Management Center에 로그인

다음 주제에서는 Firepower System에 로그인 하는 방법을 설명합니다.

Firepower System 사용자 어카운트

사용자 이름과 비밀번호를 제공해야 웹 인터페이스나 management center 또는 매니지드 디바이스의 CLI에 액세스할 수 있습니다. 매니지드 디바이스에서, 구성 레벨 액세스 권한이 있는 CLI 사용자는 `expert` 명령을 이용해 Linux 셸에 액세스할 수 있습니다. management center에서는 모든 CLI 사용자가 `expert` 명령을 사용할 수 있습니다. management center 및 FTD를 외부 인증을 사용하도록 구성하면 사용자 자격 증명을 외부 LDAP 또는 RADIUS 서버에 저장합니다. CLI 액세스 권한을 취소하거나 외부 사용자에게 제공할 수 있습니다.management center는 인증 및 권한 부여를 위해 SAML(Security Assertion Markup Language) 2.0 개방형 표준을 준수하는 SSO 제공자를 사용하여 SSO(Single Sign-On)를 지원하도록 구성할 수 있습니다.

management center CLI는 모든 명령에 액세스할 수 있는 단일 관리자 사용자를 제공합니다. management center 웹 인터페이스 사용자가 액세스할 수 있는 기능은 관리자가 사용자 계정에 부여하는 권한에 의해 제어됩니다. 매니지드 디바이스의 경우 사용자가 CLI 및 웹 인터페이스에서 액세스할 수 있는 기능은 사용자 계정에 부여된 권한과 관리자에 의해 제어됩니다.

참고 시스템은 사용자 어카운트를 기반으로 사용자 활동을 감사합니다. 따라서 사용자들이 올바른 어카운트로 시스템에 로그인하도록 해야 합니다.

주의 모든 management center CLI 사용자 및 (매니지드 디바이스의 경우) 구성 레벨 CLI 액세스 권한이 있는 사용자는 Linux 셸에서 루트 권한을 얻을 수 있으며, 따라서 보안 위험이 발생할 수 있습니다. 시스템 보안을 위해 다음을 적극 권장합니다.

- 외부 인증을 설정하는 경우 CLI 액세스 권한이 있는 사용자 목록을 적절하게 제한해야 합니다.
- 매니지드 디바이스에 CLI 액세스 권한을 부여할 때는, 구성 레벨 CLI 액세스로 내부 사용자 목록을 제한합니다.
- Linux 셸 사용자는 설정해선 안 됩니다. 사전 정의된 관리자 사용자 및 CLI에서 관리자 사용자가 생성한 사용자만 사용해야 합니다.

주의 Cisco TAC가 지시하거나 Firepower 사용자 설명서에서 명시적으로 지시하지 않는 한, Linux 셸은 사용하지 않는 것이 좋습니다.

다양한 어플라이언스가 각기 다른 기능으로 서로 다른 유형의 사용자 어카운트를 지원합니다.

Secure Firewall Management Centers

Secure Firewall Management Center다음 같은 사용자 어카운트를 지원합니다.

- 웹 인터페이스 액세스를 위한 사전 정의된 관리자 어카운트. 관리자 역할이 주어지며 웹 인터페이스를 통해 관리할 수 있습니다.
- 맞춤형 사용자 계정으로, 웹 인터페이스 액세스를 제공하며 관리자 사용자와 관리자 권한이 있는 사용자가 생성하고 관리할 수 있습니다.
- CLI 액세스를 위한 사전 정의된 관리자 계정입니다. 이 계정으로 로그인하는 사용자는 `expert` 명령을 사용해 Linux 셸 액세스 권한을 얻을 수 있습니다.

  초기 구성에서 CLI 관리자 계정과 웹 인터페이스 관리자 계정의 비밀번호가 동기화되지만, 원한다면 이후 두 관리자 계정에 별도의 비밀번호를 설정할 수 있습니다.

주의 시스템 보안을 위해 Cisco에서는 Linux 셸 사용자를 어플라이언스에서 추가로 설정하지 않도록 권장합니다.

Secure Firewall Threat Defense및 Secure Firewall Threat Defense Virtual 디바이스

Secure Firewall Threat Defense및 Secure Firewall Threat Defense Virtual 디바이스는 다음 사용자 어카운트 유형을 지원합니다.

- 사전 정의된 관리자 어카운트. 모든 형태의 디바이스 액세스에 사용될 수 있습니다.
- 맞춤형 사용자 어카운트. 관리자 사용자 및 Config(구성) 액세스 권한이 있는 사용자가 생성하고 관리할 수 있습니다.

Secure Firewall Threat Defense는 SSH 사용자에 대한 외부 인증을 지원합니다.

Firepower System 유저 인터페이스

어플라이언스 유형에 따라 웹 기반 GUI, 보조 CLI 또는 Linux 셸을 사용하여 Firepower 어플라이언스와 상호작용할 수 있습니다. Secure Firewall Management Center 구축에서는 management center GUI로 대부분의 구성 작업을 수행합니다. 소수의 작업에서만 CLI나 Linux 셸을 이용해 어플라이언스에 바로 액세스해야 합니다. Cisco TAC가 지시하거나 Firepower 사용자 설명서에서 명시적으로 지시하지 않는 한, Linux 셸 사용은 권장하지 않습니다.

브라우저 요구 사항에 대한 내용은 Firepower 릴리스 노트를 참조하십시오.

참고 어플라이언스에 상관없이 사용자가 SSH를 통한 CLI 로그인에 3회 연속 실패하면, 시스템이 SSH 연결을 종료합니다.

어플라이언스	웹 기반 **GUI**	보조 **CLI**	**Linux** 셸
Secure Firewall Management Center	• 사전 정의된 관리자 사용자 및 맞춤형 사용자 계정에서 지원됩니다. • 운영, 관리 및 분석 작업에 사용할 수 있습니다.	• 사전 정의된 관리자 사용자 및 맞춤형 외부 사용자 계정에서 지원됩니다. • SSH, 직렬 또는 키보드 및 모니터 연결을 사용하여 액세스할 수 있습니다. • Cisco TAC가 지시한 관리 및 문제해결 목적으로만 사용해야 합니다.	• 사전 정의된 관리자 사용자에 대해 지원됩니다. • Secure Firewall Management Center CLI에서 `expert` 명령을 통해 액세스해야 합니다. • SSH, 직렬 또는 키보드 및 모니터 연결을 사용하여 액세스할 수 있습니다. • Cisco TAC가 지시하거나 management center 설명서에서 명시적으로 지시한 관리 및 문제해결 목적으로만 사용해야 합니다.

어플라이언스	웹 기반 **GUI**	보조 **CLI**	**Linux** 셸
Secure Firewall Threat Defense Secure Firewall Threat Defense Virtual	—	• 사전 정의된 관리자 사용자 및 맞춤형 사용자 계정에서 지원됩니다. • SSH, 직렬 또는 키보드 및 모니터 연결을 사용하여 물리적 디바이스에 액세스할 수 있습니다. SSH 또는 VM 콘솔을 통해 가상 디바이스에 액세스할 수 있습니다. • Cisco TAC가 지시한 설정 및 문제해결 목적으로만 사용해야 합니다.	• 사전 정의된 관리자 사용자 및 맞춤형 사용자 계정에서 지원됩니다. • 구성 액세스 권한이 있는 CLI 사용자가 `expert` 명령으로 액세스할 수 있습니다. • Cisco TAC가 지시하거나 management center 설명서에서 명시적으로 지시한 관리 및 문제해결 목적으로만 사용해야 합니다.

관련 항목

내부 사용자 추가

웹 인터페이스 고려 사항

- 조직에서 인증에 CAC(Common Access Cards)를 사용한다면, LDAP로 인증한 외부 사용자는 CAC 자격 증명을 사용하여 어플라이언스의 웹 인터페이스에 대한 액세스를 얻을 수 있습니다.
- 기본 홈페이지 상단에 나열되는 메뉴 및 메뉴 옵션은 사용자 어카운트에 대한 권한을 기반으로 합니다. 그러나 기본 홈 페이지에 대한 링크에는 사용자 어카운트 권한 전반을 포괄하는 옵션이 포함되어 있습니다. 사용자 어카운트에 부여된 권한과 다른 권한을 필요로 하는 링크를 클릭하는 경우, 시스템 경고 메시지가 나타나고 활동을 기록합니다.
- 상당한 시간이 걸리는 프로세스의 경우 웹 브라우저에 스크립트가 응답하지 않는다는 메시지가 표시될 수 있습니다. 이러한 경우 완료될 때까지 스크립트가 계속 진행되도록 해야 합니다.

관련 항목

홈 페이지 지정

세션 시간 초과

세션 시간 초과에서 제외되도록 달리 구성하지 않는 한, 기본적으로 1시간 동안 활동이 없으면 시스템에서 자동으로 로그아웃됩니다.

참고 SSO 사용자의 경우 management center 세션이 시간 초과되면 디스플레이가 IdP 인터페이스로 잠시 리디렉션된 다음 management center로그인 페이지로 리디렉션됩니다. SSO 세션이 다른 곳에서 종료되지 않는 한 누구나 로그인 페이지에서 **Single Sign-On(**단일 로그인**)** 링크를 클릭하여 로그인 자격 증명을 제공하지 않고 management center에 액세스 할 수 있습니다. management center보안을 유지하고 다른 사용자가 SSO 계정을 사용하여 management center에 액세스하는 것을 방지하려면 management center 로그인 세션을 무인 상태로 두지 말고 management center에서 로그아웃할 때 IdP의 SSO 페더레이션에서 로그아웃하는 것이 좋습니다.

Administor(관리자) 역할이 부여된 사용자는 다음 설정을 통해 어플라이언스에 대한 세션 시간 초과 간격을 변경할 수 있습니다.

System(시스템**)** > **Configuration(**구성**)** > **Shell Timeout(**셸 시간 초과**)**

관련 항목

세션 시간 제한 구성

SAML SSO(Single Sign-On) 구성

Secure Firewall Management Center 웹 인터페이스 로그인

참고 이 작업은 LDAP 또는 RADIUS 서버로 인증된 내부 사용자 및 외부 사용자에게 적용됩니다. SSO 로그인에 대해서는 SSO를 사용한 FMC 웹 인터페이스 로그인, 6 페이지의 내용을 참조하십시오.

사용자는 단일 활성 세션으로 제한됩니다. 이미 활성 세션이 있는 사용자 어카운트로 로그인하려고 할 경우 다른 세션을 종료하거나 다른 사용자로 로그인하라는 프롬프트가 나타납니다.

여러 management center이(가) 동일한 IP 주소를 공유하는 NAT 환경의 경우:

- 각 management center은(는) 한 번에 하나의 로그인 세션만 지원합니다.
- 다른 management center에 액세스하려면 로그인할 때마다 (Firefox나 Chrome 같은) 다른 브라우저를 사용하거나, 브라우저를 시크릿 모드 또는 사생활 보호 모드로 설정해야 합니다.

시작하기 전에

- 웹 인터페이스에 액세스할 수 없는 경우 시스템 관리자에게 연락하여 어카운트 권한을 수정해 달라고 하거나, 관리자 액세스 권한이 있는 사용자로 로그인하여 어카운트에 대한 권한을 수정하십시오.
- 내부 사용자 추가에 설명된 대로 사용자 어카운트를 생성합니다.

프로시저

단계 **1** 브라우저에서 **https://***ipaddress_or_hostname/*으로 이동합니다. 여기서 *ipaddress* 또는 *hostname*은 management center와(과) 일치합니다.

단계 **2** **Username(**사용자 이름**)** 및 **Password(**비밀번호**)** 필드에 사용자 이름과 비밀번호를 입력합니다. 다음 지침에 유의하십시오.

- 사용자 이름은 대/소문자를 구분하지 않습니다.
- 다중 도메인 구축에서 사용자 이름 앞에 사용자 어카운트가 생성된 도메인을 추가합니다. 모든 상위 도메인을 앞에 추가할 필요는 없습니다. 예를 들어 사용자 어카운트가 SubdomainB에서 생성되고 상위 도메인이 DomainA인 경우, 사용자 이름을 다음 형식에 입력합니다.

  ```
  SubdomainB\username
  ```

- 조직에서 로그인할 때 SecurID® 토큰을 사용하는 경우, 토큰을 사용자의 SecurID PIN에 추가하고 로그인 시 비밀번호로 사용하십시오. 예를 들어, PIN이 `1111`이고 SecurID 토큰이 `222222`인 경우 `1111222222`를 입력하십시오. SecurID PIN을 먼저 생성해야 시스템에 로그인할 수 있습니다.

단계 **3** **Login(**로그인**)**을 클릭합니다.

관련 항목

세션 시간 초과, 4 페이지

SSO를 사용한 FMC 웹 인터페이스 로그인

management center는 SAML(Security Assertion Markup Language) 2.0 개방형 표준을 준수하는 SSO 제공자로 구현된 SSO(Single-Sign On) 페더레이션에 참여하도록 구성할 수 있습니다. SSO 사용자 계정은 IdP(Identityy Provider)에서 설정해야 하며 계정 이름으로 이메일 주소를 사용해야 합니다. 사용자 이름이 이메일 주소가 아니거나 SSO 로그인이 실패하면 시스템 관리자에게 문의하십시오.

참고 management center는 SSO 계정에 대한 CAC 자격 증명을 사용한 로그인을 지원하지 않습니다.

사용자는 단일 활성 세션으로 제한됩니다. 이미 활성 세션이 있는 사용자 어카운트로 로그인하려고 할 경우 다른 세션을 종료하거나 다른 사용자로 로그인하라는 프롬프트가 나타납니다.

여러 management center이(가) 동일한 IP 주소를 공유하는 NAT 환경의 경우:

- 각 management center은(는) 한 번에 하나의 로그인 세션만 지원합니다.
- 다른 management center에 액세스하려면 로그인할 때마다 (Firefox나 Chrome 같은) 다른 브라우저를 사용하거나, 브라우저를 시크릿 모드 또는 사생활 보호 모드로 설정해야 합니다.

시작하기 전에

- SSO 액세스를 위해 management center를 구성합니다. SAML SSO(Single Sign-On) 구성의 내용을 참조하십시오.
- 웹 인터페이스에 액세스할 수 없는 경우 시스템 관리자에게 문의하여 SSO IdP에서 계정을 구성하십시오.

프로시저

단계 **1** 브라우저에서 **https://***ipaddress_or_hostname/*으로 이동합니다. 여기서 *ipaddress* 또는 *hostname*은 management center와(과) 일치합니다.

참고 SSO 사용자는 SSO 액세스를 위해 특별히 구성된 로그인 URL을 사용하여 management center에 지속적으로 액세스해야 합니다. 관리자에게 문의하십시오.

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

단계 **3** 시스템은 다음 두 가지 방법 중 하나로 응답합니다.

- SSO 페더레이션에 이미 로그인한 경우 management center 기본 홈 페이지가 나타납니다.
- SSO 페더레이션에 아직 로그인하지 않은 경우에는 management center가 브라우저를 IdP의 로그인 페이지로 리디렉션합니다. IdP에서 로그인 프로세스를 완료하면 management center 기본 홈 페이지가 나타납니다.

관련 항목

세션 시간 초과, 4 페이지
SAML SSO(Single Sign-On) 구성

CAC 인증서로 Secure Firewall Management Center에 로그인

사용자는 단일 활성 세션으로 제한됩니다. 이미 활성 세션이 있는 사용자 어카운트로 로그인하려고 할 경우 다른 세션을 종료하거나 다른 사용자로 로그인하라는 프롬프트가 나타납니다.

여러 management center이(가) 동일한 IP 주소를 공유하는 NAT 환경의 경우:

- 각 management center은(는) 한 번에 하나의 로그인 세션만 지원합니다.
- 다른 management center에 액세스하려면 로그인할 때마다 (Firefox나 Chrome 같은) 다른 브라우저를 사용하거나, 브라우저를 시크릿 모드 또는 사생활 보호 모드로 설정해야 합니다.

⚠

주의 활성 브라우징 세션 중에는 CAC를 제거하지 마십시오. 세션 중에 CAC를 제거하거나 대체할 경우 웹 브라우저는 세션을 종료하며 웹 인터페이스에서 로그아웃됩니다.

시작하기 전에

- 웹 인터페이스에 액세스할 수 없는 경우 시스템 관리자에게 연락하여 어카운트 권한을 수정해 달라고 하거나, 관리자 액세스 권한이 있는 사용자로 로그인하여 어카운트에 대한 권한을 수정하십시오.
- 내부 사용자 추가에 설명된 대로 사용자 어카운트를 생성합니다.
- LADP로 CAC(Common Access Card) 인증 구성에 설명된 대로 CAC 인증 및 권한 부여를 구성합니다.

프로시저

단계 **1** 조직에서 안내하는 대로 CAC를 삽입합니다.

단계 **2** 브라우저에서 **https://***ipaddress_or_hostname/*으로 이동합니다. 여기서 *ipaddress* 또는 *hostname*은 management center와(과) 일치합니다.

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

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

단계 **5** **Continue(**계속**)**를 클릭합니다.

관련 항목

LADP로 CAC(Common Access Card) 인증 구성
세션 시간 초과, 4 페이지
Management Center에 대한 SSO 지침

Management Center Command Line Interface에 로그인

관리자 CLI 사용자와 특정 사용자 지정 외부 사용자는 management center CLI에 로그인할 수 있습니다.

주의 Cisco TAC가 지시하거나 management center 설명서에서 명시적으로 지시하지 않는 한, Linux 셸은 사용하지 않는 것이 좋습니다.

참고 어플라이언스에 상관없이 사용자가 SSH를 통한 CLI 로그인에 3회 연속 실패하면 시스템이 SSH 연결을 종료합니다.

시작하기 전에

관리자 사용자로 초기 구성 프로세스를 완료합니다. 최초 로그인의 내용을 참조하십시오.

프로시저

단계 **1** 관리자 사용자 이름과 비밀번호를 사용하여, SSH 또는 콘솔 포트를 통해 management center에 연결합니다.

조직에서 로그인할 때 SecurID® 토큰을 사용하는 경우, 토큰을 사용자의 SecurID PIN에 추가하고 로그인 시 비밀번호로 사용하십시오. 예를 들어, PIN이 `1111`이고 SecurID 토큰이 `222222`인 경우 `1111222222`를 입력하십시오. 로그인하기 전에 SecurID PIN을 생성해야 합니다.

단계 **2** 사용 가능한 CLI 명령을 사용합니다.

마지막 로그인 보기

권한이 없는 사용자가 여러분의 자격 증명을 이용해 Secure Firewall Management Center에 로그인할 것 같다면, 마지막으로 자격 증명을 이용해 로그인한 날짜, 시간, IP 주소를 확인하십시오.

시작하기 전에

이 기능은 클래식 테마를 사용할 때만 지원됩니다. 사용자 환경 설정에서 이 UI 테마를 선택할 수 있습니다.

프로시저

단계 **1** Secure Firewall Management Center에 로그인합니다.

단계 **2** 브라우저 창의 오른쪽 상단에서 로그인하는 데 사용한 사용자 ID를 찾습니다.

단계 **3** 자신의 사용자 이름을 클릭합니다.

단계 **4** 이전 로그인 관련 정보가 메뉴 하단에 표시됩니다.

Firepower System 웹 인터페이스에서 로그아웃

Firepower System 웹 인터페이스를 더 이상 활발하게 사용하지 않는 경우, Cisco에서는 로그아웃할 것을 권장합니다. 잠시 웹 브라우저에서 떨어져 있는 경우에도 마찬가지입니다. 로그아웃하면 웹 세션이 종료되며, 내 크리덴셜로 타인이 어플라이언스를 사용할 수 없도록 합니다.

참고 management center에서 SSO 세션에서 로그 아웃하는 경우 시스템에서 로그 아웃하면 브라우저가 조직의 SSO IdP로 리디렉션됩니다. management center 보안을 유지하고 다른 사용자가 SSO 계정을 사용하여 management center에 액세스하는 것을 방지하려면 IdP의 SSO 페더레이션에서 로그 아웃하는 것이 좋습니다.

프로시저

단계 **1** 사용자 이름 하단에 있는 드롭다운 목록에서 **Logout(**로그아웃**)**를 선택합니다.

단계 **2** management center의 SSO 세션에서 로그 아웃하는 경우 시스템이 조직의 SSO IdP로 리디렉션합니다. management center 보안을 위해 IdP에서 로그 아웃합니다.

관련 항목

세션 시간 초과, 4 페이지

Firepower 시스템 로그인 기록

기능	버전	세부 사항
SAML 2.0 준수 SSO 제공자를 사용하는 SSO(Single Sign-On) 지원을 추가했습니다.	6.7	타사 SAML 2.0 준수 ID 제공자(IdP)에서 설정된 사용자가 로그인 페이지에서 새로운 **SSO(Single Sign-On)** 링크를 사용하여 management center에 로그인하는 기능을 추가했습니다. 신규/수정된 화면: 로그인 화면
다음에 대한 마지막 로그인 정보 확인 Secure Firewall Management Center	6.5	마지막으로 로그인한 날짜, 시간 및 IP 주소를 확인합니다. 신규/수정된 메뉴: 창의 오른쪽 상단에 있는 메뉴로, 로그인하는 데 사용한 사용자 이름을 표시합니다. 지원되는 플랫폼: management center
다음에 대한 자동 CLI 액세스 management center	6.5	SSH를 이용해 management center에 로그인하면, CLI에 자동으로 액세스하게 됩니다. 권장 사항은 아니지만, 이후 CLI `expert` 명령을 사용하면 Linux 셸에 액세스할 수 있습니다. 참고 이 기능을 이용하면 버전 6.3 기능인 management center에 대한 CLI 액세스 활성화/비활성화가 중단됩니다. 이 옵션이 중단되면 가상 management center에서는 **System(**시스템**)** > **Configuration(**구성**)** > **Console Configuration(**콘솔 구성**)** 페이지가 표시되지 않습니다. 물리적 management center에서는 계속 표시됩니다.
SSH 로그인 실패 횟수를 제한합니다.	6.3	사용자가 SSH를 통해 디바이스에 액세스하고 3회 연속 로그인 시도가 실패한 경우, 해당 디바이스가 SSH 세션을 종료합니다.

기능	버전	세부 사항
CLI 액세스를 활성화 및 비활성화 하는 기능 management center	6.3	신규/수정된 화면: management center 웹 인터페이스 관리자가 사용할 수 있는 새 체크박스: **Enable CLI Access(CLI** 액세스 활성화**)**(시스템 (⚙) > **Configuration(**구성**)**에 위치) > (**Console Configuration(**콘솔 구성**))** 페이지 • 선택: SSH를 사용하여 management center에 로그인하면 CLI에 액세스할 수 있습니다. • 선택 취소: SSH를 사용하여 management center에 로그인하면 Linux 셸에 액세스할 수 있습니다. 이는 새 버전 6.3 설치 뿐만 아니라 이전 릴리스에서 버전 6.3으로 업그레이드 할 때의 기본 상태입니다. 지원되는 플랫폼: management center