# Positie-updates uitvoeren in ISE Offline en Online

## Inhoud



## Inleiding

Dit document beschrijft hoe u houdingsupdates moet uitvoeren in Cisco Identity Services Engine® (ISE).

## Voorwaarden

### Vereisten

Cisco raadt u aan kennis te hebben over de Posture-flow.

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende hardware- en softwareversies.

- Cisco Identity Services Engine 3.2 en hogere versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Achtergrondinformatie

De updates van de houding omvatten een reeks vooraf bepaalde controles, regels, en steungrafieken voor antivirus en antispyware voor zowel Windows als de werkende systemen van MacOS, en werkend systeeminformatie die door Cisco worden gesteund.

Wanneer u Cisco ISE voor het eerst op uw netwerk implementeert, kunt u updates voor posterijen van het web downloaden. Dit proces duurt gewoonlijk ongeveer 20 minuten. Na de eerste download kunt u Cisco ISE configureren om te controleren en stapsgewijze updates te downloaden om automatisch te worden uitgevoerd.

Cisco ISE maakt alleen tijdens een eerste postuur-updates standaardpoortbeleid, -vereisten en -herstel. Als u deze verwijdert, maakt Cisco ISE geen nieuwe items tijdens de volgende handmatige of geplande updates.

Er zijn twee soorten postuur updates die u kunt uitvoeren:

- Online briefure updates.
- Offline postuur updates.

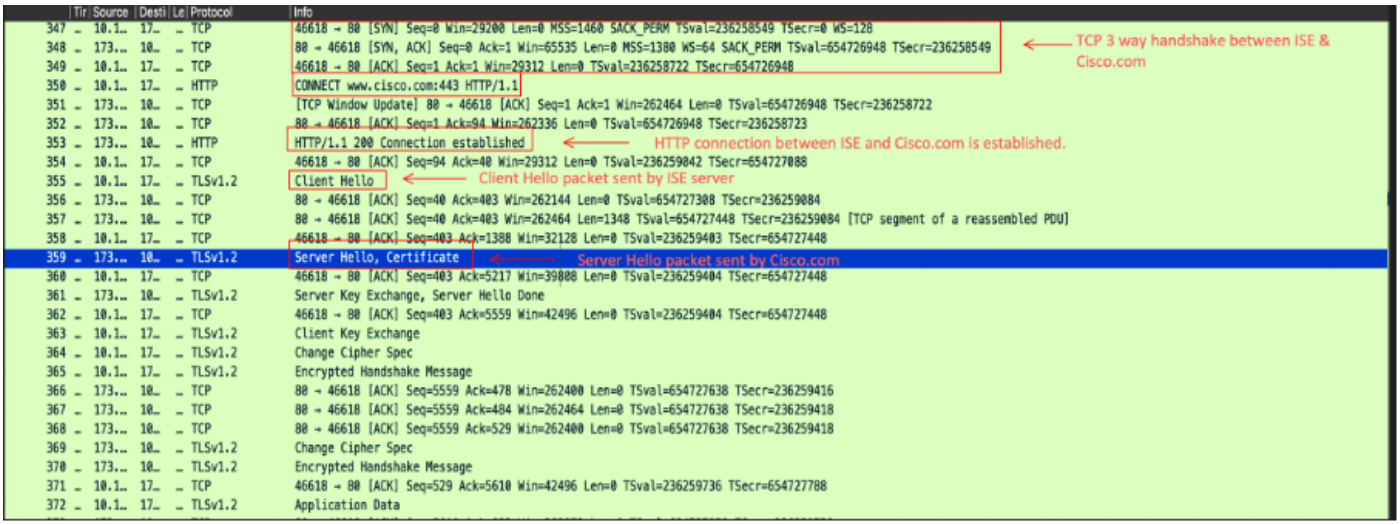
## Online briefure updates

Een Web Posture Update / Online Posture Update haalt de laatste postuur updates uit Cisco cloud of server repositories. Dit betekent dat de nieuwste beleidsregels, definities en handtekeningen rechtstreeks van Cisco-servers moeten worden gedownload. ISE moet verbinding maken met Cisco-cloudservers of repositories bijwerken om de nieuwste postuur-definities, beleidsregels en andere bijbehorende bestanden op te halen.

### Wat gebeurt er tijdens de updates van het web of de online houding?

De Identity Services Engine (ISE) heeft toegang tot de Cisco-website via een proxy of een directe internetverbinding met HTTP om een verbinding met www.cisco.com tot stand te brengen. Tijdens dit proces, de client hello en server hello uitwisseling vindt plaats, met de server die zijn certificaat verstrekt om zijn legitimiteit te verifiëren en het vertrouwen van de client-side te bevestigen. Nadat de client hello en server hello zijn voltooid, vindt de client key exchange plaats, en de server start de postuur updates. Hier is het pakket dat de communicatie tussen de ISE-server en Cisco.com

tijdens de Online Posture updates laat zien.




- Tijdens Server Hello, Cisco.com verstuurt deze certificaten naar de client om vertrouwen aan de clientzijde te bevestigen.

<#root>

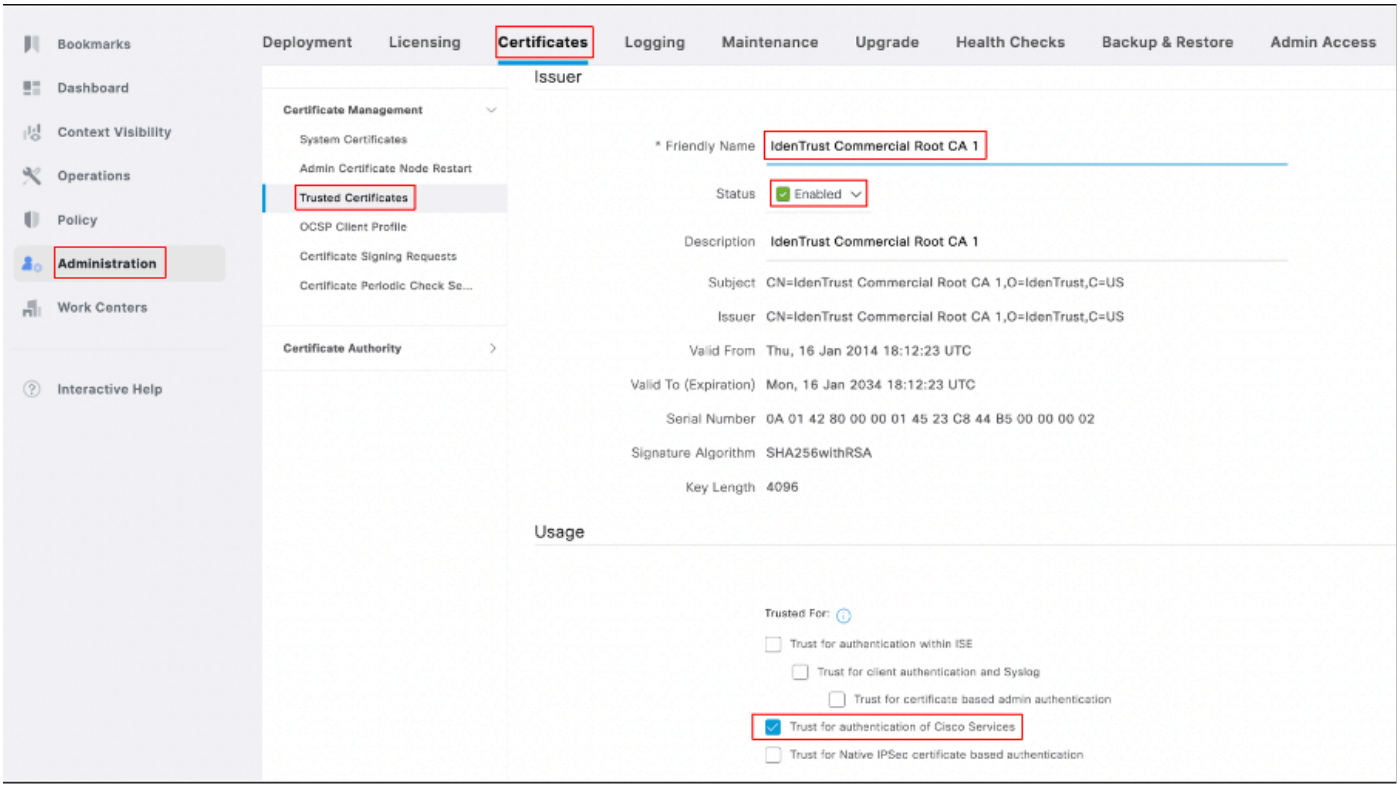
```
Certificates Length: 5083
Certificates (5083 bytes)
Certificate Length: 1940
Certificate: 3082079030820678a003020102021040191d1f3c7ec4ea73b301be3e06a90300d06092a… (id-at-commonNam
Certificate Length: 1754
Certificate: 308206d6308204bea003020102021040016efb0a205cfaebe18f71d73abb78300d06092a… (id-at-commonNam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

**IdenTrust Commercial Root CA**

**1**

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

- In ISE GUI, is het belangrijk om ervoor te zorgen dat het servercertificaat IdenTrust Commercial Root CA 1 is ingeschakeld en vertrouwen voor het verifiëren van Cisco-services om verbinding te maken met Cisco.com. Standaard is dit certificaat opgenomen in ISE en wordt "Trust for Authenticating Cisco Services" gecontroleerd, maar verificatie wordt geadviseerd.
- Controleer de certificaatstatus en het vertrouwde gebruik door naar de ISE GUI > Administration > Certificates > Trusted Certificates te gaan. Filter op de naam IdenTrust Commercial Root CA 1, selecteer het certificaat en bewerk het om het gebruik van het vertrouwen te verifiëren, zoals in deze screenshot:




- De updates van de houding kunnen nieuw of herzien postuur beleid, nieuwe antivirus/antimalware definities, en andere security-related criteria voor postuur beoordelingen omvatten.
- Deze methode vereist een actieve internetverbinding en wordt doorgaans uitgevoerd wanneer het ISE-systeem is geconfigureerd om cloudgebaseerde repositories voor postuur-updates te gebruiken.

Wanneer te gebruiken

Online poortupdates worden gebruikt als u wilt garanderen dat het posteringbeleid, de beveiligingsdefinities en de criteria up-to-date zijn met de nieuwste beschikbare versies die door Cisco worden geleverd.

## Poorten gebruikt voor Online Posture Update

Om ervoor te zorgen dat het ISE-systeem met succes Cisco-cloudservers kan bereiken om updates van posterijen te downloaden, moeten deze poorten in uw firewall open zijn en moeten ze kunnen communiceren van ISE naar het internet:

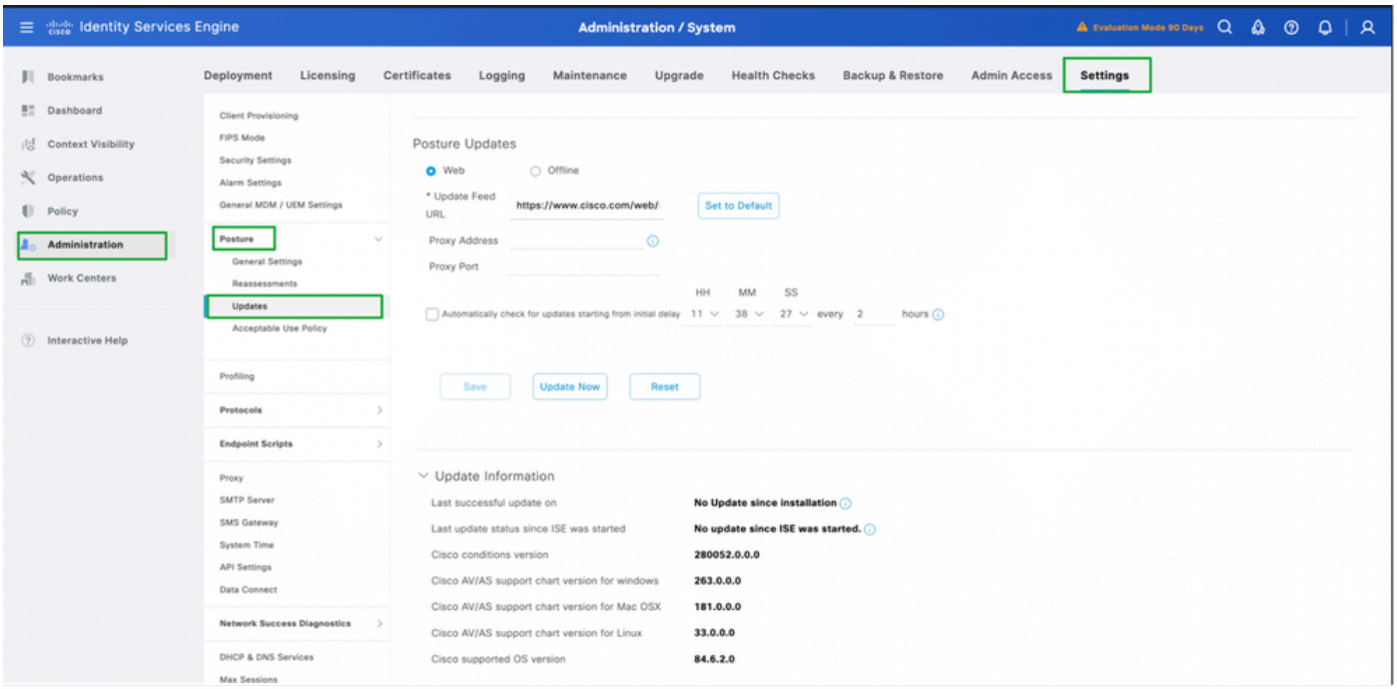
1. HTTPS (TCP 443):
    - Primaire poort voor ISE om de Cisco-cloudservers te bereiken en updates te downloaden via een beveiligde verbinding (TLS/SSL).
    - Dit is de meest cruciale poort voor het webgebaseerde postuur update proces.
2. DNS (UDP 53):
    - ISE moet in staat zijn om DNS lookups uit te voeren om de hostnamen van de update servers op te lossen.
    - Zorg ervoor dat uw ISE-systeem de DNS-servers kan bereiken en domeinnamen kan

oplossen.

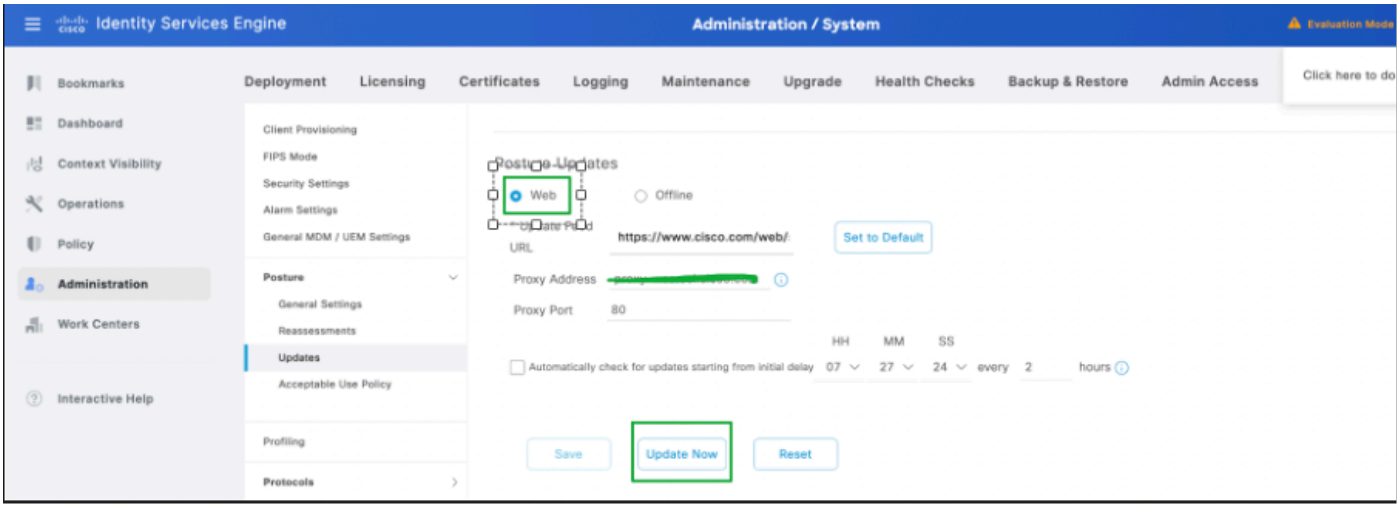
3. NTP (UDP 123):
    - ISE maakt gebruik van NTP voor tijdsynchronisatie. Dit is belangrijk om ervoor te zorgen dat het updateproces correct wordt getimd en dat het systeem van ISE in een gesynchroniseerde tijdzone werkt.
    - In veel gevallen moeten NTP-servers ook toegankelijk zijn via UDP 123.

Procedure voor het uitvoeren van online posture updates

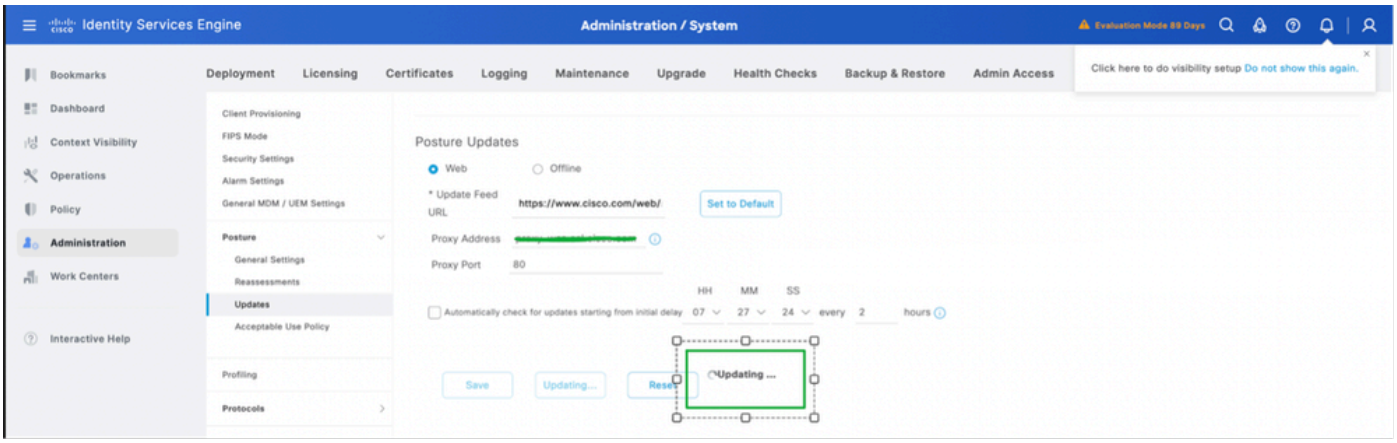
1. Log in op de GUI -> Beheer -> Systeem -> Instellingen -> Houding -> Updates.



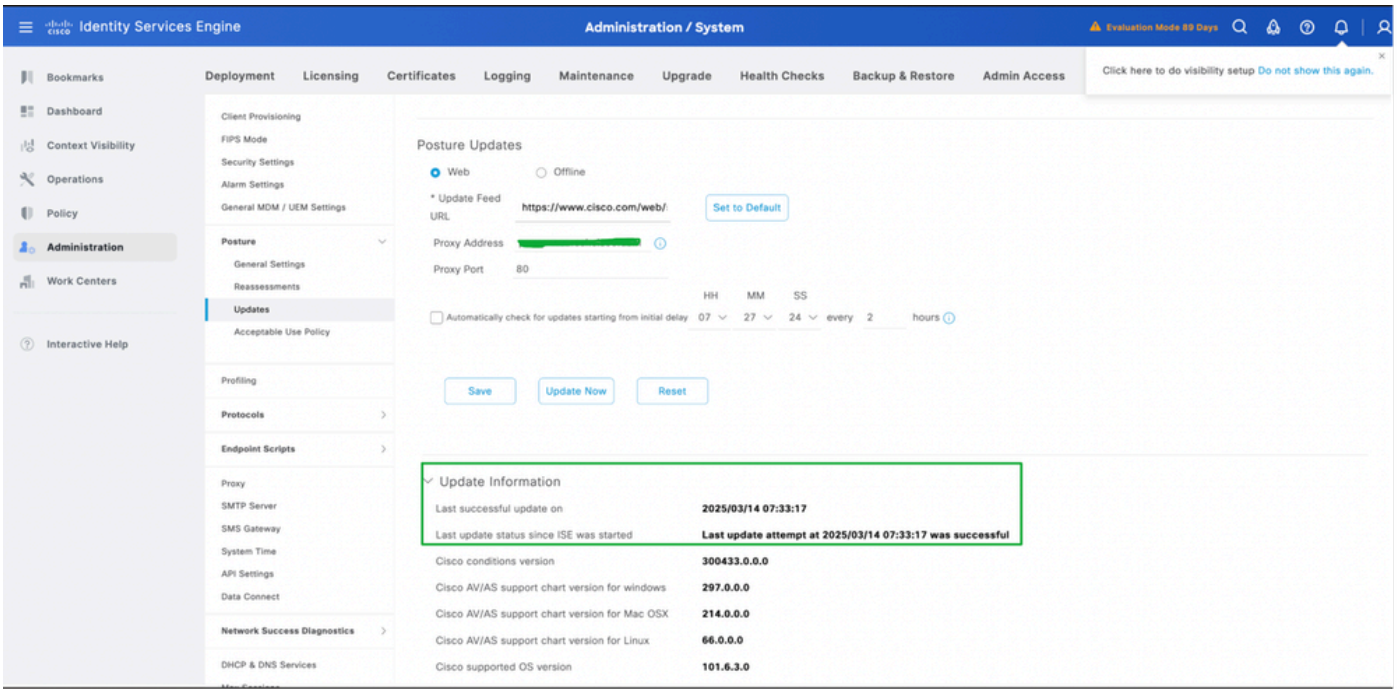

2. Selecteer de methode als Web for Online Posture Updates, klik op Nu bijwerken.




3. Zodra de positieupdates beginnen, wordt de status gewijzigd in Bijwerken.



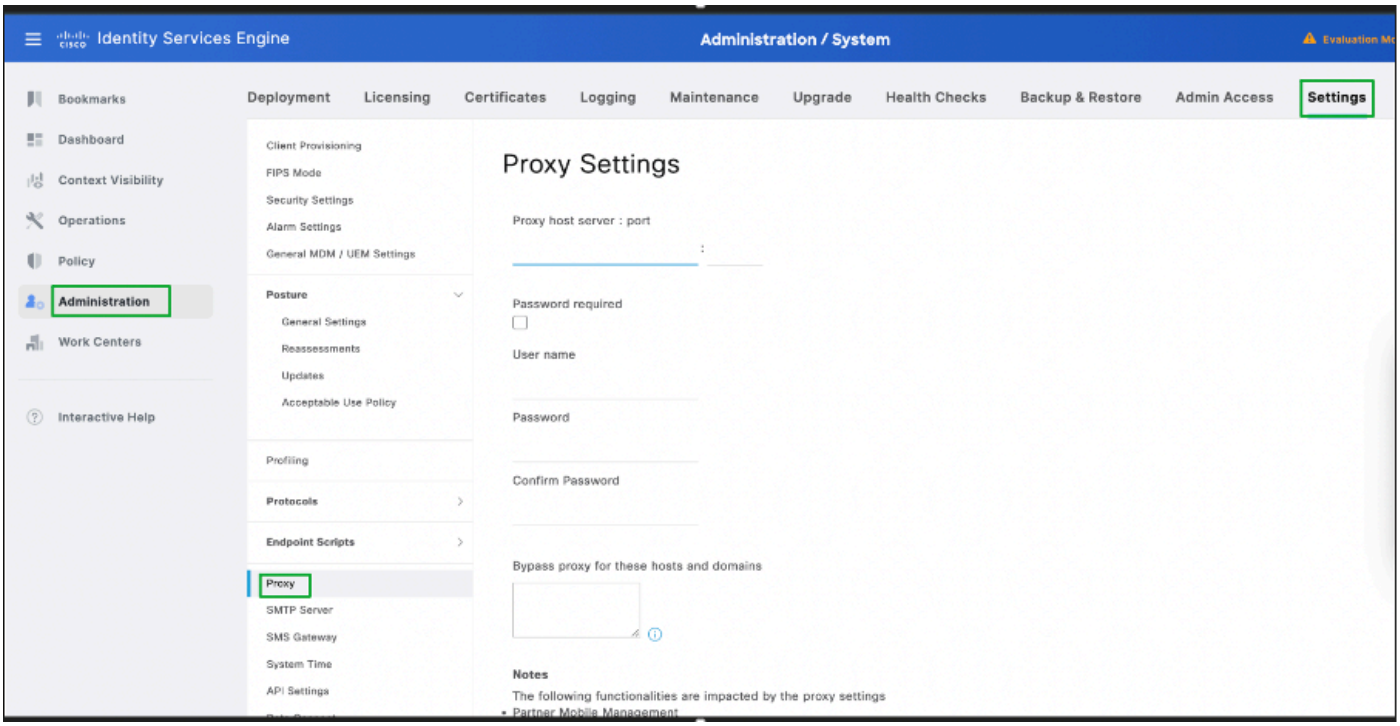

4. De status van de updates van de houding kan worden geverifieerd uit de Update Informatie volgens deze screenshot:



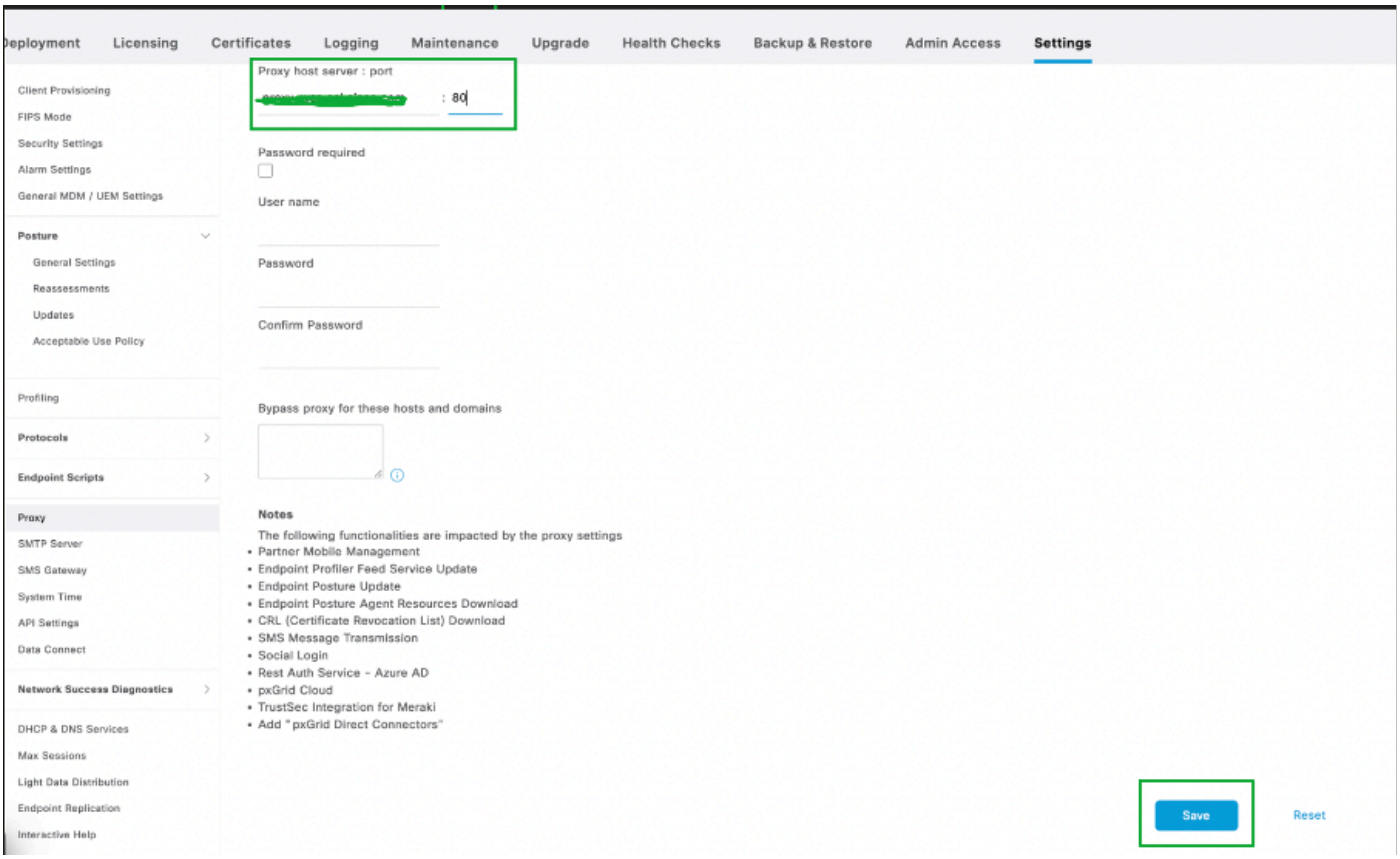

# Proxy Configuration voor Online Posture Updates

In een beperkte omgeving waar de URL van het veld Posture Update niet toegankelijk is, is in dat geval proxyconfiguratie vereist. Raadpleeg Proxy configureren in ISE.

1. Ga naar Beheer -> Systeem -> Instellingen -> Proxy.




2. Configureer de Proxy-gegevens en klik op Opslaan.




3. De details van de proxy worden automatisch door ISE gehaald wanneer Online Posture Updates worden uitgevoerd.

# Offline houding updates

Met een Offline Posture Update kunt u posture update bestanden (in de vorm van een .zip of een andere ondersteunde bestandsindeling) handmatig uploaden naar ISE.

## Wat gebeurt er als je een offline houding update?

- U uploadt de bijgewerkte formulierbestanden handmatig.
- ISE verwerkt en past deze bestanden toe, die kunnen bestaan uit bijgewerkt beleid, antivirus definities, postuur beoordelingen, onder andere soorten bestanden.
- De offline update vereist geen internetverbinding en wordt meestal gebruikt in omgevingen met strikte beveiliging of netwerkbeleid die directe toegang tot externe servers verhinderen.

Wanneer te gebruiken

Deze methode wordt vaak gebruikt in omgevingen waar het systeem is geïsoleerd van het internet of wanneer u specifieke offline update-bestanden hebt die worden geleverd door Cisco of uw beveiligingsteam.

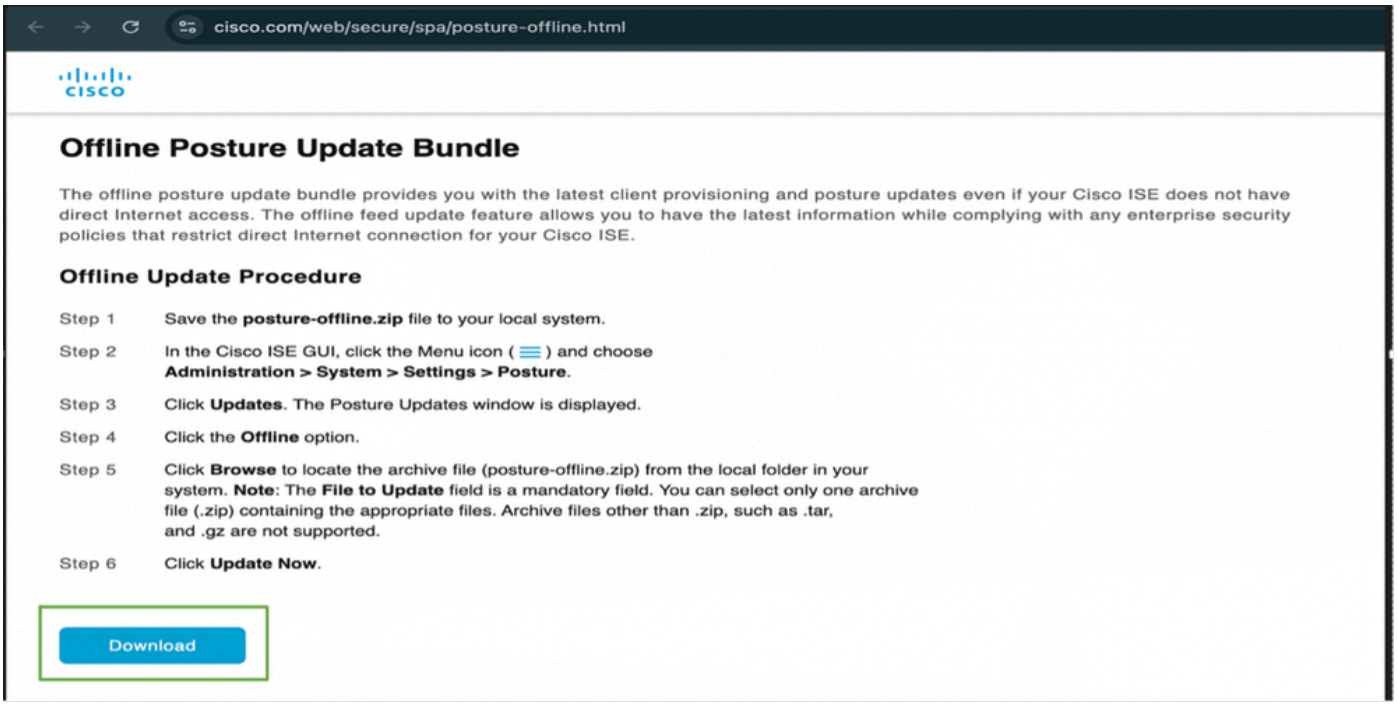
## Poorten die worden gebruikt voor updates van offline houdingen

Voor de algemene communicatie met de ISE-server (tijdens het updateproces) zijn deze poorten in veel gevallen relevant:

1. Beheertoegang (poorten 22, 43):
   - SSH (TCP/IP22): Als u SSH gebruikt om toegang te krijgen tot het ISE-systeem voor probleemoplossing of het handmatig uploaden van bestanden.
   - HTTPS (TCP 443): Als u de GUI (web interface) gebruikt voor het uploaden van de update.
2. Bestandsoverdracht (SFTP of SCP):
   - Als u bestanden handmatig naar ISE moet uploaden via SFTP of SCP, zorg er dan voor dat de corresponderende poorten (meestal poort 22 voor SSH/SFTP) open zijn op het ISE-systeem.
3. Lokale netwerktoegang:
   - Zorg ervoor dat het systeem waarvan u de update uploadt (bijvoorbeeld een beheerwerkstation of server) kan communiceren met ISE via de noodzakelijke poorten voor beheertoegang, maar nogmaals, offline poortupdates vereisen geen externe poorten omdat de bestanden handmatig worden geleverd.

## Waar Bestanden voor Offline Posture Updates zoeken?

1. Naar URL navigeren: https://www.cisco.com/web/secure/spa/posture-offline.html , klik op Downloaden en het posture-offline.zip bestand wordt gedownload naar uw lokale systeem.

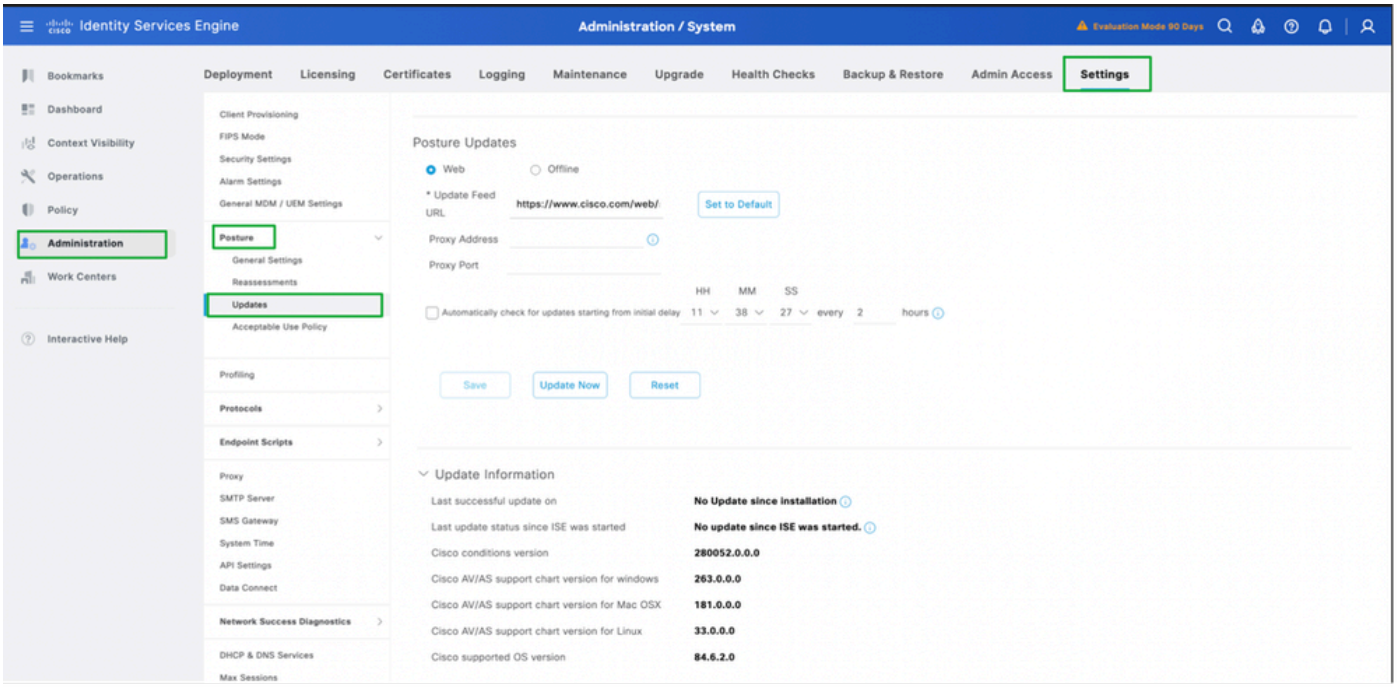



## Offline houding update bestanden omvatten

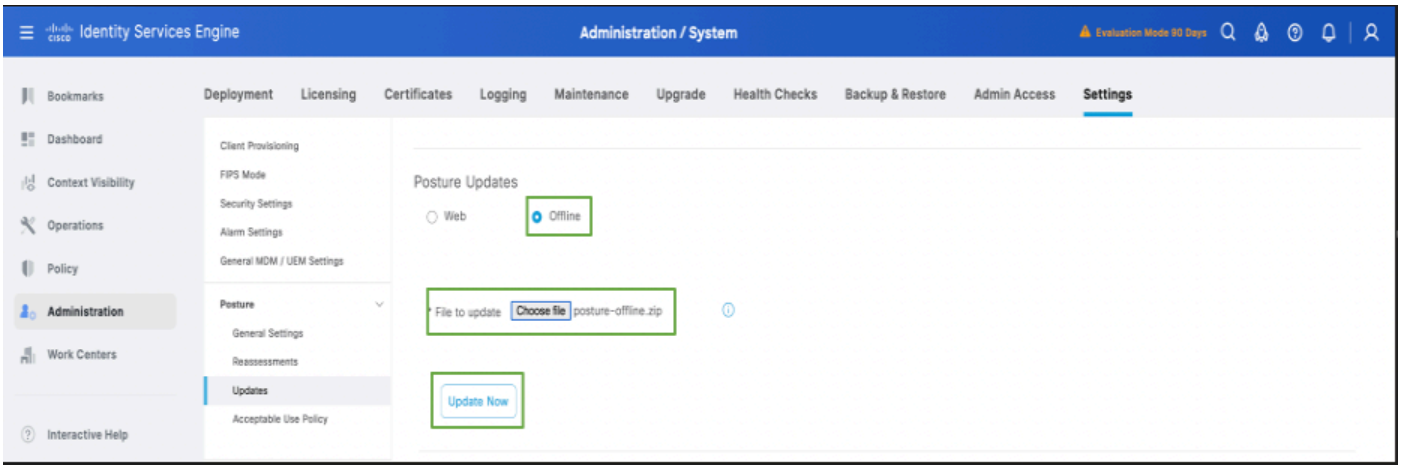
- Antivirusdefinities (handtekeningen).
- Gedragsregels en regels.
- Beveiligingsbeoordelingen en andere configuratiebestanden voor postuur-evaluatie.

## Procedure voor het uitvoeren van offline-positieupdates

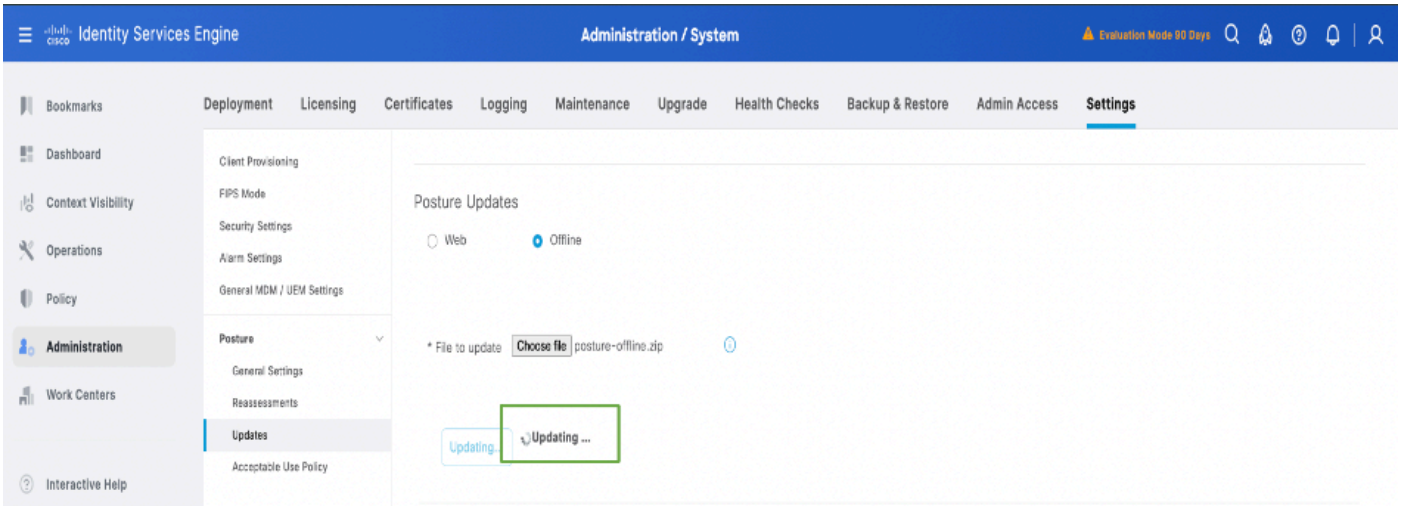
1. Log in op de ISE GUI -> Beheer -> Systeem -> Instellingen -> Houding -> Updates.

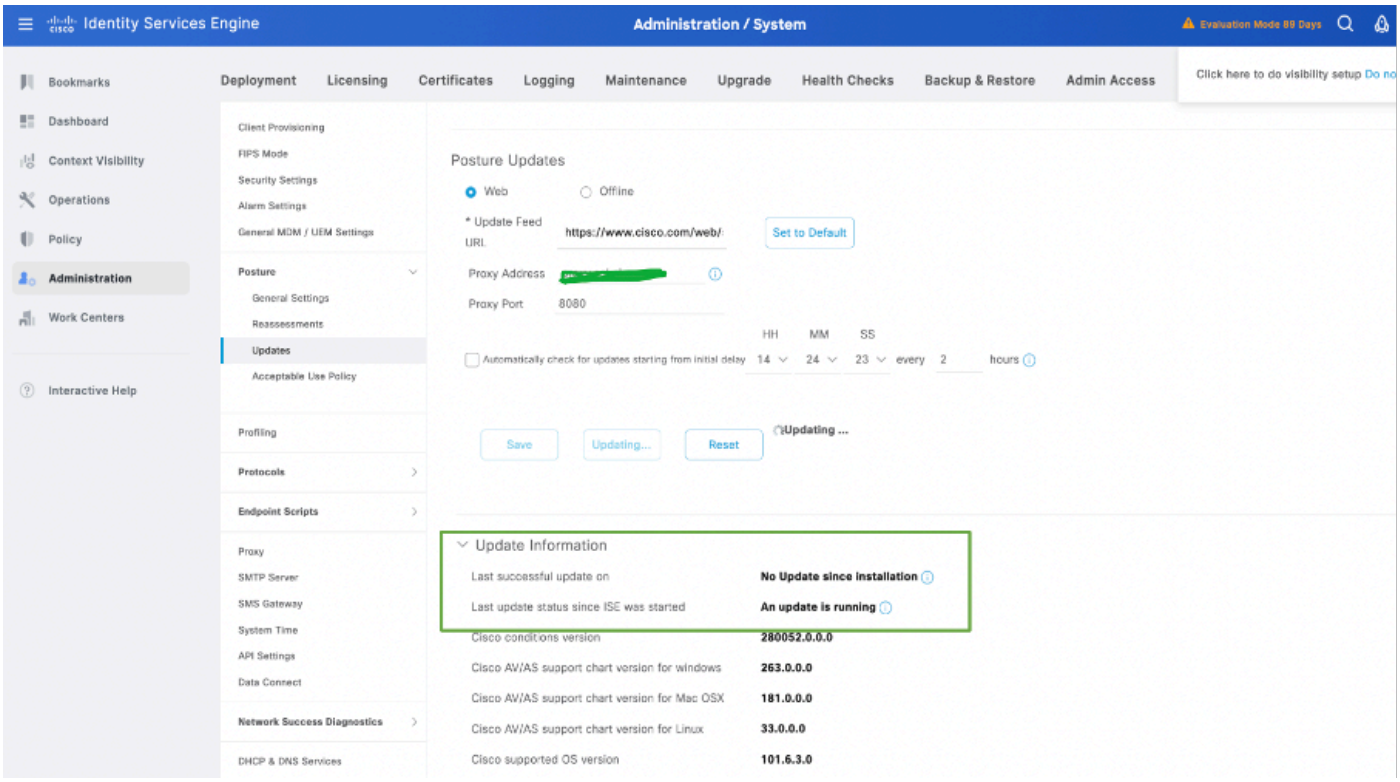



2. Selecteer offline optie, blader en selecteer posture-offline.zip map die is gedownload naar uw lokale systeem. Klik op Nu bijwerken.



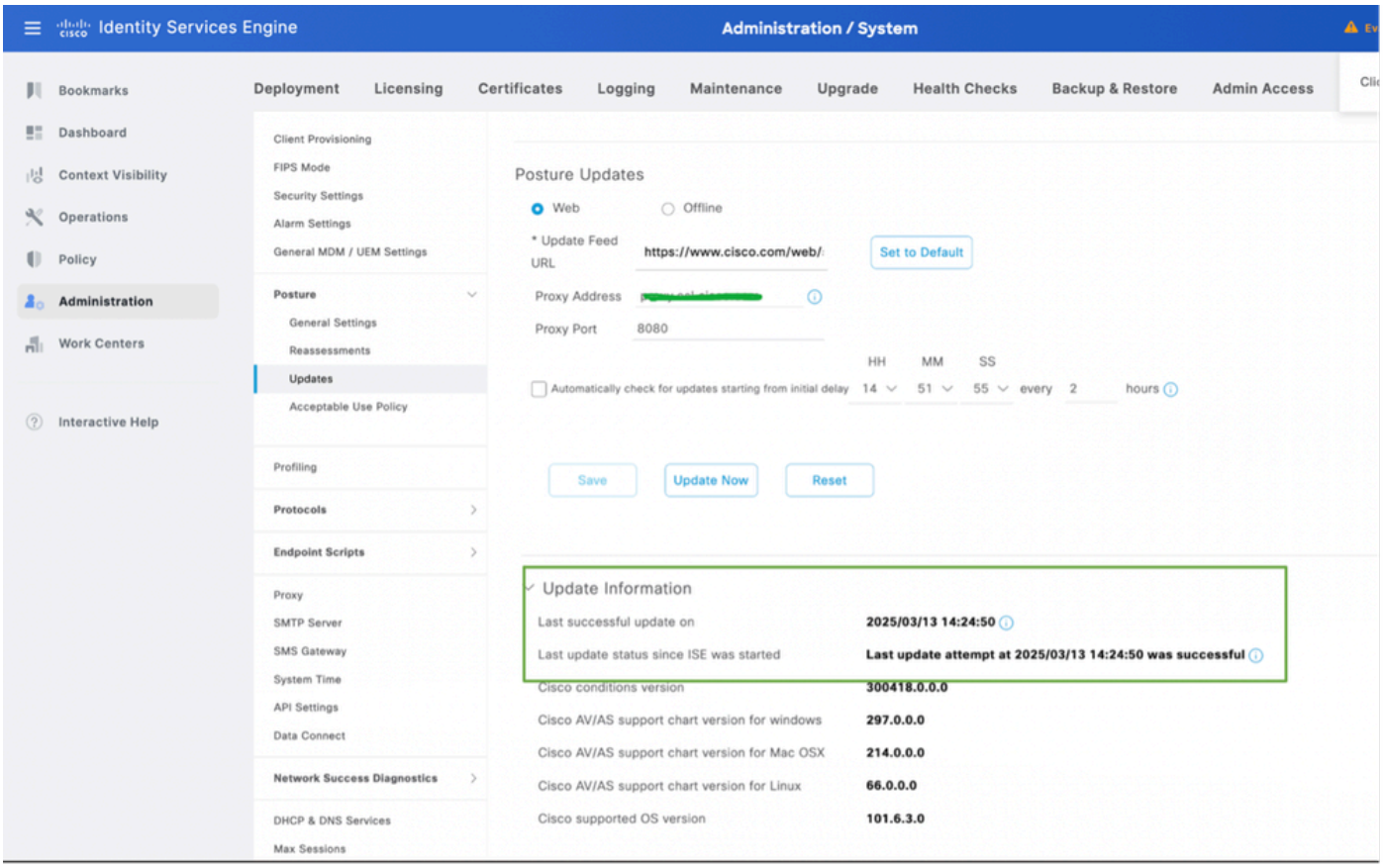

3. Zodra de positieupdates beginnen, wordt de status gewijzigd in Bijwerken.




4. De status van de updates van de houding kan worden geverifieerd uit de Update Informatie

volgens deze screenshot:




# Verificatie

Log in op de GUI van de Primaire beheerknooppunt -> Bewerkingen -> Problemen oplossen -> Downloadlogs -> Debug logs -> Toepassingslogs -> isc-psc.log , klik op ise-psc.log en het logbestand wordt gedownload naar uw lokale systeem. Open het gedownloade bestand via Kladblok of teksteditor en filter voor Opswat downloaden. U moet in staat zijn om de informatie met betrekking tot de Posture updates die worden uitgevoerd in de inzet te vinden.

U kunt de logbestanden ook bijhouden door te registreren op de CLI van Primaire Admin-knooppunt door de show logging-toepassing ise-psc.log-tail opdracht te gebruiken.

De download van Opswat, die naar houdingsupdates verwijst, is begonnen:

2025-03-13 13:58:07,246 INFO [admin-http-pool5][[]] cisco.cpm.posture.download.DownloadManager -::admin:::- Opswat downloaden

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

Voltooide Opswat Download, verwijzend naar postuur updates worden gedownload en succesvol.

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

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

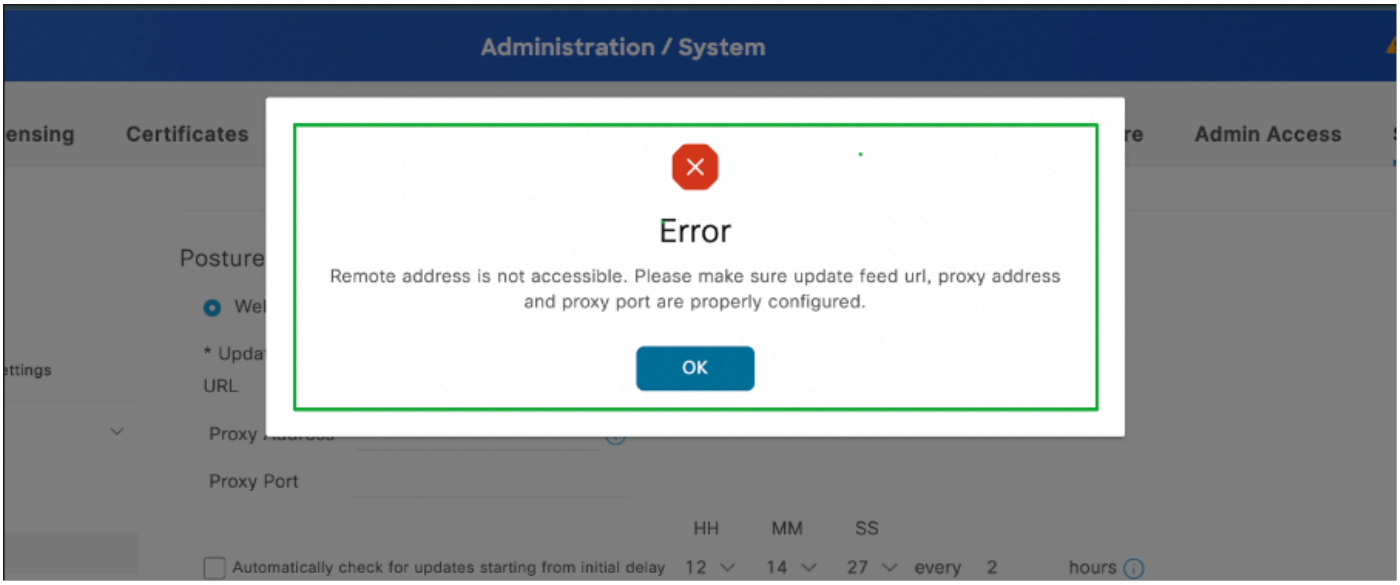
2025-03-13 14:24:50,827 INFO [admin-http-pool5][[]]
mnt.dbms.datadirect.impl.DatadirectServiceImpl -::admin:::: - Het uitvoeren van getStatus - datadirectSettings

# Problemen oplossen

## Scenario

Online Posture Updates mislukt met de fout "Remote Address is niet toegankelijk. Zorg ervoor dat de updatefeed UR, proxyadres en proxypoort goed zijn geconfigureerd".

Monsterfout:




## Oplossing

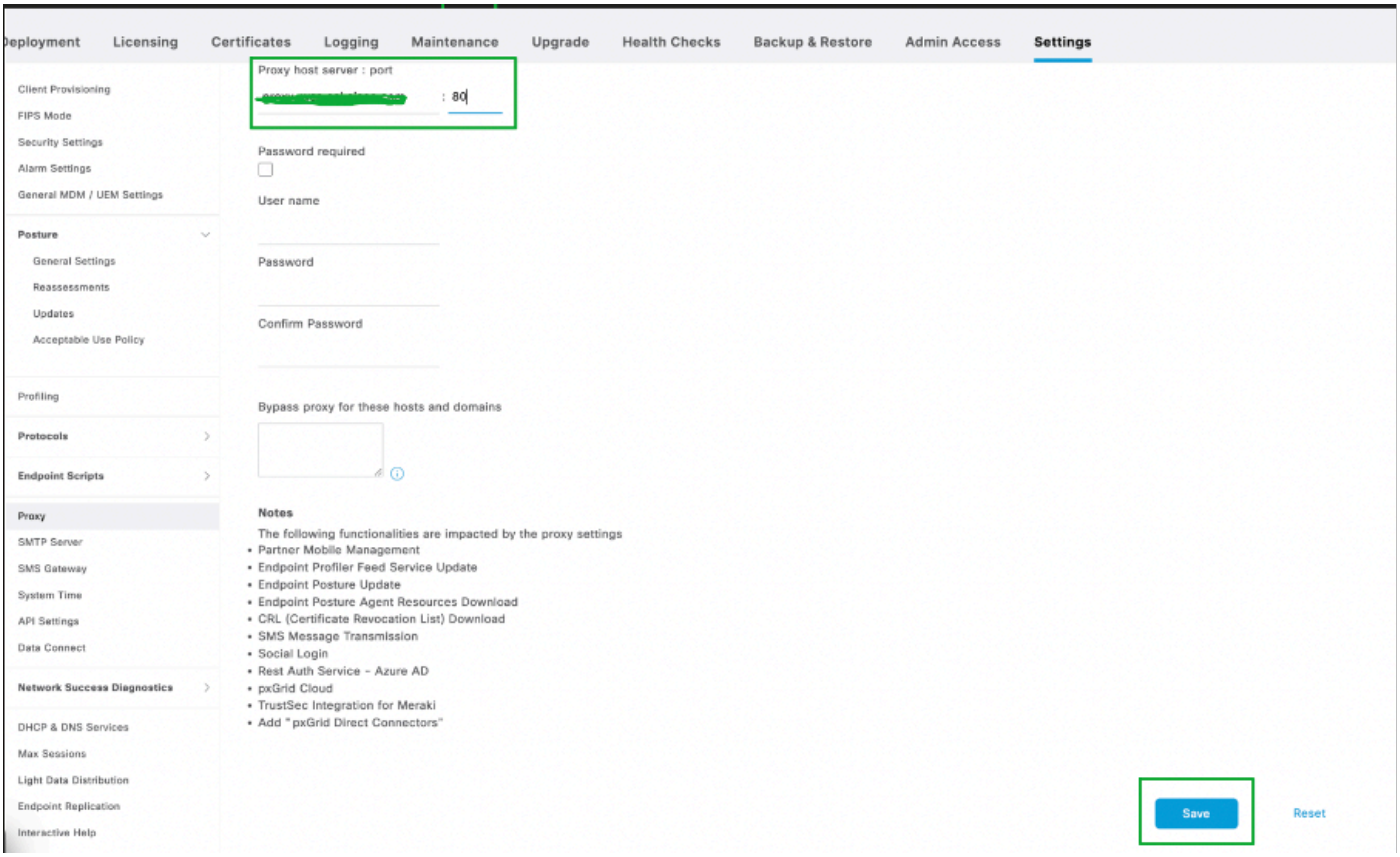
1. Controleer of ISE met de CLI van ISE bereikbaar is via cisco.com met de opdracht "ping cisco.com".

isehostname/admin#ping cisco.com
PING cisco.com (72.163.4.161) 56(84) bytes van gegevens.
64 bytes vanaf 72.163.4.161: icmp_seq=1 ttl=235 tijd=238 ms
64 bytes vanaf 72.163.4.161: icmp_seq=2 ttl=235 tijd=238 ms
64 bytes vanaf 72.163.4.161: icmp_seq=3 ttl=235 tijd=239 ms

64 bytes vanaf 72.163.4.161: icmp_seq=4 ttl=235 tijd=238 ms

— cisco.com pingstatistieken —
4 verzonden pakketten, 4 ontvangen, 0% pakketverlies, tijd 3004ms
rtt min/avg/max/mdev = 238,180/238,424/238,766/0,410 ms

2. Navigeer naar Beheer -> Systeem -> Instellingen -> Proxy is geconfigureerd met de juiste poorten.




3. Controleer of de poorten TCP 443, UDP 53 en UDP 123 op alle hops op het internet zijn toegestaan.

### Bekende tekortkomingen voor problemen met de update van de houding

01523 van Cisco-bug-id

## Referentie

- Beheerdershandleiding voor Cisco Identity Services Engine, release 3.3

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.