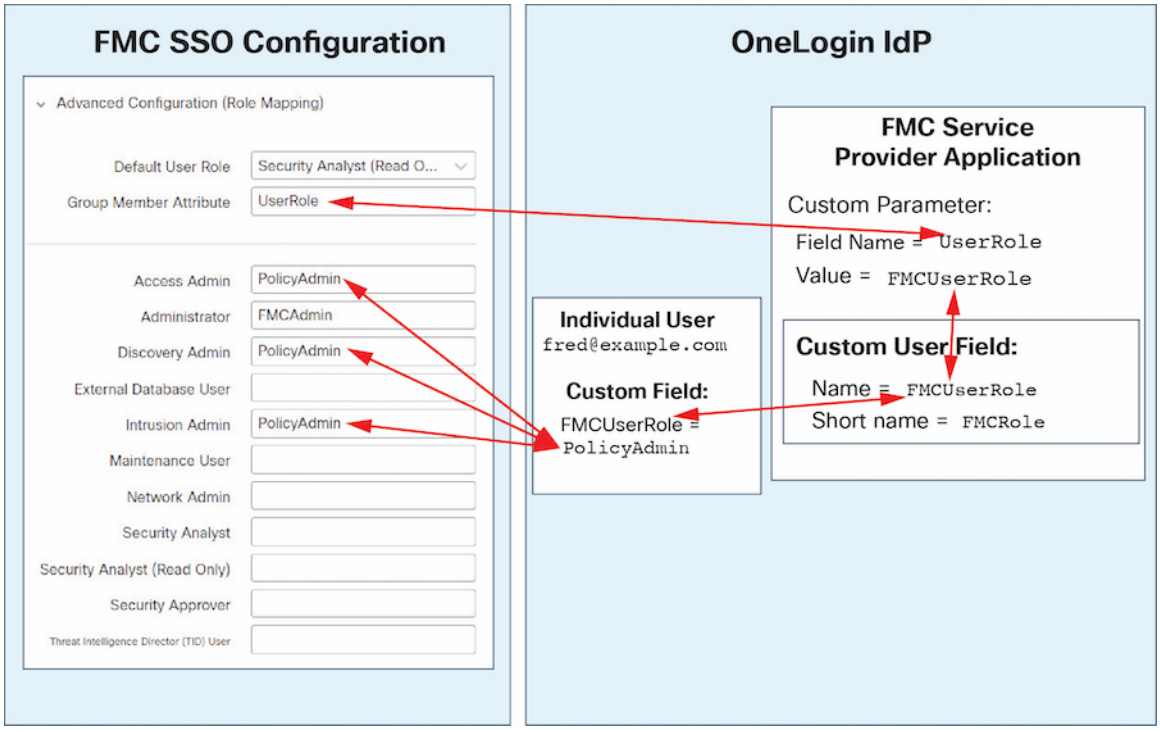
Note 단일 FMC는 그룹 및 개별 사용자 모두에 대해 역할 매핑을 지원할 수 없습니다. FMC 서비스 제공자 애플리케이션에 대해 하나의 매핑 방법을 선택하여 일관되게 사용해야 합니다. FMC는 OneLogin에 설정된 하나의 맞춤형 사용자 필드만 이용한 역할 매핑을 지원할 수 있습니다. 여러 사용자가 있는 경우, 일반적으로 그룹 기반 역할 매핑은 FMC에 더 효율적입니다. OneLogin 하위 도메인 전체에 설정된 사용자 및 그룹 정의를 고려해야 합니다.

개별 사용자 계정에 대한 OneLogin 역할 매핑 예

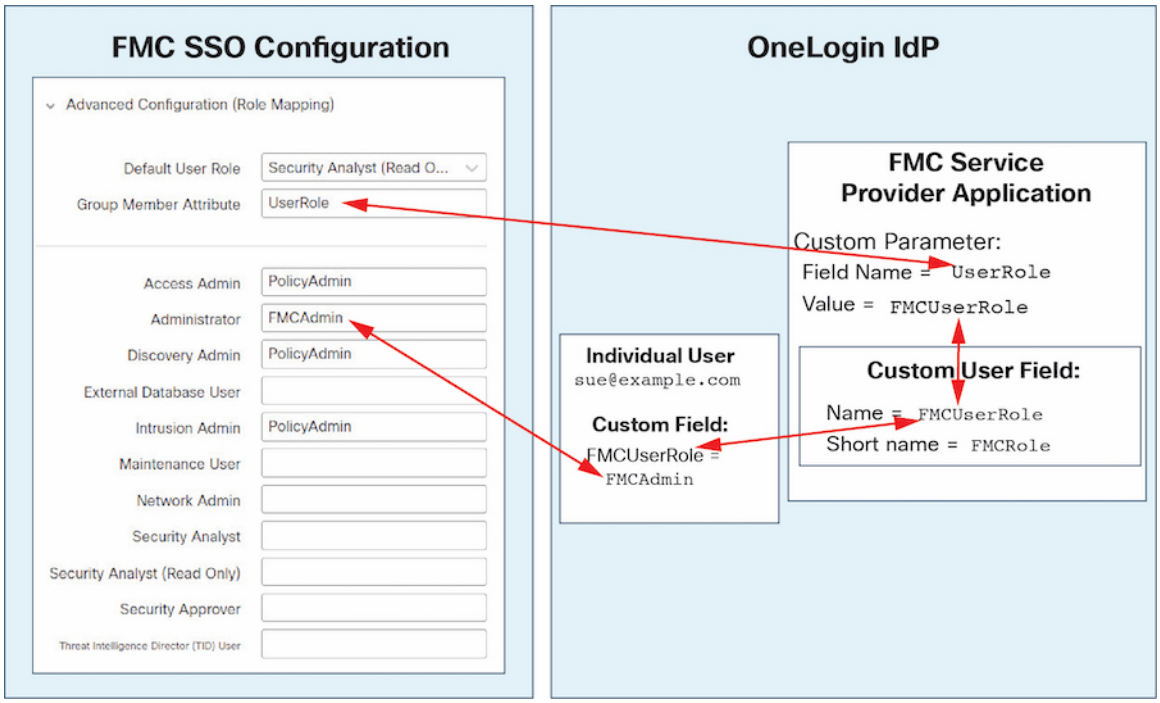
개별 사용자에 대한 역할 매핑에서 OneLogin FMC 서비스 애플리케이션에는 FMC의 그룹 멤버 속성 이름과 일치하는 이름을(이 예에서는 `UserRole`) 갖는 사용자 지정 속성이 있습니다. OneLogin에는 맞춤형 사용자 필드도 정의되어 있습니다(이 예에서는 `FMCUserRole`). 애플리케이션 사용자 지정 속성 `UserRole`에 대한 정의는 OneLogin이 사용자 역할 매핑 정보를 FMC에 전달할 때 해당 사용자의 사용자 지정 필드 `FMCUserRole`의 값을 사용하도록 설정합니다.

다음 다이어그램은 FMC 및 OneLogin 구성의 관련 필드와 값이 개별 계정에 대한 사용자 역할 매핑에서 서로 어떻게 대응하는지를 보여줍니다. 각 다이어그램은 FMC 및 OneLogin 관리 포털에서 동일한 SSO 컨피그레이션을 사용하지만, OneLogin 관리 포털의 각 사용자에 대한 컨피그레이션은 각 사용자에게 FMC에서 서로 다른 역할을 할당하기 위해서 달라집니다.

- 이 다이어그램에서 fred@example.com은 `FMCUserrole` 값 `PolicyAdmin`을 사용하며, FMC는 액세스 관리자, 검색 관리 및 침입 관리자 역할을 할당합니다.



- 이 다이어그램에서 sue@example.com은 `FMCUserRole` 값 `FMCAdmin`을 사용하며, FMC는 관리자 역할을 할당합니다.



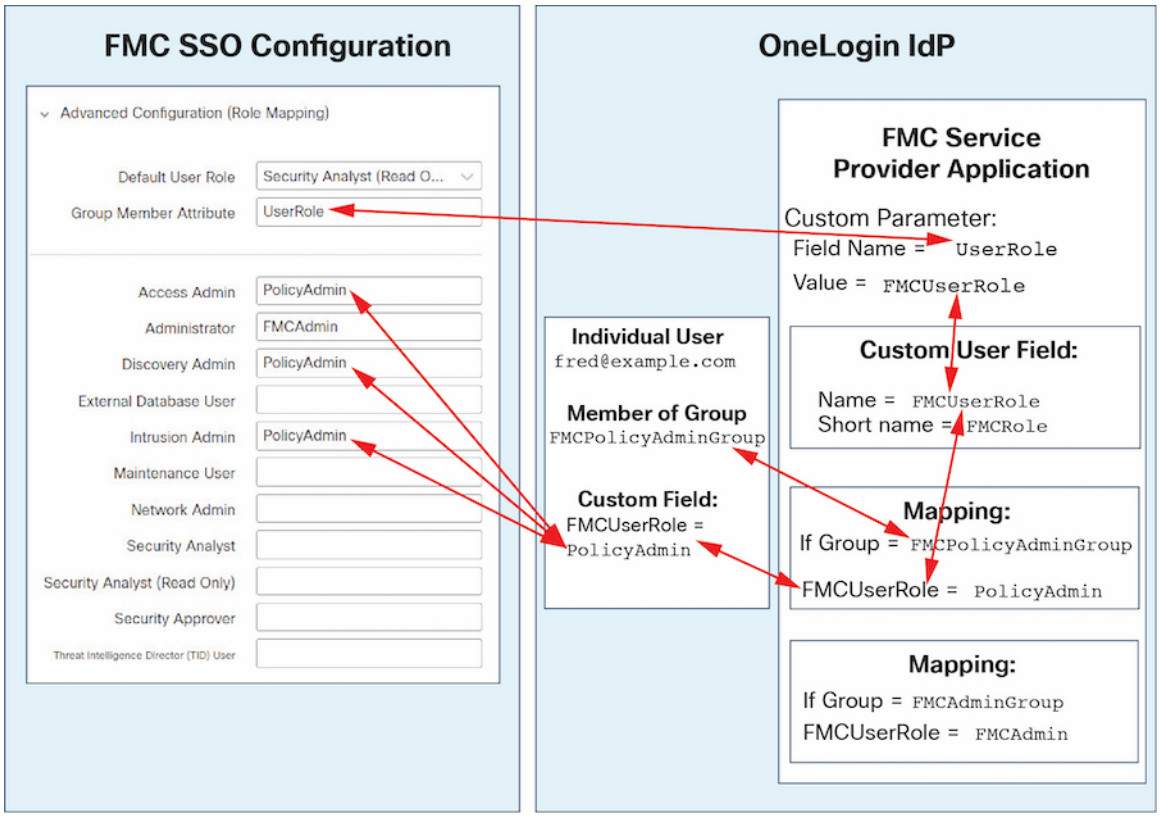
- 이 FMC를 위해 OneLogin 서비스 애플리케이션에 할당된 다른 사용자에게는 다음 중 하나의 이유로 기본 사용자 역할 보안 분석(읽기 전용)이 할당됩니다.
  - `FMCUserRole` 맞춤형 사용자 필드에 할당된 값이 없습니다.
  - `FMCUserRole` 맞춤형 사용자 필드에 할당된 값이 FMC의 SSO 구성에서 사용자 역할에 대해 구성된 식과 일치하지 않습니다.

그룹에 대한 **OneLogin** 역할 매핑 예

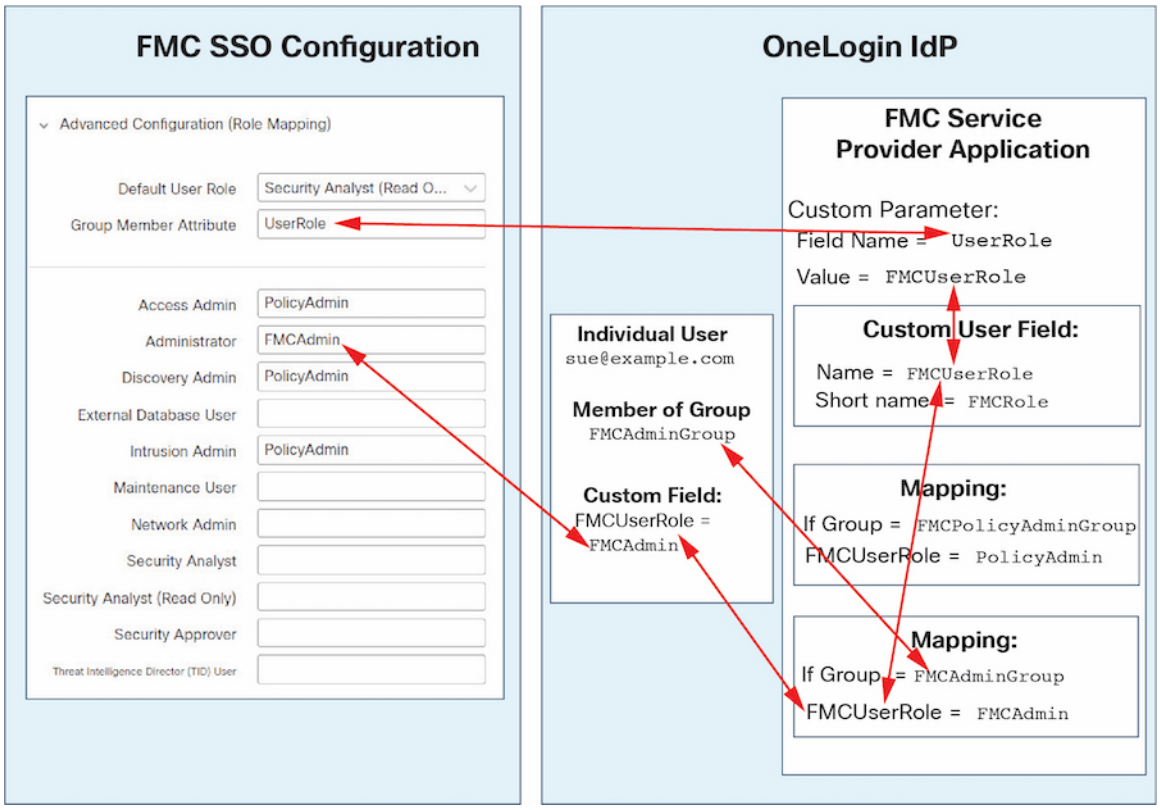
그룹에 대한 역할 매핑에서 OneLogin FMC 서비스 애플리케이션에는 FMC의 그룹 멤버 속성의 이름(이 예에서는 `UserRole`)과 일치하는 이름을 갖는 사용자 지정 매개 변수가 있습니다. OneLogin에는 맞춤형 사용자 필드도 정의되어 있습니다(이 예에서는 `FMCUserRole`). 애플리케이션 사용자 지정 속성 `UserRole`에 대한 정의는 OneLogin이 사용자 역할 매핑 정보를 FMC에 전달할 때 해당 사용자의 사용자 지정 필드 `FMCUserRole`의 값을 사용하도록 설정합니다. 사용자 그룹 매핑을 지원하려면 OneLogin 내에서 매핑을 설정하여 해당 사용자의 OneLogin 그룹 멤버십을 기반으로 각 사용자의 `FMCUserRole` 필드에 값을 할당해야 합니다.

다음 다이어그램은 FMC 및 OneLogin 구성의 관련 필드와 값이 그룹에 대한 사용자 역할 매핑에서 서로 어떻게 일치 하는지를 보여줍니다. 각 다이어그램은 FMC 및 OneLogin 관리 포털에서 동일한 SSO 구성을 사용하지만, OneLogin 관리 포털의 각 사용자에 대한 구성은 각 사용자에게 FMC에서 서로 다른 역할을 할당하기 위해서 달라집니다.

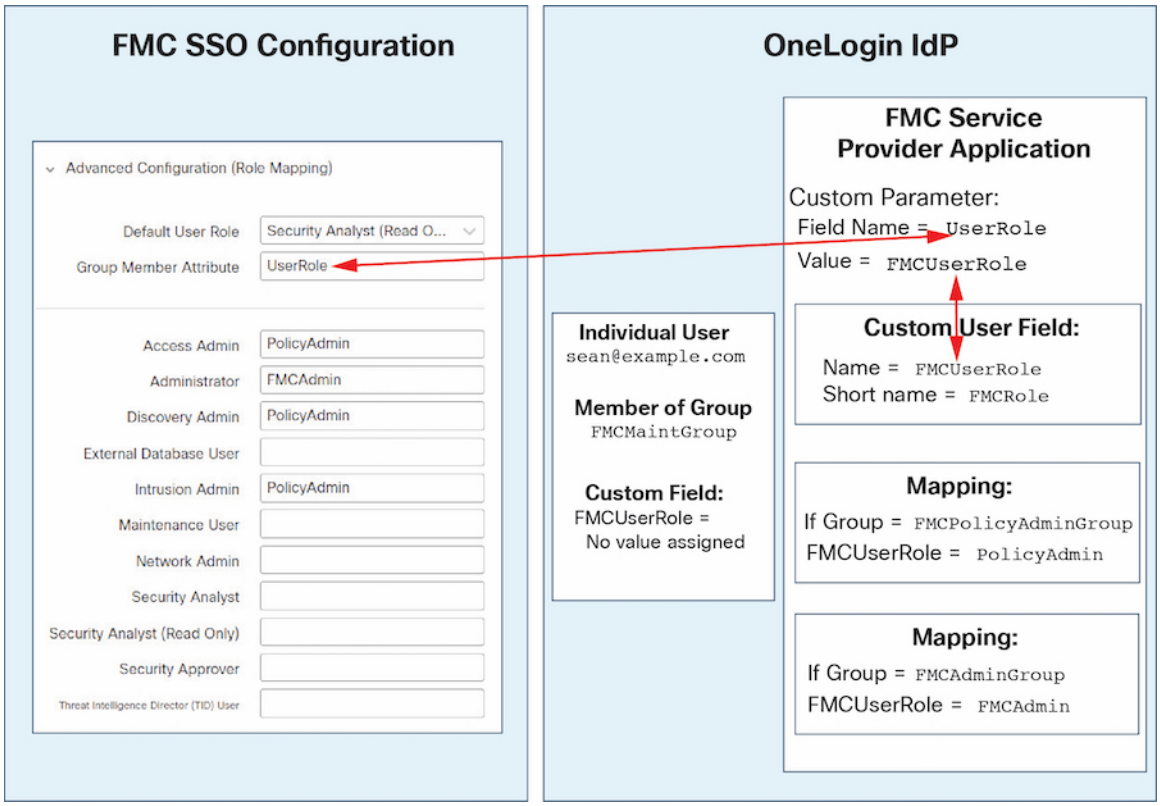
- 이 다이어그램에서 fred@example.com은 OneLogin IdP 그룹 `FMCPolicyAdminGroup`의 멤버입니다. OneLogin 매핑은 `PolicyAdmin` 값을 `FMCPolicyAdminGroup` 멤버에 대한 맞춤형 사용자 필드 `FMCUserRole`에 할당합니다. FMC에서는 프레드 및 `FMCPolicyAdminGroup`의 다른 멤버에게 Access Admin, Discovery Admin 및 Intrusion Admin 역할을 할당합니다.



- 이 다이어그램에서 sue@example.com은 OneLogin IdP 그룹 `FMCAdminGroup`의 멤버입니다. OneLogin 매핑은 FMCAdmin 값을 `FMCPolicyAdminGroup` 멤버에 대한 맞춤형 사용자 필드 `FMCUserRole`에 할당합니다. FMC는 Sue 및 `FMCAdminGroup`의 다른 멤버에게 관리자 역할을 할당합니다.

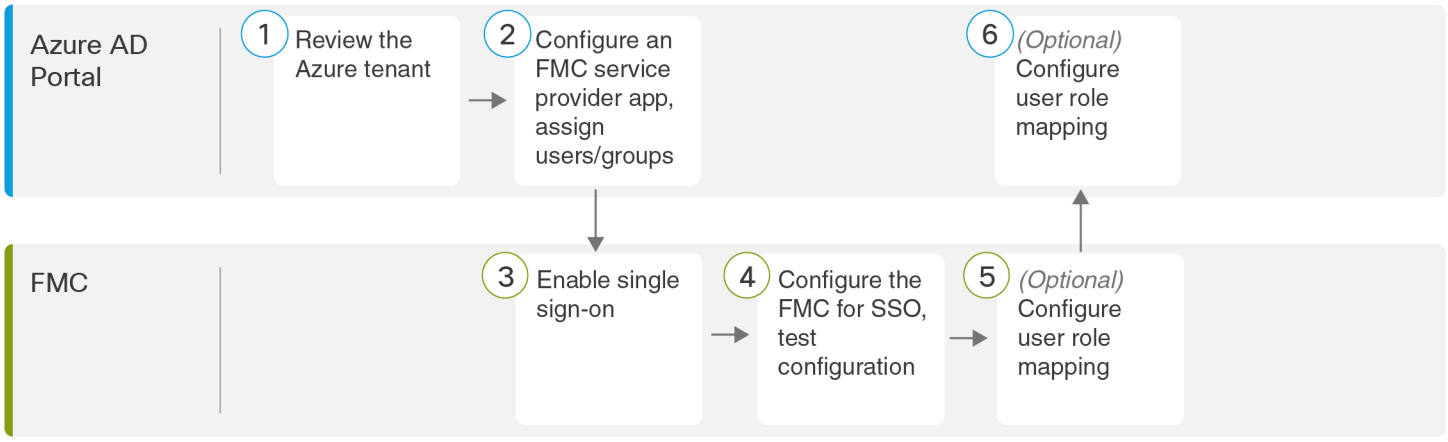


- 이 다이어그램에서 sean@example.com은 Idp 그룹 `FMCMaintGroup`의 멤버입니다. 이 그룹과 연결된 OneLogin 매핑이 없으므로 OneLogin은 사용자 지정 사용자 필드 `FMCUserRole`에 대해 값을 할당하지 않습니다. FMC에서는 유지 보수 사용자 역할이 아닌 기본 사용자 역할(보안 분석가 (읽기 전용))을 할당합니다.



Azure AD로 SSO(Single Sign-On, 단일 인증) 구성

Azure를 사용하여 SSO를 설정하려면 다음 작업을 참조하십시오.



1	Azure AD 포털	Azure 테넌트 검토, on page 56
2	Azure AD 포털	Azure용 FMC 서비스 제공자 애플리케이션 구성, on page 56

3	FMC	FMC에서 SSO(Single Sign-On) 활성화, on page 28
4	FMC	Azure SSO용 FMC 구성, on page 58
5	FMC	FMC에서 Azure에 대한 사용자 역할 매핑 구성, on page 60
6	Azure AD 포털	Azure IdP에서 사용자 역할 매핑 구성, on page 60

Azure 테넌트 검토

Azure AD는 Microsoft의 멀티 테넌트 클라우드 기반 ID 및 액세스 관리 서비스입니다. Azure에서는 사용자가 동일한 SSO 계정으로 액세스할 수 있는 모든 페더레이션된 디바이스를 포함하는 엔터티를 테넌트라고 합니다. Azure 테넌트에 FMC를 추가하기 전에 해당 조직에 대해 잘 알고 있어야 합니다. 다음 질문을 고려해보십시오.

- FMC에 액세스할 수 있는 사용자는 몇 명입니까?
- 사용자가 그룹의 Azure 테넌트 구성원 내에 있습니까?
- 사용자 및 그룹이 다른 디렉토리 제품입니까?
- FMC에서 SSO를 지원하려면 Azure 테넌트에 더 많은 사용자 또는 그룹을 추가해야 합니까?
- 어떤 종류의 FMC 사용자 역할을 지정 하시겠습니까? (사용자 역할을 할당하지 않는 경우 FMC가 모든 SSO 사용자에게 구성 가능한 기본 사용자 역할을 자동으로 할당합니다.)
- 필요한 사용자 역할 매핑을 지원하려면 Azure 테넌트 내의 사용자 및 그룹을 어떻게 구성해야합니까?
- 개별 사용자 또는 그룹을 기준으로 매핑할 FMC 역할을 구성할 수 있지만 단일 FMC 애플리케이션이 그룹 및 개별 사용자 모두에 대해 역할 매핑을 지원할 수는 없습니다.

이 문서에서는 사용자가 이미 Azure Active Directory 포털에 익숙하며 Azure AD 테넌트에 대한 애플리케이션 관리자 권한이 있는 계정을 가지고 있다고 가정합니다. FMC는 테넌트별 단일 로그인 및 단일 로그 아웃 엔드포인트에서만 Azure SSO를 지원합니다. Azure AD Premium P1 이상 라이선스 및 전역 관리자 권한이 있어야 합니다. 자세한 내용은 Azure 설명서를 참조하십시오.

Azure용 FMC 서비스 제공자 애플리케이션 구성

Azure Active Directory 포털을 사용하여 Azure Active Directory 테넌트 내에 FMC 서비스 제공자 애플리케이션을 만들고 기본 구성 설정을 구성합니다.

Note FMC 애플리케이션에 사용자 그룹을 할당하려는 경우 해당 그룹의 사용자를 개인으로 할당하지 마십시오.

Note FMC는 여러 SSO 특성을 사용하는 역할 매핑을 지원할 수 없습니다. 사용자 역할 매핑 또는 그룹 역할 매핑을 선택하고 사용자 특성을 OneLogin에서 FMC로 전달하도록 단일 속성을 구성해야 합니다.

Before you begin

- Azure 테넌트와 해당 사용자 및 그룹을 숙지하십시오. Azure 테넌트 검토, on page 56 참조하십시오.
- 필요한 경우 Azure 테넌트에서 사용자 계정 및/또는 그룹을 생성합니다.

  Note FMC에서는 SSO 계정의 사용자 이름과 SAML 로그인 프로세스 중에 IdP가 FMC에 전송하는 NameID 속성이 모두 유효한 이메일 주소여야 합니다. 대부분의 IdP는 자동으로 NameID 속성으로 로그온하려는 사용자의 사용자 이름을 사용하지만, 이 기능이 현재 사용 중인 IdP에도 적용되는지 확인해야 합니다. IdP에서 서비스 제공자 애플리케이션을 설정하고 FMC에 SSO 액세스 권한을 부여할 IdP 사용자 계정을 생성할 때 이 점에 유의하십시오.

- 대상 FMC(`https://ipaddress_or_hostname`)의 로그인 URL을 확인합니다.

  Note 여러 URL(예: 정규화된 도메인 이름 및 IP 주소)로 FMC 웹 인터페이스에 연결할 수 있는 경우, SSO 사용자는 이 작업에서 구성한 로그인 URL을 사용하여 FMC에 일관되게 액세스해야 합니다.

Procedure

단계 **1** Azure AD SAML 툴킷을 기본으로 사용하여 FMC 서비스 제공자 애플리케이션을 생성합니다.

단계 **2** 기본 **SAML** 구성에 대한 다음 설정을 사용하여 애플리케이션을 구성합니다.

- **Identifier(**엔티티 **ID)**의 경우, `/saml/metadata` 문자열을 FMC 로그인 URL에 추가합니다. 예: `https://ExampleFMC/saml/metadata`
- 회신 **URL(**어설션 소비자 서비스 **URL)**의 경우 `/saml/acs` 문자열을 FMC 로그인 URL에 추가합니다. 예: `https://ExampleFMC/saml/acs`
- **URL** 로그인의 경우 `/sam/acs` 문자열을 FMC 로그인 URL에 추가합니다. 예: `https://ExampleFMC/saml/acs`

단계 **3** FMC에서 로그인을 위한 사용자 이름을 사용자 계정과 연결된 이메일 주소로 지정하도록 애플리케이션의 고유 사용자 식별자 이름**(**이름 **ID)** 클레임을 편집합니다.

- **Source(**소스**)**에 대해 `Attribute(속성)`를 선택합니다.

- 소스 속성의 경우: `user.mail`을 선택합니다.

단계 **4** FMC에서 SSO를 보호하기 위한 인증서를 생성합니다. 인증서에 다음 옵션을 사용합니다.

- Signing option(서명 옵션)을 Sign SAML response and assertion(SAML 응답 및 어설션 서명)으로 변경합니다.
- Signing Algorithm(서명 알고리즘)으로 SHA-256을 선택합니다.

단계 **5** 인증서의 Base-64 버전을 로컬 컴퓨터에 다운로드합니다. FMC 웹 인터페이스에서 Azure SSO를 구성할 때 필요합니다.

단계 **6** 애플리케이션의 SAML 기반 로그인 정보에서 다음 값을 확인합니다.

- 로그인 **URL**
- **Azure AD** 식별자

FMC 웹 인터페이스에서 Azure SSO를 구성할 때 이러한 값이 필요합니다.

단계 **7** (선택 사항) FMC에 SSO를 보다 쉽게 설정할 수 있도록 FMC 서비스 제공자 애플리케이션(Azure 포털의 페더레이션 메타데이터 **XML**이라고 하는)의 SAML XML 메타데이터 파일을 로컬 컴퓨터에 다운로드할 수 있습니다.

단계 **8** 기존 Azure 사용자 및 그룹을 FMC 서비스 애플리케이션에 할당합니다.

Note FMC 애플리케이션에 사용자 그룹을 할당하려는 경우 해당 그룹의 사용자를 개인으로 할당하지 마십시오.

Note 사용자 역할 매핑을 구성하려는 경우 개별 사용자 권한 또는 그룹 권한에 따라 역할을 매핑하도록 구성할 수 있지만 단일 FMC 애플리케이션이 그룹 및 개별 사용자 모두에 대해 역할 매핑을 지원할 수는 없습니다.

What to do next

SSO(Single Sign-On)을 활성화합니다. FMC에서 SSO(Single Sign-On) 활성화, on page 28의 내용을 참조하십시오.

Azure SSO용 FMC 구성

FMC 웹 인터페이스에서 다음 지침을 사용하십시오.

Before you begin

- Azure AD 포털에서 FMC 서비스 제공자 애플리케이션을 생성합니다. Azure용 FMC 서비스 제공자 애플리케이션 구성, on page 56의 내용을 참조하십시오.
- SSO(Single Sign-On)을 활성화합니다. FMC에서 SSO(Single Sign-On) 활성화, on page 28의 내용을 참조하십시오.

Procedure

단계 **1** 이 단계는 FMC에서 SSO(Single Sign-On) 활성화, on page 28에서 곧바로 이어집니다. **Configure Azure Metadata(Azure** 메타 데이터 구성**)** 대화 상자에서 두 가지 옵션을 선택할 수 있습니다.

- SSO 설정 정보를 수동으로 입력하려면 다음을 수행합니다.
  a. **Manual Configuration(**수동 구성**)** 라디오 버튼을 클릭합니다.
  b. Azure SSO 서비스 제공자 애플리케이션에서 검색한 값을 입력합니다.
     - **ID** 제공자 **SSO(Single Sign-On) URL**의 경우 Azure용 FMC 서비스 제공자 애플리케이션 구성, on page 56의 6단계에서 적어둔 로그인 **URL**을 입력합니다.
     - **Identity Provider Issuer(ID** 공급자 발급자**)**에 대해 Azure용 FMC 서비스 제공자 애플리케이션 구성, on page 56의 6단계에서 적어둔 **Azure AD** 식별자를 입력합니다.
     - **X.509** 인증서의 경우 Azure용 FMC 서비스 제공자 애플리케이션 구성, on page 56의 5단계에서 Azure에서 다운로드한 인증서를 사용합니다. (텍스트 편집기를 사용하여 인증서 파일을 열고 내용을 복사하여 **X.509 Certificate(X.509** 인증서**)** 필드에 붙여 넣습니다.)
- Azure에서 생성한 XML 메타데이터 파일을 로컬 컴퓨터에 저장한 경우(Azure용 FMC 서비스 제공자 애플리케이션 구성, on page 56의 7단계) 파일을 FMC에 업로드할 수 있습니다.
  a. **Upload XML File(XML** 파일 업로드**)** 라디오 버튼을 클릭합니다.
  b. 화면의 지침에 따라 로컬 컴퓨터에서 XML 메타데이터 파일을 찾아 선택합니다.

단계 **2** **Next(**다음**)**를 클릭합니다.

단계 **3** **Verify Metadata(**메타데이터 확인**)** 대화 상자에서 컨피그레이션 매개변수를 검토하고 **Save(**저장**)**를 클릭합니다.

단계 **4** **Test Configuration(**컨피그레이션 테스트**)**을 클릭합니다. 시스템에 오류 메시지가 표시되면 FMC의 SSO 구성과 Azure 서비스 제공자 애플리케이션을 검토하고 오류를 수정한 후 다시 시도하십시오.

단계 **5** 시스템에서 컨피그레이션 테스트에 성공했다고 보고하면 **Apply(**적용**)**를 클릭합니다.

What to do next

선택적으로 SSO 사용자에 대한 역할 매핑을 구성할 수 있습니다. FMC에서 Azure에 대한 사용자 역할 매핑 구성, on page 60의 내용을 참조하십시오. 역할 매핑을 구성하지 않도록 선택하는 경우, 기본적으로 FMC에 로그인하는 모든 SSO 사용자에게 FMC에서 Azure에 대한 사용자 역할 매핑 구성, on page 60의 4단계에서 구성한 기본 사용자 역할이 할당됩니다.

FMC에서 Azure에 대한 사용자 역할 매핑 구성

FMC 웹 인터페이스에서 사용자 역할 매핑을 구성할 수 있는 필드는 선택한 SSO 제공자와 상관 없이 동일합니다. 하지만 구성한 값은 반드시 사용하는 SAML SSO 제공자가 사용자 역할 매핑을 구현하는 방법을 고려해야 합니다.

Before you begin

- 기존 Azure 사용자 및 그룹을 검토합니다. Azure 테넌트 검토, on page 56을 참조하십시오.
- FMC에 대한 SSO 서비스 제공자 애플리케이션을 구성합니다. Azure용 FMC 서비스 제공자 애플리케이션 구성, on page 56의 내용을 참조하십시오.
- FMC에서 단일 인증(SSO)을 활성화 및 구성합니다. FMC에서 SSO(Single Sign-On) 활성화, on page 28 그리고 Azure SSO용 FMC 구성, on page 58을 참조하십시오.

Procedure

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

단계 **2** **Single Sign-On**(단일 인증) 탭을 클릭합니다.

단계 **3** 고급 구성(역할 매핑)을 펼칩니다.

단계 **4** **Default User Role**(기본 사용자 역할) 드롭 다운에서 FMC 사용자 역할을 선택해서 사용자를 기본값으로 할당합니다.

단계 **5** **Group Member Attribute**(그룹 멤버 속성)을 입력합니다. 이 문자열은 Azure의 FMC 서비스 제공자 애플리케이션에 대해 생성하는 사용자 클레임의 이름과 일치해야 합니다. Azure IdP에서 개별 사용자의 사용자 역할 매핑 구성, on page 61의 1 단계 또는 Azure IdP에서 그룹용 사용자 역할 매핑 구성, on page 62의 1 단계를 참조하십시오.

단계 **6** SSO 사용자에게 할당할 각 FMC 사용자 역할 옆에 정규식을 입력합니다. (FMC는 Golang 및 Perl에서 지원하는 Google의 RE2 정규식 표준의 제한된 버전을 사용합니다.) FMC에서는 이러한 값을 SSO 사용자 정보를 사용하여 IdP가 FMC에 전송하는 사용자 역할 매핑 속성값과 비교합니다. FMC는 사용자에게 일치하는 항목이 발견된 모든 역할의 통합을 허용합니다.

What to do next

서비스 제공자 애플리케이션에서 사용자 역할 매핑을 구성합니다. Azure IdP에서 사용자 역할 매핑 구성, on page 60을 참조하십시오.

Azure IdP에서 사용자 역할 매핑 구성

개별 사용자 권한 또는 그룹 권한을 기반으로 Azure AD 포털에서 SSO 사용자 역할 매핑을 설정할 수 있습니다.

- 개별 사용자 권한을 기반으로 매핑하려면 Azure IdP에서 개별 사용자의 사용자 역할 매핑 구성을 참조하십시오.

- 그룹 권한을 기준으로 매핑하려면 Azure IdP에서 그룹용 사용자 역할 매핑 구성을 참조하십시오.

SSO 사용자가 FMC에 로그인하면 Azure는 Azure AD 포털에 설정된 애플리케이션 역할에서 값을 얻는 사용자 또는 그룹 역할 속성값을 FMC에 제공합니다. FMC에서는 해당 속성값을 SSO 설정의 각 FMC 사용자 역할에 할당된 정규식과 비교하고, 일치하는 항목이 있는 모든 역할을 사용자에게 부여합니다. (일치 항목이 없으면 FMC는 사용자에게 설정 가능한 기본 사용자 역할을 부여합니다.) 각 FMC 사용자 역할에 할당하는 식은 Golang 및 Perl에서 지원하는 제한된 버전의 Google RE2 정규식 표준을 준수해야 합니다. FMC는 FMC 사용자 역할 식과의 비교를 위해 동일한 표준을 사용하여 Azure에서 받은 속성값을 정규식으로 처리합니다.

Note 단일 FMC는 그룹 및 개별 사용자 모두에 대해 역할 매핑을 지원할 수 없습니다. FMC 서비스 제공자 애플리케이션에 대해 하나의 매핑 방법을 선택하여 일관되게 사용해야 합니다. FMC는 Azure에 설정된 하나의 클레임만 사용하여 역할 매핑을 지원할 수 있습니다. 여러 사용자가 있는 경우, 일반적으로 그룹 기반 역할 매핑은 FMC에 더 효율적입니다. Azure 테넌트 전체에 설정된 사용자 및 그룹 정의를 고려해야 합니다.

Azure IdP에서 개별 사용자의 사용자 역할 매핑 구성

Azure에서 FMC 서비스 애플리케이션의 개별 사용자에 대한 역할 매핑을 설정하려면 Azure AD Portal을 사용하여 애플리케이션에 클레임을 추가하고, 애플리케이션의 등록 매니페스트에 역할을 추가한 다음 사용자에게 역할을 할당합니다.

Before you begin

- Azure 테넌트를 검토합니다. Azure 테넌트 검토, on page 56의 내용을 참조하십시오.
- Azure에서 FMC 서비스 제공자 애플리케이션 생성하고 구성합니다. Azure용 FMC 서비스 제공자 애플리케이션 구성, on page 56의 내용을 참조하십시오.
- FMC에서 Azure에 대한 사용자 역할 매핑 구성, on page 60에 설명된 대로 SSO 사용자 역할 매핑을 설정합니다.

Procedure

단계 **1** 다음 특성을 사용하여 FMC 서비스 애플리케이션의 SSO 설정에 사용자 클레임을 추가합니다.

- **Name(**이름**)**: FMC SSO 설정에서 **Group Member Attribute(**그룹 멤버 속성**)**에 입력한 것과 같은 문자열을 사용합니다. (FMC에서 Azure에 대한 사용자 역할 매핑 구성, on page 60의 5단계 참조)
- **Source(**소스**)**: `Attribute(속성)`를 선택합니다.
- **Source attribute(**소스 속성**)**: `user.assignedroles`를 선택합니다.

단계 **2** FMC 서비스 애플리케이션의 매니페스트(JSON 형식)를 편집하고 애플리케이션 역할을 추가하여 SSO 사용자에게 할당할 FMC 사용자 역할을 나타냅니다. 가장 간단한 방법은 기존 애플리케이션 역할 정의를 복사하고 다음 속성을 변경하는 것입니다.

- `displayName`: AD Azure Portal에 표시될 역할의 이름입니다.
- `description`: 역할에 대한 짧은 설명입니다.
- `Id`: 매니페스트 내의 ID 속성 중에서 고유해야 하는 영문숫자 문자열입니다.
- `value`: 하나 이상의 FMC 사용자 역할을 나타내는 문자열입니다. (참고: Azure에서는 이 문자열에 공백을 허용하지 않습니다.)

단계 **3** FMC 서비스 애플리케이션에 할당된 각 사용자에 대해 해당 애플리케이션의 매니페스트에 추가한 애플리케이션 역할 중 하나를 할당합니다. 사용자가 SSO를 사용하여 FMC에 로그인할 때 해당 사용자에게 할당하는 애플리케이션 역할은 서비스 애플리케이션에 대한 클레임에서 Azure가 FMC에 전송하는 값입니다. FMC에서는 클레임을 SSO 설정에서 FMC 사용자 역할에 할당한 식과 비교하고 (FMC에서 Azure에 대한 사용자 역할 매핑 구성, on page 60의 6단계 참조), 일치하는 모든 FMC 사용자 역할을 사용자에게 할당합니다.

What to do next

- 다양한 계정에서 SSO를 사용하여 FMC에 로그인하고 사용자에게 예상대로 FMC 사용자 역할이 할당되었는지 확인하여 역할 매핑 체계를 테스트합니다.

Azure IdP에서 그룹용 사용자 역할 매핑 구성

Azure에서 FMC 서비스 애플리케이션의 사용자 그룹에 대한 역할 매핑을 설정하려면 Azure AD Portal을 사용하여 애플리케이션에 클레임을 추가하고, 애플리케이션의 등록 매니페스트에 역할을 추가한 다음 그룹에 역할을 할당합니다.

Before you begin

- Azure 테넌트를 검토합니다. Azure 테넌트 검토, on page 56의 내용을 참조하십시오.
- Azure에서 FMC 서비스 제공자 애플리케이션 생성하고 구성합니다. Azure용 FMC 서비스 제공자 애플리케이션 구성, on page 56의 내용을 참조하십시오.
- FMC에서 Azure에 대한 사용자 역할 매핑 구성, on page 60에 설명된 대로 SSO 사용자 역할 매핑을 구성합니다.

Procedure

단계 **1** 다음 특성을 사용하여 FMC 서비스 애플리케이션의 SSO 설정에 사용자 클레임을 추가합니다.

- **Name(**이름**)**: FMC SSO 구성에서 **Group Member Attribute(**그룹 멤버 속성**)**에 입력한 것과 같은 문자열을 사용합니다. (FMC에서 Azure에 대한 사용자 역할 매핑 구성, on page 60의 5단계 참조)
- **Source(**소스**)**: `Attribute(속성)`를 선택합니다.
- **Source attribute(**소스 속성**)**: `user.assignedroles`를 선택합니다.

단계 **2** FMC 서비스 애플리케이션의 매니페스트(JSON 형식)를 편집하고 애플리케이션 역할을 추가하여 SSO 사용자에게 할당할 FMC 사용자 역할을 나타냅니다. 가장 간단한 방법은 기존 애플리케이션 역할 정의를 복사하고 다음 속성을 변경하는 것입니다.

- `displayName`: AD Azure Portal에 표시될 역할의 이름입니다.
- `description`: 역할에 대한 짧은 설명입니다.
- `Id`: 매니페스트 내의 ID 속성 중에서 고유해야 하는 영문숫자 문자열입니다.
- `value`: 하나 이상의 FMC 사용자 역할을 나타내는 문자열입니다. (Azure에서는이 문자열에 공백을 허용하지 않습니다.)

단계 **3** FMC 서비스 애플리케이션에 할당된 각 그룹에 대해 해당 애플리케이션의 매니페스트에 추가한 애플리케이션 역할 중 하나를 할당합니다. 사용자가 SSO를 사용하여 FMC에 로그인할 때 해당 사용자 그룹에 할당하는 애플리케이션 역할은 서비스 애플리케이션에 대한 클레임에서 Azure가 FMC에 전송하는 값입니다. FMC에서는 클레임을 SSO 설정에서 FMC 사용자 역할에 할당한 식과 비교하고 (FMC에서 Azure에 대한 사용자 역할 매핑 구성, on page 60의 6단계 참조), 일치하는 모든 FMC 사용자 역할을 사용자에게 할당합니다.

What to do next

다양한 계정에서 SSO를 사용하여 FMC에 로그인하고 사용자에게 예상대로 FMC 사용자 역할이 할당되었는지 확인하여 역할 매핑 체계를 테스트합니다.

Azure 사용자 역할 매핑 예

다음 예에서와 같이 사용자 역할 매핑을 지원하기 위한 FMC의 SSO 설정은 개별 사용자 및 그룹에 대해 동일합니다. 차이점은 Azure의 FMC 서비스 제공자 애플리케이션 설정에 있습니다.

Note 개별 권한 또는 그룹 권한에 따라 FMC 역할을 매핑하도록 설정할 수 있지만, 단일 FMC 애플리케이션은 그룹 및 개별 사용자 모두에 대해 역할 매핑을 지원할 수 없습니다. FMC는 Azure에 설정된 하나의 클레임만 사용하여 역할 매핑을 지원할 수 있습니다.

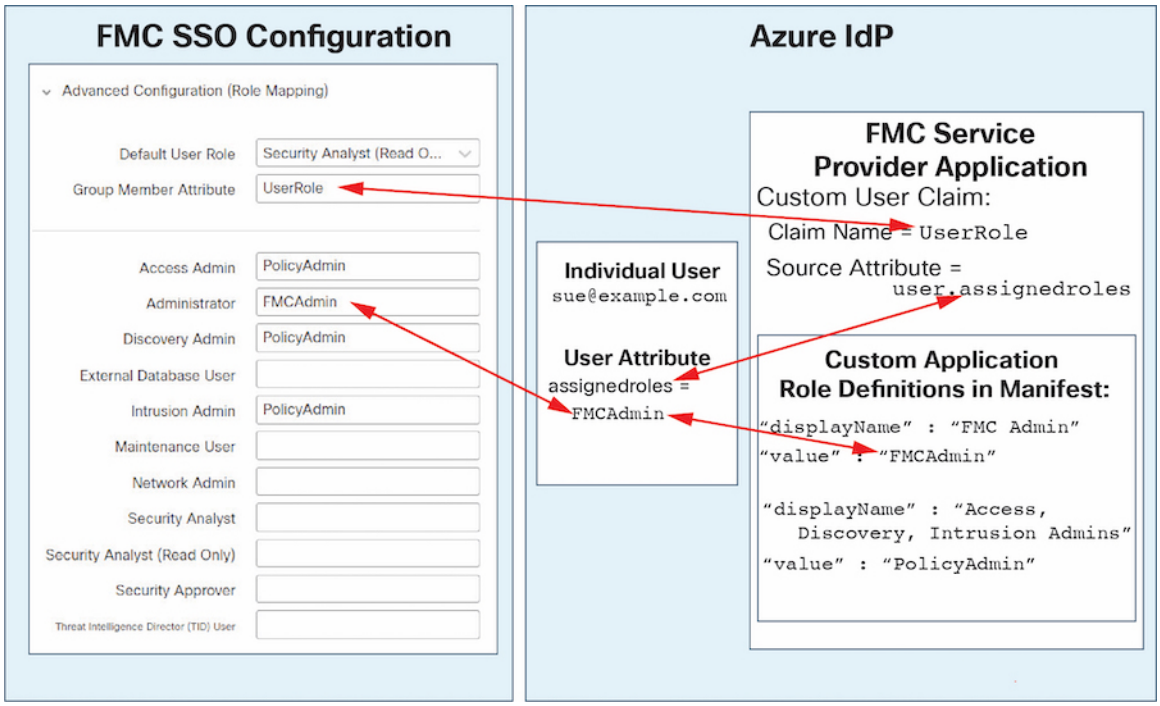
개별 사용자 계정에 대한 Azure 역할 매핑 예제

개별 사용자에 대한 역할 매핑에서 Azure FMC 서비스 애플리케이션에는 매니페스트 내에 정의된 사용자 지정 역할이 있습니다. (이 경우에는 FMCAdmin 및 PolicyAdmin입니다.) 이러한 역할은 사용자에게 할당할 수 있습니다. Azure는 해당 사용자의 할당된 역할 속성에 각 사용자에 대한 역할 할당을 저장합니다. 애플리케이션에 맞춤형 사용자 클레임도 정의되어 있으며, 이 클레임은 SSO를 통해 FMC에 로그인하는 사용자에 대해 할당된 사용자 역할에서 해당 값을 가져오도록 설정됩니다. Azure는 SSO 로그인 프로세스 중에 FMC에 클레임 값을 전달하고 FMC에서는 클레임 값을 FMCSSO 설정의 각 FMC 사용자 역할에 할당된 문자열과 비교합니다.

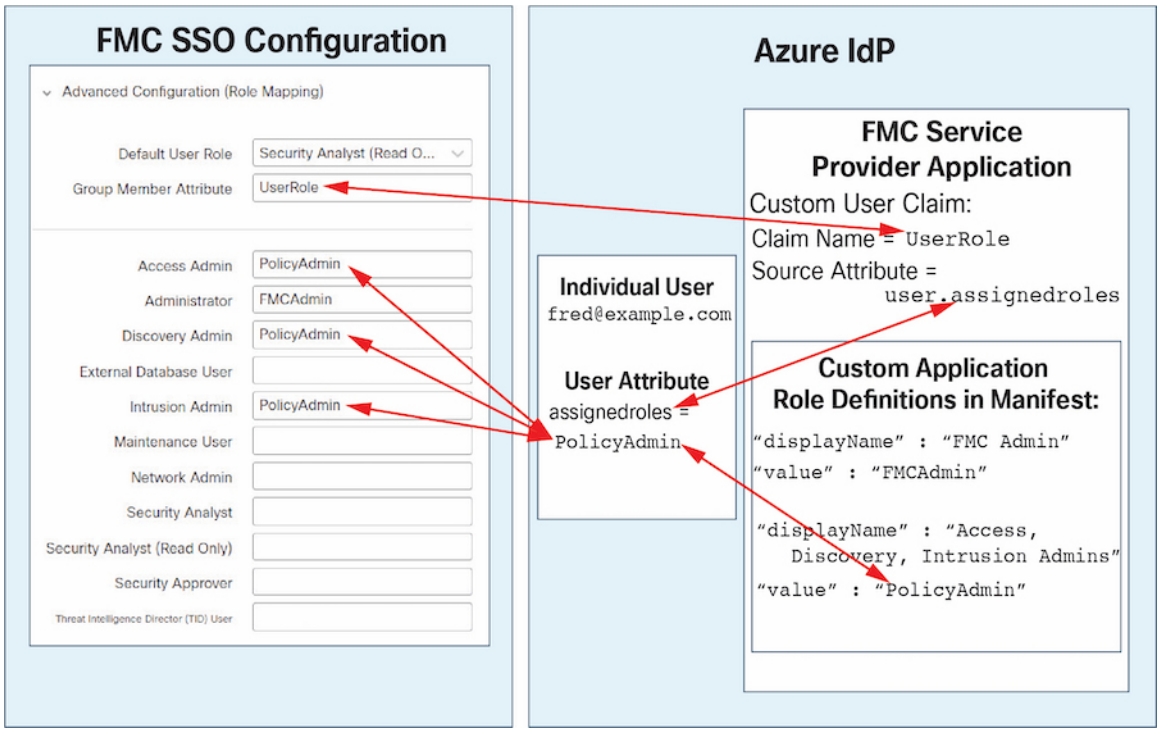
다음 다이어그램은 FMC 및 Azure 설정의 관련 필드와 값이 개별 계정에 대한 사용자 역할 매핑에서 서로 어떻게 대응하는지를 보여줍니다. 각 다이어그램은 FMC 및 Azure AD 포털에서 동일한 SSO 구

성을 사용하지만, Azure AD 포털의 각 사용자에 대한 설정은 FMC에서 각 사용자에게 서로 다른 역할을 할당하는 방식이 다릅니다.

- 이 다이어그램에서 sue@example.com은 assignedroles 속성값 `FMCAdmin`을 사용하며, FMC는 FMC 관리자 역할을 할당합니다.



- 이 다이어그램에서 fred@example.com은 assignedroles 속성값 `PolicyAdmin`을 사용하며 FMC는 액세스 관리자, 검색 관리자 및 침입 관리자 역할을 할당합니다.



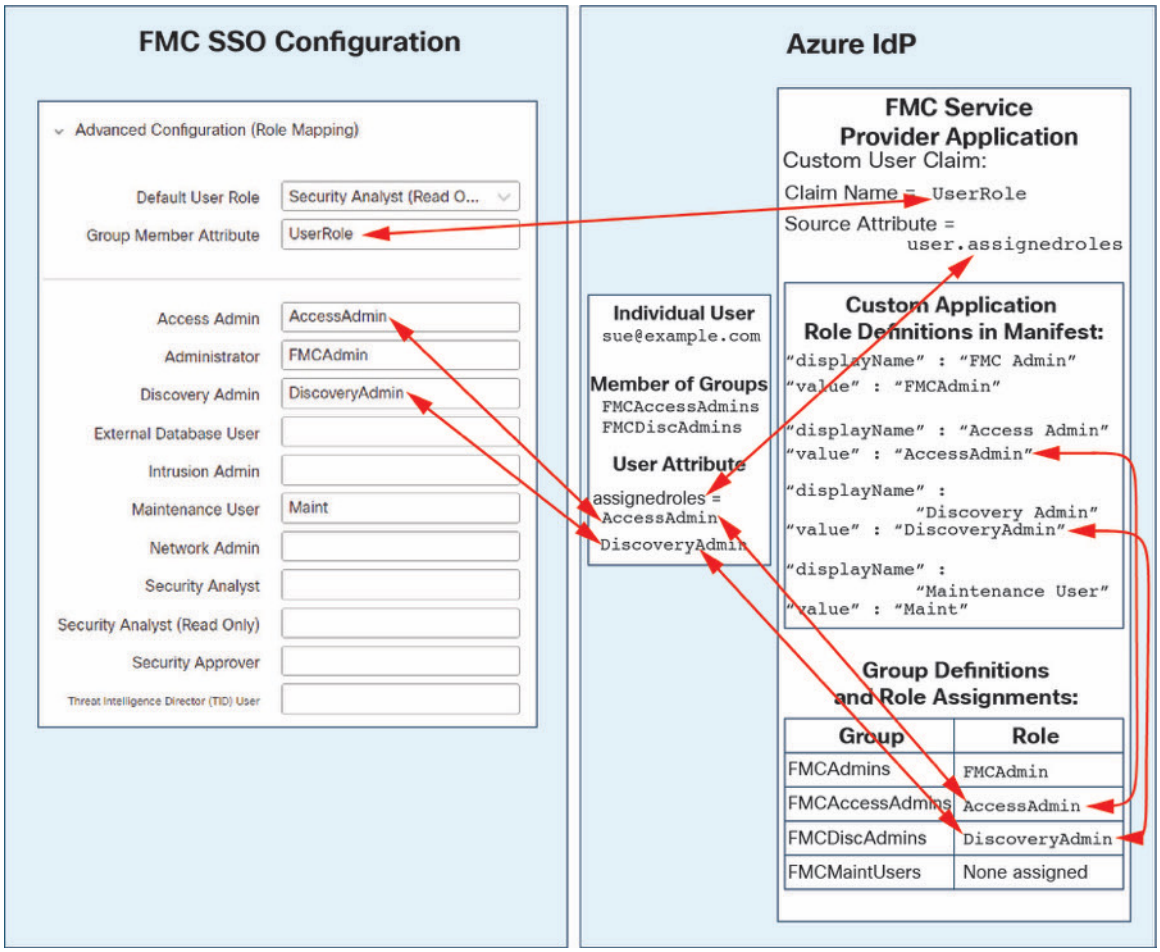
- FMC를 위해 Azure 서비스 애플리케이션에 할당된 기타 사용자에게는 다음 중 하나의 이유로 기본 사용자 역할 보안 분석가(읽기 전용)가 할당됩니다.
  - assignedroles 속성에 할당된 값이 없습니다.
  - assignedroles 속성에 할당된 값이 FMC의 SSO 설정에서 사용자 역할에 대해 구성된 식과 일치하지 않습니다.

그룹에 대한 **Azure** 역할 매핑 예

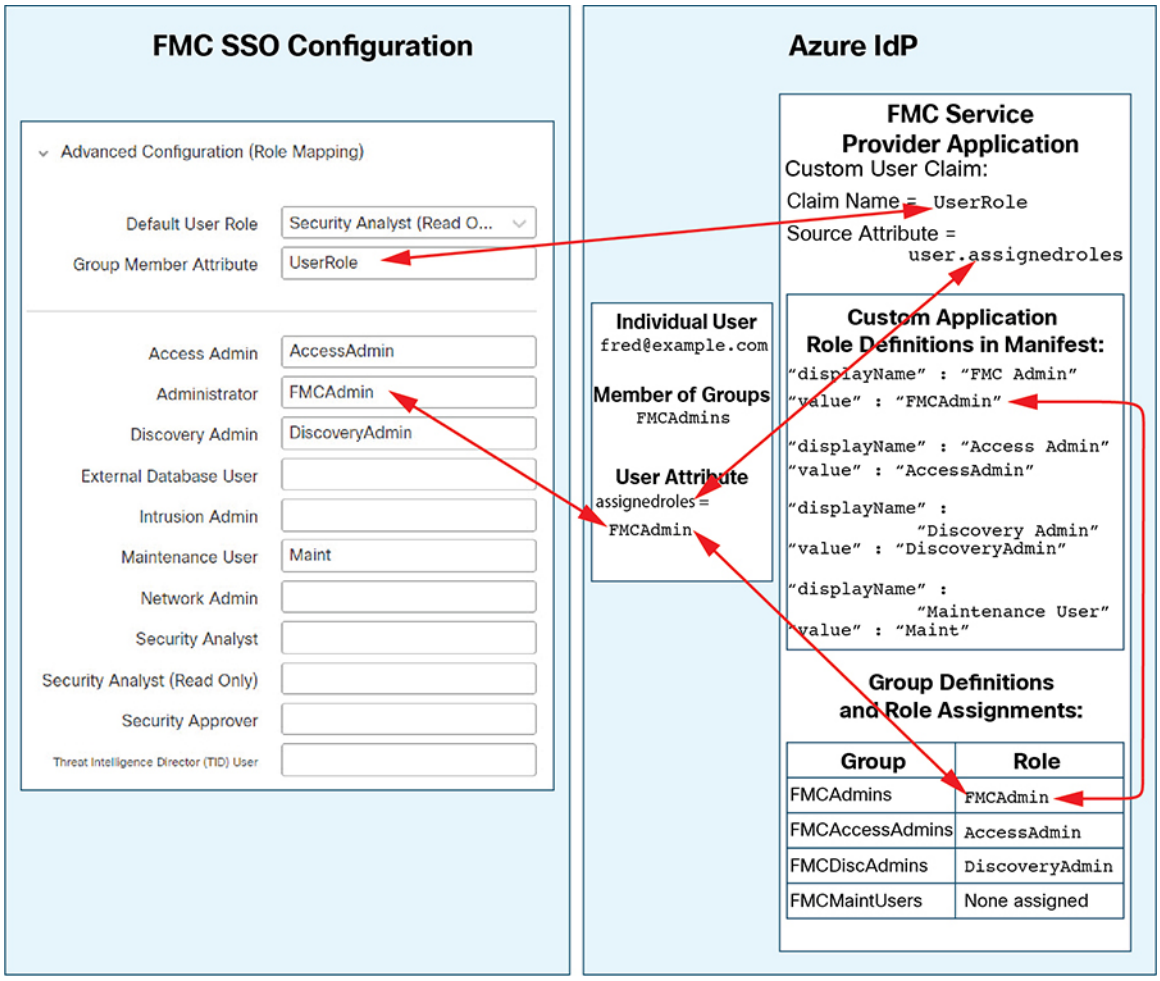
그룹에 대한 역할 매핑에서 Azure FMC 서비스 애플리케이션에는 매니페스트 내에 정의된 사용자 지정 역할이 있습니다. (이 경우 FMCAdmin, AccessAdmin, Discovery Admin 및 Maint입니다.) 이러한 역할은 그룹에 할당할 수 있습니다. Azure는 해당 그룹의 할당된 역할 속성에 각 그룹 멤버에 대한 역할 할당을 전달합니다. 애플리케이션에 맞춤형 사용자 클레임도 정의되어 있으며, 이 클레임은 SSO를 통해 FMC에 로그인하는 사용자에 대해 할당된 사용자 역할에서 해당 값을 가져오도록 설정됩니다. Azure는 SSO 로그인 프로세스 중에 FMC에 클레임 값을 전달하고 FMC에서는 클레임 값을 FMCSSO 설정의 각 FMC 사용자 역할에 할당된 문자열과 비교합니다.

다음 다이어그램은 FMC 및 Azure 구성의 관련 필드와 값이 그룹에 대한 사용자 역할 매핑에서 서로 어떻게 일치하는지를 보여줍니다. 각 다이어그램은 FMC 및 Azure AD 포털에서 동일한 SSO 구성을 사용하지만, Azure AD 포털의 각 사용자에 대한 설정은 FMC에서 각 사용자에게 서로 다른 역할을 할당하는 방식이 다릅니다.

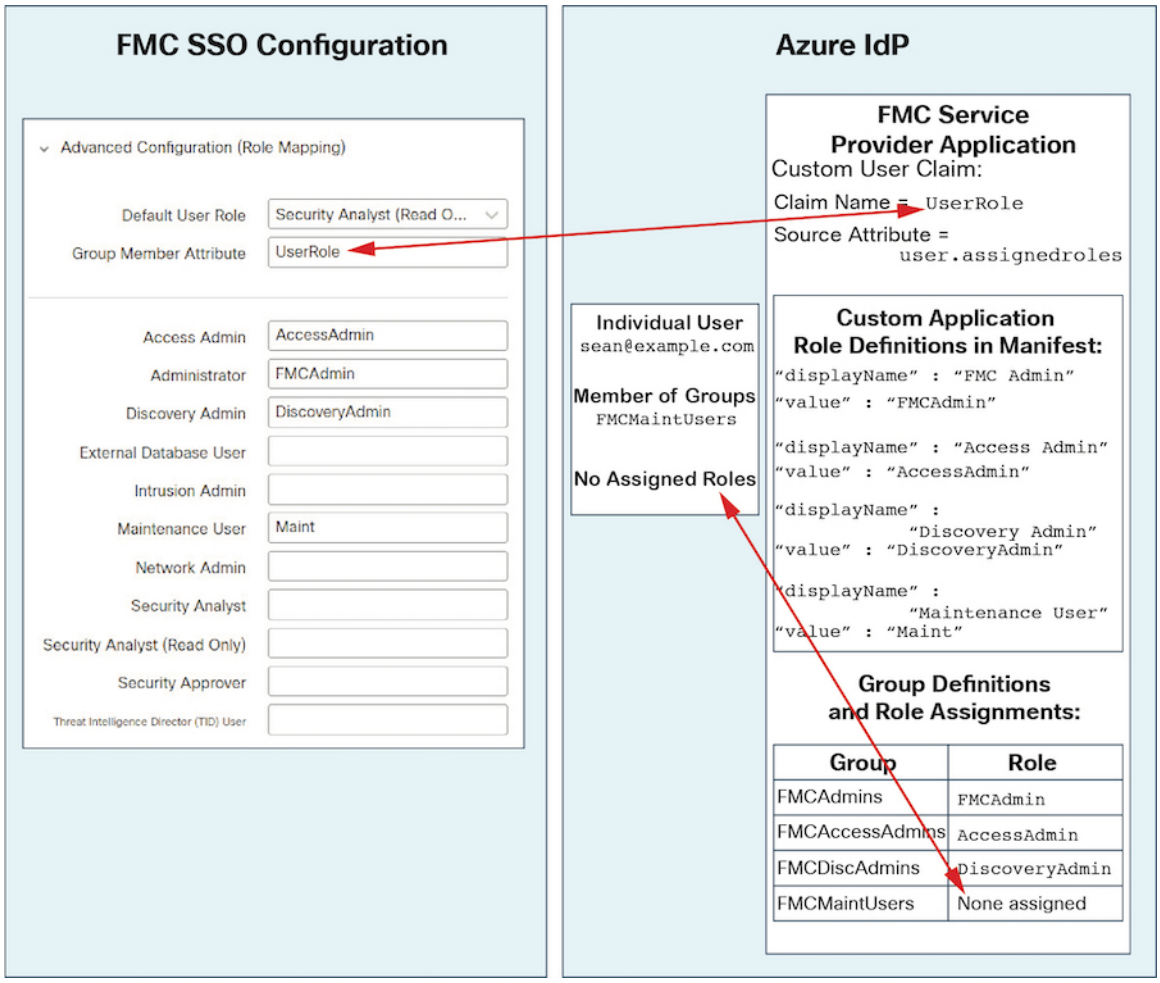
- 이 다이어그램에서 sue@example.com은 `FMCAccessAdmins` 및 `FMCDiscoveryAdmins` 그룹의 멤버입니다. 이러한 그룹에서 맞춤형 역할 `AccessAdmin` 및 `DiscoveryAdmin`을 상속합니다. Sue가 SSO를 사용하여 FMC에 로그인하면 FMC에서는 액세스 관리자 및 검색 관리자 역할을 할당합니다.



- 이 다이어그램에서 fred@example.com은 `FMCAdmins` 그룹의 멤버이며, 이 그룹에서 맞춤형 역할 `FMCAdmin`을 상속합니다. 프레드가 SSO를 사용하여 FMC에 로그인하면 FMC는 관리자 역할을 할당합니다.

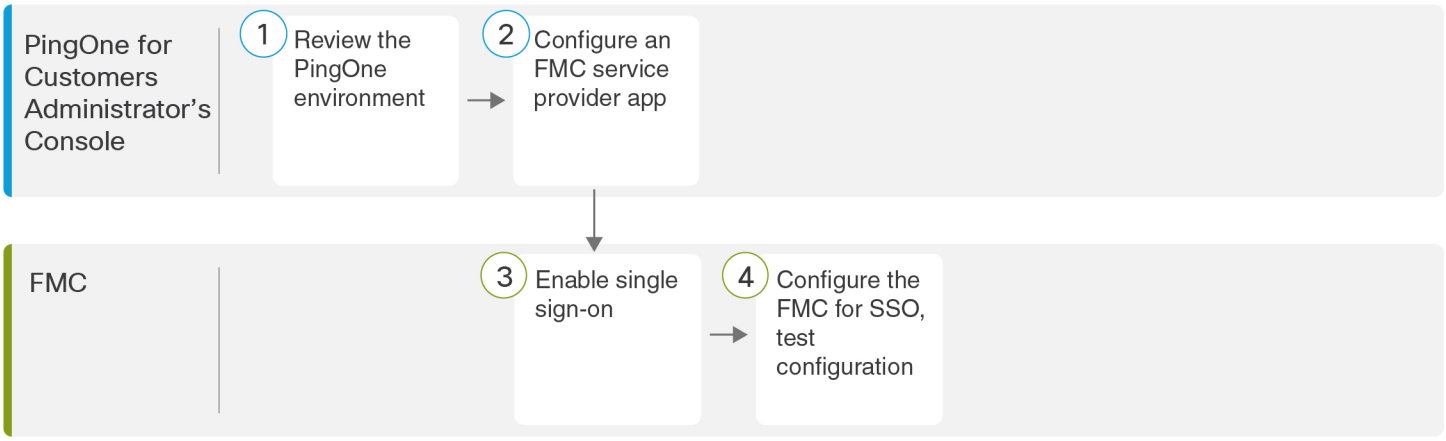


- 이 다이어그램에서 sean@example.com은 `FMCMaintUsers` 그룹의 멤버입니다. 그러나 Azure FMC 서비스 제공자 애플리케이션 내에서 `FMCMaintUsers`에 맞춤형 역할이 할당되지 않았기 때문에, 해당 사용자에게 할당된 역할이 없으며, SSO를 사용하여 FMC에 로그인할 때, FMC는 기본 역할인 Security Analyst(읽기 전용)를 지정합니다.



PingID로 SSO(Single Sign-On) 구성

PingID의 PingOne for Customers 제품을 사용하여 SSO를 설정하려면 다음 작업을 참조하십시오.



1	PingOne for Customers 관리자 콘솔	PingID PingOne for Customers 환경 검토, on page 69.
2	PingOne for Customers 관리자 콘솔	PingID PingOne for Customers에 대한 FMC 서비스 제공자 애플리케이션 설정, on page 69.
3	FMC	FMC에서 SSO(Single Sign-On) 활성화, on page 28.
4	FMC	PingID PingOne for Customers을 사용하여 SSO용 FMC을 구성합니다., on page 71.

PingID PingOne for Customers 환경 검토

PingOne for Customers는 PingID의 클라우드 호스팅 IDaaS(Identity-as-a-Service) 제품입니다. PingOne for Customers에서는 사용자가 동일한 SSO 계정으로 액세스할 수 있는 모든 페더레이션된 디바이스를 포함하는 엔터티를 환경이라고 합니다. PingOne 환경에 FMC를 추가하기 전에 해당 조직에 대해 잘 알고 있어야합니다. 다음 질문을 고려해 보십시오.

- FMC에 액세스할 수 있는 사용자는 몇 명입니까?
- FMC에 대한 SSO 액세스를 지원하려면 사용자를 더 추가해야 합니까?

이 문서에서는 사용자가 PingOne for Customers 관리자 콘솔에 대해 잘 알고 있으며 조직 관리자 역할의 계정을 가지고 있다고 가정합니다.

PingID PingOne for Customers에 대한 FMC 서비스 제공자 애플리케이션 설정

PingOne for Customers 관리자 콘솔을 사용하여 PingOne for Customers 환경에서 FMC 서비스 제공자 애플리케이션을 생성하고 기본 구성 설정을 구성합니다. 이 문서에서는 모든 기능을 갖춘 SSO 환경을 설정하는 데 필요한 PingOne for Customers 기능을 전부 설명하지 않습니다. 가령 사용자를 생성하려면 PingOne for Customers 문서를 참조하면 됩니다.

Before you begin

- PingOne for Customers 환경 및 해당 사용자를 숙지하십시오.
- 필요한 경우, 사용자를 추가로 생성합니다.

Note FMC에서는 SSO 계정의 사용자 이름과 SAML 로그인 프로세스 중에 IdP가 FMC에 전송하는 NameID 속성이 모두 유효한 이메일 주소여야 합니다. 대부분의 IdP는 자동으로 NameID 속성으로 로그온하려는 사용자의 사용자 이름을 사용하지만, 이 기능이 현재 사용 중인 IdP에도 적용되는지 확인해야 합니다. IdP에서 서비스 제공자 애플리케이션을 설정하고 FMC에 SSO 액세스 권한을 부여할 IdP 사용자 계정을 생성할 때 이 점에 유의하십시오.

- 대상 FMC(`https://ipaddress_or_hostname`)의 로그인 URL을 확인합니다.

Note 여러 URL(예: 정규화된 도메인 이름 및 IP 주소)로 FMC 웹 인터페이스에 연결할 수 있는 경우, SSO 사용자는 이 작업에서 구성한 로그인 URL을 사용하여 FMC에 일관되게 액세스해야 합니다.

Procedure

단계 **1** 다음 설정을 사용하여 사용자 환경에서 애플리케이션을 생성하려면 PingOne for Customers 관리자 콘솔을 확인하십시오.

- **Web App(**웹 앱**)** 애플리케이션 유형을 선택합니다.
- **SAML** 연결 유형을 선택합니다.

단계 **2** SAML 연결에 대해 다음 설정으로 애플리케이션을 구성합니다.

- **ACS URL**의 경우, `/sam/acs` 문자열을 FMC 로그인 URL에 추가합니다. 예: `https://ExampleFMC/saml/acs`
- **Signing Certificate(**서명 인증서**)**에 대해 Sign Assertion & Response(어설션 서명 및 응답)를 선택합니다.
- **Signing Algorithm(**서명 알고리즘**)**에 대해 RSA_SHA256을 선택합니다.
- **Entity ID(**엔티티 **ID)**의 경우, `/saml/metadata` 문자열을 FMC 로그인 URL에 추가합니다. 예: `https://ExampleFMC/saml/metadata`
- **SLO Binding(SLO** 바인딩**)**의 경우, HTTP POST를 선택합니다.
- **Assertion Validity Duration(**어설션 유효 기간**)**에 300을 입력합니다.

단계 **3** 애플리케이션의 SAMLConnection 정보에서 다음 값을 확인합니다.

- **SSO(Single Sign-On)** 서비스
- 발급자 **ID**

FMC 웹 인터페이스에서 PingID의 PingOne for Customers 제품을 사용하여 SSO를 설정할 때 이러한 값이 필요합니다.

단계 **4** **SAML ATTRIBUTES(SAML** 속성**)**의 경우, 단일 필수 속성에 대해 다음을 선택합니다.

- **PINGONE USER ATTRIBUTE(PINGONE** 사용자 속성**):** `이메일 주소`
- **APPLICATION ATTRIBUTE(**애플리케이션 속성**):** `saml_subject`

단계 **5** X509 PEM(`.crt`) 형식으로 서명 인증서를 다운로드하여 로컬 컴퓨터에 저장합니다.

단계 6 (선택 사항) FMC에 SSO를 보다 쉽게 설정할 수 있도록 FMC 서비스 제공자 애플리케이션의 SAML XML 메타데이터 파일을 로컬 컴퓨터에 다운로드할 수 있습니다.

단계 7 애플리케이션을 활성화합니다.

What to do next

SSO(Single Sign-On)를 활성화합니다. FMC에서 SSO(Single Sign-On) 활성화, on page 28의 내용을 참조하십시오.

PingID PingOne for Customers을 사용하여 SSO용 FMC을 구성합니다.

FMC 웹 인터페이스에서 다음 지침을 참조하십시오.

Before you begin

- PingOne for Customers Administrator Console에서 FMC 서비스 제공자 애플리케이션을 생성합니다. PingID PingOne for Customers에 대한 FMC 서비스 제공자 애플리케이션 설정, on page 69의 내용을 참조하십시오.
- SSO(Single Sign-On)을 활성화합니다. FMC에서 SSO(Single Sign-On) 활성화, on page 28의 내용을 참조하십시오.

Procedure

단계 1 이 단계는 FMC에서 SSO(Single Sign-On) 활성화, on page 28에서 곧바로 이어집니다. **Configure PingID Metadata(PingID** 메타데이터 구성**)** 대화 상자에서 두 가지 옵션을 선택할 수 있습니다.

- SSO 컨피그레이션 정보를 수동으로 입력하려면 다음을 수행합니다.
  a. **Manual Configuration(**수동 구성**)** 라디오 버튼을 클릭합니다.
  b. PingOne for Customers Administrator Console에서 검색한 값을 입력합니다.
     - **ID** 제공자 **SSO(Single Sign-On) URL**의 경우 PingID PingOne for Customers에 대한 FMC 서비스 제공자 애플리케이션 설정, on page 69 3단계에서 적어둔 **SSO(Single Sign-On)** 서비스를 입력합니다.
     - **Identity Provider Issuer(ID** 제공자 발급자**)**의 경우 PingID PingOne for Customers에 대한 FMC 서비스 제공자 애플리케이션 설정, on page 69 3단계에서 적어둔 발급자 **ID**를 입력합니다.
     - **X.509** 인증서의 경우 PingID PingOne for Customers에 대한 FMC 서비스 제공자 애플리케이션 설정, on page 69 5단계 중 PingOne for Customers에서 다운로드한 인증서를 사용합니다. (텍스트 편집기를 사용하여 인증서 파일을 열고 내용을 복사하여 **X.509 Certificate(X.509** 인증서**)** 필드에 붙여 넣습니다.)

- PingOne for Customers에서 생성한 XML 메타데이터 파일을 로컬 컴퓨터에 저장한 경우, (PingID PingOne for Customers에 대한 FMC 서비스 제공자 애플리케이션 설정, on page 69의 6단계) 파일을 FMC에 업로드할 수 있습니다.

  a. **Upload XML File(XML** 파일 업로드**)** 라디오 버튼을 클릭합니다.

  b. 화면의 지침에 따라 로컬 컴퓨터에서 XML 메타데이터 파일을 찾아 선택합니다.

단계 **2** **Next(**다음**)**를 클릭합니다.

단계 **3** **Verify Metadata(**메타데이터 확인**)** 대화 상자에서 컨피그레이션 매개변수를 검토하고 **Save(**저장**)**를 클릭합니다.

단계 **4** **Advanced Configuration(Role Mapping)(**고급 구성**(**역할 매핑**))**을 펼칩니다.

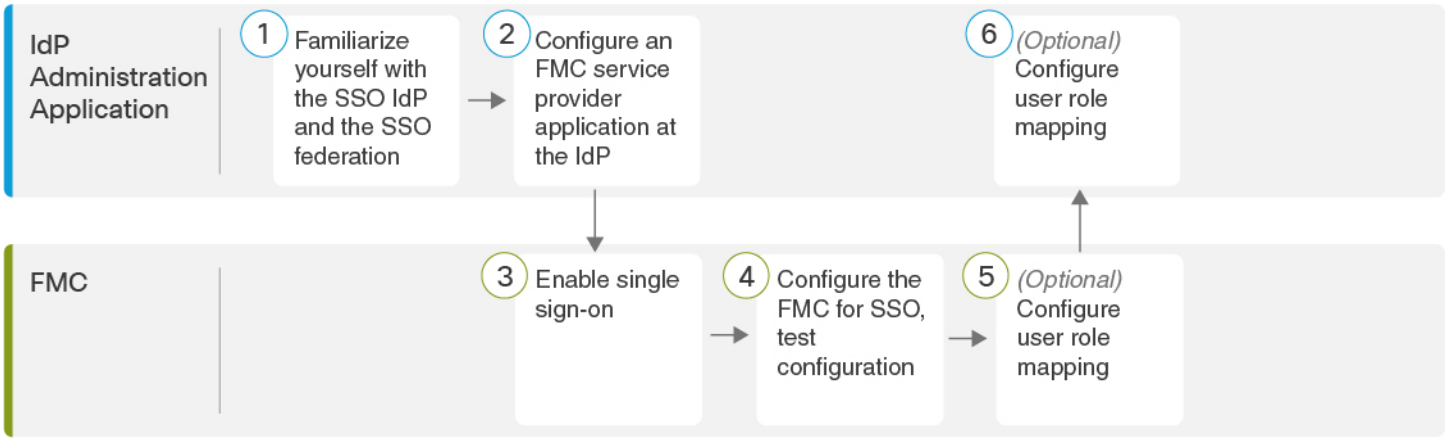
단계 **5** **Default User Role(**기본 사용자 역할**)** 드롭다운에서 FMC 사용자 역할을 선택해서 사용자를 기본값으로 할당합니다.

단계 **6** **Test Configuration(**컨피그레이션 테스트**)**을 클릭합니다. 시스템에 오류 메시지가 표시되면 FMC의 SSO 구성과 PingOne for Customers 서비스 제공자 애플리케이션 구성을 검토하고 오류를 수정한 후 다시 시도하십시오.

단계 **7** 시스템에서 컨피그레이션 테스트에 성공했다고 보고하면 **Apply(**적용**)**를 클릭합니다.

SAML 2.0 규정준수 SSO 제공자로 SSO(Single Sign-On) 구성

FMC에서는 SAML 2.0 SSO 프로토콜을 준수하는 모든 SSO ID 제공자(IdP)에서 SSO(Single Sign-On)를 지원합니다. 광범위한 SSO 제공자를 사용하기 위한 일반적인 지침은 높은 수준에서 수행할 작업을 처리해야 합니다. 이 문서에서 구체적으로 다루지 않은 제공자를 사용하여 SSO를 설정하려면 선택한 IdP를 능숙하게 다루어야 합니다. 이러한 작업을 통해 SAML 2.0을 준수하는 SSO 제공자를 사용하여 SSO(Single Sign-On)에 대해 FMC를 설정하는 단계를 결정할 수 있습니다.



1	IdP 관리 애플리케이션	SSO ID 제공자 및 SSO 페더레이션을 숙지합니다., on page 73.

2	IdP 관리 애플리케이션	SAML 2.0 호환 SSO 제공자에 대한 FMC 서비스 제공자 애플리케이션 구성, on page 74.
3	FMC	FMC에서 SSO(Single Sign-On) 활성화, on page 28.
4	FMC	SAML 2.0 호환 SSO 제공자를 사용하여 SSO용 FMC 구성, on page 75.
5	FMC	SAML 2.0 호환 SSO 제공자에 대해 FMC에서 사용자 역할 매핑 설정, on page 77.
6	IdP 관리 애플리케이션	SAML 2.0 호환 SSO 제공자에 대해 IdP에서 FMC 사용자 역할 매핑 설정, on page 78에 전달하는 고성능 고속 어플라이언스입니다.

SSO ID 제공자 및 SSO 페더레이션을 숙지합니다.

다음 사항을 고려하여 IdP 벤더 설명서를 읽으십시오.

- SSO 제공자가 사용자에게 IdP를 사용하기 전에 서비스를 구독하거나 등록하도록 요구합니까?
- SSO 제공자가 일반적인 SSO 개념에 사용하는 용어는 무엇입니까? 예를 들어 페더레이션 서비스 공급자 애플리케이션 그룹을 참조하기 위해 Okta는 "org"를 사용하고 Azure는 "tenant"를 사용합니다.
- SSO 제공자가 SSO만 지원합니까 아니면 여러 요인(예: 다단계 인증 또는 도메인 관리)을 지원합니까? (이는 기능 간에 공유되는 일부 요소(특히 사용자 및 그룹)의 구성에 영향을 줄 수 있습니다.)
- IdP 사용자 계정에서 SSO를 구성하려면 어떤 권한이 필요합니까?
- SSO 제공자가 서비스 제공자 애플리케이션에 대해 설정해야 하는 구성은 무엇입니까? 예를 들어 Okta는 FMC와의 통신을 보호하기 위해 X509 인증서를 자동으로 생성하지만, Azure에서는 Azure 포털 인터페이스를 사용하여 해당 인증서를 생성해야 합니다.
- 사용자 및 그룹은 어떻게 생성되고 구성됩니까? 사용자는 그룹에 어떻게 할당됩니까? 사용자 및 그룹은 어떻게 서비스 제공자 애플리케이션에 대한 액세스 권한을 부여 받습니까?
- SSO 연결을 테스트하기 전에 SSO 제공자가 하나 이상의 사용자를 서비스 제공자 애플리케이션에 할당해야 합니까?
- SSO 제공자가 사용자 그룹을 지원합니까? 사용자 및 그룹 속성은 어떻게 구성됩니까? SSO 구성에서 어떻게 FMC 사용자 역할에 속성을 매핑할 수 있습니까

- FMC에서 SSO를 지원하려면 페더레이션에 사용자 또는 그룹을 더 추가해야 합니까?
- 사용자가 그룹의 페더레이션 구성원 내에 있습니까?
- 사용자 및 그룹 정의가 IdP에 기본적이거나 Active Directory, RADIUS 또는 LDAP와 같은 사용자 관리 애플리케이션에서 가져온 것입니까?
- 어떤 종류의 사용자 역할을 지정하시겠습니까? (사용자 역할을 할당하지 않도록 선택하는 경우 FMC는 모든 SSO 사용자에게 구성 가능한 기본 사용자 역할을 자동으로 할당합니다.)
- 사용자 역할 매핑을 위한 계획을 지원하려면 페더레이션 내의 사용자 및 그룹을 어떻게 구성해야 합니까?

SAML 2.0 호환 SSO 제공자에 대한 FMC 서비스 제공자 애플리케이션 구성

일반적으로 SSO 제공자는 각 연동 애플리케이션에 대해 IdP에서 서비스 제공자 애플리케이션을 구성해야 합니다. SAML 2.0 SSO를 지원하는 모든 IdP는 서비스 제공자 애플리케이션에 대해 동일한 구성 정보가 필요하지만 일부 IdP는 자동으로 일부 구성 설정을 생성하는 반면, 일부는 모든 설정을 직접 구성해야 합니다.

Note FMC 애플리케이션에 사용자 그룹을 할당하려는 경우 해당 그룹의 사용자를 개인으로 할당하지 마십시오.

Note FMC는 여러 SSO 특성을 사용하는 역할 매핑을 지원할 수 없습니다. 사용자 역할 매핑 또는 그룹 역할 매핑을 선택하고 사용자 특성을 IdP에서 FMC로 전달하도록 단일 속성을 구성해야 합니다.

Before you begin

- SSO 페더레이션 그리고 해당 사용자 및 그룹을 숙지하십시오. SSO ID 제공자 및 SSO 페더레이션을 숙지합니다., on page 73의 내용을 참조하십시오.
- IdP 계정에 이 작업을 수행하는 데 필요한 권한이 있는지 확인합니다.
- 필요한 경우 SSO 페더레이션에서 사용자 계정 및/또는 그룹을 생성합니다.

  Note FMC에서는 SSO 계정의 사용자 이름과 SAML 로그인 프로세스 중에 IdP가 FMC에 전송하는 NameID 속성이 모두 유효한 이메일 주소여야 합니다. 대부분의 IdP는 자동으로 NameID 속성으로 로그온하려는 사용자의 사용자 이름을 사용하지만, 이 기능이 현재 사용 중인 IdP에도 적용되는지 확인해야 합니다. IdP에서 서비스 제공자 애플리케이션을 설정하고 FMC에 SSO 액세스 권한을 부여할 IdP 사용자 계정을 생성할 때 이 점에 유의하십시오.

- 대상 FMC(`https://ipaddress_or_hostname`)의 로그인 URL을 확인합니다.

Note 여러 URL로 FMC 웹 인터페이스에 연결할 수 있는 경우 (예: 정규화된 도메인 이름 및 IP 주소) SSO 사용자는 이 작업에서 구성한 로그인 URL을 사용하여 FMC에 일관되게 액세스해야 합니다.

Procedure

단계 **1** IdP에서 새 서비스 제공자 애플리케이션을 생성합니다.

단계 **2** IdP에 필요한 값을 구성합니다. FMC에 SAML 2.0 SSO 기능을 지원하는 데 필요한 아래에 나열된 필드를 포함해야 합니다. 각기 다른 SSO 서비스 제공자가 SAML 개념에 대해 다른 용어를 사용하므로 이 목록은 IdP 애플리케이션에서 올바른 설정을 찾는 데 도움이 되도록 이러한 필드에 대한 대체 이름을 제공합니다.

- 서비스 제공자 엔티티 ID, 서비스 제공자 식별자, 대상 URI: URL 형식의 서비스 제공자(FMC)에 대한 전역 고유 이름. 이를 생성하려면 `/saml/metadata` 문자열(예: `https://ExampleFMC/saml/metadata`)을 FMC 로그인 URL에 추가합니다.
- SSO(Single Sign-On, 단일 인증) URL, 수신자 URL, 어설션 소비자 서비스 URL: 브라우저가 IdP를 대신하여 정보를 전송하는 서비스 제공자(FMC) 주소입니다. 이를 생성하려면 FMC 로그인 URL에 `saml/acs` 문자열(예: `https://ExampleFMC/saml/acs`)을 추가합니다.
- X.509 인증서: FMC와 IdP 간의 통신을 보호하기 위한 인증서입니다. 일부 IdP는 인증서를 자동으로 생성할 수 있으며, 일부는 IdP 인터페이스를 사용하여 명시적으로 생성해야 할 수 있습니다.

단계 **3** (선택적으로 애플리케이션에 그룹을 할당하는 경우) 개별 사용자를 FMC 애플리케이션에 할당합니다. (FMC 애플리케이션에 그룹을 할당하려는 경우 해당 그룹의 멤버를 개인으로 할당하지 마십시오.)

단계 **4** (애플리케이션에 개별 사용자를 할당하는 경우엔 선택 사항입니다.) FMC 애플리케이션에 사용자 그룹을 할당합니다.

단계 **5** (선택 사항) 일부 IdP는 이 작업에서 구성한 정보가 포함된 SAML XML 메타데이터 파일을 생성하는 기능을 제공합니다. IdP가 이 기능을 제공하는 경우, 파일을 로컬 컴퓨터에 다운로드하여 FMC에서 SSO 구성 프로세스를 쉽게 수행할 수 있습니다.

What to do next

SSO(Single Sign-On)을 활성화합니다. FMC에서 SSO(Single Sign-On) 활성화, on page 28의 내용을 참조하십시오.

SAML 2.0 호환 SSO 제공자를 사용하여 SSO용 FMC 구성

FMC 웹 인터페이스에서 다음 지침을 사용하십시오. SAML 2.0 호환 SSO 제공자를 사용하여 SSO에 대해 FMC를 구성하려면 IdP의 정보가 필요합니다.

Before you begin

- SSO 페더레이션의 조직과 해당 사용자 및 그룹을 검토합니다.
- IdP에서 FMC 서비스 제공자 애플리케이션을 구성합니다. SAML 2.0 호환 SSO 제공자를 사용하여 SSO용 FMC 구성, on page 75의 내용을 참조하십시오.
- IdP에서 서비스 제공자 애플리케이션에 대한 다음 SSO 구성 정보를 수집합니다. 각기 다른 SSO 서비스 제공자가 SAML 개념에 대해 다른 용어를 사용하므로 이 목록은 IdP 애플리케이션에서 올바른 값을 찾는 데 도움이 되도록 이러한 필드에 대한 대체 이름을 제공합니다.
  - ID 공급자 SSO(Single Sign-On) URL, 로그인 URL: 브라우저가 FMC 대신 정보를 전송하는 IdP URL입니다.
  - ID 제공자 발급자, ID 제공자 발급자 URL, 발급자 URL: IdP의 전역 고유 이름으로, 대개 URL 형식으로 지정됩니다.
  - FMC와 IdP 간의 통신을 보호하기 위한 X.509 디지털 인증서.
- SSO(Single Sign-On)을 활성화합니다. FMC에서 SSO(Single Sign-On) 활성화, on page 28의 내용을 참조하십시오.

Procedure

단계 **1** (이 절차는 FMC에서 SSO(Single Sign-On) 활성화, on page 28에서 곧바로 이어집니다.) **Configure SAML Metadata(SAML** 메타데이터 구성**)** 대화 상자에서 두 가지 옵션을 선택할 수 있습니다.

- SSO 컨피그레이션 정보를 수동으로 입력하려면 다음을 수행합니다.
  a. **Manual Configuration(**수동 구성**)** 라디오 버튼을 클릭합니다.
  b. SSO 서비스 제공자 애플리케이션에서 이전에 얻은 다음 값을 입력합니다.
     - **ID** 제공자 **SSO(Single Sign-On) URL**
     - **ID** 제공자 발급자
     - **X.509** 인증서
- IdP에서 생성된 XML 메타데이터 파일을 저장한 경우(SAML 2.0 호환 SSO 제공자에 대한 FMC 서비스 제공자 애플리케이션 구성, on page 74의 5 단계) FMC에 파일을 업로드 할 수 있습니다.
  a. **Upload XML File(XML** 파일 업로드**)** 라디오 버튼을 클릭합니다.
  b. 화면의 지침에 따라 로컬 컴퓨터에서 XML 메타데이터 파일을 찾아 선택합니다.

단계 **2** **Next(**다음**)**를 클릭합니다.

단계 **3** **Verify Metadata(**메타데이터 확인**)** 대화 상자에서 컨피그레이션 매개변수를 검토하고 **Save(**저장**)**를 클릭합니다.

단계 4 **Test Configuration(**컨피그레이션 테스트**)**을 클릭합니다. 시스템에 오류 메시지가 표시되면 FMC의 SSO 구성과 IdP의 서비스 제공자 애플리케이션 구성을 검토하고 오류를 수정한 후 다시 시도하십시오.

단계 5 시스템에서 컨피그레이션 테스트에 성공했다고 보고하면 **Apply(**적용**)**를 클릭합니다.

What to do next

선택적으로 SSO 사용자에 대한 사용자 역할 매핑을 구성할 수 있습니다. SAML 2.0 호환 SSO 제공자에 대해 FMC에서 사용자 역할 매핑 설정, on page 77의 내용을 참조하십시오. 역할 매핑을 구성하지 않도록 선택하는 경우, 기본적으로 FMC에 로그인하는 모든 SSO 사용자에게 SAML 2.0 호환 SSO 제공자에 대해 FMC에서 사용자 역할 매핑 설정, on page 77의 4단계에서 구성한 기본 사용자 역할이 할당됩니다.

SAML 2.0 호환 SSO 제공자에 대해 FMC에서 사용자 역할 매핑 설정

SAML SSO 사용자 역할 매핑을 구현하려면 IdP 및 FMC에서 조정 구성을 설정해야 합니다.

- IdP에서 사용자 또는 그룹 속성을 설정하여 사용자 역할 정보를 전달하고 값을 할당합니다. IdP는 SSO 사용자를 인증하고 권한을 부여하고 나서 FMC에 이를 전송합니다.
- FMC에서 값을 사용자에게 할당할 각 FMC 사용자 역할과 연결합니다.

IdP가 권한 있는 사용자와 연결된 사용자 또는 그룹 속성을 FMC에 전송하는 경우, FMC에서는 속성 값을 각 FMC 사용자 역할에 연결된 값과 비교하고 일치를 생성하는 모든 역할을 사용자에게 할당합니다. FMC는 Golang 및 Perl에서 지원하는 Google RE2 정규식 표준의 제한된 버전을 준수하는 정규식으로 두 값을 모두 처리하며 비교를 수행합니다.

FMC 웹 인터페이스에서 사용자 역할 매핑을 구성할 수 있는 필드는 선택한 SSO 제공자와 상관없이 동일합니다. 그러나 구성하는 값의 경우, 사용하는 SAML SSO 제공자가 사용자 역할 매핑을 구현하는 방식을 고려해야 합니다. IdP가 사용자 또는 그룹 속성에 대해 구문 제한을 적용할 수 있습니다. 그러한 경우에는 역할 이름 및 해당 요건과 호환되는 정규식으로 사용자 역할 매핑 체계를 구성해야 합니다.

Before you begin

- FMC에 대한 SSO 서비스 제공자 애플리케이션을 설정합니다. SAML 2.0 호환 SSO 제공자에 대한 FMC 서비스 제공자 애플리케이션 구성, on page 74의 내용을 참조하십시오.
- FMC에서 SSO(Single Sign-On)를 활성화하고 설정합니다. FMC에서 SSO(Single Sign-On) 활성화, on page 28 및 SAML 2.0 호환 SSO 제공자를 사용하여 SSO용 FMC 구성, on page 75의 내용을 참조하십시오.

Procedure

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

단계 2 **Single Sign-On(**단일 인증**)** 탭을 클릭합니다.

단계 **3** **Advanced Configuration (Role Mapping)**(고급 설정(역할 매핑))을 펼칩니다.

단계 **4** **Default User Role**(기본 사용자 역할) 드롭다운에서 FMC 사용자 역할을 선택해서 사용자를 기본값으로 할당합니다.

단계 **5** **Group Member Attribute**(그룹 멤버 속성)을 입력합니다. 이 문자열은 사용자 또는 그룹에 대한 사용자 역할을 매핑하기 위해 IdP FMC 서비스 제공자 애플리케이션에 설정된 속성 이름과 일치해야 합니다. (SAML 2.0 호환 SSO 제공자에 대해 IdP에서 FMC 사용자 역할 매핑 설정, on page 78의 1단계 참조)

단계 **6** SSO 사용자에게 할당할 각 FMC 사용자 역할 옆에 정규식을 입력합니다. (FMC는 Golang 및 Perl에서 지원하는 Google의 RE2 정규식 표준의 제한된 버전을 사용합니다.) FMC에서는 이러한 값을 SSO 사용자 정보를 사용하여 IdP가 FMC에 전송하는 사용자 역할 매핑 속성값과 비교합니다. FMC는 사용자에게 일치하는 항목이 발견된 모든 역할의 통합을 허용합니다.

What to do next

서비스 제공자 애플리케이션에서 사용자 역할 매핑을 구성합니다. SAML 2.0 호환 SSO 제공자에 대해 IdP에서 FMC 사용자 역할 매핑 설정, on page 78의 내용을 참조하십시오.

SAML 2.0 호환 SSO 제공자에 대해 IdP에서 FMC 사용자 역할 매핑 설정

사용자 역할 매핑을 구성하는 자세한 단계는 IdP마다 다릅니다. 통신 사업자 애플리케이션에 대한 사용자 지정 사용자 또는 그룹 특성을 생성하는 방법을 결정하고 IdP에서 각 사용자 또는 그룹의 특성에 값을 할당하여 FMC에 사용자 또는 그룹 권한을 전달해야 합니다. 다음 사항에 주의하십시오.

- IdP가 서드 파티 사용자 관리 애플리케이션(예: Active Directory, LDAP 또는 Radius)에서 사용자 또는 그룹 프로파일을 가져오는 경우, 이는 역할 매핑에 속성을 사용하는 방법에 영향을 줄 수 있습니다.
- SSO 페더레이션 전체에서 사용자 및 그룹 역할 정의를 고려합니다.
- FMC는 여러 SSO 특성을 사용하는 역할 매핑을 지원할 수 없습니다. 사용자 역할 매핑 또는 그룹 역할 매핑을 선택하고 사용자 특성을 IdP에서 FMC로 전달하도록 단일 속성을 구성해야 합니다.
- 여러 사용자가 있는 경우, 그룹 역할 매핑은 일반적으로 FMC에 더 효율적입니다.
- FMC 애플리케이션에 사용자 그룹을 할당하는 경우 해당 그룹의 사용자를 개인으로 할당하지 마십시오.
- FMC 사용자 역할과의 일치를 확인하기 위해 FMC에서는 IdP에서 수신한 사용자 및 그룹 역할 속성 값을 Golang 및 Perl에서 지원하는 Google RE2 정규식 표준의 제한된 버전을 준수하는 정규식으로 처리합니다. IdP가 사용자 또는 그룹 속성에 대해 특정 구문 제한을 적용할 수 있습니다. 그러한 경우에는 역할 이름 및 해당 요건과 호환되는 정규식으로 사용자 역할 매핑 체계를 구성해야 합니다.

Before you begin

- IdP 계정에 이 작업을 수행하는 데 필요한 권한이 있는지 확인합니다.

- IdP에서 FMC 서비스 제공자 애플리케이션을 구성합니다(SAML 2.0 호환 SSO 제공자에 대한 FMC 서비스 제공자 애플리케이션 구성, on page 74 참조).

Procedure

단계 **1** IdP에서 FMC로 전송될 속성을 생성하거나 지정하여 각 사용자 로그인에 대한 역할 매핑 정보를 포함합니다. 이는 사용자 속성, 그룹 속성 또는 IdP 또는 서드 파티 사용자 관리 애플리케이션에서 유지 관리하는 사용자 또는 그룹 정의와 같은 소스에서 값을 가져오는 다른 속성일 수 있습니다.

단계 **2** 속성의 값을 가져오는 방법을 구성합니다. 가능한 값을 FMC SSO 구성의 사용자 역할과 연결된 값으로 조정합니다.

웹 인터페이스의 사용자 역할 맞춤화

각 사용자 어카운트는 사용자 역할과 함께 정의해야 합니다. 이 섹션에서는 사용자 역할을 관리하는 방법 및 웹 인터페이스 액세스에 대한 맞춤형 사용자 역할을 구성하는 방법을 설명합니다. 기본 사용자 역할에 대해서는 사용자 역할, 2 페이지의 내용을 참조하십시오.

맞춤형 사용자 역할 생성

맞춤형 사용자 역할은 메뉴 기반 및 시스템 권한 집합을 보유할 수 있으며, 사전 정의된 사용자 역할 또는 또 다른 맞춤형 사용자 역할을 원래 그대로 유지하거나 복사하거나 또 다른 디바이스에서 가져올 수 있습니다.

참고 동시 세션 제한을 위해 시스템에서 읽기 전용으로 간주하는 맞춤형 사용자 역할은 **System(**시스템**)** > **Users(**사용자**)** > **Users(**사용자**)** 탭과 **System(**시스템**)** > **Users(**사용자**)** > **User Roles(**사용자 역할**)** 탭의 역할 이름에 **(**읽기 전용**)**이라고 자동으로 표시됩니다. 사용자 역할의 역할 이름에 **(**읽기 전용**)**이라는 표시가 없다면, 시스템은 역할을 읽기/쓰기로 간주합니다.

사용자 지정 역할을 생성하거나 기존 사용자 지정 역할을 수정하는 경우, 역할에 대해 선택된 모든 허가가 읽기 전용 기준을 충족한다면 시스템은 **(**읽기 전용**)**을 역할 이름에 자동으로 적용합니다. 텍스트 문자열을 역할 이름에 수동으로 추가하는 방법으로는 역할을 읽기 전용을 만들 수 없습니다. 동시 세션 제한에 대한 자세한 내용은 전역 사용자 구성의 내용을 참조하십시오.

주의 메뉴 기반 사용자 관리 권한이 있는 사용자는 자신의 권한을 높이거나 관리자 사용자 역할을 포함하여 광범위한 권한으로 새 사용자 계정을 생성할 수 있습니다. 시스템 보안을 위해 사용자 관리 권한이 있는 사용자 목록을 적절하게 제한하는 것이 좋습니다.

프로시저

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

단계 **2** **User Roles(**사용자 역할**)**을 클릭합니다.

단계 **3** 다음 방법 중 하나로 새 사용자 역할을 추가합니다.

- **Create User Role(**사용자 역할 생성**)**을 클릭합니다.
- 복사하려는 사용자 역할 옆에 있는 복사 ( )을 클릭합니다.
- 또 다른 디바이스에서 맞춤형 사용자 역할을 가져옵니다.

  1. 기존 디바이스에서 내보내기( )을 클릭하고 해당 역할을 PC에 저장합니다.
  2. 새 디바이스에서 **System(**시스템**)** > **Tools(**도구**)** > **Import(**가져오기/내보내기**)**를 선택합니다.
  3. **Upload Package(**패키지 업로드**)**를 클릭한 후 지침에 따라 새 디바이스에 저장된 사용자 역할을 가져 옵니다.

단계 **4** 새 사용자 역할의 **Name(**이름**)**을 입력합니다. 사용자 역할 이름은 대/소문자를 구별합니다.

단계 **5** (선택 사항) **Description(**설명**)**을 추가합니다.

단계 **6** 새 역할에 대해 **Menu-Based Permissions(**메뉴 기반 권한**)**를 선택합니다.

권한을 선택하면 모든 하위 항목이 선택되고 다중 값 권한이 첫 번째 값을 사용합니다. 상위 수준 권한의 선택을 취소할 경우 모든 하위 권한의 선택도 취소됩니다. 권한을 선택하지만 권한의 하위 항목은 선택하지 않는 경우, 권한이 기울임꼴 텍스트로 나타납니다.

사전 정의된 사용자 역할을 맞춤형 역할의 기반으로 사용하기 위해 복사하면 사전 정의 역할과 관련된 권한이 미리 선택됩니다.

맞춤형 사용자 역할에 제한적 검색을 적용할 수 있습니다. 이러한 검색은 사용자가 Analysis(분석) 메뉴에서 사용 가능한 페이지의 테이블에서 볼 수 있는 데이터를 제한합니다. 먼저 비공개 저장 검색을 생성하고 해당 메뉴 기반 권한의 **Restrictive Search(**제한된 검색**)** 드롭다운 메뉴에서 이를 선택하는 방법으로 제한적 검색을 구성할 수 있습니다.

단계 **7** (선택 사항) **External Database Access(**외부 데이터 액세스**)** 확인란을 선택하고 새 역할에 대한 데이터베이스 액세스 권한을 설정합니다.

이 옵션은 JDBC SSL 연결을 지원하는 애플리케이션을 사용하여 데이터베이스에 읽기 전용 액세스를 제공합니다. 타사 애플리케이션으로 디바이스를 인증하려면 시스템 설정에서 데이터베이스 액세스를 활성화해야 합니다.

단계 **8** (선택 사항) 새 사용자 역할에 대한 확대 권한을 설정하려면 사용자 역할 확대 활성화, 82 페이지을 참조하십시오.

단계 **9** **Save(**저장**)**를 클릭합니다.

예

액세스 제어 관련 기능을 위한 맞춤형 사용자 역할을 생성해 사용자가 액세스 제어 및 연결된 정책을 보고 수정할 수 있는지 여부를 지정할 수 있습니다.

다음 테이블에는 생성할 수 있는 맞춤형 역할과 각 예에 대해 부여되는 사용자 권한이 나열되어 있습니다. 이 테이블에는 각 맞춤형 역할에 필요한 권한이 나열되어 있습니다. 이 예에서 정책 승인자는 액세스 제어 및 침입 정책을 볼 수 있지만 수정할 수는 없습니다. 정책 승인자는 디바이스에 구성 변경 사항을 구축할 수도 있습니다.

표 *1:* 샘플 액세스 제어 맞춤형 역할

맞춤형 역할 권한	예: 액세스 제어 편집기	예: 침입 및 네트워크 분석 편집기	예: 정책 승인자
액세스 제어	예	아니요	예
액세스 제어 정책	예	아니요	예
액세스 제어 정책 수정	예	아니요	아니요
침입 정책	아니요	예	예
침입 정책 수정	아니요	예	아니요
디바이스에 구성 구축	아니요	아니요	예

사용자 역할 비활성화

어떤 역할을 비활성화하면 해당 역할을 할당 받은 모든 사용자에게서 역할 및 관련 권한이 제거됩니다. 사전 정의 사용자 역할은 삭제할 수 없지만 이를 비활성화할 수는 있습니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 맞춤형 사용자 역할을 표시하며 이러한 역할은 수정할 수 있습니다. 상위 도메인에서 생성된 맞춤형 사용자 역할도 표시되지만, 이러한 역할은 수정할 수 없습니다. 하위 도메인에서 생성된 맞춤형 사용자 역할을 보고 수정하려면 해당 도메인으로 전환하십시오.

프로시저

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

단계 **2** **User Roles(**사용자 역할**)**을 클릭합니다.

단계 **3** 활성화하거나 비활성화할 사용자 역할의 옆에 있는 슬라이더를 클릭합니다.

컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.

어떤 역할의 사용자가 로그인한 상태에서 Lights-Out Management로 해당 역할을 비활성화했다가 다시 활성화할 경우 또는 사용자의 로그인 세션 중에 백업에서 사용자 또는 사용자 역할을 복원할 경우, 사용자가 다시 웹 인터페이스에 로그인해야 IPMItool 명령에 다시 액세스할 수 있습니다.

사용자 역할 확대 활성화

이러한 기본 역할 외에 대상 지정된 다른 사용자 역할의 권한을 임시로 얻을 수 있는 권한과 비밀번호를 맞춤형 사용자 역할에 제공할 수 있습니다. 그러면 부재 시 어떤 사용자를 손쉽게 다른 사용자로 대체하거나 고급 사용자 권한의 사용을 면밀하게 추적하는 것이 가능합니다. 기본 사용자 역할은 에스컬레이션을 지원하지 않습니다.

예를 들어 기반 역할의 권한이 매우 제한적인 사용자가 관리자 역할로 에스컬레이션하여 관리 작업을 수행할 수 있습니다. 사용자가 자신의 비밀번호를 사용하거나 지정된 다른 사용자의 비밀번호를 사용하도록 이 기능을 구성할 수 있습니다. 두 번째 옵션에서는 해당되는 모든 사용자를 대상으로 하나의 확대 비밀번호를 손쉽게 관리할 수 있습니다.

사용자 역할 확대를 구성하려면 다음 워크플로를 참조하십시오.

프로시저

단계 **1** 확대 대상 역할 설정, 82 페이지. 한 번에 하나의 사용자 역할만 확대 대상 역할이 될 수 있습니다.

단계 **2** 확대를 위한 맞춤형 사용자 역할 구성, 83 페이지.

단계 **3** (로그인된 사용자의 경우) 사용자 역할 확대, 84 페이지.

확대 대상 역할 설정

어떤 사전 정의 또는 맞춤형 사용자 역할도 시스템 차원 확대 대상 역할이 되도록 지정할 수 있습니다. 이는 맞춤형 역할이 능력이 된다면 에스컬레이션할 수 있는 역할입니다. 한 번에 하나의 사용자 역할만 확대 대상 역할이 될 수 있습니다. 각 확대는 로그인 세션 동안 지속되며 감사 로그에 기록됩니다.

프로시저

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

단계 **2** **User Roles(**사용자 역할**)**을 클릭합니다.

단계 **3** **Configure Permission Escalation(**권한 확대 구성**)**을 클릭합니다.

단계 **4** **Excalation Target(**확대 대상**)** 드롭다운 목록에서 사용자 역할을 선택합니다.

단계 **5** **OK(**확인**)**를 클릭하여 변경 사항을 저장합니다.

확대 대상 역할의 변경은 즉시 적용됩니다. 확대된 세션의 사용자는 이제 새 확대 대상의 권한을 갖습니다.

확대를 위한 맞춤형 사용자 역할 구성

확대 활성화의 대상이 되는 사용자는 확대가 활성화된 맞춤형 사용자 역할에 속해야 합니다. 이 절차에서는 맞춤형 사용자 역할에 대한 에스컬레이션을 활성화하는 방법을 설명합니다.

맞춤형 역할에 대해 에스컬레이션 비밀번호를 구성할 때 조직의 요구 사항을 고려하십시오. 여러 에스컬레이션 사용자를 손쉽게 관리하길 원할 경우 또 다른 사용자를 선택하여 해당 비밀번호를 확대 비밀번호로 사용하는 방법이 있습니다. 해당 사용자의 비밀번호를 변경하거나 사용자를 비활성화할 경우 해당 비밀번호를 필요로 하는 모든 에스컬레이션 사용자가 영향을 받습니다. 이 작업은 더 효율적으로 사용자 역할 확대를 관리할 수 있습니다. 특히 중앙에서 관리할 수 있는 외부 인증 사용자를 선택할 경우 더욱 그렇습니다.

시작하기 전에

확대 대상 역할 설정, 82 페이지에 따라 대상 사용자 역할을 설정합니다.

프로시저

단계 **1** 맞춤형 사용자 역할 생성, 79 페이지에 설명된 대로 맞춤형 사용자 역할의 구성을 시작합니다.

단계 **2** **System Permissions(**시스템 권한**)**에서 **Set this role to escalate to: Maintenance User(**이 역할을 다음으로 에스컬레이션하도록 설정**:** 유지 보수 사용자**)** 확인란을 선택합니다.

현재 에스컬레이션 대상 목표가 확인란 옆에 나열됩니다.

단계 **3** 이 역할에서 에스컬레이션에 사용할 비밀번호를 선택합니다. 다음 2가지 옵션을 사용할 수 있습니다.

- 이 역할을 갖는 사용자가 확대 시 각자의 비밀번호를 사용하게 하려면 **Authenticate with the assigned user's password(**할당된 사용자의 비밀번호로 인증**)**를 선택합니다.
- 이 역할의 사용자가 다른 사용자의 비밀번호를 사용하게 하려면 **Authenticate with the specified user's password(**지정한 사용자의 비밀번호로 인증**)**를 선택하고 해당 사용자 이름을 입력합니다.

  참고 다른 사용자의 비밀번호로 인증할 경우 어떠한 사용자 이름이라도, 심지어 비활성화되었거나 존재하지 않는 사용자의 이름도 입력할 수 있습니다. 비밀번호가 에스컬레이션에 사용되는 사용자를 비활성화할 경우 해당 비밀번호를 필요로 하는 역할의 사용자는 에스컬레이션이 불가능해집니다. 에스컬레이션을 신속하게 제거해야 하는 경우 이 기능을 사용할 수 있습니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

사용자 역할 확대

사용자가 확대 권한이 있는 맞춤형 사용자 역할이 있는 경우, 해당 사용자는 언제라도 대상 역할의 권한으로 확대할 수 있습니다. 확대는 사용자 환경 설정에 영향을 주지 않습니다.

프로시저

단계 **1** 사용자 이름 하단에 있는 드롭다운 목록에서 **Escalate Permissions(**권한 확대**)**를 선택합니다.

이 옵션이 표시되지 않는다면 관리자가 사용자 역할에 대해 확대를 활성화 하지 않은 것입니다

단계 **2** 인증 비밀번호를 입력합니다.

단계 **3** **Escalate(**확대**)**를 클릭합니다. 이제 현재 역할 외에도 확대 대상 역할의 모든 권한을 갖게 되었습니다.

확대 로그인 세션의 남은 시간 동안 지속됩니다. 다시 기본 역할의 권한만 가지려면 로그아웃했다가 새 세션을 시작해야 합니다.

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'
```

  에를 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.

FMC 사용자 계정 히스토리

기능	버전	세부 사항
SAML 2.0 호환 SSO 제공자를 사용하는 단일 로그인 지원을 추가했습니다.	6.7	타사 SAML 2.0 준수 ID 제공자 (IdP)에 구성된 외부 사용자에 대해 단일 로그인을 지원하는 기능을 추가했습니다. 여기에는 IdP에서 FMC 사용자 역할로 사용자 또는 그룹 역할을 매핑하는 기능이 포함됩니다. 내부 또는 LDAP 또는 RADIUS에 의해 인증된 관리자 역할의 사용자만 SSO를 설정할 수 있습니다. 신규/수정된 화면: 시스템 > 사용자 > **SSO(Single Sign-On)**
사용자 계정의 이름에 대한 새 필드를 추가했습니다.	6.6	내부 사용자 계정을 담당하는 사용자 또는 부서를 식별할 수 있는 필드를 추가했습니다. 신규/수정된 화면: **System(**시스템**)** > **Users(**사용자**)** > **Users(**사용자**)> Real Name(**실제 이름**)** 필드
Cisco Security Manager SSO(Single Sign-On)가 더 이상 지원되지 않음	6.5	FMC와 Cisco Security Manager 간의 SSO(Single Sign-On)는 Firepower 6.5부터 더 이상 지원되지 않습니다. 신규/수정된 화면: **System(**시스템**)** > **Users(**사용자**)CSM SSO(CSM Single Sign-on)**을 선택합니다.
향상된 비밀번호 보안	6.5	이제 새로운 강력한 비밀번호 요구 사항이 장의 단일 위치에 표시되며, 다른 장에서 상호참조됩니다. 수정된 화면 없음 지원되는 플랫폼: FMC