ISEでのオフラインおよびオンラインでのポスチャ更新の実行

内容

はじめに

このドキュメントでは、Cisco Identity Services Engine®(ISE)でポスチャ更新を実行する方法について説明します。

前提条件

要件

ポスチャフローに関する知識があることが推奨されます。

使用するコンポーネント

このドキュメントの情報は、次のハードウェアとソフトウェアのバージョンに基づくものです。

- Cisco Identity Services Engine(ISE)3.2以降のバージョン

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

ポスチャアップデートには、WindowsとMacOSの両方のオペレーティングシステムに対応するアンチウイルスとアンチスパイウェア、およびシスコがサポートするオペレーティングシステム情報に関する、一連の定義済みチェック、ルール、およびサポートチャートが含まれます。

Cisco ISEをネットワークに初めて導入する場合は、ポスチャアップデートをWebからダウンロードできます。通常、このプロセスには約20分かかります。最初のダウンロードの後、差分アップデートが自動的に実行されることを確認し、ダウンロードするようにCisco ISEを設定できます。

Cisco ISEは、初期ポスチャアップデート中に1回だけ、デフォルトのポスチャポリシー、要件、および修復を作成します。これらを削除しても、Cisco ISEは、その後の手動またはスケジュールされたアップデート中に再作成を行いません。

実行できるポスチャ更新には、次の2つのタイプがあります。

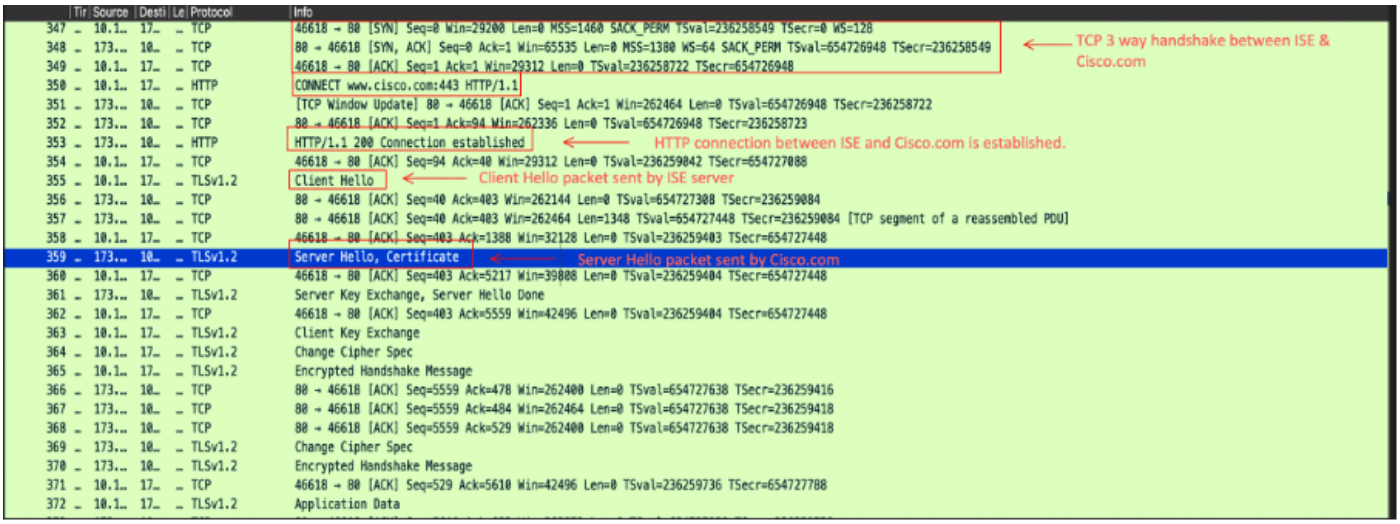
- オンラインポスチャアップデート
- オフラインでのポスチャの更新

オンラインポスチャアップデート

Web Posture Update/Online Posture Updateは、シスコのクラウドまたはサーバリポジトリから最新のポスチャアップデートを取得します。これには、シスコのサーバから最新のポリシー、定義、およびシグニチャを直接ダウンロードすることが含まれます。ISEは、最新のポスチャ定義、ポリシー、およびその他の関連ファイルを取得するために、シスコのクラウドサーバに接続するか、リポジトリを更新する必要があります。

Webまたはオンラインポスチャアップデート中に発生すること

Identity Services Engine(ISE)は、プロキシまたはHTTPを使用した直接インターネット接続を介してシスコのWebサイトにアクセスし、www.cisco.comとの接続を確立します。このプロセスの間に、client helloおよびserver helloの交換が行われ、サーバはその証明書を提供して自身の正当性を検証し、クライアント側の信頼を確認します。client helloとserver helloが完了した後、クライアントキー交換が行われ、サーバがポスチャのアップデートを開始します。次のパケットキャプチャは、オンラインポスチャ更新中のISEサーバとCisco.com間の通信を示しています。



- Server Helloの実行中、Cisco.comはクライアント側の信頼を確認するためにこれらの証明書をクライアントに送信します。

<#root>

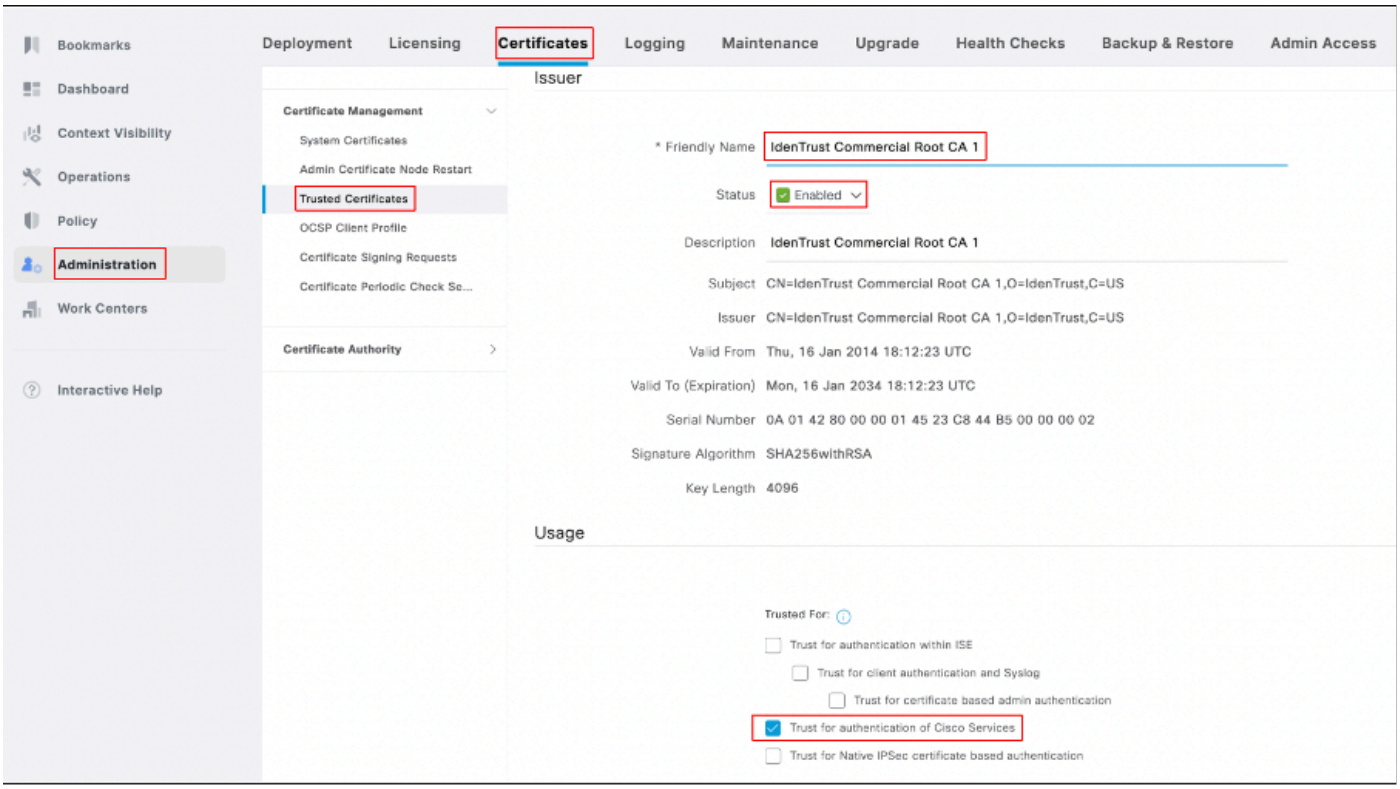
```
Certificates Length: 5083
Certificates (5083 bytes)
Certificate Length: 1940
Certificate: 3082079030820678a003020102021040191d1f3c7ec4ea73b301be3e06a90300d06092a… (id-at-commonNam
Certificate Length: 1754
Certificate: 308206d6308204bea003020102021040016efb0a205cfaebe18f71d73abb78300d06092a… (id-at-commonNam
Certificate Length: 1380
Certificate: 3082056030820348a003020102021040142800000014523c844b500000002300d06092a… (id-at-commonNam
```

IdenTrust Commercial Root CA

1

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

- ISE GUIでは、Cisco.comとの接続を確立するために、サーバ証明書Identrust Commercial Root CA 1が有効になっており、シスコサービスの認証が信頼できることを確認することが重要です。デフォルトでは、この証明書はISEに含まれており、「Trust for authenticating Cisco services」にチェックマークが付いていますが、検証が推奨されます。
- ISE GUI > Administration > Certificates > Trusted Certificatesの順に選択して、証明書のステータスと信頼できる使用方法を確認します。次のスクリーンショットに示すように、名前Identrust Commercial Root CA 1でフィルタリングし、証明書を選択し、証明書を編集して信頼度の使用状況を確認します。



- ポスチャ更新には、ポスチャポリシーの新規または改訂、新しいウイルス対策/マルウェア対策定義、ポスチャ評価に関するその他のセキュリティ関連基準が含まれます。
- この方法にはアクティブなインターネット接続が必要で、通常は、ポスチャ更新にクラウドベースのリポジトリを使用するようにISEシステムを設定するときに実行されます。

使用するケース

オンラインポスチャアップデートは、ポスチャポリシー、セキュリティ定義、および基準を、シスコが提供する最新バージョンで確実に最新にするのに使用されます。

オンラインポスチャ更新に使用されるポート

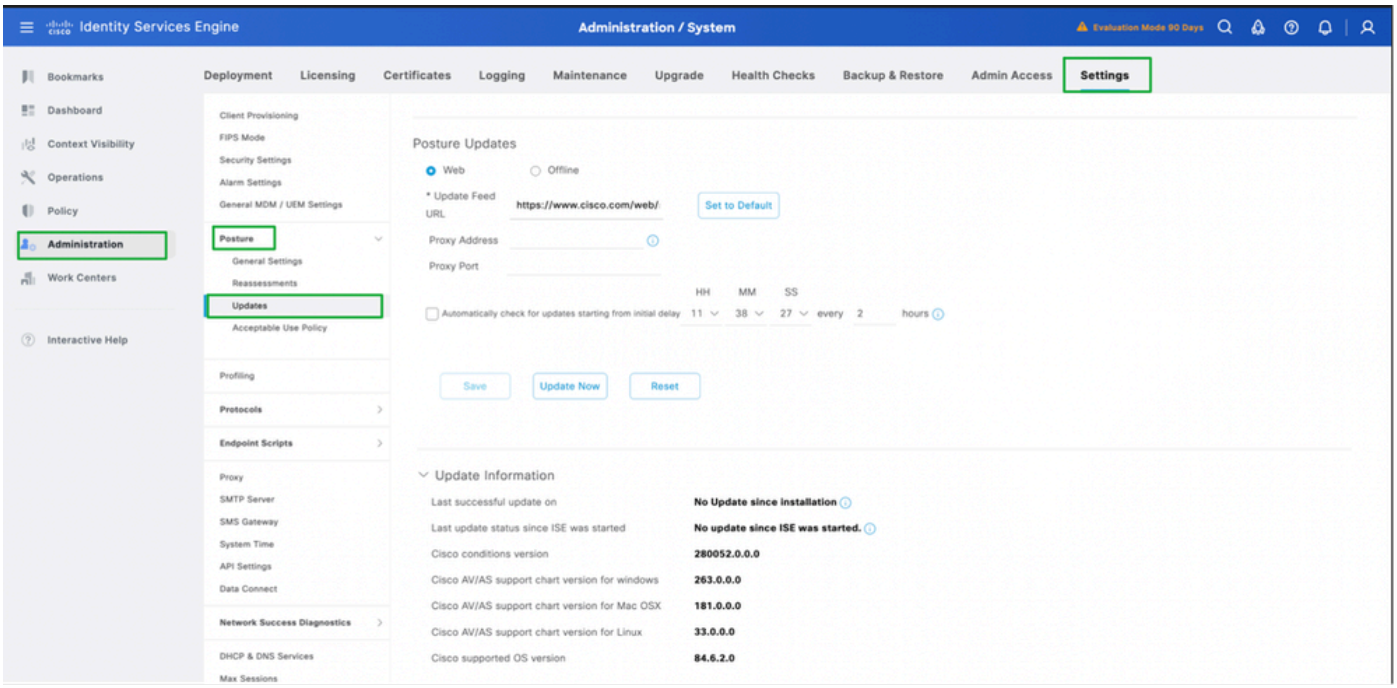
ISEシステムが正常にシスコのクラウドサーバに到達してポスチャアップデートをダウンロードできるようにするには、ファイアウォールで次のポートを開き、ISEからインターネットへのアウトバウンド通信を許可する必要があります。

1. HTTPS(TCP 443):
   - ISEがシスコのクラウドサーバに到達し、セキュアな接続(TLS/SSL)経由でアップデートをダウンロードするためのプライマリポート。
   - これは、Webベースのポスチャ更新プロセスで最も重要なポートです。
2. DNS(UDP 53):
   - ISEは、DNSルックアップを実行して、アップデートサーバのホスト名を解決できる必要があります。
   - ISEシステムがDNSサーバに到達してドメイン名を解決できることを確認します。
3. NTP(UDP 123):
   - ISEは時刻の同期にNTPを使用します。これは、更新プロセスが正しくタイムスタンプされ、ISEシステムが同期されたタイムゾーンで動作することを確認するために重

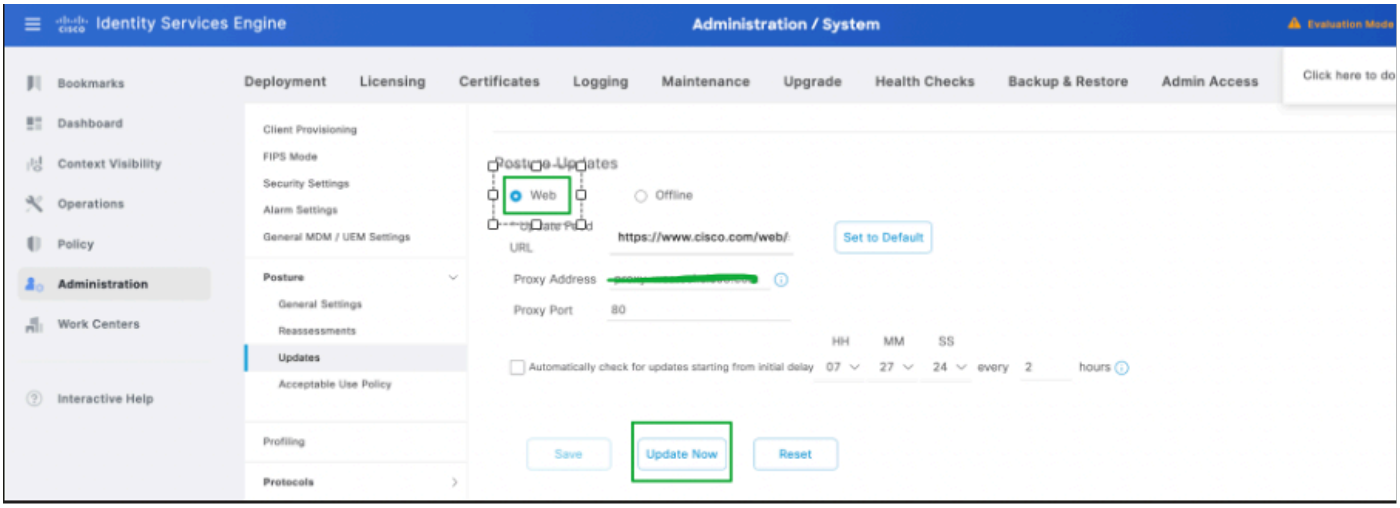
要です。
- 多くの場合、NTPサーバもUDP 123経由でアクセスできる必要があります。

オンラインポスチャ更新を実行する手順

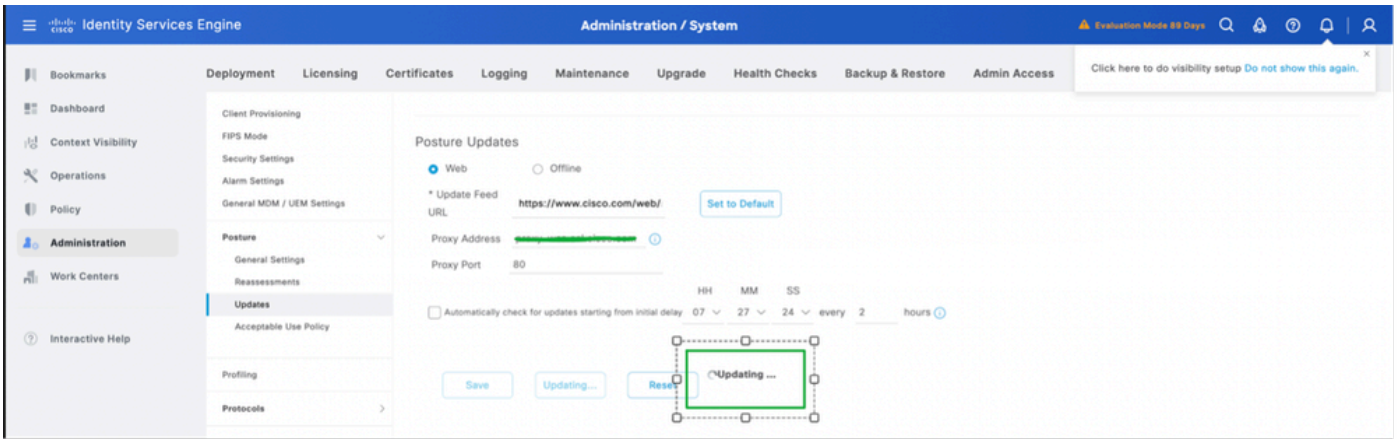
1. GUI -> Administration -> System -> Settings -> Posture -> Updatesの順に選択してログインします。



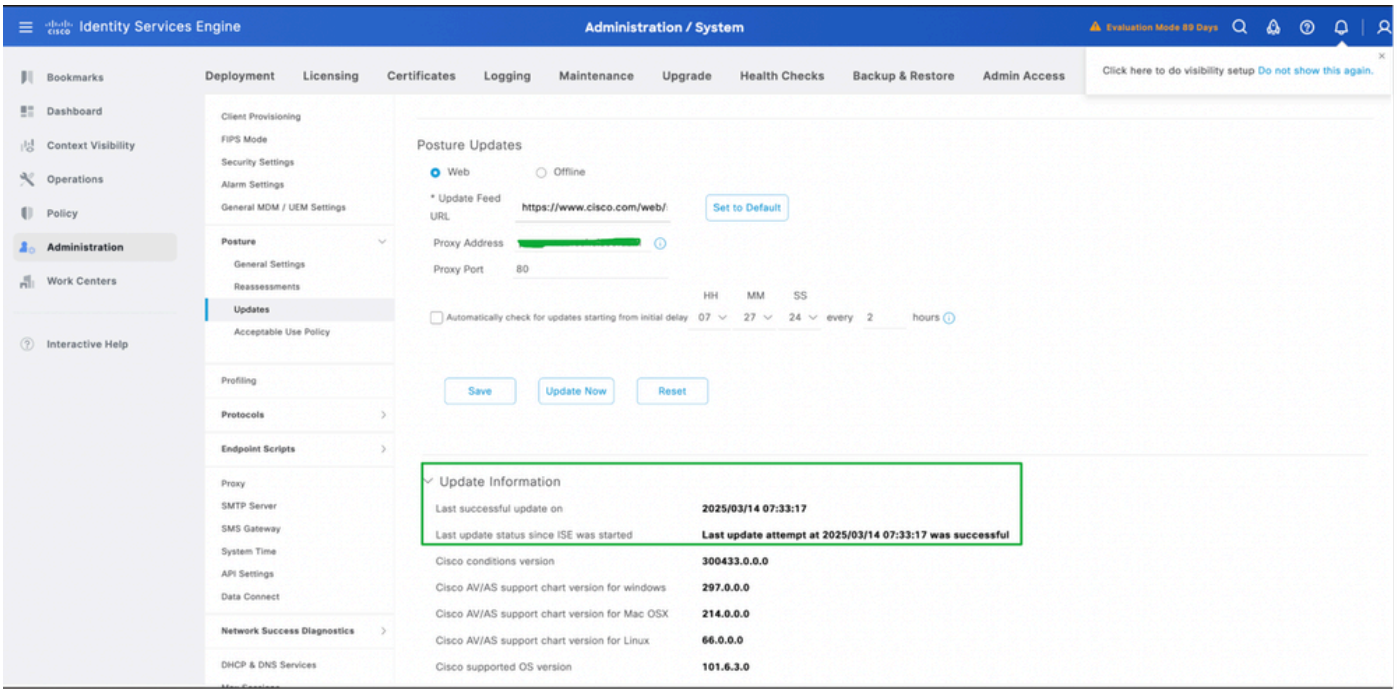
2. 方法としてWeb for Online Posture Updatesを選択し、Update Nowをクリックします。



3. ポスチャの更新が開始されると、ステータスはUpdatingに変更されます。



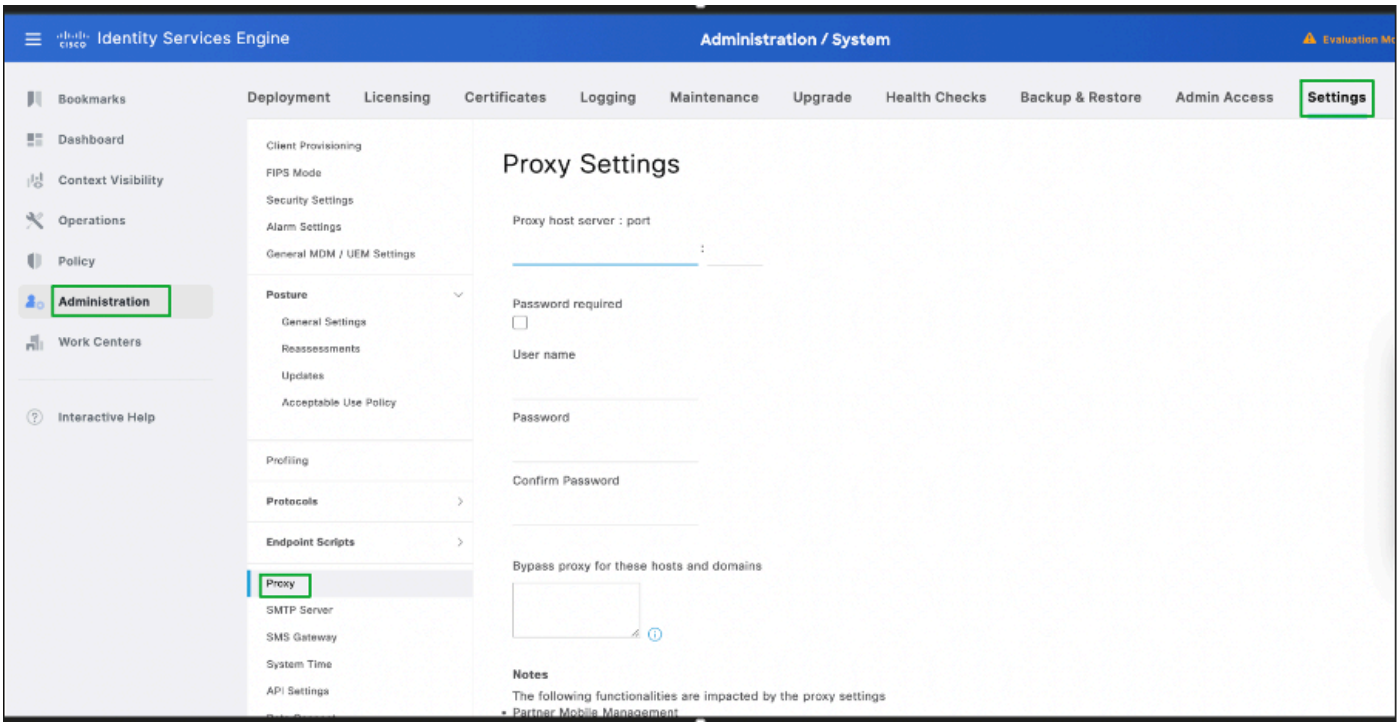
4. ポスチャ更新のステータスは、次のスクリーンショットに示すように、更新情報で確認できます。



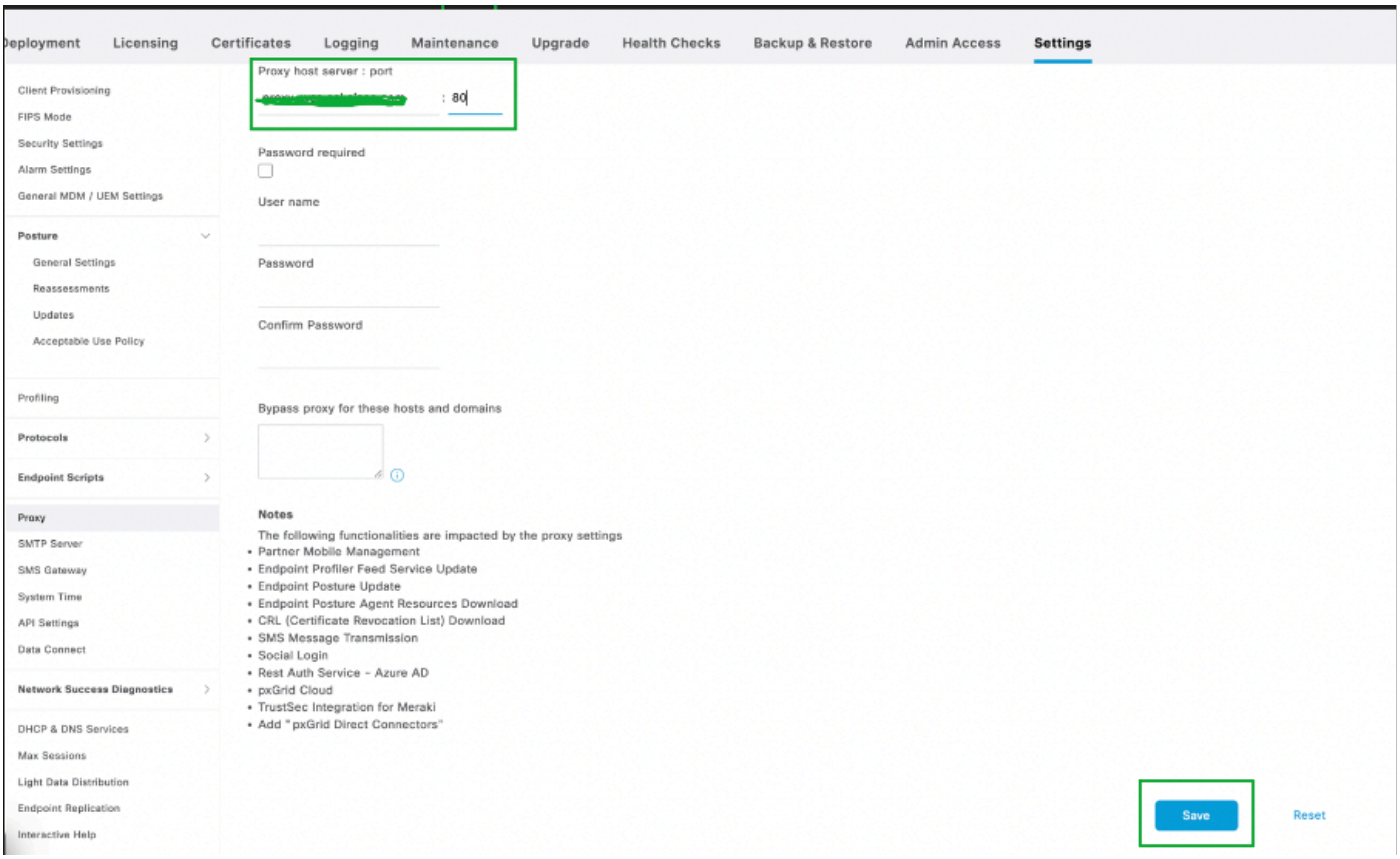
オンラインポスチャ更新のためのプロキシ設定

Posture UpdateフィールドのURLにアクセスできない制限された環境では、プロキシ設定が必要です。ISEでのプロキシの設定を参照してください。

1. Administration -> System -> Settings -> Proxyの順に移動します。



2. プロキシの詳細を設定し、Saveをクリックします。



3. オンラインポスチャ更新が実行されると、プロキシの詳細がISEによって自動的にフェッチされます。

オフラインでのポスチャ更新

オフラインポスチャ更新を使用すると、（.zipまたは他のサポートされているファイル形式の）ポスチャ更新ファイルをISEに手動でアップロードできます。

オフラインポスチャ更新を実行するとどうなりますか。

- 更新されたポスチャファイルを手動でアップロードします。
- ISEはこれらのファイルを処理して適用します。これには、更新されたポリシー、ウイルス対策定義、ポスチャアセスメントなどのファイルが含まれます。
- オフラインアップデートは、インターネット接続を必要とせず、通常は、外部サーバへの直接アクセスを妨げる厳格なセキュリティポリシーまたはネットワークポリシーが設定された環境で使用されます。

使用するケース

この方法は、システムがインターネットから隔離されている環境や、シスコまたはセキュリティチームから提供された特定のオフラインアップデートファイルがある場合によく使用されます。

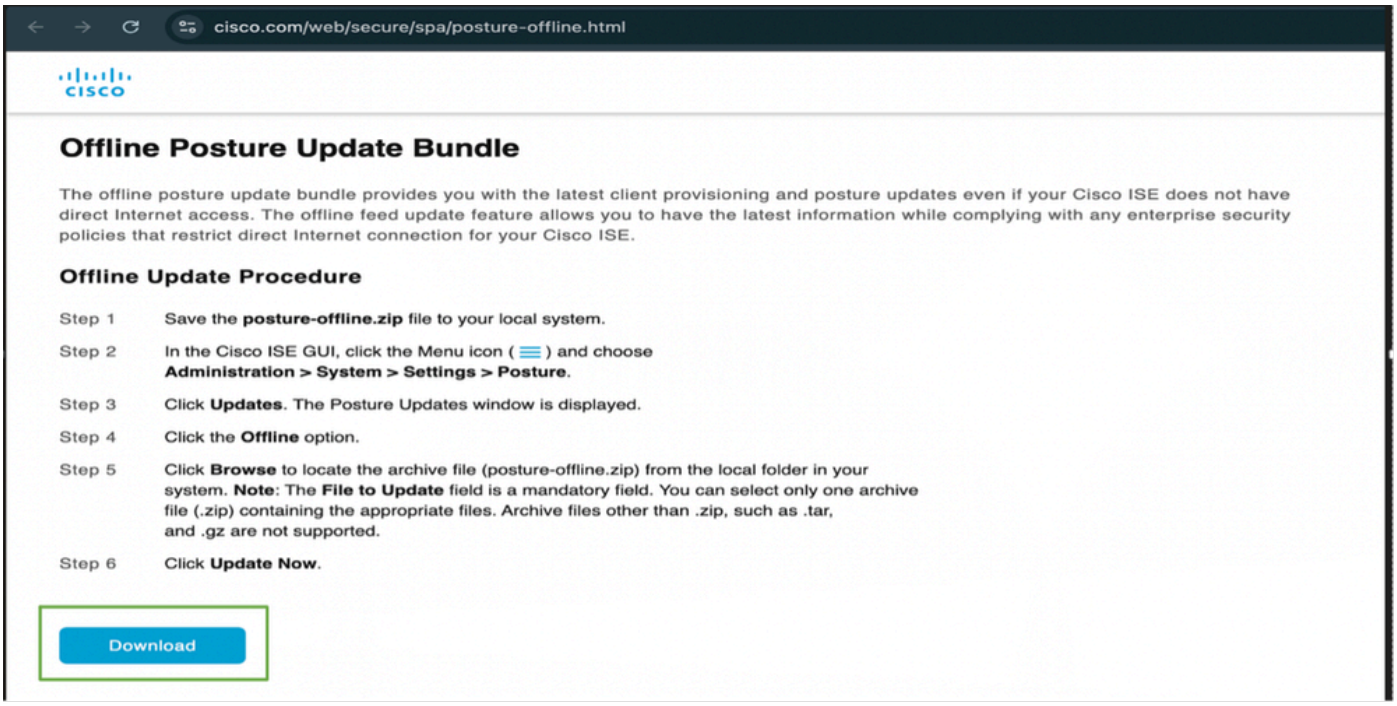
オフラインポスチャ更新に使用されるポート

ISEサーバとの（更新プロセス中の）一般的な通信では、多くの場合、次のポートが関連します。

1. 管理アクセス（ポート22、443）:
   - SSH(TCP 22):SSHを使用して、トラブルシューティングまたは手動アップロードのためにISEシステムにアクセスしている場合。
   - HTTPS(TCP 443)：更新のアップロードにGUI（Webインターフェイス）を使用している場合。
2. ファイル転送（SFTPまたはSCP）:
   - SFTPまたはSCP経由でISEにファイルを手動でアップロードする必要がある場合は、対応するポート（通常はSSH/SFTPのポート22）がISEシステムで開いていることを確認します。
3. ローカルネットワークアクセス:
   - 更新のアップロード元のシステム（たとえば、管理ワークステーションまたはサーバ）が、管理アクセスに必要なポートを介してISEと通信できることを確認します。ただし、オフラインポスチャ更新ではファイルが手動で提供されるため、外部ポートは必要ありません。

オフラインポスチャ更新のファイルの場所

1. URL(https://www.cisco.com/web/secure/spa/posture-offline.html)に移動し、Downloadをクリックします。これにより、ローカルシステムにposture-offline.zipファイルがダウンロードされます。

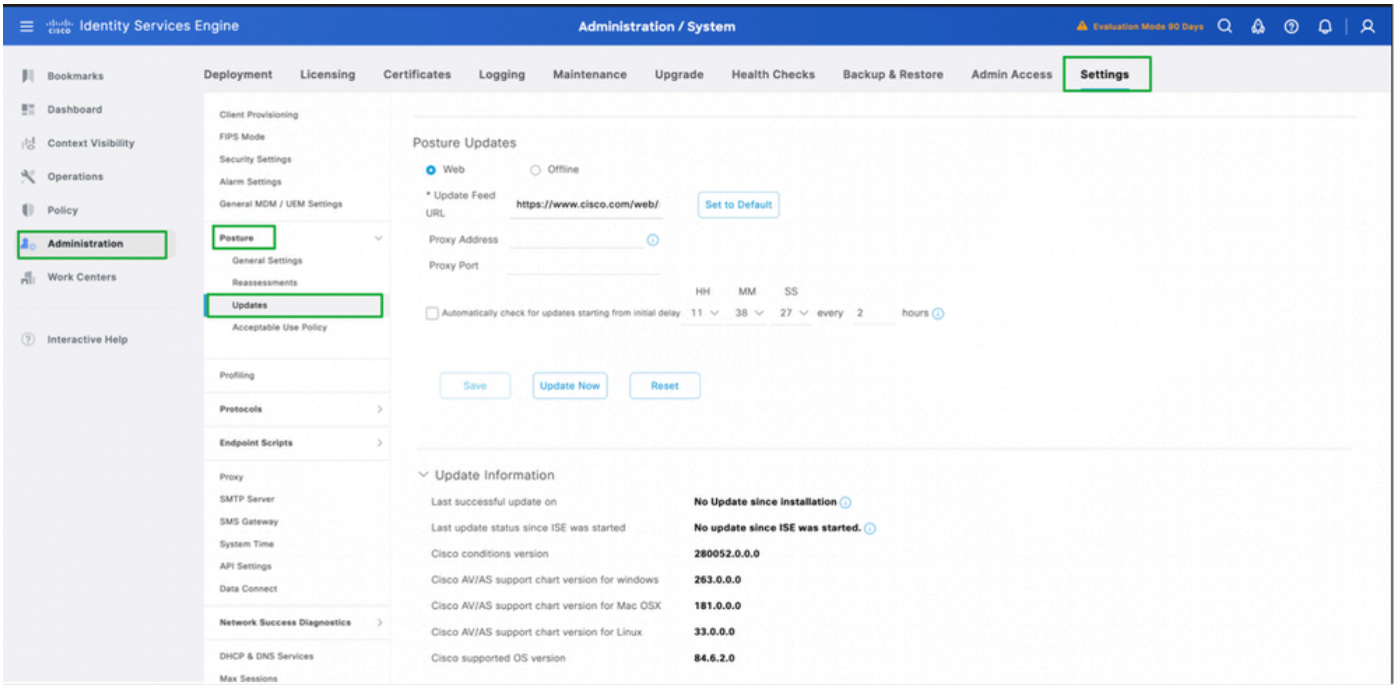


オフラインのポスチャ更新ファイルの内容

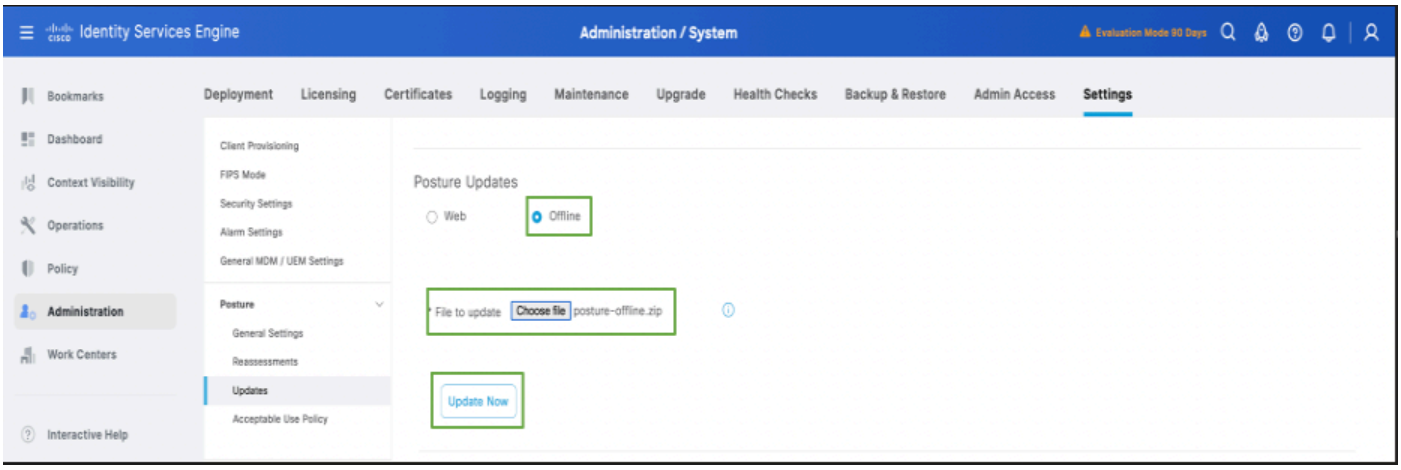
- ウイルス対策の定義（シグニチャ）。
- ポスチャポリシーおよびルール。
- ポスチャ評価用のセキュリティアセスメントおよびその他のコンフィギュレーションファイル。

オフラインでポスチャ更新を実行する手順

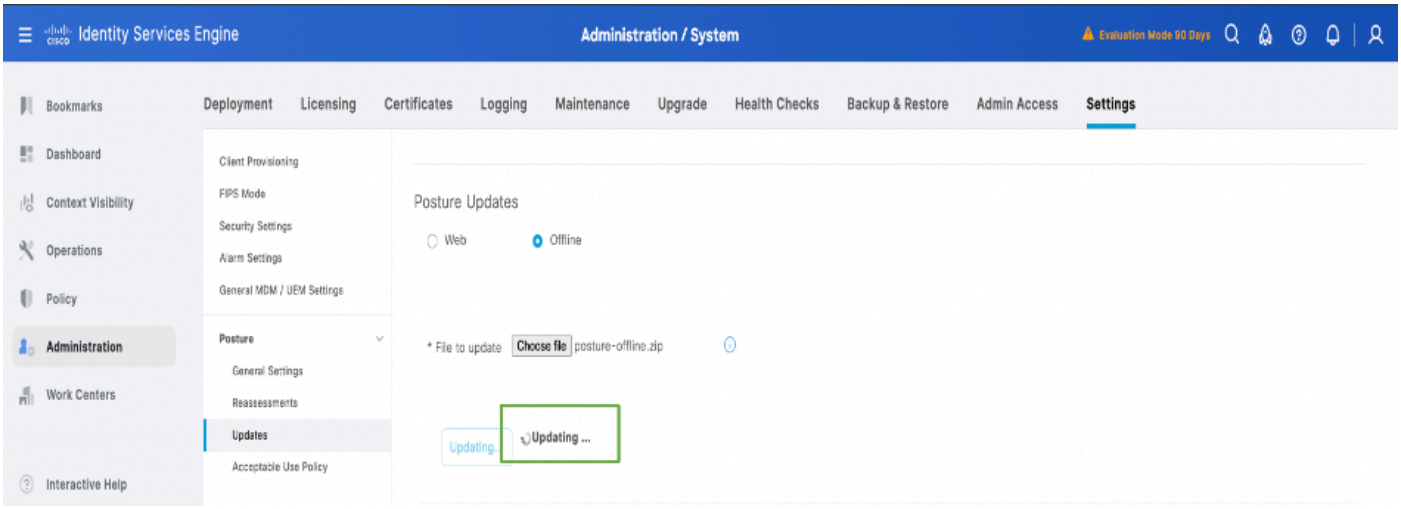
1. ISE GUI -> Administration -> System -> Settings -> Posture -> Updatesの順に選択してログインします。

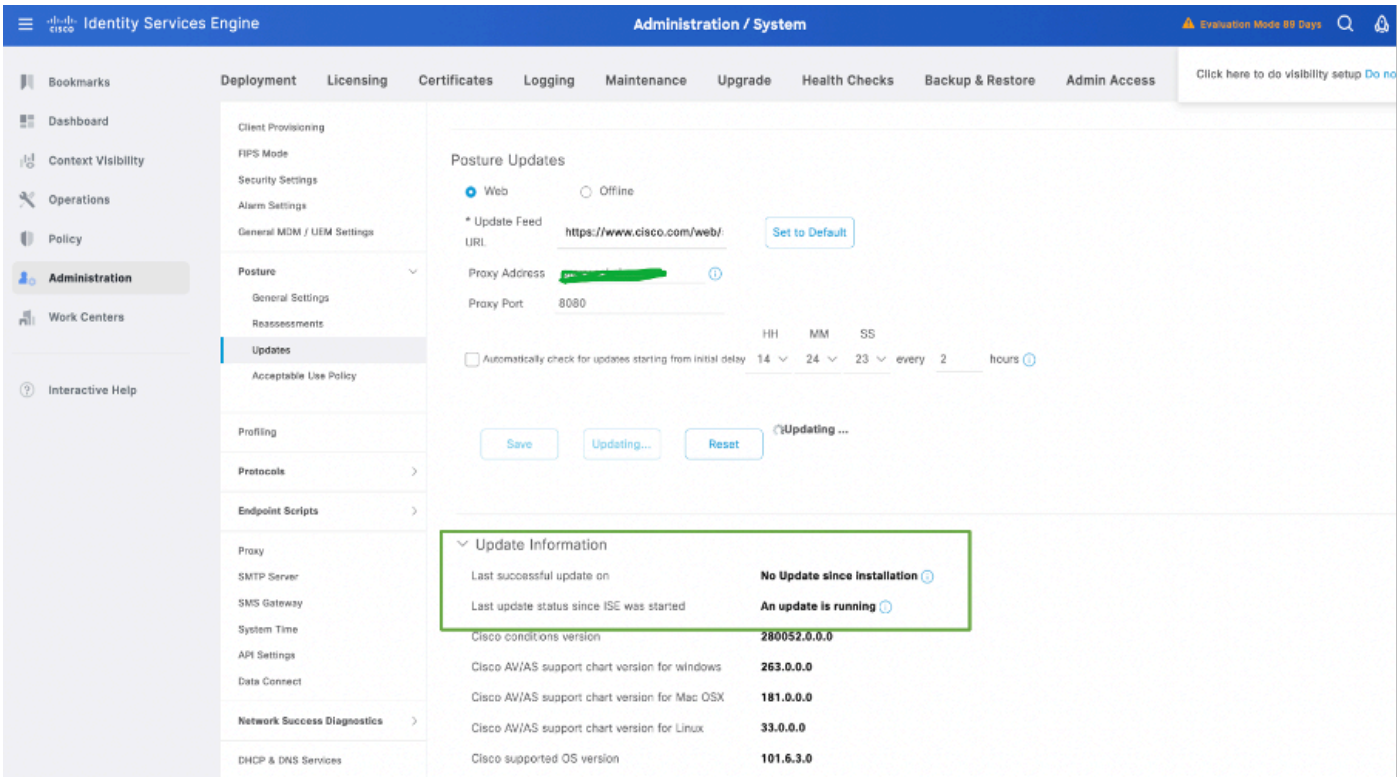


2. offlineオプションを選択し、ローカルシステムにダウンロードされたposture-offline.zipフォルダをブラウズして選択します。Update Nowをクリックします。

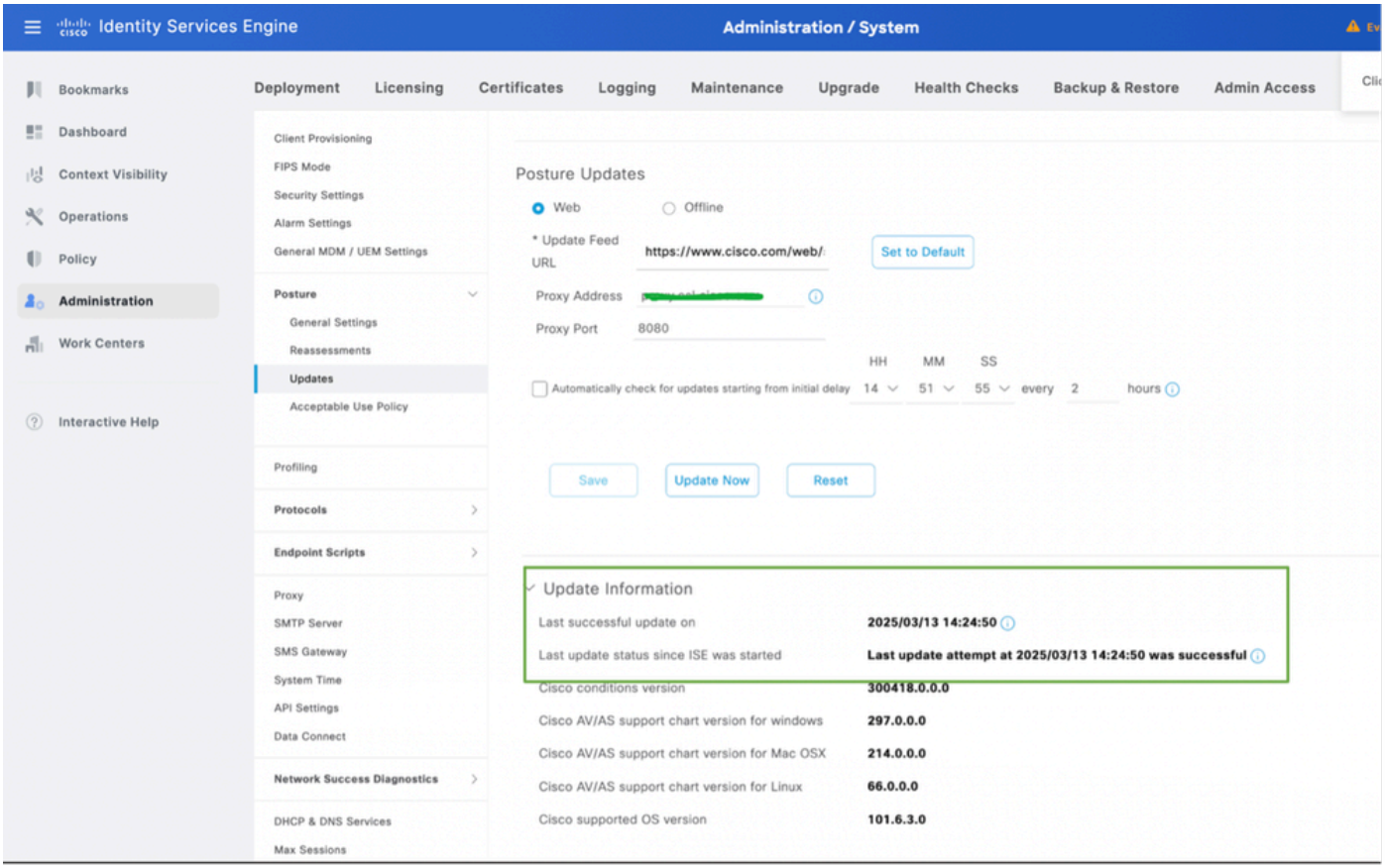


3. ポスチャの更新が開始されると、ステータスはUpdatingに変更されます。





4. ポスチャ更新のステータスは、次のスクリーンショットに示すように、更新情報で確認できます。



検証

Primary Adminノード – > Operations -> Troubleshooting -> Download Logs -> Debug logs -> Application logs -> isc-psc.logのGUIにログインし、ise-psc.logをクリックすると、ローカルシステムにログがダウンロードされます。メモ帳またはテキストエディタでダウンロードしたファイルを開き、Opswat downloadでフィルタリングします。展開で実行されているポスチャ更新に関連する情報を見つける必要があります。

show logging application ise-psc.log tailコマンドを使用してプライマリ管理ノードのCLIにロギングすることで、ログを追跡することもできます。

ポスチャ更新を参照するOpswatのダウンロードが開始されます。

2025-03-13 13:58:07,246 INFO [admin-http-pool5][[]]
cisco.cpm.posture.download.DownloadManager -::admin::- opswatのダウンロードを開始

2025-03-13 13:58:07,251 INFO [admin-http-pool5][]
cisco.cpm.posture.download.DownloadManager -::admin:: – オフラインダウンロードファイル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:: – オフラインダウンロードファイルURI : /opt/CSCOcpm/temp/cp/update/5c064701-a1ee-4a09-a190-3bf83c190af6/osgroups.tar.gz

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

Opswatのダウンロードが完了しました。ポスチャ更新がダウンロードされ、正常に実行されたことを示しています。

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

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

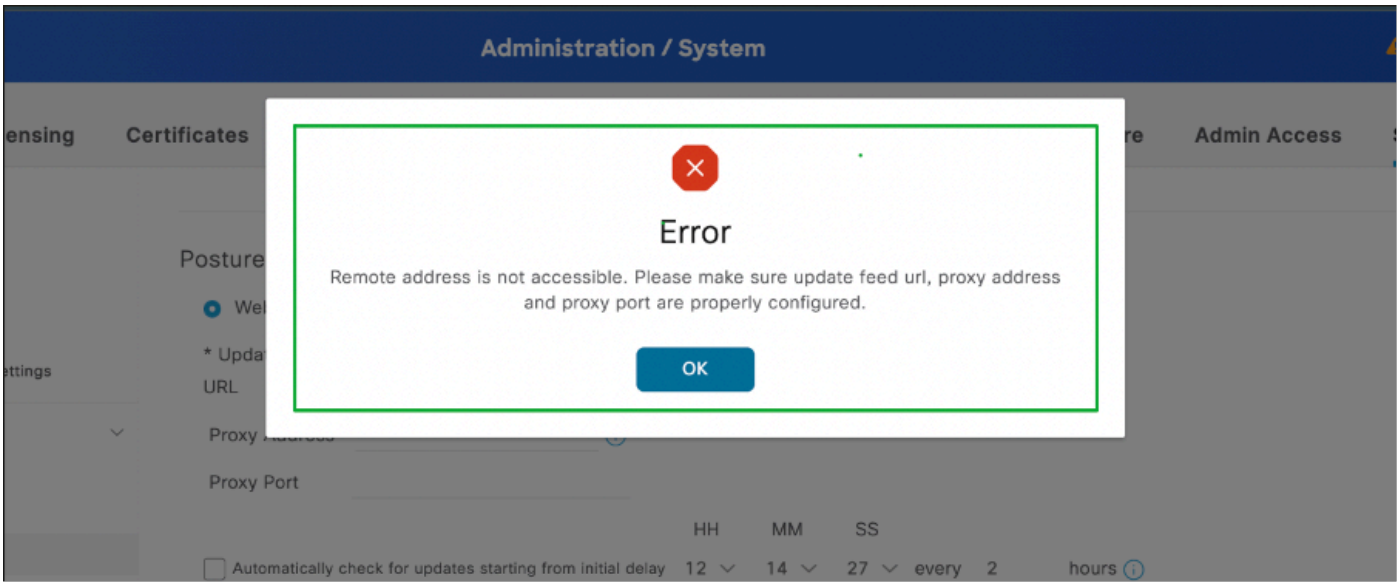
2025-03-13 14:24:50,827 INFO [admin-http-pool5][[]
mnt.dbms.datadirect.impl.DatadirectServiceImpl -::admin::- getStatusの実行 – datadirectSettings

トラブルシュート

シナリオ

オンラインポスチャの更新がエラー「Remote Address is not accessible.アップデートフィードUR、プロキシアドレス、およびプロキシポートが正しく設定されていることを確認してください。

サンプルエラー：



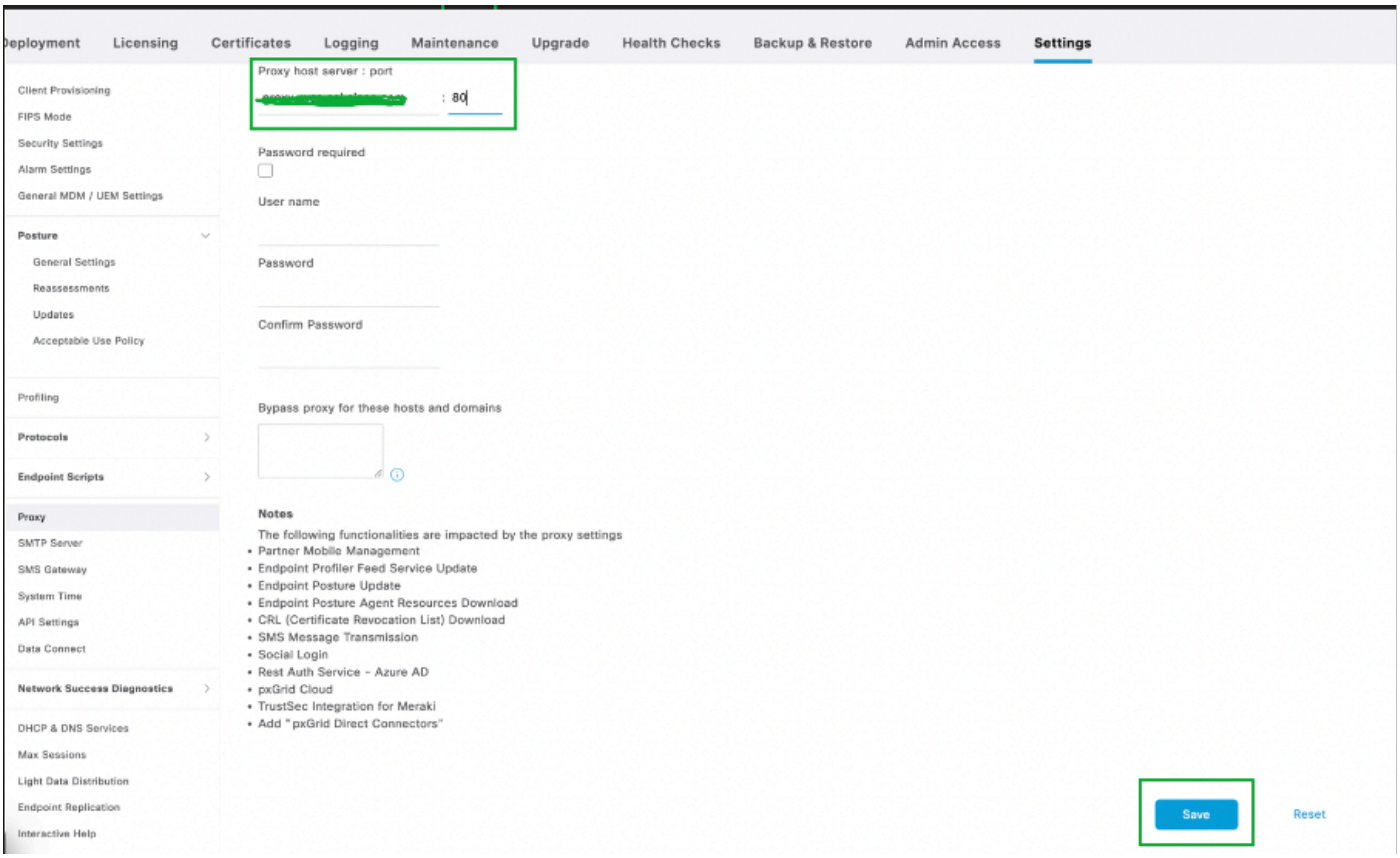
解決方法

1. ISEのCLIにログインし、コマンド「ping cisco.com」を使用して、ISEがcisco.comに到達できることを確認します。

isehostname/admin#ping cisco.com
cisco.com (72.163.4.161) 56(84)バイトのデータに対してPINGを実行します。
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パケット送信、4受信、0 %パケット損失、時間3004ミリ秒
rtt最小/平均/最大/デバイス= 238.180/238.424/238.766/0.410ミリ秒

2. Administration -> System -> Settings -> Proxy is configured with proper portsの順に移動します。



3. インターネットへのすべてのホップでポートTCP 443、UDP 53、およびUDP 123が許可されているかどうかを確認します。

ポスチャ更新の問題の既知の不具合

Cisco Bug ID 01523

参考

- Cisco Identity Services Engine 管理者ガイド リリース 3.3

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。