Statusaktualisierungen in der ISE offline und online durchführen

Inhalt

Einleitung

In diesem Dokument wird die Durchführung von Statusaktualisierungen in der Cisco Identity Services Engine® (ISE) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse zum Fluss von Status verfügen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Hardware- und Software-Versionen.

- Cisco Identity Services Engine 3.2 und höher

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Statusaktualisierungen umfassen eine Reihe vordefinierter Prüfungen, Regeln und Support-Diagramme für Antivirus- und Antispyware-Programme für Windows- und MacOS-Betriebssysteme sowie Informationen zu Betriebssystemen, die von Cisco unterstützt werden.

Wenn Sie die Cisco ISE zum ersten Mal in Ihrem Netzwerk implementieren, können Sie Statusaktualisierungen aus dem Internet herunterladen. Dieser Vorgang dauert in der Regel etwa 20 Minuten. Nach dem ersten Download können Sie die Cisco ISE so konfigurieren, dass inkrementelle Updates automatisch überprüft und heruntergeladen werden.

Die Cisco ISE erstellt Standard-Statusrichtlinien, Anforderungen und Problembehebungen nur einmal während der ersten Aktualisierungen. Wenn Sie diese löschen, werden sie von der Cisco ISE bei späteren manuellen oder geplanten Updates nicht erneut erstellt.

Es gibt zwei Arten von Statusaktualisierungen:

- Online-Statusaktualisierungen.
- Offline-Status-Updates.

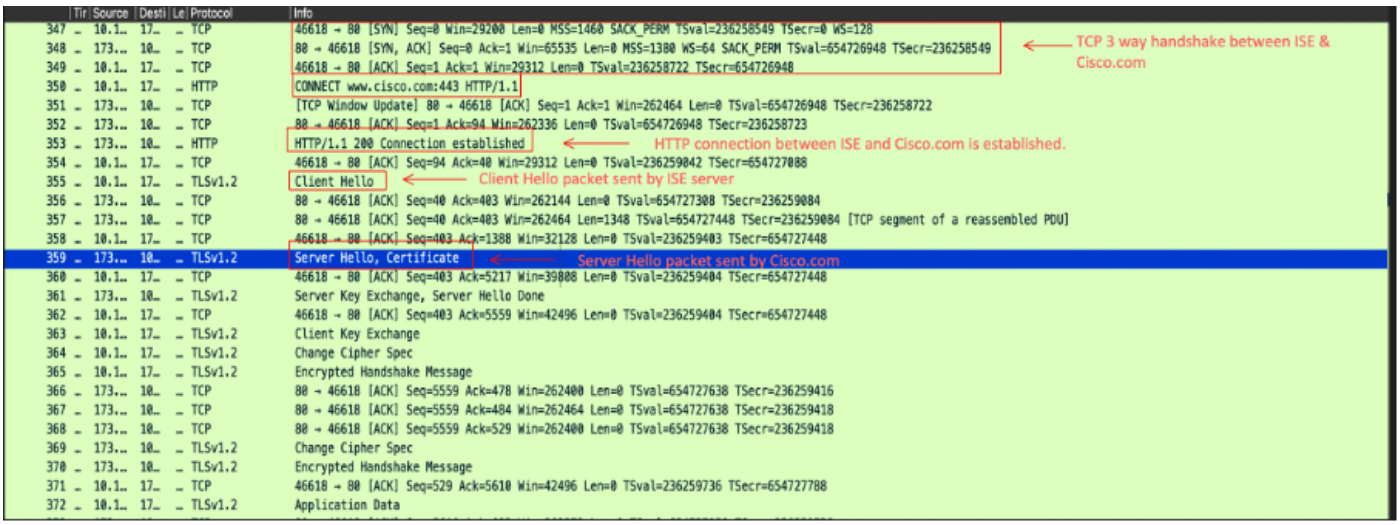
Aktualisierungen des Online-Status

Ein Web Posture Update/Online Posture Update ruft die neuesten Statusaktualisierungen aus Cisco Cloud- oder Server-Repositorys ab. Dazu müssen die neuesten Richtlinien, Definitionen und Signaturen direkt von den Cisco Servern heruntergeladen werden. Die ISE muss sich mit Cisco Cloud-Servern verbinden oder Repositorys aktualisieren, um die neuesten Statusdefinitionen, Richtlinien und andere zugehörige Dateien abzurufen.

Was passiert während der Aktualisierungen des Web- oder Online-Status?

Die Identity Services Engine (ISE) greift entweder über einen Proxy oder eine direkte Internetverbindung über HTTP auf die Cisco Website zu und stellt eine Verbindung mit www.cisco.com her. Während dieses Vorgangs findet der Client-Hello- und Server-Hello-Austausch statt, wobei der Server sein Zertifikat bereitstellt, um seine Legitimität zu überprüfen und die clientseitige Vertrauenswürdigkeit zu bestätigen. Nach Abschluss der Client-Hello- und

Server-Hello-Phase findet der Client-Key-Austausch statt, und der Server initiiert die Statusaktualisierungen. Hier sehen Sie die Paketerfassung, die die Kommunikation zwischen dem ISE-Server und Cisco.com während der Online Posture-Updates veranschaulicht.



- Während des Server Hello sendet Cisco.com diese Zertifikate an den Client, um die clientseitige Vertrauenswürdigkeit zu bestätigen.

<#root>

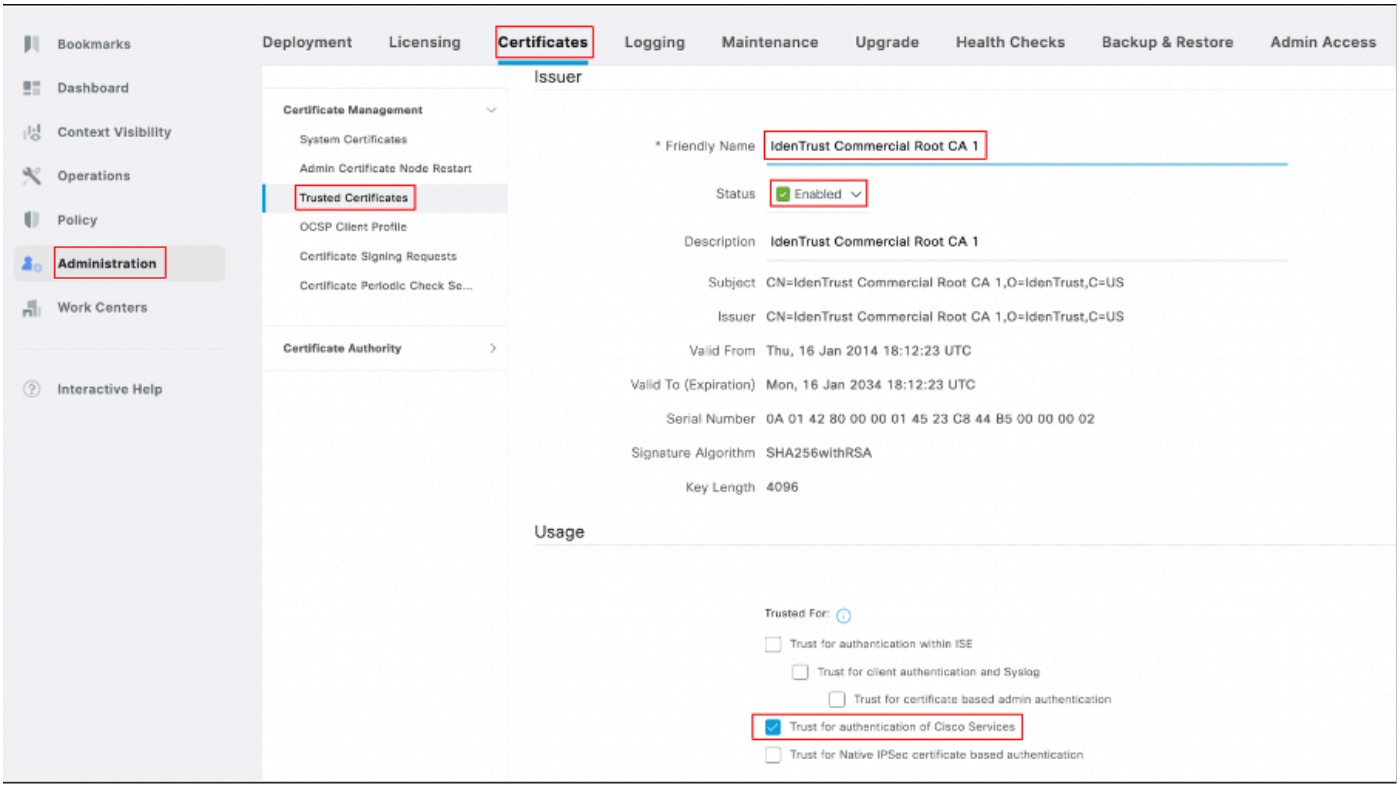
```
Certificates Length: 5083
Certificates (5083 bytes)
Certificate Length: 1940
Certificate: 3082079030820678a003020102021040191d1f3c7ec4ea73b301be3e06a90300d06092a… (id-at-commonNam
Certificate Length: 1754
Certificate: 308206d6308204bea003020102021040016efb0a205cfaebe18f71d73abb78300d06092a… (id-at-commonNam
Certificate Length: 1380
Certificate: 3082056030820348a00302010202100a0142800000014523c844b500000002300d06092a… (id-at-commonNam
```

IdenTrust Commercial Root CA

1

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

- In der ISE-GUI ist es wichtig, sicherzustellen, dass das Serverzertifikat IdenTrust Commercial Root CA 1 aktiviert ist und Trust zur Authentifizierung von Cisco Services verwendet, um die Verbindung mit Cisco.com herzustellen. Dieses Zertifikat ist standardmäßig in der ISE enthalten, und die Option "Zur Authentifizierung von Cisco Services vertrauenswürdig" ist aktiviert. Es wird jedoch zur Verifizierung geraten.
- Überprüfen Sie den Zertifikatsstatus und die vertrauenswürdige Verwendung, indem Sie zu ISE GUI > Administration > Certificates > Trusted Certificates wechseln. Filtern Sie nach dem Namen IdenTrust Commercial Root CA 1, wählen Sie das Zertifikat aus, und bearbeiten Sie es, um die Verwendung der Vertrauensstellung zu überprüfen, wie in diesem Screenshot gezeigt:



- Statusaktualisierungen können neue oder überarbeitete Statusrichtlinien, neue Antivirus-/Anti-Malware-Definitionen und andere sicherheitsrelevante Kriterien für Statusüberprüfungen enthalten.
- Diese Methode erfordert eine aktive Internetverbindung und wird in der Regel durchgeführt, wenn das ISE-System für die Verwendung Cloud-basierter Repositorys für Statusaktualisierungen konfiguriert ist.

Verwendungszweck

Online-Statusaktualisierungen werden verwendet, wenn Sie sicherstellen möchten, dass die Statusrichtlinien, Sicherheitsdefinitionen und Kriterien mit den neuesten verfügbaren Versionen von Cisco übereinstimmen.

Ports für die Online-Statusaktualisierung

Um sicherzustellen, dass das ISE-System die Cisco Cloud-Server zum Herunterladen von Statusaktualisierungen erreichen kann, müssen diese Ports in Ihrer Firewall offen sein und für ausgehende Kommunikation von der ISE zum Internet zugelassen werden:

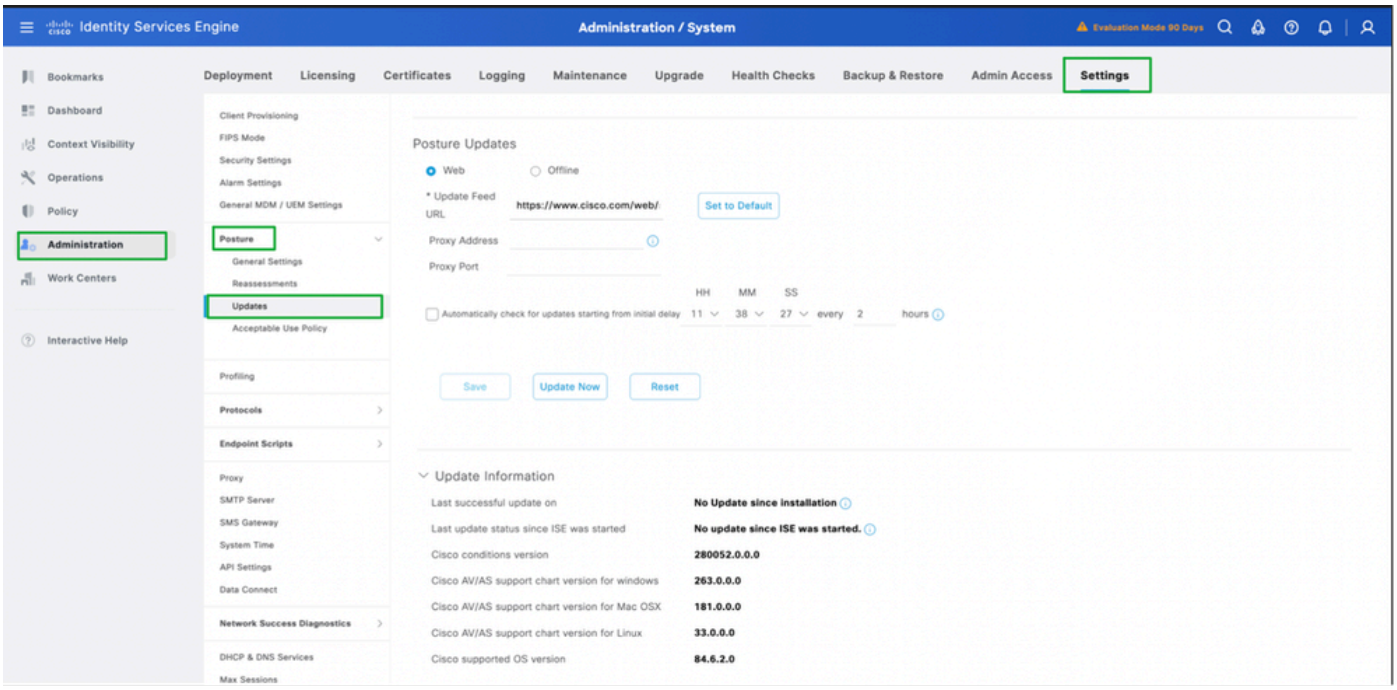
1. HTTPS (TCP 443):
    - Primärer Port für ISE zum Erreichen der Cisco Cloud-Server und Herunterladen von Updates über eine sichere Verbindung (TLS/SSL).
    - Dies ist der wichtigste Port für den webbasierten Statusaktualisierungsprozess.
2. DNS (UDP 53):
    - Die ISE muss DNS-Lookups durchführen können, um die Hostnamen der Update-Server aufzulösen.
    - Stellen Sie sicher, dass Ihr ISE-System die DNS-Server erreichen und

Domänennamen auflösen kann.

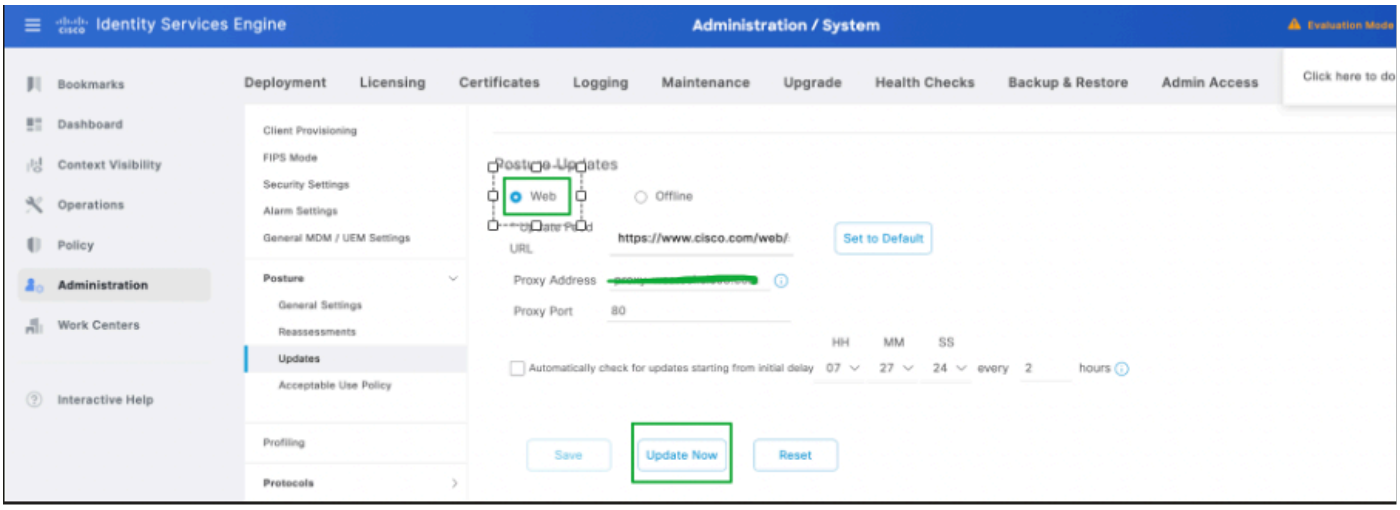
3. NTP (UDP 123):
    - Die ISE verwendet NTP für die Zeitsynchronisierung. Dies ist wichtig, um sicherzustellen, dass der Aktualisierungsvorgang korrekt mit einem Zeitstempel versehen ist und das ISE-System in einer synchronisierten Zeitzone arbeitet.
    - In vielen Fällen muss der Zugriff auf NTP-Server auch über UDP 123 möglich sein.

Verfahren zur Durchführung von Online-Statusaktualisierungen

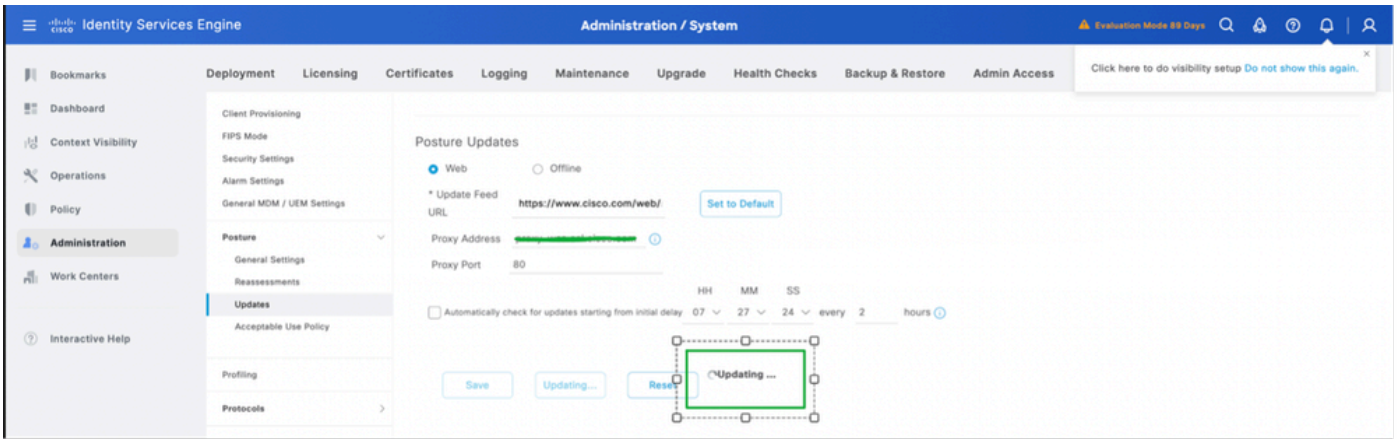
1. Melden Sie sich bei der GUI an -> Administration -> System -> Settings -> Posture -> Updates.



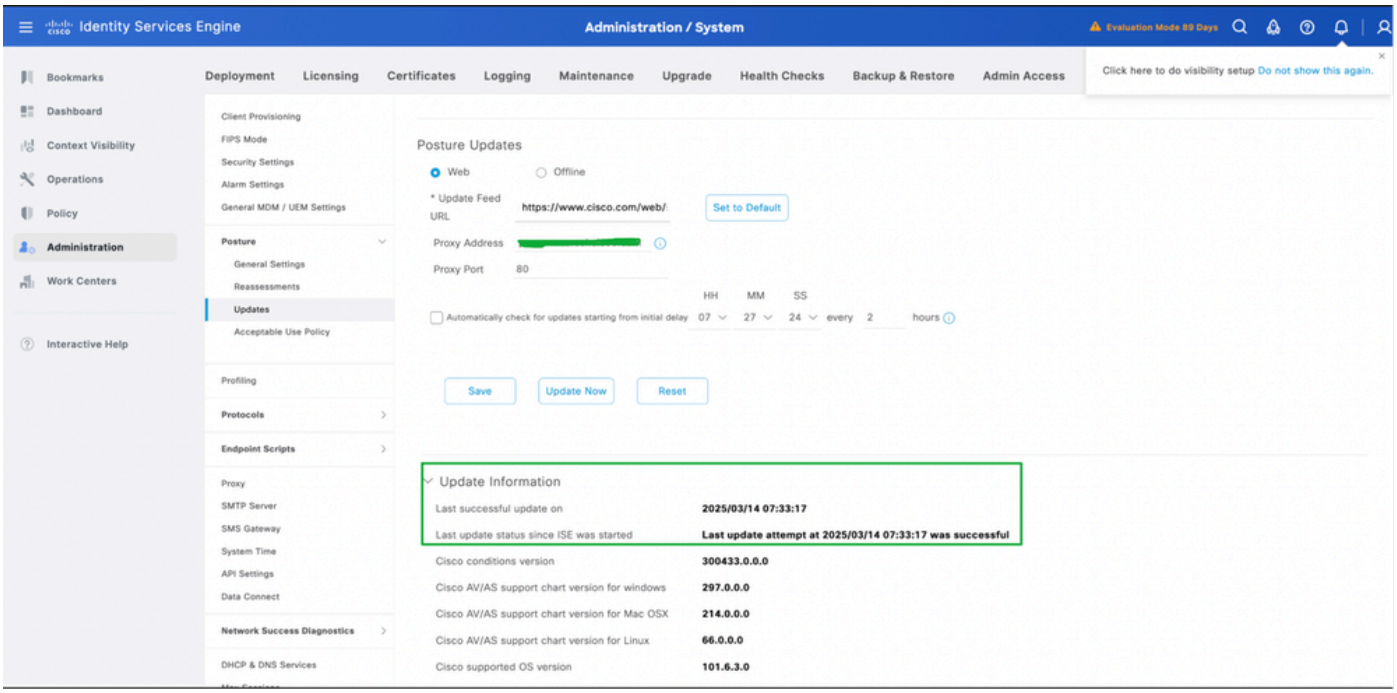
2. Wählen Sie die Methode als Web für Online-Statusaktualisierungen aus, und klicken Sie auf Jetzt aktualisieren.



3. Sobald die Statusaktualisierungen beginnen, wird der Status in Aktualisieren geändert.



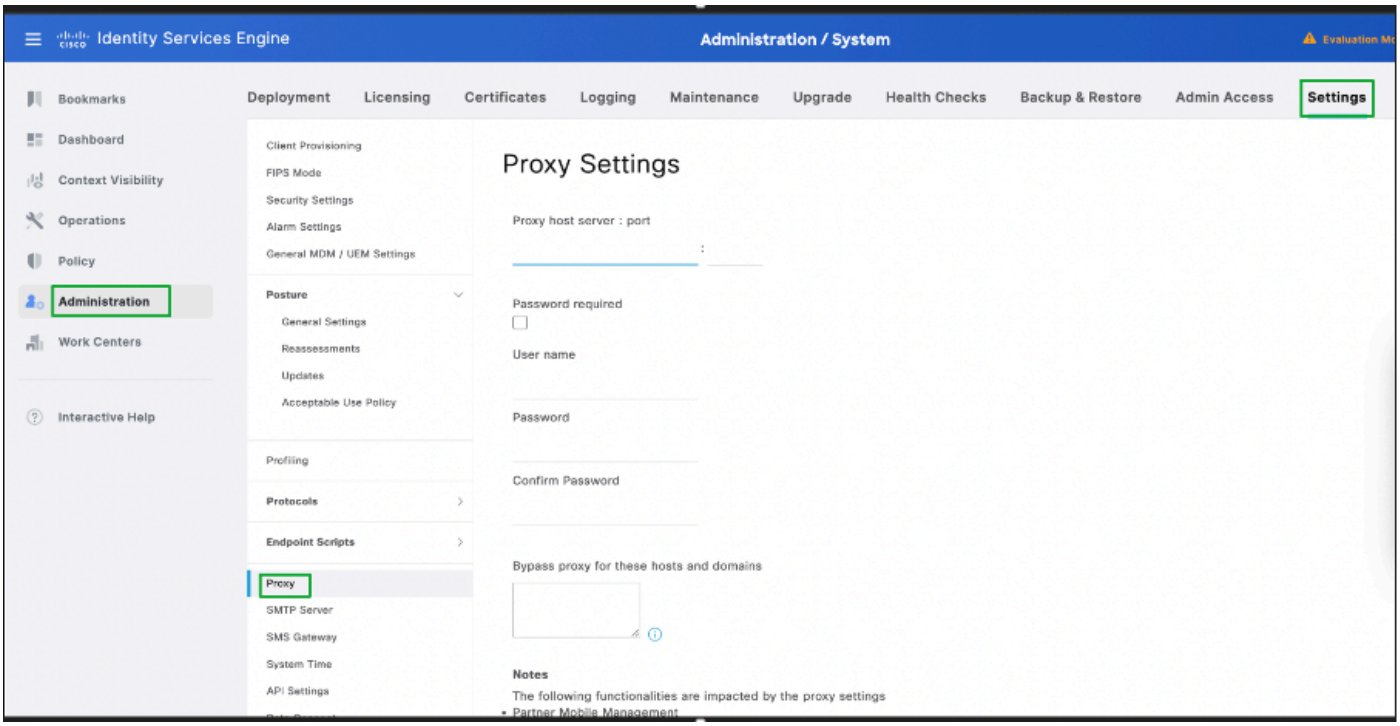
4. Der Status der Statusaktualisierungen kann anhand der Aktualisierungsinformationen wie in diesem Screenshot überprüft werden:



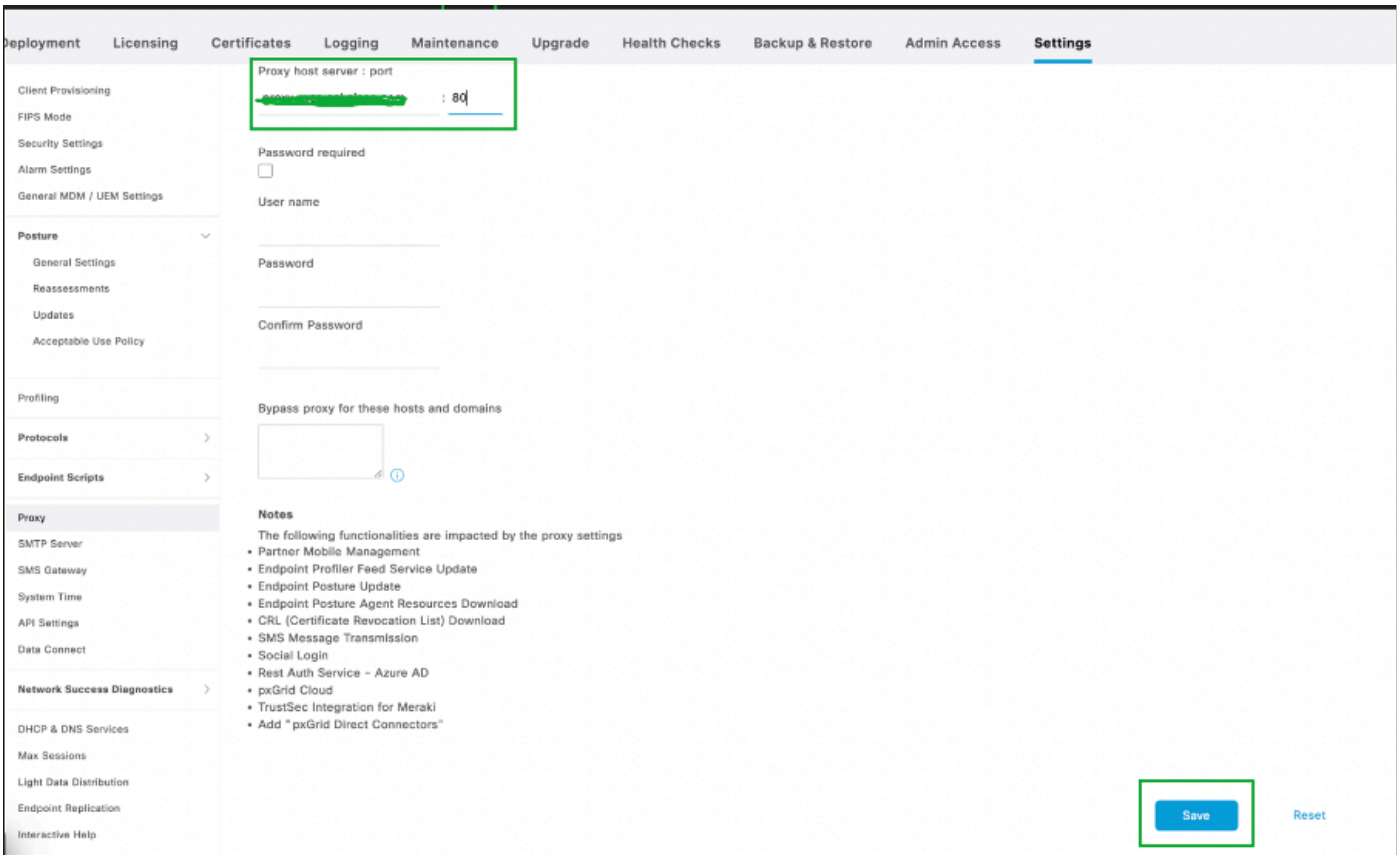
Proxykonfiguration für Online-Statusaktualisierungen

In einer eingeschränkten Umgebung, in der der Zugriff auf die URL des Posture Update-Felds nicht möglich ist, ist in diesem Fall eine Proxy-Konfiguration erforderlich. Weitere Informationen finden Sie unter Proxy in ISE konfigurieren.

1. Navigieren Sie zu Administration -> System -> Settings -> Proxy.



2. Konfigurieren Sie die Proxydetails, und klicken Sie auf Speichern.



3. Die Details des Proxys werden automatisch von der ISE abgerufen, wenn Online-Statusaktualisierungen durchgeführt werden.

Offline-Status-Updates

Mit einer Offline-Statusaktualisierung können Sie Statusaktualisierungsdateien (in Form einer ZIP-Datei oder eines anderen unterstützten Dateiformats) manuell auf die ISE hochladen.

Was geschieht, wenn Sie eine Aktualisierung der Offlinestatus durchführen?

- Sie laden die aktualisierten Statusdateien manuell hoch.
- Die ISE verarbeitet und wendet diese Dateien an, z. B. aktualisierte Richtlinien, Antivirus-Definitionen, Statusanalysen usw.
- Das Offline-Update erfordert keine Internetverbindung und wird in der Regel in Umgebungen mit strengen Sicherheits- oder Netzwerkrichtlinien verwendet, die den direkten Zugriff auf externe Server verhindern.

Verwendungszweck

Diese Methode wird häufig in Umgebungen verwendet, in denen das System vom Internet isoliert ist, oder wenn Sie bestimmte Offline-Update-Dateien von Cisco oder Ihrem Sicherheitsteam bereitgestellt haben.

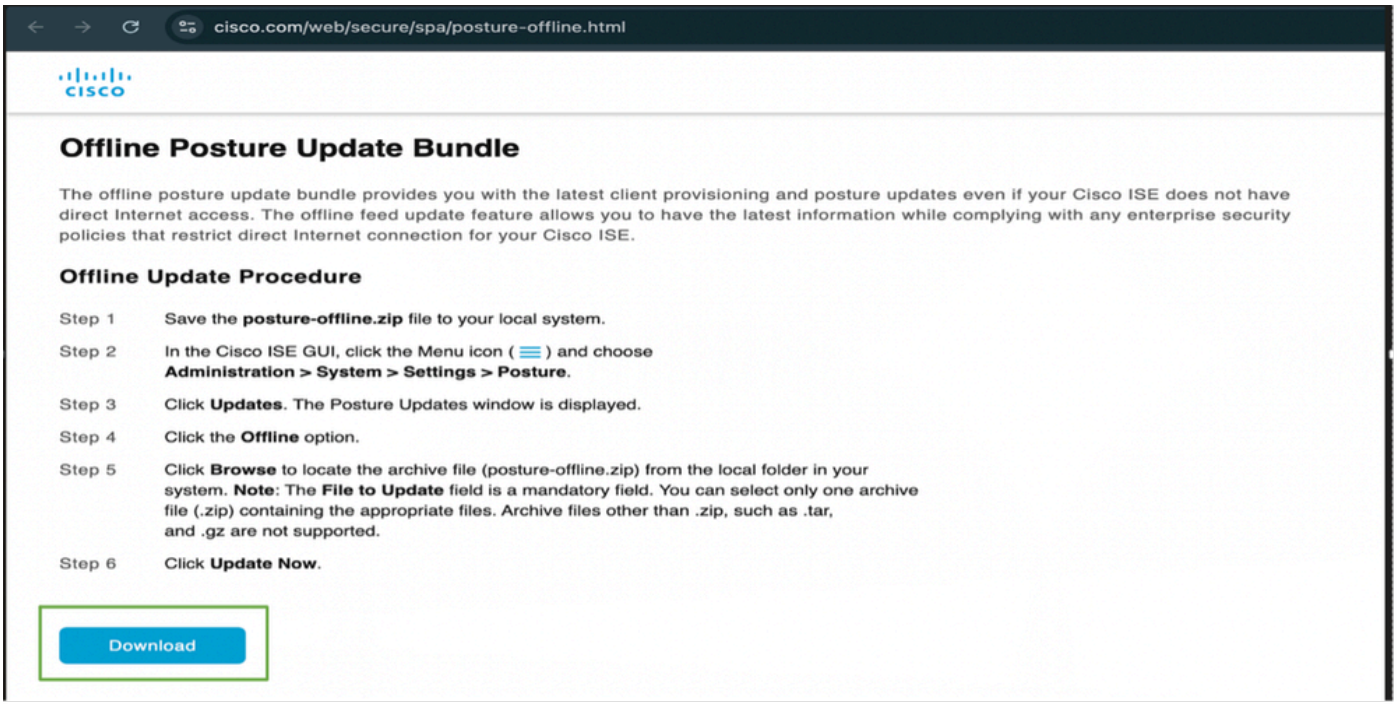
Ports für Offline-Statusaktualisierungen

Für die allgemeine Kommunikation mit dem ISE-Server (während des Update-Vorgangs) sind in vielen Fällen folgende Ports relevant:

1. Verwaltungszugriff (Ports 22, 443):
   - SSH (TCP 2): Wenn Sie SSH verwenden, um zur Fehlerbehebung oder zum manuellen Upload auf das ISE-System zuzugreifen.
   - HTTPS (TCP 443): Wenn Sie die grafische Benutzeroberfläche (Web-Oberfläche) für den Update-Upload verwenden.
2. Dateiübertragung (SFTP oder SCP):
   - Wenn Sie Dateien manuell über SFTP oder SCP auf die ISE hochladen müssen, stellen Sie sicher, dass die entsprechenden Ports (normalerweise Port 22 für SSH/SFTP) auf dem ISE-System offen sind.
3. Lokaler Netzwerkzugriff:
   - Stellen Sie sicher, dass das System, von dem Sie das Update hochladen (z. B. eine Admin-Workstation oder ein Server), über die für den Verwaltungszugriff erforderlichen Ports mit der ISE kommunizieren kann. Offline-Statusaktualisierungen erfordern jedoch keine externen Ports, da die Dateien manuell bereitgestellt werden.

Wo finde ich Dateien für Offline-Status-Updates?

1. Navigieren Sie zu URL: https://www.cisco.com/web/secure/spa/posture-offline.html , klicken Sie auf Download, und die Datei stature-offline.zip wird auf Ihr lokales System heruntergeladen.

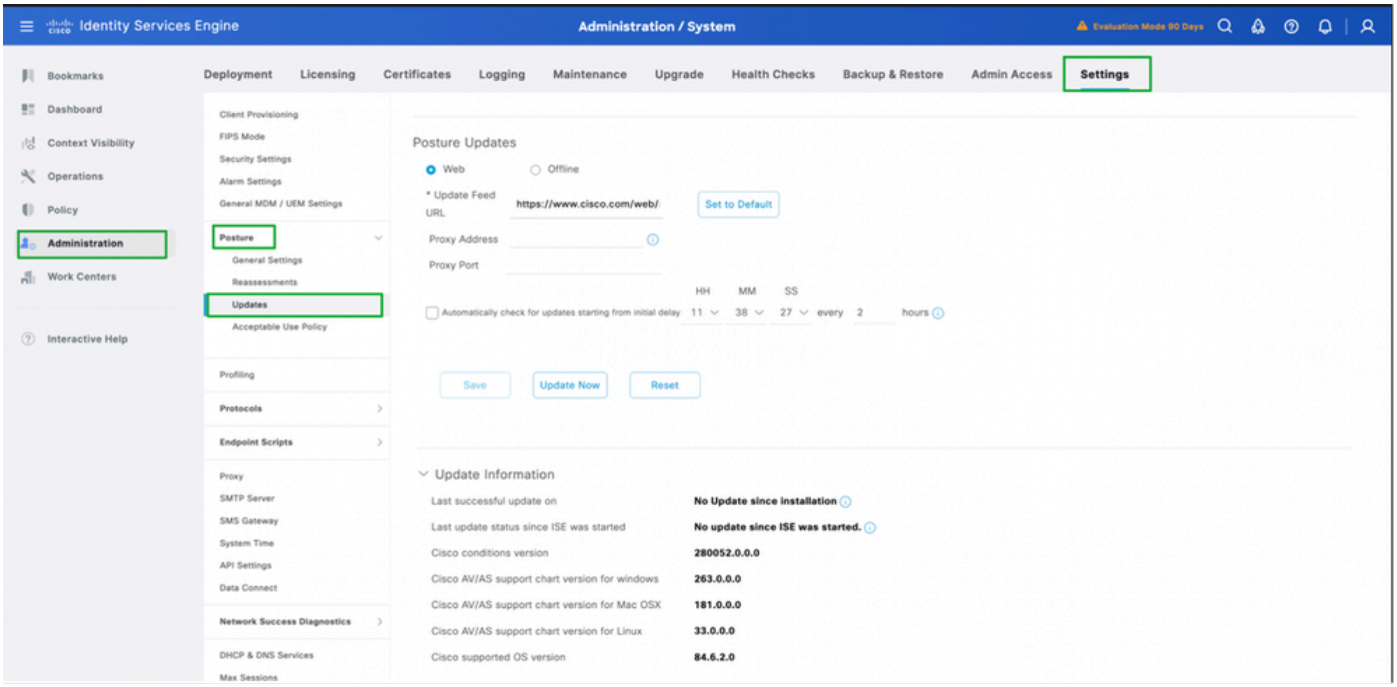


Offline-Statusaktualisierungsdateien enthalten

- Virenschutzdefinitionen (Signaturen).
- Statusrichtlinien und -regeln.
- Sicherheitsbewertungen und andere Konfigurationsdateien für die Statusbewertung.

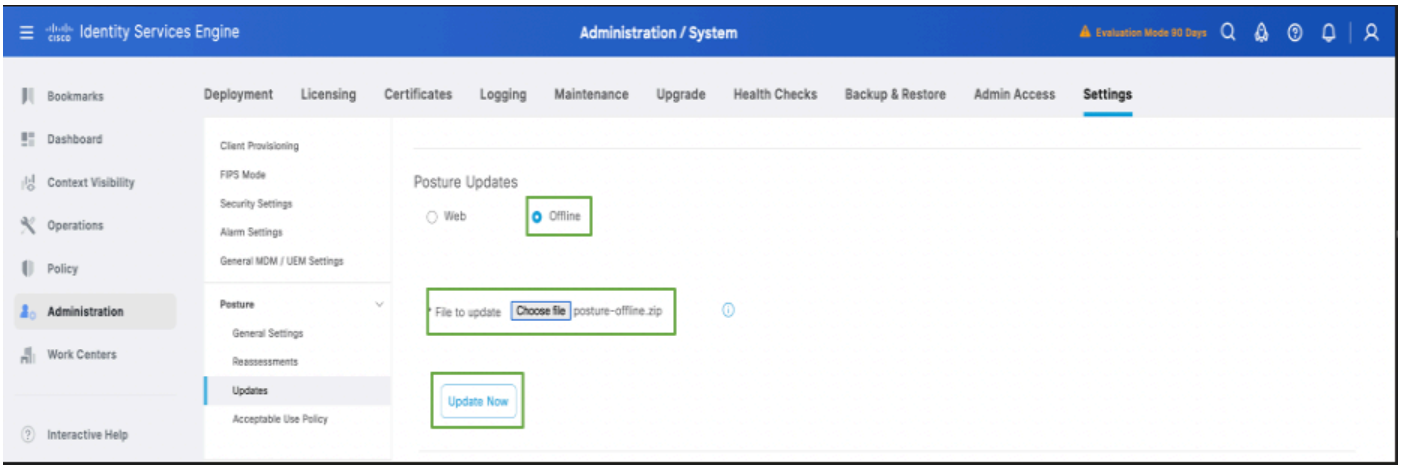
Verfahren zur Durchführung von Offline-Statusaktualisierungen

1. Melden Sie sich bei der ISE-GUI an -> Administration -> System -> Settings -> Posture -> Updates.

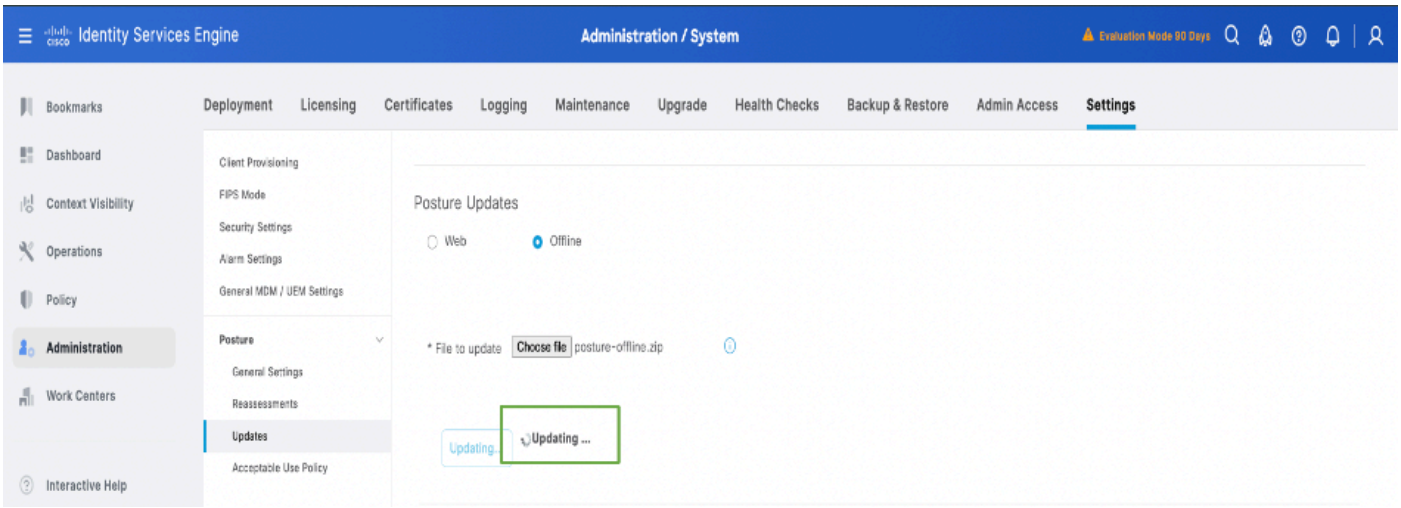


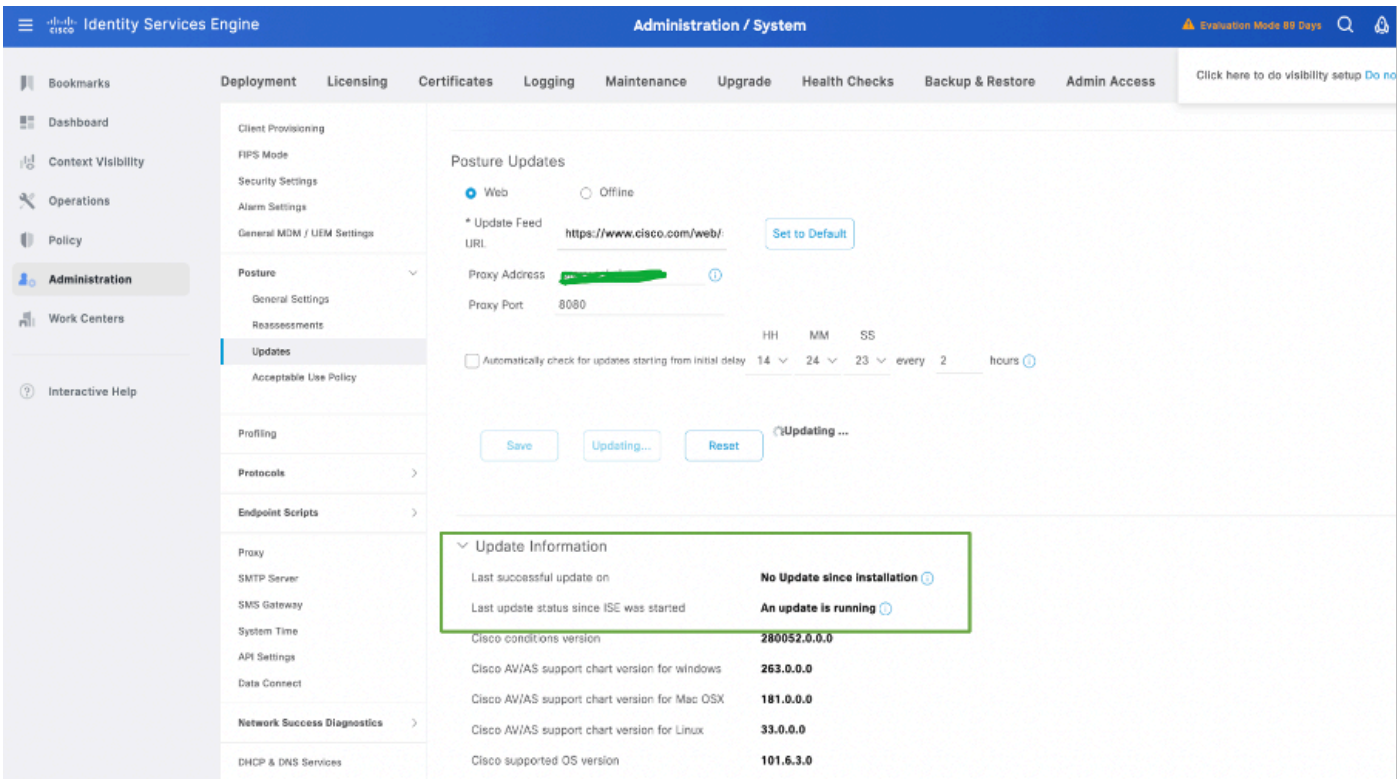
2. Wählen Sie offline Option, durchsuchen und wählen Sie Statusoffline.zip Ordner, die auf Ihr

lokales System heruntergeladen wurde. Klicken Sie auf Jetzt aktualisieren.

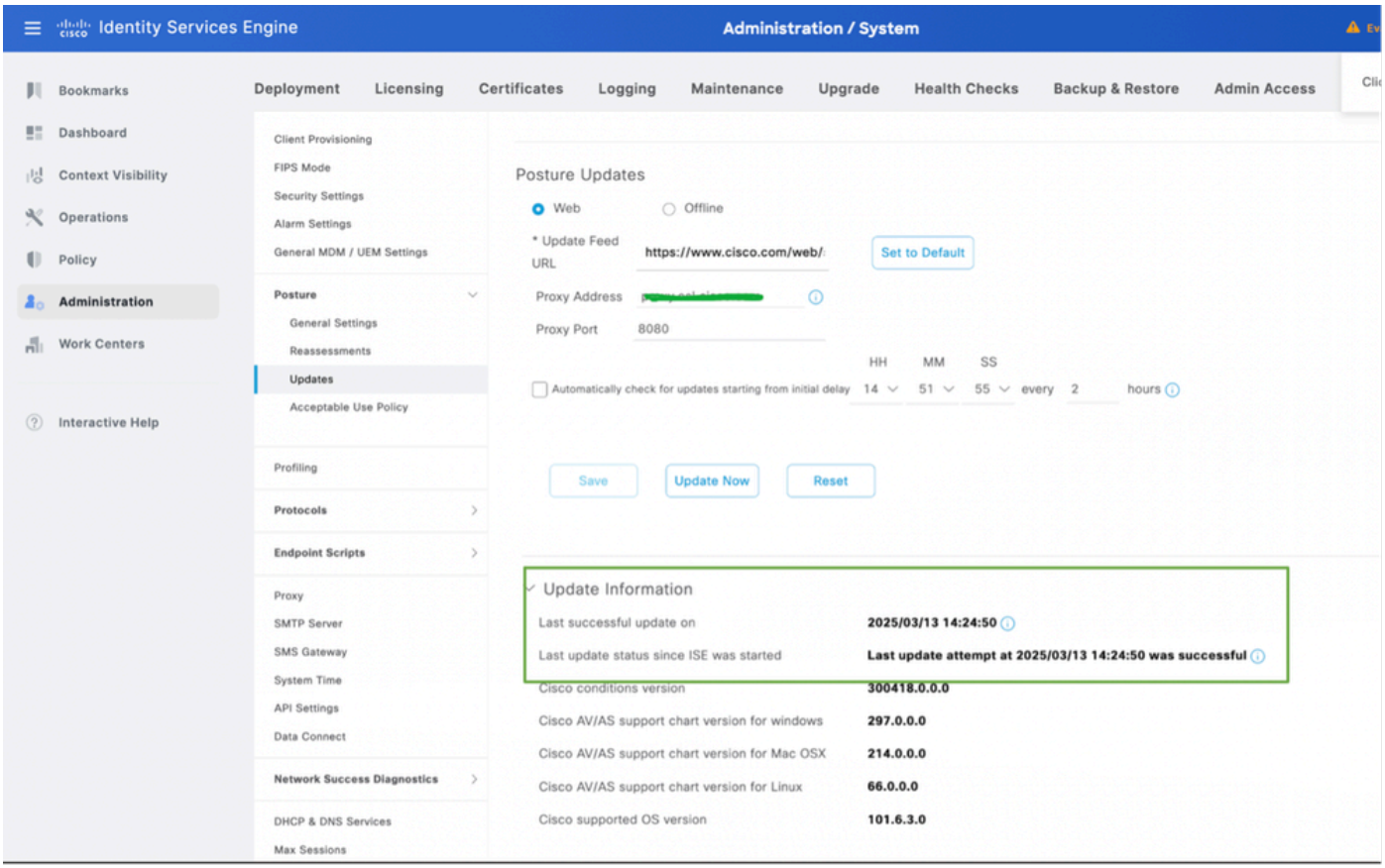


3. Sobald die Statusaktualisierungen beginnen, wird der Status in Aktualisieren geändert.





4. Der Status der Statusaktualisierungen kann anhand der Aktualisierungsinformationen wie in diesem Screenshot überprüft werden:



Verifizierung

Melden Sie sich an der GUI des primären Admin-Knotens an -> Operations -> Troubleshooting -> Download Logs -> Debug logs -> Application logs -> isc-psc.log , klicken Sie auf ise-psc.log, und das Protokoll wird auf Ihr lokales System heruntergeladen. Öffnen Sie die heruntergeladene Datei über den Editor oder einen Texteditor, und filtern Sie nach dem Opswat-Download. Sie müssen in der Lage sein, die Informationen zu den Posture-Updates zu finden, die in der Bereitstellung durchgeführt werden.

Sie können die Protokolle auch per Tail an die CLI des Knotens "Primary Admin" (Primärer Admin) protokollieren, indem Sie den Befehl show logging application ise-psc.log tail verwenden.

Der Opswat-Download, der sich auf Statusaktualisierungen bezieht, wird gestartet:

2025-03-13 13:58:07,246 INFO [admin-http-pool5][[] cisco.cpm.posture.download.DownloadManager -::admin::- Starten des Download-Vorgangs

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

2025-03-13 13:58:07,251 INFO [admin-http-pool5][[]] cisco.cpm.posture.download.DownloadManager -::admin::- Offline-Download-Datei-URI:

/opt/CSCOcpm/temp/cp/update/5c064701-a1ee-4a09-a190-3bf83c190af6/osgroups.tar.gz

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

Abgeschlossener Opswat-Download, der sich auf Statusaktualisierungen bezieht, wird heruntergeladen und erfolgreich abgeschlossen.

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

2025-03-13 14:24:50,803 INFO [admin-http-pool5][[]
cisco.cpm.posture.download.DownloadManager -::admin::- Abgeschlossener opswat-Download

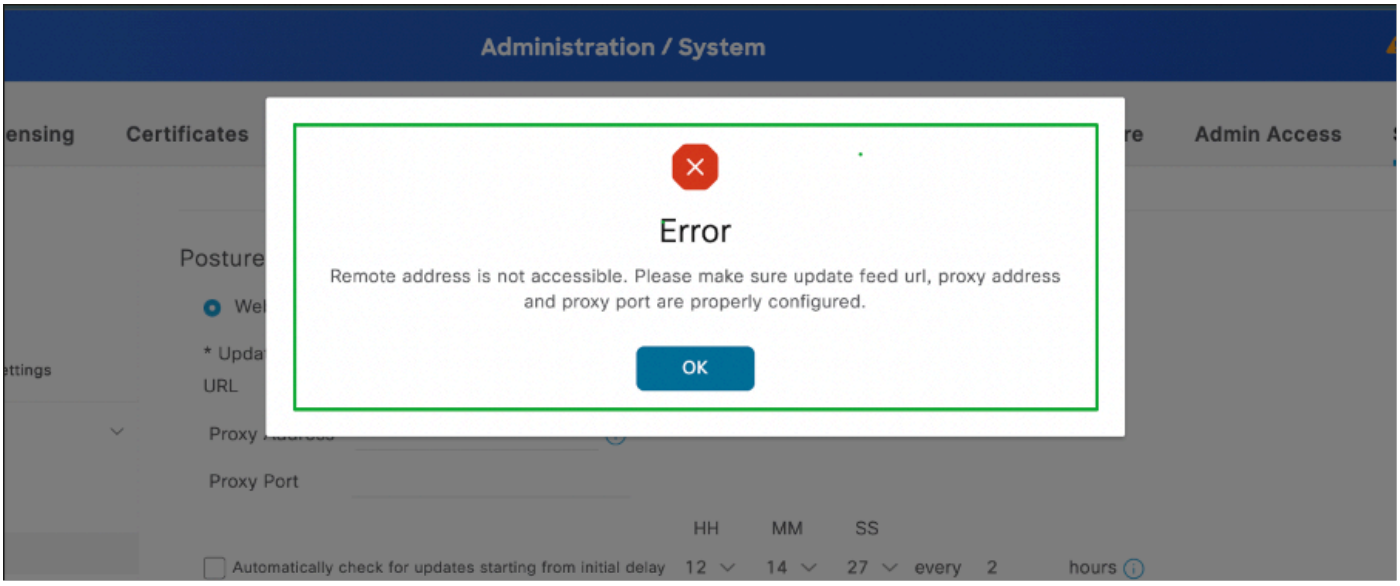
2025-03-13 14:24:50,827 INFO [admin-http-pool5][[]]
mnt.dbms.datadirect.impl.DatadirectServiceImpl -::admin::- Executing getStatus - datadirectSettings

Fehlerbehebung

Szenario

Fehler bei der Online-Statusaktualisierung. Fehler: "Remoteadresse ist nicht zugänglich. Bitte stellen Sie sicher, dass Update-Feed UR, Proxy-Adresse und Proxy-Port richtig konfiguriert sind."

Beispielfehler:



Lösung

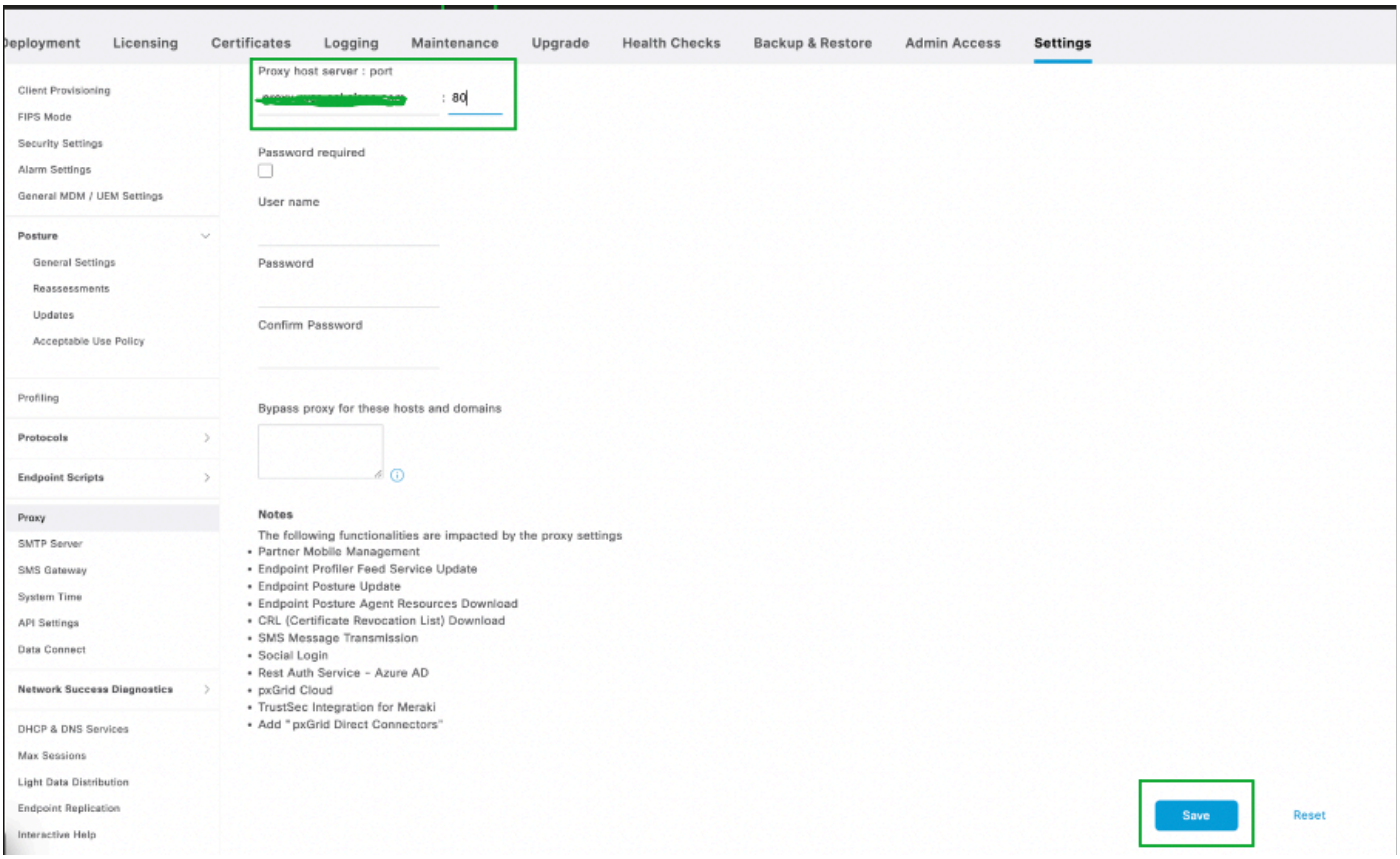
1. Melden Sie sich bei der CLI der ISE an, und überprüfen Sie, ob die ISE über den Befehl "ping cisco.com" auf cisco.com erreichbar ist.

isehostname/admin#ping cisco.com
PING cisco.com (72.163.4.161) 56(84) Bytes.

64 Bytes von 72.163.4.161: icmp_seq=1 ttl=235 time=238 ms
64 Bytes von 72.163.4.161: icmp_seq=2 ttl=235 time=238 ms
64 Bytes von 72.163.4.161: icmp_seq=3 ttl=235 time=239 ms
64 Bytes von 72.163.4.161: icmp_seq=4 ttl=235 time=238 ms

— cisco.com Ping-Statistik —
4 übertragene Pakete, 4 empfangen, 0 % Paketverlust, Zeit 3004 ms
rtt min/avg/max/mdev = 238,180/238,424/238,766/0,410 ms

2. Navigieren Sie zu Administration -> System -> Settings -> Proxy ist mit den richtigen Ports konfiguriert.



3. Überprüfen Sie, ob die Ports TCP 443, UDP 53 und UDP 123 auf allen Hops zum Internet zulässig sind.

Bekannte Fehler bei Statusaktualisierungsproblemen

Cisco Bug-ID: 01523

Referenz

- Administratorleitfaden für die Cisco Identity Services Engine, Version 3.3

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.