

# Mises à jour de la position dans ISE hors ligne et en ligne

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Mises à jour de posture en ligne](#)

[Que se passe-t-il pendant les mises à jour de posture Web ou en ligne ?](#)

[Cas d'utilisation](#)

[Ports utilisés pour la mise à jour de position en ligne](#)

[Procédure de mise à jour de posture en ligne](#)

[Configuration du proxy pour les mises à jour de posture en ligne](#)

[Mises à jour de posture hors ligne](#)

[Que se passe-t-il lorsque vous effectuez une mise à jour de position hors connexion ?](#)

[Cas d'utilisation](#)

[Ports utilisés pour les mises à jour de position hors connexion](#)

[Où trouver des fichiers pour les mises à jour de posture hors connexion ?](#)

[Fichiers de mise à jour de posture hors connexion inclus](#)

[Procédure de mise à jour des postures hors connexion](#)

[Vérification](#)

[Dépannage](#)

[Scénario](#)

[Solution](#)

[Problèmes connus de mise à jour de posture](#)

[Référence](#)

---

## Introduction

Ce document décrit comment effectuer des mises à jour de posture dans Cisco Identity Services Engine® (ISE).

## Conditions préalables

### Exigences

Cisco recommande que vous ayez des connaissances sur le flux de posture.

## Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes .

- Cisco Identity Services Engine 3.2 et versions ultérieures.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Informations générales

Les mises à jour de posture incluent un ensemble de vérifications prédéfinies, de règles et de tableaux de prise en charge des antivirus et des logiciels anti-espions pour les systèmes d'exploitation Windows et MacOS, ainsi que des informations sur les systèmes d'exploitation pris en charge par Cisco.

Lorsque vous déployez Cisco ISE sur votre réseau pour la première fois, vous pouvez télécharger des mises à jour de position à partir du Web. Ce processus prend généralement environ 20 minutes. Après le téléchargement initial, vous pouvez configurer Cisco ISE pour qu'il vérifie et télécharge automatiquement les mises à jour incrémentielles.

Cisco ISE ne crée des politiques de posture par défaut, des exigences et des corrections qu'une seule fois lors des mises à jour de posture initiales. Si vous les supprimez, Cisco ISE ne les crée plus lors des mises à jour manuelles ou planifiées ultérieures.

Il existe deux types de mises à jour de posture que vous pouvez effectuer :

- Mises à jour de posture en ligne.
- Mises à jour de posture hors connexion.

## Mises à jour de posture en ligne

Une mise à jour de posture Web/mise à jour de posture en ligne récupère les dernières mises à jour de posture à partir des référentiels cloud ou serveur Cisco. Cela implique le téléchargement des dernières politiques, définitions et signatures directement à partir des serveurs Cisco. ISE doit se connecter à des serveurs cloud Cisco ou mettre à jour des référentiels pour récupérer les dernières définitions de position, politiques et autres fichiers associés.

Que se passe-t-il pendant les mises à jour de posture Web ou en ligne ?

Identity Services Engine (ISE) accède au site Web de Cisco par le biais d'un proxy ou d'une connexion Internet directe via HTTP, établissant ainsi une connexion avec [www.cisco.com](http://www.cisco.com). Au cours de ce processus, l'échange Hello client et Hello serveur se produit, le serveur fournissant son certificat pour vérifier sa légitimité et confirmer l'approbation côté client. Une fois les opérations Hello client et serveur terminées, l'échange de clés client a lieu et le serveur lance les

mise à jour de position. Voici la capture de paquets illustrant la communication entre le serveur ISE et Cisco.com pendant les mises à jour de la position en ligne.

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=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=5618 Win=42496 Len=0 TSval=236259736 TSecr=654727788
372	10.1.	17.		TLSv1.2	Application Data

- Pendant le paquet Hello du serveur, Cisco.com envoie ces certificats au client pour confirmer l'approbation côté client.

<#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)

- Dans l'interface utilisateur graphique d'ISE, il est important de s'assurer que le certificat de serveur IdenTrust Commercial Root CA 1 est activé et Trust pour l'authentification des services Cisco afin d'établir la connectivité avec Cisco.com. Par défaut, ce certificat est inclus dans ISE et la case « Trust for authenticating Cisco services » est cochée, mais la vérification est conseillée.
- Vérifiez l'état du certificat et l'utilisation approuvée en accédant à l'interface utilisateur graphique ISE > Administration > Certificates > Trusted Certificates. Filtrez par le nom IdenTrust Commercial Root CA 1, sélectionnez le certificat, puis modifiez-le pour vérifier l'utilisation de la confiance, comme indiqué dans cette capture d'écran :

The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance', 'Upgrade', 'Health Checks', 'Backup & Restore', and 'Admin Access'. The left sidebar has 'Administration' selected. The main content area is titled 'Issuer' and shows the configuration for 'IdenTrust Commercial Root CA 1'. The configuration details are as follows:

- \* Friendly Name: IdenTrust Commercial Root CA 1
- Status: Enabled
- Description: IdenTrust Commercial Root CA 1
- Subject: CN=IdenTrust Commercial Root CA 1,O=IdenTrust,C=US
- Issuer: CN=IdenTrust Commercial Root CA 1,O=IdenTrust,C=US
- Valid From: Thu, 16 Jan 2014 18:12:23 UTC
- Valid To (Expiration): Mon, 16 Jan 2034 18:12:23 UTC
- Serial Number: 0A 01 42 80 00 00 01 45 23 C8 44 B5 00 00 00 02
- Signature Algorithm: SHA256withRSA
- Key Length: 4096

Under the 'Usage' section, the 'Trusted For' options are:

- Trust for authentication within ISE
- Trust for client authentication and Syslog
- Trust for certificate based admin authentication
- Trust for authentication of Cisco Services
- Trust for Native IPSec certificate based authentication

- Les mises à jour de posture peuvent inclure des stratégies de posture nouvelles ou révisées, de nouvelles définitions d'antivirus/antimalware et d'autres critères liés à la sécurité pour les évaluations de posture.
- Cette méthode nécessite une connexion Internet active et est généralement exécutée lorsque le système ISE est configuré pour utiliser des référentiels basés sur le cloud pour les mises à jour de position.

## Cas d'utilisation

Les mises à jour de posture en ligne sont utilisées lorsque vous souhaitez vous assurer que les stratégies de posture, les définitions de sécurité et les critères sont à jour avec les dernières versions disponibles fournies par Cisco.

## Ports utilisés pour la mise à jour de position en ligne

Pour que le système ISE puisse atteindre les serveurs cloud Cisco afin de télécharger les mises à jour de posture, ces ports doivent être ouverts dans votre pare-feu et autorisés pour les communications sortantes d'ISE vers Internet :

### 1. HTTPS (TCP 443) :

- Port principal permettant à ISE d'atteindre les serveurs cloud Cisco et de télécharger les mises à jour via une connexion sécurisée (TLS/SSL).
- Il s'agit du port le plus important pour le processus de mise à jour de posture basé sur le Web.

### 2. DNS (UDP 53) :

- ISE doit être en mesure d'effectuer des recherches DNS pour résoudre les noms d'hôte des serveurs de mise à jour.

- Assurez-vous que votre système ISE peut atteindre les serveurs DNS et résoudre les noms de domaine.

### 3. NTP (UDP 123) :

- ISE utilise NTP pour la synchronisation temporelle. Ceci est important pour s'assurer que le processus de mise à jour est correctement horodaté et que le système ISE fonctionne dans un fuseau horaire synchronisé.
- Dans de nombreux cas, les serveurs NTP doivent également être accessibles via UDP 123.

Procédure de mise à jour de posture en ligne

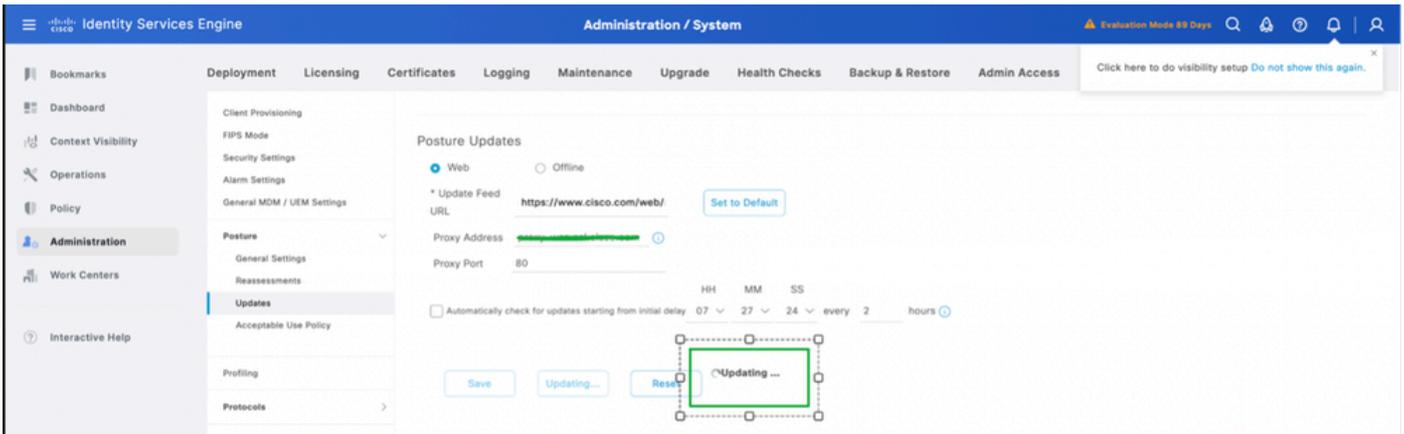
1. Connectez-vous à l'interface graphique utilisateur -> Administration -> System -> Settings -> Posture -> Updates.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration / System Settings page. The 'Settings' tab is active, and the 'Updates' section under 'Posture' is selected. The 'Posture Updates' configuration is displayed, showing the 'Web' method selected. The 'Update Feed URL' is set to 'https://www.cisco.com/web/'. The 'Proxy Address' and 'Proxy Port' fields are empty. The 'Automatically check for updates starting from initial delay' is set to 11 hours, 38 minutes, and 27 seconds every 2 hours. The 'Update Information' section shows the last successful update on 'No Update since installation' and the last update status since ISE was started as 'No update since ISE was started.' The Cisco conditions version is 280052.0.0.0, and the Cisco AV/AS support chart versions for Windows, Mac OS X, and Linux are 263.0.0.0, 181.0.0.0, and 33.0.0.0 respectively. The Cisco supported OS version is 84.6.2.0.

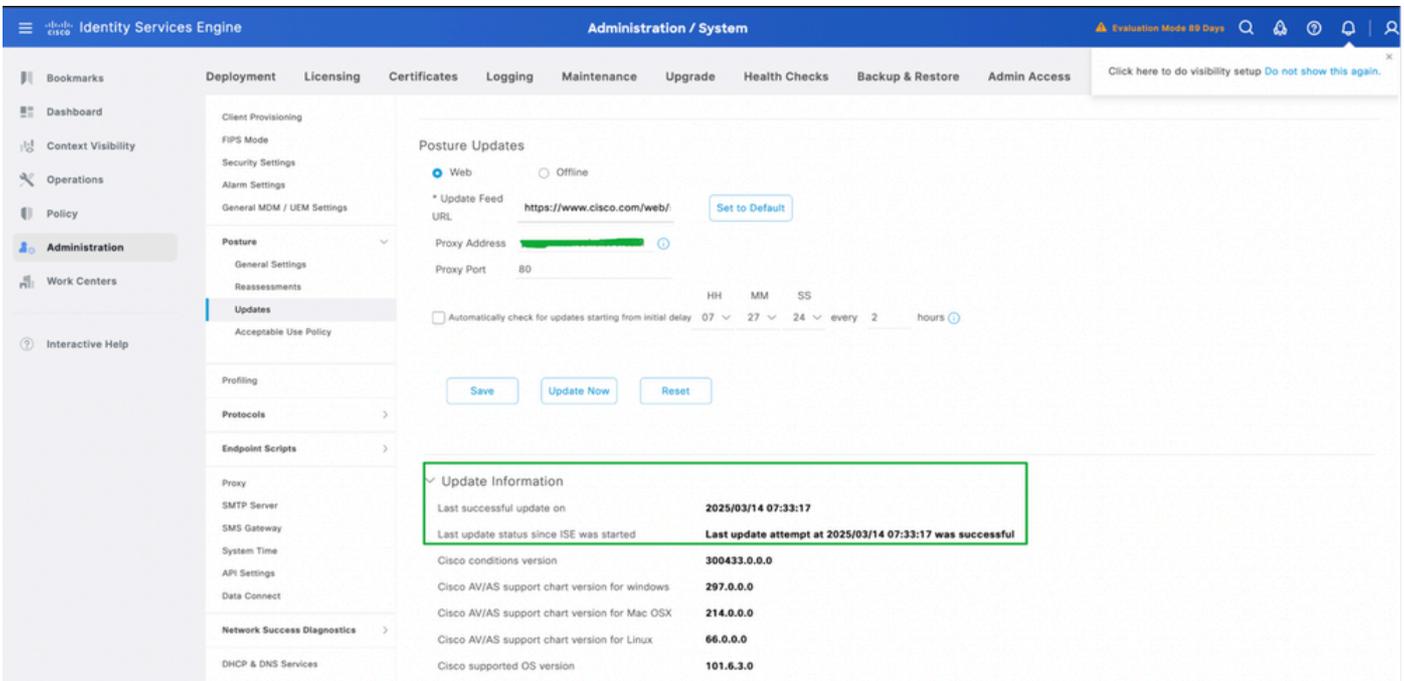
2. Sélectionnez la méthode Web pour les mises à jour de posture en ligne, puis cliquez sur Mettre à jour maintenant.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration / System Settings page. The 'Settings' tab is active, and the 'Updates' section under 'Posture' is selected. The 'Posture Updates' configuration is displayed, showing the 'Web' method selected. The 'Update Feed URL' is set to 'https://www.cisco.com/web/'. The 'Proxy Address' and 'Proxy Port' fields are empty. The 'Automatically check for updates starting from initial delay' is set to 07 hours, 27 minutes, and 24 seconds every 2 hours. The 'Update Information' section shows the last successful update on 'No Update since installation' and the last update status since ISE was started as 'No update since ISE was started.' The Cisco conditions version is 280052.0.0.0, and the Cisco AV/AS support chart versions for Windows, Mac OS X, and Linux are 263.0.0.0, 181.0.0.0, and 33.0.0.0 respectively. The Cisco supported OS version is 84.6.2.0.

3. Une fois les mises à jour de posture commencées, le statut devient Mise à jour.



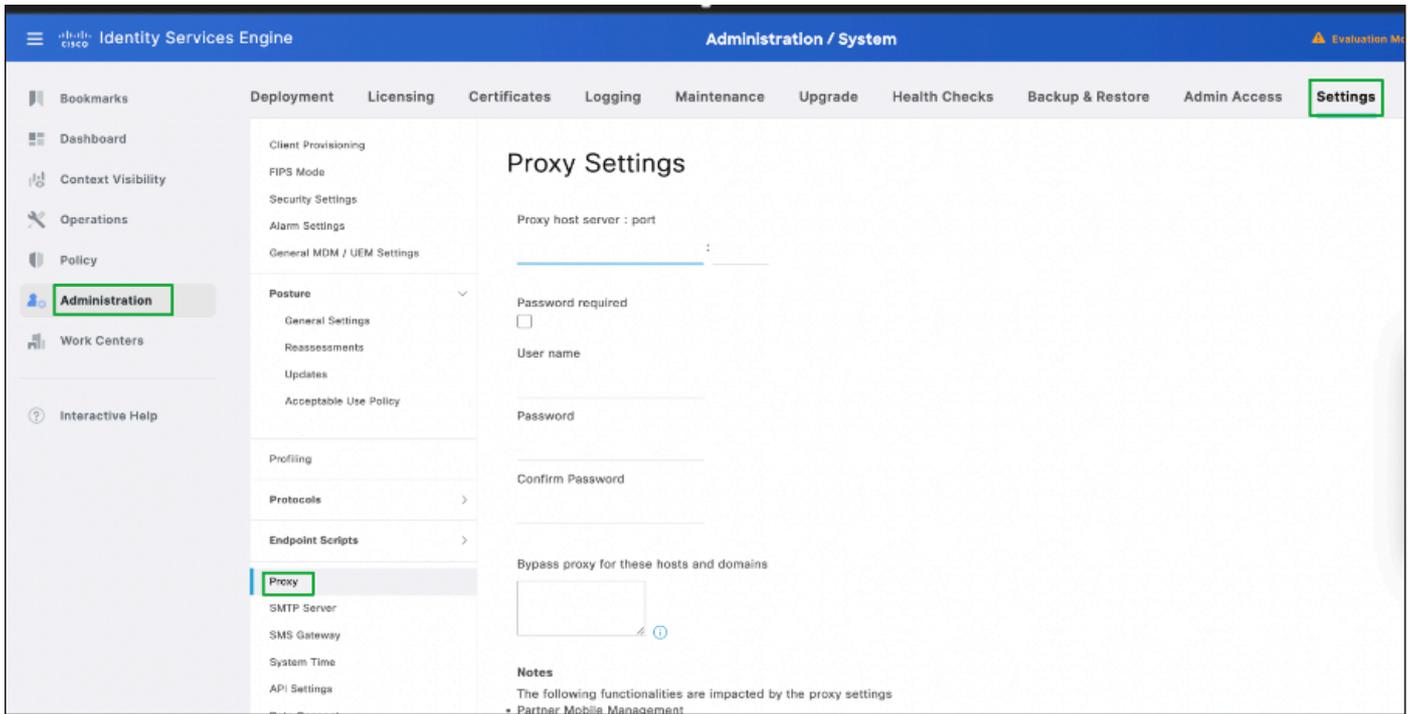
4. État des mises à jour de la position peut être vérifié à partir des informations de mise à jour selon cette capture d'écran :



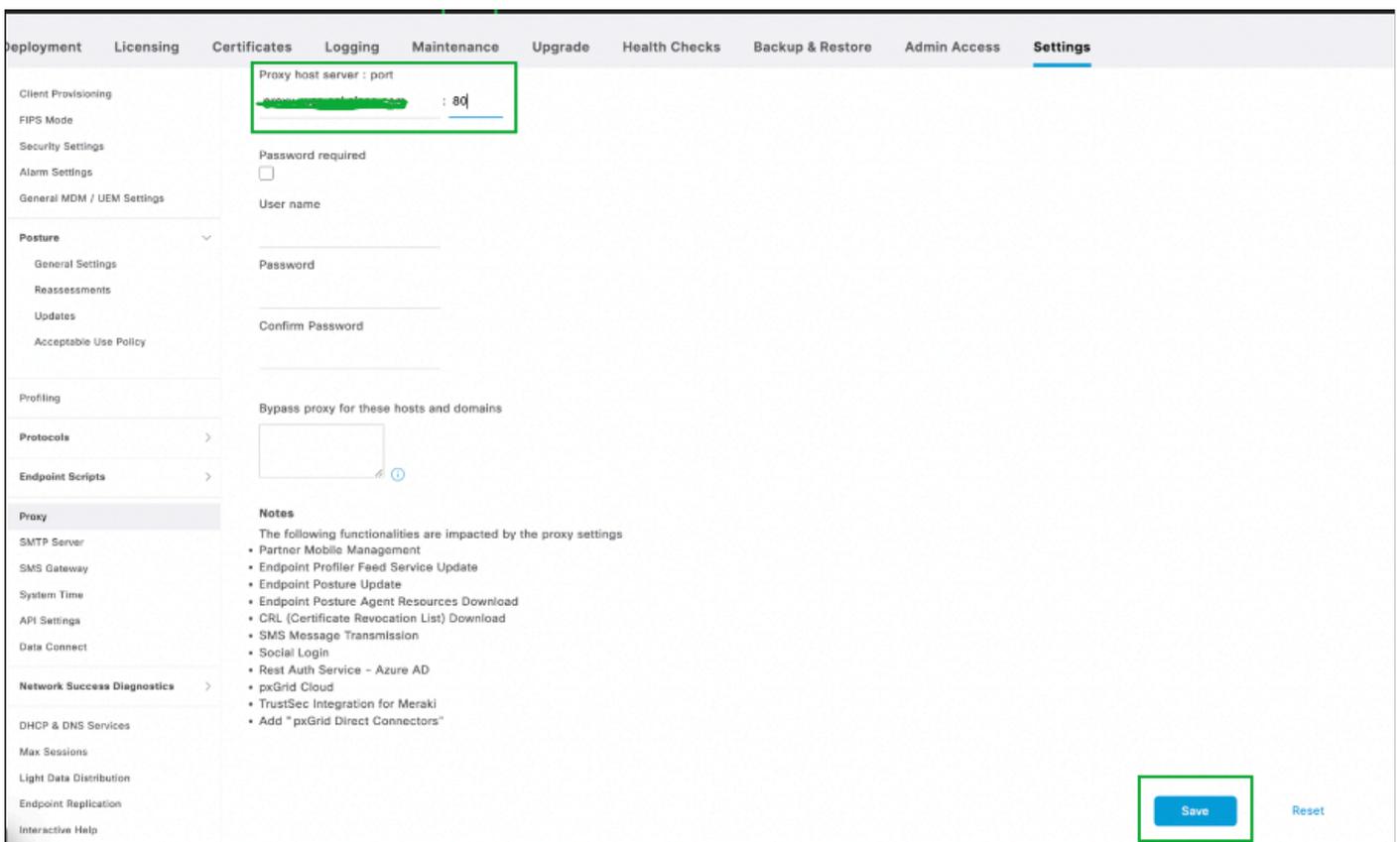
## Configuration du proxy pour les mises à jour de posture en ligne

Dans un environnement restreint où l'URL du champ Mise à jour de la position n'est pas accessible, la configuration du proxy est alors requise. Reportez-vous à Configurer le proxy dans ISE.

1. Accédez à Administration -> Système -> Paramètres -> Proxy.



2. Configurez les détails du proxy, cliquez sur Enregistrer.



3. Les détails du proxy seraient automatiquement récupérés par ISE lorsque les mises à jour de position en ligne sont effectuées.

## Mises à jour de posture hors ligne

Une mise à jour de posture hors ligne vous permet de télécharger manuellement des fichiers de mise à jour de posture (sous la forme d'un fichier .zip ou d'un autre format de fichier pris en charge) vers ISE.

Que se passe-t-il lorsque vous effectuez une mise à jour de position hors connexion ?

- Vous téléchargez manuellement les fichiers de posture mis à jour.
- ISE traite et applique ces fichiers, qui peuvent inclure des stratégies mises à jour, des définitions d'antivirus, des évaluations de position, entre autres types de fichiers.
- La mise à jour hors connexion ne nécessite pas de connectivité Internet et est généralement utilisée dans des environnements dotés de politiques de sécurité ou de réseau strictes qui empêchent l'accès direct aux serveurs externes.

### Cas d'utilisation

Cette méthode est souvent utilisée dans des environnements où le système est isolé d'Internet ou lorsque vous disposez de fichiers de mise à jour hors connexion spécifiques fournis par Cisco ou votre équipe de sécurité.

### Ports utilisés pour les mises à jour de position hors connexion

Pour une communication générale avec le serveur ISE (pendant le processus de mise à jour), dans de nombreux cas, ces ports sont pertinents :

1. Accès à la gestion (ports 22 et 43) :
  - SSH (TCP 22) : Si vous utilisez SSH pour accéder au système ISE à des fins de dépannage ou de téléchargement manuel.
  - HTTPS (TCP 443) : Si vous utilisez l'interface utilisateur graphique (Web interface) pour le téléchargement de la mise à jour.
2. Transfert de fichiers (SFTP ou SCP) :
  - Si vous devez télécharger des fichiers manuellement vers ISE via SFTP ou SCP, assurez-vous que les ports correspondants (généralement le port 22 pour SSH/SFTP) sont ouverts sur le système ISE.
3. Accès au réseau local :
  - Assurez-vous que le système à partir duquel vous téléchargez la mise à jour (par exemple, une station de travail ou un serveur d'administration) peut communiquer avec ISE via les ports nécessaires pour l'accès à la gestion, mais là encore, les mises à jour de position hors connexion ne nécessitent aucun port externe puisque les fichiers sont fournis manuellement.

### Où trouver des fichiers pour les mises à jour de posture hors connexion ?

1. Accédez à l'URL : <https://www.cisco.com/web/secure/spa/posture-offline.html>, cliquez sur Download et le fichier posture-offline.zip est téléchargé sur votre système local.

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**.

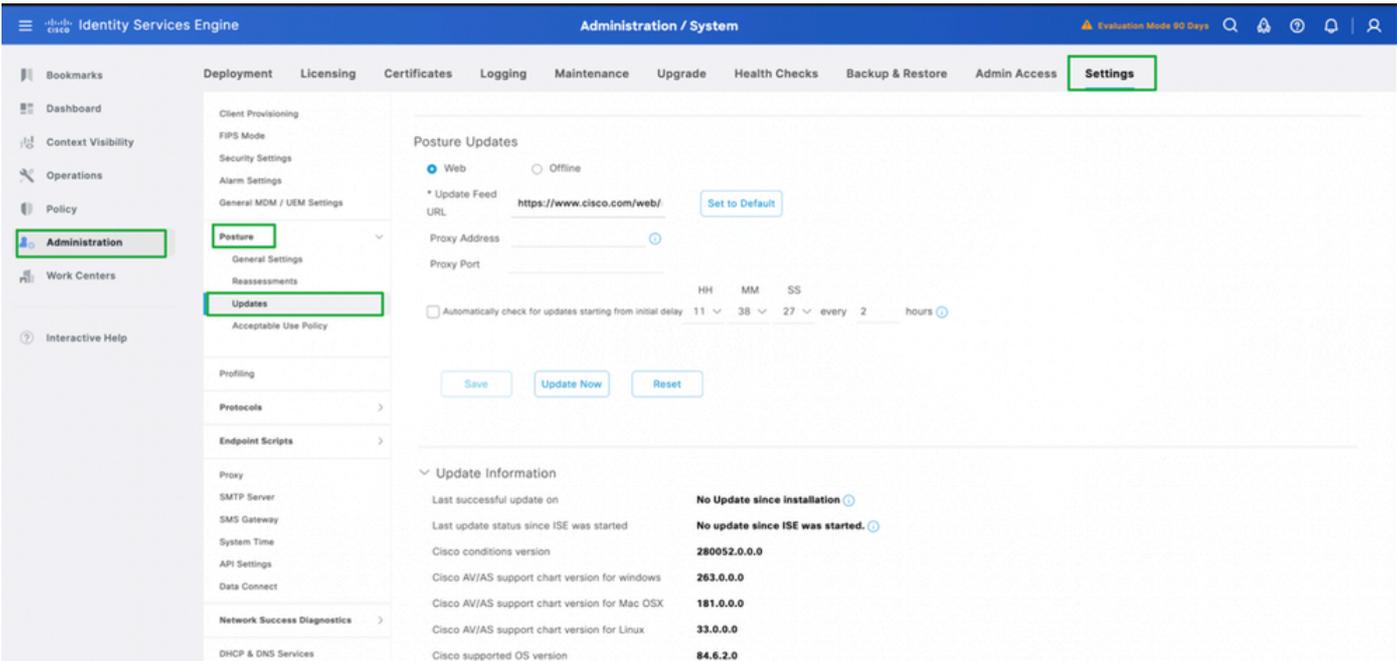
[Download](#)

## Fichiers de mise à jour de posture hors connexion inclus

- Définitions d'antivirus (signatures).
- Stratégies et règles de posture.
- Évaluations de sécurité et autres fichiers de configuration pour l'évaluation de la position.

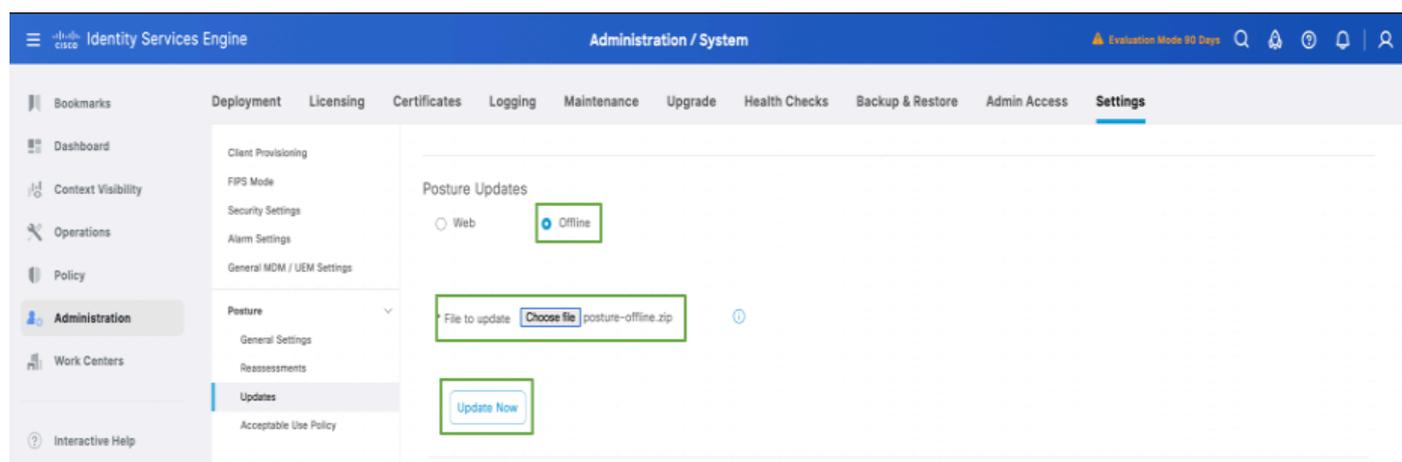
## Procédure de mise à jour des postures hors connexion

1. Connectez-vous à l'interface utilisateur graphique ISE -> Administration -> System -> Settings -> Posture -> Updates.

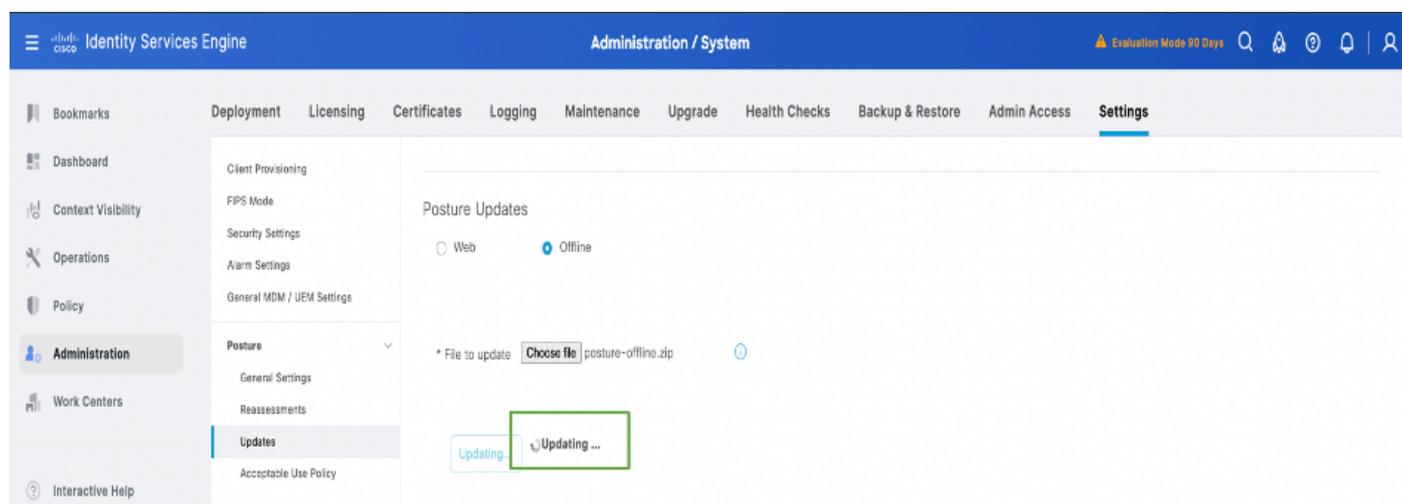


The screenshot shows the Cisco Identity Services Engine (ISE) Administration GUI. The breadcrumb navigation is Administration / System > Settings > Posture > Updates. The 'Posture Updates' section is active, showing the 'Offline' radio button selected. The 'Update Feed URL' is set to https://www.cisco.com/web/. The 'Proxy Address' and 'Proxy Port' fields are empty. The 'Automatically check for updates starting from initial delay' is set to 11:38:27 every 2 hours. The 'Update Information' section shows the last successful update as 'No Update since installation' and the last update status as 'No update since ISE was started'. The Cisco conditions version is 280052.0.0.0, and the supported OS versions are listed as 263.0.0.0 for Windows, 181.0.0.0 for Mac OS X, 33.0.0.0 for Linux, and 84.6.2.0 for Cisco supported OS version.

2. Sélectionnez l'option hors connexion, parcourez et sélectionnez le dossier posture-offline.zip qui a été téléchargé sur votre système local. Cliquez sur Mettre à jour maintenant.



3. Une fois les mises à jour de posture commencées, le statut devient Mise à jour.



The screenshot shows the 'Posture Updates' configuration page in the Cisco Identity Services Engine. The 'Update Information' section is highlighted with a green box and contains the following data:

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. État des mises à jour de la position peut être vérifié à partir des informations de mise à jour selon cette capture d'écran :

The screenshot shows the 'Posture Updates' configuration page in the Cisco Identity Services Engine. The 'Update Information' section is highlighted with a green box and contains the following data:

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

Vérification

Connectez-vous à l'interface graphique du noeud Administrateur principal -> Opérations -> Dépannage -> Journaux de téléchargement -> Journaux de débogage -> Journaux d'application -> isc-psc.log , cliquez sur ise-psc.log et le journal est téléchargé sur votre système local. Ouvrez le fichier téléchargé via le Bloc-notes ou l'éditeur de texte, et filtrez pour le téléchargement d'Opswat. Vous devez être en mesure de trouver les informations relatives aux mises à jour de posture effectuées dans le déploiement.

Vous pouvez également suivre les journaux en vous connectant à l'interface de ligne de commande du noeud Administrateur principal à l'aide de la commande show logging application ise-psc.log tail.

Le téléchargement d'Opswat, faisant référence aux mises à jour de posture, est lancé :

```
2025-03-13 13:58:07,246 INFO [admin-http-pool5][[]]
cisco.cpm.posture.download.DownloadManager -::admin::- Démarrage du téléchargement
d'opswat
```

```
2025-03-13 13:58:07,251 INFO [admin-http-pool5][[]]
cisco.cpm.posture.download.DownloadManager -::admin::- URI du fichier de téléchargement hors
connexion : /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 du fichier de téléchargement hors
connexion : /opt/CSCOCpm/temp/cp/update/5c064701-a1ee-4a09-a190-
3bf83c190af6/osgroups.tar.gz
```

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

Téléchargement Opswat terminé, se référant aux mises à jour de posture sont téléchargés et réussi.

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

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

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

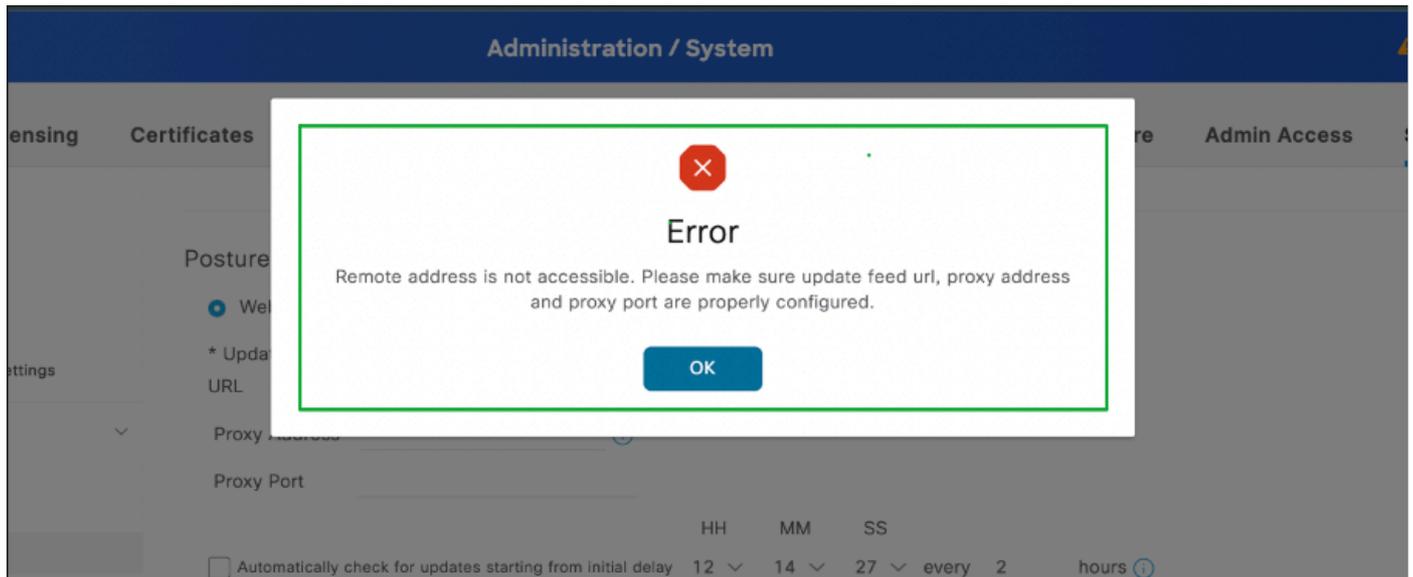
## Dépannage

### Scénario

Échec des mises à jour de position en ligne avec l'erreur « L'adresse distante n'est pas accessible. Assurez-vous que l'URL du flux de mise à jour, l'adresse proxy et le port proxy sont

correctement configurés.

Exemple d'erreur :



## Solution

1. Connectez-vous à l'interface de ligne de commande d'ISE, vérifiez qu'ISE est accessible à cisco.com en utilisant la commande "ping cisco.com".

```
isehostname/admin#ping cisco.com
```

Envoyez une requête ping à cisco.com (72.163.4.161) avec 56(84) octets de données.

```
64 octets de 72.163.4.161 : icmp_seq=1 ttl=235 time=238 ms
```

```
64 octets de 72.163.4.161 : icmp_seq=2 ttl=235 time=238 ms
```

```
64 octets de 72.163.4.161 : icmp_seq=3 ttl=235 time=239 ms
```

```
64 octets de 72.163.4.161 : icmp_seq=4 ttl=235 time=238 ms
```

— cisco.com statistiques ping —

4 paquets transmis, 4 paquets reçus, 0 % de perte de paquets, durée 3004 ms

rtt min/avg/max/mdev = 238,180/238,424/238,766/0,410 ms

2. Accédez à Administration -> Système -> Paramètres -> Le proxy est configuré avec les ports appropriés.

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 : 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. Vérifiez si les ports TCP 443, UDP 53 et UDP 123 sont autorisés sur tous les sauts vers Internet.

Problèmes connus de mise à jour de posture

[ID de bogue Cisco 01523](#)

## Référence

- [Guide de l'administrateur de Cisco Identity Services Engine, version 3.3](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.