ISE 오프라인 및 온라인에서 포스처 업데이트 수행

목차

소개

이 문서에서는 Cisco ISE(Identity Services Engine®)에서 포스처 업데이트를 수행하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 Posture Flow에 대한 지식이 있는 것을 권장합니다.

사용되는 구성 요소

이 문서의 정보는 이러한 하드웨어 및 소프트웨어 버전을 기반으로 합니다.

- Cisco Identity Services Engine 3.2 이상 버전.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

상태 업데이트에는 Windows 및 MacOS 운영 체제에 대한 안티바이러스 및 안티스파이웨어에 대한 사전 정의된 검사, 규칙 및 지원 차트와 Cisco에서 지원하는 운영 체제 정보가 포함됩니다.

네트워크에 Cisco ISE를 처음 구축 할 때 웹에서 상태 업데이트를 다운로드 할 수 있습니다. 이 프로세스는 일반적으로 약 20분 정도 소요됩니다. 초기 다운로드 후, Cisco ISE가 증분 업데이트를 확인하고 자동으로 수행 하도록 다운로드 할 수 있습니다.

Cisco ISE는 초기 상태 업데이트 중에 한 번만 기본 상태 정책, 요구 사항 및 교정을 만듭니다. 삭제할 경우 Cisco ISE는 후속 수동 업데이트 또는 예약된 업데이트 중에 다시 생성하지 않습니다.

수행할 수 있는 포스처 업데이트에는 두 가지 유형이 있습니다.

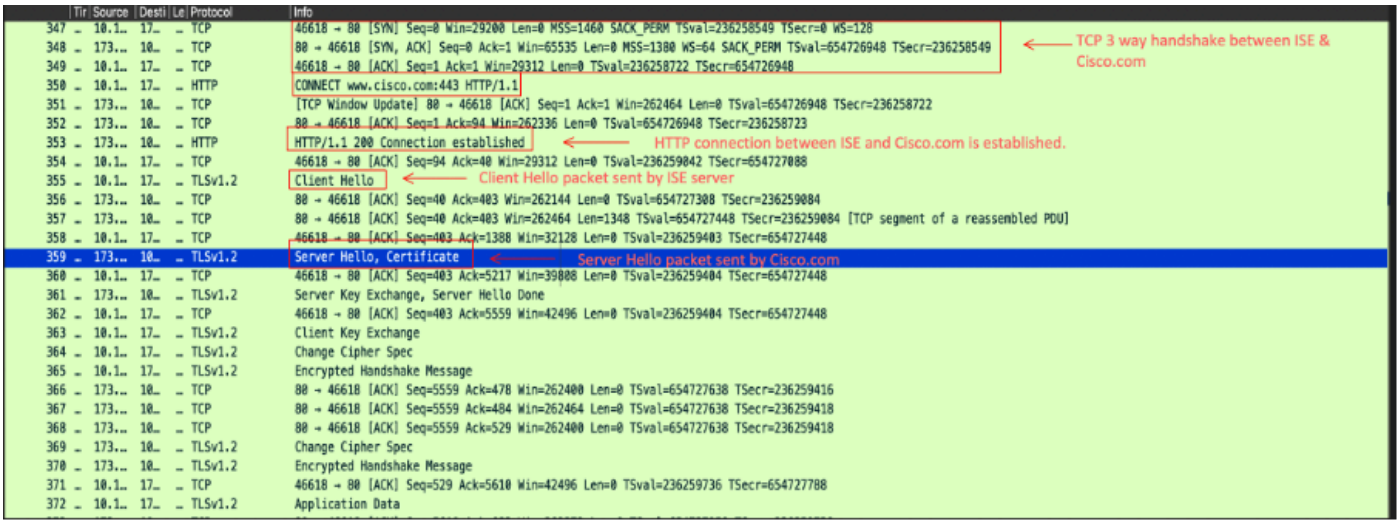
- 온라인 상태 업데이트.
- 오프라인 상태 업데이트.

온라인 상태 업데이트

Web Posture Update/Online Posture Update는 Cisco 클라우드 또는 서버 저장소에서 최신 상태 업데이트를 검색합니다. 여기에는 Cisco 서버에서 직접 최신 정책, 정의 및 서명을 다운로드하는 작업이 포함됩니다. ISE는 최신 상태 정의, 정책 및 기타 관련 파일을 검색하려면 Cisco 클라우드 서버에 연결하거나 리포지토리를 업데이트해야 합니다.

웹 또는 온라인 상태 업데이트 중에 발생하는 일?

ISE(Identity Services Engine)는 프록시 또는 HTTP를 사용하는 직접 인터넷 연결을 통해 Cisco 웹 사이트에 액세스하여 www.cisco.com과의 연결을 설정합니다. 이 과정에서 클라이언트 hello와 서버 hello 교환이 수행되며, 서버는 인증서를 제공하여 합법성을 검증하고 클라이언트 측 신뢰를 확인합니다. 클라이언트 hello 및 서버 hello가 완료되면 클라이언트 키 교환이 수행되고 서버가 포스처 업데이트를 시작합니다. 다음은 Online Posture 업데이트 중에 ISE 서버와 Cisco.com 간의 통신을 보여주는 패킷 캡처입니다.



- Server Hello 중에 Cisco.com은 클라이언트 측 트러스트를 확인하기 위해 이러한 인증서를 클라이언트로 전송합니다.

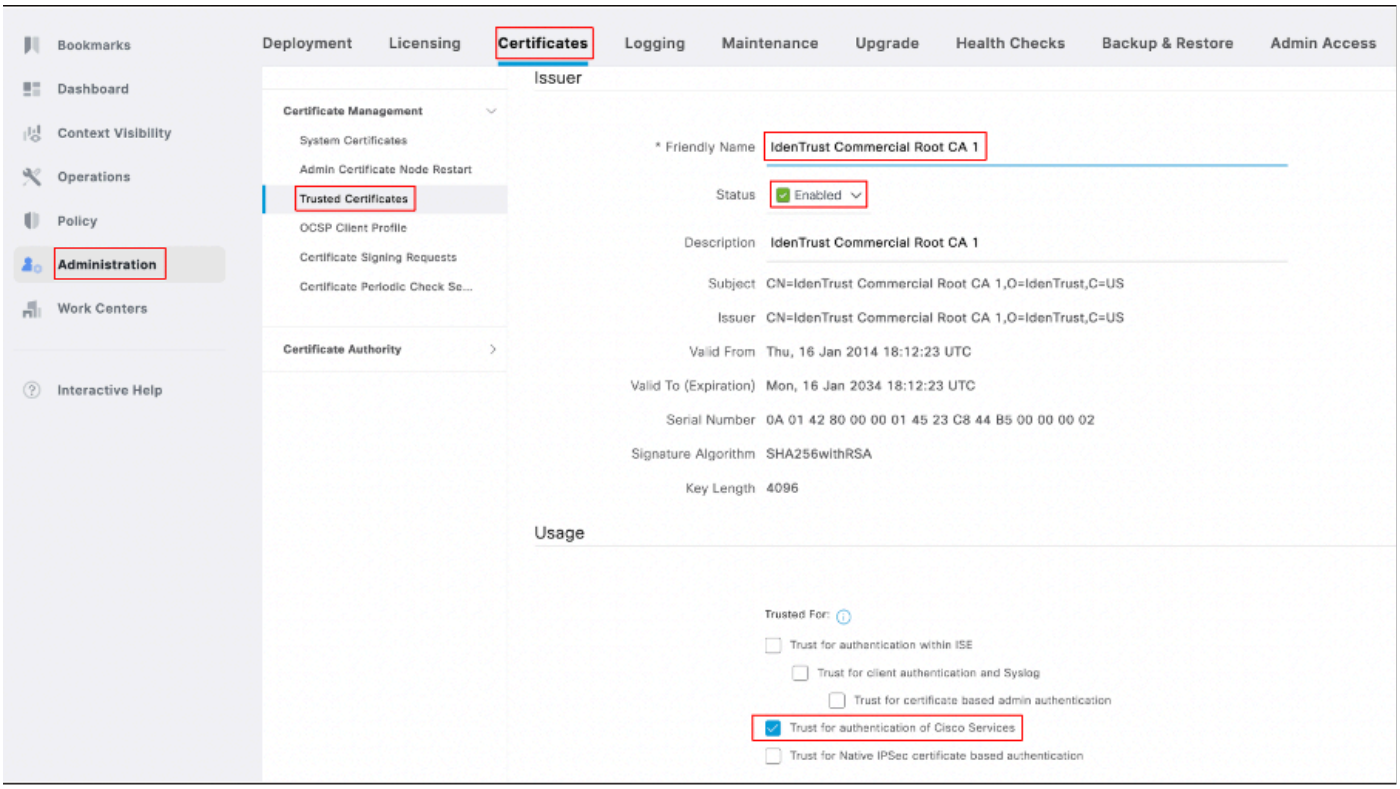

```
Certificates Length: 5083
Certificates (5083 bytes)
Certificate Length: 1940
Certificate: 3082079030820678a003020102021040191d1f3c7ec4ea73b301be3e06a90300d06092a… (id-at-commonNam
Certificate Length: 1754
Certificate: 308206d6308204bea003020102021040016efb0a205cfaebe18f71d73abb78300d06092a… (id-at-commonNam
Certificate Length: 1380
Certificate: 3082056030820348a003020102021040142800000014523c844b500000002300d06092a… (id-at-commonNam
```

IdenTrust Commercial Root CA

1

,id-at-organizationName=IdenTrust,id-at-countryName=US)

- ISE GUI에서는 서버 인증서 IdenTrust Commercial Root CA 1이 활성화되어 있는지 확인하고 Cisco.com과의 연결을 설정하기 위해 Cisco 서비스를 인증하기 위한 Trust를 사용해야 합니다. 기본적으로 이 인증서는 ISE에 포함되어 있으며 "Trust for authenticating Cisco services(Cisco 서비스를 인증하기 위한 신뢰)"를 선택하지만, 검증하는 것이 좋습니다.
- ISE GUI > Administration(관리) > Certificates(인증서) > Trusted Certificates(신뢰할 수 있는 인증서)로 이동하여 인증서 상태 및 신뢰할 수 있는 사용을 확인합니다. 이 스크린샷과 같이 IdenTrust Commercial Root CA 1이라는 이름으로 필터링하고 인증서를 선택한 다음 이를 편집하여 트러스트 사용을 확인합니다.



- 포스처 업데이트에는 새로운 또는 수정된 포스처 정책, 새로운 안티바이러스/안티멀웨어 정의, 포스처 평가를 위한 기타 보안 관련 기준이 포함될 수 있습니다.
- 이 방법은 활성 인터넷 연결이 필요하며 일반적으로 ISE 시스템이 포스처 업데이트를 위해 클라우드 기반 리포지토리를 사용하도록 구성된 경우 수행됩니다.

사용 시기

온라인 상태 업데이트는 Cisco에서 제공하는 최신 버전을 사용하여 상태 정책, 보안 정의 및 기준을 최신 상태로 유지하려는 경우에 사용됩니다.

온라인 상태 업데이트에 사용되는 포트

ISE 시스템이 상태 업데이트를 다운로드하기 위해 Cisco 클라우드 서버에 성공적으로 연결할 수 있도록 하려면 방화벽에서 이러한 포트가 열려 있어야 하며 ISE에서 인터넷으로의 아웃바운드 통신이 허용되어야 합니다.

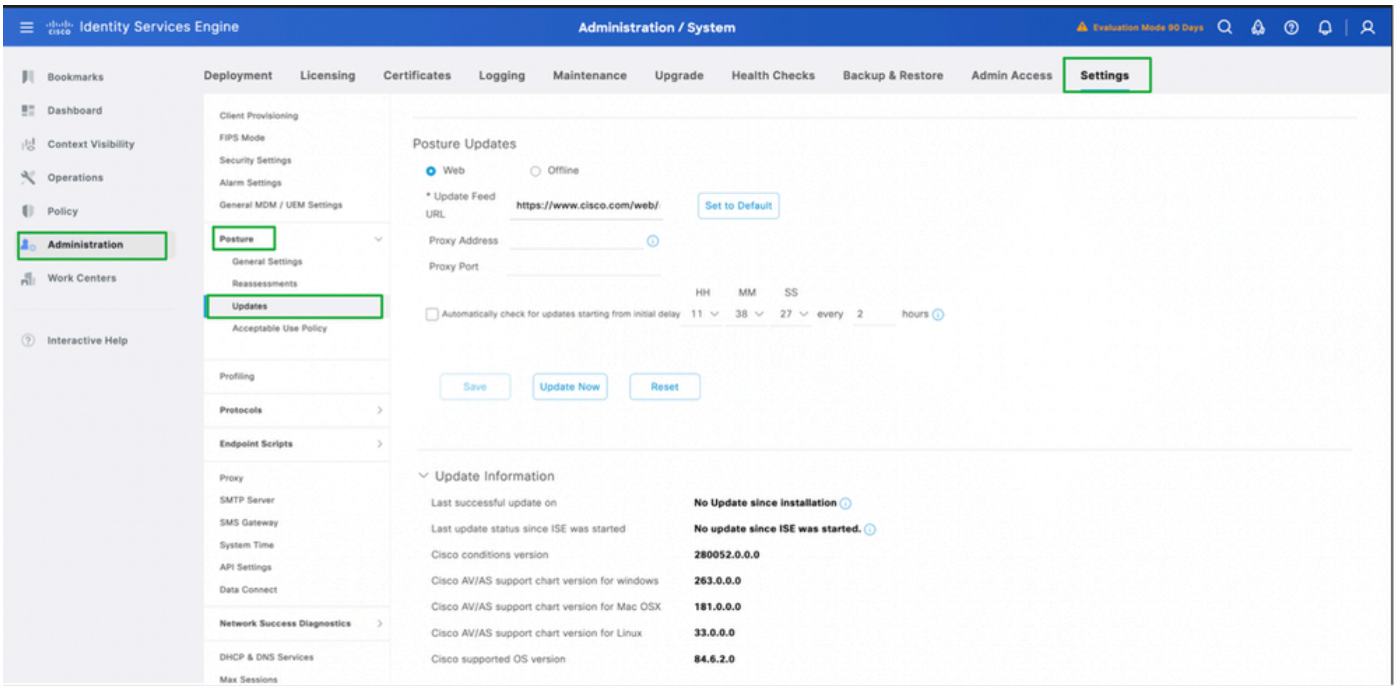
1. HTTPS(TCP 443):
   - ISE가 Cisco 클라우드 서버에 연결하고 보안 연결(TLS/SSL)을 통해 업데이트를 다운로드하기 위한 기본 포트입니다.
   - 이는 웹 기반 포스처 업데이트 프로세스에 가장 중요한 포트입니다.
2. DNS(UDP 53):
   - ISE는 업데이트 서버의 호스트 이름을 확인하기 위해 DNS 조회를 수행할 수 있어야 합니다.
   - ISE 시스템이 DNS 서버에 연결하고 도메인 이름을 확인할 수 있는지 확인합니다.
3. NTP(UDP 123):
   - ISE는 시간 동기화를 위해 NTP를 사용합니다. 이는 업데이트 프로세스가 올바르게 타임스탬프를 작성하고 ISE 시스템이 동기화된 표준 시간대에서 작동하도록 하는 데 중요

합니다.

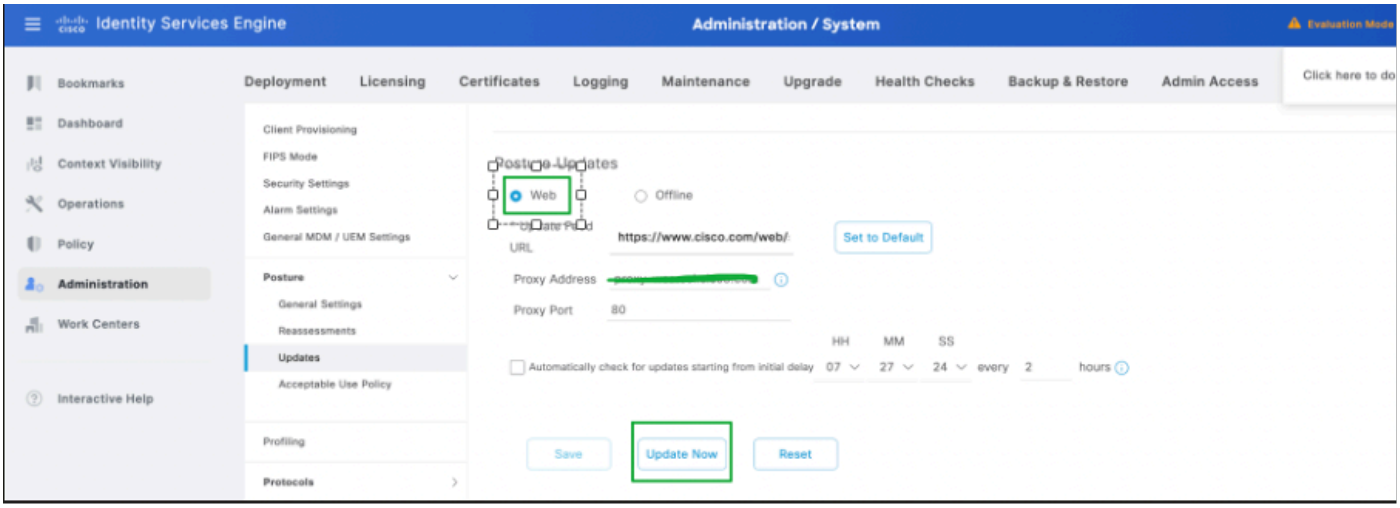
- 대부분의 경우 NTP 서버는 UDP 123을 통해 액세스할 수 있어야 합니다.

온라인 상태 업데이트를 수행하는 절차

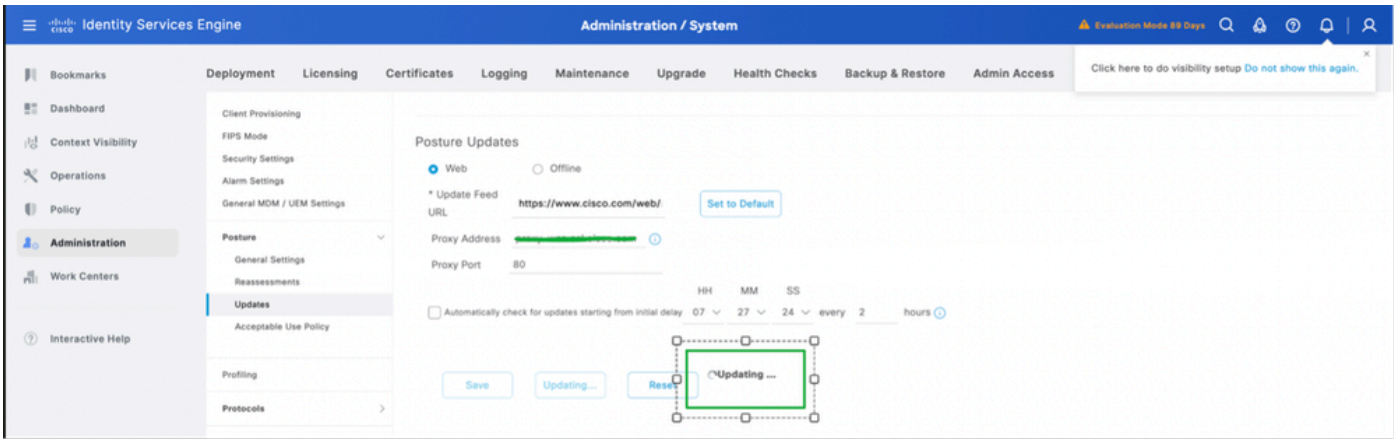
1. GUI -> Administration -> System -> Settings -> Posture -> Updates에 로그인합니다.



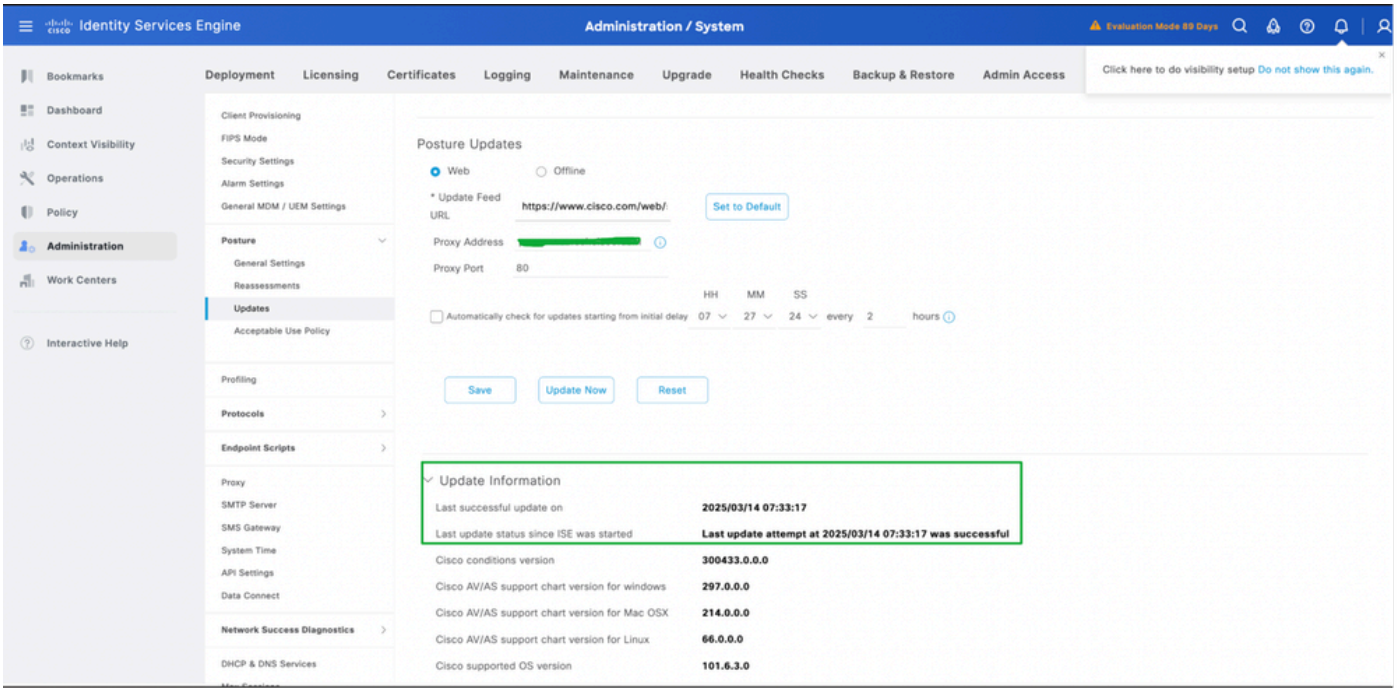
2. 온라인 상태 업데이트에 대한 웹으로 방법을 선택하고 지금 업데이트를 클릭합니다.



3. 상태 업데이트가 시작되면 상태가 업데이트로 변경됩니다.



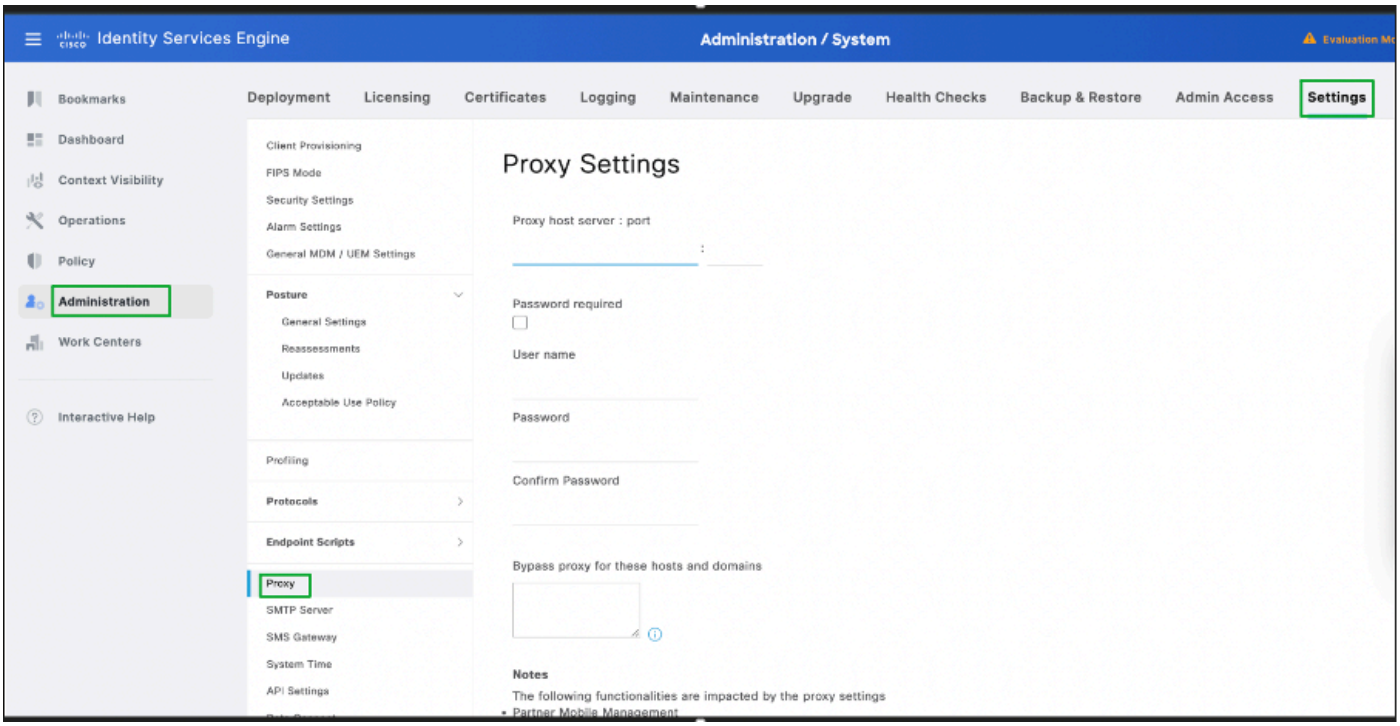
4. 상태 업데이트의 상태는 이 스크린샷에 따라 업데이트 정보에서 확인할 수 있습니다.



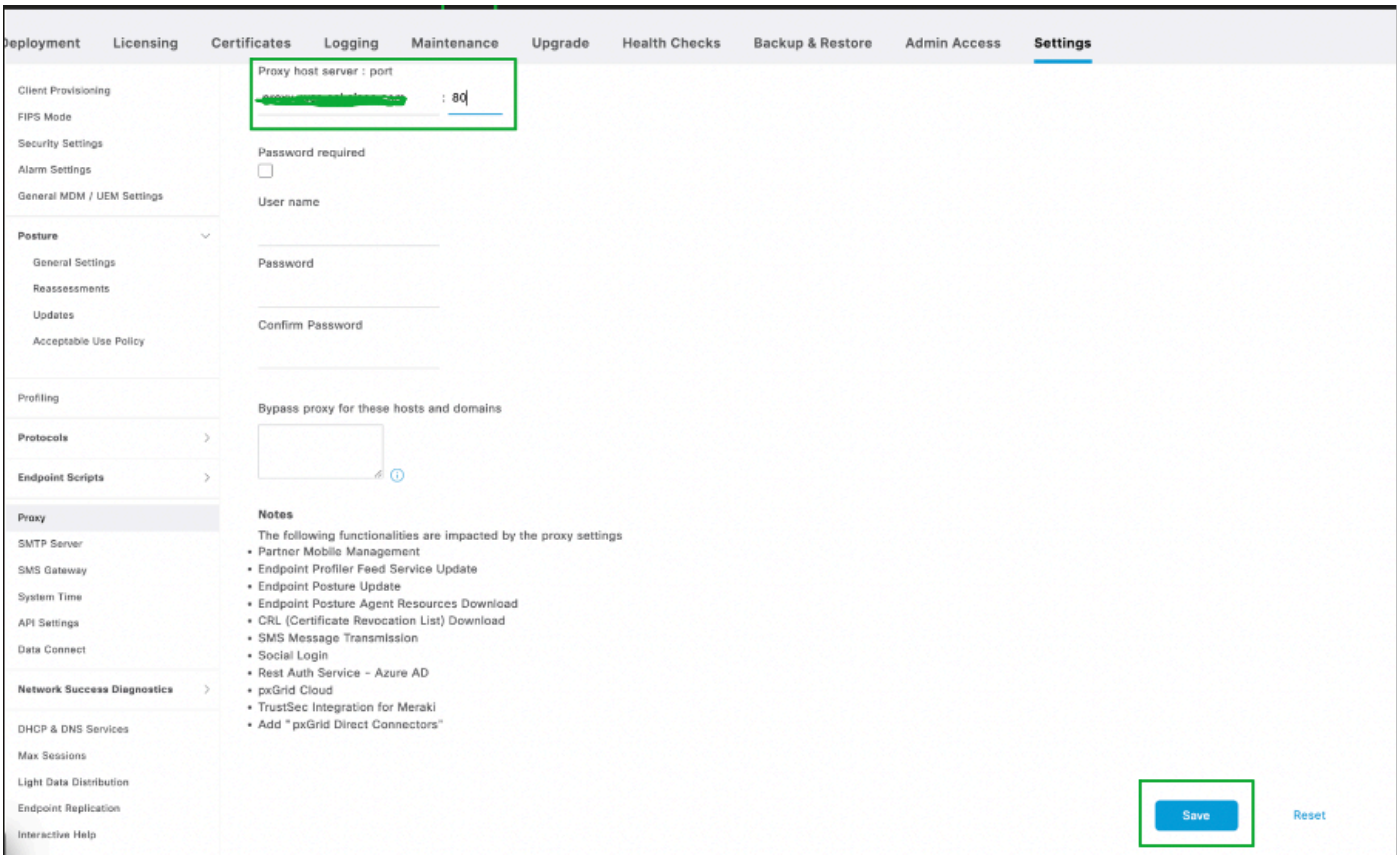
온라인 상태 업데이트를 위한 프록시 구성

Posture Update(포스처 업데이트) 필드 URL에 액세스할 수 없는 제한된 환경에서는 프록시 컨피그레이션이 필요합니다. ISE에서 프록시 구성을 참조하십시오.

1. Administration(관리) -> System(시스템) -> Settings(설정) -> Proxy(프록시)로 이동합니다.



2. 프록시 세부 정보를 구성하고 저장을 클릭합니다.



3. 온라인 상태 업데이트가 수행될 때 ISE에서 프록시의 세부사항을 자동으로 가져옵니다.

오프라인 상태 업데이트

오프라인 상태 업데이트를 사용하면 상태 업데이트 파일(.zip 또는 지원되는 다른 파일 형식)을

ISE에 수동으로 업로드할 수 있습니다.

오프라인 상태 업데이트를 수행 할 때 무슨 일이 수행 합니까?

- 업데이트된 포스처 파일을 수동으로 업로드합니다.
- ISE는 이러한 파일을 처리하고 적용합니다. 여기에는 다른 유형의 파일 중에서도 업데이트된 정책, 안티바이러스 정의, 상태 평가가 포함될 수 있습니다.
- 오프라인 업데이트는 인터넷 연결이 필요하지 않으며 일반적으로 외부 서버에 직접 액세스하지 못하도록 엄격한 보안 또는 네트워크 정책이 적용되는 환경에서 사용됩니다.

사용 시기

이 방법은 시스템이 인터넷과 격리되어 있거나 Cisco 또는 보안 팀에서 제공한 특정 오프라인 업데이트 파일이 있는 환경에서 자주 사용됩니다.

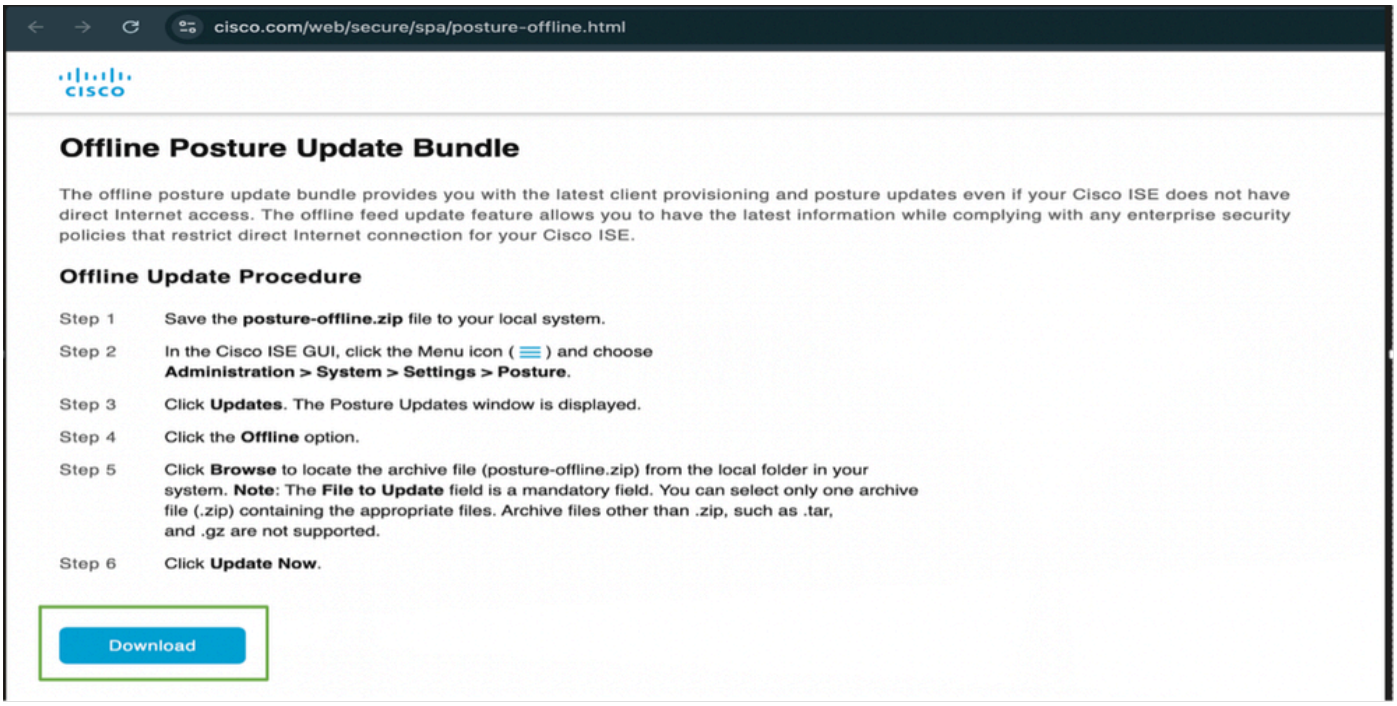
오프라인 상태 업데이트에 사용되는 포트

(업데이트 프로세스 중에) ISE 서버와의 일반적인 통신을 위해, 대부분의 경우 이러한 포트가 관련됩니다.

1. 관리 액세스(포트 22, 443):
   - SSH(TCP 22): SSH를 사용하여 문제 해결 또는 수동 업로드를 위해 ISE 시스템에 액세스하는 경우.
   - HTTPS(TCP 443): 업데이트 업로드에 GUI(웹 인터페이스)를 사용하는 경우.
2. 파일 전송(SFTP 또는 SCP):
   - SFTP 또는 SCP를 통해 ISE에 파일을 수동으로 업로드해야 하는 경우 ISE 시스템에서 해당 포트(일반적으로 SSH/SFTP의 경우 포트 22)가 열려 있는지 확인합니다.
3. 로컬 네트워크 액세스:
   - 업데이트를 업로드하는 시스템(예: 관리 워크스테이션 또는 서버)이 관리 액세스에 필요한 포트를 통해 ISE와 통신할 수 있는지 확인합니다. 그러나 오프라인 상태 업데이트는 파일이 수동으로 제공되므로 외부 포트가 필요하지 않습니다.

오프라인 상태 업데이트에 대한 파일을 찾는 위치?

1. URL로 이동: https://www.cisco.com/web/secure/spa/posture-offline.html에서 Download를 클릭하면 posture-offline.zip 파일이 로컬 시스템에 다운로드됩니다.

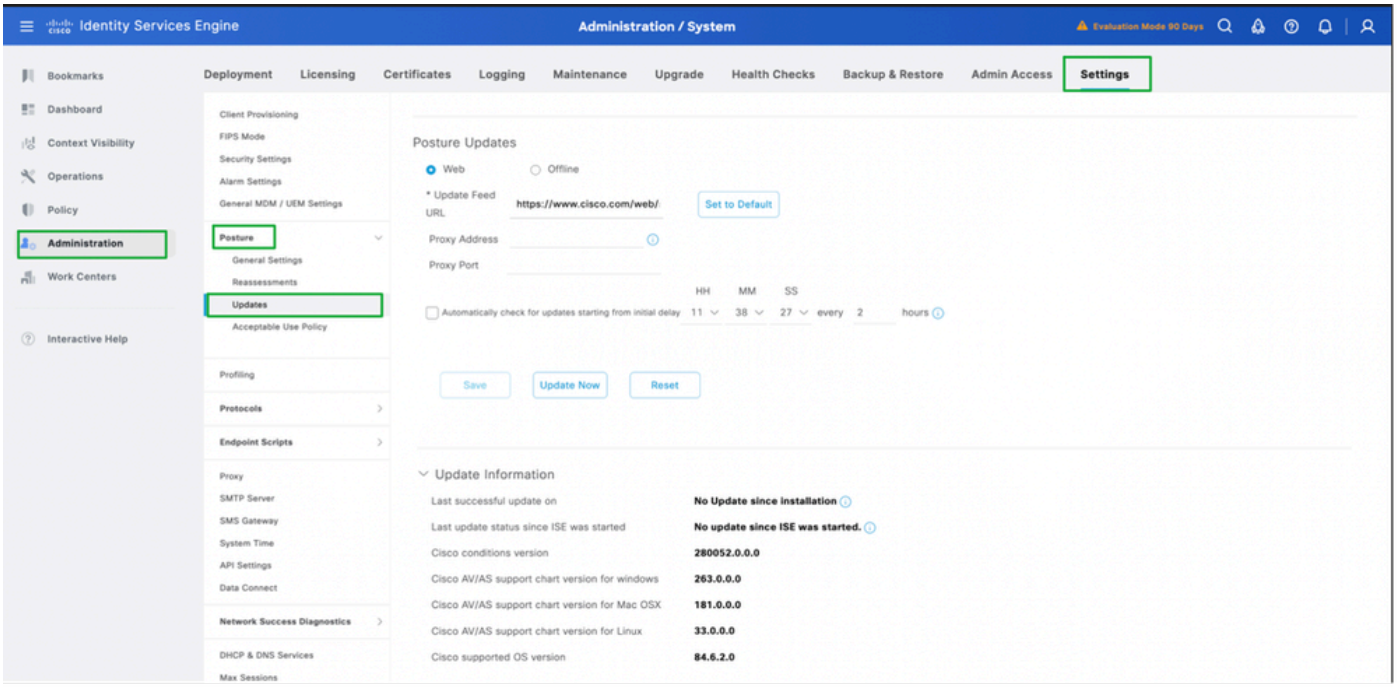


오프라인 상태 업데이트 파일 포함

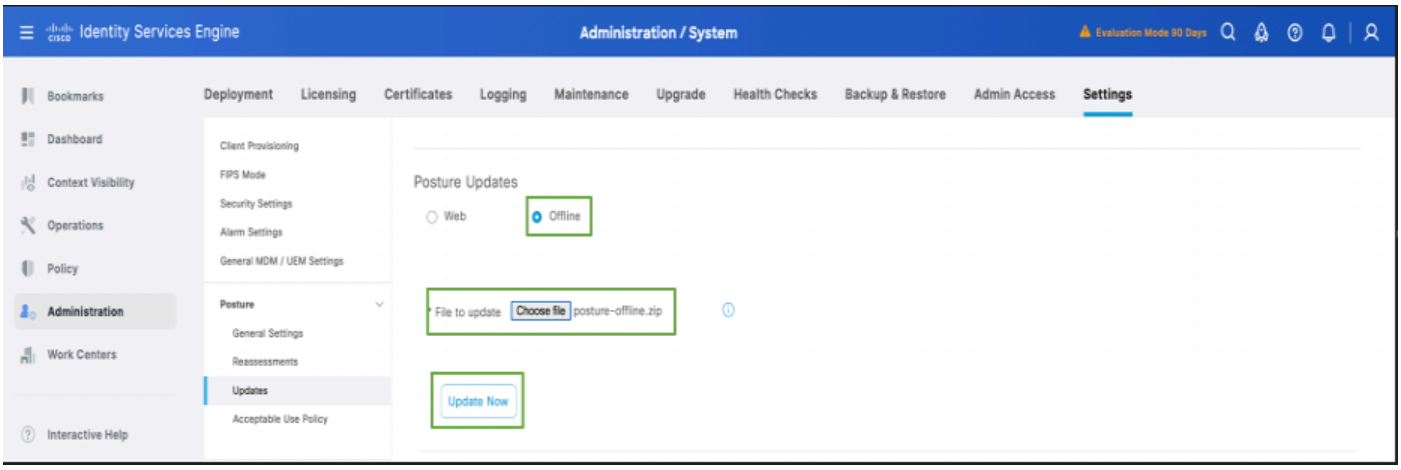
- 안티바이러스 정의(서명).
- 상태 정책 및 규칙.
- 보안 평가 및 상태 평가를 위한 기타 구성 파일

오프라인 상태 업데이트를 수행 하는 절차

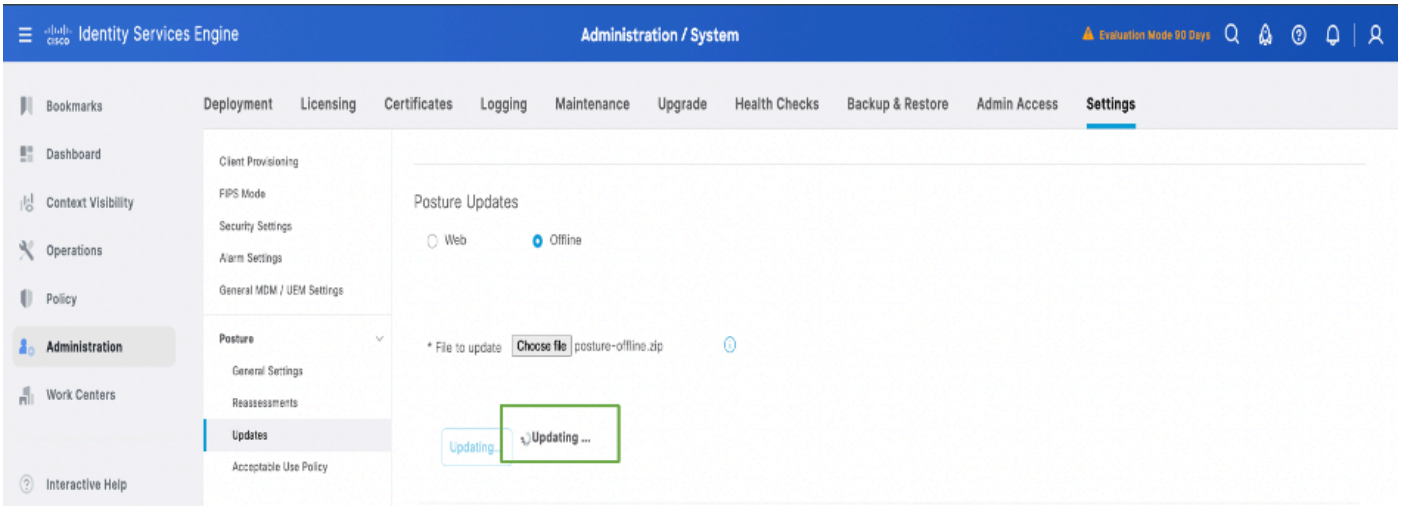
1. ISE GUI -> Administration -> System -> Settings -> Posture -> Updates에 로그인합니다.

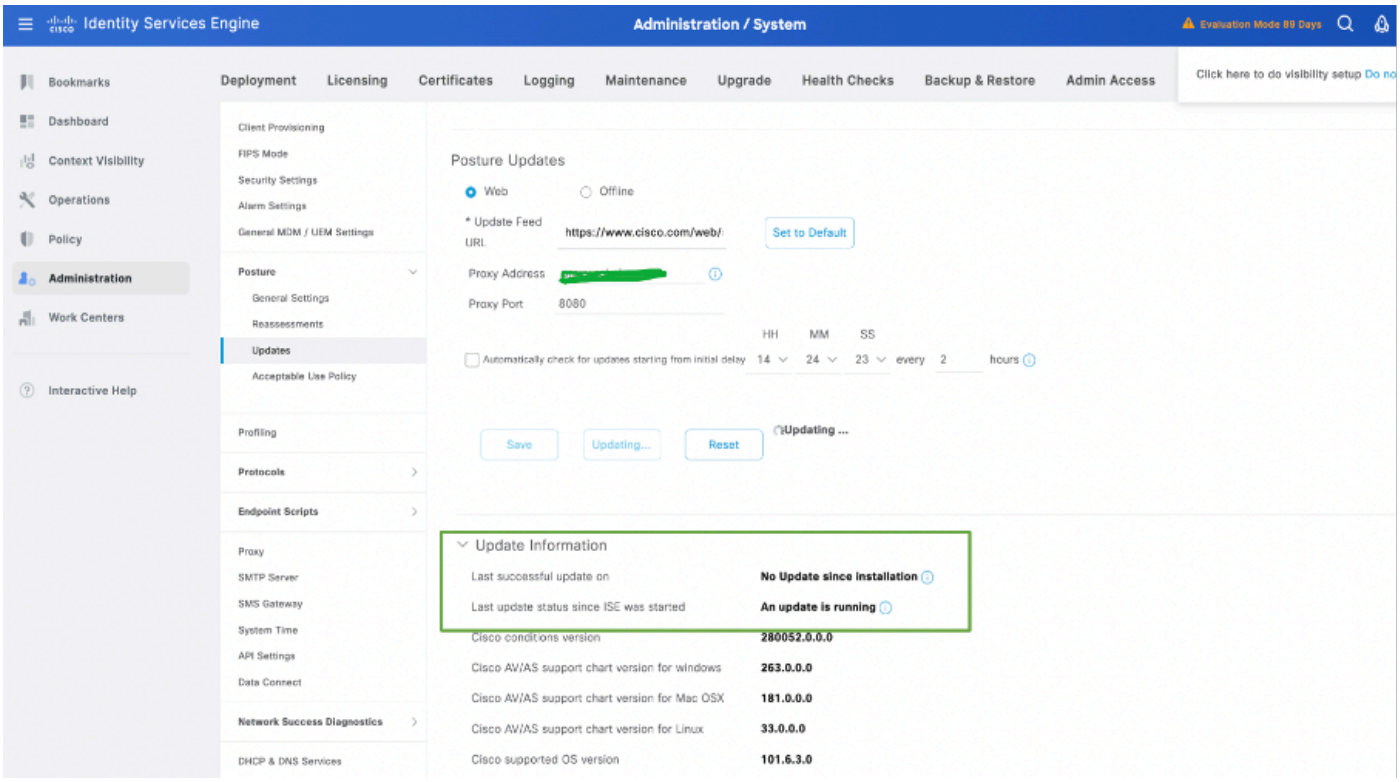


2. offline 옵션을 선택하고 로컬 시스템에 다운로드된 posture-offline.zip 폴더를 찾아 선택합니다. Update Now(지금 업데이트)를 클릭합니다.

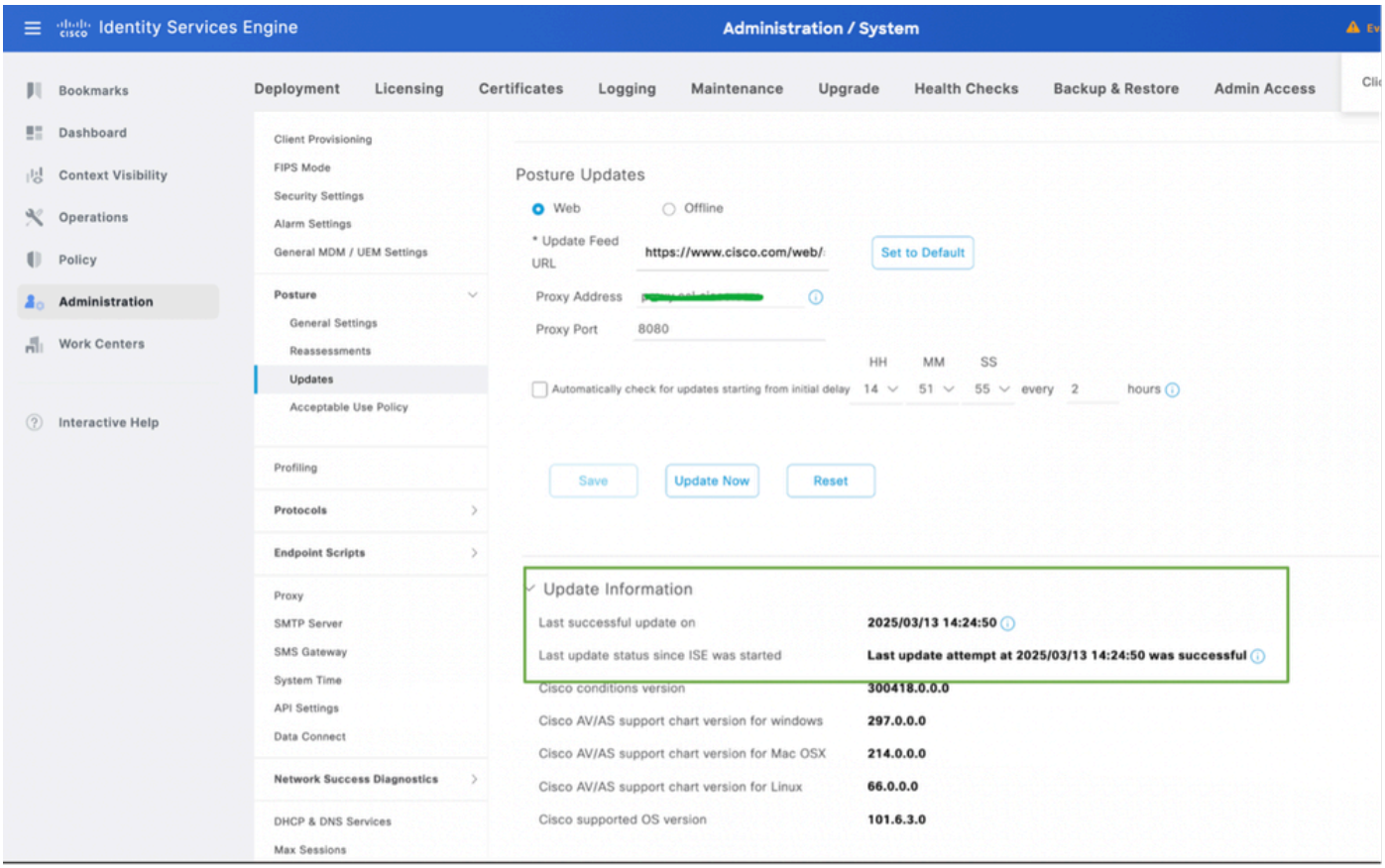


3. 상태 업데이트가 시작되면 상태가 업데이트로 변경됩니다.





4. 상태 업데이트의 상태는 이 스크린샷에 따라 업데이트 정보에서 확인할 수 있습니다.



확인

기본 관리 노드의 GUI에 로그인합니다. -> 작업 -> 문제 해결 -> 로그 다운로드 -> 디버그 로그 -> 애플리케이션 로그 -> isc-psc.log를 클릭하고 ise-psc.log를 클릭하면 로그가 로컬 시스템으로 다운로드됩니다. 다운로드한 파일을 메모장이나 텍스트 편집기를 통해 열고 Opswat 다운로드를 필터링합니다. 구축에서 수행 중인 포스처 업데이트와 관련된 정보를 찾을 수 있어야 합니다.

또한 show logging application ise-psc.log tail 명령을 사용하여 기본 관리 노드의 CLI에 로그인하여 로그를 테일링할 수 있습니다.

포스처 업데이트를 참조하여 Opswat 다운로드가 시작됩니다.

2025-03-13 13:58:07,246 정보 [admin-http-pool5][[]]
cisco.cpm.posture.download.DownloadManager -::admin::- opswat 다운로드 시작

2025-03-13 13:58:07,251 정보 [admin-http-pool5][[]]
cisco.cpm.posture.download.DownloadManager -::admin::- 오프라인 다운로드 파일 URI:
/opt/CSCOcpm/temp/cp/update/5c064701-a1ee-4a09-a190-3bf83c190af6/osgroupsV2.tar.gz

2025-03-13 13:58:07,251 정보 [admin-http-pool5][[]]
cisco.cpm.posture.download.DownloadManager -::admin::- 오프라인 다운로드 파일 URI:
/opt/CSCOcpm/temp/cp/update/5c064701-a1ee-4a09-a190-3bf83c190af6/osgroups.tar.gz

2025-03-13 13:58:07,251 정보 [admin-http-pool5][[]]

완료된 Opswat 다운로드, 상태 업데이트를 참조 하여 다운로드 및 성공.

2025-03-13 14:24:50,796 정보 [pool-25534-thread-1][[]]
mnt.dbms.datadirect.impl.DatadirectServiceImpl -:::- getStatus 실행 - datadirectSettings

2025-03-13 14:24:50,803 정보 [admin-http-pool5][[]]
cisco.cpm.posture.download.DownloadManager -::admin::- opswat 다운로드 완료

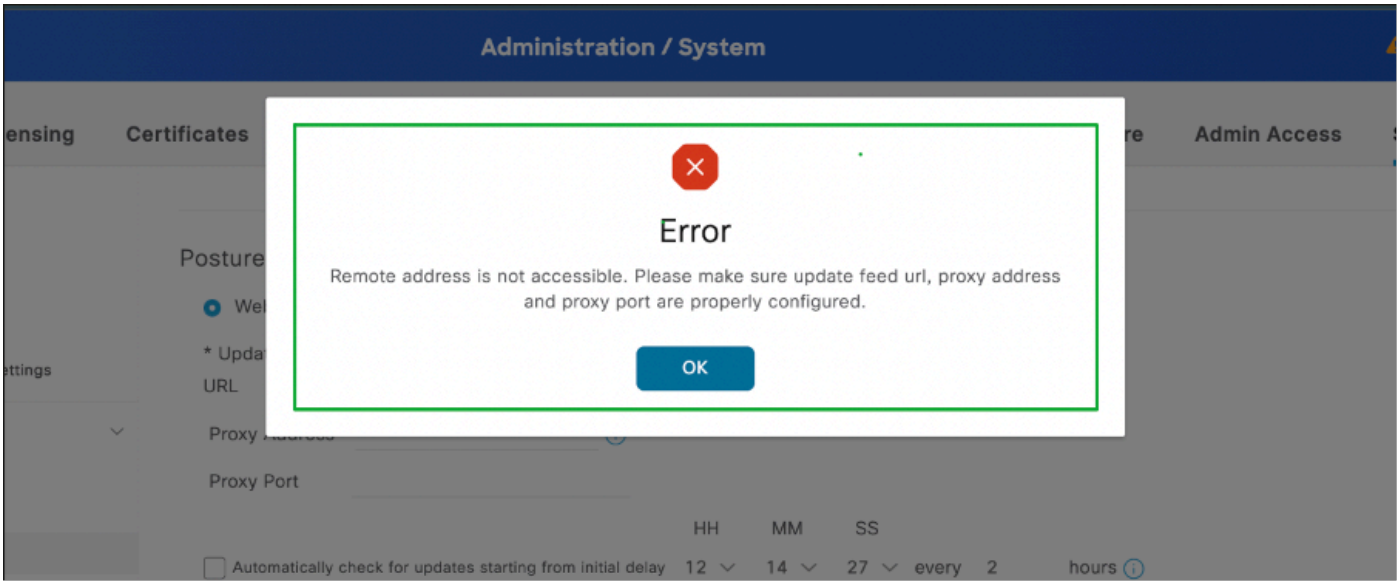
2025-03-13 14:24:50,827 정보 [admin-http-pool5][[]]
mnt.dbms.datadirect.impl.DatadirectServiceImpl -::admin::- getStatus 실행 - datadirectSettings

문제 해결

시나리오

"원격 주소에 액세스할 수 없습니다. 업데이트 피드 UR, 프록시 주소 및 프록시 포트가 올바르게 구성되었는지 확인하십시오."

샘플 오류:



솔루션

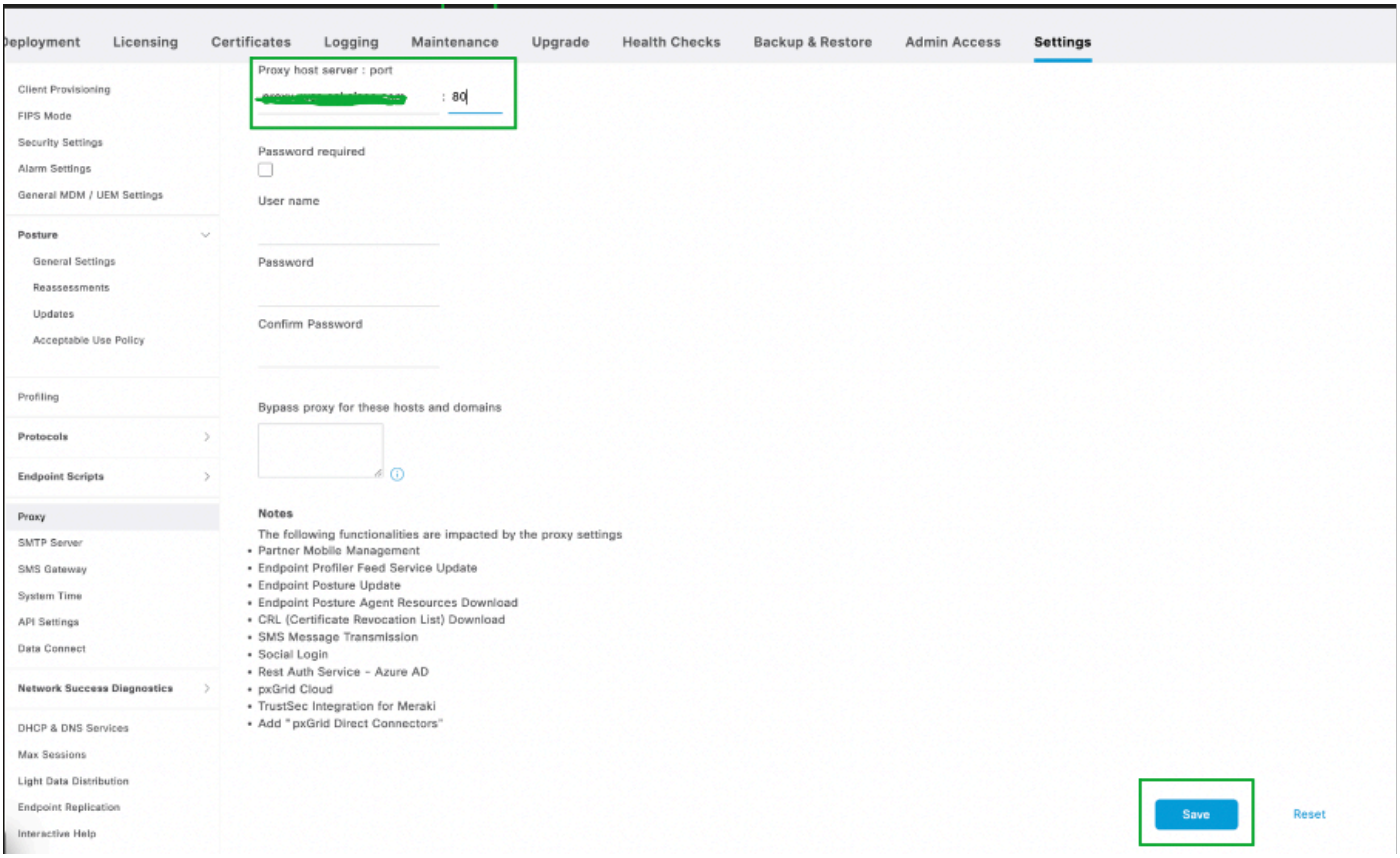
1. ISE의 CLI에 로그인하고 "ping cisco.com" 명령을 사용하여 ISE가 cisco.com에 연결할 수 있는지 확인합니다.

isehostname/admin#ping cisco.com
PING cisco.com (72.163.4.161) 56(84) 바이트의 데이터
72.163.4.161에서 64바이트: icmp_seq=1 ttl=235 시간=238ms
72.163.4.161에서 64바이트: icmp_seq=2 ttl=235 시간=238ms
72.163.4.161에서 64바이트: icmp_seq=3 ttl=235 시간=239ms
72.163.4.161에서 64바이트: icmp_seq=4 ttl=235 시간=238ms

— cisco.com ping 통계 —
전송된 패킷 4개, 수신된 패킷 4개, 0% 패킷 손실, 시간 3004ms

rtt min/avg/max/mdev = 238.180/238.424/238.766/0.410ms

2. Administration(관리) -> System(시스템) -> Settings(설정) -> Proxy is configured with appropriate ports(프록시가 적절한 포트로 구성되어 있음)로 이동합니다.



3. 인터넷에 대한 모든 홉에서 포트 TCP 443, UDP 53 및 UDP 123이 허용되는지 확인합니다.

상태 업데이트 문제에 대한 알려진 결함

Cisco 버그 ID 01523

참조

- Cisco Identity Services Engine 관리자 가이드, 릴리스 3.3

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.