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

Table des matières

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.

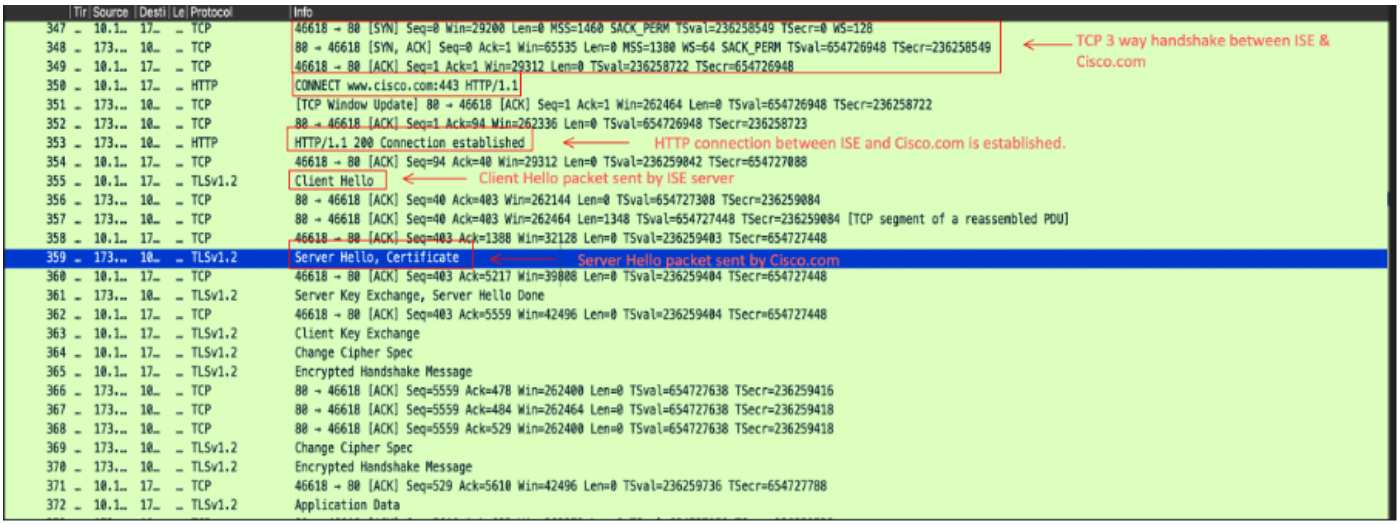
Mises à jour de posture en ligne

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. 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

mises 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.



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

<#root>

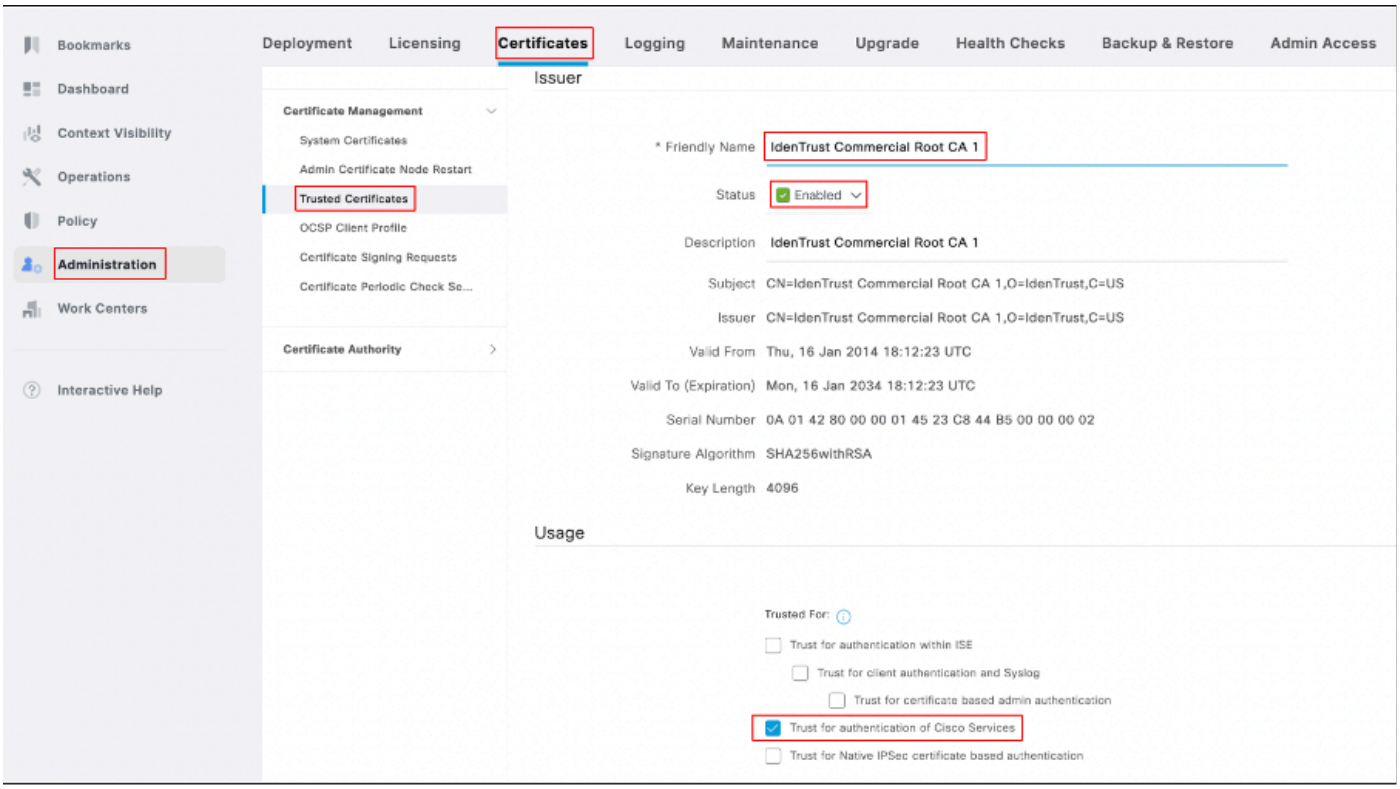
```
Certificates Length: 5083
Certificates (5083 bytes)
Certificate Length: 1940
Certificate: 3082079030820678a003020102021040191d1f3c7ec4ea73b301be3e06a90300d06092a… (id-at-commonNam
Certificate Length: 1754
Certificate: 308206d6308204bea003020102021040016efb0a205cfaebe18f71d73abb78300d06092a… (id-at-commonNam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

IdenTrust Commercial Root CA

1

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

- 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 :



- 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 :

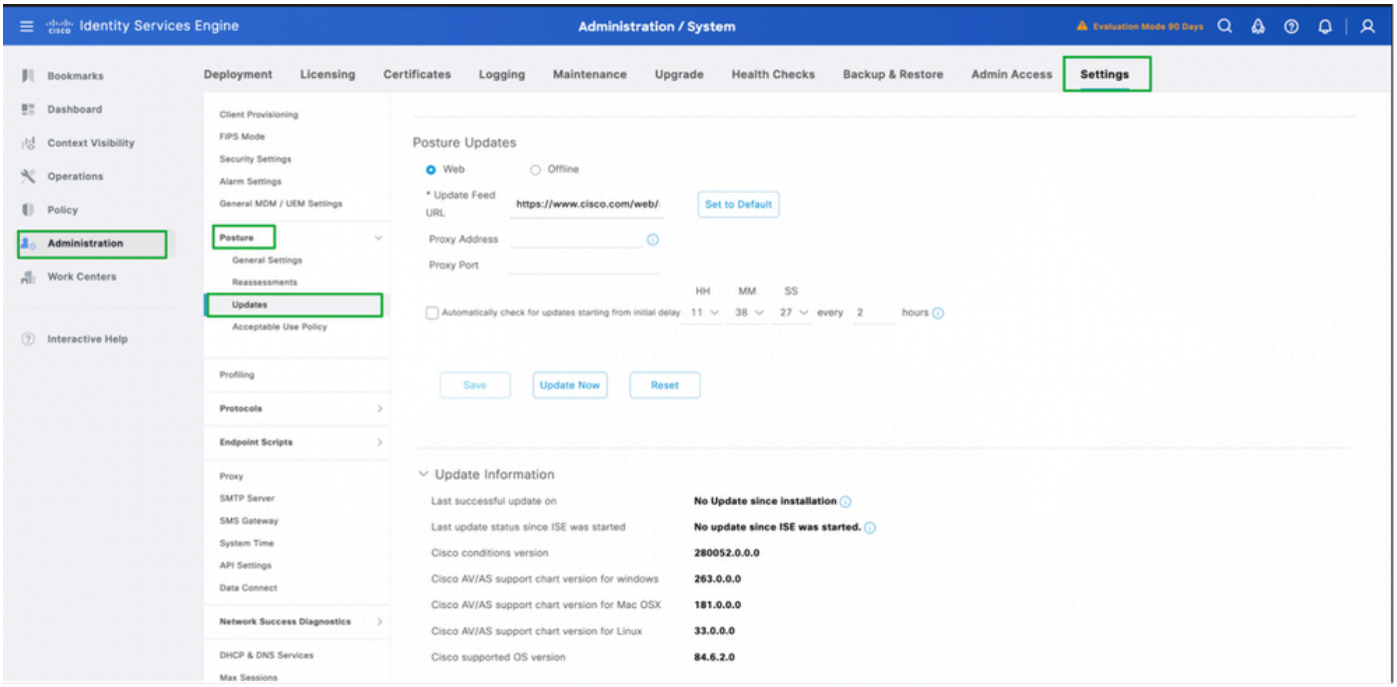
1. HTTPS (TCP 443) :
    - Port principal permettant à ISE d'atteindre les serveurs cloud Cisco et de télécharger les mises à jour via une connexion sécurisée (TLS/SSL).
    - Il s'agit du port le plus important pour le processus de mise à jour de posture basé sur le Web.
2. DNS (UDP 53) :
    - ISE 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.

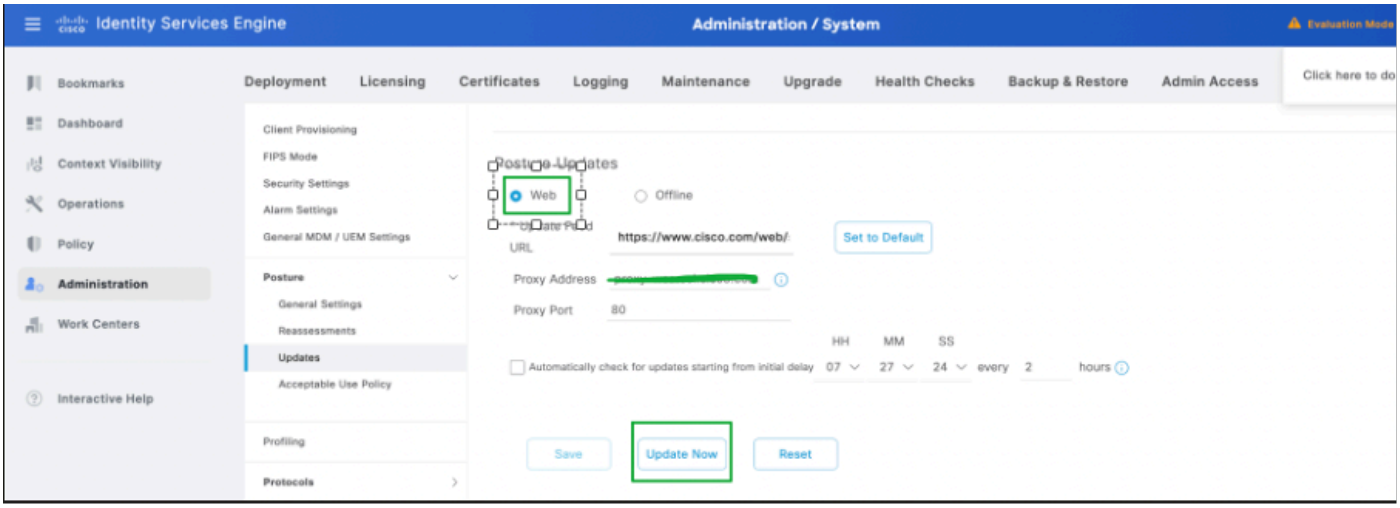
3. NTP (UDP 123) :
   - ISE utilise NTP pour la synchronisation temporelle. Ceci est important pour s'assurer que le processus de mise à jour est correctement horodaté et que le système ISE fonctionne dans un fuseau horaire synchronisé.
   - Dans de nombreux cas, les serveurs NTP doivent également être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

Procédure de mise à jour de posture en ligne

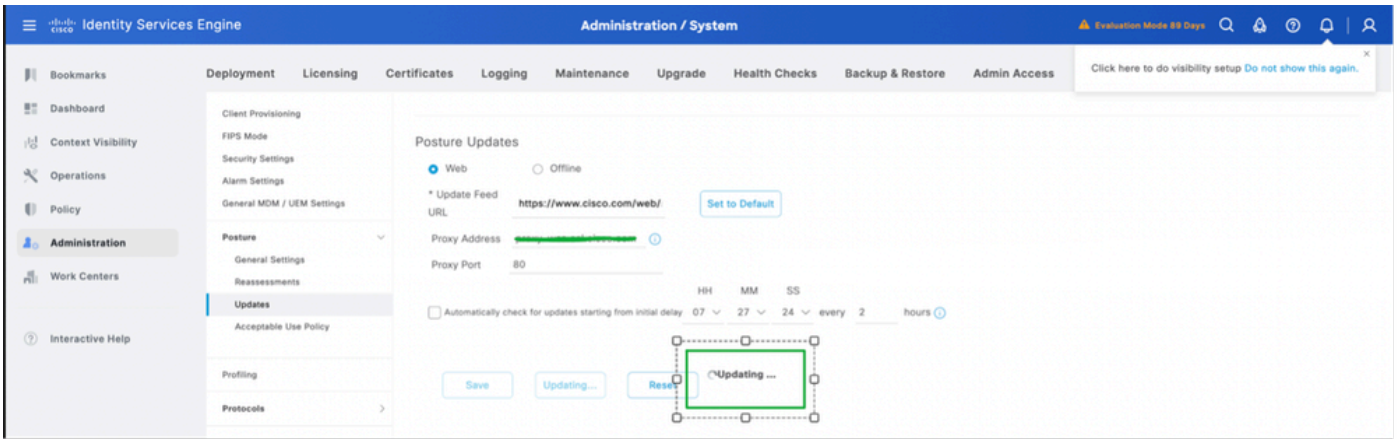
1. Connectez-vous à l'interface graphique utilisateur -> Administration -> System -> Settings -> Posture -> Updates.



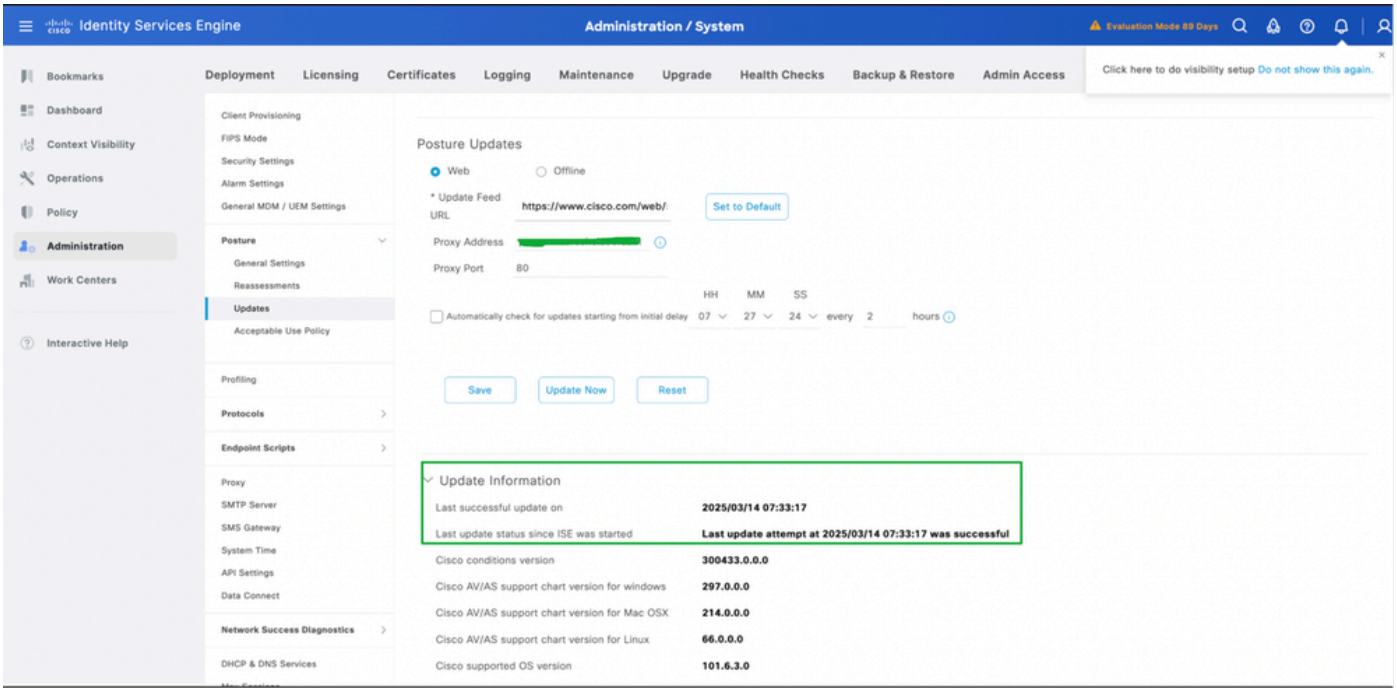
2. Sélectionnez la méthode Web pour les mises à jour de posture en ligne, puis cliquez sur Mettre à jour maintenant.



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



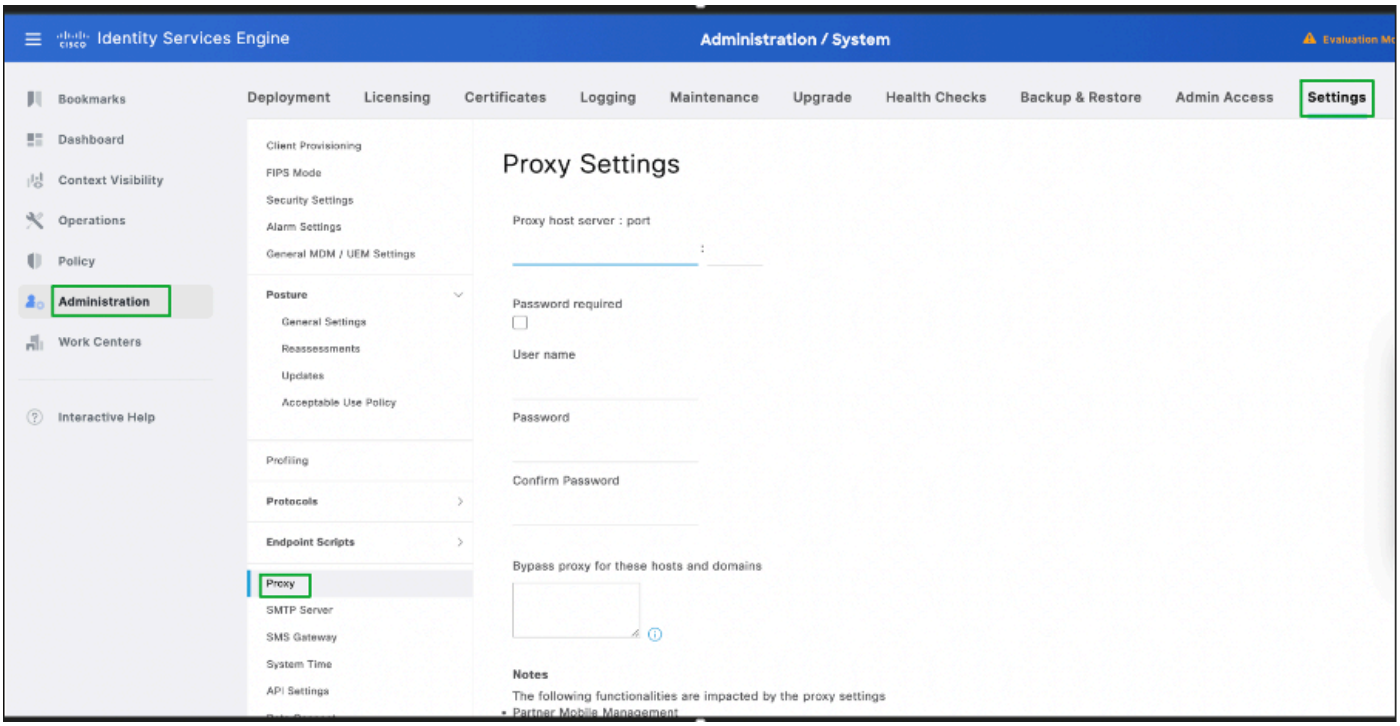
4. État des mises à jour de la position peut être vérifié à partir des informations de mise à jour selon cette capture d'écran :



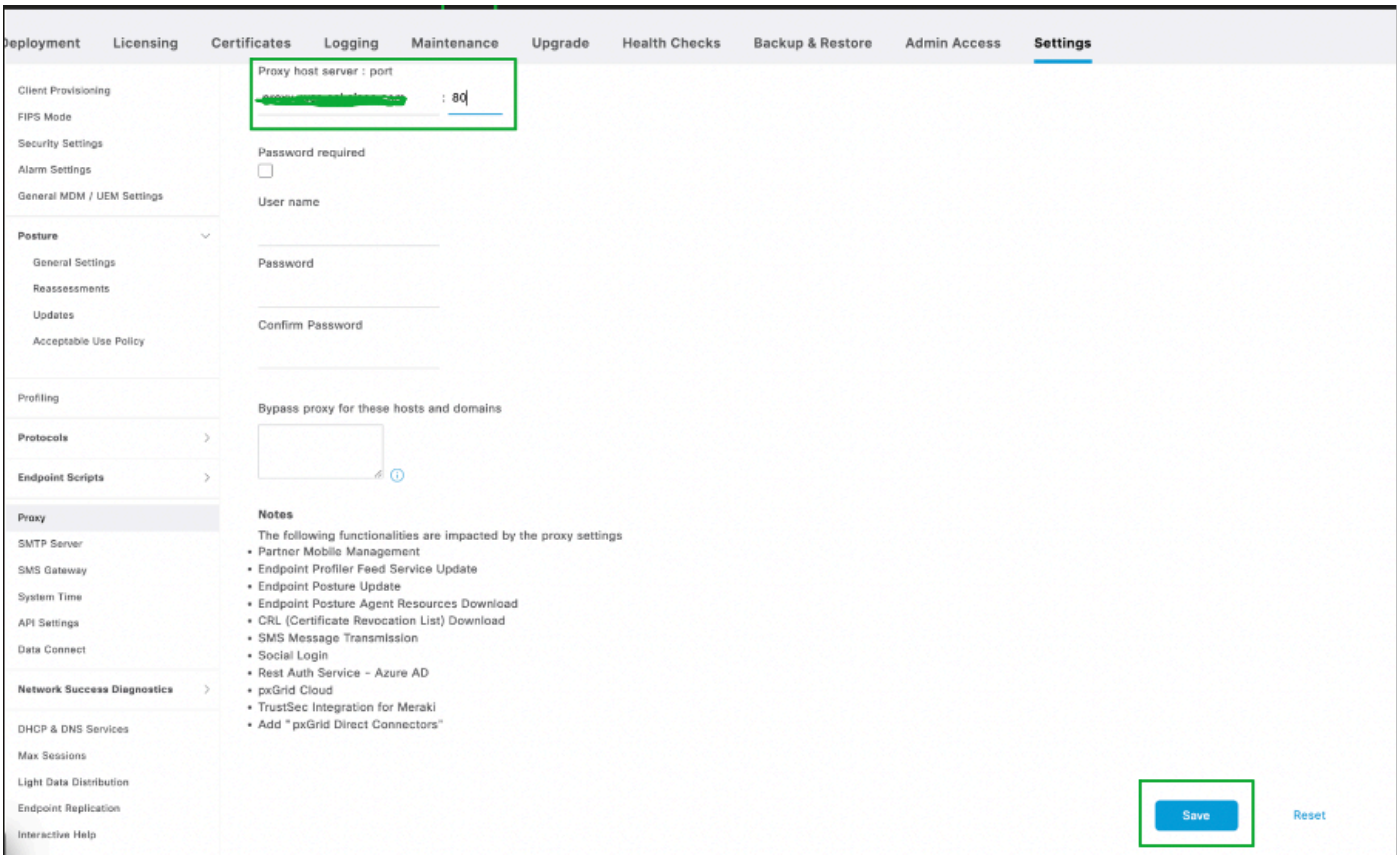
Configuration du proxy pour les mises à jour de posture en ligne

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.

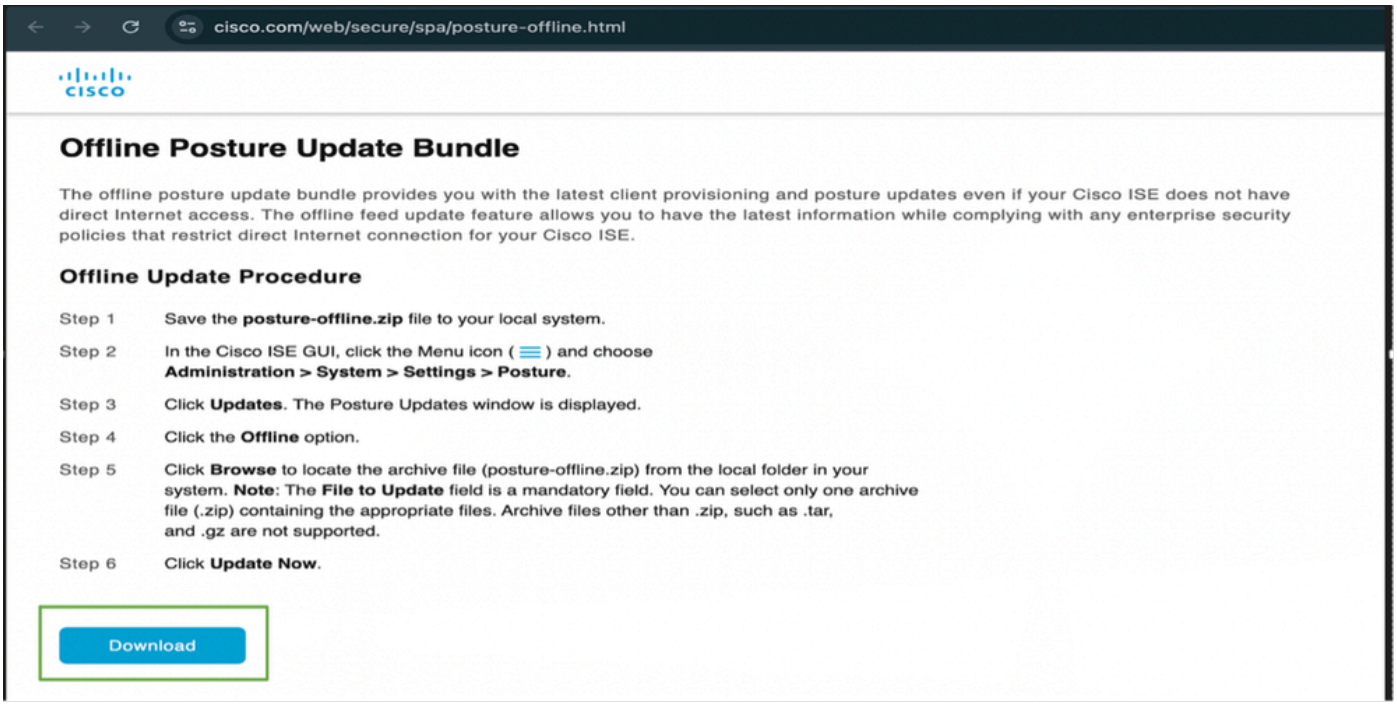
Ports utilisés pour les mises à jour de position hors connexion

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.

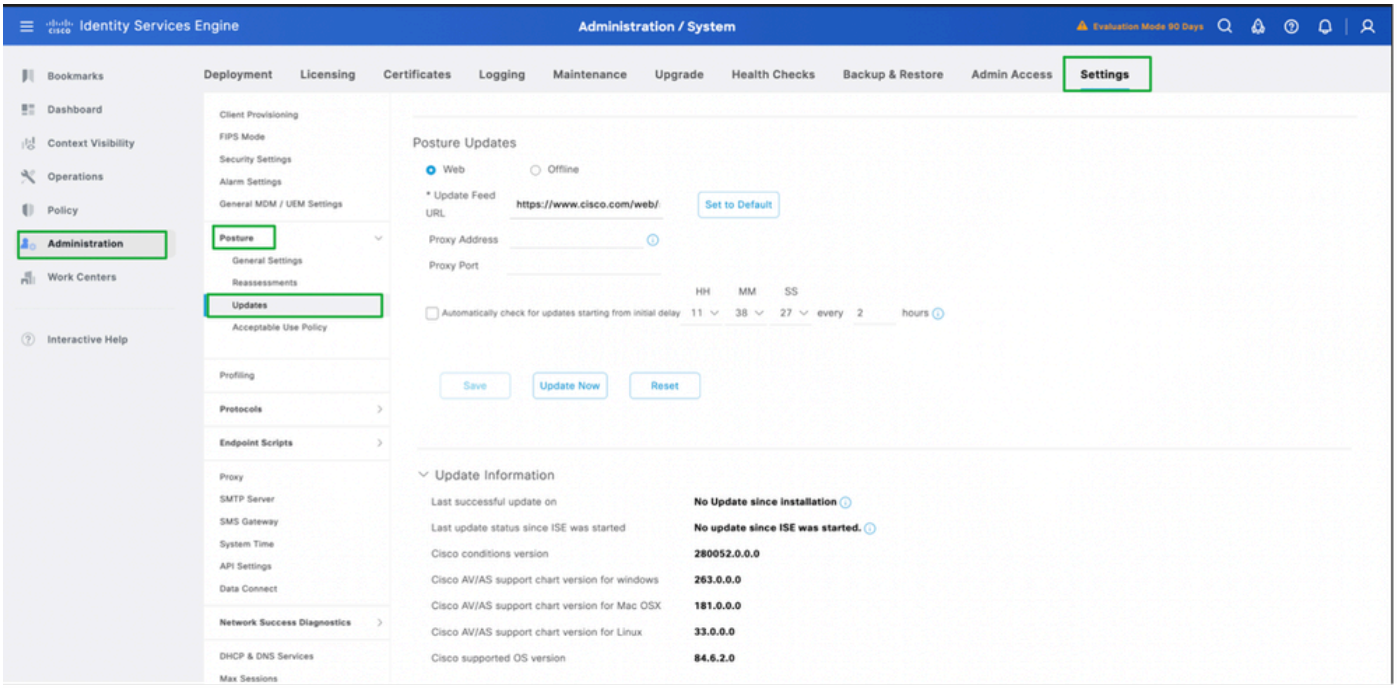


Fichiers de mise à jour de posture hors connexion inclus

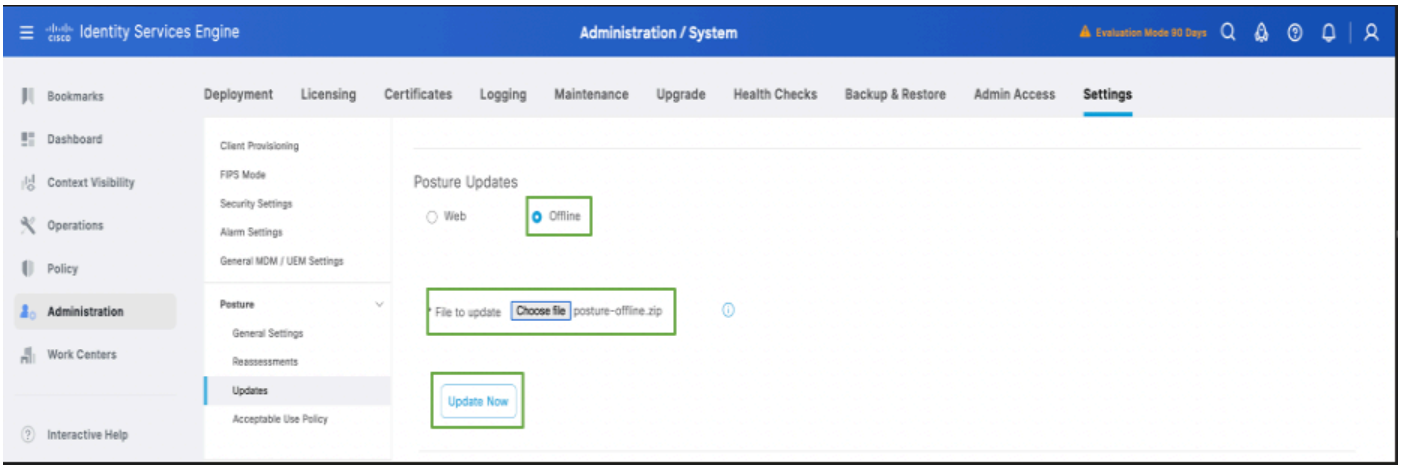
- Définitions d'antivirus (signatures).
- Stratégies et règles de posture.
- Évaluations de sécurité et autres fichiers de configuration pour l'évaluation de la position.

Procédure de mise à jour des postures hors connexion

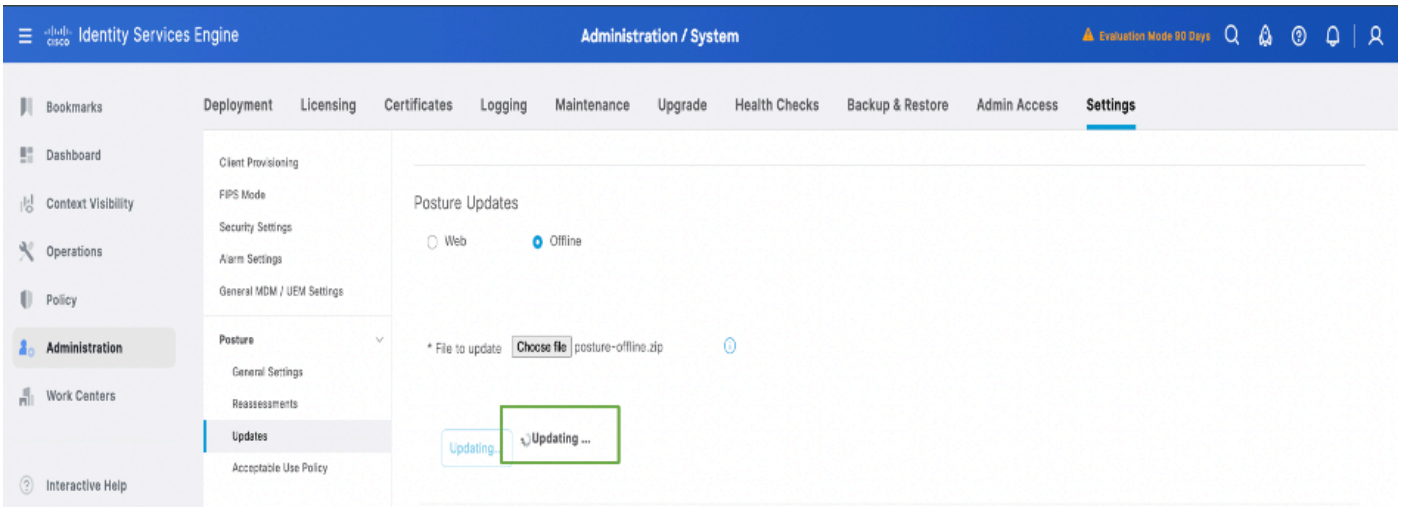
1. Connectez-vous à l'interface utilisateur graphique ISE -> Administration -> System -> Settings -> Posture -> Updates.

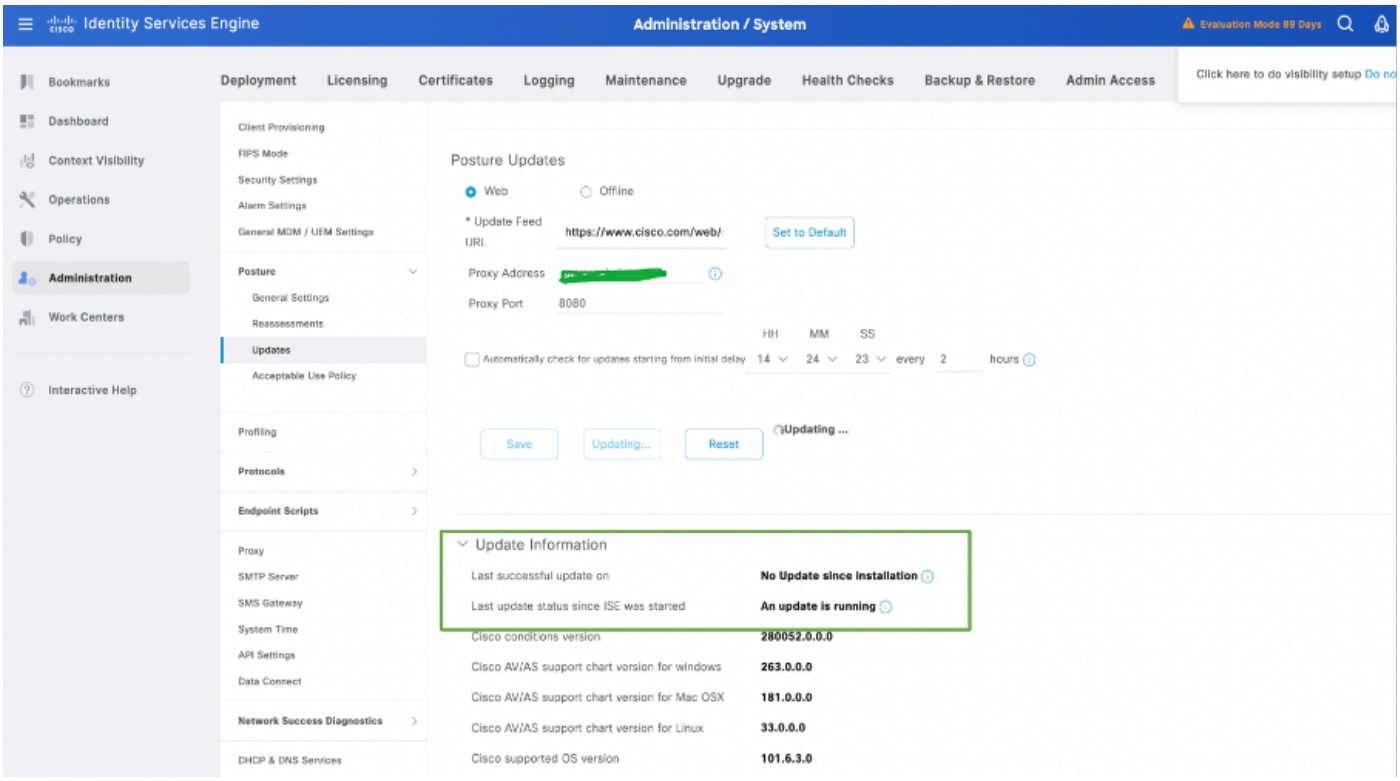


2. Sélectionnez l'option hors connexion, parcourez et sélectionnez le dossier posture-offline.zip qui a été téléchargé sur votre système local. Cliquez sur Mettre à jour maintenant.

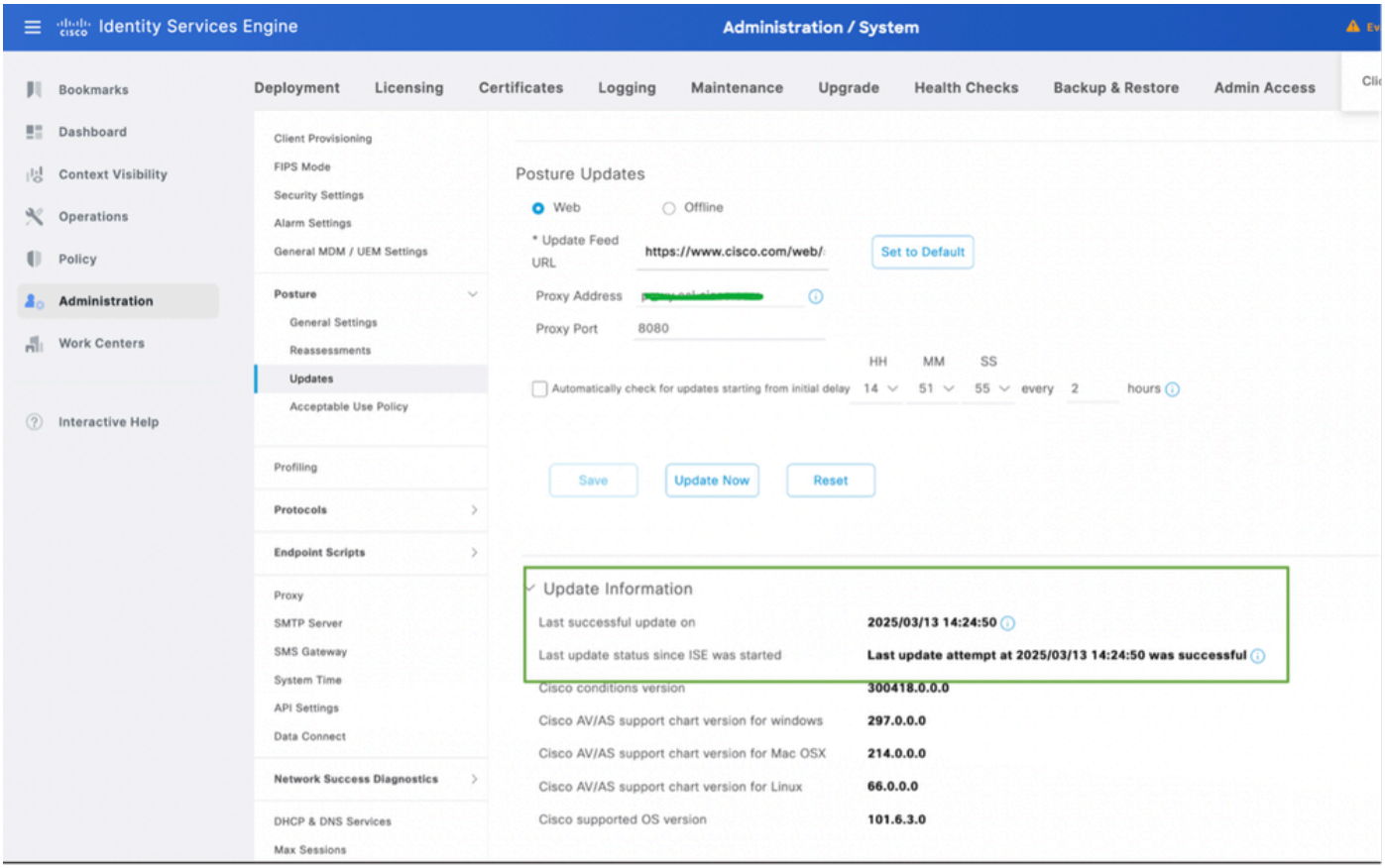


3. Une fois les mises à jour de posture commencées, le statut devient Mise à jour.





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 :



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

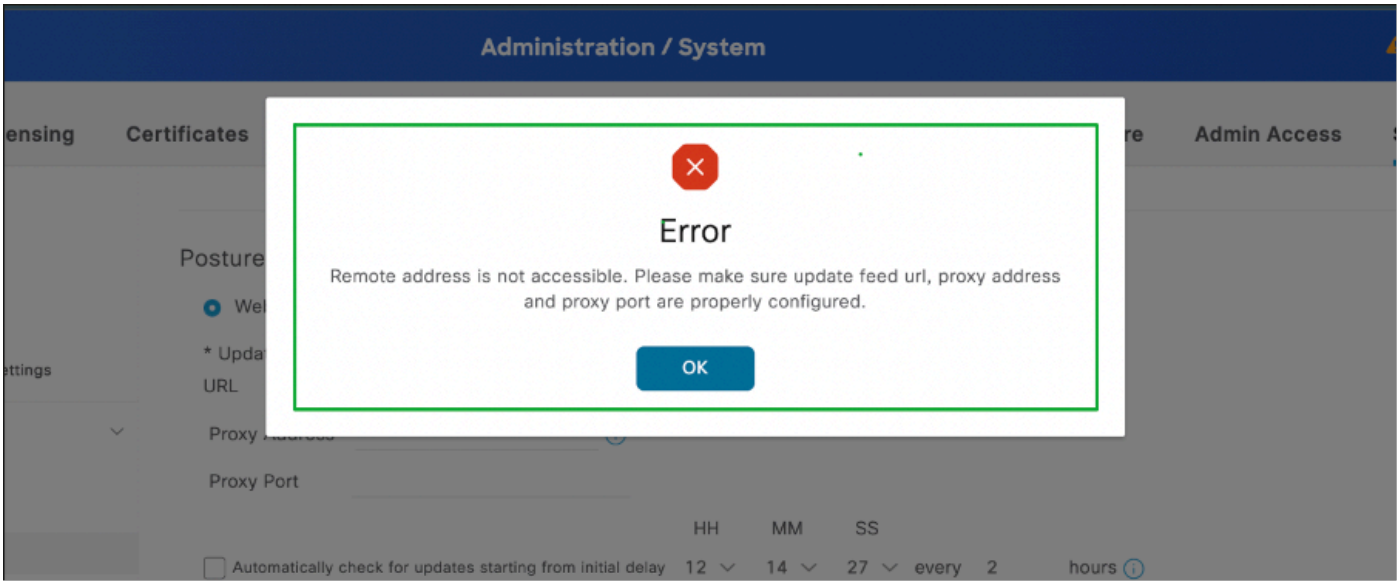
Dépannage

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 :



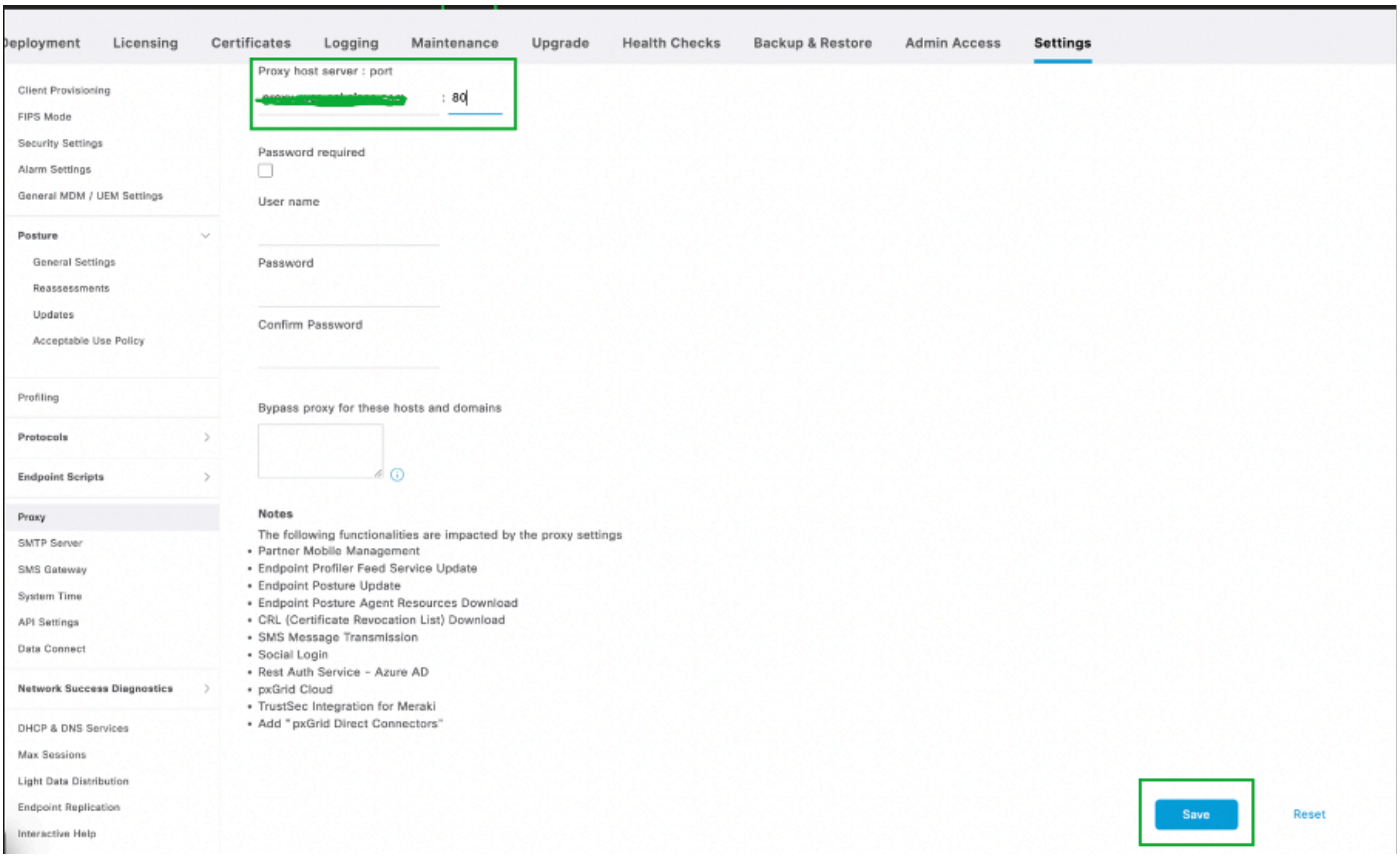
Solution

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.



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.