# 사용자 ID 개요

다음 주제에서는 사용자 ID에 대해 설명합니다.



# 사용자 ID 정보

사용자 ID 정보를 이용하면 정책 위반, 공격, 네트워크 취약성의 원인을 파악하고, 이를 추적해 관련 사용자를 확인할 수 있습니다. 예를 들어, 다음을 확인할 수 있습니다.

- 영향 레벨이 Vulnerable(취약 - 레벨 1: 빨간색)인 침입 이벤트가 대상으로 지정한 호스트의 소유자
- 내부 공격 또는 포트스캔을 시작한 사용자
- 지정한 호스트에 무단 액세스를 시도하는 사용자
- 대역폭을 너무 많이 사용하는 사용자
- 중요한 운영체제 업데이트를 적용하지 않은 사용자
- 회사 IT 정책을 위반하며 인스턴트 메시징 소프트웨어나 P2P 파일 공유 애플리케이션을 사용하는 사용자
- 네트워크의 각 보안 침해 지표와 관련된 사용자

이러한 정보를 충분히 파악하면 Firepower System의 다른 기능을 사용하여 위험을 완화하고, 액세스 제어를 수행하고, 다른 사용자의 작업 중단을 방지하는 조치를 취할 수 있습니다. 또한 이러한 기능을 통해 감사 제어 효과를 크게 높이고 규정 준수를 강화할 수 있습니다.

사용자 데이터를 수집하도록 사용자 ID 소스를 구성한 후에는 사용자 인식 및 사용자 제어를 수행할 수 있습니다.

관련 항목


ID 용어, 2 페이지
사용자 ID 소스 정보, 2 페이지

ID 구축, 5 페이지
ID 정책 설정 방법, 10 페이지

# ID 용어

이 주제에서는 사용자 ID 및 사용자 제어와 관련해 자주 사용하는 용어를 설명합니다.

사용자 인식

*ID* 소스( 또는 TS 에이전트 등)를 이용해 네트워크 상의 사용자를 식별합니다. 사용자 인식을 이용하면 신뢰할 수 있는(Active Directory 등) 소스와 신뢰할 수 없는(애플리케이션 기반) 소스의 사용자를 모두 식별할 수 있습니다. Active Directory를 ID 소스로 사용하려면 영역과 디렉터리를 설정해야 합니다. 자세한 내용은 사용자 ID 소스 정보, 2 페이지를 참고하십시오.

사용자 제어

액세스 컨트롤 정책과 연결한 *ID* 정책을 설정합니다. (이후 ID 정책은 액세스 컨트롤 하위 정책으로 참조됩니다.) ID 정책은 ID 소스를 지정하면, 경우에 따라 해당 소스에 속하는 사용자와 그룹도 지정합니다.

ID 정책을 액세스 컨트롤 정책과 연결하면, 네트워크 트래픽에서의 사용자나 사용자 활동 모니터링, 신뢰, 차단 또는 허용 여부를 결정하게 됩니다. 자세한 내용은 액세스 제어 정책를 참고하십시오.

권한 있는 **ID** 소스

사용자 로그인(예: Active Directory)을 검증한 신뢰할 수 있는 서버입니다. 권한 있는 로그인에서 가져온 데이터를 사용하여 사용자 인식 및 사용자 제어를 수행할 수 있습니다. 권한 있는 사용자 로그인은 수동 및 활성 인증에서 가져옵니다.

- 패시브 인증은 외부 소스를 통해 사용자를 인증할 때 수행됩니다. ISE/ISE-PIC 및 TS 에이전트는 Firepower System에서 지원하는 패시브 인증 방법입니다.
- 액티브 인증은 사전 구성된 매니지드 디바이스를 통해 사용자를 인증할 때 수행됩니다. 캡티브 포털(captive portal) 및 원격 액세스 VPN은 Firepower System에서 지원하는 액티브 인증 방법입니다.

권한 없는 **ID** 소스

사용자 로그인이 검증된 알 수 없거나 신뢰할 수 없는 서버입니다. 트래픽 기반 탐지는 Firepower System에서 지원하는 유일한 권한 없는 ID 소스입니다. 권한 없는 로그인에서 가져온 데이터를 사용하여 사용자 인식을 수행할 수 있습니다.

# 사용자 ID 소스 정보

다음 표에는 시스템에서 지원되는 사용자 ID 소스에 대한 간략한 개요가 나와 있습니다. 각 ID 소스는 사용자 인식을 위한 사용자의 저장소를 제공합니다. 이러한 사용자는 ID 및 액세스 컨트롤 정책으로 제어할 수 있습니다.

| 사용자 ID 소스 | 정책 | 서버 요구 사항 | 유형 | 인증 유형 | 사용자 인식 여부 | 사용자 제어 여부 | 자세한 내용은 다음을 참조하십시오. |
|---|---|---|---|---|---|---|---|
| ISE/ISE-PIC | ID | Microsoft Active Directory | 신뢰할 수 있는 로그인 | 수동 | 예 | 예 | ISE/ISE-PIC ID 소스 |
| TS 에이전트 | ID | Microsoft Windows 터미널 서버 | 신뢰할 수 있는 로그인 | 수동 | 예 | 예 | TS(Terminal Services) 에이전트 ID 소스 |
| 캡티브 포털 | ID | OpenLDAP<br>Microsoft Active Directory | 신뢰할 수 있는 로그인 | 활성 | 예 | 예 | 캡티브 포털 ID 소스 |
| 원격 액세스 VPN | ID | OpenLDAP 또는 Microsoft Active Directory | 신뢰할 수 있는 로그인 | 활성 | 예 | 예 | Remote Access VPN ID 소스 |
| | ID | RADIUS | 신뢰할 수 있는 로그인 | 활성 | 예 | 아니요 | |
| 트래픽 기반 탐지 | 네트워크 검색 | 해당 없음 | 신뢰할 수 없는 로그인 | 해당 없음 | 예 | 아니요 | 트래픽 기반 탐지 ID 소스 |

구축할 ID 소스를 선택할 경우 다음 사항을 고려하십시오.

- 비 LDAP 사용자 로그인에는 트래픽 기반 탐지를 사용해야 합니다.
- 트래픽 기반 탐지 또는 캡티브 포털(captive portal)을 사용하여 실패한 로그인 또는 인증 활동을 기록해야 합니다. 실패한 로그인 또는 인증 시도는 데이터베이스의 사용자 목록에 새 사용자를 추가하지 않습니다.
- 캡티브 포털 ID 소스는 라우팅 인터페이스를 이용하는 매니지드 디바이스를 요구합니다. 캡티브 포털은 인라인(탭 모드라고도 함) 인터페이스로는 사용할 수 없습니다.

이러한 ID 소스의 데이터는 Secure Firewall Management Center의 사용자 데이터베이스 및 사용자 활동 데이터베이스에 저장됩니다. 새로운 사용자 데이터를 데이터베이스에 자동으로 정기적으로 다운로드하도록 management center-서버의 사용자 다운로드를 구성할 수 있습니다.

원하는 ID 소스를 이용해 ID 규칙을 설정한 후에는, 각 규칙을 액세스 컨트롤 정책에 연결하고 정책이 효력을 발휘할 매니지드 디바이스에 해당 정책을 구축합니다. 액세스 컨트롤 정책과 구축에 관한 자세한 내용은 액세스 제어에 다른 정책 연결 섹션을 참조하십시오.

사용자 ID에 대한 일반 정보는 사용자 ID 정보, 1 페이지의 내용을 참조하십시오.

# 사용자 ID 모범 사례

ID 정책을 설정하기 전에 다음 정보를 검토하는 것이 좋습니다.

- 사용자 제한 확인
- AD 도메인당 하나의 영역 생성
- 상태 모니터
- 최신 버전의 ISE/ISE-PIC, 두 가지 교정 유형 사용
- 6.7에서 사용자 에이전트 지원 중단
- 캡티브 포털에는 라우팅 인터페이스, 여러 개별 작업이 필요함

### Active Directory, LDAP 및 영역

Firepower System은 사용자 인식 및 제어를 위해 Active Directory 또는 LDAP를 지원합니다. Active Directory 또는 LDAP 리포지토리와 FMC 간의 연결을 영역이라고 합니다. LDAP 서버 또는 Active Directory 도메인당 하나의 영역을 생성해야 합니다. 지원되는 버전에 대한 자세한 내용은 영역에 지원되는 서버의 내용을 참조하십시오.

LDAP에서 지원하는 유일한 사용자 ID 소스는 캡티브 포털입니다. 다른 ID 소스(ISE/ISE-PIC 제외)를 사용하려면 Active Directory를 사용해야 합니다.

Active Directory에만 해당:

- 도메인 컨트롤러당 하나의 디렉터리를 생성합니다.

  자세한 내용은 다음 섹션을 참조하십시오. Active Directory 영역 및 영역 디렉터리 생성

- 두 도메인 간의 신뢰 관계에 있는 사용자 및 그룹이 지원됩니다. 단, 모든 Active Directory 도메인 및 도메인 컨트롤러를 영역과 디렉터리로 각각 추가해야 합니다.

  자세한 내용은 영역 및 신뢰할 수 있는 도메인를 참고하십시오.

### 프록시 시퀀스

프록시 시퀀스는 LDAP, Active Directory 또는 ISE/ISE-PIC 서버와 통신하는 데 사용할 수 있는 하나 이상의 매니지드 디바이스입니다. 이는 Cisco Defense Orchestrator(CDO)가 Active Directory 또는 ISE/ISE-PIC 서버와 통신할 수 없는 경우에만 필요합니다. (예를 들어 CDO는 퍼블릭 클라우드에 있지만 Active Directory 또는 ISE/ISE-PIC는 프라이빗 클라우드에 있을 수 있습니다.)

하나의 매니지드 디바이스를 프록시 시퀀스로 사용할 수 있지만, 둘 이상의 매니지드 디바이스를 설정하는 것이 좋습니다. 그러면 하나의 매니지드 디바이스가 Active Directory 또는 ISE/ISE-PIC와 통신할 수 없는 경우 다른 매니지드 디바이스가 인계받을 수 있습니다.

### 최신 버전의 ISE/ISE-PIC 사용

ISE/ISE-PIC ID 소스를 사용할 것으로 예상되는 경우 항상 최신 버전을 사용하여 최신 기능과 버그를 수정하는 것이 좋습니다.

pxGrid 2.0(버전 2.6 패치 6 이상 또는 2.7 패치 2 이상에서 사용됨)도 ISE/ISE-PIC에서 사용하는 교정을 EPS(Endpoint Protection Service)에서 ANC(Adaptive Network Control)로 변경합니다. ISE/ISE-PIC를 업그레이드하는 경우 EPS에서 ANC로 교정 정책을 마이그레이션해야 합니다.

ISE/ISE-PIC 사용에 대한 자세한 내용은 ISE/ISE-PIC 지침 및 제한 사항에서 확인할 수 있습니다.

ISE/ISE-PIC ID 소스를 설정하려면 사용자 제어에 대한 ISE/ISE-PIC 설정 방법의 내용을 참조하십시오.

캡티브 포털 정보

캡티브 포털은 LDAP 또는 Active Directory를 사용할 수 있는 유일한 사용자 ID 소스입니다. 또한 매니지드 디바이스는 라우팅된 인터페이스를 사용하도록 구성해야 합니다.

추가 지침은 캡티브 포털 가이드라인 및 제한 사항에서 볼 수 있습니다.

캡티브 포털을 설정하려면 여러 독립적인 작업을 수행해야 합니다. 자세한 내용은 사용자 제어에 대한 캡티브 포털 설정 방법를 참고하십시오.

**TS Agent** 정보

TS 에이전트 사용자 ID 소스는 Windows 터미널 서버에서 사용자 세션을 식별하는 데 필요합니다. TS 에이전트 소프트웨어는 *Cisco TS(Terminal Services)* 에이전트 가이드에 설명된 대로 터미널 서버 시스템에 설치해야 합니다. 또한 TS 에이전트 서버의 시간을 management center의 시간과 동기화해야 합니다.

TS 에이전트 데이터는 Users(사용자), User Activity(사용자 활동), Connection Event(연결 이벤트) 테이블에 표시되며 사용자 인식 및 사용자 제어에 사용할 수 있습니다.

자세한 내용은 TS 에이전트 가이드라인를 참고하십시오.

**ID** 정책을 액세스 제어 정책과 연결합니다**.**

영역, 디렉터리 및 사용자 ID 소스를 구성한 후에는 ID 정책에서 ID 규칙을 설정해야 합니다. 정책을 적용하려면 ID 정책을 액세스 제어 정책과 연결해야 합니다.

ID 정책 생성에 대한 자세한 내용은 ID 정책 생성의 내용을 참조하십시오.

ID 규칙 생성에 대한 자세한 내용은 ID 규칙 생성의 내용을 참조하십시오.

ID 정책을 액세스 제어 정책과 연결하려면 액세스 제어에 다른 정책 연결의 내용을 참조하십시오.

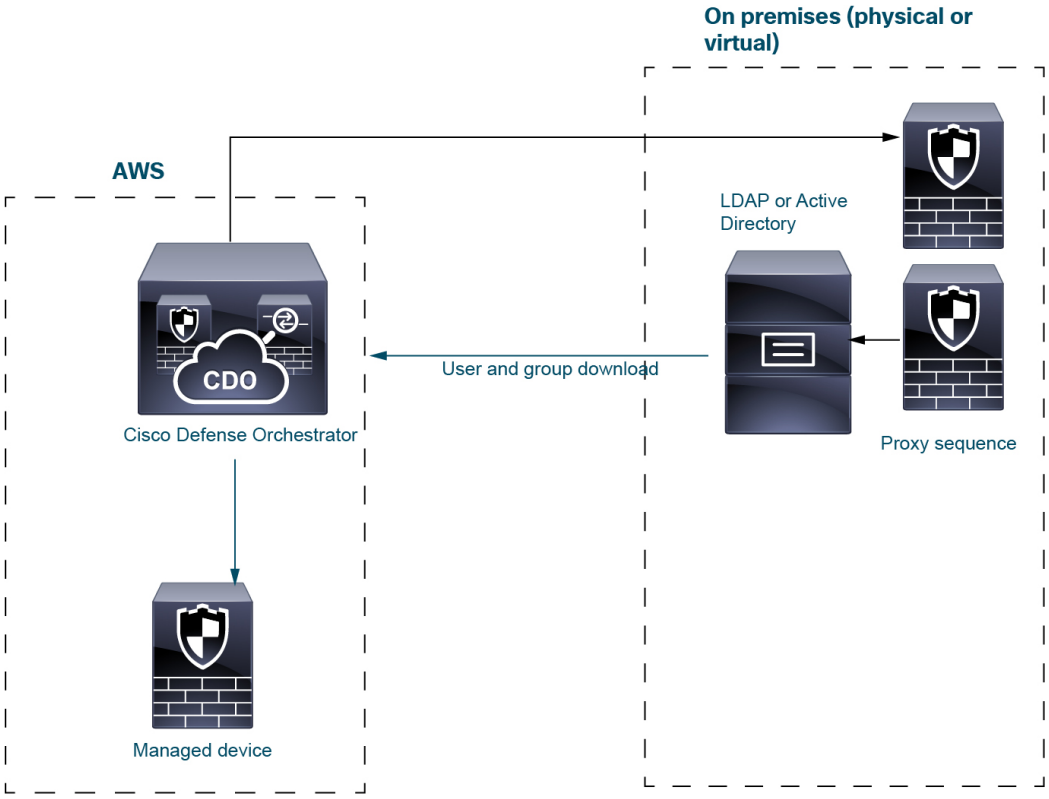
# ID 구축

시스템이 사용자 로그인, ID 소스로부터 사용자 데이터를 탐지하면 해당 로그인의 사용자는 management center 사용자 데이터베이스의 사용자 목록과 비교하여 확인됩니다. 로그인 사용자가 기존 사용자와 일치하면 로그인의 데이터가 사용자에게 할당됩니다. 로그인이 기존 사용자와 일치하지 않으면 SMTP 트래픽의 로그인이 아닌 경우 새 사용자가 생성됩니다. SMTP 트래픽의 일치하지 않는 로그인은 삭제됩니다.

사용자가 속하는 그룹은 management center가 사용자를 확인하고 사용자와 연결됩니다.

### 샘플 ID 구축

이 섹션에서 설명하는 샘플 구축은 다음 그림에 나와 있는 시스템을 기반으로 합니다.




위의 그림에서는 CDO 및 하나의 매니지드 디바이스가 AWS에 구축되고 다른 디바이스는 온프레미스에 있습니다. 이러한 디바이스는 물리적 또는 가상일 수 있습니다. 서로 통신할 수만 있으면 됩니다.

두 개의 온프레미스 매니지드 디바이스는 프록시 시퀀스로 사용됩니다. 이러한 디바이스도 CDO에 추가해야 합니다.

프록시 시퀀스는 LDAP, Active Directory 또는 ISE/ISE-PIC 서버와 통신하는 데 사용할 수 있는 하나 이상의 매니지드 디바이스입니다. 이는 Cisco Defense Orchestrator(CDO)가 Active Directory 또는 ISE/ISE-PIC 서버와 통신할 수 없는 경우에만 필요합니다. (예를 들어 CDO는 퍼블릭 클라우드에 있지만 Active Directory 또는 ISE/ISE-PIC는 프라이빗 클라우드에 있을 수 있습니다.)

LDAP 또는 Active Directory는 다음 단락에서 설명하는 것처럼 TS 에이전트 및 캡티브 포털에만 필요합니다.

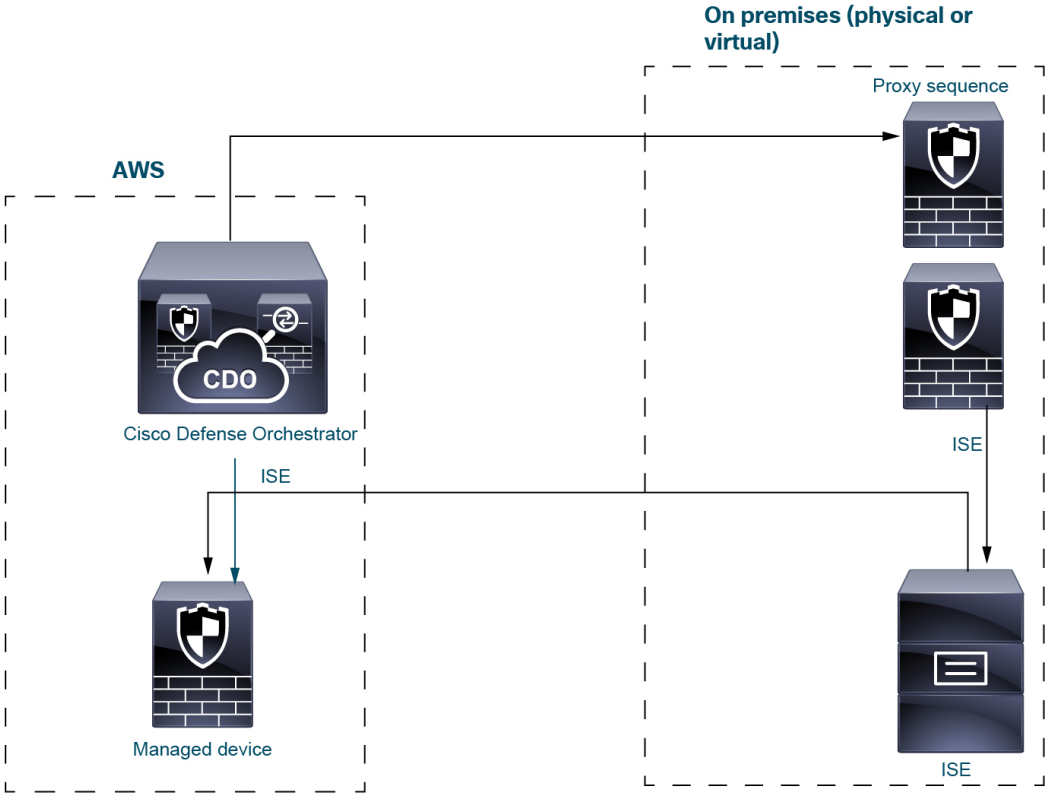
이와 같은 시스템 설정에 대한 자세한 내용은 ID 정책 설정 방법, 10 페이지의 내용을 참조하십시오.

**ISE/ISE-PIC ID 소스**

ISE/ISE-PIC ID 소스를 구축할 때 CDO는 CDO에서 ISE/ISE-PIC 서버에 직접 연결할 수 없는 경우 프록시 시퀀스에 연결합니다. 사용자, 그룹 및 구독은 ISE/ISE-PIC 서버에서 AWS의 매니지드 디바이스로 전송됩니다.

선택적으로 ISE/ISE-PIC 구축에 LDAP 서버를 포함할 수 있지만 선택 사항이므로 다음 그림에는 표시되지 않습니다.

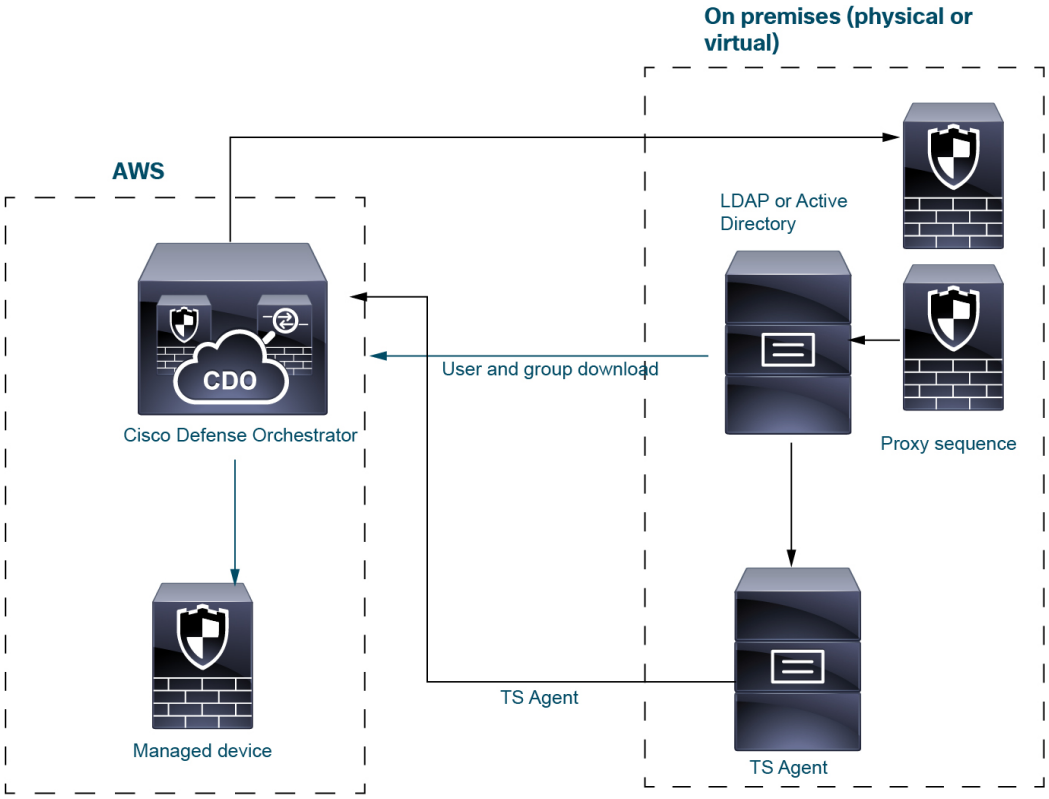
ISE/ISE-PIC에 대한 자세한 내용은 ISE/ISE-PIC ID 소스의 내용을 참조하십시오.




**TS** 에이전트 **ID** 소스

TS(Terminal Services) 에이전트 소프트웨어는 Microsoft Server에서 실행되며 사용자가 서버에 로그인하는 데 사용하는 포트 범위를 기반으로 CDO 사용자 정보를 전송합니다. TS 에이전트는 LDAP 또는 Active Directory에서 사용자 ID 정보를 가져와서 CDO로 전송합니다.

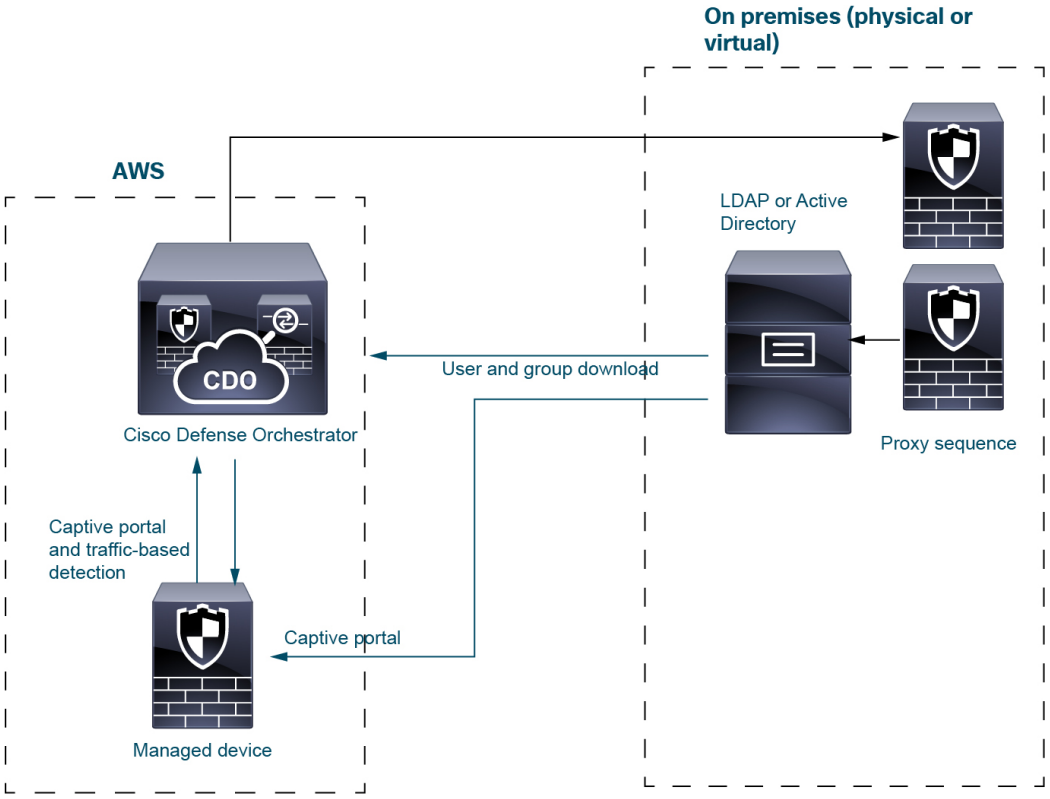
TS 에이전트 ID 소스에 대한 자세한 내용은 TS(Terminal Services) 에이전트 ID 소스의 내용을 참조하십시오.




캡티브 포털 **ID** 소스

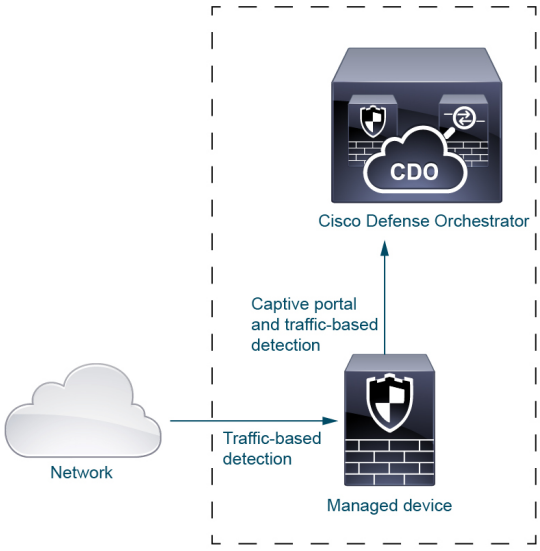
캡티브 포털은 Active Directory 외에 LDAP를 지원하는 유일한 ID 소스입니다. 캡티브 포털 ID 소스는 사용자가 IP 주소 또는 호스트 이름을 사용하여 AWS에서 매니지드 디바이스를 사용하여 네트워크 리소스에 액세스하려고 할 때 트리거됩니다. 캡티브 포털은 프록시 시퀀스를 사용하여 LDAP 또는 Active Directory에서 사용자 정보를 가져와서 CDO에 사용자 정보를 전송합니다.

캡티브 포털 ID 소스에 대한 자세한 내용은 캡티브 포털 ID 소스의 내용을 참조하십시오.




트래픽 기반 탐지

트래픽 기반 탐지는 네트워크의 애플리케이션만 탐지하도록 설계되었으므로 Active Directory와 같은 사용자 저장소 또는 프록시 시퀀스가 필요하지 않습니다. 자세한 내용은 호스트, 애플리케이션 및 사용자 데이터 탐지 정보의 내용을 참조하십시오.



# ID 정책 설정 방법

이번 주제에서는 사용 가능한 사용자 ID 소스, 즉 TS 에이전트, ISE/ISE-PIC, 캡티브 포털, 원격 액세스 VPN을 이용해 ID 정책을 설정하는 방법을 개략적으로 설명합니다.

프로시저

| | 명령 또는 동작 | 목적 |
|---|---|---|
| 단계 **1** | (선택 사항). 프록시 시퀀스를 생성합니다. | 프록시 시퀀스는 LDAP, Active Directory 또는 ISE/ISE-PIC 서버와 통신하는 데 사용할 수 있는 하나 이상의 매니지드 디바이스입니다. 이는 Cisco Defense Orchestrator(CDO)가 Active Directory 또는 ISE/ISE-PIC 서버와 통신할 수 없는 경우에만 필요합니다. (예를 들어 CDO는 퍼블릭 클라우드에 있지만 Active Directory 또는 ISE/ISE-PIC는 프라이빗 클라우드에 있을 수 있습니다.)<br><br>하나의 매니지드 디바이스를 프록시 시퀀스로 사용할 수 있지만, 둘 이상의 매니지드 디바이스를 설정하는 것이 좋습니다. 그러면 하나의 매니지드 디바이스가 Active Directory 또는 ISE/ISE-PIC와 통신할 수 없는 경우 다른 매니지드 디바이스가 인계받을 수 있습니다.<br><br>프록시 시퀀스 생성의 내용을 참조하십시오. |
| 단계 **2** | (선택 사항). 영역 및 디렉터리를 생성합니다. 사용자 제어에서 사용할 사용자를 포함하는 포리스트의 모든 도메인에 대해 하나의 영역을 생성합니다. 또한 모든 도메인 컨트롤러에 대해 하나의 디렉터리를 생성합니다. 해당하는 management center 영역 및 디렉터리가 있는 사용자 및 그룹만 ID 정책에서 사용할 수 있습니다. | 다음 중 하나라도 해당하는 경우 영역, 영역 디렉터리, 프록시 시퀀스 생성은 선택 사항입니다.<br>• SGT ISE 속성 조건은 사용하고 사용자/그룹/영역/엔드포인트 위치/엔드포인트 프로파일 조건은 사용하지 않습니다.<br>• ID 정책을 사용하여 네트워크 트래픽 만 필터링하고 있습니다.<br>• Cisco Defense Orchestrator(CDO)를 사용하는 경우에만 프록시 시퀀스가 필요하며, 프록시 시퀀스는 Active Directory 또는 ISE/ISE-PIC와 직접 통신할 수 없습니다.<br><br>영역은 신뢰할 수 있는 사용자 및 그룹 저장소로, 대부분의 경우 Microsoft Active Directory 저장소입니다. management center는 |

| | 명령 또는 동작 | 목적 |
|---|---|---|
| | | 사용자와 그룹을 사용자가 지정한 간격에 따라 다운로드합니다. 사용자와 그룹을 다운로드 대상에 추가하거나 대상에서 제외할 수 있습니다.<br><br>Active Directory 영역 및 영역 디렉터리 생성의 내용을 참조하십시오. 영역을 생성하는 옵션에 대한 자세한 내용은 영역 필드의 내용을 참조하십시오.<br><br>디렉터리는 컴퓨터 네트워크의 사용자 및 네트워크 공유에 대한 정보를 구성하는 Active Directory 도메인 컨트롤러입니다. Active Directory 컨트롤러는 영역에 대한 디렉터리 서비스를 제공합니다. Active Directory는 사용자 및 그룹 개체를 여러 도메인 컨트롤러에 배포하며, 이러한 컨트롤러는 디렉터리 서비스 사용을 통해 로컬 변경사항을 서로에게 전파하는 피어 컨트롤러입니다. 자세한 내용은 MSDN의 Active Directory 기술 사양 용어를 참조하십시오.<br><br>한 영역에 하나 이상의 디렉터리를 지정할 수 있으며, 이 경우 사용자 제어를 위해 각 도메인 컨트롤러는 영역의 **Directory(**디렉터리**)** 탭 페이지에 나열된 순서에 따라 사용자 및 그룹 인증서에 맞게 쿼리됩니다.<br><br>참고 SGT ISE 속성 조건은 구성하고 사용자/그룹/영역/엔드포인트 위치/엔드포인트 프로파일 조건은 구성하지 않으려는 경우에는 필요에 따라 영역 또는 영역 시퀀스를 구성하면 됩니다. |
| 단계 **3** | 영역에서 사용자 및 그룹을 동기화합니다. | 사용자와 그룹을 제어하려면 사용자와 그룹을 management center에 동기화해야 합니다. 언제든 원할 때 사용자와 그룹을 동기화하거나, 지정된 주기로 사용자와 그룹을 동기화하도록 시스템을 구성할 수 있습니다.<br><br>사용자와 그룹을 동기화할 때 예외를 지정할 수 있습니다. 예를 들어 Engineering(엔지니어링) 그룹을 해당 영역에 대한 모든 사용자 제어에서 제외하거나, Engineering(엔지니어링) |

| | 명령 또는 동작 | 목적 |
|---|---|---|
| | | 그룹에 적용하는 사용자 제어에서 사용자 **joe.smith**를 제외하는 식입니다.<br>의 내용을 참조하십시오.사용자 및 그룹 동기화 |
| 단계 **4** | (선택 사항). 영역 시퀀스를 생성합니다. | 영역 시퀀스는 ID 정책에서 사용될 때 시스템이 지정된 순서로 영역을 검색하여 규칙과 일치하는 사용자를 찾는 영역의 순서가 지정된 목록입니다. 영역 시퀀스 생성의 내용을 참조하십시오. |
| 단계 **5** | 사용자 및 그룹 데이터를 검색하는 메서드(*ID* 소스)를 만듭니다. | 영역에 저장한 데이터를 이용해 사용자와 그룹을 제어하려면 고유 설정을 적용한 ID 소스를 설정해야 합니다. ID 소스에는 TS 에이전트, 캡티브 포털, 원격 VPN 등이 있습니다. 다음 중 하나를 참조하십시오.<br>• 사용자 제어에 대한 캡티브 포털 설정 방법<br>• 사용자 제어를 위한 ISE/ISE-PIC 설정<br>• 사용자 제어에 대한 RA VPN 설정 |
| 단계 **6** | ID 정책을 생성합니다. | ID 정책은 카테고리별로 구성할 수도 있는, 하나 이상의 ID 규칙을 포함합니다. ID 정책 생성의 내용을 참조하십시오.<br>참고 사용자, 그룹, 영역, 엔드포인트 위치 또는 엔드포인트 프로파일 조건이 아닌 SGT ISE 속성 조건을 설정하려는 경우 또는 ID 정책을 사용하여 네트워크 트래픽을 필터링하는 경우에만 영역 또는 영역 시퀀스 설정이 선택 사항입니다. |
| 단계 **7** | 하나 이상의 ID 규칙을 생성합니다. | ID 규칙을 이용하면 인증 유형, 네트워크 영역, 네트워크 또는 지리 위치, 영역, 영역 시퀀스 유형을 포함한 다양한 일치 기준을 지정할 수 있습니다. ID 규칙 생성의 내용을 참조하십시오. |
| 단계 **8** | ID 정책을 액세스 제어 정책과 연결합니다. | 액세스 컨트롤 정책은 트래픽을 필터링하며 필요하다면 검사도 진행합니다. ID 정책을 적용하려면 액세스 제어 정책과 연결해야 합 |

| | 명령 또는 동작 | 목적 |
|---|---|---|
| | | 니다. 액세스 제어에 다른 정책 연결의 내용을 참조하십시오. |
| 단계 **9** | 액세스 컨트롤 정책을 하나 이상의 매니지드 디바이스에 구축합니다. | 정책을 이용해 사용자 활동을 제어하려면, 클라이언트를 연결할 매니지드 디바이스에 정책을 구축해야 합니다. 구성 변경 사항 구축의 내용을 참조하십시오. |
| 단계 **10** | 사용자 활동을 모니터링합니다. | 사용자 ID 소스가 수집하는 활성 세션 목록이나 사용자 ID 소스가 수집하는 사용자 정보 목록을 확인합니다. .<br>ID 정책은 다음이 모두 참인 경우 필요하지 않습니다.<br>• ISE/ISE-PIC ID 소스를 사용합니다.<br>• 액세스 제어 정책에서 사용자 또는 그룹을 사용하지 않습니다.<br>• 액세스 제어 정책에서 SGT(Security Group Tag)를 사용합니다. 자세한 내용은 ISE SGT 및 맞춤형 SGT 규칙 조건 비교를 참고하십시오. |

관련 항목

트래픽 기반 사용자 탐지 구성

# 사용자 활동 데이터베이스

Secure Firewall Management Center의 사용자 활동 데이터베이스에는 구성된 모든 ID 소스에서 탐지하거나 보고하는 네트워크의 사용자 활동 기록이 포함됩니다. 시스템에서는 다음과 같은 상황에서 이벤트를 기록합니다.

- 개별 로그인 또는 로그오프를 탐지한 경우
- 새 사용자를 탐지한 경우
- 시스템 관리자가 사용자를 수동으로 삭제하는 경우
- 데이터베이스에 없는 사용자를 탐지했으나 사용자 제한에 도달하여 사용자를 추가할 수 없는 경우
- 사용자와 관련된 침해 지표를 해결하거나, 사용자에 대한 침해 규칙 침해 지표를 활성화 또는 비활성화하는 경우

참고 TS 에이전트가 동일한 사용자를 다른 패시브 인증 ID 소스(ISE/ISE-PIC 등)로 모니터링할 경우, management center는 TS 에이전트 데이터에 우선순위를 둡니다. TS 에이전트 및 다른 패시브 소스가 동일한 IP 주소에서 동일한 활동을 보고할 경우, TS 에이전트 데이터만 management center에 로깅됩니다.

시스템이 탐지한 사용자 활동은 Secure Firewall Management Center로 확인할 수 있습니다. (**Analysis(**분석**)** > **Users(**사용자**)** > **User Activity(**사용자의 활동**)**.)

# 사용자 데이터베이스

Secure Firewall Management Center의 사용자 데이터베이스에는 구성된 모든 ID 소스에서 탐지하거나 보고한 기록이 포함됩니다. 사용자 제어에 대한 신뢰할 수 있는 소스에서 얻은 데이터를 사용할 수 있습니다.

지원되는 신뢰할 수 있거나 신뢰할 수 없는 ID 소스에 대한 자세한 내용은 사용자 ID 소스 정보, 2 페이지 섹션을 참조하십시오.

에서도 설명하지만, Secure Firewall Management Center가 저장할 수 있는 총 사용자 수는 Secure Firewall Management Center 모델에 따라 다릅니다. 사용자 한도에 도달하면, 시스템은 이전에 탐지하지 않은 사용자 데이터의 다음과 같은 ID 소스를 바탕으로 우선순위를 지정합니다.

- 새 사용자가 신뢰할 수 없는 ID 소스에서 왔다면, 시스템은 사용자를 데이터베이스에 추가하지 않습니다. 새 사용자를 추가하려면, 사용자를 수동으로 삭제하거나 데이터베이스 비우기를 이용해 삭제해야 합니다.
- 새 사용자가 신뢰할 수 있는 ID 소스에서 왔다면, 시스템은 가장 오랫동안 비활성 상태인 신뢰할 수 없는 사용자를 삭제하고 새 사용자를 데이터베이스에 추가합니다.

특정 사용자 이름을 제외하도록 ID 소스를 구성한 경우 해당 사용자 이름의 사용자 활동 데이터는 Secure Firewall Management Center에 보고되지 않습니다. 이러한 제외된 사용자 이름은 데이터베이스에 남아 있지만 IP 주소와는 연결되지 않습니다.

management center 고가용성을 설정한 상태이고 기본 디바이스가 실패할 경우, 페일오버 다운타임 동안에는 캡티브 포털, ISE/ISE-PIC, TS 에이전트 또는 원격 액세스 VPN 디바이스에서 보고된 로그인을 식별할 수 없습니다. 사용자가 이전에 확인된 적이 있고 management center에 다운로드된 적이 있더라도 마찬가지입니다. 식별되지 않은 사용자는 management center에서 알 수 없는 사용자로 로깅됩니다. 다운타임이 끝나면 ID 정책의 규칙에 따라 알 수 없는 사용자가 다시 식별되고 처리됩니다.

참고 TS 에이전트가 동일한 사용자를 다른 패시브 인증 ID 소스(ISE/ISE-PIC)로 모니터링할 경우, management center는 TS 에이전트 데이터에 우선순위를 둡니다. TS 에이전트 및 다른 패시브 소스가 동일한 IP 주소에서 동일한 활동을 보고할 경우, TS 에이전트 데이터만 management center에 로깅됩니다.

시스템이 새로운 사용자 세션을 탐지하면, 사용자 세션 데이터는 다음 중 하나가 발생할 때까지 사용자 데이터베이스 보관됩니다.

- management center의 사용자가 사용자 세션을 수동으로 삭제합니다.
- ID 소스가 해당 사용자 세션의 로그오프를 보고합니다.
- 영역의 **User Session Timeout: Authenticated Users(**사용자 세션 시간 초과**:** 인증된 사용자**)**, **User Session Timeout: Failed Authentication Users(**사용자 세션 시간 초과**:** 실패한 인증 사용자**)** 또는 **User Session Timeout: Guest Users(**사용자 세션 시간 초과**:** 게스트 사용자**)** 설정에서 지정된 대로 영역의 사용자 세션이 종료됩니다.

# Cisco Defense Orchestrator 호스트 및 사용자 한도

## 클라우드 사용 Firewall Management Center 호스트 제한

클라우드 사용 Firewall Management Center은 모니터링 중인 네트워크의 IP 주소와 관련된 활동을 감지하는 경우 (네트워크 검색 정책에 정의된 대로) 네트워크 맵에 호스트를 추가합니다.

클라우드 사용 Firewall Management Center는 호스트 데이터베이스에 최대 600,000명의 호스트를 저장할 수 있지만 다음을 권장합니다.

| **CDO**에서 관리하는 디바이스 수 | 권장 호스트 수 |
|---|---|
| 150 | 100,000 |
| 51-300 | 300,000 |
| 301-1000 | 600,000 |

네트워크 맵에 없는 호스트에 대한 상황 데이터를 볼 수 없습니다. 그러나 액세스 제어를 수행할 수 있습니다. 예를 들어, 호스트의 네트워크 규정준수 상황을 모니터하기 위한 규정준수 허용리스트를 사용할 수 없는 경우에도 네트워크 맵에 없는 호스트를 오가는 트래픽에 대한 애플리케이션 제어를 수행할 수 있습니다.

참고 시스템은 MAC 전용 호스트를 IP 주소와 MAC 주소 모두로 식별하는 호스트와 별도로 계산합니다. 호스트와 연결된 모든 IP 주소는 하나의 호스트로 계산됩니다.

호스트 제한 도달 및 호스트 삭제

네트워크 검색 정책은 호스트 제한에 도달한 후 새 호스트가 탐지될 때 수행되는 작업을 제어합니다. 새 호스트를 삭제하거나 가장 오랫동안 비활성 상태였던 호스트를 교체할 수 있습니다. 또한 시스템 비활성화로 네트워크 맵에서 호스트를 제거하는 기간을 설정할 수 있습니다. 그러나 시스템이 삭제된 호스트와 관련된 활동을 탐지하는 경우 네트워크 맵에서 호스트, 전체 서브넷 또는 모든 호스트를 수동으로 제거할 수 있습니다.

다중 도메인 구축의 경우 각 리프 도메인에는 독립적인 네트워크 검색 정책이 있습니다. 따라서 각 리프 도메인은 시스템이 새 호스트를 검색하는 경우 고유한 동작을 제어합니다.

# Cisco Defense Orchestrator클라우드 사용 Firewall Management Center 사용자 제한

다음과 같은 경우 사용자가 클라우드 사용 Firewall Management Center 사용자 데이터베이스에 추가됩니다.

- 사용자가 영역에서 다운로드됩니다.
- 캡티브 포털 또는 RA-VPN 사용자가 로그인합니다.
- 모든 ID 소스(예: TS Agent)에서 사용자가 탐지됩니다.

클라우드 사용 Firewall Management Center는 호스트 데이터베이스에 최대 600,000명의 사용자를 저장할 수 있지만 다음을 권장합니다.

| **CDO**에서 관리하는 디바이스 수 | 권장 사용자 수 |
|---|---|
| 150 | 100,000 |
| 51-300 | 300,000 |
| 301-1000 | 600,000 |

액세스 컨트롤 정책을 이용한 사용자 제어는 신뢰할 수 있는 사용자에만 적용됩니다.

클라우드 사용 Firewall Management Center는 사용자 데이터베이스에 600,000개의 세션을 저장할 수 있습니다.

사용자 한도 도달 후 이전에 탐지하지 않은 새 사용자를 탐지하면, 시스템은 사용자 데이터의 ID 소스를 바탕으로 해당 데이터의 우선순위를 정합니다.

- 새 사용자를 신뢰할 수 없는 소스의 경우, 시스템은 권한 없는 사용자 데이터베이스에 추가 되지 않습니다. 새 사용자를 추가하려면, 사용자를 수동으로 삭제하거나 데이터베이스를 비워야 합니다.
- 새 사용자가 신뢰할 수 있는 ID 소스에서 왔다면, 시스템은 가장 오랫동안 비활성 상태인 신뢰할 수 없는 사용자를 삭제하고 신뢰할 수 있는 새 사용자를 데이터베이스에 추가합니다.

  모든 사용자가 신뢰할 수 있는 사용자라면, 시스템은 가장 오랫동안 비활성 상태인 신뢰할 수 있는 사용자를 삭제하고 새 사용자를 데이터베이스에 추가합니다.

사용자 제어 문제 해결에서 문제 해결 정보를 확인할 수 있습니다.

팁 트래픽 기반 탐지를 사용한다면, 프로토콜별로 사용자 기록을 제한해 불필요한 사용자 이름을 최소화하고 데이터베이스의 공간을 확보할 수 있습니다. 예를 들어 시스템이 AIM, POP3 및 IMAP 트래픽에서 발견한 사용자를 추가하지 못하게 할 수도 있습니다. 모니터링 대상이 아닌 계약자나 방문자가 보내는 트래픽임이 확실하기 때문입니다.