

在ISE中執行狀態更新，離線和線上

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[線上狀態更新](#)

[網路或線上狀態更新期間會發生什麼情況？](#)

[使用時機](#)

[用於線上狀態更新的埠](#)

[執行線上狀態更新的過程](#)

[線上狀態更新的代理配置](#)

[離線狀態更新](#)

[執行離線狀態更新時會發生什麼情況？](#)

[使用時機](#)

[用於離線狀態更新的埠](#)

[在哪裡查詢用於離線狀態更新的檔案？](#)

[離線狀態更新檔案包括](#)

[執行離線狀態更新的過程](#)

[驗證](#)

[疑難排解](#)

[案例](#)

[解決方案](#)

[狀態更新問題的已知缺陷](#)

[參考](#)

簡介

本文檔介紹如何在Cisco Identity Services Engine®(ISE)中執行狀態更新。

必要條件

需求

思科建議您瞭解安全評估流程。

採用元件

本檔案中的資訊是根據這些硬體和軟體版本。

- Cisco Identity Services Engine 3.2及更高版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

終端安全評估更新包括一組預定義的檢查、規則和支援圖表，用於針對Windows和MacOS作業系統的防病毒和反間諜軟體以及思科支援的作業系統資訊。

當您首次在網路中部署思科ISE時，您可以從Web下載終端安全評估更新。此過程通常需要大約20分鐘。初始下載後，您可以配置思科ISE以驗證並下載自動發生的增量更新。

思科ISE僅在初始狀態更新期間建立一次預設狀態策略、要求和補救。如果刪除它們，思科ISE不會在後續手動或計畫更新期間再次建立它們。

您可以執行兩種狀態更新：

- 線上狀態更新。
- 離線狀態更新。

線上狀態更新

Web Posture Update/ Online Posture Update可從思科雲或伺服器儲存庫檢索最新的狀態更新。這包括直接從思科伺服器下載最新的策略、定義和簽名。ISE需要連線到思科雲伺服器或更新儲存庫，以檢索最新的狀態定義、策略和其他關聯檔案。

網路或線上狀態更新期間會發生什麼情況？

身份服務引擎(ISE)使用HTTP通過代理或直接網際網路連線訪問思科網站，建立與www.cisco.com的連線。在此過程中，發生客戶端hello和伺服器hello交換，伺服器提供證書以驗證其合法性和確認客戶端信任。完成客戶端hello和伺服器hello後，客戶端金鑰交換發生，伺服器啟動狀態更新。以下資料包捕獲演示線上狀態更新期間ISE伺服器與Cisco.com之間的通訊。

Ttl	Source	Dest	Len	Protocol	Info
347	10.1...	17...	-	TCP	46618 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=236258549 TSecr=0 WS=128
348	173...	10...	-	TCP	80 → 46618 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1380 WS=64 SACK_PERM TSval=654726948 TSecr=236258549
349	10.1...	17...	-	TCP	46618 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=236258722 TSecr=654726948
350	10.1...	17...	-	HTTP	CONNECT www.cisco.com:443 HTTP/1.1
351	173...	10...	-	TCP	[TCP Window Update] 80 → 46618 [ACK] Seq=1 Ack=1 Win=262464 Len=0 TSval=654726948 TSecr=236258722
352	173...	10...	-	TCP	80 → 46618 [ACK] Seq=1 Ack=94 Win=262336 Len=0 TSval=654726948 TSecr=236258723
353	173...	10...	-	HTTP	HTTP/1.1 200 Connection established
354	10.1...	17...	-	TCP	46618 → 80 [ACK] Seq=94 Ack=40 Win=29312 Len=0 TSval=236259042 TSecr=654727088
355	10.1...	17...	-	TLSv1.2	Client Hello
356	173...	10...	-	TCP	80 → 46618 [ACK] Seq=40 Ack=403 Win=262144 Len=0 TSval=654727308 TSecr=236259084
357	173...	10...	-	TCP	80 → 46618 [ACK] Seq=40 Ack=403 Win=262464 Len=1348 TSval=654727448 TSecr=236259084 [TCP segment of a reassembled PDU]
358	10.1...	17...	-	TCP	46618 → 80 [ACK] Seq=403 Ack=1388 Win=32128 Len=0 TSval=236259403 TSecr=654727448
359	173...	10...	-	TLSv1.2	Server Hello, Certificate
360	10.1...	17...	-	TCP	46618 → 80 [ACK] Seq=403 Ack=5217 Win=39808 Len=0 TSval=236259404 TSecr=654727448
361	173...	10...	-	TLSv1.2	Server Key Exchange, Server Hello Done
362	10.1...	17...	-	TCP	46618 → 80 [ACK] Seq=403 Ack=5559 Win=42496 Len=0 TSval=236259404 TSecr=654727448
363	10.1...	17...	-	TLSv1.2	Client Key Exchange
364	10.1...	17...	-	TLSv1.2	Change Cipher Spec
365	10.1...	17...	-	TLSv1.2	Encrypted Handshake Message
366	173...	10...	-	TCP	80 → 46618 [ACK] Seq=5559 Ack=478 Win=262400 Len=0 TSval=654727638 TSecr=236259416
367	173...	10...	-	TCP	80 → 46618 [ACK] Seq=5559 Ack=484 Win=262464 Len=0 TSval=654727638 TSecr=236259418
368	173...	10...	-	TCP	80 → 46618 [ACK] Seq=5559 Ack=529 Win=262400 Len=0 TSval=654727638 TSecr=236259418
369	173...	10...	-	TLSv1.2	Change Cipher Spec
370	173...	10...	-	TLSv1.2	Encrypted Handshake Message
371	10.1...	17...	-	TCP	46618 → 80 [ACK] Seq=529 Ack=5610 Win=42496 Len=0 TSval=236259736 TSecr=654727788
372	10.1...	17...	-	TLSv1.2	Application Data

- 在Server Hello期間，Cisco.com會將這些證書傳送給客戶端，以確認客戶端信任。

<#root>

Certificates Length: 5083

Certificates (5083 bytes)

Certificate Length: 1940

Certificate: 3082079030820678a0030201020210400191d1f3c7ec4ea73b301be3e06a90300d06092a... (id-at-commonName

Certificate Length: 1754

Certificate: 308206d6308204bea003020102021040016efb0a205cfaebe18f71d73abb78300d06092a... (id-at-commonName

Certificate Length: 1380

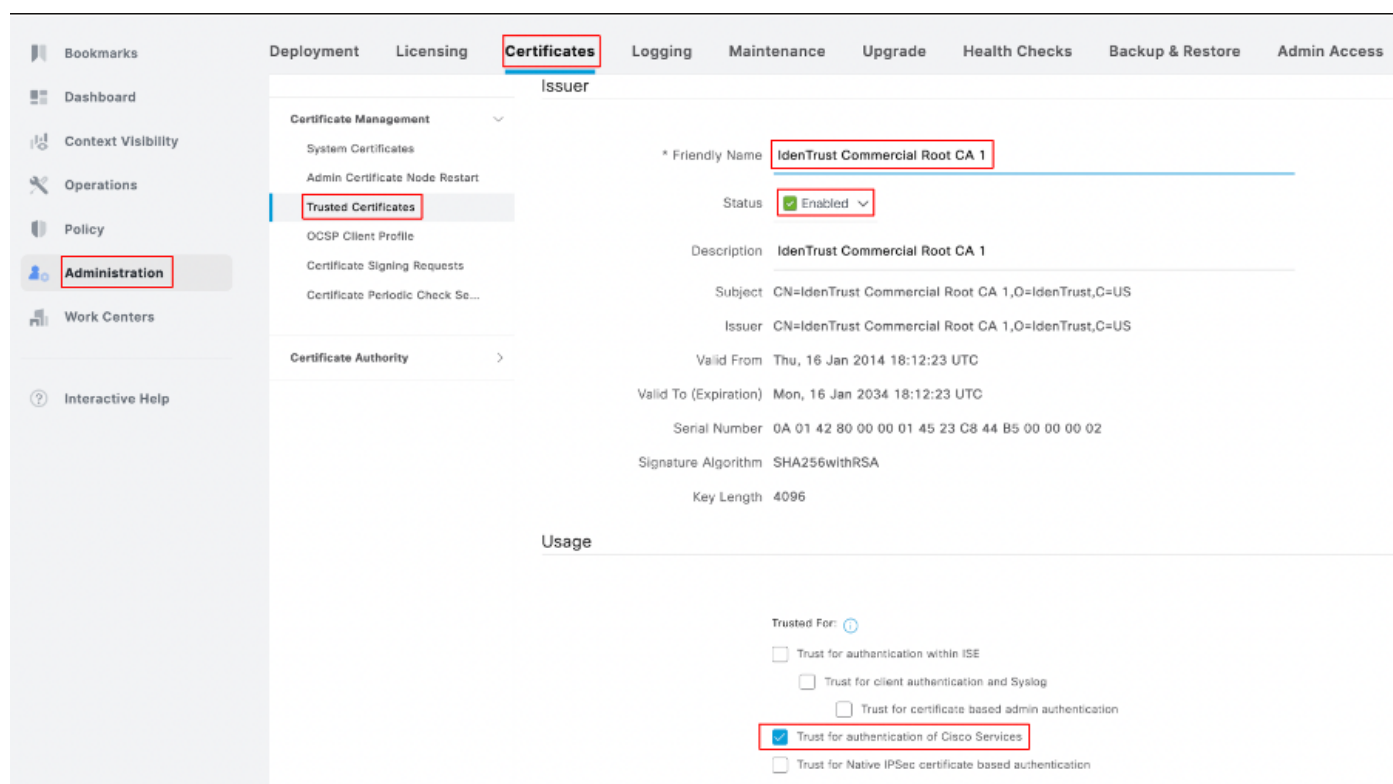
Certificate: 3082056030820348a00302010202100a0142800000014523c844b500000002300d06092a... (id-at-commonName

IdenTrust Commercial Root CA

1

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

- 在ISE GUI中，務必確保啟用伺服器證書IdenTrust商業根CA 1，並啟用用於驗證Cisco服務的Trust以建立與Cisco.com的連線。預設情況下，此證書包含在ISE中，並選中「Trust for authentication Cisco services」，但建議進行驗證。
- 通過轉至ISE GUI > Administration > Certificates > Trusted Certificates檢查證書狀態和受信任的使用。按名稱IdenTrust Commercial Root CA 1進行篩選，選擇證書，然後編輯證書以驗證信任使用情況，如下螢幕截圖所示：



- 安全狀態更新可以包括新的或修訂的安全狀態策略、新的防病毒/防惡意軟體定義，以及其他安全相關標準以進行安全狀態評估。

- 此方法需要活動網際網路連線，通常在ISE系統配置為使用基於雲的儲存庫進行狀態更新時執行。

使用時機

當您希望確保安全評估策略、安全定義和標準與思科提供的最新可用版本保持一致時，可使用線上安全評估更新。

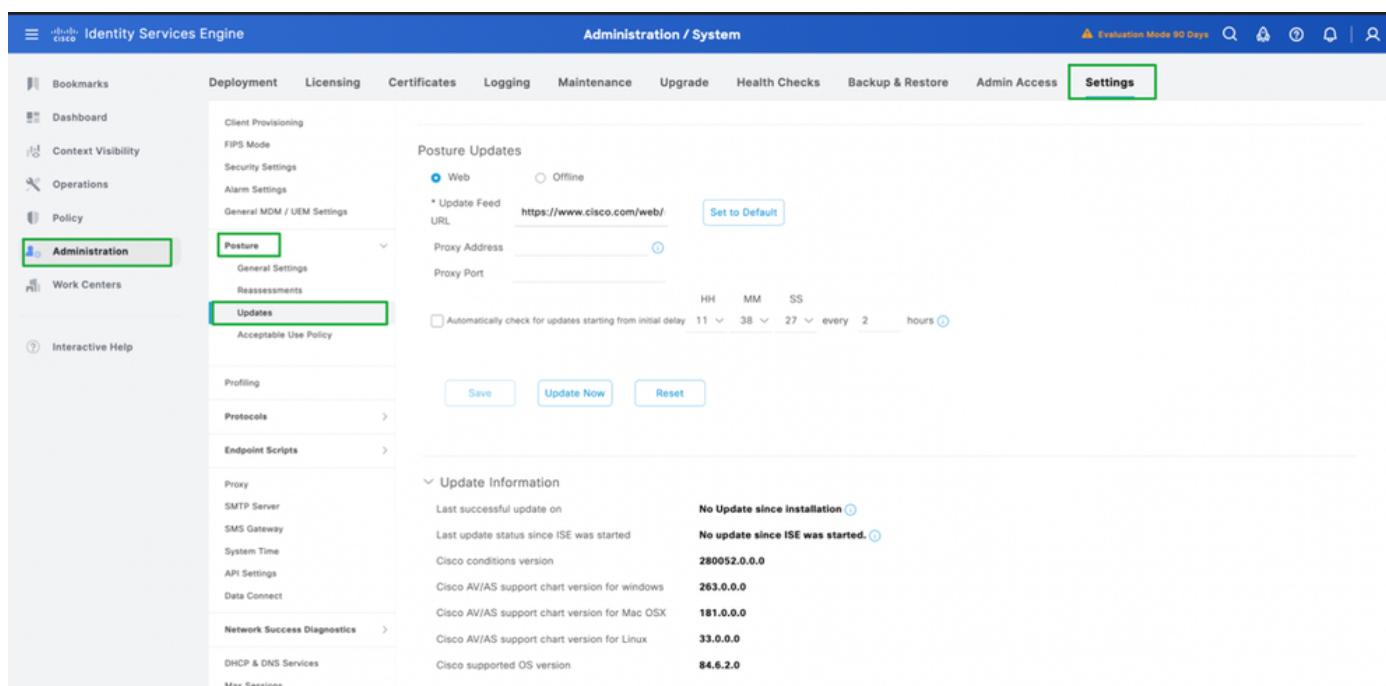
用於線上狀態更新的埠

要確保ISE系統可以成功到達思科雲伺服器下載狀態更新，必須在防火牆中開啟這些埠並允許從ISE到網際網路的出站通訊：

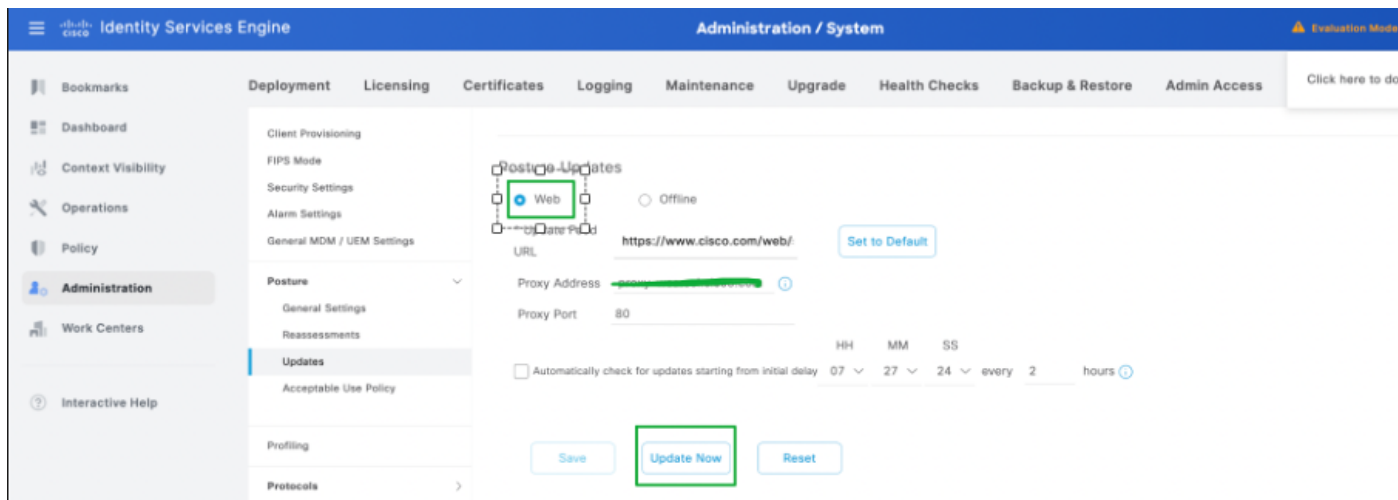
1. HTTPS(TCP 443):
 - ISE通過安全連線(TLS/SSL)訪問思科雲伺服器和下載更新的主埠。
 - 這是基於Web的終端安全評估更新流程的最關鍵埠。
2. DNS(UDP 53):
 - ISE必須能夠執行DNS查詢以解析更新伺服器的主機名。
 - 確保ISE系統可以訪問DNS伺服器並解析域名。
3. NTP(UDP 123):
 - ISE使用NTP進行時間同步。這對於確保更新過程的時間戳正確以及ISE系統在同步的時區運行非常重要。
 - 在許多情況下，還需要通過UDP 123訪問NTP伺服器。

執行線上狀態更新的過程

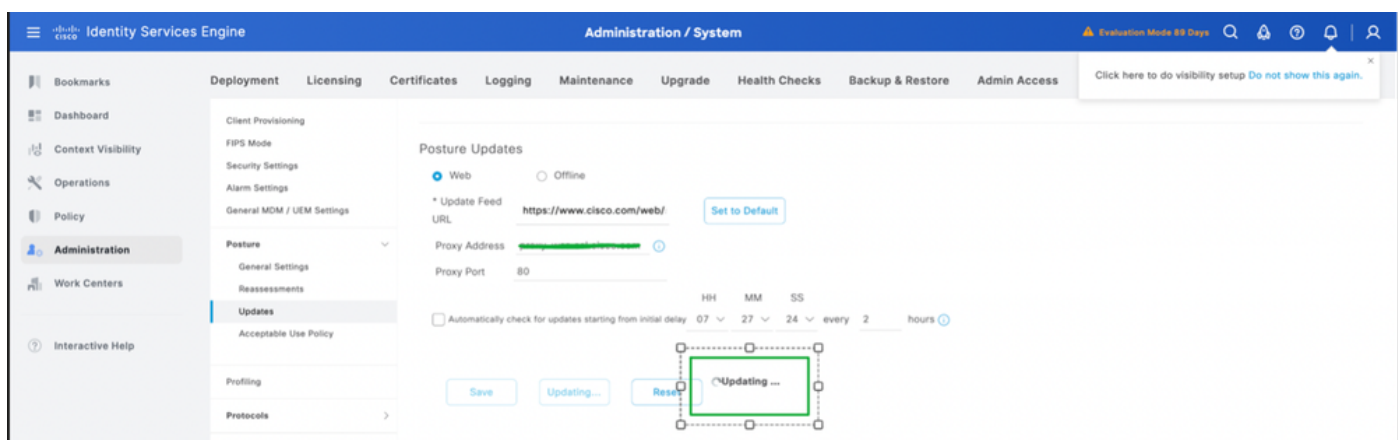
1. 登入到GUI -> Administration -> System -> Settings -> Posture -> Updates。



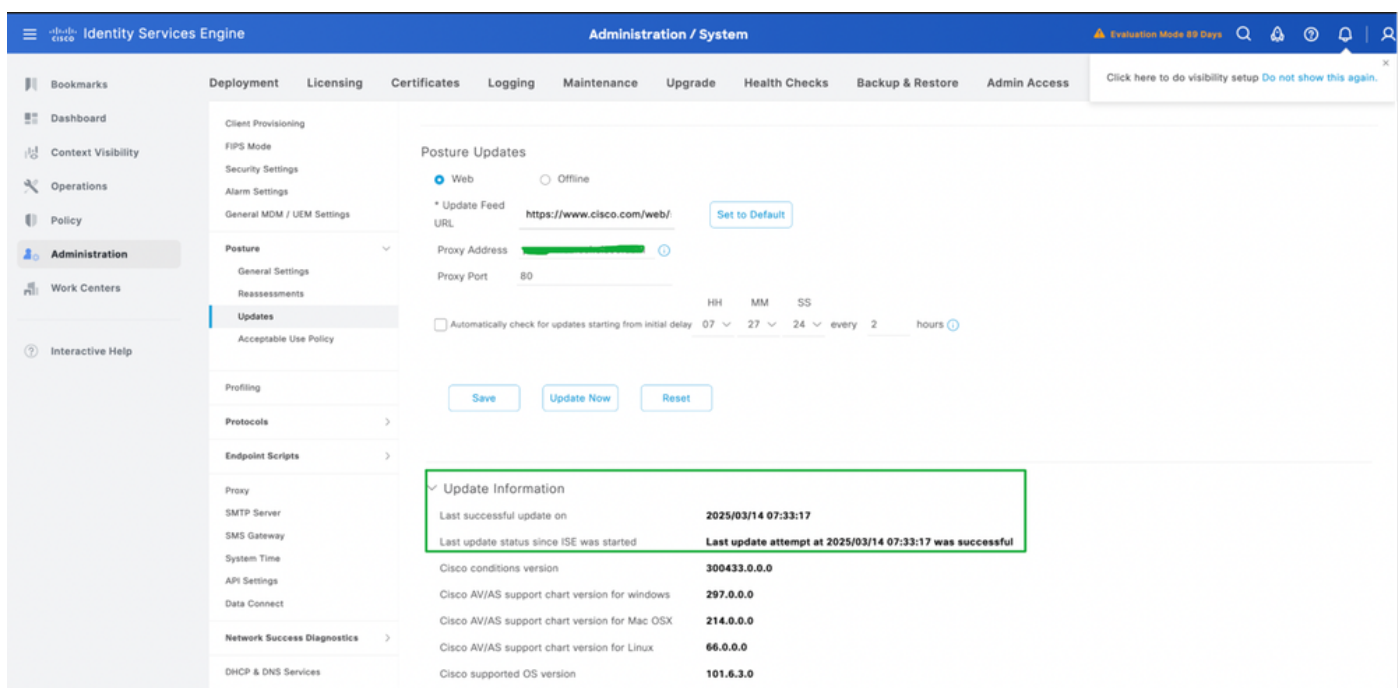
2. 選擇方法作為Web for Online Posture Updates，然後按一下Update Now。



3.狀態更新開始後，狀態將更改為Updating。



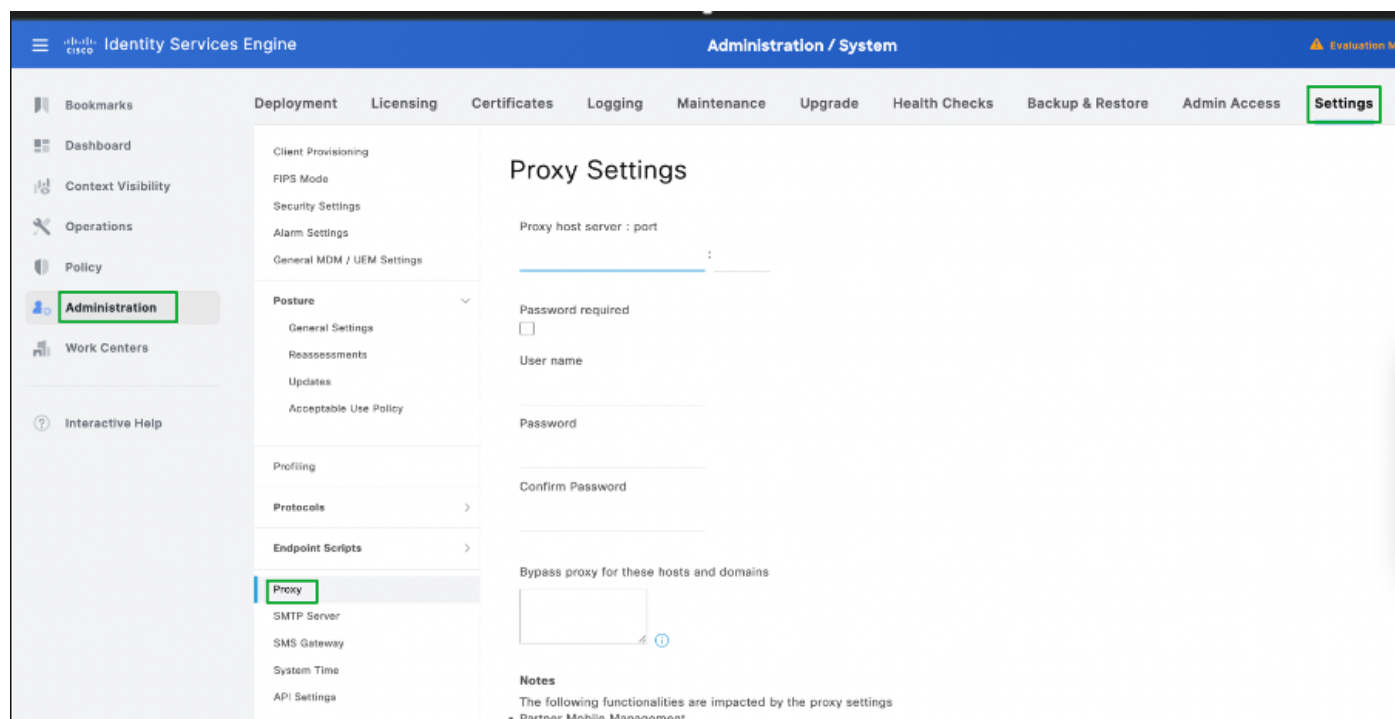
4.根據此螢幕截圖，可以從更新資訊驗證終端安全評估更新的狀態：



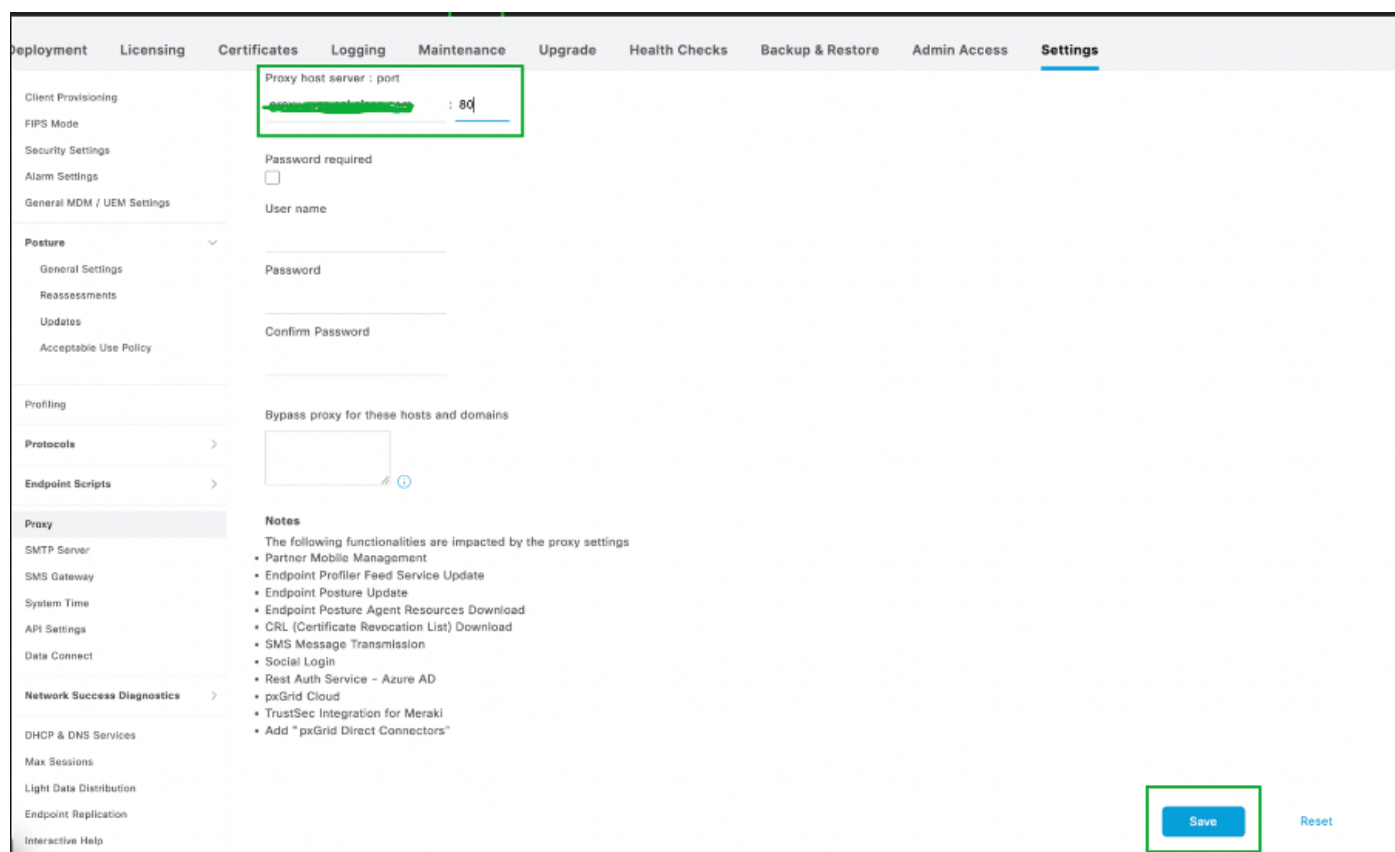
線上狀態更新的代理配置

在無法訪問終端安全評估更新欄位URL的受限環境中，在這種情況下，需要代理配置。請參閱在ISE中配置代理。

1. 導覽至Administration -> System -> Settings -> Proxy。



2. 配置代理詳細資訊，按一下儲存。



3. 執行線上狀態更新時，ISE會自動獲取代理的詳細資訊。

離線狀態更新

Offline Posture Update允許您手動將狀態更新檔案（以.zip或其他支援的檔案格式）上傳到ISE。

執行離線狀態更新時會發生什麼情況？

- 您手動上傳更新的狀態檔案。
- ISE處理和應用這些檔案，其中包括更新的策略、防病毒定義、狀況評估以及其他型別的檔案。
- 離線更新不需要Internet連線，通常用於具有嚴格安全或網路策略，防止直接訪問外部伺服器的環境中。

使用時機

此方法通常用於系統與Internet隔離的環境中，或者您擁有思科或您的安全團隊提供的特定離線更新檔案。

用於離線狀態更新的埠

對於與ISE伺服器的常規通訊（更新過程中），在許多情況下，這些埠是相關的：

1. 管理訪問（埠22、443）：
 - SSH(TCP 22):如果您使用SSH訪問ISE系統以進行故障排除或手動上傳。
 - HTTPS(TCP 443):如果您使用的是GUI（Web介面）進行更新上傳。
2. 檔案傳輸（SFTP或SCP）：
 - 如果需要通過SFTP或SCP手動將檔案上傳到ISE，請確保在ISE系統上開啟相應的埠（通常為SSH/SFTP的埠22）。
3. 本地網路訪問：
 - 確保您上傳更新的系統（例如，管理工作站或伺服器）可以通過管理訪問所需的埠與ISE通訊，但同樣，離線狀態更新不需要任何外部埠，因為檔案是手動提供的。

在哪裡查詢用於離線狀態更新的檔案？

1. 導覽至URL:<https://www.cisco.com/web/secure/spa/posture-offline.html>，按一下Download，將[posture-offline.zip](#) 檔案下載到您的本地系統。

cisco.com/web/secure/spa/posture-offline.html

Offline Posture Update Bundle

The offline posture update bundle provides you with the latest client provisioning and posture updates even if your Cisco ISE does not have direct Internet access. The offline feed update feature allows you to have the latest information while complying with any enterprise security policies that restrict direct Internet connection for your Cisco ISE.

Offline Update Procedure

- Step 1 Save the **posture-offline.zip** file to your local system.
- Step 2 In the Cisco ISE GUI, click the Menu icon (☰) and choose **Administration > System > Settings > Posture**.
- Step 3 Click **Updates**. The Posture Updates window is displayed.
- Step 4 Click the **Offline** option.
- Step 5 Click **Browse** to locate the archive file (posture-offline.zip) from the local folder in your system. **Note:** The **File to Update** field is a mandatory field. You can select only one archive file (.zip) containing the appropriate files. Archive files other than .zip, such as .tar, and .gz are not supported.
- Step 6 Click **Update Now**.

[Download](#)

離線狀態更新檔案包括

- 防病毒定義（簽名）。
- 狀態策略和規則。
- 安全評估和其他狀態評估配置檔案。

執行離線狀態更新的過程

1. 登入到ISE GUI -> Administration -> System -> Settings -> Posture -> Updates。

Identity Services Engine Administration / System

Settings

Posture Updates

☒ Web ☐ Offline

* Update Feed URL: <https://www.cisco.com/web/> [Set to Default](#)

Proxy Address:

Proxy Port:

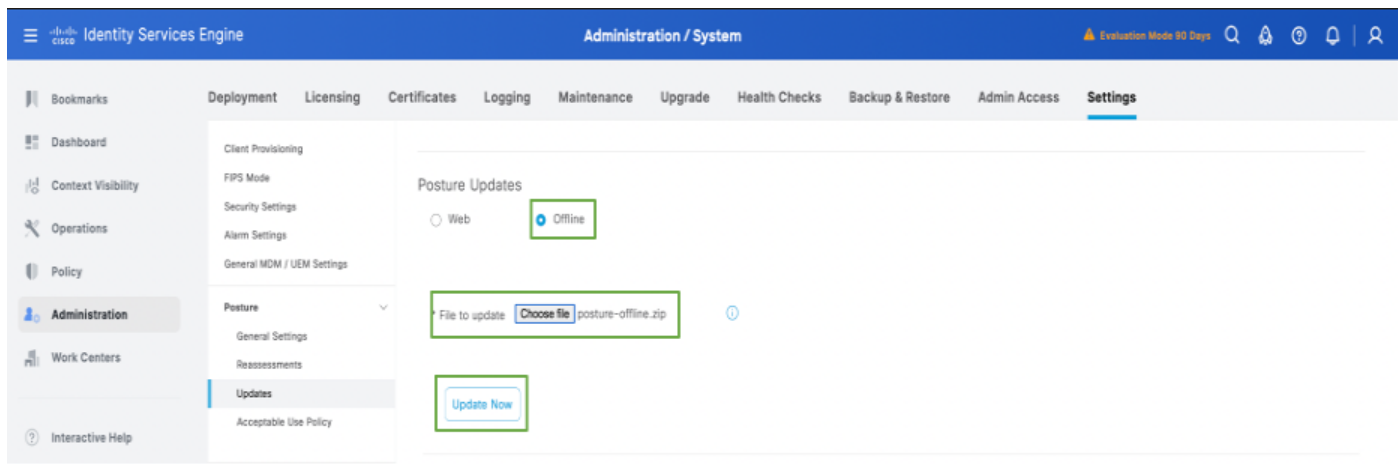
☐ Automatically check for updates starting from initial delay: HH:MM:SS every 2 hours

[Save](#) [Update Now](#) [Reset](#)

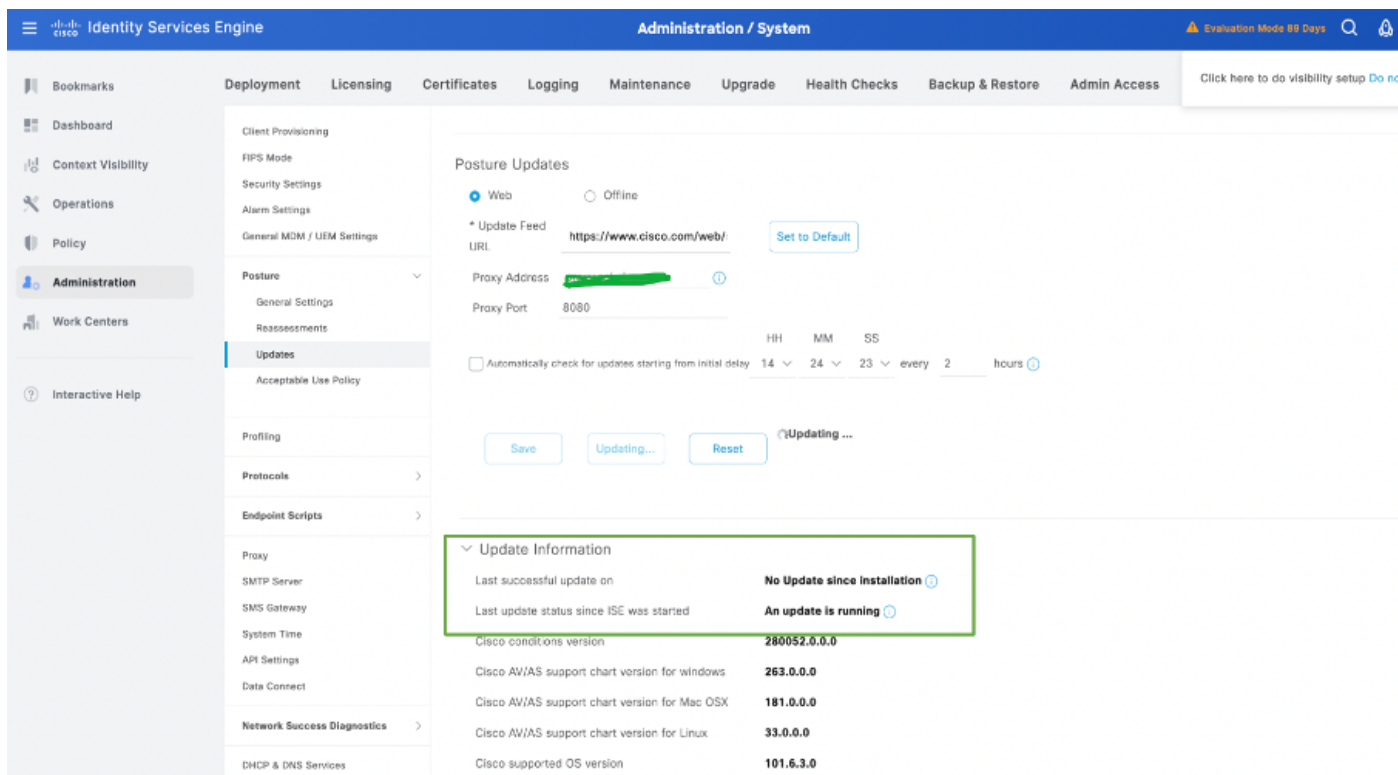
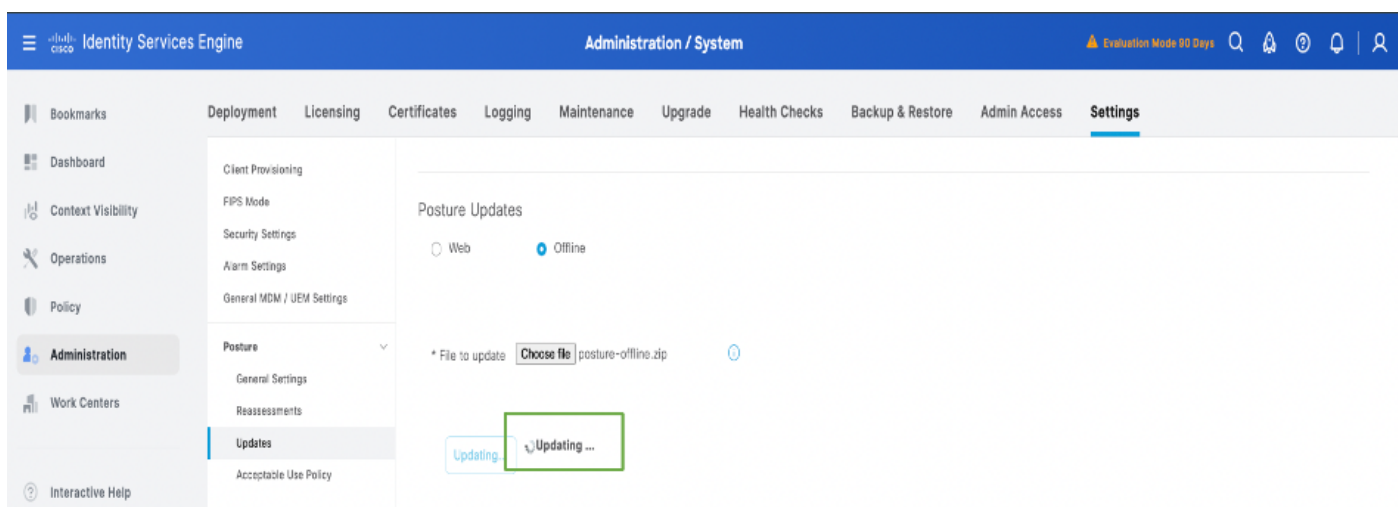
Update Information

Last successful update on	No Update since installation
Last update status since ISE was started	No update since ISE was started.
Cisco conditions version	280052.0.0.0
Cisco AV/AS support chart version for windows	263.0.0.0
Cisco AV/AS support chart version for Mac OSX	181.0.0.0
Cisco AV/AS support chart version for Linux	33.0.0.0
Cisco supported OS version	84.6.2.0

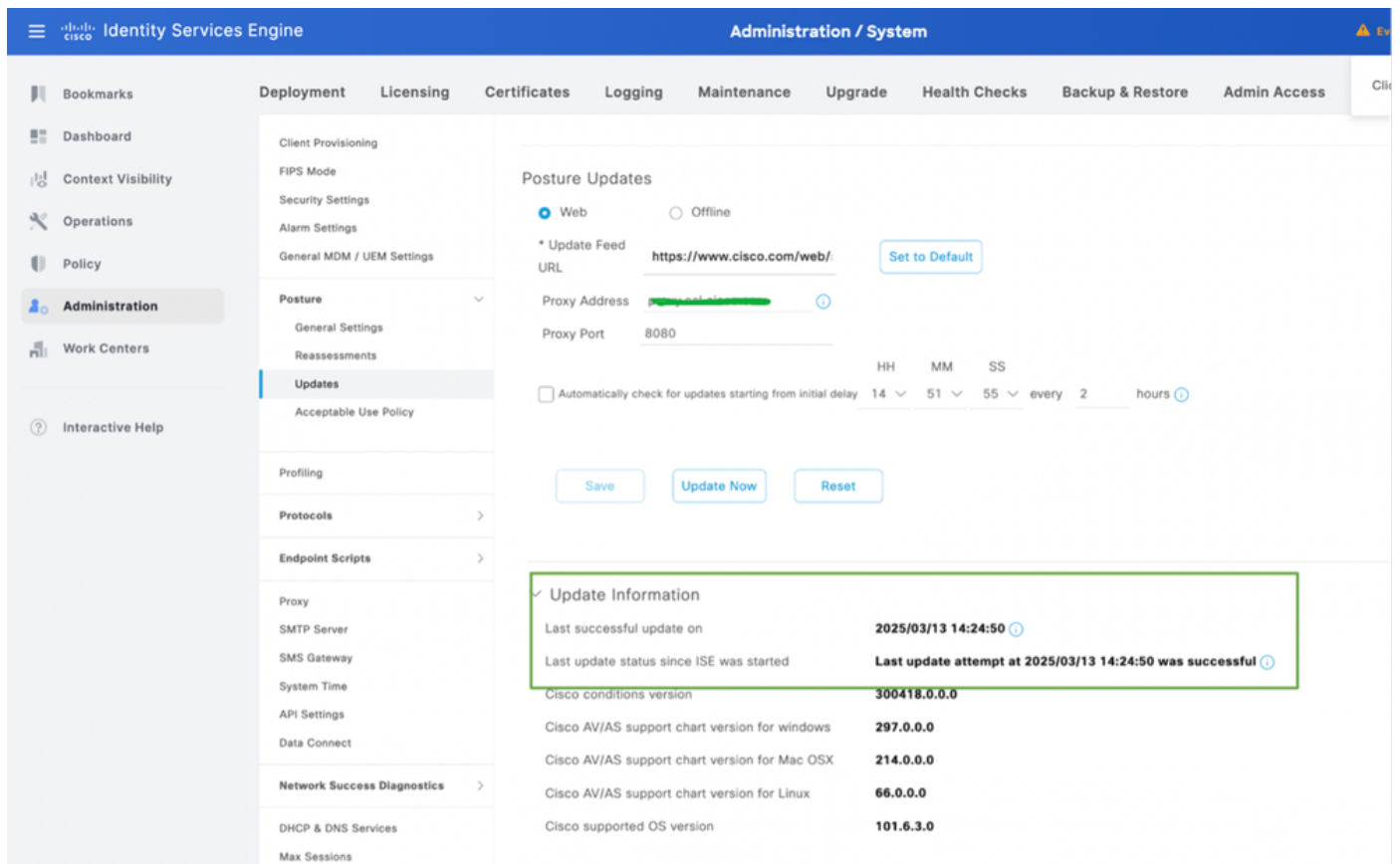
2. 選擇offline選項，瀏覽並選擇已下載到本地系統的posture-offline.zip資料夾。按一下「Update Now」。



3.狀態更新開始後，狀態將更改為Updating。



4.根據此螢幕截圖，可以從更新資訊驗證終端安全評估更新的狀態：



驗證

登入到Primary Admin節點的GUI -> Operations -> Troubleshooting -> Download Logs -> Debug logs -> Application logs -> isc-psc.log，按一下isc-psc.log，日誌將下載到您的本地系統。透過記事本或文字編輯器開啟下載的檔案，並篩選以下載Opswat。您必須能夠找到與在部署中執行的狀態更新相關的資訊。

您還可以使用show logging application ise-psc.log tail命令，通過登入到主管理節點的CLI來跟蹤日誌。

Opswat下載（指安全評估更新）已啟動：

```
2025-03-13 13:58:07,246 INFO [admin-http-pool5][[]]
```

```
cisco.cpm.posture.download.DownloadManager -::admin::: Starting opswat download
```

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

```
cisco.cpm.posture.download.DownloadManager -::admin::: — 離線下載檔案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::: — 離線下載檔案URI
```

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

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

已完成的Opswat下載，表示狀態更新已下載並成功。

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

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

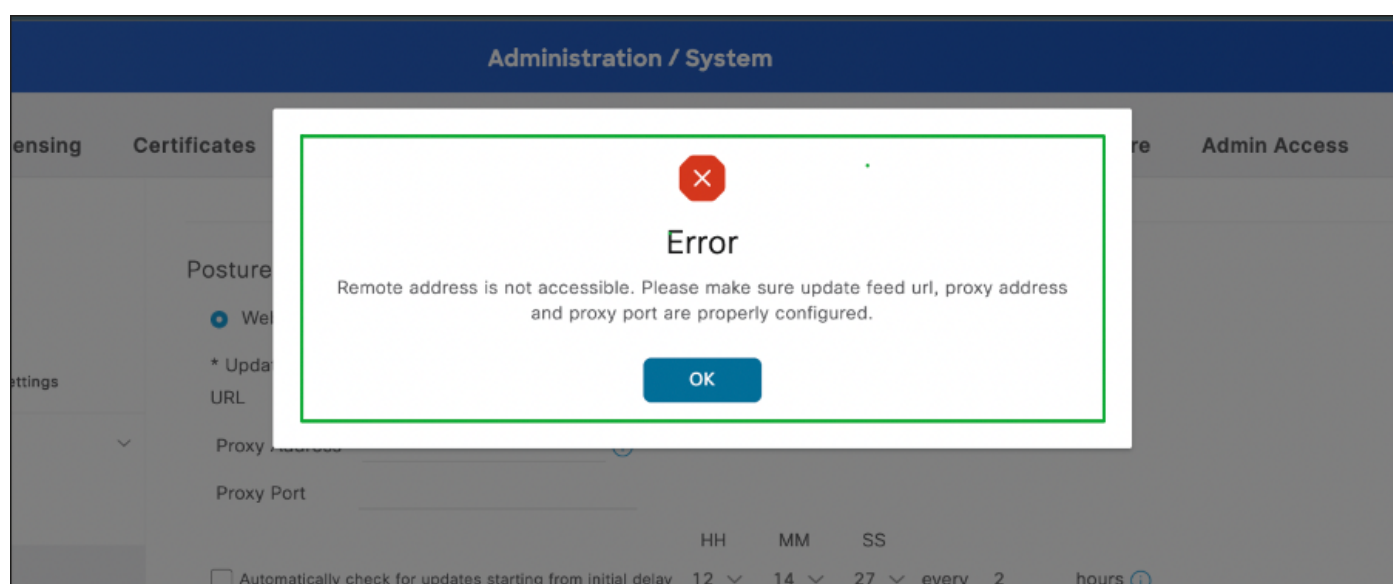
2025-03-13 14:24:50,827 INFO [admin-http-pool5][[]]
mnt.dbms.datadirect.impl.DatadirectServiceImpl -::admin:: — 正在執行getStatus - datadirectSettings

疑難排解

案例

聯機狀態更新失敗，並出現錯誤「Remote Address is not access (遠端地址不可訪問)」。請確保更新源UR、代理地址和代理埠配置正確」。

示例錯誤：



解決方案

1. 登入ISE的CLI，使用ping cisco.com命令驗證ISE是否可以訪問cisco.com。

isehostname/admin#ping cisco.com

PING cisco.com(72.163.4.161)56(84)位元組資料。

從72.163.4.161開始的64個位元組：icmp_seq=1 ttl=235 time=238 ms

從72.163.4.161開始的64個位元組：icmp_seq=2 ttl=235 time=238 ms

從72.163.4.161開始的64個位元組：icmp_seq=3 ttl=235 time=239 ms

從72.163.4.161開始的64個位元組：icmp_seq=4 ttl=235 time=238 ms

— cisco.com ping統計資訊 —

4 packets transmitted, 4 received, 0% packet loss, time 3004ms

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

2.導覽至Administration -> System -> Settings -> Proxy is configured with proper ports。

The screenshot shows the Cisco ISE Administration console with the 'Settings' tab selected. The left sidebar lists various configuration areas, and the main content area displays the 'Proxy' settings. The 'Proxy host server : port' field is highlighted with a green box and contains the value '10.10.10.10 : 8080'. The 'Bypass proxy for these hosts and domains' field is also highlighted with a green box and is empty. The 'Save' button is highlighted with a green box. The 'Reset' button is visible next to it.

3.驗證到網際網路的所有躍點上是否允許埠TCP 443、UDP 53和UDP 123。

狀態更新問題的已知缺陷

[思科錯誤ID 01523](#)

參考

- [思科身份服務引擎管理員指南3.3版](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。