시작하기 ISE-PIC

관리자 액세스 콘솔

다음 단계에서는 관리 포털에 로그인하는 방법을 설명합니다.

시작하기 전에

Cisco ISE-PIC를 올바르게 설치(또는 업그레이드)하고 구성했는지 확인합니다. Cisco ISE-PIC의 설치, 업그레이드 및 컨피그레이션에 대한 자세한 정보와 지원은 *Identity Services Engine Passive Identity Connector(ISE-PIC)* 설치 및 관리자 가이드를 참조하십시오.

단계 **1** 브라우저의 주소 표시줄에서 Cisco ISE-PIC URL을 입력합니다(예: https://<ise 호스트 이름 또는 IP 주소>/admin/).

단계 **2** 초기 Cisco ISE 설정 중에 지정 및 구성한 사용자 이름과 대/소문자를 구분한 비밀번호를 입력합니다.

단계 **3** **Login(**로그인**)**을 클릭하거나 **Enter** 키를 누릅니다.

로그인이 실패하면 로그인 페이지에서 **Problem logging in?(**로그인하는 데 문제가 있나요**?)** 링크를 클릭하여 지침을 따릅니다.

관리자 로그인 브라우저 지원

Cisco ISE 관리 포털은 다음 HTTPS 사용 가능 브라우저를 지원합니다.

- Mozilla Firefox 61 이하 버전
- Mozilla Firefox ESR 60.9 이하 버전
- Google Chrome 84 이하 버전

ISE 커뮤니티 리소스

Adblock Plus 사용 시 ISE 페이지가 완전히 로드되지 않는 경우

실패한 로그인 시도 이후에 관리자 잠금

관리자 사용자 ID의 암호를 여러 번 잘못 입력하면 지정된 시간 동안 구성에 따라 계정이 일시 중단되거나 잠기게 됩니다. 잠그도록 선택하면 관리 포털이 시스템에서 "잠금" 상태가됩니다. Cisco ISE는 서버 관리자 로그인 보고서에 로그 항목을 추가하고 해당 관리자 ID의 자격 증명을 일시 중단합니다. Cisco Identity Services Engine 설치 가이드의 "관리자 잠금에 따라 비활성화된 암호 재설정" 섹션에 설명된 대로 해당 관리자 ID의 암호를 재설정할 수 있습니다. 관리자 계정을 비활성화하기 전에 허용되는 시도 실패 횟수는 *Cisco Identity Services Engine* 관리자 가이드의 Cisco ISE-PIC에 대한 관리 액세스 섹션에 설명된 대로 구성할 수 있습니다. 관리자 사용자 계정이 잠기면 Cisco ISE는 해당 정보가 구성된 경우 연결된 관리자에게 이메일을 보냅니다.

Diffie-Hellman 알고리즘을 사용하여 SSH 키 교환 보호

Diffie-Hellman-Group14-SHA1 SSH 키 교환만 허용하도록 Cisco ISE-PIC를 구성할 수 있습니다. 이렇게 하려면 Cisco ISE-PIC CLI(Command-Line Interface) 환경 설정 모드에서 다음 명령을 입력해야 합니다.

service sshd key-exchange-algorithm diffie-hellman-group14-sha1

아래에 이 명령의 예제가 나와 있습니다.

```
ise/admin#conf t
ise/admin (config)#service sshd key-exchange-algorithm diffie-hellman-group14-sha1
```

초기 설정 및 컨피그레이션

Cisco ISE-PIC를 빠르게 사용하려면 다음 흐름을 따르십시오.

1. 라이센스를 설치하고 등록합니다. 자세한 내용은 Cisco ISE-PIC 라이센싱, 3 페이지를 참고하십시오.
2. DNS 서버를 올바르게 구성했는지 확인합니다(Cisco ISE-PIC에서의 클라이언트 머신에 대한 역방향 조회 구성 포함). 자세한 내용은 DNS 서버, 5 페이지를 참고하십시오.
3. NTP 서버의 시계 설정을 동기화합니다.
4. ISE-PIC 설정을 사용하여 초기 서비스 제공자를 구성합니다. 자세한 내용은 다음을 참조하십시오. PassiveID(패시브 ID) 설정 시작하기
5. 단일 또는 다중 가입자를 구성합니다. 자세한 내용은 다음을 참조하십시오. Subscribers(가입자)

최초 서비스 제공자와 가입자를 설정하면 추가 서비스 제공자를 쉽게 생성하고(제공자 참조) ISE-PIC에서 다른 서비스 제공자의 패시브 ID를 관리할 수 있습니다(PassiveID Work Center(패시브 ID 작업 센터)에서의 모니터링 및 문제 해결 ISE-PIC 참조).

Cisco ISE-PIC 라이센싱

Cisco ISE-PIC는 90일 평가 기간과 함께 제공됩니다. 90일 평가 라이센스 만료 후 Cisco ISE-PIC를 계속 사용하려면 라이센스를 얻어 시스템에 등록해야 합니다. ISE-PIC는 평가 라이센스 만료 90, 60, 30일 전에 사용자에게 알림을 보냅니다.

각 영구 라이센스는 단일 ISE-PIC 노드에 업로드되며 , 구축에 노트가 2개 있다면 두 번째 노드에 대한 별도의 라이센스를 받아야 합니다. 설치가 끝나면 UDI별로 별도의 라이센스를 생성한 다음 각 노드에 개별적으로 라이센스를 추가합니다.

라이센싱 설치 및 등록 흐름

1. ISE-PIC 라이센스를 설치하고 등록합니다. ISE-PIC 라이센스 설치 및 등록에 관한 자세한 내용은 라이센스 등록, 4 페이지 항목을 참조하십시오. 라이센스는 다음 시점에 설치할 수 있습니다.
   - ISE-PIC 설치 직후
   - 90일 평가 기간 중 언제든지
2. 먼저 Cisco ISE-PIC 업그레이드 라이선스를 설치한 다음 다음을 수행 하 여 기본 ISE 구축으로 쉽게 업그레이드할 수 있습니다.
   - Base ISE license(기본 ISE 라이센스)를 설치하여 이전 ISE-PIC 노드를 구축을 위한 기본 관리 노드(PAN)로 사용합니다.
   - 업그레이드된 PIC ISE-PIC 노드를 기존 ISE 구축에 추가합니다.
3. 다른 관련 라이센스(Plus, Apex, TACACs+ 등)를 설치하여 기본 ISE 구축을 쉽게 업그레이드하고 스마트 라이센싱으로 업그레이드합니다. ISE 라이센스 설치에 관한 자세한 내용은 *Cisco Identity Services Engine* 관리자 설명서를 참조하십시오.

Cisco ISE 라이센싱 패키지

표 ***1:*** 전체 ***Cisco ISE*** 라이센싱 패키지 옵션

ISE 라이센스 패키지	영구/서브스크립션**(**사용 가능한 기간**)**	포함된 **ISE** 기능	메모
ISE-PIC	영구	패시브 ID 서비스	노드당 라이센스 1개. 각 라이센스는 병렬 세션을 3,000개까지 지원합니다.

ISE-PIC upgrade	영구	이 라이센스는 다음 옵션을 허용합니다. • 추가(최대 300,000개) 병렬 세션을 활성화합니다. • 전체 ISE 인스턴스로 업그레이드	노드당 라이센스 1개. 각 라이센스는 병렬 세션을 300,000개까지 지원합니다. 이 라이센스를 설치하면 업그레이드된 노드가 기존 ISE 구축에 가입할 수 있습니다. 기본 라이센스를 노드에 설치하여 PAN으로 작동하게 할 수도 있습니다.
Base	영구	• 기본 네트워크 액세스: AAA, IEEE-802.1X • 게스트 서비스 • 링크 암호화(MACSec) • TrustSec • ISE 애플리케이션 프로그래밍 인터페이스	
평가	임시(90일)	90일 동안 전체 ISE-PIC 기능을 활성화합니다.	

라이센스 등록

시작하기 전에

ISE-PIC 설치가 끝나면 90일 평가 기간이 진행됩니다. 작업을 원활하게 진행하려면 ISE-PIC 라이센스를 구매, 등록 및 설치해야 합니다. 만료일 전에 라이센서를 등록하고 설치하지 않고 만료일 후에 ISE-PIC에 액세스하면, 모든 ISE-PIC 서비스가 비활성화되고 프로세스를 완료할 수 있는 **Import License(**라이센스 가져오기**)** 영역으로 자동 이동합니다. ISE-PIC 라이센스 관련 문의는 Cisco 파트너/계정 팀에 하십시오.

단계 **1** Cisco 웹사이트(www.cisco.com)의 주문 시스템(CCW - Cisco Commerce Workspace)에서 필요한 라이센스를 주문할 수 있습니다. 구축 내 ISE-PIC 노드별로 라이센스가 하나씩 필요합니다(구축별로 노드 최대 2개).

약 1시간 후에 PAK(Product Authorization Key)가 포함된 확인 이메일이 전송됩니다.

단계 **2** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Licensing(**라이센싱**)**. **Licensing Details(**라이센싱 세부사항**)** 섹션에서 PID(Product Identifier), VID(Version Identifier), SN(Serial Number) 등의 노드 정보를 적어 둡니다.

단계 **3** www.cisco.com/go/licensing으로 이동한 다음 메시지가 표시되면 받은 라이센스의 PAK, 노드 정보 및 회사에 대한 몇 가지 세부사항을 입력합니다.

1일 후에 Cisco에서 라이센스 파일을 전송합니다.

단계 **4** 시스템에서 쉽게 확인할 수 있는 위치에 이 라이센스 파일을 저장합니다.

단계 **5** Cisco ISE-PIC 관리 포털에서 다음을 선택합니다. **Administration(**관리**)** > **Licensing(**라이센싱**)**.

단계 **6** **Licenses(**라이센스**)**섹션에서 **Import License(**라이센스 가져오기**)** 버튼을 클릭합니다.

단계 **7** **Choose File(**파일 선택**)**을 클릭하고 이전에 시스템에 저장한 라이센스 파일을 선택합니다.

단계 **8** **Import(**가져오기**)**를 클릭합니다.

이제 새 라이센스가 시스템에 설치되었습니다.

다음에 수행할 작업

라이센싱 대시보드, **Administration(**관리**)** > **Licensing(**라이센싱**)**을 선택하고 새로 입력한 라이센스가 올바른 세부사항과 함께 표시되는지 확인합니다.

라이센스 제거

시작하기 전에

만료되었거나 불필요한 라이센스를 제거하면 팝업 알림이 표시되지 않으며 라이센싱 대시보드에서 공간이 확보됩니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Licensing(**라이센싱**)**

단계 **2** **License Files(**라이센스 파일**)** 섹션에서 관련 파일 이름 옆의 확인란을 클릭하고 **Delete License(**라이센스 삭제**)**를 클릭합니다.

단계 **3** **OK(**확인**)**를 클릭합니다.

DNS 서버

DNS 서버를 구성하는 경우 주의해야 할 사항은 다음과 같습니다.

- Cisco ISE에 구성한 DNS 서버는 사용자가 사용하려는 도메인에 대한 정방향 및 역방향 DNS 쿼리를 모두 확인할 수 있어야 합니다.
- DNS 회귀는 지연을 유발하고 심각한 성능 저하를 유발할 수 있으므로, 권한 있는 DNS 서버를 통해 Active Directory 레코드 확인하는 것이 좋습니다.
- 모든 DNS 서버는 추가 사이트 정보 사용 여부와 관계없이 DC, GC 및 KDC에 대한 SRV 쿼리에 응답할 수 있어야 합니다.
- Cisco에서는 성능 향상을 위해서는 서버 IP 주소를 SRV 응답에 추가하는 방법을 권장합니다.

- DNS 서버를 사용하여 공용 인터넷에 쿼리하면 안 됩니다. 이 경우 알 수 없는 이름을 확인해야 할 때 네트워크 관련 정보가 유출될 수 있습니다.

시스템 시간 및 NTP 서버 설정 지정

Cisco ISE-PIC에서는 최대 3개의 NTP(Network Time Protocol) 서버를 구성할 수 있습니다. NTP 서버를 사용하면 정확한 시간을 유지하고 서로 다른 표준 시간대 간에 시간을 동기화할 수 있습니다. 또한 Cisco ISE-PIC가 인증된 NTP 서버만 사용해야 하는지 여부를 지정할 수 있으며 이를 위해 인증 키를 하나 이상 입력할 수 있습니다.

모든 Cisco ISE-PIC 노드는 협정 세계시(UTC) 표준 시간대로 설정하는 것이 좋습니다. . 이 절차를 수행하면 구축 내 여러 노드의 보고서 및 로그에서 타임스탬프가 항상 동기화됩니다.

Cisco ISE는 또한 NTP 서버에 대 한 공개 키 인증을 지원 합니다. NTPv4는 대칭 키 암호화를 사용하며, 공개 키 암호화를 기반으로 하는 새로운 Autokey 스키마도 제공합니다. 공개 키 암호화는 일반적으로 대칭 키 암호화 보다 안전하다고 간주됩니다. 보안이 각 서버에서 생성하며 절대로 공개되지 않는 비공개 값을 기반으로 하기 때문입니다. Autokey를 사용하면 모든 키 배포 및 관리 기능에 공개 값만 포함되며, 따라서 키 배포 및 저장이 대폭 간소화됩니다.

Configuration Mode(구성 모드)에서 Cisco ISE CLI의 NTP 서버용 Autokey를 구성할 수 있습니다. 가장 많이 사용하는 IFF(Friend 또는 Foe 식별) 식별 스키마 사용을 권장합니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Settings(**설정**)** > **System Time(**시스템 시간**)**

단계 **2** NTP 서버의 고유한 IP 주소(IPv4/IPv6/FQDN)를 입력합니다.

단계 **3** Cisco ISE가 인증된 NTP 서버만 사용하여 시스템 및 네트워크 시간을 유지하도록 제한하려면 **Only allow authenticated NTP servers(**인증된 **NTP** 서버만 허용**)** 확인란을 선택합니다.

단계 **4** (선택 사항) 개인 키를 이용하여 NTP 서버를 인증하고 싶다면 **NTP Authentication Keys(NTP** 인증 키**)** 탭을 클릭하고, 지정하는 서버에서 인증 키를 통한 인증을 수행해야 하는 경우 다음과 같이 인증 키를 하나 이상 지정합니다.

a) **Add(**추가**)**를 클릭합니다.

b) 필요한 **Key ID(**키 **ID)** 및 **Key Value(**키 값**)**을 입력합니다. 드롭다운 목록에서 **HMAC**를 선택합니다.Key ID(키 ID) 필드에는 1~65,535 사이의 숫자 값을 입력할 수 있으며 Key Value(키 값) 필드에는 영숫자 문자를 15자까지 입력할 수 있습니다.

c) NTP 서버 인증 키 입력을 완료한 후 NTP Server Configuration(NTP 서버 컨피그레이션) 탭으로 돌아옵니다.

단계 **5** (선택 사항) 공개 키 인증을 사용하여 NTP 서버를 인증하려는 경우 CLI(command-line interface)의 Cisco ISE에서 Autokey를 구성합니다. 자세한 내용은 해당 ISE 릴리스용 Cisco Identity Services Engine CLI 참조 가이드에서 **ntp server** 및 **crypto** 명령을 참조하십시오.

단계 **6** **Save(**저장**)**를 클릭합니다.

ISE-PIC Home(홈) Dashboard(대시보드)

Cisco ISE-PICHome(홈) 대시보드에는 상관관계가 분석되고 통합된 요약 및 통계 데이터가 표시되는데, 이는 효과적인 모니터링 및 문제 해결을 위해서는 필수적이며 실시간으로 업데이트됩니다. dashlet에서는 별도의 설명이 없는 한 지난 24시간 동안의 활동을 표시합니다.

- **Main(**기본**)** 보기에는 선형 메트릭 대시보드, 차트 dashlet 및 목록 dashlet이 있습니다. ISE-PIC에서는 dashlet을 구성할 수 없습니다. 일부 dashlet은 비활성화되어 있으며 ISE의 전체 버전에서만 사용할 수 있습니다. 엔드포인트 데이터를 표시하는 dashlet을 예로 들 수 있습니다. 제공되는 dashlet은 다음과 같습니다.
  - **Passive Identity Metrics(**패시브 **ID** 메트릭**)** - 현재 추적 중인 총 고유 라이브 세션 수, 시스템에 구성된 총 ID 제공자 수, ID 데이터를 능동적으로 전달하는 총 에이전트 수, 현재 구성된 총 가입자 수를 표시합니다.
  - **Provider(**제공자**)** - 제공자는 사용자 ID 정보를 ISE-PIC에 제공합니다. 제공자 소스에서 정보를 수신하는 데 사용할 ISE-PIC 프로브(주어진 소스에서 데이터를 수집하는 메커니즘)를 구성합니다. 예를 들어 AD(Active Directory) 프로브와 에이전트 프로브는 각기 다른 기술을 사용하여 ISE-PIC가 AD에서 데이터를 수집하는 데 도움을 주는 한편, 시스템 로그 프로브는 시스템 로그 메시지를 읽는 파서에서 데이터를 수집합니다.
  - **Subscribers(**가입자**)** - 가입자는 사용자 ID 정보를 검색하기 위해 ISE-PIC에 연결합니다.
  - OS Types (OS 유형)-표시 할 수있는 OS 유형은 Windows뿐입니다. Windows 유형은 Windows 버전별로 표시됩니다. 제공자는 OS 유형을 보고하지 않지만 ISE-PIC는 Active Directory를 쿼리하여 해당 정보를 가져올 수 있습니다. dashlet에는 최대 1,000개의 항목이 표시됩니다. 이보다 많은 엔드 포인트가 있거나 Windows보다 많은 OS 유형을 표시하려는 경우 ISE로 업그레이드 할 수 있습니다.
  - **Alarms(**알람**)** - 사용자 ID 관련 알람입니다.
- **Additional(**추가**)** 보기에는 PIC의 활성 세션 및 PIC 시스템의 시스템 요약이 표시됩니다.