

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 higher 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 antispyware for both Windows and MacOS operating systems, and operating systems information that are 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 usually 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.

There are two types of posture updates you can perform:

- **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 needs to 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. Here is the packet capture demonstrating the communication between the ISE server and Cisco.com during the Online Posture updates.

Tir	Source	Desti	Le	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=39888 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

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

</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

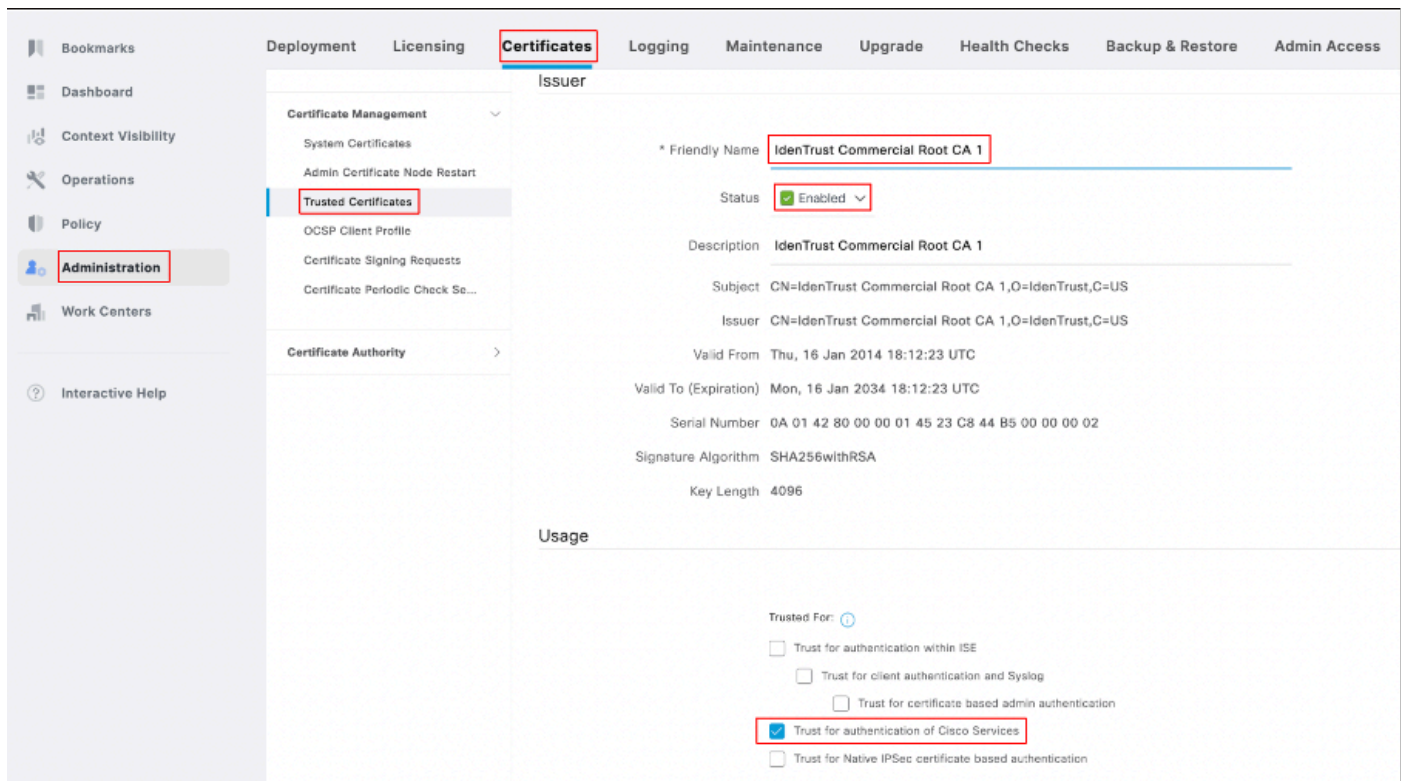
Certificate: 3082056030820348a00302010202100a0142800000014523c844b500000002300d06092a... (id-at-commonName

IdenTrust Commercial Root CA

1

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

- In ISE GUI, it is important to ensure that 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 this screenshot:



- Posture updates can include new or revised posture policies, new antivirus/antimalware 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 when you want to ensure that the posture policies, security definitions, and criteria are up to date with the latest available versions provided by Cisco.

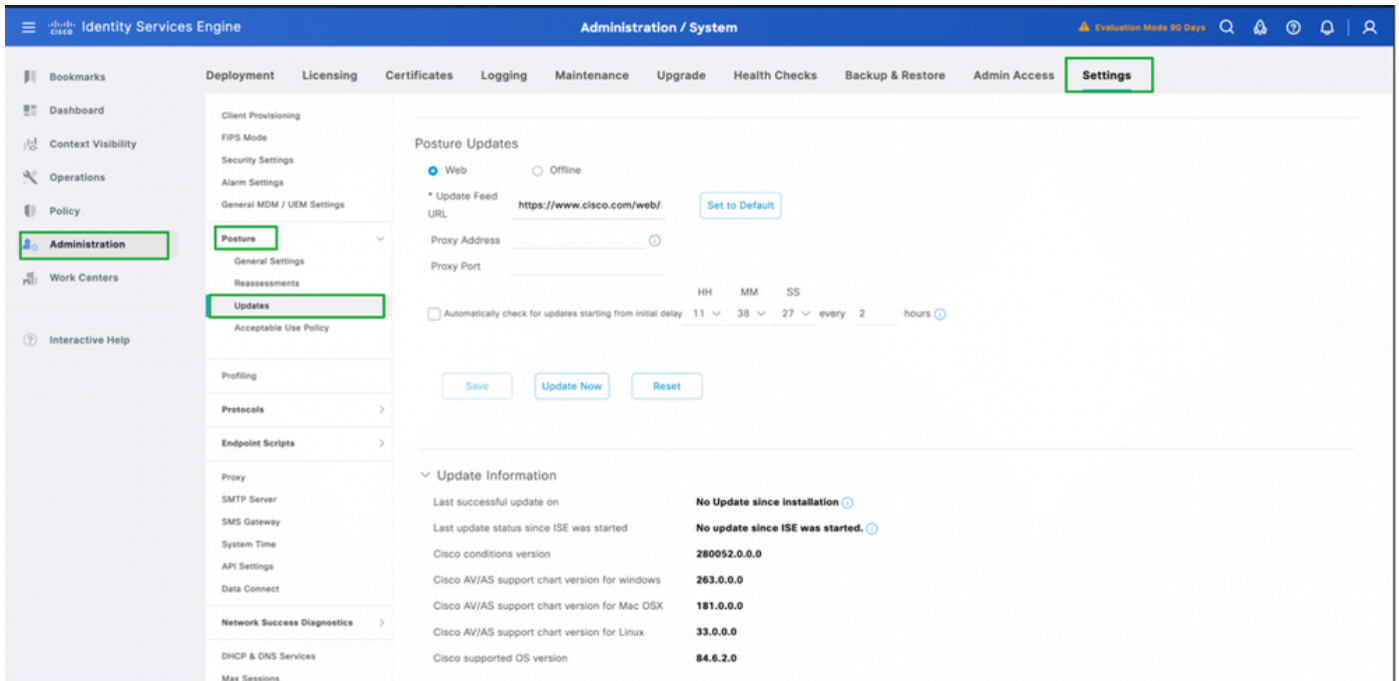
Ports Used for Online Posture Update

To ensure that 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:

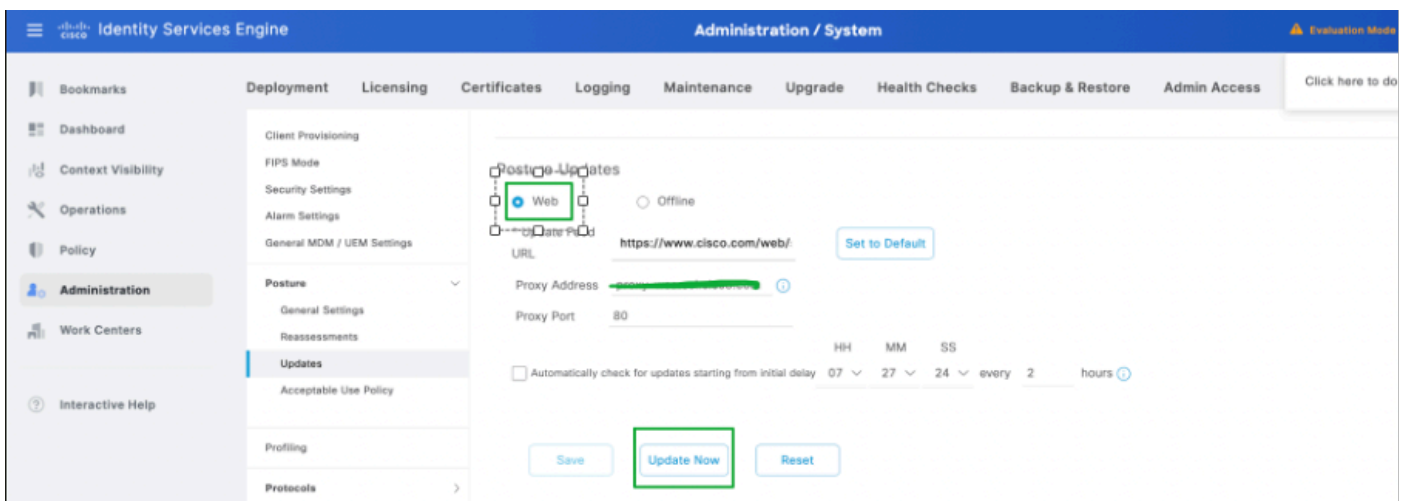
- 1. HTTPS (TCP 443):**
 - Primary port for ISE to reach the Cisco cloud servers and download updates over a secure connection (TLS/SSL).
 - This is the most crucial port for the web-based posture update process.
- 2. DNS (UDP 53):**
 - ISE must be able to perform DNS lookups to resolve the hostnames of the update servers.
 - Ensure that 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

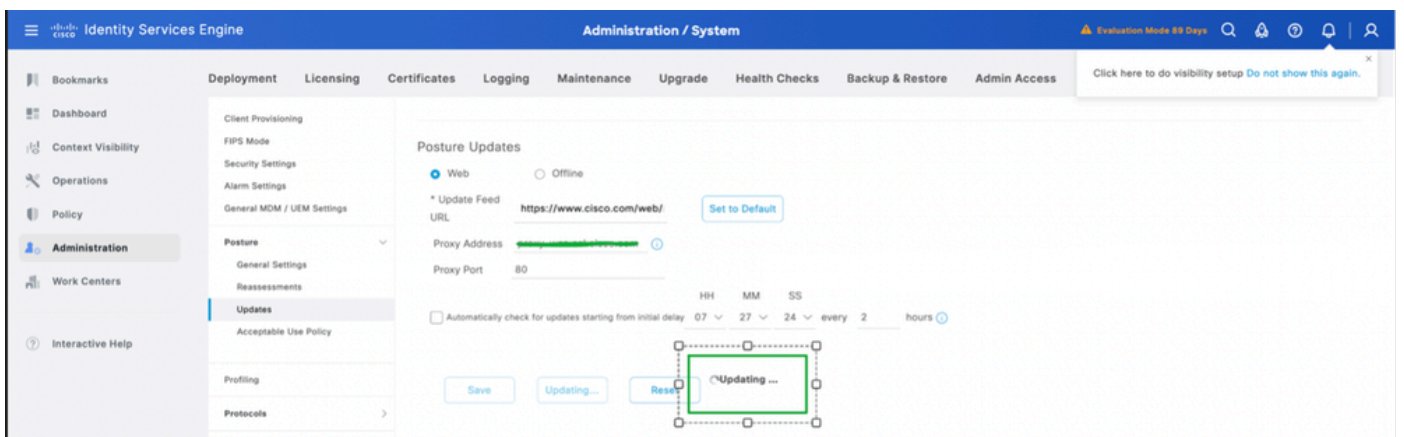
1. Log in to the **GUI -> Administration -> System -> Settings -> Posture -> Updates.**



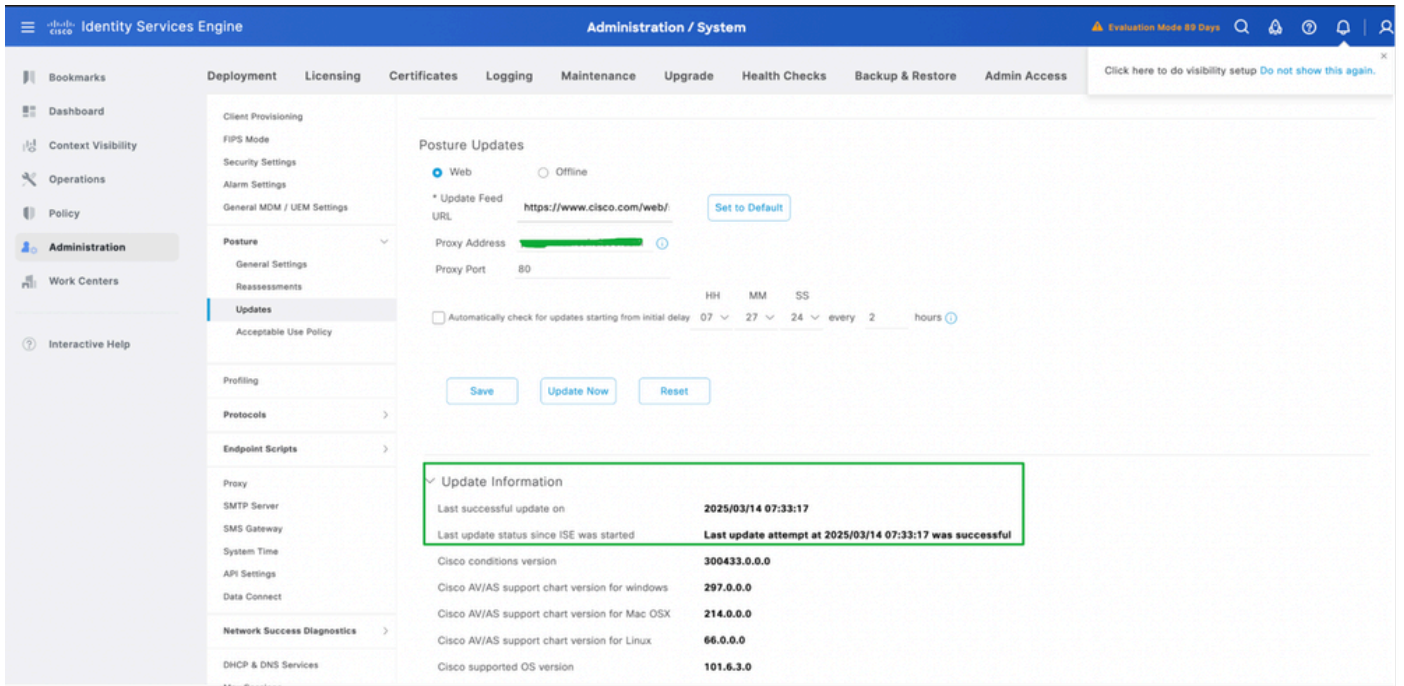
2. Select the method as **Web** for Online Posture Updates, click **Update Now**.



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



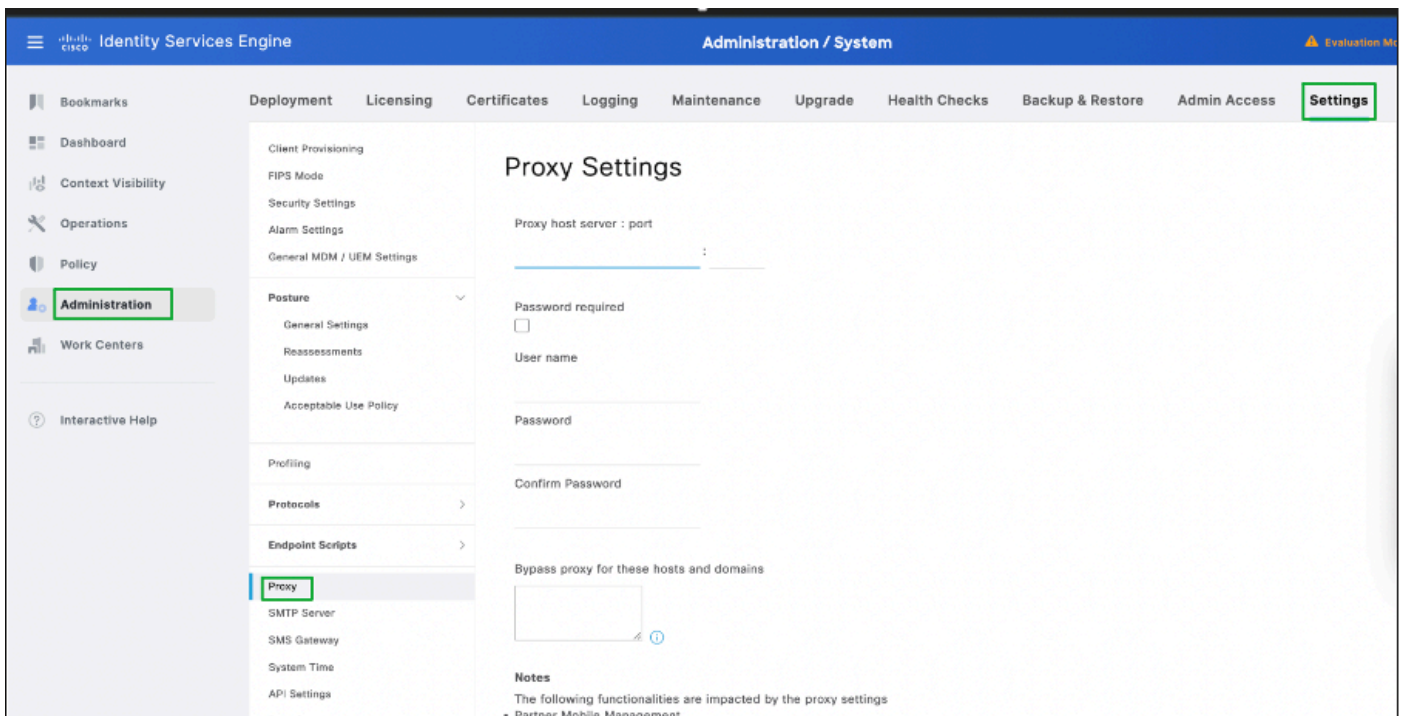
4. Status of the Posture updates can be verified from the **Update Information** as per this screenshot:



Proxy Configuration for Online Posture Updates

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

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



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

The screenshot shows the Cisco ISE Settings page. The 'Proxy' section is active, showing the 'Proxy host server : port' field set to '10.10.10.10:80'. Other fields include 'Password required' (unchecked), 'User name', 'Password', and 'Confirm Password'. A 'Bypass proxy for these hosts and domains' text box is also present. A 'Notes' section lists functionalities impacted by proxy settings. At the bottom right, there are 'Save' and 'Reset' buttons, with the 'Save' button highlighted by a green box.

3. The details of the proxy would be 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):

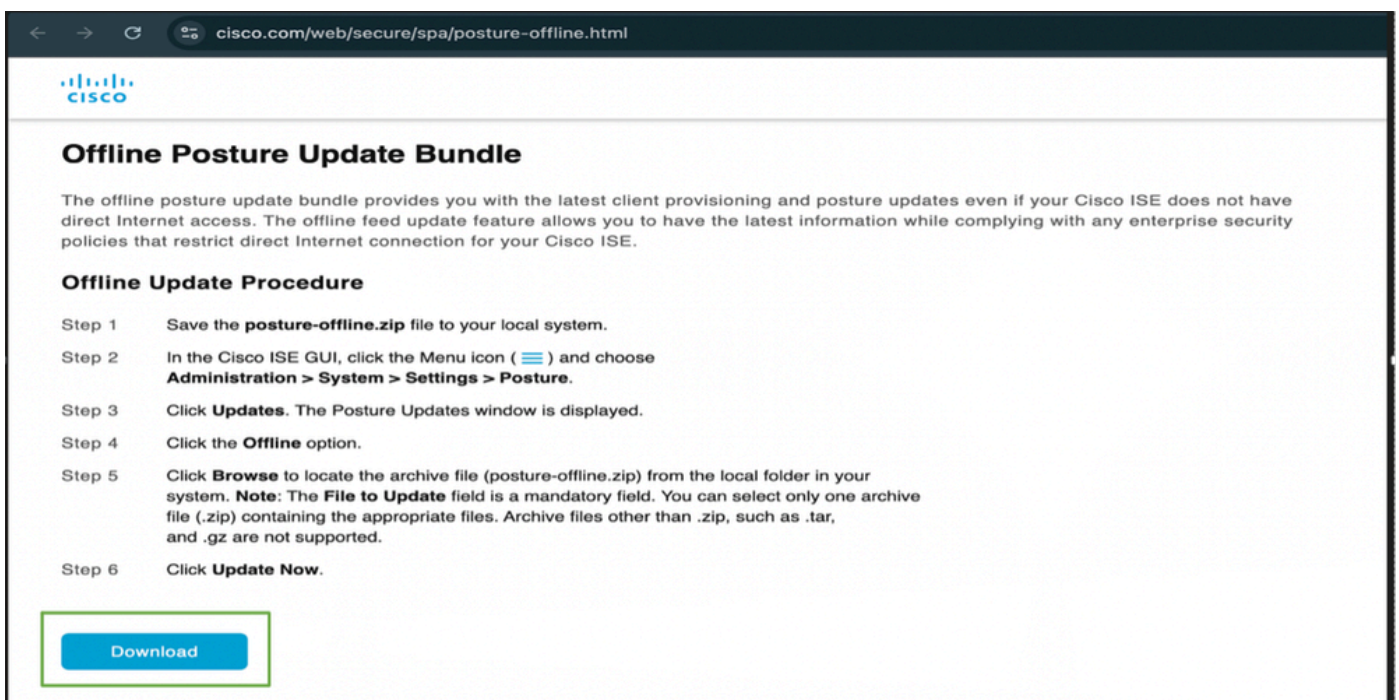
- If you need to upload files manually to ISE via SFTP or SCP, ensure the corresponding ports (typically Port 22 for SSH/SFTP) are open on the ISE system.

3. Local Network Access:

- Ensure that the system from which 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: <https://www.cisco.com/web/secure/spa/posture-offline.html> , click **Download** and the **posture-offline.zip** file is downloaded to your local system.

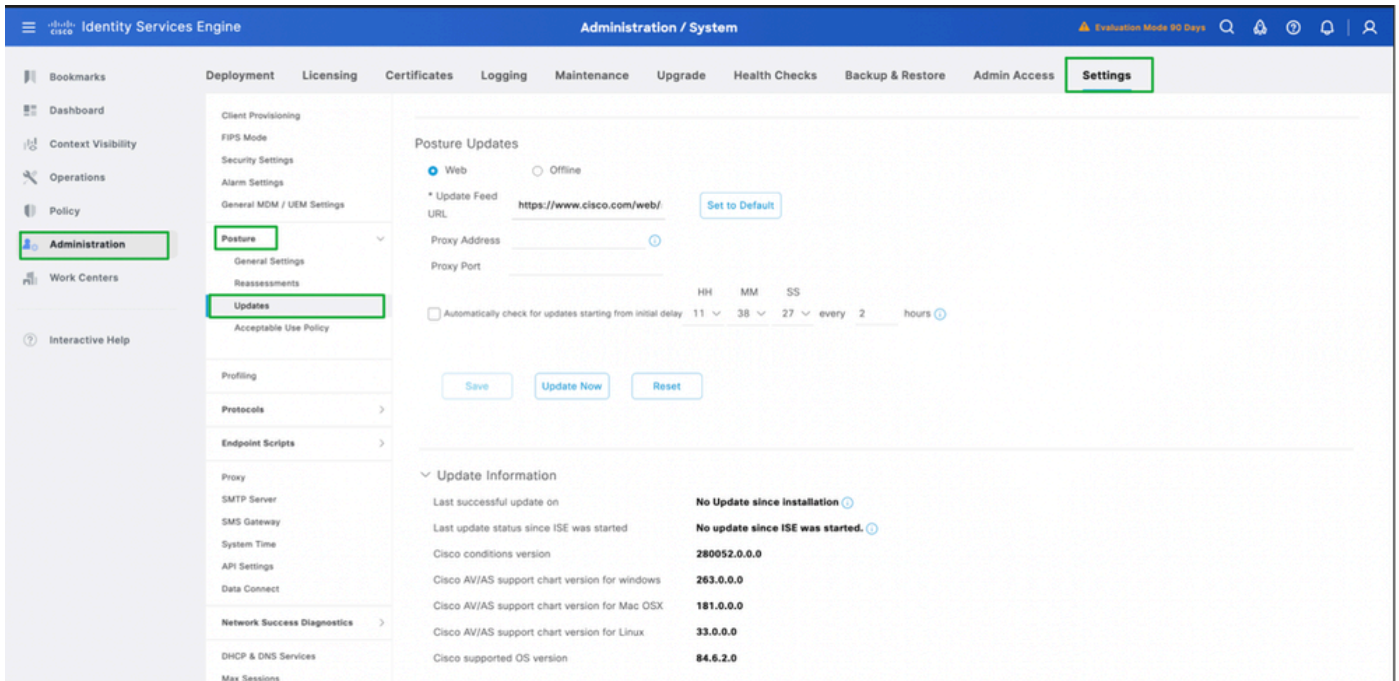


Offline Posture Update Files Include

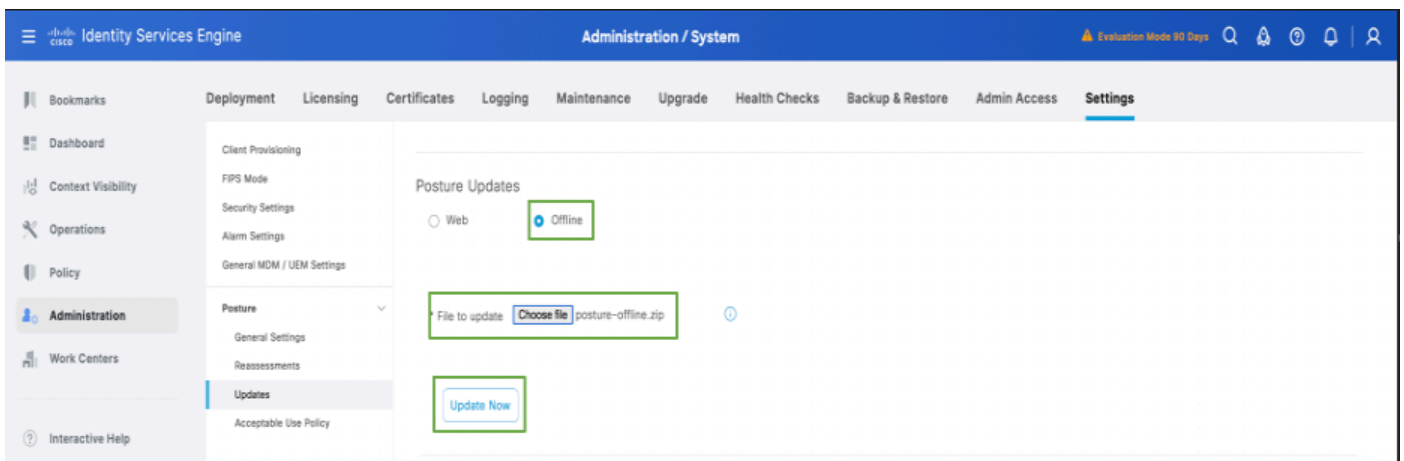
- Antivirus definitions (signatures).
- Posture policies and rules.
- Security assessments and other configuration files for posture evaluation.

Procedure to Perform Offline Posture Updates

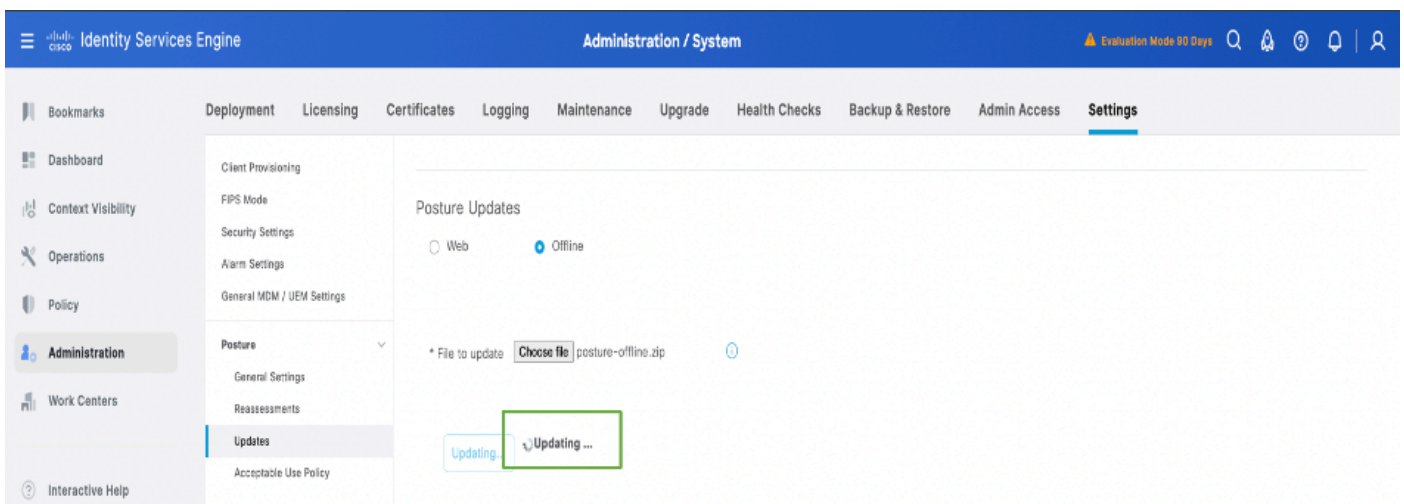
1. Log in to the **ISE GUI -> Administration -> System -> Settings -> Posture -> Updates.**



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



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



The screenshot shows the Cisco Identity Services Engine (ISE) Administration / System page. The left sidebar contains navigation links: Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (selected), and Work Centers. The main content area is divided into two sections: Posture Updates and Update Information.

Posture Updates Configuration:

- Mode:** Web (selected), Offline
- Update Feed URL:** <https://www.cisco.com/web/> (Set to Default button)
- Proxy Address:** [Redacted]
- Proxy Port:** 8080
- Automatic check for updates:** ☐ Automatically check for updates starting from initial delay 14 HH 24 MM 23 SS every 2 hours
- Buttons:** Save, Updating..., Reset, Updating...

Update Information (Highlighted):

Update Information	
Last successful update on	No Update since Installation
Last update status since ISE was started	An update is running
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	101.6.3.0

4. Status of the Posture updates can be verified from the **Update Information** as per this screenshot:

The screenshot shows the Cisco Identity Services Engine (ISE) Administration / System page. The left sidebar contains navigation links: Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (selected), and Work Centers. The main content area is divided into two sections: Posture Updates and Update Information.

Posture Updates Configuration:

- Mode:** Web (selected), Offline
- Update Feed URL:** <https://www.cisco.com/web/> (Set to Default button)
- Proxy Address:** [Redacted]
- Proxy Port:** 8080
- Automatic check for updates:** ☐ Automatically check for updates starting from initial delay 14 HH 51 MM 55 SS every 2 hours
- Buttons:** Save, Update Now, Reset

Update Information (Highlighted):

Update Information	
Last successful update on	2025/03/13 14:24:50
Last update status since ISE was started	Last update attempt at 2025/03/13 14:24:50 was successful
Cisco conditions version	300418.0.0.0
Cisco AV/AS support chart version for windows	297.0.0.0
Cisco AV/AS support chart version for Mac OSX	214.0.0.0
Cisco AV/AS support chart version for Linux	66.0.0.0
Cisco supported OS version	101.6.3.0

Verification

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 be able to find the information related to the Posture updates being performed in the deployment.

You could also tail the logs by logging to the CLI of Primary Admin node by using the **show logging application ise-psc.log tail** command.

The Opswat download, referring to posture updates is started:

```
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
```

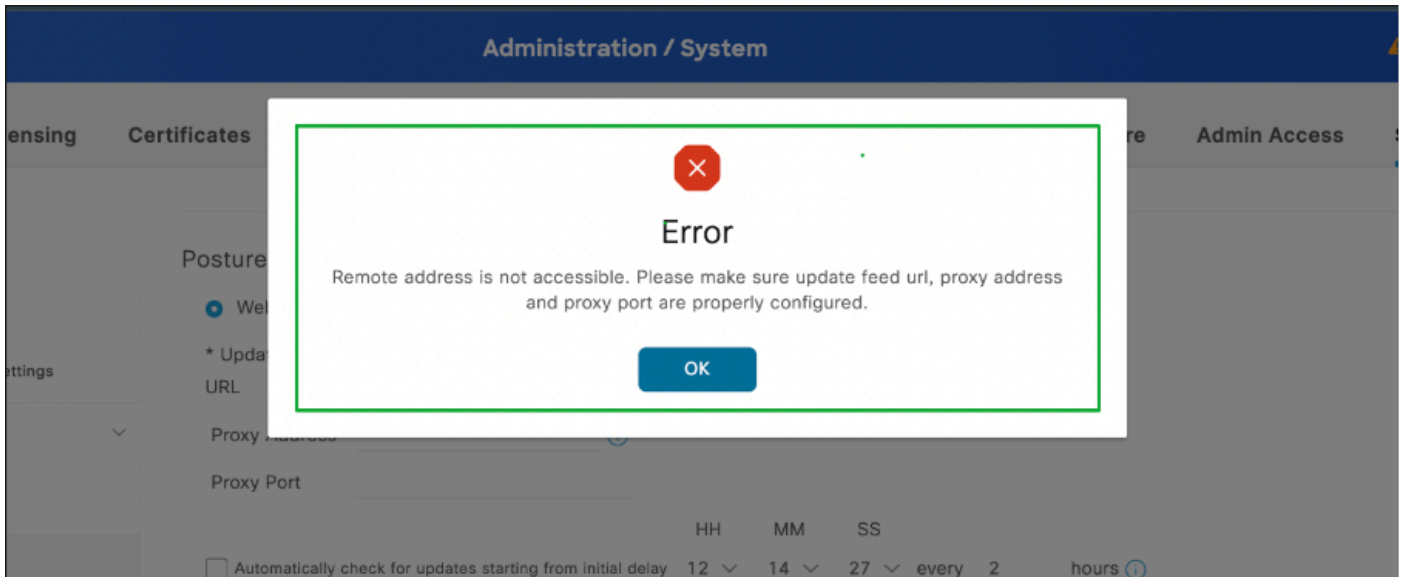
```
2025-03-13 14:24:50,827 INFO [admin-http-pool5][[]] mnt.dbms.datadirect.impl.DatadirectServiceImpl -  
::admin::: Executing getStatus - datadirectSettings
```

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 using 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.

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access **Settings**

Client Provisioning
FIPS Mode
Security Settings
Alarm Settings
General MDM / UEM Settings

Posture ▾
General Settings
Reassessments
Updates
Acceptable Use Policy

Profiling

Protocols >

Endpoint Scripts >

Proxy
SMTP Server
SMS Gateway
System Time
API Settings
Data Connect

Network Success Diagnostics >
DHCP & DNS Services
Max Sessions
Light Data Distribution
Endpoint Replication
Interactive Help

Proxy host server : port
10.10.10.10 : 80

Password required
☐

User name

Password

Confirm Password

Bypass proxy for these hosts and domains

Notes
The following functionalities are impacted by the proxy settings

- Partner Mobile Management
- Endpoint Profiler Feed Service Update
- Endpoint Posture Update
- Endpoint Posture Agent Resources Download
- CRL (Certificate Revocation List) Download
- SMS Message Transmission
- Social Login
- Rest Auth Service - Azure AD
- pxGrid Cloud
- TrustSec Integration for Meraki
- Add "pxGrid Direct Connectors"

Save Reset

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

Known Defects for Posture Update Issues

[Cisco bug ID 01523](#)

Reference

- [Cisco Identity Services Engine Administrator Guide, Release 3.3](#)