Esegui aggiornamenti della postura in ISE offline e online

Sommario

Introduzione

Questo documento descrive come eseguire gli aggiornamenti della postura in Cisco Identity Services Engine® (ISE).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza del flusso di postura.

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni hardware e software.

- Cisco Identity Services Engine 3.2 e versioni successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Gli aggiornamenti della postura includono una serie di controlli predefiniti, regole e grafici di supporto per antivirus e antispyware per i sistemi operativi Windows e MacOS e informazioni sui sistemi operativi supportati da Cisco.

Quando si distribuisce Cisco ISE sulla rete per la prima volta, è possibile scaricare gli aggiornamenti della postura dal Web. Questo processo richiede in genere circa 20 minuti. Dopo il download iniziale, è possibile configurare Cisco ISE in modo che verifichi e scarichi automaticamente gli aggiornamenti incrementali.

Cisco ISE crea policy, requisiti e misure correttive di postura predefiniti solo una volta durante gli aggiornamenti iniziali della postura. Se li elimini, Cisco ISE non li crea nuovamente durante i successivi aggiornamenti manuali o pianificati.

È possibile eseguire due tipi di aggiornamenti della postura:

- Aggiornamenti postura online.
- Aggiornamenti della postura offline.

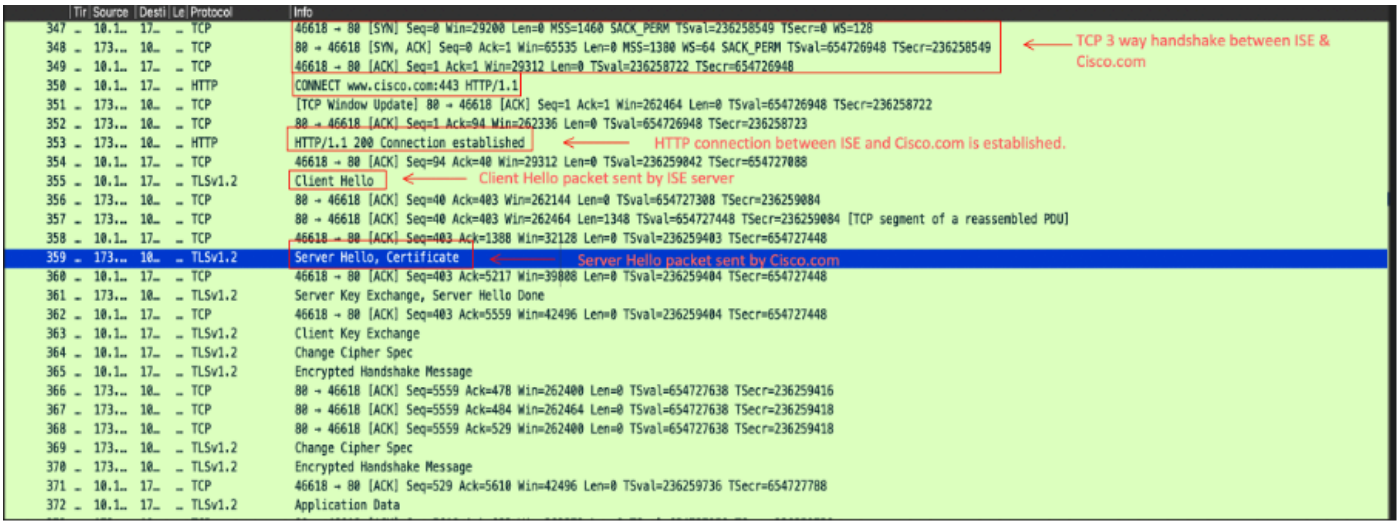
Aggiornamenti postura online

Un aggiornamento Web della postura/aggiornamento online della postura recupera gli ultimi aggiornamenti della postura dal cloud Cisco o dai repository del server. Ciò comporta il download delle policy, delle definizioni e delle firme più recenti direttamente dai server Cisco. ISE deve connettersi ai server cloud Cisco o aggiornare i repository per recuperare le definizioni delle posture, le policy e gli altri file associati più recenti.

Cosa succede durante gli aggiornamenti Web o delle posture online?

Identity Services Engine (ISE) accede al sito Web Cisco tramite un proxy o una connessione Internet diretta tramite HTTP, stabilendo una connessione con www.cisco.com. Durante questo processo, si verifica lo scambio di salve client e salve server, con il server che fornisce il proprio certificato per verificarne la legittimità e confermare la fiducia sul lato client. Al termine dell'operazione, viene eseguito lo scambio della chiave client e il server avvia gli aggiornamenti della postura. Ecco l'acquisizione dei pacchetti che dimostra la comunicazione tra il server ISE e

Cisco.com durante gli aggiornamenti di Online Posture.



- Durante l'esecuzione di Server Hello, Cisco.com invia questi certificati al client per confermare l'attendibilità sul lato client.

<#root>

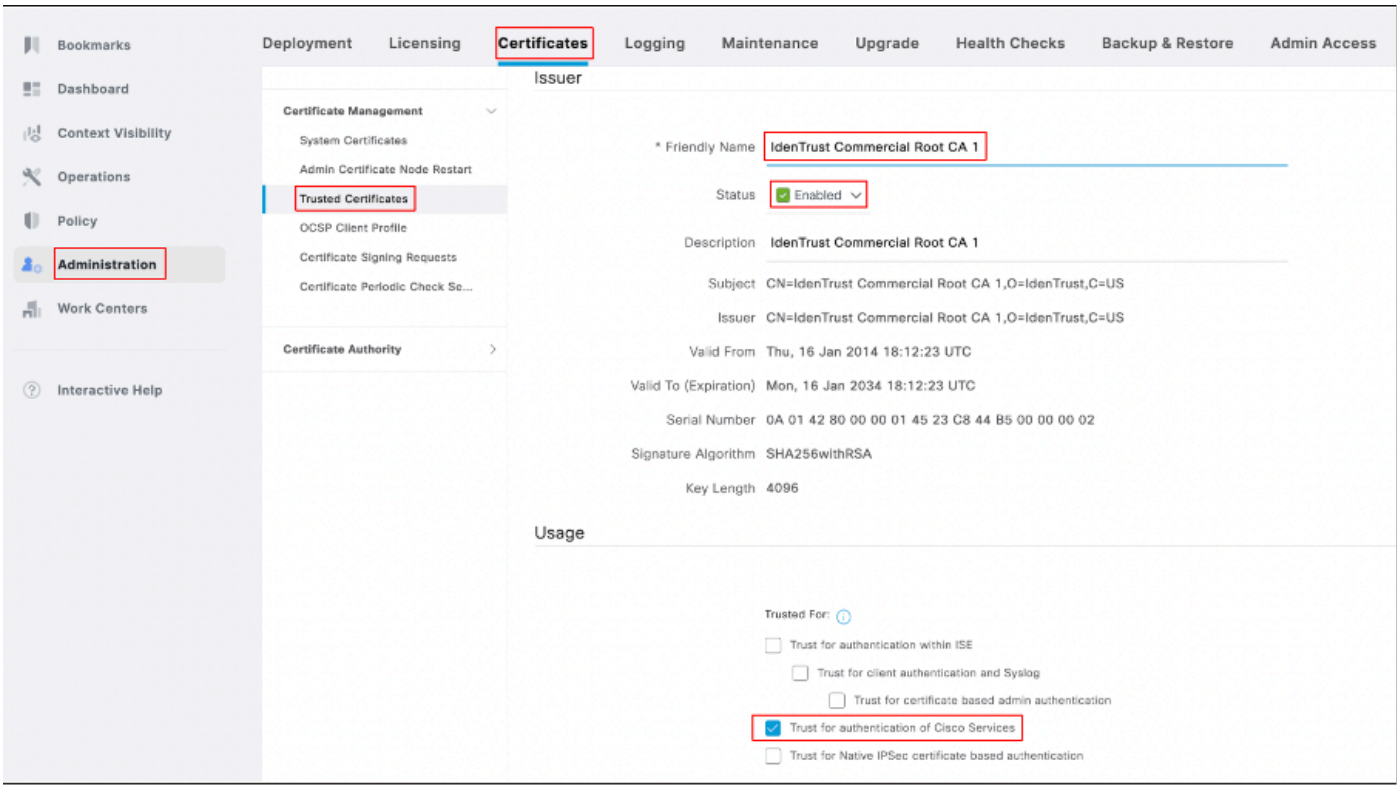
```
Certificates Length: 5083
Certificates (5083 bytes)
Certificate Length: 1940
Certificate: 3082079030820678a003020102021040191d1f3c7ec4ea73b301be3e06a90300d06092a… (id-at-commonNam
Certificate Length: 1754
Certificate: 308206d6308204bea003020102021040016efb0a205cfaebe18f71d73abb78300d06092a… (id-at-commonNam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

IdenTrust Commercial Root CA

1

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

- Nell'interfaccia utente di ISE, è importante verificare che il certificato server IdenTrust Commercial Root CA 1 sia abilitato e che Trust per l'autenticazione dei servizi Cisco stabilisca la connettività con Cisco.com. Per impostazione predefinita, questo certificato è incluso in ISE e viene selezionata l'opzione "Trust for authentication Cisco services" (Affidabilità per l'autenticazione dei servizi Cisco), ma è consigliata la verifica.
- Controllare lo stato e l'utilizzo attendibile del certificato accedendo alla GUI ISE > Amministrazione > Certificati > Certificati attendibili. Filtrare in base al nome IdenTrust Commercial Root CA 1, selezionare il certificato e quindi modificarlo per verificare l'utilizzo del trust, come mostrato in questo screenshot:



- Gli aggiornamenti della postura possono includere criteri di postura nuovi o modificati, nuove definizioni antivirus/antimalware e altri criteri relativi alla sicurezza per le valutazioni della postura.
- Questo metodo richiede una connessione Internet attiva e viene in genere eseguito quando il sistema ISE è configurato per l'utilizzo di repository basati su cloud per gli aggiornamenti della postura.

Scenari d'uso

Gli aggiornamenti della postura online vengono utilizzati quando si desidera essere certi che i criteri di postura, le definizioni di sicurezza e i criteri siano aggiornati rispetto alle ultime versioni disponibili fornite da Cisco.

Porte utilizzate per l'aggiornamento della postura online

Per garantire che il sistema ISE possa raggiungere correttamente i server cloud Cisco per scaricare gli aggiornamenti della postura, queste porte devono essere aperte nel firewall e consentite per la comunicazione in uscita da ISE a Internet:

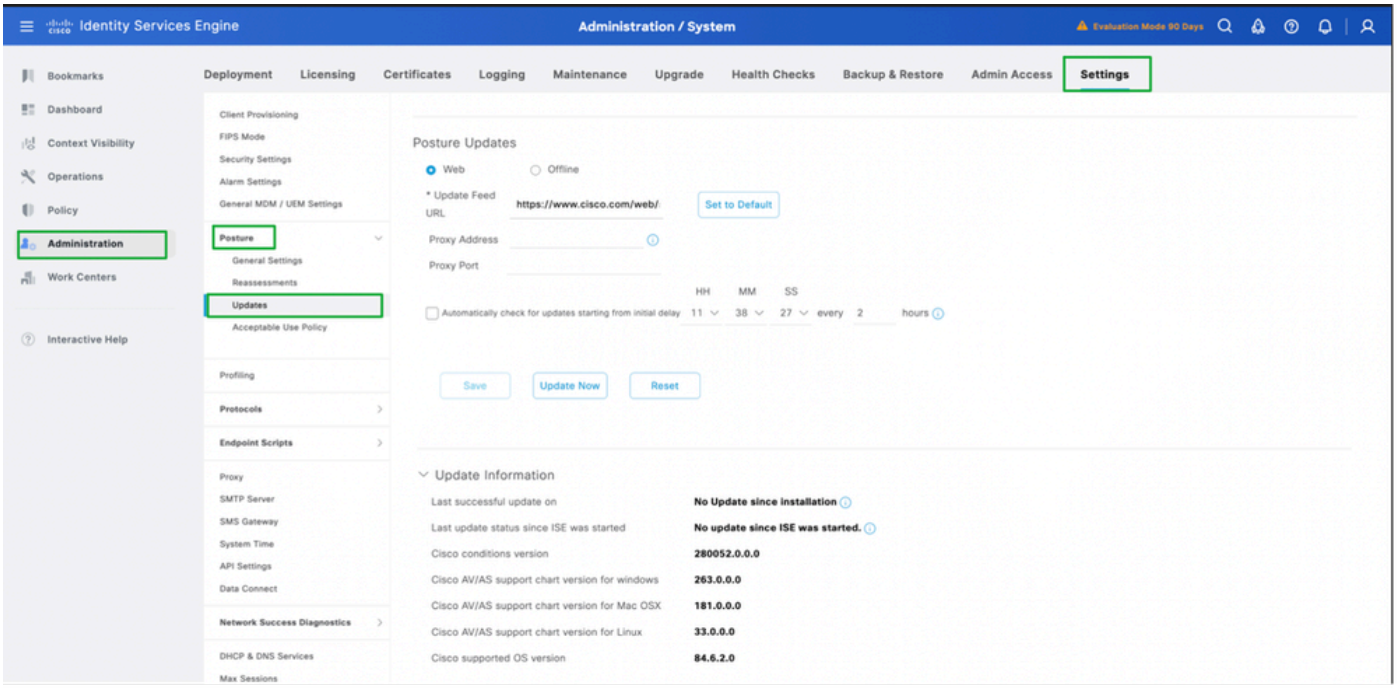
1. HTTPS (TCP 443):
    - La porta principale che consente ad ISE di raggiungere i server cloud Cisco e scaricare gli aggiornamenti tramite una connessione sicura (TLS/SSL).
    - Questa è la porta più importante per il processo di aggiornamento della postura basato sul Web.
2. DNS (UDP 53):
    - ISE deve essere in grado di eseguire ricerche DNS per risolvere i nomi host dei server di aggiornamento.

- Verificare che il sistema ISE in uso sia in grado di raggiungere i server DNS e risolvere i nomi di dominio.

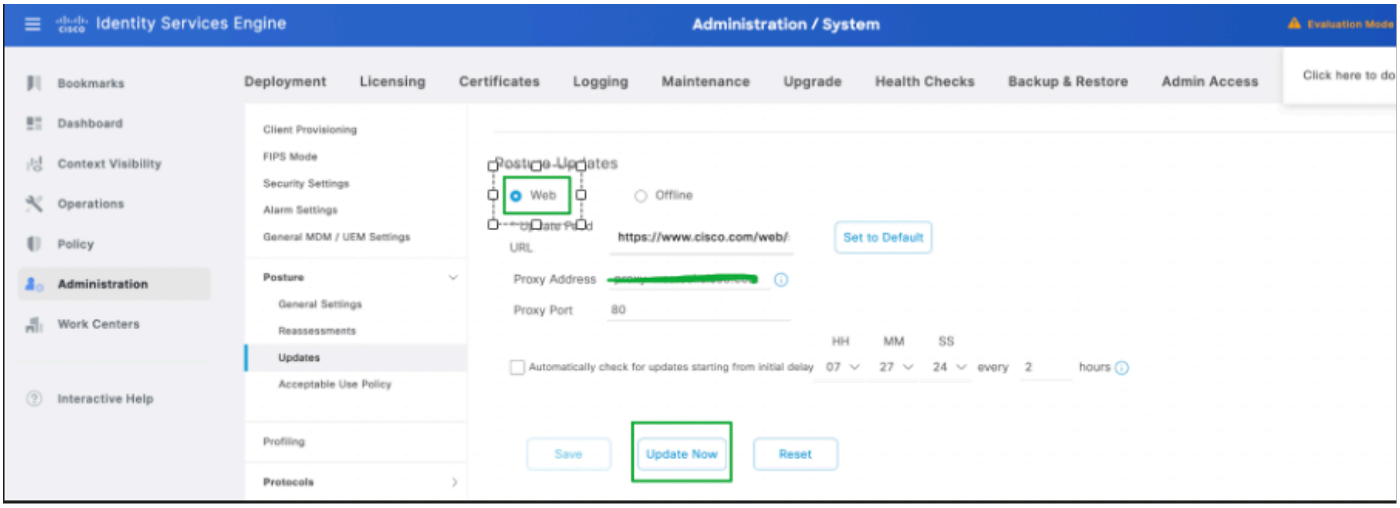
3. NTP (UDP 123):
   - ISE utilizza il protocollo NTP per la sincronizzazione dell'ora. Ciò è importante per assicurare che il processo di aggiornamento sia contrassegnato correttamente dall'indicatore orario e che il sistema ISE funzioni in un fuso orario sincronizzato.
   - In molti casi, i server NTP devono essere accessibili anche tramite UDP 123.

Procedura per eseguire gli aggiornamenti della postura in linea

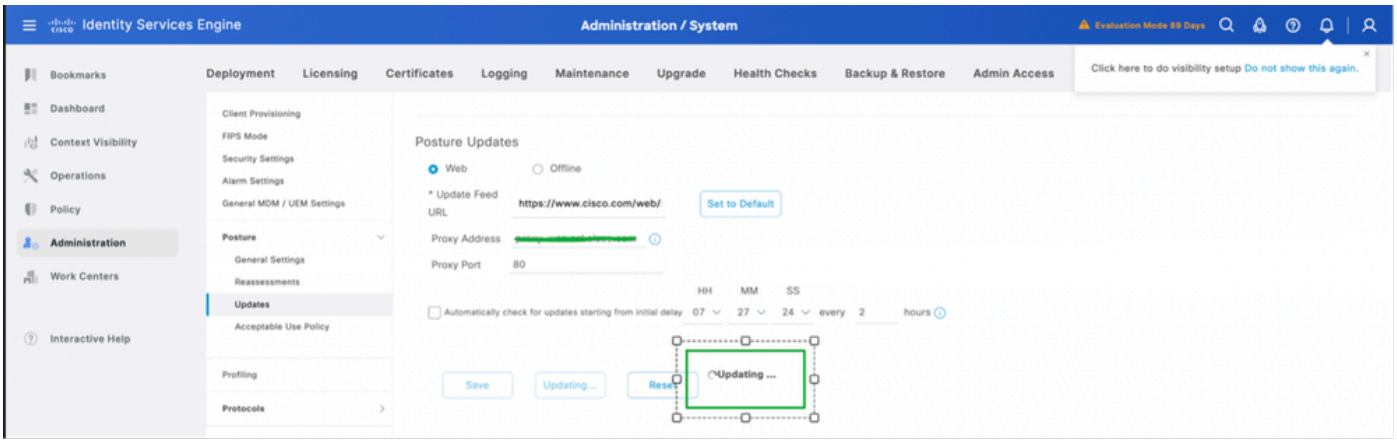
1. Accedere alla GUI -> Amministrazione -> Sistema -> Impostazioni -> Postura -> Aggiornamenti.



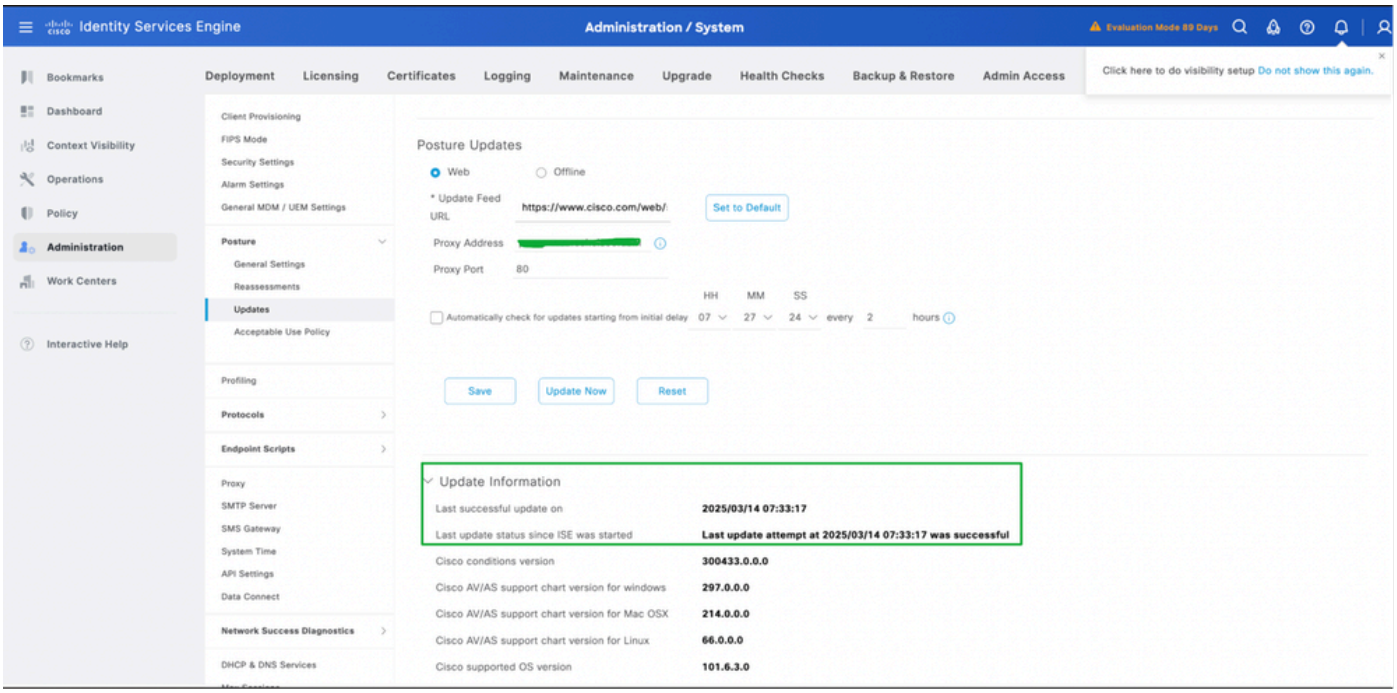
2. Selezionare il metodo come Web per Aggiornamenti postura in linea, fare clic su Aggiorna adesso.



3. Una volta iniziati gli aggiornamenti della postura, lo stato viene modificato in Aggiornamento.



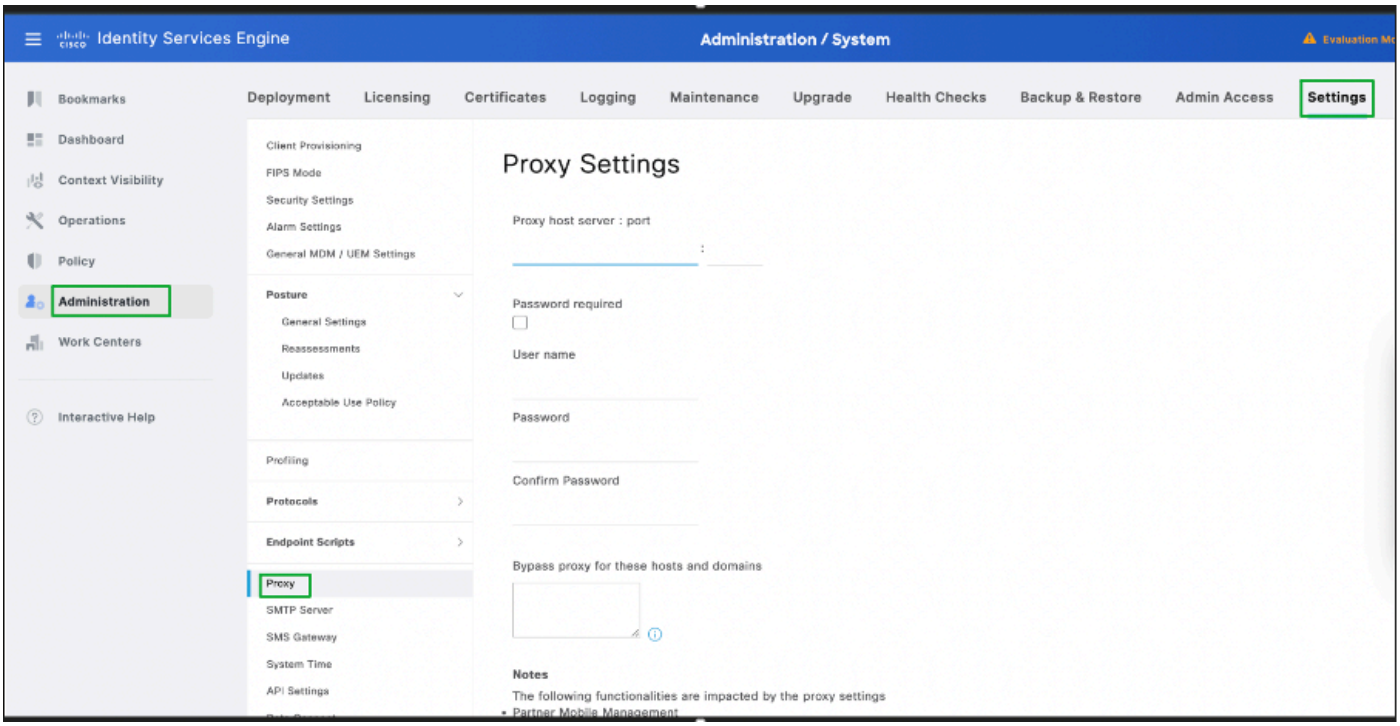
4. Lo stato degli aggiornamenti delle posture può essere verificato dalla finestra Aggiorna informazioni come indicato in questo screenshot:



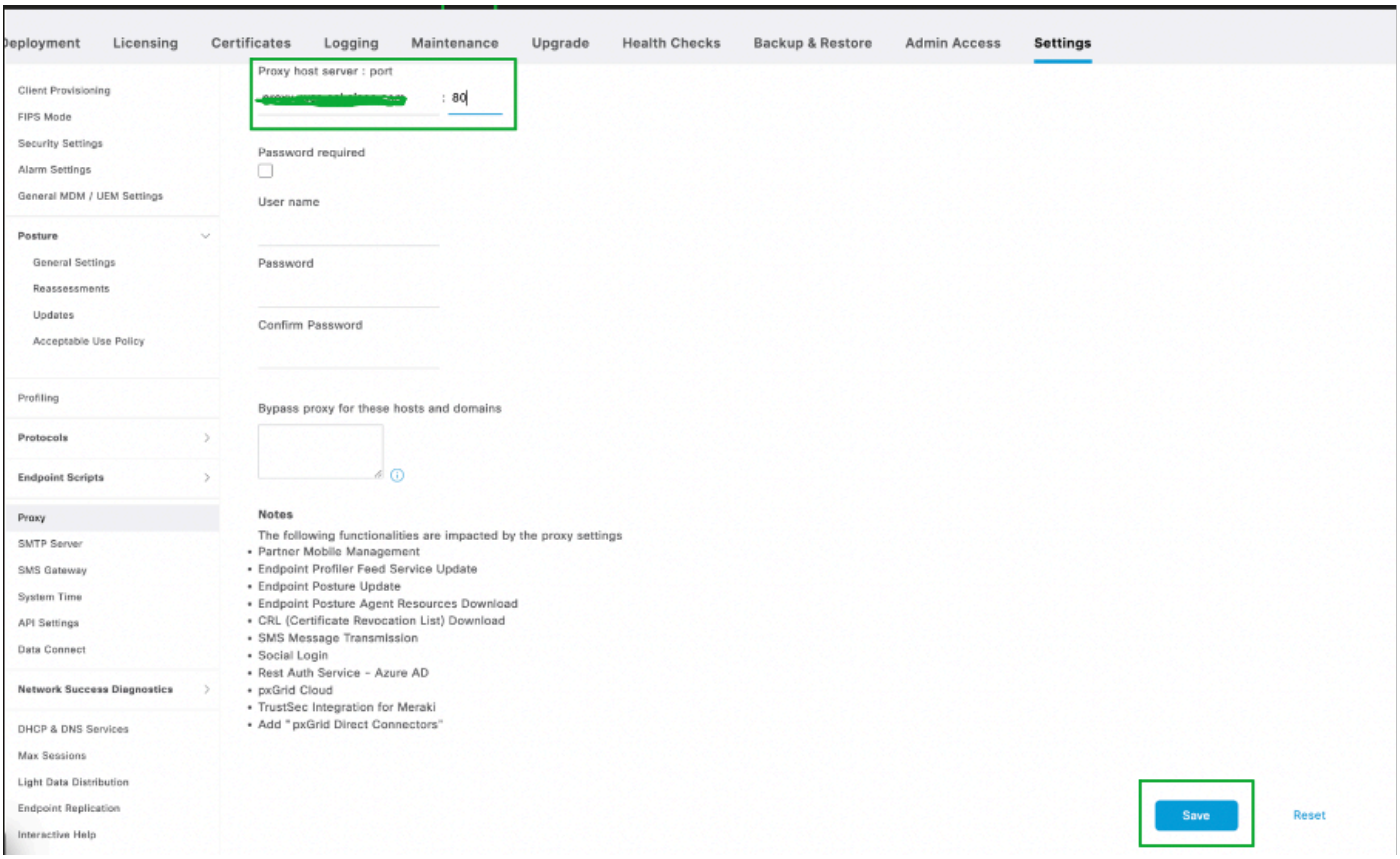
Configurazione proxy per gli aggiornamenti della postura online

In un ambiente limitato in cui l'URL del campo Aggiornamento postura non è accessibile, in questo caso è necessaria la configurazione proxy. Fare riferimento a Configure Proxy in ISE.

1. Passare a Amministrazione -> Sistema -> Impostazioni -> Proxy.



2. Configurare i dettagli del proxy e fare clic su Salva.



3. I dettagli del proxy vengono recuperati automaticamente da ISE quando vengono eseguiti gli aggiornamenti della postura online.

Aggiornamenti postura offline

L'opzione Offline Posture Update (Aggiornamento postura offline) consente di caricare manualmente i file di aggiornamento della postura (in formato .zip o in un altro formato di file supportato) in ISE.

Cosa succede quando si aggiorna la postura offline?

- I file di postura aggiornati vengono caricati manualmente.
- ISE elabora e applica questi file, che possono includere policy aggiornate, definizioni antivirus, valutazioni della postura, tra gli altri tipi di file.
- L'aggiornamento offline non richiede la connettività Internet e viene in genere utilizzato in ambienti con rigidi criteri di sicurezza o di rete che impediscono l'accesso diretto ai server esterni.

Scenari d'uso

Questo metodo viene spesso utilizzato in ambienti in cui il sistema è isolato da Internet o quando si hanno file di aggiornamento offline specifici forniti da Cisco o dal team di sicurezza.

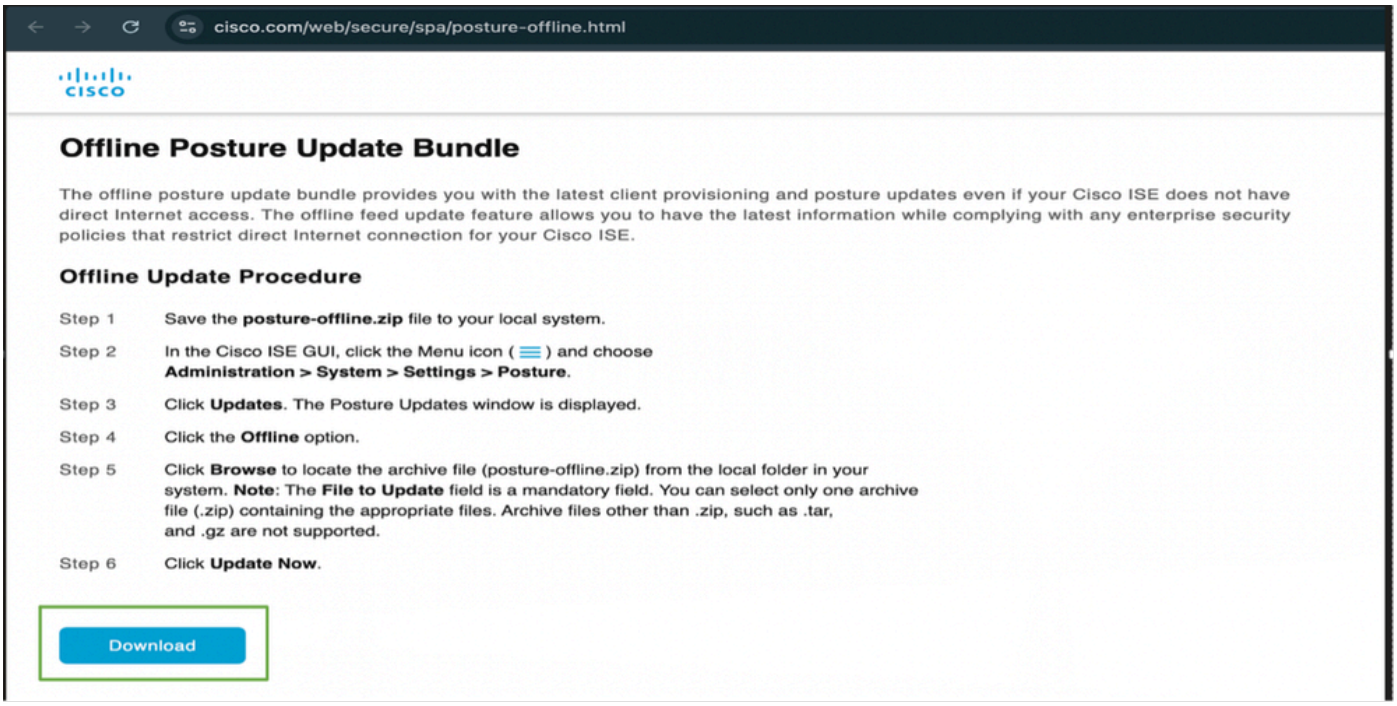
Porte utilizzate per gli aggiornamenti della postura offline

Per le comunicazioni generali con il server ISE (durante il processo di aggiornamento), in molti casi queste porte sono rilevanti:

1. Accesso alla gestione (porte 22, 443):
   - SSH (TCP 2): Se si utilizza SSH per accedere al sistema ISE per la risoluzione dei problemi o il caricamento manuale.
   - HTTPS (TCP 443): Se si utilizza la GUI (interfaccia Web) per il caricamento dell'aggiornamento.
2. Trasferimento file (SFTP o SCP):
   - Se è necessario caricare i file manualmente nell'ISE tramite SFTP o SCP, verificare che le porte corrispondenti (in genere la porta 22 per SSH/SFTP) siano aperte sul sistema ISE.
3. Accesso alla rete locale:
   - Assicurarsi che il sistema da cui si sta caricando l'aggiornamento (ad esempio, una postura di amministrazione o un server) possa comunicare con ISE attraverso le porte necessarie per l'accesso di gestione, ma anche in questo caso gli aggiornamenti di postura offline non richiedono porte esterne poiché i file vengono forniti manualmente.

Dove trovare i file per gli aggiornamenti della postura offline?

1. Passa all'URL: https://www.cisco.com/web/secure/spa/posture-offline.html , fare clic su Download e il file posture-offline.zip viene scaricato nel sistema locale.

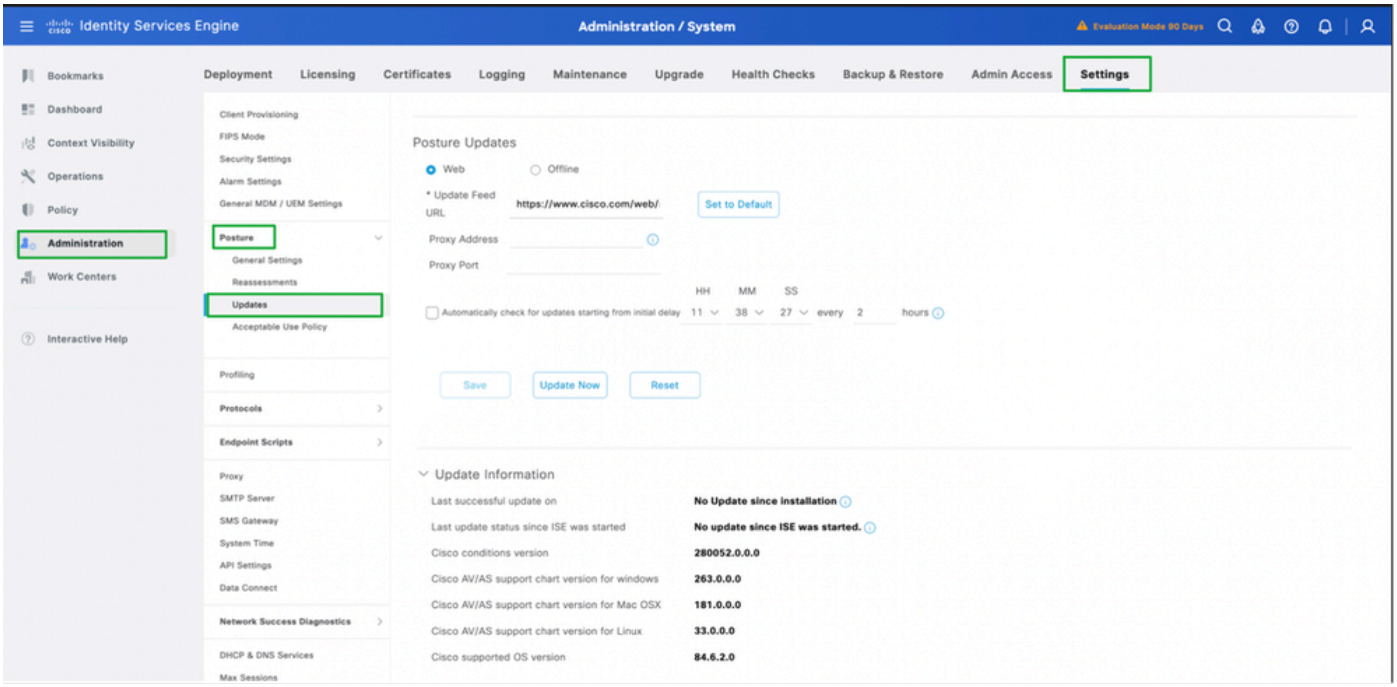


I file di aggiornamento della postura non in linea includono

- Definizioni antivirus (firme).
- Regole e criteri di postura.
- Valutazioni della sicurezza e altri file di configurazione per la valutazione della postura.

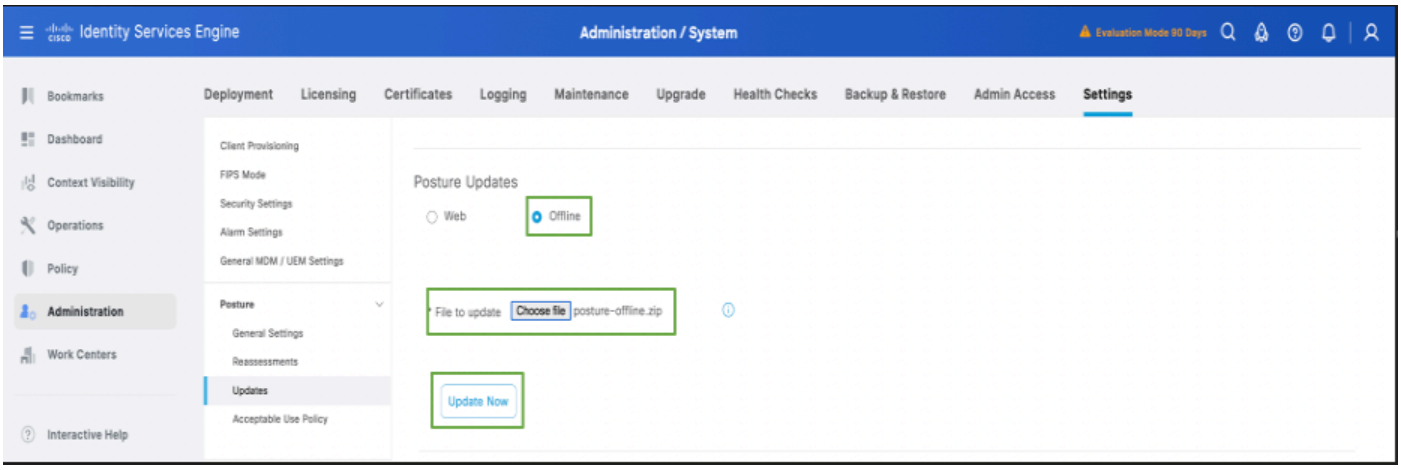
Procedura per eseguire gli aggiornamenti della postura non in linea

1. Accedere alla GUI di ISE -> Administration > System > Settings > Posture > Updates (Amministrazione > Sistema > Impostazioni > Postura > Aggiornamenti).

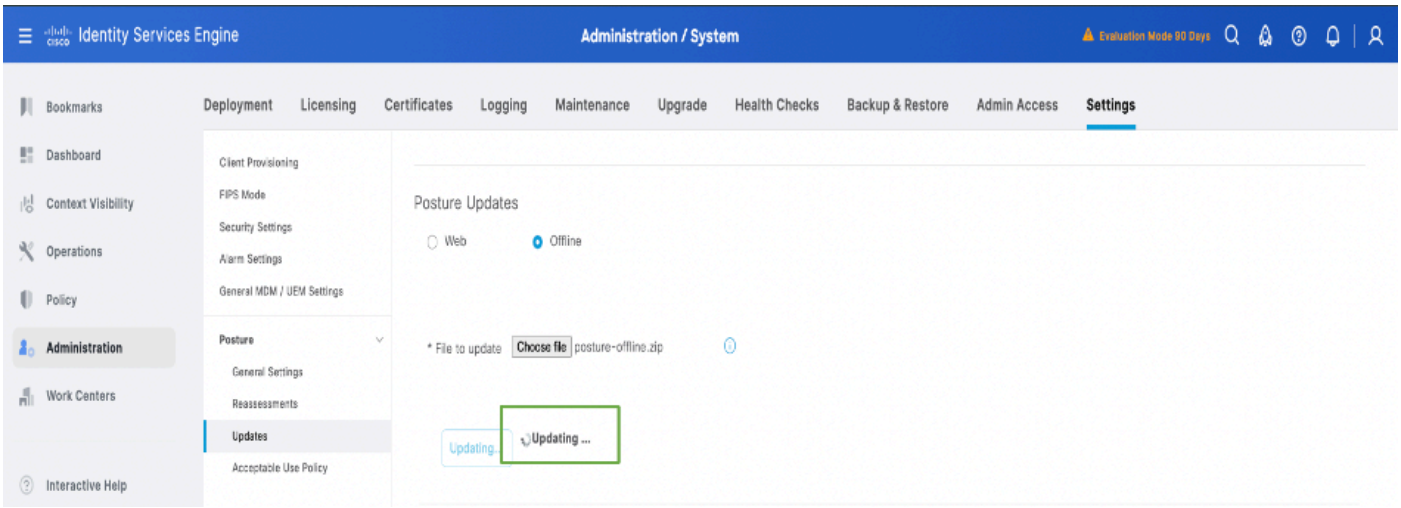


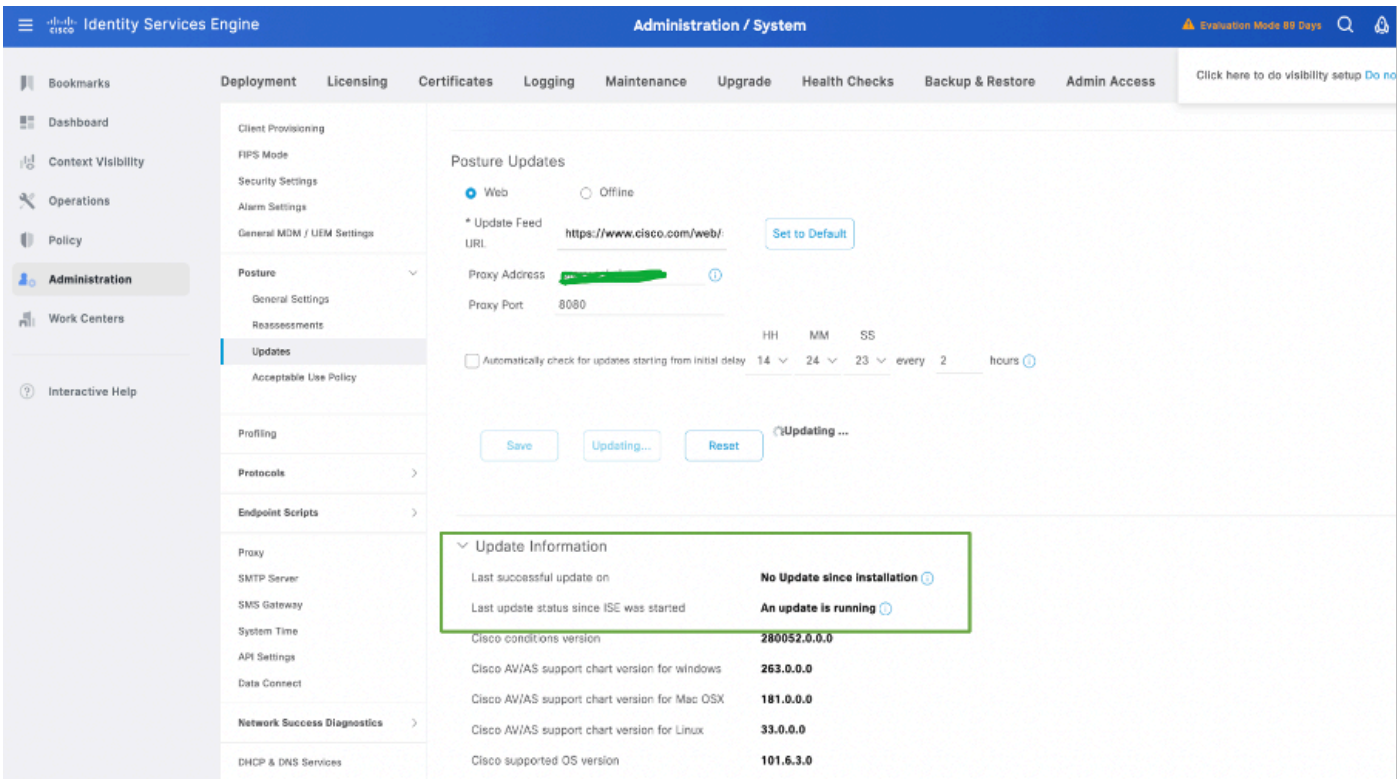
2. Selezionare l'opzione offline, sfogliare e selezionare la cartella posture-offline.zip che è stata

scaricata nel sistema locale. Fare clic su Aggiorna.

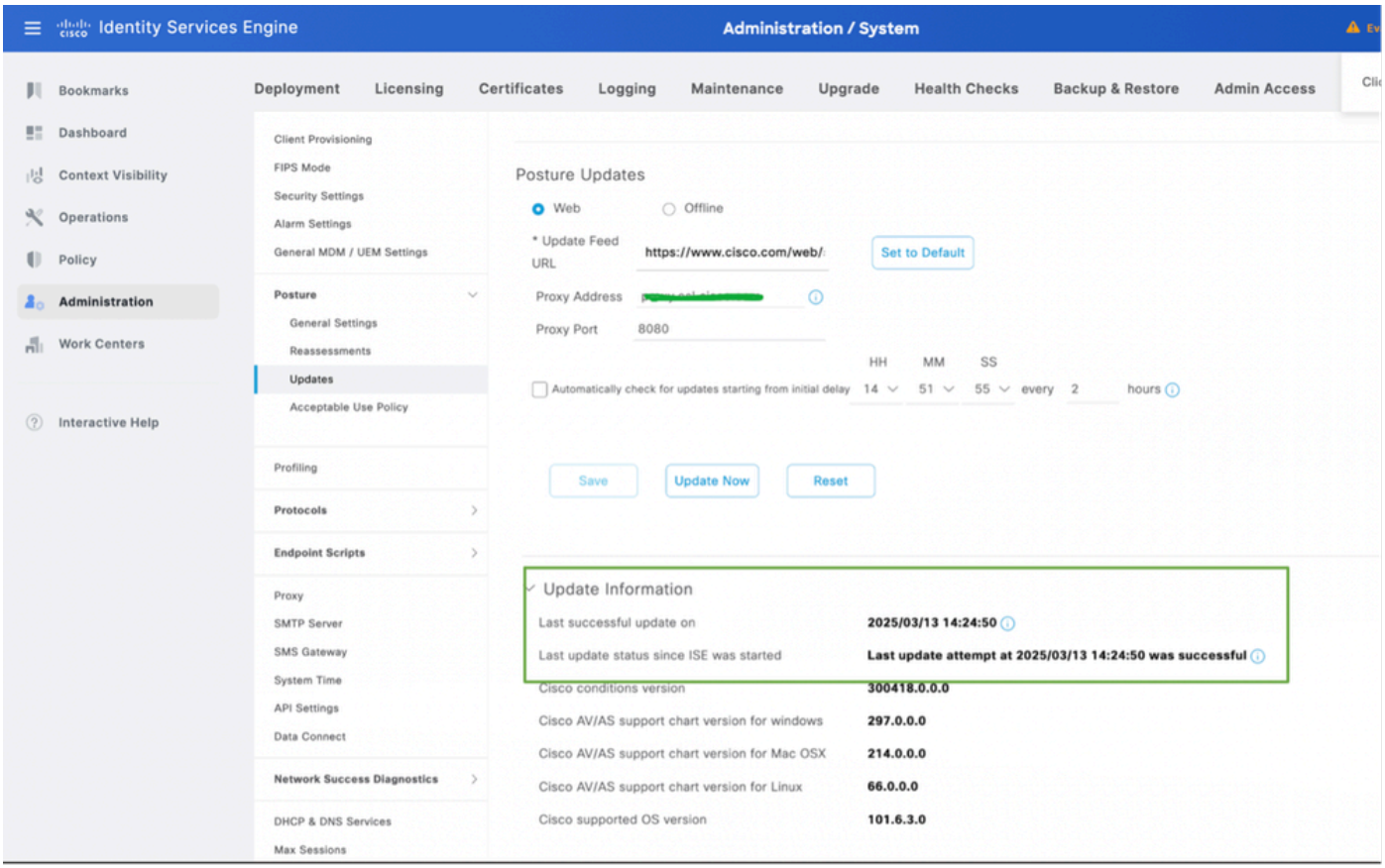


3. Una volta iniziati gli aggiornamenti della postura, lo stato viene modificato in Aggiornamento.





4. Lo stato degli aggiornamenti delle posture può essere verificato dalla finestra Aggiorna informazioni come indicato in questo screenshot:



Verifica

Accedere alla GUI del nodo Amministratore primario -> Operazioni -> Risoluzione dei problemi -> Log di download -> Log di debug -> Log applicazioni -> isc-psc.log , fare clic su ise-psc.log e il log viene scaricato nel sistema locale. Aprire il file scaricato tramite il Blocco note o l'editor di testo e filtrare per il download Opswat. È necessario essere in grado di trovare le informazioni relative agli aggiornamenti di postura eseguiti nella distribuzione.

È inoltre possibile limitare i log eseguendo il login alla CLI del nodo Admin primario utilizzando il comando show logging application ise-psc.log tail.

Viene avviato il download di Opswat, che fa riferimento agli aggiornamenti della postura:

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

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

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

Download di Opswat completato. Gli aggiornamenti della postura sono stati scaricati e completati.

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

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

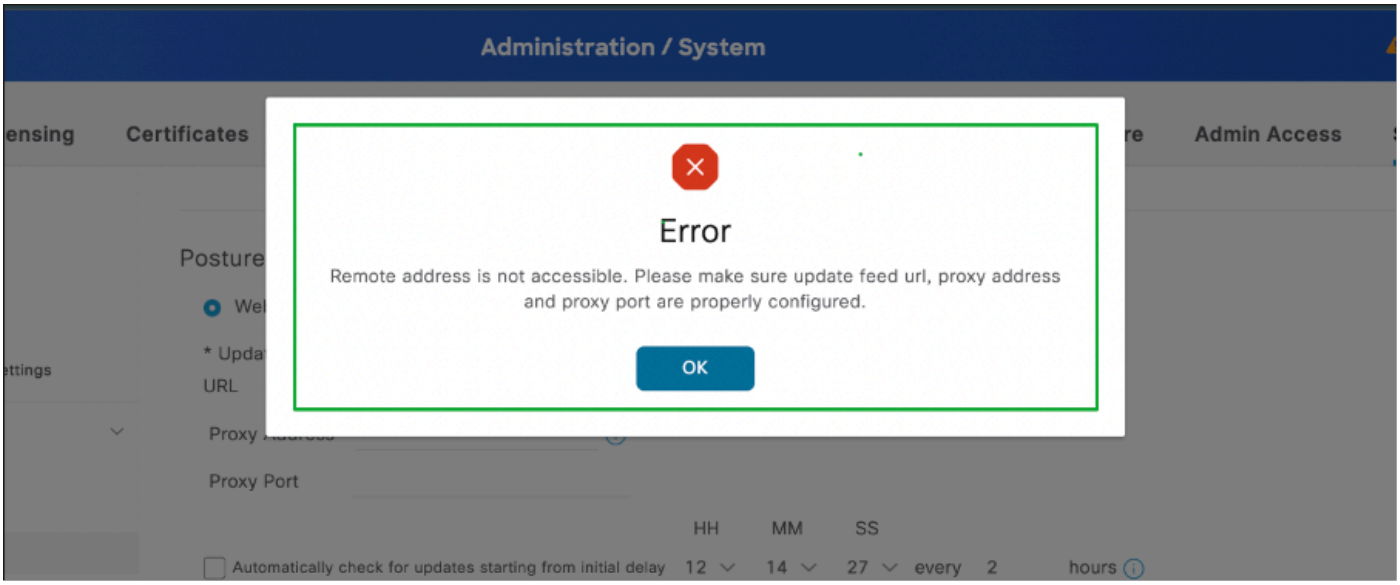
2025-03-13 14:24:50,827 INFO [admin-http-pool5][[]]
mnt.dbms.datadirect.impl.DatadirectServiceImpl -::admin::- Esecuzione di getStatus - datadirectSettings

Risoluzione dei problemi

Scenario

Aggiornamenti postura online non riusciti con l'errore "Indirizzo remoto non accessibile. Verificare che l'URL del feed di aggiornamento, l'indirizzo proxy e la porta proxy siano configurati correttamente".

Errore di esempio:



Soluzione

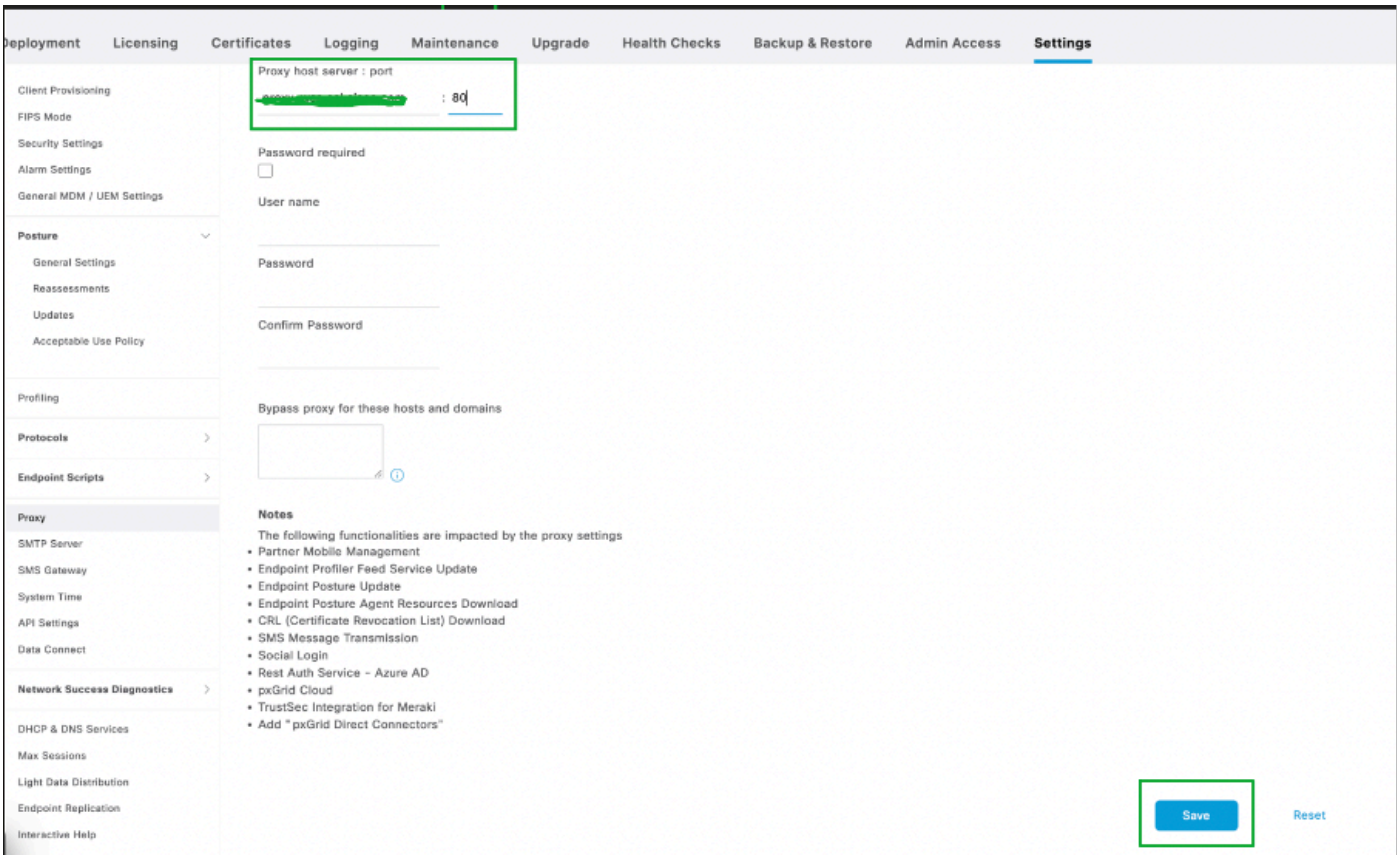
1. Accedere alla CLI di ISE e verificare che ISE sia raggiungibile da cisco.com usando il comando "ping cisco.com".

nomehost/admin#ping cisco.com
PING cisco.com (72.163.4.161) 56(84) byte di dati.
64 byte da 72.163.4.161: icmp_seq=1 ttl=235 time=238 ms
64 byte da 72.163.4.161: icmp_seq=2 ttl=235 time=238 ms

64 byte da 72.163.4.161: icmp_seq=3 ttl=235 tempo=239 ms
64 byte da 72.163.4.161: icmp_seq=4 ttl=235 time=238 ms

— cisco.com statistiche ping —
4 pacchetti trasmessi, 4 ricevuti, 0% di perdita, tempo 3004 ms
rtt min/media/max/mdev = 238,180/238,424/238,766/0,410 ms

2. Passare a Amministrazione -> Sistema -> Impostazioni -> Il proxy è configurato con le porte corrette.



3. Verificare che le porte TCP 443, UDP 53 e UDP 123 siano consentite su tutti gli hop verso Internet.

Difetti noti per problemi di aggiornamento della postura

ID bug Cisco 01523

Riferimento

- Guida dell'amministratore di Cisco Identity Services Engine, versione 3.3

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).