Perform Posture Updates in ISE Offline and Online

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

Online Posture Updates

- What Happens During the Web or Online Posture Updates?
  - When to Use
- Ports Used for Online Posture Update
- Procedure to Perform Online Posture Updates

Proxy Configuration for Online Posture Updates

Offline Posture Updates

- What Happens When You Do an Offline Posture Update?
  - When to Use
- Ports Used for Offline Posture Updates
- Where to Find Files for Offline Posture Updates?
- Offline Posture Update Files Include
- Procedure to Perform Offline Posture Updates

Verification

Troubleshoot

- Scenario
- Solution
- Known Defects for Posture Update Issues

Reference

Introduction

This document describes how to perform Posture Updates in Cisco Identity Services Engine® (ISE).

Prerequisites

Requirements

Cisco recommends that you have knowledge on Posture flow.

Components Used

The information in this document is based on these hardware and software versions:

- Cisco Identity Services Engine 3.2 and later versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Posture updates include a set of predefined checks, rules, and support charts for antivirus and anti-spyware for both Windows and MacOS operating systems, and operating systems information supported by Cisco.

When you deploy Cisco ISE on your network for the first time, you can download posture updates from the web. This process takes approximately 20 minutes. After the initial download, you can configure Cisco ISE to verify and download incremental updates to occur automatically.

Cisco ISE creates default posture policies, requirements, and remediation only once during an initial posture updates. If you delete them, Cisco ISE does not create them again during subsequent manual or scheduled updates.

You can perform two types of posture updates:

- Online Posture Updates
- Offline Posture Updates

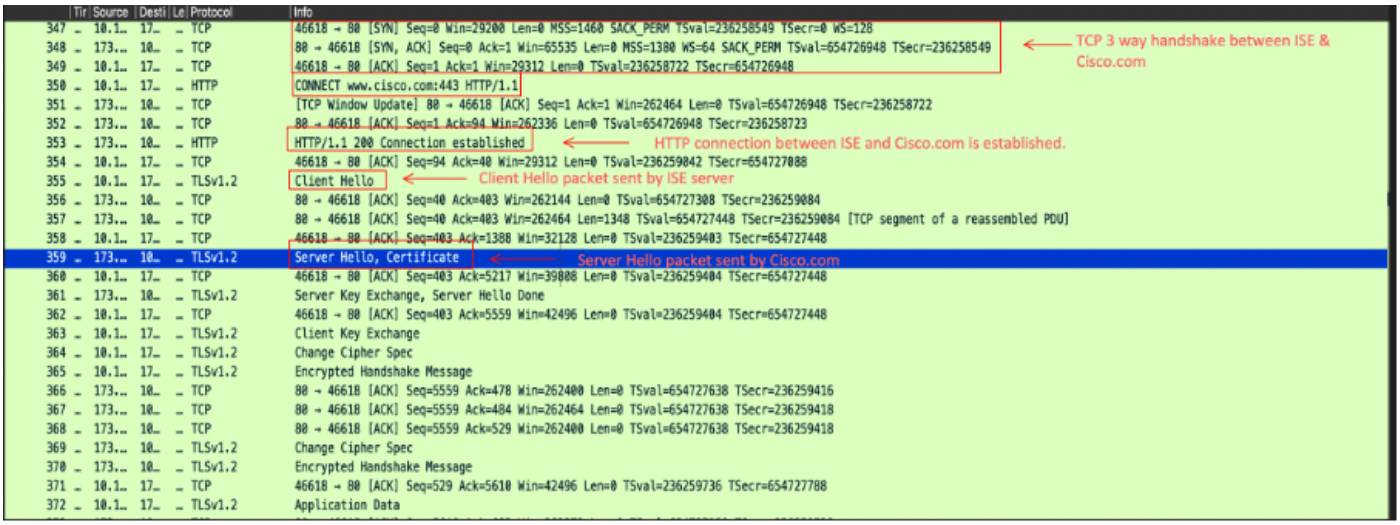
Online Posture Updates

A **Web Posture Update**/**Online Posture Update** retrieves the latest posture updates from Cisco cloud or server repositories. This involves downloading the latest policies, definitions, and signatures directly from Cisco servers. ISE must connect to Cisco cloud servers or update repositories to retrieve the latest posture definitions, policies, and other associated files.

What Happens During the Web or Online Posture Updates?

The Identity Services Engine (ISE) accesses the Cisco website either through a proxy or a direct internet connection using HTTP, establishing a connection with www.cisco.com. During this process, the client hello and server hello exchange occurs, with the server providing its certificate to verify its legitimacy and confirm client-side trust. After the client hello and server hello are completed, the client key exchange takes

place, and the server initiates the posture updates. This is the packet capture demonstrating the communication between the ISE server and Cisco.com during the Online Posture updates.

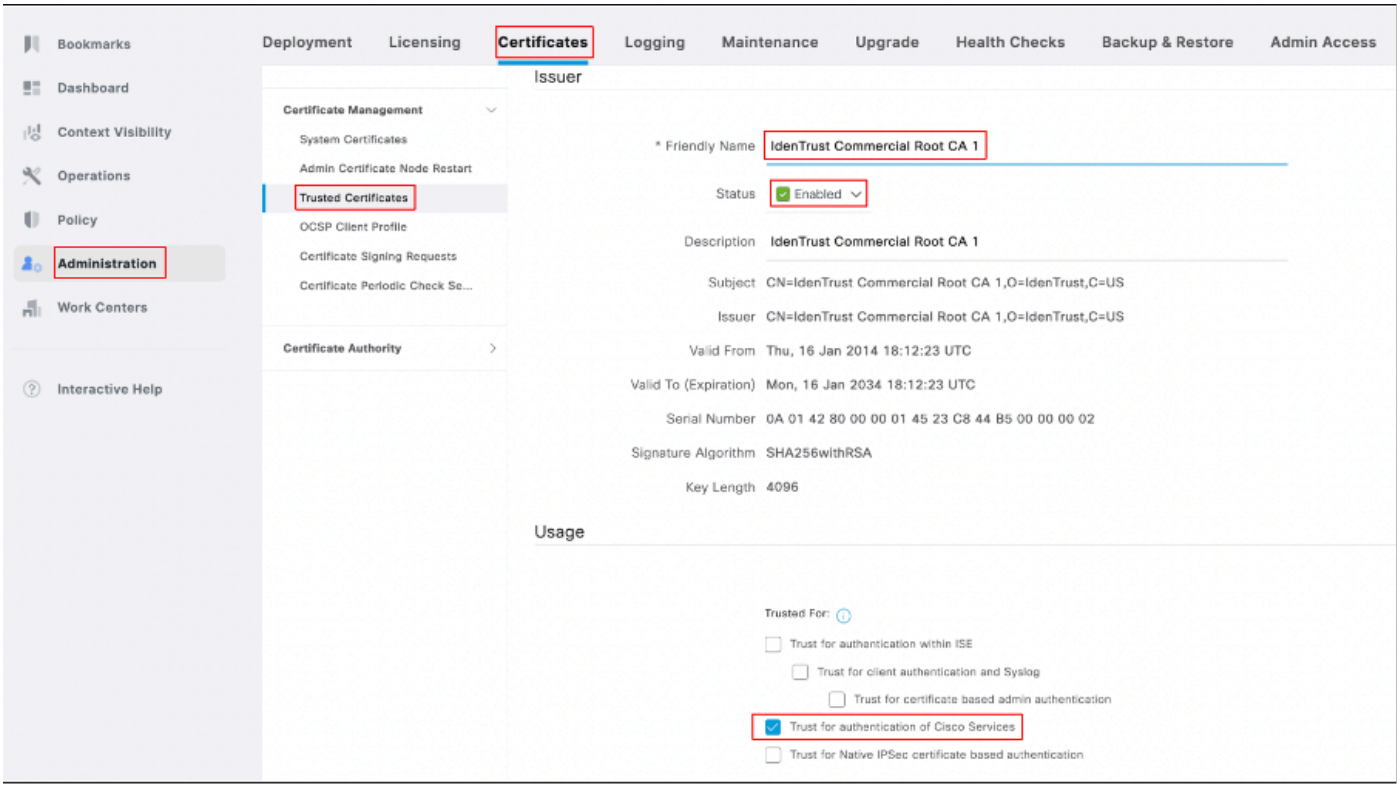


- During the Server Hello, Cisco.com sends these certificates to the client to confirm client-side trust:

```
Certificates Length: 5083
Certificates (5083 bytes)
Certificate Length: 1940
Certificate: 3082079030820678a003020102021040016efb0a205cfaebe18f71d73abb78300d06092a… (id-at-commonNam
Certificate Length: 1754
Certificate: 308206d6308204bea003020102021040016efb0a205cfaebe18f71d73abb78300d06092a… (id-at-commonNam
Certificate Length: 1380
Certificate: 3082056030820348a00302010202100a0142800000014523c844b500000002300d06092a… (id-at-commonNam
```

In ISE GUI, it is important to ensure the server certificate IdenTrust Commercial Root CA 1 is enabled and **Trust for authenticating Cisco services** to establish connectivity with Cisco.com. By default, this certificate is included in ISE and "**Trust for authenticating Cisco services**" is checked, but verification is advised.

Check the certificate status and trusted usage by going to the **ISE GUI** > **Administration** > **Certificates** > **Trusted Certificates**. Filter by the name **IdenTrust Commercial Root CA 1**, select the certificate, and then edit it to verify the trust usage, as shown in the next screenshot:



Posture updates can include new or revised posture policies, new antivirus/anti-malware definitions, and other security-related criteria for posture assessments.

This method requires an active internet connection and is typically performed when the ISE system is configured to use cloud-based repositories for posture updates.

When to Use

Online posture updates are used to ensure the posture policies, security definitions, and criteria are up to date with the latest available versions provided by Cisco.

Ports Used for Online Posture Update

To ensure the ISE system can successfully reach Cisco cloud servers to download posture updates, these ports must be open in your firewall and allowed for outbound communication from ISE to the internet:

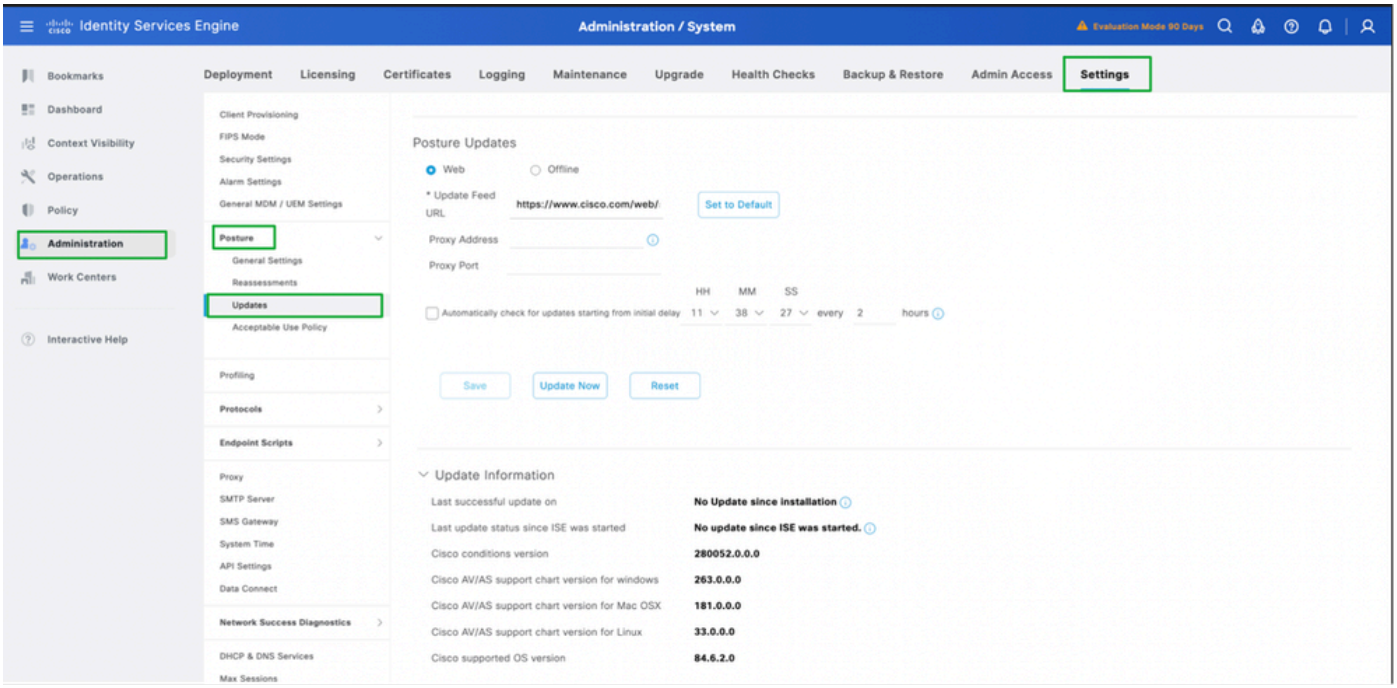
1. **HTTPS (TCP 443)**:
   - Primary port for ISE to reach the Cisco cloud servers and download updates over a secure connection (TLS/SSL).
   - This is the most crucial port for the web-based posture update process.
2. **DNS (UDP 53)**:
   - ISE must perform DNS lookups to resolve the hostnames of the update servers.
   - Ensure your ISE system can reach the DNS servers and resolve domain names.
3. **NTP (UDP 123)**:
   - ISE uses NTP for time synchronization. This is important to ensure that the update process is

correctly timestamped and that the ISE system operates in a synchronized time zone.

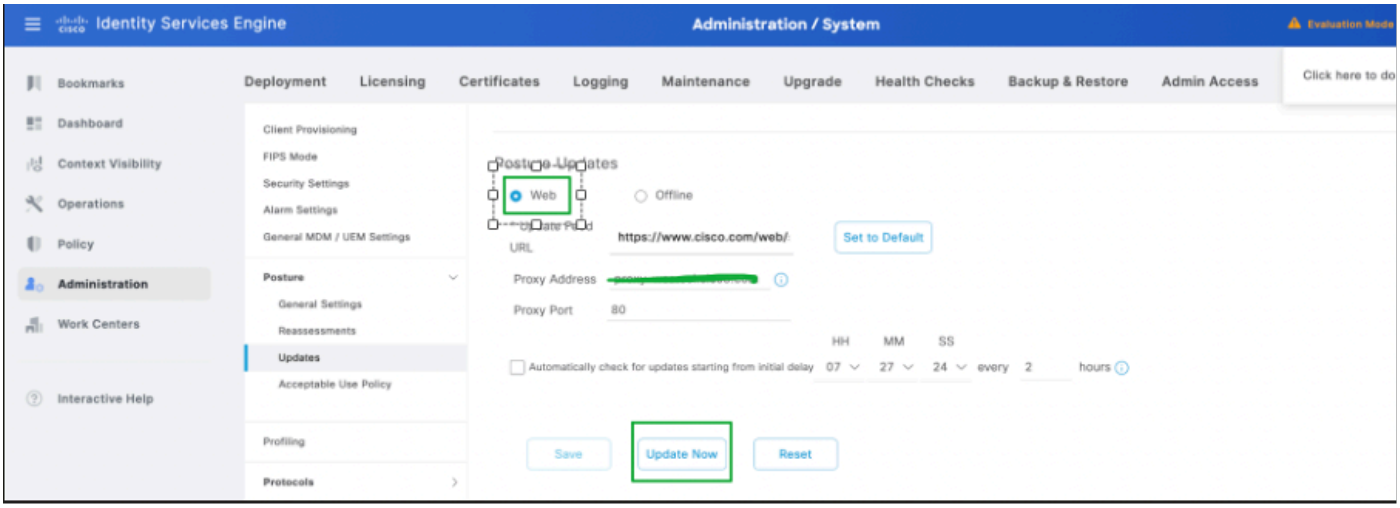
- In many cases, NTP servers also need to be accessible over UDP 123.

Procedure to Perform Online Posture Updates

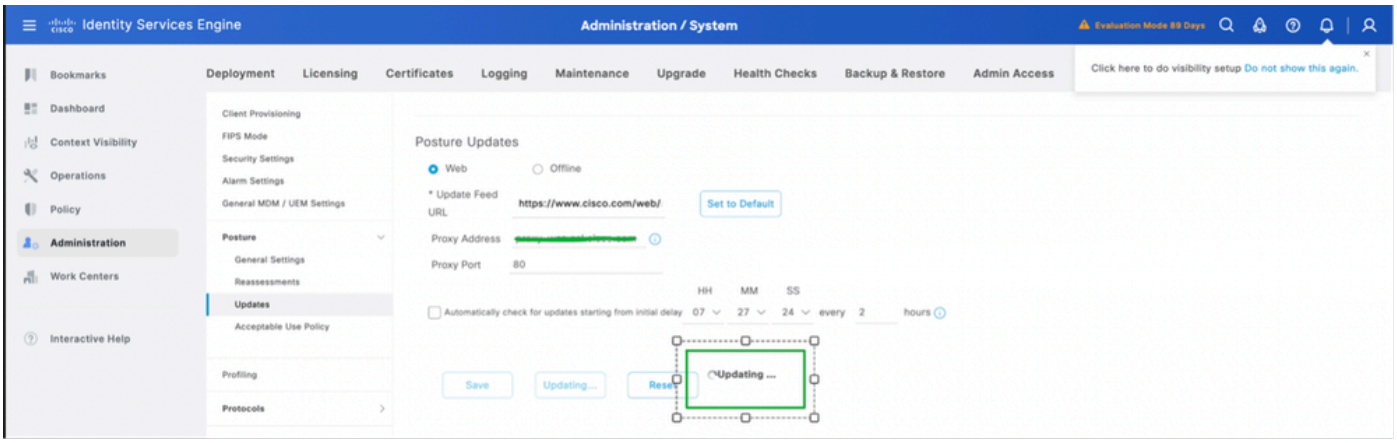
1. Log in to the **GUI** > **Administration** > **System** > **Settings** > **Posture** > **Updates**.



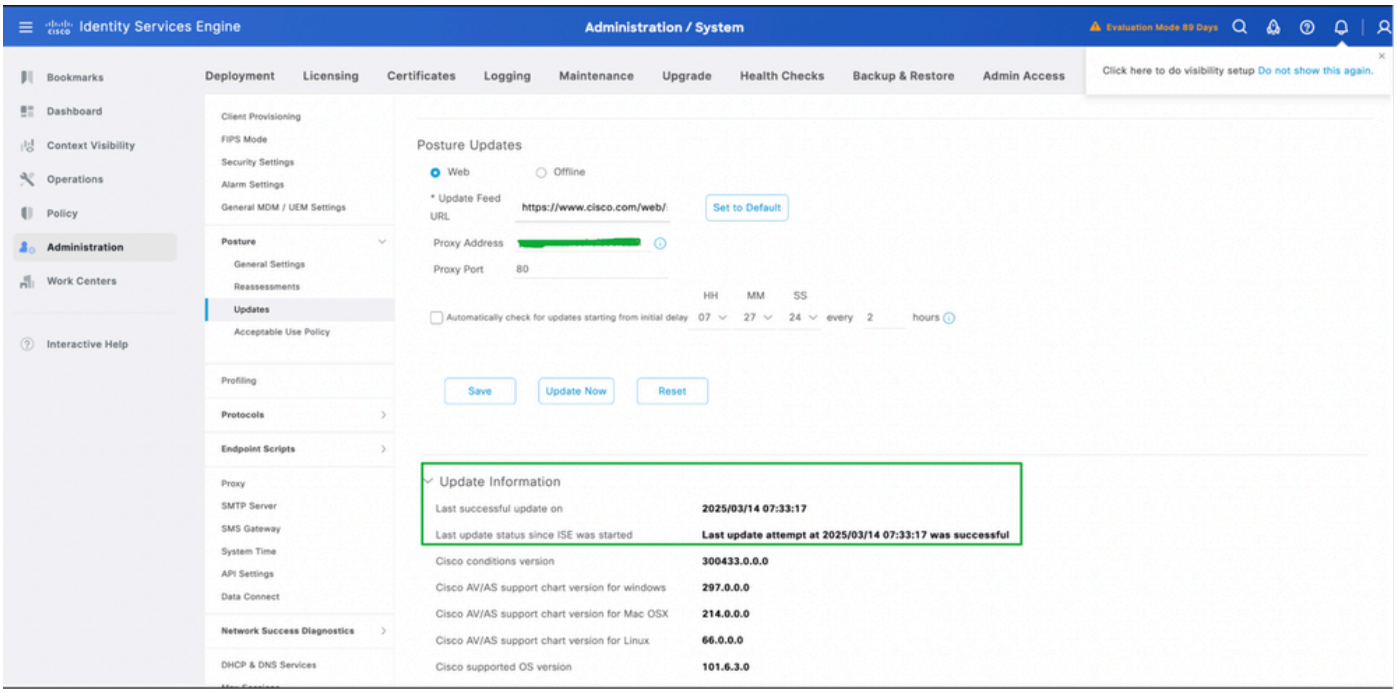
2. Select the method as **Web** for Online Posture Updates, click **Update Now**.



3. Once the posture updates begin, the status is changed to **Updating**.



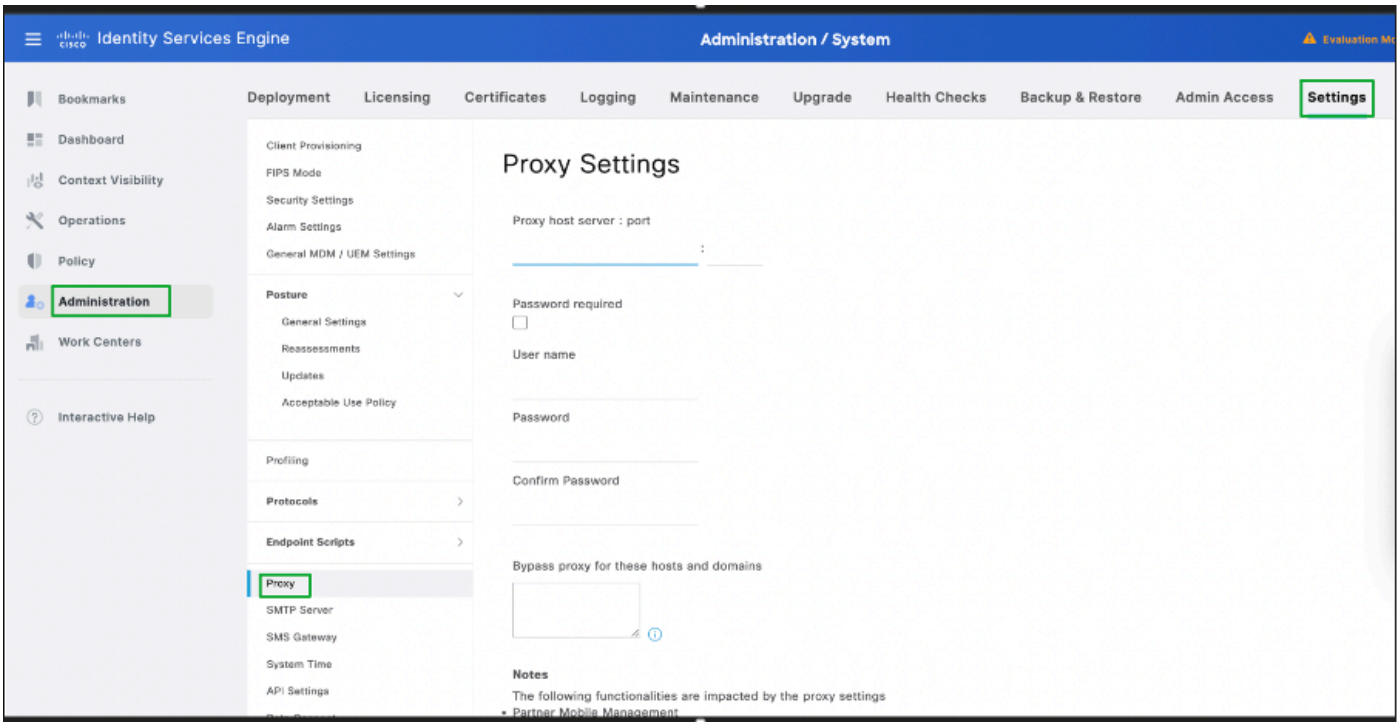
4. The status of Posture updates can be verified from the **Update Information**.



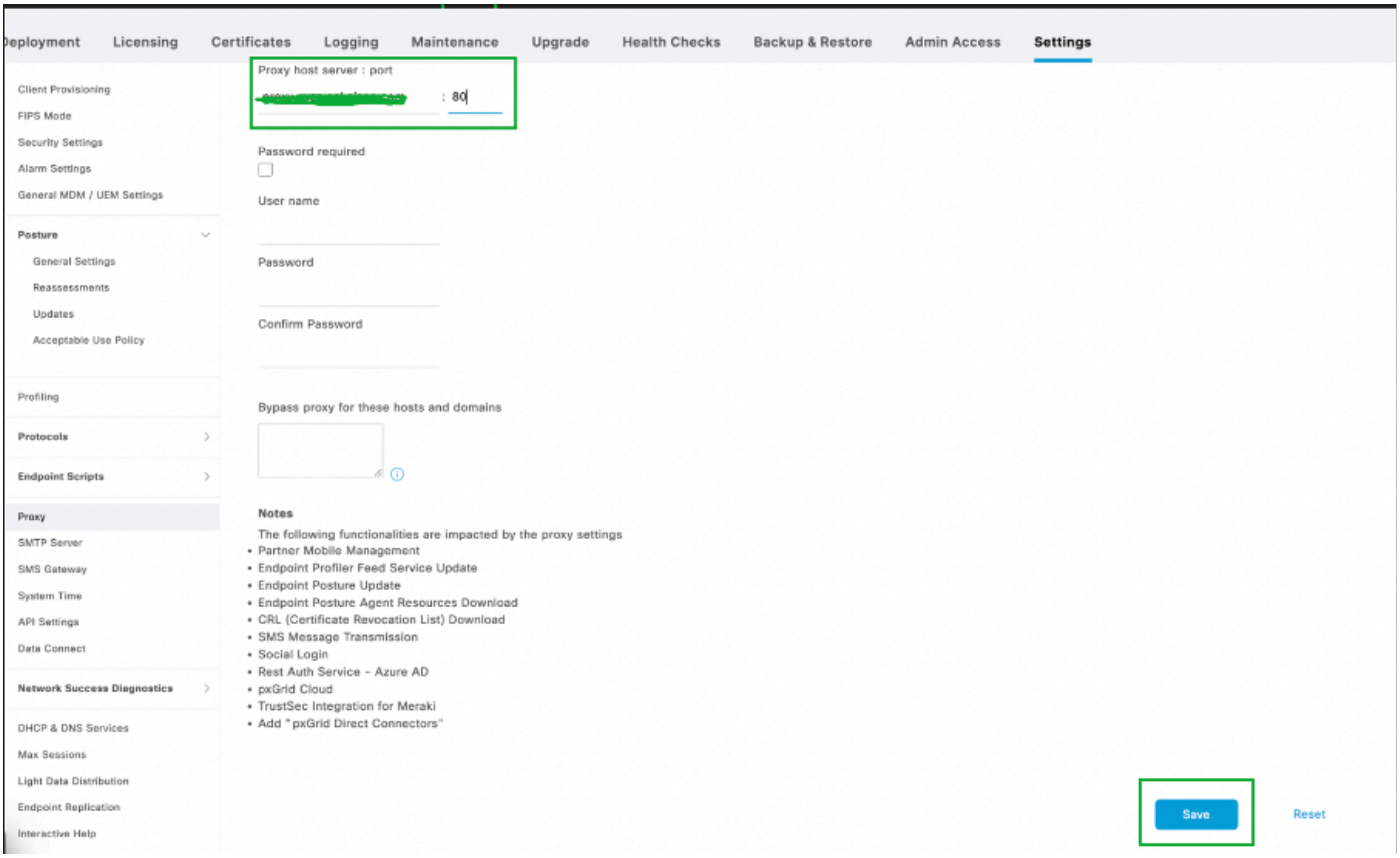
Proxy Configuration for Online Posture Updates

In a restricted environment where the Posture Update field URL is not accessible, proxy configuration is required. Refer to Configure Proxy in ISE.

1. Navigate to **Administration** > **System** > **Settings** > **Proxy**.



2. Configure the Proxy details, click **Save**.



3. The details of the proxy is automatically fetched by ISE when Online Posture Updates are performed.

Offline Posture Updates

An **Offline Posture Update** allows you to manually upload posture update files (in the form of a .zip or another supported file format) to ISE.

What Happens When You Do an Offline Posture Update?

- You upload the updated posture files manually.
- ISE processes and applies these files, which can include updated policies, antivirus definitions, posture assessments, among other types of files.
- The offline update does not require internet connectivity and is typically used in environments with strict security or network policies that prevent direct access to external servers.

When to Use

This method is often used in environments where the system is isolated from the internet or when you have specific offline update files provided by Cisco or your security team.

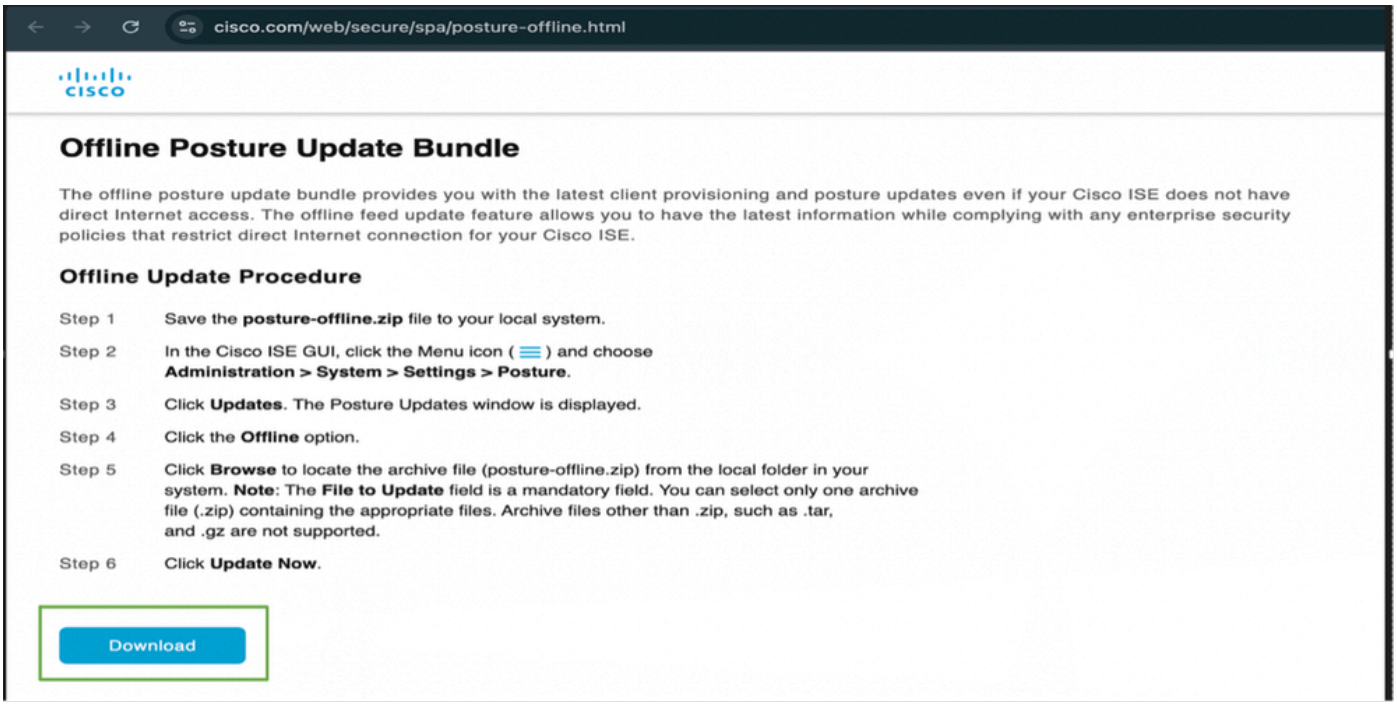
Ports Used for Offline Posture Updates

For general communication with the ISE server (during the update process), in many cases, these ports are relevant:

1. **Management Access** (Ports 22, 443):
    - SSH (TCP 22): If you are using SSH to access the ISE system for troubleshooting or manual upload.
    - HTTPS (TCP 443): If you are using the GUI (web interface) for the update upload.
2. **File Transfer (SFTP or SCP)**:
    - If you need to upload files manually to ISE via SFTP or SCP, ensure the corresponding ports (typically Port 22 for SSH/SFTP) are open on the ISE system.
3. **Local Network Access**:
    - Ensure the system you are uploading the update (for example, an admin workstation or server) can communicate with ISE over the necessary ports for management access, but again, offline posture updates do not require any external ports since the files are manually provided.

Where to Find Files for Offline Posture Updates?

1. Navigate to URL: Offline Posture Update Bundle, click **Download** and the **posture-offline.zip** file is downloaded to your local system.

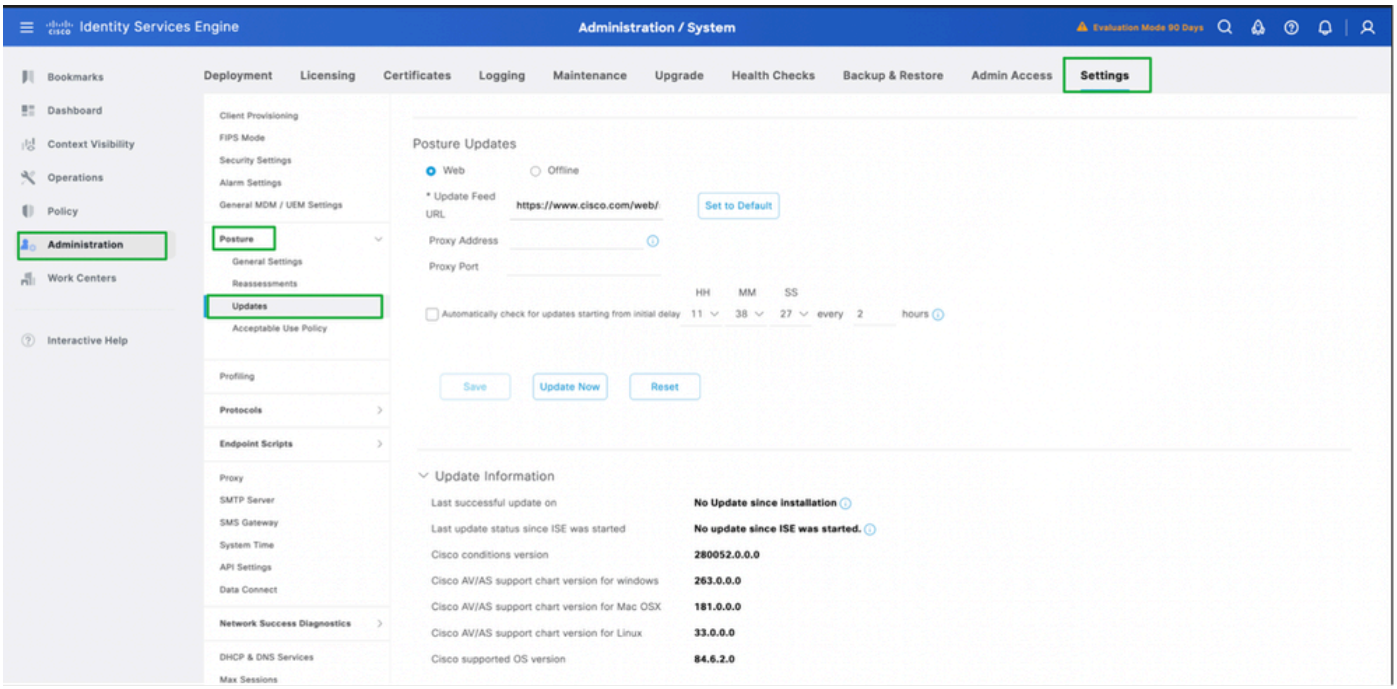


Offline Posture Update Files Include

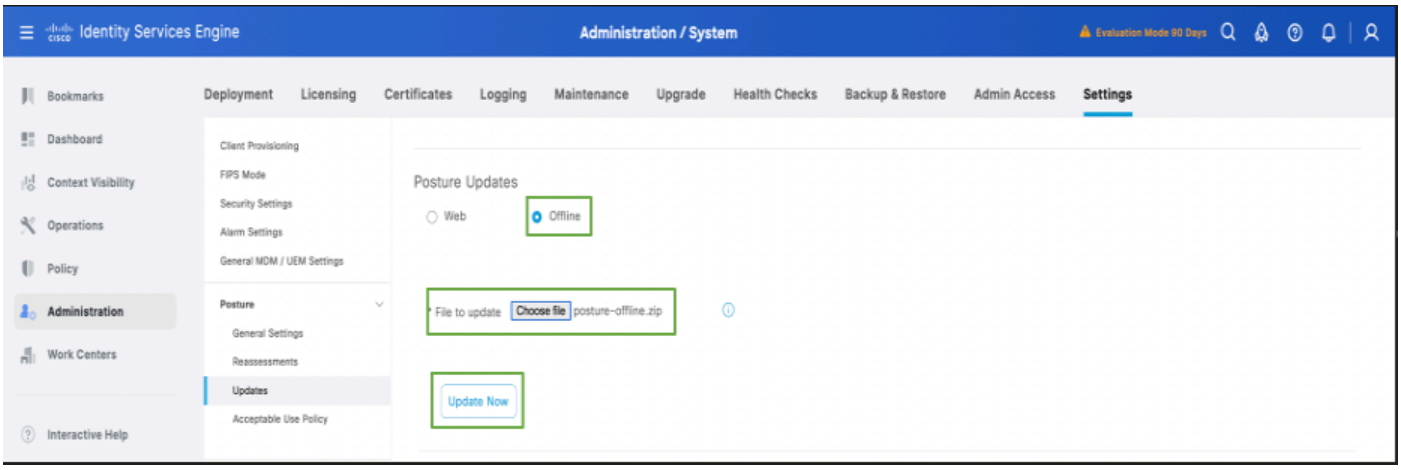
- Posture policies and rules
- Antivirus definitions (signatures)
- Security assessments and other configuration files for posture evaluation

Procedure to Perform Offline Posture Updates

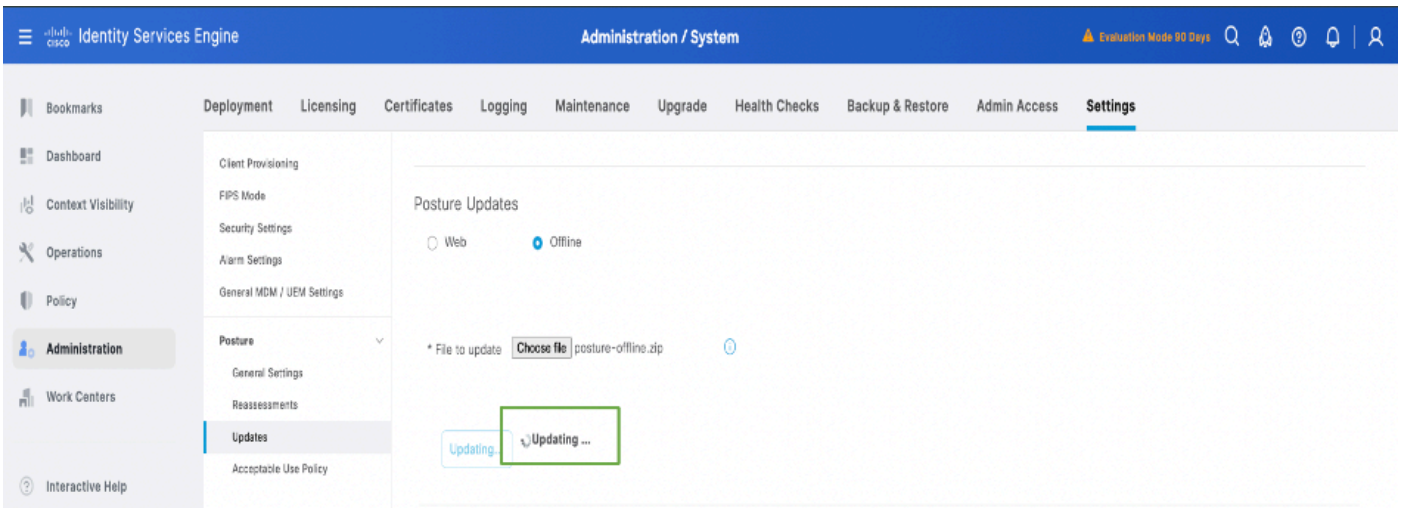
1. Log in to the **ISE GUI** > **Administration** > **System** > **Settings** > **Posture** > **Updates**.

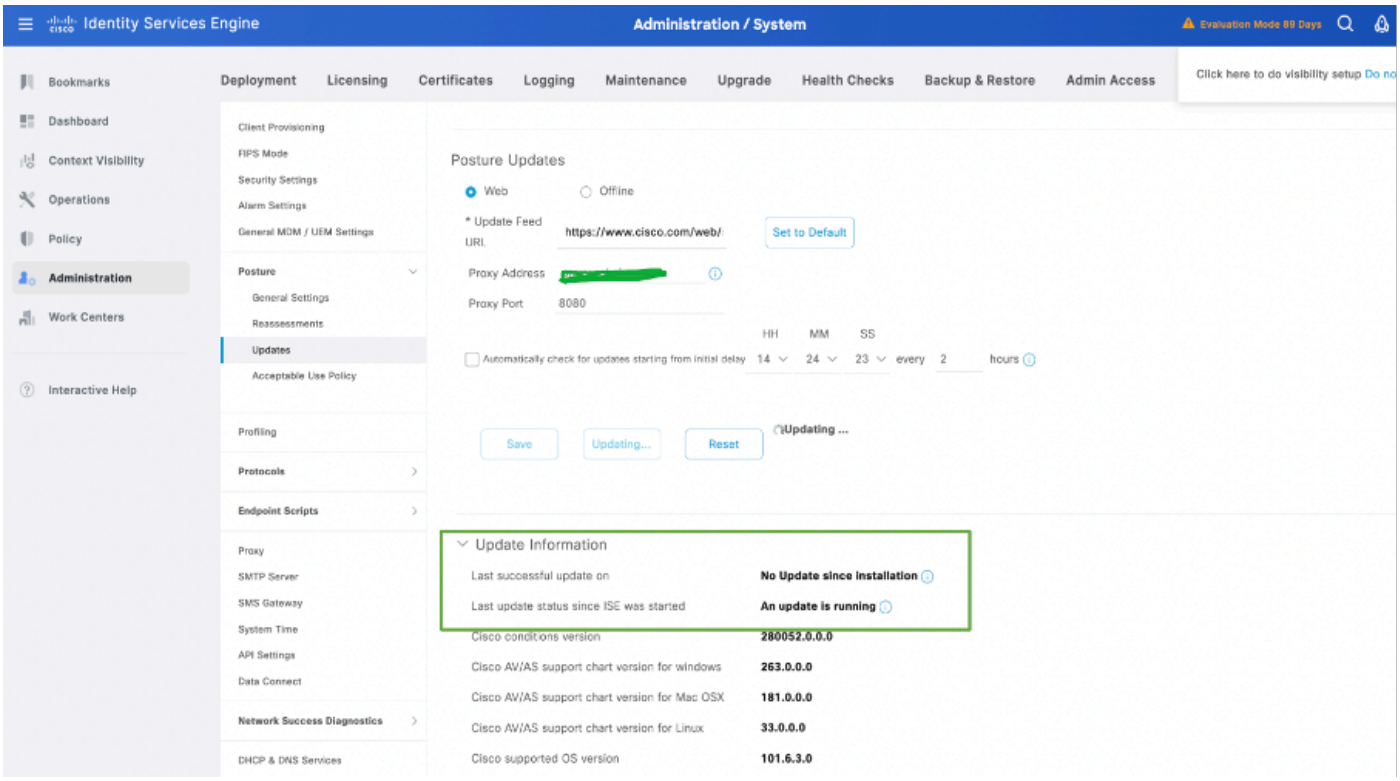


2. Select the **offline** option, browse and select the **posture-offline.zip** folder that was downloaded to your local system. Click **Update Now**.

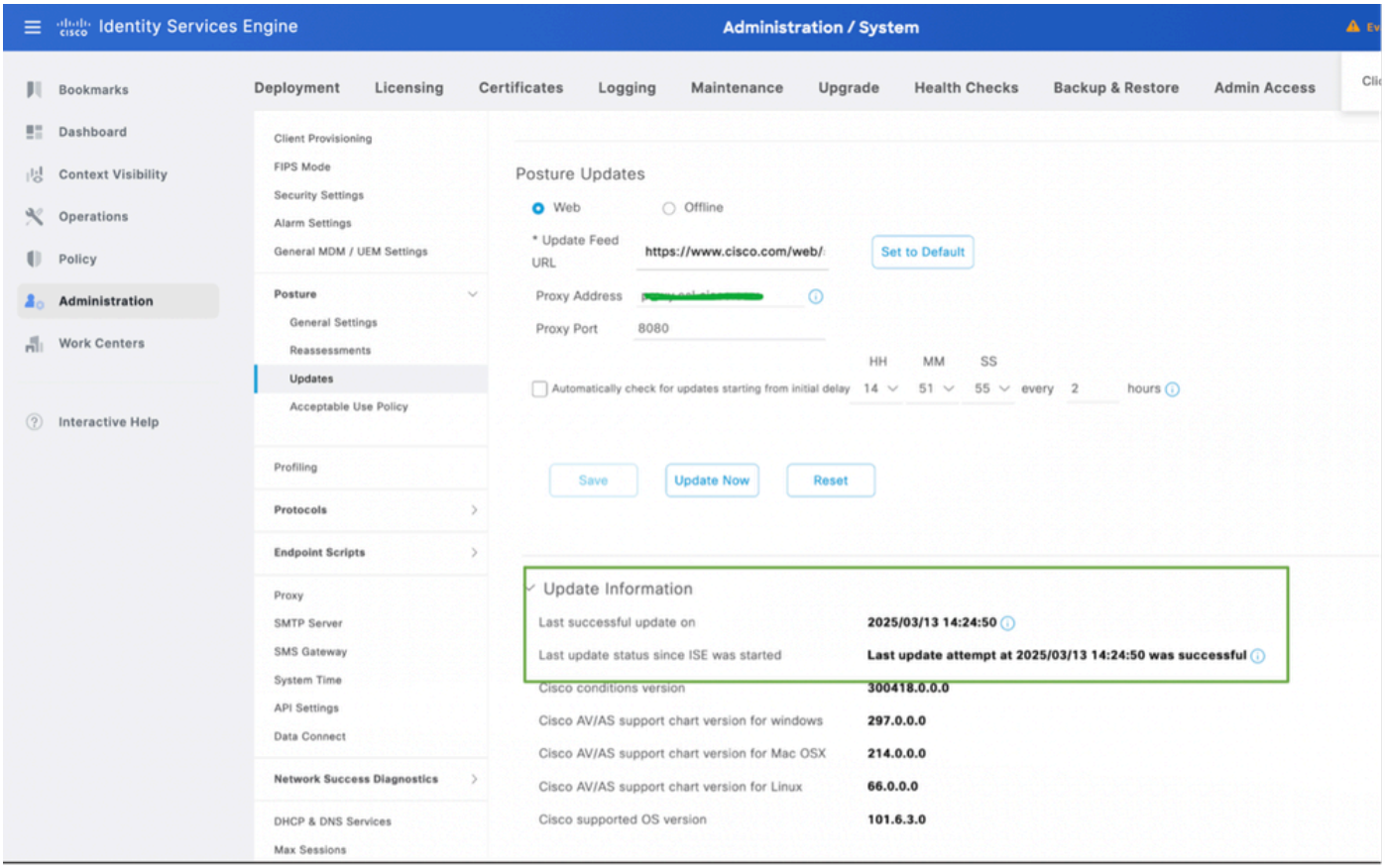


3. Once the posture updates begin, the status is changed to **Updating**.





4. The status of the Posture updates can be verified from the **Update Information**:



Verification

1. Log in to the GUI of the **Primary Admin Node** > **Operations** > **Troubleshooting** > **Download Logs** > **Debug Logs** > **Application Logs** > **isc-psc.log**, click **ise-psc.log** and the log is downloaded to your local system. Open the downloaded file through Notepad or text editor, and filter for **Opswat download**. You must find the information related to the Posture updates being performed in the deployment.

You can also tail the logs by logging to the CLI of Primary Admin Node by running the **show logging application ise-psc.log tail** command.

The Opswat download, referring to posture updates begin:

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:::- Offline download file 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 file 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][[]]

Completed Opswat Download, referring to posture updates are downloaded and successful.

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:::- **Completed opswat download**

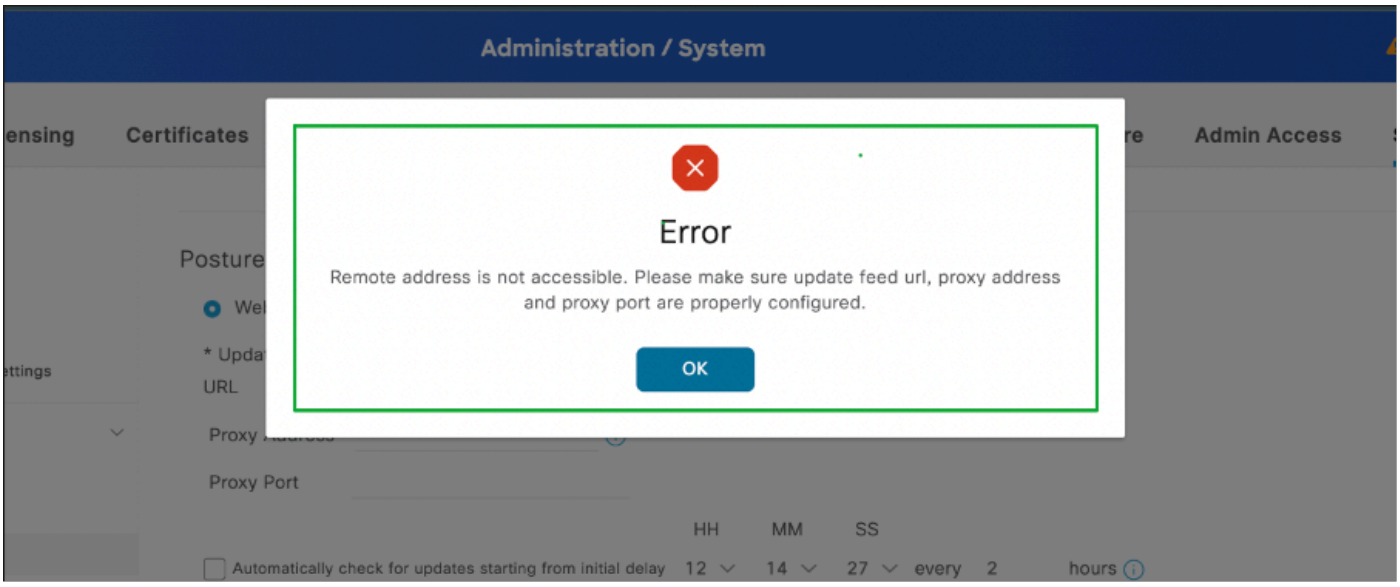
2025-03-13 14:24:50,827 INFO [admin-http-pool5][[]] mnt.dbms.datadirect.impl.DatadirectServiceImpl -::admin:::- Executing getStatus - datadirectSettings

Troubleshoot

Scenario

Online Posture Updates failed with the error "Remote Address is not accessible. Please make sure update feed UR, proxy address and proxy port are properly configured".

Sample error:



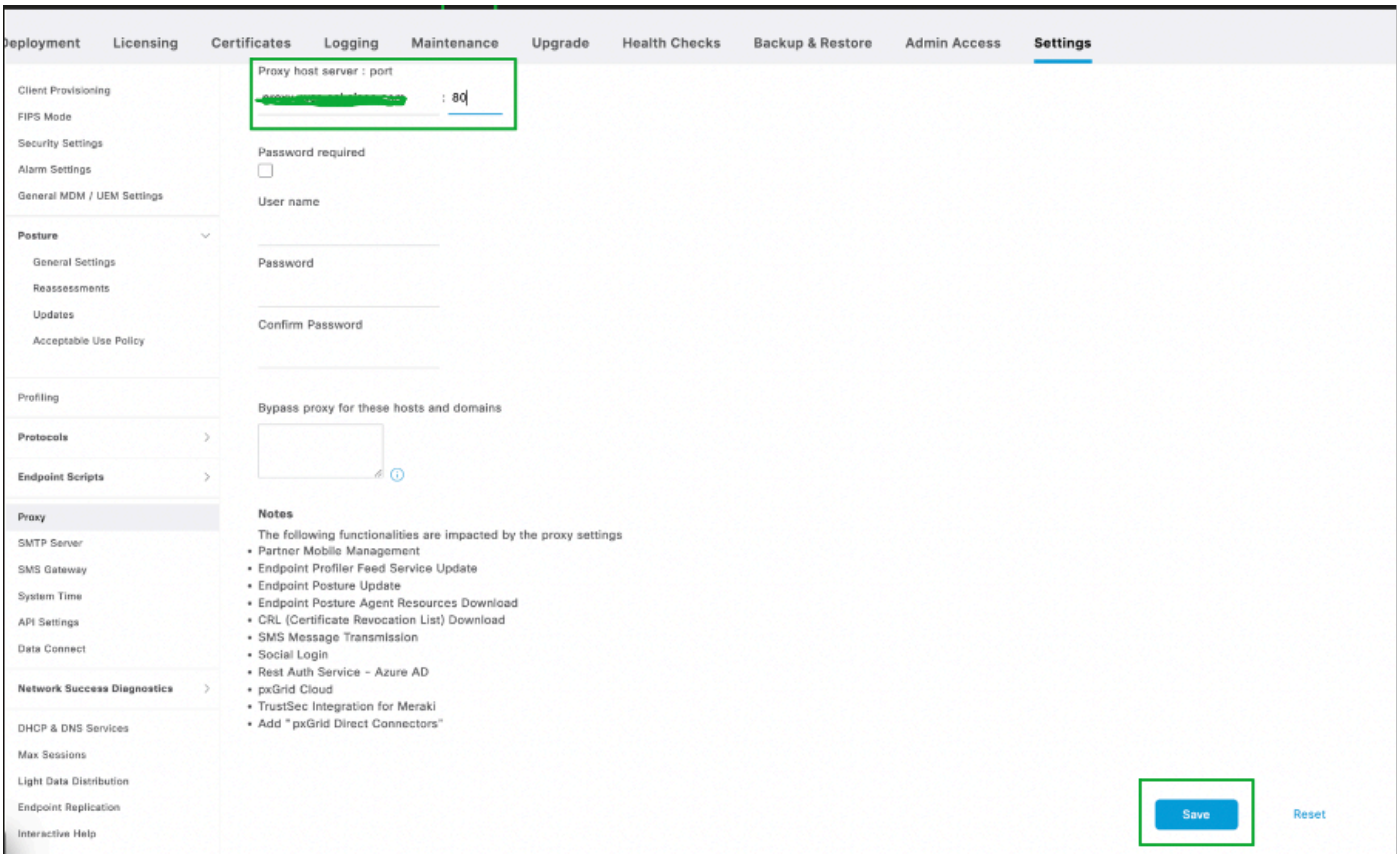
Solution

1. Log in to the CLI of ISE, verify ISE is reachable to cisco.com by running the command "**ping cisco.com**".

isehostname/admin#**ping cisco.com**
PING cisco.com (72.163.4.161) 56(84) bytes of data.
64 bytes from 72.163.4.161: icmp_seq=1 ttl=235 time=238 ms
64 bytes from 72.163.4.161: icmp_seq=2 ttl=235 time=238 ms
64 bytes from 72.163.4.161: icmp_seq=3 ttl=235 time=239 ms
64 bytes from 72.163.4.161: icmp_seq=4 ttl=235 time=238 ms

--- cisco.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 238.180/238.424/238.766/0.410 ms

2. Navigate to **Administration > System > Settings >** Proxy is configured with proper ports.



3. Verify if the **TCP 443, UDP 53 and UDP 123** ports are allowed on all hops to the internet.

Known Defects for Posture Update Issues

- Cisco bug ID 01523

Reference

- Cisco Identity Services Engine Administrator Guide, Release 3.3