사용자 관리

사용자 계정

사용자 계정을 사용하여 시스템에 액세스합니다. 최대 48개의 로컬 사용자 계정을 구성할 수 있습니다. 각 사용자 계정에는 고유한 사용자 이름 및 비밀번호가 있어야 합니다.

관리자 어카운트

관리자 계정은 기본 사용자 계정이며 수정하거나 삭제할 수 없습니다. 이 어카운트는 시스템 관리자 또는 Superuser 어카운트이며 전체 권한을 가집니다. 관리자 어카운트에 할당된 기본 비밀번호가 없습니다. 초기 시스템 설정을 하는 동안 비밀번호를 선택해야 합니다.

관리자 어카운트는 항상 활성 상태이며 만료되지 않습니다. 관리자 어카운트는 비활성 상태로 구성할 수 없습니다.

로컬 인증 사용자 계정

로컬로 인증된 사용자 계정은 섀시를 통해 직접 인증되며 관리자 또는 AAA 권한을 보유한 사용자에 의해 활성화 또는 비활성화될 수 있습니다. 로컬 사용자 계정이 비활성화되면 사용자가 로그인할 수 없습니다. 비활성화된 로컬 사용자 계정에 대한 구성 세부사항은 데이터베이스에 의해 삭제되지 않습니다. 비활성화된 로컬 사용자 계정을 다시 활성화하면 계정이 기존 구성으로 다시 활성화됩니다. 그러나 계정 비밀번호는 재설정해야 합니다.

원격 인증 사용자 계정

원격으로 인증된 사용자 계정은 LDAP, RADIUS 또는 TACACS+를 통해 인증되는 사용자 계정입니다. 모든 원격 사용자는 초기에 기본적으로 **Read-Only(**읽기 전용**)** 역할이 할당됩니다.

사용자가 로컬 사용자 계정과 원격 사용자 계정을 동시에 유지할 경우 로컬 사용자 계정에 정의된 역할이 원격 사용자 계정의 역할을 재정의합니다.

폴백 인증 방법은 로컬 데이터베이스를 사용하는 것입니다. 이 폴백 방법은 구성할 수 없습니다.

원격 인증 지침, 그리고 원격 인증 공급자의 구성 및 삭제 방법에 대한 자세한 내용은 다음 항목을 참조하십시오.

- 원격 인증에 대한 지침, 4 페이지
- LDAP 제공자 구성
- RADIUS 제공자 구성
- TACACS+ 제공자 구성

사용자 계정 만료

미리 정의된 시간에 만료하도록 사용자 계정을 구성할 수 있습니다. 만료 시간이 되면 사용자 계정은 비활성화됩니다.

기본적으로, 사용자 계정은 만료되지 않습니다.

만료일이 지정된 사용자 계정을 구성한 후에는 이 어카운트가 만료되지 않도록 재구성할 수 없습니다. 단, 최신 만료일이 있는 어카운트를 구성할 수 있습니다.

사용자 이름 지침

사용자 이름은 Firepower Chassis Manager 및 FXOS CLI의 로그인 ID로도 사용됩니다. 사용자 계정에 로그인 ID를 할당할 때 다음 지침 및 제한 사항을 고려합니다.

- 로그인 ID는 1~32자로 구성하며 다음을 포함할 수 있습니다.
  - 알파벳 문자
  - 숫자
  - _(밑줄)

- -(대시)
- . (점)

- 로그인 ID는 고유해야 합니다.
- 로그인 ID는 알파벳 문자로 시작해야 합니다. 숫자 또는 밑줄과 같은 특수 문자로 시작할 수 없습니다.
- 로그인 ID는 대/소문자를 구분합니다.
- 모두 숫자인 로그인 ID를 생성할 수 없습니다.
- 사용자 계정을 생성한 후, 로그인 ID를 변경할 수 없습니다. 사용자 계정을 삭제하고 새로 만들어야 합니다.

비밀번호 지침

로컬에서 인증되는 각 사용자 계정에는 비밀번호가 필요합니다. 관리자 또는 AAA 권한이 있는 사용자는 사용자 비밀번호에 대한 비밀번호 보안 수준을 확인하도록 시스템을 구성할 수 있습니다. 비밀번호 길이 검사를 활성화하면 각 사용자는 강력한 비밀번호를 사용해야 합니다.

각 사용자가 강력한 비밀번호를 사용하는 것이 좋습니다. 로컬로 인증된 사용자를 위해 비밀번호 보안 수준 확인을 활성화한 경우, FXOS에서는 다음 요건을 충족하지 않는 비밀번호를 거부합니다.

- 8자 이상, 127자 이하여야 합니다.

참고 Common Criteria 요구 사항을 준수하기 위해 시스템에서 최소 15자 비밀번호 길이를 선택적으로 구성할 수 있습니다. 자세한 내용은 최소 비밀번호 길이 확인 구성, 14 페이지를 참고하십시오.

- 하나 이상의 알파벳 대문자를 포함해야 합니다.
- 하나 이상의 알파벳 소문자를 포함해야 합니다.
- 하나 이상의 영숫자 외 문자(특수 문자)를 포함해야 합니다.
- 공백을 포함할 수 없습니다.
- aaabbb와 같이 한 문자가 3번 이상 연속적으로 나와서는 안 됩니다.
- 어떤 순서로든 3개의 연속 숫자 또는 문자를 포함해서는 안 됩니다(예: passwordABC 또는 password321).
- 사용자 이름 또는 사용자 이름을 반대로 한 이름과 동일하지 않아야 합니다.
- 비밀번호 딕셔너리 검사를 통과해야 합니다. 예를 들어, 비밀번호는 표준 사전 단어에 기반을 둘 수 없습니다.

- 다음 기호는 포함할 수 없습니다. 예: $(달러 기호), ? (물음표) 및 =(등호)

참고 이 제한 사항은 비밀번호 보안 수준 확인의 활성화 여부를 적용합니다.

- 로컬 사용자 및 관리자 계정 비밀번호는 비어 있지 않아야 합니다.

원격 인증에 대한 지침

지원되는 원격 인증 서비스 중 하나가 시스템에 구성될 경우, Firepower 4100/9300 섀시에서 시스템과 통신할 수 있도록 그 서비스에 대한 제공자를 생성해야 합니다. 다음 지침은 사용자 인증에 영향을 미칩니다.

원격 인증 서비스의 사용자 계정

사용자 계정은 Firepower 4100/9300 섀시의 로컬에 두거나 원격 인증 서버에 둘 수 있습니다.

Firepower Chassis Manager 또는 FXOS CLI에서 원격 인증 서비스로 로그인한 사용자의 임시 세션을 볼 수 있습니다.

원격 인증 서비스의 사용자 역할

원격 인증 서버에 사용자 계정을 생성할 경우 그 계정은 Firepower 4100/9300 섀시에서 작업하는 데 필요한 역할을 포함하고 그 역할의 이름이 FXOS에서 사용되는 이름과 일치해야 합니다. 역할 정책에 따라 사용자가 로그인하지 못하거나 읽기 전용 권한만 가질 수도 있습니다.

원격 인증 제공자의 사용자 특성

RADIUS 및 TACACS+ 구성에서는 사용자가 Firepower Chassis Manager 또는 FXOS CLI에 로그인하는 원격 인증 제공자 각각에서 Firepower 4100/9300 섀시에 대한 사용자 속성을 구성해야 합니다. 이 사용자 특성은 각 사용자에 지정된 역할 및 로캘을 저장합니다.

사용자가 로그인하면 FXOS에서 다음을 수행합니다.

1. 원격 인증 서비스를 쿼리합니다.
2. 사용자를 검증합니다.
3. 사용자가 검증되면 해당 사용자에게 할당된 역할 및 로케일을 확인합니다.

다음 표에서는 FXOS에서 지원하는 원격 인증 제공자의 사용자 특성 요구 사항을 비교합니다.

인증 제공자	맞춤형 속성	스키마 확장	속성 **ID** 요구 사항
LDAP	선택 사항	다음 중 하나를 선택하여 수행할 수 있습니다. • LDAP 스키마를 확장하지 않고 요구 사항에 맞는 기존의 미사용 속성을 구성합니다. • LDAP 스키마를 확장하고 CiscoAVPair와 같은 고유한 이름으로 맞춤형 속성을 생성합니다.	Cisco LDAP 구현에서는 유니코드 형식의 속성이 필요합니다. CiscoAVPair 맞춤형 속성을 생성하려는 경우 속성 ID로 1.3.6.1.4.1.9.287247.1을 사용합니다. 샘플 OID가 다음 섹션에 나와 있습니다.
RADIUS	선택 사항	다음 중 하나를 선택하여 수행할 수 있습니다. • RADIUS 스키마를 확장하지 않고 요구 사항에 맞는 기존의 미사용 속성을 사용합니다. • RADIUS 스키마를 확장하고 cisco-avpair와 같은 고유한 이름으로 맞춤형 속성을 생성합니다.	Cisco RADIUS 구현의 벤더 ID는 009, 속성의 벤더 ID는 001입니다. 다음 구문의 예에서는 cisco-avpair 속성을 생성하려는 경우 여러 사용자 역할 및 로케일을 지정하는 방법을 보여줍니다. `shell:roles="admin,aaa" shell:locales="L1,abc"`. 여러 값을 구분하는 기호로 쉼표 ","를 사용합니다.
TACACS+	필수	스키마를 확장하고 cisco-av-pair라는 이름으로 맞춤형 속성을 생성해야 합니다.	cisco-av-pair 이름은 TACACS+ 제공자에 대한 속성 ID를 제공하는 문자열입니다. 다음 구문의 예에서는 cisco-av-pair 속성을 생성할 경우 여러 사용자 역할 및 로케일을 지정하는 방법을 보여줍니다. `cisco-av-pair=shell:roles="admin aaa" shell:locales*"L1 abc"`. cisco-av-pair 속성 구문에 별표(*)를 사용하면 로케일에 선택 사항 플래그를 지정합니다. 그러면 동일한 권한 부여 프로필을 사용하는 다른 Cisco 디바이스의 인증이 실패하지 않습니다. 여러 값을 구분하는 구분 기호로 공백을 사용합니다.

LDAP 사용자 속성에 대한 샘플 **OID**

다음은 맞춤형 CiscoAVPair 속성에 대한 샘플 OID입니다.

```
CN=CiscoAVPair,CN=Schema,
CN=Configuration,CN=X
objectClass: top
objectClass: attributeSchema
cn: CiscoAVPair
distinguishedName: CN=CiscoAVPair,CN=Schema,CN=Configuration,CN=X
instanceType: 0x4
uSNCreated: 26318654
attributeID: 1.3.6.1.4.1.9.287247.1
attributeSyntax: 2.5.5.12
isSingleValued: TRUE
showInAdvancedViewOnly: TRUE
adminDisplayName: CiscoAVPair
adminDescription: UCS User Authorization Field
oMSyntax: 64
lDAPDisplayName: CiscoAVPair
name: CiscoAVPair
objectCategory: CN=Attribute-Schema,CN=Schema,CN=Configuration,CN=X
```

사용자 역할

시스템에는 다음과 같은 사용자 역할이 포함됩니다.

관리자

전체 시스템에 대한 완전한 읽기 및 쓰기 액세스가 가능합니다. 기본 관리자 계정이 기본적으로 이 역할에 할당되며 변경할 수 없습니다.

읽기 전용

시스템 구성에 대한 읽기 전용 액세스로, 시스템 상태를 수정할 권한이 없습니다.

운영

NTP 구성, Smart Licensing에 대한 Smart Call Home 구성, 시스템 로그(syslog 서버 및 장애 포함)에 대한 읽기 및 쓰기 액세스. 나머지 시스템에 대한 읽기 액세스 권한입니다.

AAA 관리자

사용자, 역할, AAA 구성에 대한 읽기-쓰기 액세스 권한입니다. 나머지 시스템에 대한 읽기 액세스 권한입니다.

로컬 인증 사용자에 대한 비밀번호 프로파일

비밀번호 프로파일에는 모든 로컬로 인증된 사용자에 대한 비밀번호 기록 및 비밀번호 변경 간격 속성이 포함되어 있습니다. 로컬에서 인증된 각 사용자에게는 다른 비밀번호 프로필을 지정할 수 없습니다.

비밀번호 기록 수

비밀번호 기록 수를 사용하면 로컬로 인증된 사용자가 동일한 비밀번호를 계속해서 재사용하는 것을 방지할 수 있습니다. 이 속성을 구성할 때, Firepower 섀시는 로컬로 인증된 사용자가 이전에 사용한 비밀번호를 최대 15개까지 저장합니다. 비밀번호는 최근 항목부터 시간순으로 저장되며, 기록 수 임계값에 도달할 경우 가장 오래된 비밀번호만 재사용될 수 있습니다.

사용자는 비밀번호를 재사용할 수 있기 전에 비밀번호 기록 수에 구성되어 있는 비밀번호 수를 생성하고 사용해야 합니다. 예를 들어, 비밀번호 기록 수를 8로 설정한 경우 로컬로 인증된 사용자는 9번째 비밀번호가 만료될 때까지 첫 번째 비밀번호를 재사용할 수 없습니다.

기본적으로 비밀번호 기록은 0으로 설정되어 있습니다. 이 값이 설정되면 기록 수를 비활성화하고 사용자가 언제든지 이전의 비밀번호를 재사용할 수 있습니다.

필요한 경우, 로컬로 인증된 사용자의 비밀번호 기록 수를 지우고 이전 비밀번호 재사용을 활성화할 수 있습니다.

비밀번호 변경 간격

비밀번호 변경 간격을 사용하면 로컬로 인증된 사용자가 지정된 시간 이내에 변경할 수 있는 비밀번호 변경 횟수를 제한할 수 있습니다. 다음 표는 비밀번호 변경 간격의 구성 옵션 2개를 설명합니다.

간격 구성	설명	예
비밀번호 변경 허용 안 됨	이 옵션을 사용하면 비밀번호 변경 이후 지정된 시간 동안 로컬로 인증된 사용자 비밀번호의 변경이 허용되지 않습니다. 변경 안 함 간격을 1~745시간으로 지정할 수 있습니다. 기본적으로, 변경 안 함 간격은 24시간입니다.	예를 들어, 로컬로 인증된 사용자가 비밀번호를 변경한 후 48시간 이내에 비밀번호가 변경되는 것을 방지하려면 다음을 설정합니다. • 해당 간격 동안 변경을 비활성화로 설정 • 변경 안 함 간격을 48시간으로 설정
변경 간격 내에 비밀번호 변경 허용됨	이 옵션은 로컬로 인증된 사용자가 미리 정의한 간격 동안 비밀번호를 변경할 수 있는 최대 횟수를 지정합니다. 변경 간격을 1~745시간으로 지정하고 비밀번호 변경 최대 횟수를 0~10으로 지정할 수 있습니다. 기본적으로, 로컬로 인증된 사용자는 48시간 동안 비밀번호 변경이 최대 2회 허용됩니다.	예를 들어, 로컬로 인증된 사용자가 비밀번호를 변경한 후 24시간 이내에 비밀번호를 최대 한 번 변경하도록 허용하려면 다음을 설정합니다. • 해당 간격 동안 변경을 활성화로 설정 • 변경 횟수를 1로 설정 • 변경 간격을 24로 설정

사용자 설정 구성

프로시저

단계 **1** **System(**시스템**)** > **User Management(**사용자 관리**)**를 선택합니다.

단계 **2** **Settings(**설정**)** 탭을 클릭합니다.

단계 **3** 다음 필드에 필수 정보를 입력합니다.

참고 **Default Authentication(**기본 인증**)** 및 **Console Authentication(**콘솔 인증**)**이 모두 동일한 원격 인증 프로토콜(RADIUS, TACACS+ 또는 LDAP)을 사용하도록 설정된 경우, 이러한 사용자 설정을 업데이트해야 해당 서버 구성의 특정 측면(예: 해당 서버 삭제 또는 할당 순서 변경)을 변경할 수 있습니다.

이름	설명
Default Authentication(기본 인증**)** 필드	사용자가 원격 로그인 중에 인증되는 기본 방법입니다. 다음 중 하나일 수 있습니다. • 로컬 — 사용자 계정이 섀시에서 로컬로 정의되어야 합니다. • **Radius** — 사용자 계정이 섀시에 지정된 RADIUS 서버에서 정의되어야 합니다. • **TACACS** — 사용자 계정이 섀시에 지정된 TACACS+ 서버에서 정의되어야 합니다. • **LDAP** — 사용자 계정이 섀시에 지정된 LDAP/MS-AD 서버에서 정의되어야 합니다. • **None(**없음**)** — 사용자 계정이 섀시에서 로컬인 경우, 사용자가 원격으로 로그인할 때 비밀번호가 필요하지 않습니다. 참고 모든 **Radius**, **TACACS** 및 **LDAP** 설정은 Platform Settings(플랫폼 설정)에서 구성해야 합니다. 자세한 내용은 플랫폼 설정 장의 AAA 정보를 참조하십시오.

이름	설명
Console Authentication(콘솔 인증**)** 필드	콘솔 포트를 통해 FXOS CLI에 연결될 때 사용자를 인증하는 방식입니다. 다음 중 하나일 수 있습니다. • 로컬 — 사용자 계정이 섀시에서 로컬로 정의되어야 합니다. • **Radius** — 사용자 계정이 섀시에 지정된 RADIUS 서버에서 정의되어야 합니다. • **TACACS** — 사용자 계정이 섀시에 지정된 TACACS+ 서버에서 정의되어야 합니다. • **LDAP** — 사용자 계정이 섀시에 지정된 LDAP/MS-AD 서버에서 정의되어야 합니다. • **None(**없음**)** — 사용자 계정이 섀시에 대해 로컬인 경우, 사용자가 콘솔 포트를 사용하여 FXOS CLI에 연결할 때 비밀번호가 필요하지 않습니다.
원격 사용자 설정	
원격 사용자 역할 정책	사용자가 로그인을 시도하고 원격 인증 제공자가 인증 정보와 함께 사용자 역할을 제공하지 않는 경우, 발생하는 결과를 제어합니다. • **Assign Default Role(**기본 역할 지정**)**—사용자가 읽기 전용 사용자 역할로 로그인할 수 있습니다. • **No-Login(**로그인 안 함**)** — 사용자 이름 및 비밀번호가 올바른 경우에도 사용자가 시스템에 로그인할 수 없습니다.
로컬 사용자 설정	
Password Strength Check(비밀번호 길이 검사**)** 체크 박스	이 옵션을 선택하면 모든 로컬 사용자 비밀번호가 강력한 비밀번호의 지침을 따라야 합니다(비밀번호 지침, 3 페이지 참조). 기본적으로 강력한 비밀번호가 활성화되어 있습니다.
History Count(기록 수**)** 필드	사용자가 이전에 사용한 비밀번호를 재사용하기 전에 생성해야 하는 고유한 비밀번호 수입니다. 기록 수는 최근 항목부터 시간순으로 저장되며, 기록 수 임계값에 도달할 경우 가장 오래된 비밀번호만 재사용될 수 있습니다. 0 ~ 15의 어떤 값이든 가능합니다. **History Count(**기록 수**)** 필드를 0으로 설정하여 기록 수를 비활성화하고 사용자가 언제든지 이전에 사용한 비밀번호를 재사용하게 할 수 있습니다.

이름	설명
Change During Interval(해당 간격 동안 변경**)** 필드	로컬로 인증된 사용자가 비밀번호를 변경할 수 있는 시기를 제어합니다. 가능한 값은 다음과 같습니다. • **Enable(**활성화**)** — 로컬로 인증된 사용자는 변경 간격 및 변경 횟수에 대한 설정을 기초로 비밀번호를 변경할 수 있습니다. • **Disable(**비활성화**)** — 로컬로 인증된 사용자는 변경 안 함 간격 동안 지정된 시간 간격에 비밀번호를 변경할 수 없습니다.
Change Interval(변경 간격**)** 필드	**Change Count(**변경 횟수**)** 필드에 지정된 비밀번호 변경 횟수가 적용되는 시간입니다. 1시간 ~ 745시간의 어떤 값이든 가능합니다. 예를 들어, 이 필드가 48로 설정되고 **Change Count(**변경 횟수**)** 필드가 2로 설정된 경우 로컬로 인증된 사용자는 48시간 이내에 비밀번호를 최대 2번 변경할 수 있습니다.
Change Count(변경 수**)** 필드	로컬로 인증된 사용자가 변경 간격 동안 비밀번호를 변경할 수 있는 최대 횟수입니다. 0 ~ 10의 어떤 값이든 가능합니다.
No Change Interval(변경 안 함 간격**)** 필드	로컬로 인증된 사용자가 새로 생성된 비밀번호를 변경하기 전에 기다려야 하는 최소 시간입니다. 이 값은 1~745시간으로 선택할 수 있습니다. 이 간격은 **Change During Interval(**해당 간격 동안 변경**)** 속성이 **Disable(**비활성화**)**로 설정되지 않은 경우 무시됩니다.
암호문구 만료일 필드	1~9999일 사이의 만료일을 설정합니다. 기본적으로 만료는 비활성화되어 있습니다.
암호문구 만료 경고 기간 필드	로그인할 때마다 사용자에게 비밀번호 만료에 대해 경고할 만료 전 일수를 0~9999 범위에서 설정합니다. 기본값은 14일입니다.
만료 유예 기간 필드	비밀번호 만료 후 사용자가 비밀번호를 변경해야 하는 일수를 0~9999 사이로 설정합니다. 기본값은 3일입니다.
비밀번호 재사용 간격 필드	비밀번호를 재사용할 수 있는 기간(일)을 1~365 범위에서 설정합니다. 기본값은 15일입니다. **History Count(**기록 수**)**와 **Password Reuse Interval(**비밀번호 재사용 간격**)**을 모두 활성화하는 경우 두 요구사항을 모두 충족해야 합니다. 예를 들어 기록 수를 3으로 설정하고 재사용 간격을 10일로 설정한 경우, 10일이 경과하고 비밀번호를 3번 변경해야 비밀번호를 변경할 수 있습니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

세션 시간 초과 구성

FXOS CLI를 사용하여 Firepower 4100/9300 섀시에서 사용자 세션을 종료할 때까지 사용자가 아무런 작업을 수행하지 않는 상태로 경과할 수 있는 시간을 지정할 수 있습니다. 콘솔 세션과 HTTPS, SSH, 텔넷 세션에 대해 각기 다른 설정을 구성할 수 있습니다.

최대 3600초(60분)의 시간 초과 값을 설정할 수 있습니다. 기본값은 600초입니다. 이 설정을 비활성화하려면 세션 시간 초과 값을 0으로 설정합니다.

프로시저

단계 **1** 보안 모드를 입력합니다.

Firepower-chassis #**scope security**

단계 **2** 기본 권한 부여 보안 모드를 입력합니다.

Firepower-chassis /security # **scope default-auth**

단계 **3** HTTPS, SSH 및 텔넷 세션에 대한 유휴 시간 초과를 설정합니다.

Firepower-chassis /security/default-auth # **set session-timeout** 초

단계 **4** (선택 사항) 콘솔 세션에 대한 유휴 시간 초과를 설정합니다.

Firepower-chassis /security/default-auth # **set con-session-timeout** 초

단계 **5** 시스템 구성에 트랜잭션을 커밋합니다.

Firepower-chassis /security/default-auth # **commit-buffer**

단계 **6** (선택 사항) 세션 및 절대 세션 시간 초과 설정을 봅니다.

Firepower-chassis /security/default-auth # **show detail**

예제**:**

```
Default authentication:
 Admin Realm: Local
 Operational Realm: Local
 Web session refresh period(in secs): 600
 Idle Session timeout (in secs) for web, ssh, telnet sessions: 600
 Absolute Session timeout (in secs) for web, ssh, telnet sessions: 3600
 Serial Console Session timeout(in secs): 600
 Serial Console Absolute Session timeout(in secs): 3600
 Admin Authentication server group:
 Operational Authentication server group:
 Use of 2nd factor: No
```

절대 세션 시간 초과 구성

Firepower 4100/9300 섀시에는 세션 사용과 상관없이 절대 세션 시간 초과 기간이 지나면 사용자 세션을 닫는 절대 세션 시간 초과 설정이 있습니다. 이 절대 시간 초과 기능은 시리얼 콘솔, SSH, HTTPS를 비롯한 모든 액세스 형식에서 전역적으로 적용됩니다.

시리얼 콘솔 세션의 절대 세션 시간 초과를 별도로 구성할 수 있습니다. 이렇게 하면 다른 형식의 액세스에 대한 시간 초과를 유지하면서 디버깅 요구에 대한 시리얼 콘솔 절대 세션 시간 초과를 비활성화할 수 있습니다.

절대 시간 초과 기본값은 3600초(60분)이며 FXOS CLI를 사용해 변경할 수 있습니다. 이 설정을 비활성화하려면 절대 세션 시간 초과 값을 0으로 설정합니다.

프로시저

단계 **1** 보안 모드를 입력합니다.

Firepower-chassis #**scope security**

단계 **2** 기본 권한 부여 보안 모드를 입력합니다.

Firepower-chassis /security # **scope default-auth**

단계 **3** 절대 세션 시간 초과를 설정합니다.

Firepower-chassis /security/default-auth # **set absolute-session-timeout** 초

단계 **4** (선택 사항) 별도의 콘솔 절대 세션 시간 초과를 설정합니다.

Firepower-chassis /security/default-auth # **set con-absolute-session-timeout** 초

단계 **5** 시스템 구성에 트랜잭션을 커밋합니다.

Firepower-chassis /security/default-auth # **commit-buffer**

단계 **6** (선택 사항) 세션 및 절대 세션 시간 초과 설정을 봅니다.

Firepower-chassis /security/default-auth # **show detail**

예제:

```
Default authentication:
 Admin Realm: Local
 Operational Realm: Local
 Web session refresh period(in secs): 600
 Idle Session timeout (in secs) for web, ssh, telnet sessions: 600
 Absolute Session timeout (in secs) for web, ssh, telnet sessions: 3600
 Serial Console Session timeout(in secs): 600
 Serial Console Absolute Session timeout(in secs): 3600
 Admin Authentication server group:
 Operational Authentication server group:
 Use of 2nd factor: No
```

최대 로그인 시도 횟수 설정

허용된 최대 횟수만큼 로그인 시도에 실패하면 지정된 시간 동안 사용자가 잠기도록 Firepower 4100/9300 섀시를 구성할 수 있습니다. 설정된 로그인 최대 시도 횟수를 초과하면 사용자가 시스템에서 잠깁니다. 사용자가 잠겼음을 나타내는 알림이 표시되지 않습니다. 이 경우 사용자는 다시 로그인을 시도하려면 지정된 시간 동안 기다려야 합니다.

최대 로그인 시도 횟수를 구성하려면 다음 단계를 수행하십시오.

참고

- 최대 로그인 시도 횟수를 초과하면 모든 유형의 사용자 계정(관리자 포함)이 시스템에서 잠깁니다.
- 기본 최대 로그인 시도 실패 횟수는 0입니다. 최대 로그인 시도 횟수를 초과한 후 사용자가 시스템에서 잠기는 기본 시간은 30분(1800초)입니다.
- 사용자의 잠금 상태를 보고 이를 지우기 위한 단계는 사용자 잠금 상태 보기 및 지우기, 14 페이지 섹션을 참조하십시오.

이 옵션은 시스템에서 Common Criteria 인증 컴플라이언스를 얻기 위해 제공되는 숫자 중 하나입니다. 자세한 내용은 보안 인증서 컴플라이언스를 참고하십시오.

프로시저

단계 **1** FXOS CLI에서 보안 모드로 들어갑니다.

scope security

단계 **2** 최대 로그인 시도 실패 횟수를 설정합니다.

set max-login-attempts *num_attempts*

num_attempts 값은 0~10의 정수입니다.

단계 **3** 최대 로그인 시도 횟수에 도달한 후 사용자가 시스템에서 잠긴 상태로 유지되는 시간(초)을 지정합니다.

set user-account-unlock-time

unlock_time

단계 **4** 구성을 커밋합니다.

commit-buffer

사용자 잠금 상태 보기 및 지우기

관리자는 Maximum Number of Login Attempts(최대 로그인 시도 횟수) CLI 설정에 지정된 최대 로그인 시도 실패 횟수를 초과한 후 Firepower 4100/9300 섀시에서 잠긴 사용자의 잠금 상태를 확인하고 해제할 수 있습니다. 자세한 내용은 최대 로그인 시도 횟수 설정, 13 페이지을 참고하십시오.

프로시저

단계 **1** FXOS CLI에서 보안 모드로 들어갑니다.

scope security

단계 **2** 해당 사용자의 사용자 정보(잠금 상태 포함)를 표시합니다.

Firepower-chassis /security # **show local-user** *user* **detail**

예제**:**

```
Local User(□□ □□□) □□□:
 □□:
 □:
 □□□:
 □□:
 □□: □□□□ □□
Password:
 □□□ □□ □□: □□
 □□□□ □□: □□
 □□□ □□:
 □□: □□ □□
 □□□ SSH □□ □:
```

단계 **3** (선택 사항) 사용자의 잠금 상태를 지웁니다.

Firepower-chassis /security # **scope local-user** *user*

Firepower-chassis /security/local-user # **clear lock-status**

최소 비밀번호 길이 확인 구성

최소 비밀번호 길이 확인을 활성화하는 경우 지정된 최소 문자 수의 비밀번호를 만들어야 합니다. 예를 들어 *min_length* 옵션이 15로 설정된 경우 15자 이상을 사용해 비밀번호를 만들어야 합니다. 이 옵션은 시스템에서 Common Criteria 인증 컴플라이언스를 허용하는 숫자 중 하나입니다. 더 자세한 내용은 Security Certifications Compliance(보안 인증 컴플라이언스)의 내용을 참조하십시오.

최소 비밀번호 길이 확인을 구성하려면 다음 단계를 수행하십시오.

프로시저

단계 **1** FXOS CLI에서 보안 모드로 들어갑니다.

scope security

단계 **2** 최소 비밀번호 길이를 지정합니다.

set min-password-length *min_length*

단계 **3** 구성을 커밋합니다.

commit-buffer

로컬 사용자 계정 생성

프로시저

단계 **1** **System(**시스템**)** > **User Management(**사용자 관리**)**를 선택합니다.

단계 **2** **Local Users(**로컬 사용자**)** 탭을 클릭합니다.

단계 **3** **Add User(**사용자 추가**)**를 클릭하여 **Add User(**사용자 추가**)** 대화 상자를 엽니다.

단계 **4** 사용자에 대한 필수 정보로 다음 필드를 완성합니다.

이름	설명
User Name(사용자 이름**)** 필드	계정 로그인에 사용하는 계정 이름. 이름은 고유해야 하며 사용자 계정 이름에 대한 지침 및 제한 사항을 따라야 합니다(사용자 이름 지침, 2 페이지 참조). 사용자를 저장하면 로그인 ID는 변경할 수 없습니다. 사용자 계정을 삭제하고 새로 만들어야 합니다.
First Name(이름**)** 필드	사용자의 이름입니다. 최대 32자입니다.
Last Name(성**)** 필드	사용자의 성입니다. 최대 32자입니다.
Email(이메일**)** 필드	사용자의 이메일 주소입니다.
Phone Number(전화번호**)** 필드	사용자의 전화 번호.

이름	설명
Password(비밀번호**)** 필드	이 계정의 비밀번호. 비밀번호 보안 수준 확인을 활성화하면 사용자의 비밀번호가 더욱 강력해지며, 보안 수준 확인 요건을 충족하지 않는 비밀번호를 FXOS에서 거부합니다(비밀번호 지침, 3 페이지 참조). 참고 비밀번호는 다음 기호는 포함할 수 없습니다. 예: $(달러 기호), ? (물음표) 및 =(등호) 이 제한 사항은 비밀번호 보안 수준 확인의 활성화 여부를 적용합니다.
Confirm Password(비밀번호 확인**)** 필드	확인을 위해 두 번째로 입력하는 비밀번호.
Account Status(계정 상태**)** 필드	상태가 **Active(**활성**)**로 설정된 경우, 사용자는 이 로그인 ID와 비밀번호를 사용하여 Firepower Chassis Manager 및 FXOS CLI에 로그인할 수 있습니다.
User Role(사용자 역할**)** 목록	사용자 계정에 할당할 수 있는 권한에 해당하는 역할입니다(사용자 역할, 6 페이지 참조). 모든 사용자에게 기본적으로 읽기 전용 역할이 할당되며 이 역할은 선택 취소할 수 없습니다. 여러 역할을 할당하려면 **Ctrl** 키를 누른 상태에서 원하는 역할을 클릭합니다. 참고 사용자 역할을 삭제하면 사용자의 현재 세션 ID가 취소됩니다. 즉, 사용자의 모든 활성 세션(CLI 및 웹)이 즉시 종료됩니다.
Account Expires(어카운트 만료**)** 체크 박스	이 체크 박스를 선택한 경우, 해당 계정은 만료되며 **Expiration Date(**만료일**)** 필드에 지정된 날짜 이후에 사용할 수 없습니다. 참고 만료일이 지정된 사용자 계정을 구성한 후에는 이 어카운트가 만료되지 않도록 재구성할 수 없습니다. 단, 최신 만료일이 있는 어카운트를 구성할 수 있습니다.
Expiry Date(만료일**)** 필드	계정이 만료되는 날. 날짜는 yyyy-mm-dd 형식이어야 합니다. 만료일을 선택하기 위해 달력을 보려면 이 필드의 마지막에 있는 달력 아이콘을 클릭합니다.

단계 **5** **Add(**추가**)**를 클릭합니다.

로컬 사용자 계정 삭제

프로시저

단계 **1** **System(**시스템**)** > **User Management(**사용자 관리**)**를 선택합니다.

단계 **2** **Local Users(**로컬 사용자**)** 탭을 클릭합니다.

단계 **3** 삭제하려는 사용자 계정 행에서 **Delete(**삭제**)**를 클릭합니다.

단계 **4** **Confirm(**확인**)** 대화 상자에서 **Yes(**예**)**를 클릭합니다.

로컬 사용자 계정 활성화 또는 비활성화

로컬 사용자 계정을 활성화하거나 비활성화하려면 사용자에게 관리자 또는 AAA 권한이 있어야 합니다.

프로시저

단계 **1** **System(**시스템**)** > **User Management(**사용자 관리**)**를 선택합니다.

단계 **2** **Local Users(**로컬 사용자**)** 탭을 클릭합니다.

단계 **3** 활성화 또는 비활성화하려는 사용자 계정 행에서 **Edit(**편집**)(**연필 모양 아이콘**))**을 클릭합니다.

단계 **4** **Edit User(**사용자 편집**)** 대화 상자에서 다음 중 하나를 수행합니다.

- 사용자 계정을 활성화하려면 **Account Status(**어카운트 상태**)** 필드에서 **Active(**활성**)** 라디오 버튼을 클릭합니다. 사용자 어카운트를 재활성화할 때 어카운트 비밀번호를 재설정해야 합니다.
- 사용자 계정을 비활성화하려면 **Account Status(**어카운트 상태**)** 필드에서 **Inactive(**비활성**)** 라디오 버튼을 클릭합니다.

관리자 사용자 계정은 항상 활성 상태로 설정됩니다. 수정할 수 없습니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

단계 **6** 시스템 구성에 트랜잭션을 커밋합니다.

Firepower-chassis /security/local-user # **commit-buffer**

로컬로 인증된 사용자의 비밀번호 기록 지우기

프로시저

단계 **1** 보안 모드를 입력합니다.

Firepower-chassis #**scope security**

단계 **2** 지정된 사용자 계정에 대한 로컬 사용자 보안 모드를 입력합니다.

Firepower-chassis /security # **scope local-user** *user-name*

단계 **3** 지정된 사용자 계정에 대한 비밀번호 기록을 지웁니다.

Firepower-chassis /security/local-user # **clear password-history**

단계 **4** 시스템 구성에 트랜잭션을 커밋합니다.

Firepower-chassis /security/local-user # **commit-buffer**

예

다음 예에서는 비밀번호 기록을 지우고 트랜잭션을 커밋합니다.

```
Firepower-chassis # scope security
Firepower-chassis /security # scope local-user admin
Firepower-chassis /security/local-user # clear password-history
Firepower-chassis /security/local-user* # commit-buffer
Firepower-chassis /security/local-user #
```