

Execute atualizações de postura no ISE offline e online

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Atualizações de postura online](#)

[O que acontece durante as atualizações de postura on-line ou na Web?](#)

[Quando usar](#)

[Portas usadas para atualização de postura online](#)

[Procedimento para executar atualizações de postura online](#)

[Configuração de Proxy para Atualizações de Postura Online](#)

[Atualizações de postura offline](#)

[O que acontece quando você faz uma atualização de postura off-line?](#)

[Quando usar](#)

[Portas usadas para atualizações de postura offline](#)

[Onde encontrar arquivos para atualizações de postura offline?](#)

[Arquivos de Atualização de Postura Offline Incluem](#)

[Procedimento para executar atualizações de postura offline](#)

[Verificação](#)

[Troubleshooting](#)

[Cenário](#)

[Solução](#)

[Defeitos conhecidos para problemas de atualização de postura](#)

[Referência](#)

Introdução

Este documento descreve como executar atualizações de postura no Cisco Identity Services Engine® (ISE).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento sobre o fluxo de postura.

Componentes Utilizados

As informações neste documento são baseadas nas seguintes versões de hardware e software.

- Cisco Identity Services Engine 3.2 e versões posteriores.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

As atualizações de postura incluem um conjunto de verificações predefinidas, regras e gráficos de suporte para antivírus e antispymware em sistemas operacionais Windows e MacOS, além de informações sobre sistemas operacionais compatíveis com a Cisco.

Quando você implanta o Cisco ISE na rede pela primeira vez, é possível baixar atualizações de postura da Web. Esse processo geralmente leva aproximadamente 20 minutos. Após o download inicial, você pode configurar o Cisco ISE para verificar e baixar atualizações incrementais automaticamente.

O Cisco ISE cria políticas de postura padrão, requisitos e remediação apenas uma vez durante atualizações de postura iniciais. Se você excluí-los, o Cisco ISE não os criará novamente durante atualizações manuais ou programadas subsequentes.

Há dois tipos de atualizações de postura que você pode executar:

- Atualizações de postura online.
- Atualizações de postura offline.

Atualizações de postura online

Uma atualização de postura da Web/ atualização de postura on-line recupera as atualizações de postura mais recentes dos repositórios de nuvem ou servidor da Cisco. Isso envolve o download das políticas, definições e assinaturas mais recentes diretamente dos servidores da Cisco. O ISE precisa se conectar aos servidores em nuvem da Cisco ou atualizar repositórios para recuperar as definições de postura, políticas e outros arquivos associados mais recentes.

O que acontece durante as atualizações de postura on-line ou na Web?

O Identity Services Engine (ISE) acessa o site da Cisco por meio de um proxy ou de uma conexão direta com a Internet usando HTTP, estabelecendo uma conexão com www.cisco.com. Durante esse processo, ocorre a troca de hello do cliente e hello do servidor, com o servidor fornecendo seu certificado para verificar sua legitimidade e confirmar a confiança do lado do cliente. Após a conclusão do hello do cliente e do hello do servidor, ocorre a troca de chaves do cliente e o servidor inicia as atualizações de postura. Esta é a captura de pacote que demonstra a

comunicação entre o servidor ISE e Cisco.com durante as atualizações de postura on-line.

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=5610 Win=42496 Len=0 TSval=236259736 TSecr=654727788
372	10.1...	17...		TLSv1.2	Application Data

- Durante o Hello do servidor, Cisco.com envia esses certificados ao cliente para confirmar a confiança do lado do cliente.

<#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

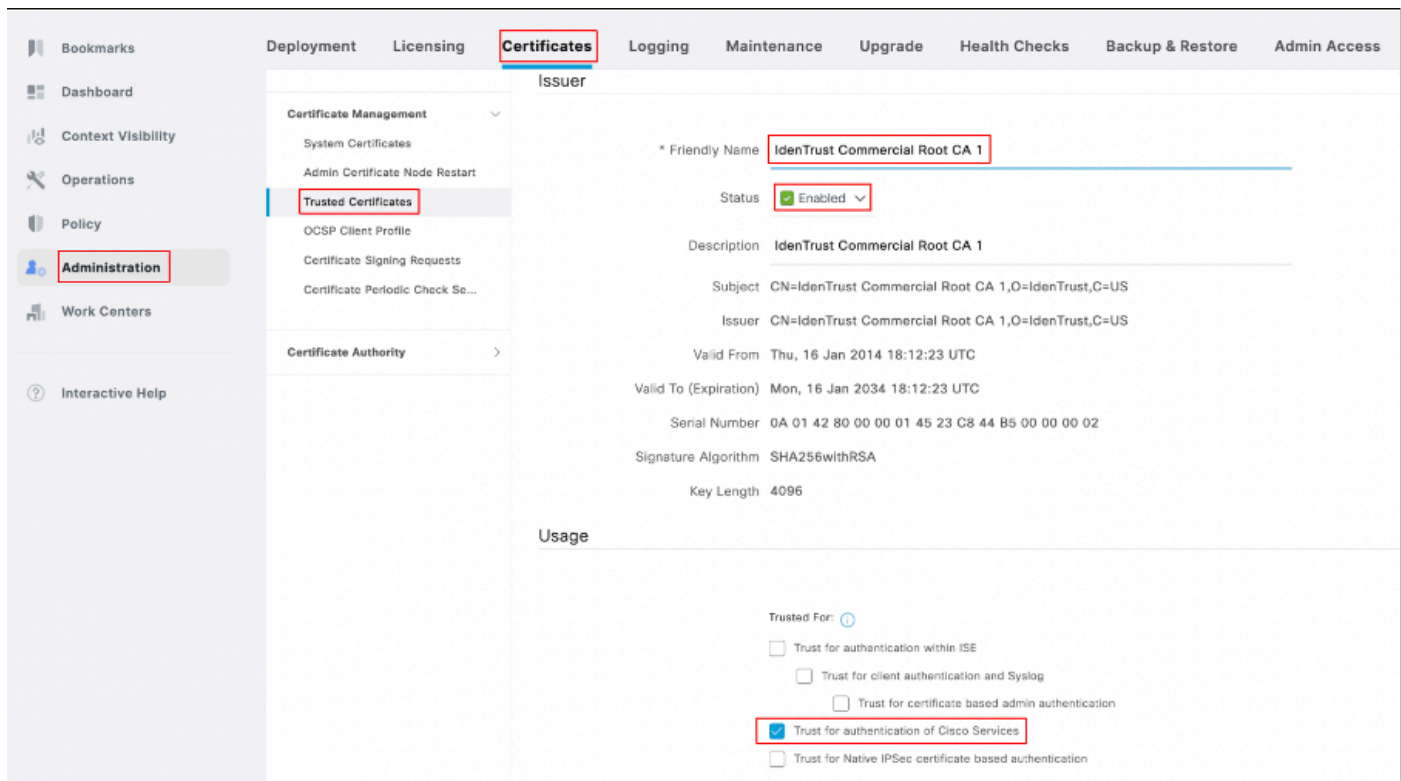
Certificate: 3082056030820348a00302010202100a0142800000014523c844b500000002300d06092a... (id-at-commonName

IdenTrust Commercial Root CA

1

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

- Na GUI do ISE, é importante garantir que o certificado do servidor IdenTrust Commercial Root CA 1 esteja habilitado e Trust para autenticar serviços Cisco para estabelecer conectividade com Cisco.com. Por padrão, esse certificado está incluído no ISE e a opção "Confiança para autenticar serviços Cisco" está marcada, mas a verificação é recomendada.
- Verifique o status do certificado e o uso confiável indo para ISE GUI > Administração > Certificados > Certificados confiáveis. Filtre pelo nome IdenTrust Commercial Root CA 1, selecione o certificado e edite-o para verificar o uso confiável, como mostrado nesta captura de tela:



- As atualizações de postura podem incluir políticas de postura novas ou revisadas, novas definições de antivírus/antimalware e outros critérios relacionados à segurança para avaliações de postura.
- Esse método requer uma conexão ativa com a Internet e geralmente é executado quando o sistema ISE está configurado para usar repositórios baseados em nuvem para atualizações de postura.

Quando usar

As atualizações de postura online são usadas quando você deseja garantir que as políticas de postura, definições de segurança e critérios estejam atualizados com as versões mais recentes disponíveis fornecidas pela Cisco.

Portas usadas para atualização de postura online

Para garantir que o sistema ISE possa acessar com êxito os servidores em nuvem da Cisco para baixar atualizações de postura, essas portas devem estar abertas no firewall e ter permissão para comunicação de saída do ISE para a Internet:

1. HTTP (TCP 443):

- Porta primária para o ISE acessar os servidores em nuvem da Cisco e baixar atualizações através de uma conexão segura (TLS/SSL).
- Essa é a porta mais crucial para o processo de atualização de postura baseado na Web.

2. DNS (UDP 53):

- O ISE deve ser capaz de executar pesquisas de DNS para resolver os nomes de host dos servidores de atualização.

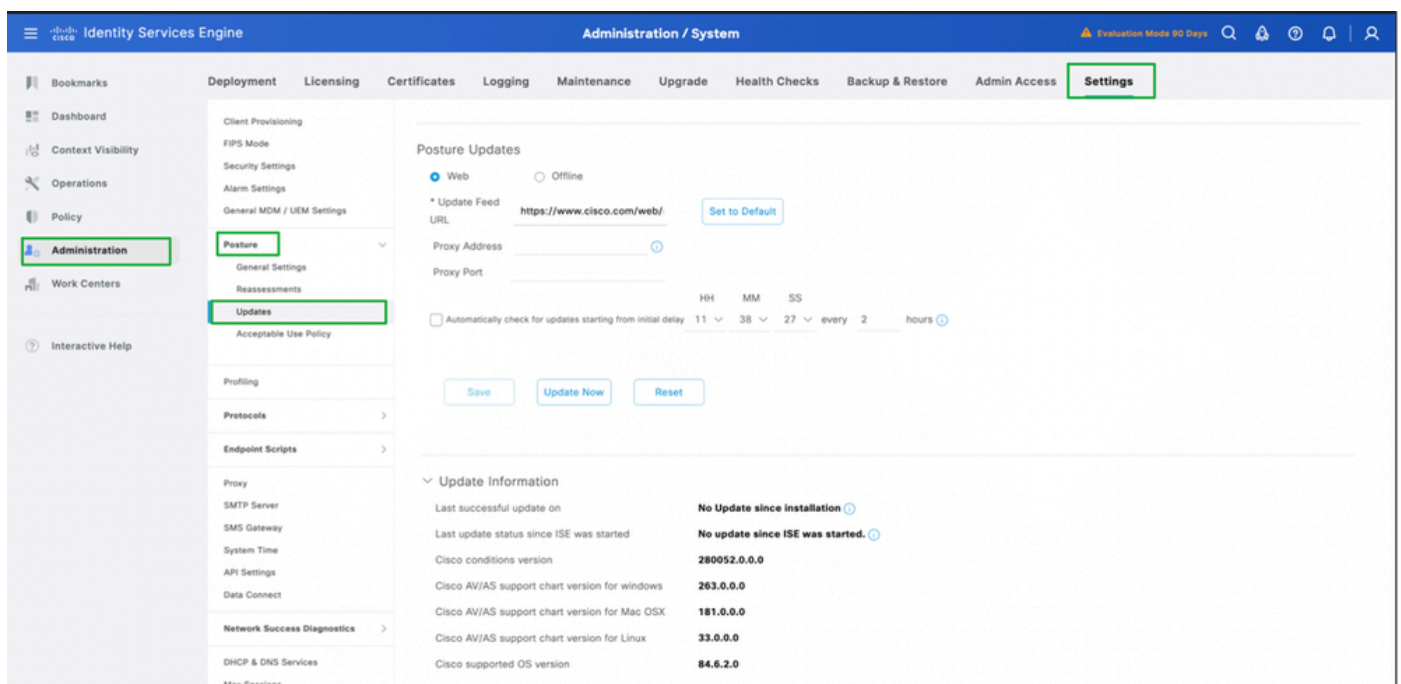
- Verifique se o sistema ISE pode acessar os servidores DNS e resolver nomes de domínio.

3. NTP (UDP 123):

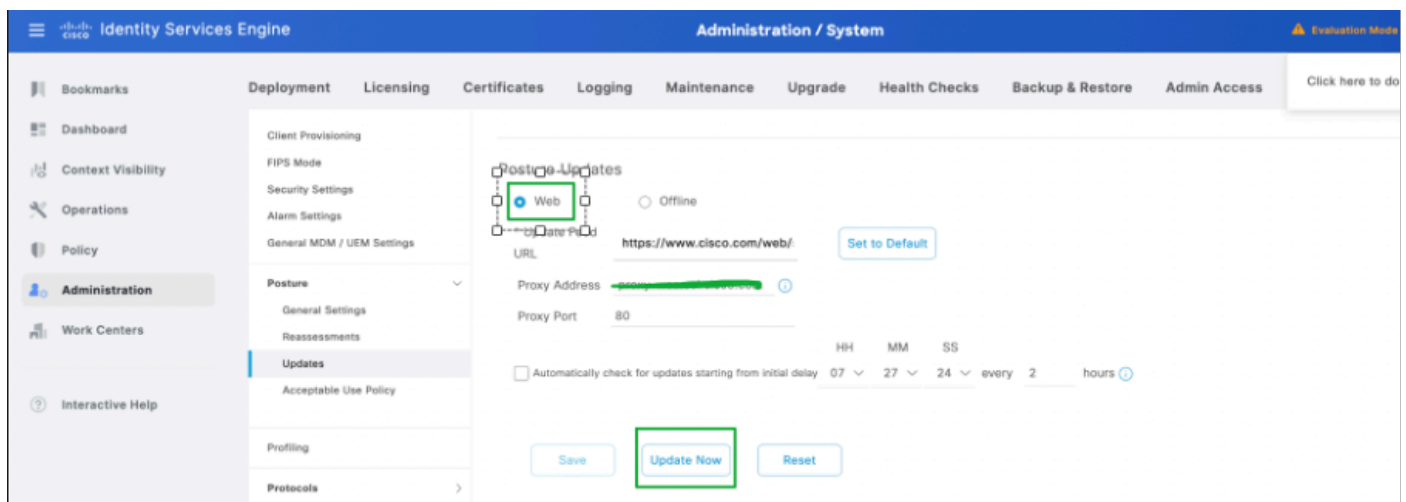
- O ISE usa NTP para sincronização de horário. Isso é importante para garantir que o processo de atualização tenha o carimbo de data e hora correto e que o sistema ISE opere em um fuso horário sincronizado.
- Em muitos casos, os servidores NTP também precisam estar acessíveis pelo UDP 123.

Procedimento para executar atualizações de postura online

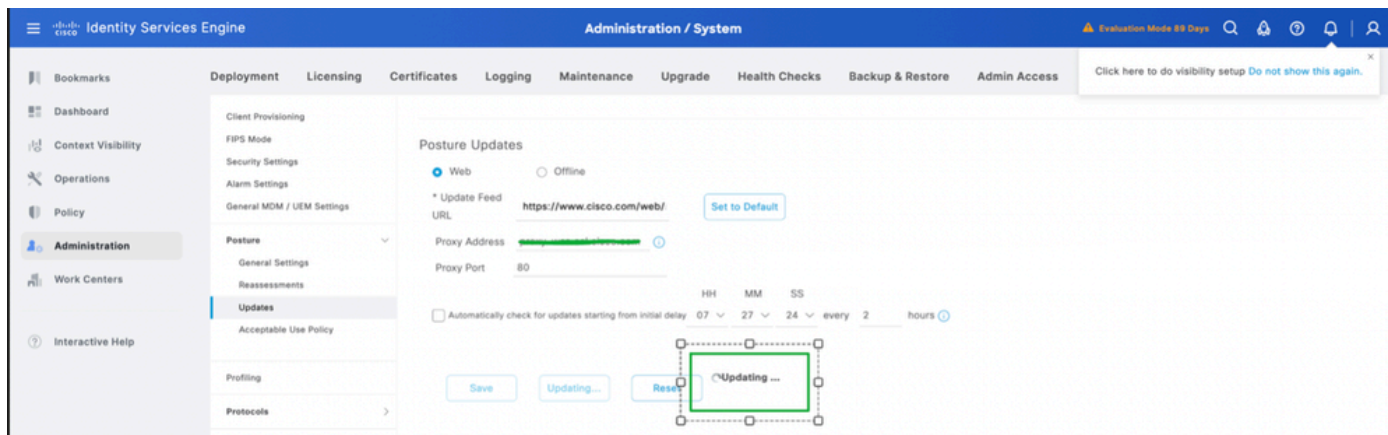
1. Faça login na GUI -> Administração -> Sistema -> Configurações -> Postura -> Atualizações.



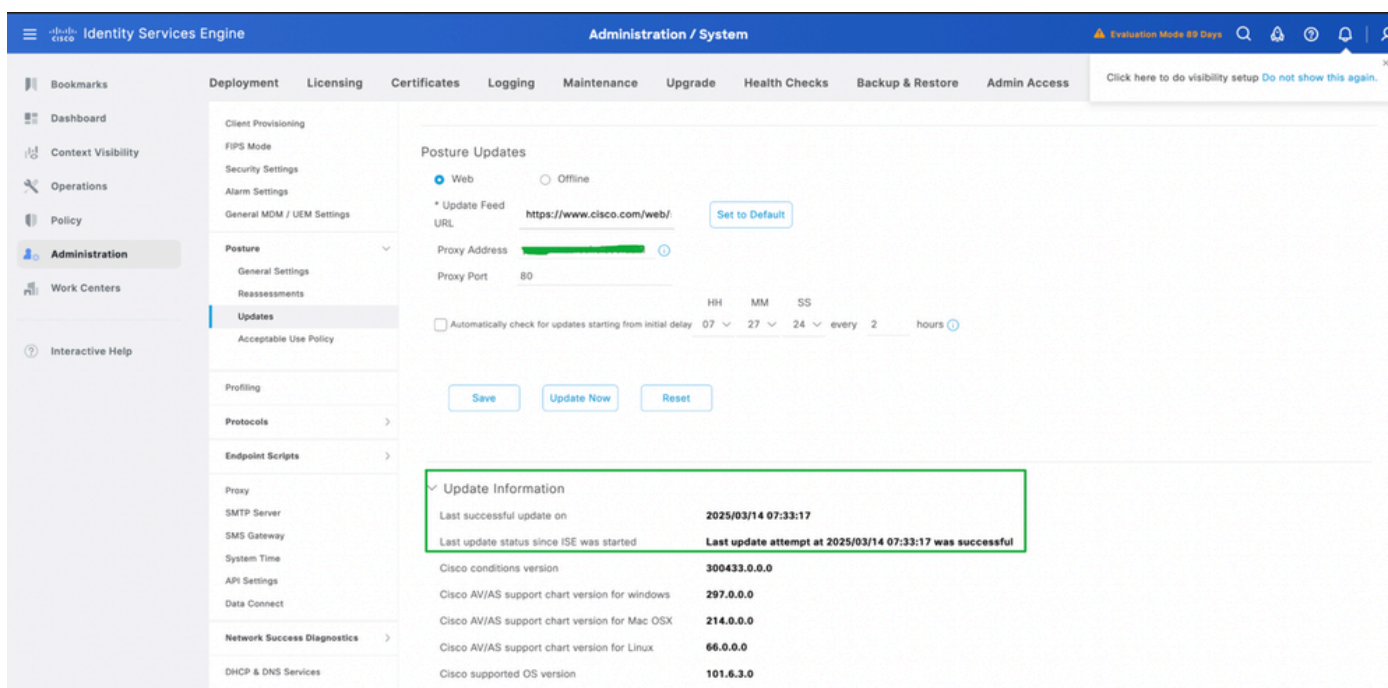
2. Selecione o método como Web para Online Posture Updates, clique em Update Now.



3. Quando as atualizações de postura começarem, o status será alterado para Atualizando.



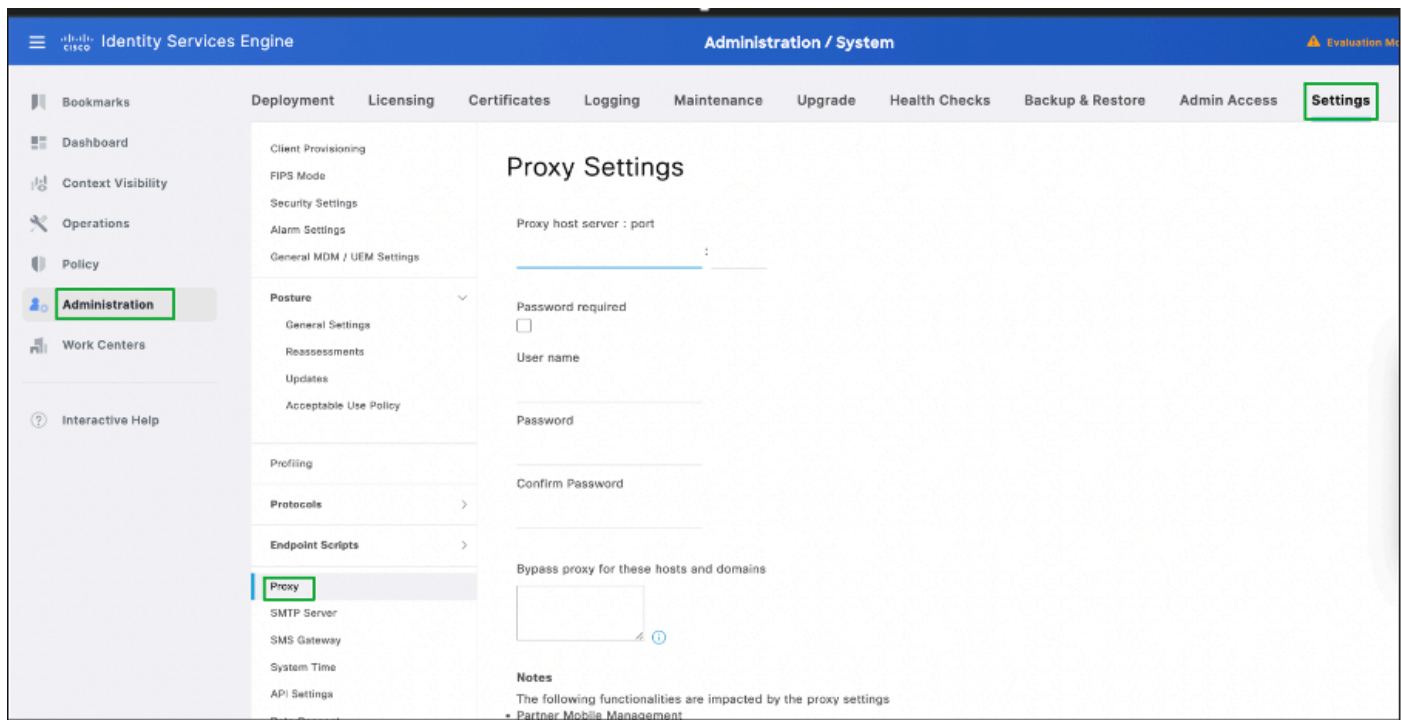
4. O status das atualizações de postura pode ser verificado a partir das Informações de atualização conforme esta captura de tela:



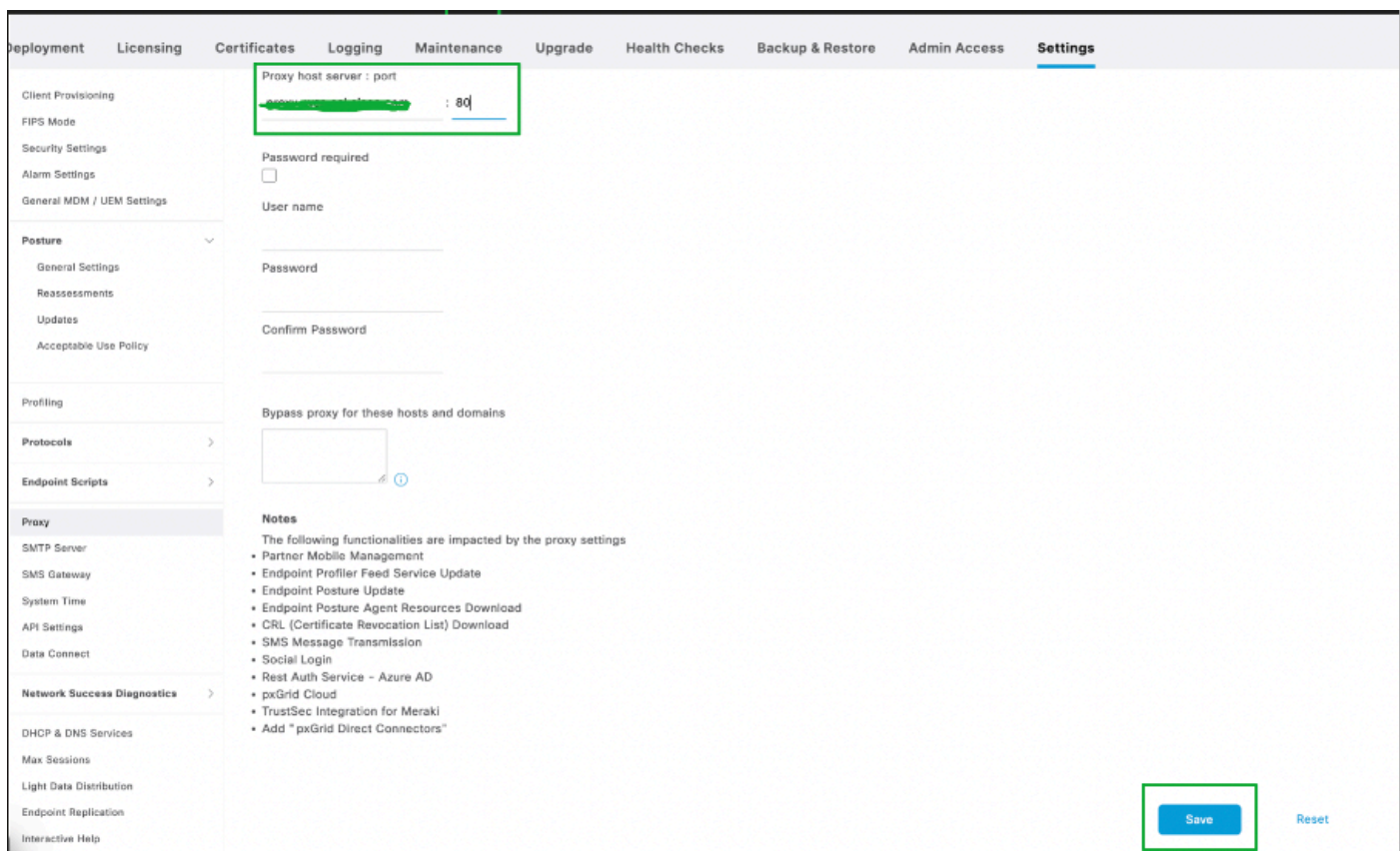
Configuração de Proxy para Atualizações de Postura Online

Em um ambiente restrito onde a URL do campo Atualização de postura não está acessível, nesse caso, a configuração de proxy é necessária. Consulte Configurar o Proxy no ISE.

1. Navegue até Administração -> Sistema -> Configurações -> Proxy.



2. Configure os detalhes do Proxy, clique em Salvar.



3. Os detalhes do proxy seriam buscados automaticamente pelo ISE quando as Atualizações de postura on-line fossem executadas.

Atualizações de postura offline

Uma Atualização de postura offline permite carregar manualmente arquivos de atualização de postura (na forma de um .zip ou outro formato de arquivo com suporte) no ISE.

O que acontece quando você faz uma atualização de postura off-line?

- Carregue os arquivos de postura atualizados manualmente.
- O ISE processa e aplica esses arquivos, que podem incluir políticas atualizadas, definições de antivírus, avaliações de postura, entre outros tipos de arquivos.
- A atualização off-line não requer conectividade com a Internet e é normalmente usada em ambientes com políticas rígidas de segurança ou de rede que impedem o acesso direto a servidores externos.

Quando usar

Esse método é frequentemente usado em ambientes onde o sistema é isolado da Internet ou quando você tem arquivos de atualização off-line específicos fornecidos pela Cisco ou pela sua equipe de segurança.

Portas usadas para atualizações de postura offline

Para a comunicação geral com o servidor ISE (durante o processo de atualização), em muitos casos, essas portas são relevantes:

1. Acesso de Gerenciamento (Portas 22, 443):
 - SSH (TCP 22): Se você estiver usando SSH para acessar o sistema ISE para solução de problemas ou carregamento manual.
 - HTTPS (TCP 443): Se você estiver usando a GUI (interface da Web) para o upload da atualização.
2. Transferência de arquivos (SFTP ou SCP):
 - Se você precisar carregar arquivos manualmente no ISE via SFTP ou SCP, verifique se as portas correspondentes (geralmente a porta 22 para SSH/SFTP) estão abertas no sistema ISE.
3. Acesso à rede local:
 - Verifique se o sistema do qual você está carregando a atualização (por exemplo, uma estação de trabalho ou servidor administrativo) pode se comunicar com o ISE pelas portas necessárias para acesso de gerenciamento, mas, novamente, as atualizações de postura offline não exigem nenhuma porta externa, pois os arquivos são fornecidos manualmente.

Onde encontrar arquivos para atualizações de postura offline?

1. Navegue até a URL: <https://www.cisco.com/web/secure/spa/posture-offline.html> , clique em Download [e o arquivo](#) posture-offline.zip [será baixado para o seu sistema 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](#)

Arquivos de Atualização de Postura Offline Incluem

- Definições de antivírus (assinaturas).
- Políticas e regras de postura.
- Avaliações de segurança e outros arquivos de configuração para avaliação de postura.

Procedimento para executar atualizações de postura offline

1. Faça login na GUI do ISE -> Administração -> Sistema -> Configurações -> Postura -> Atualizações.

Identity Services Engine Administration / System

Settings

Posture Updates

☒ Web ☐ Offline

* Update Feed URL: [Set to Default](#)

Proxy Address:

Proxy Port:

☐ Automatically check for updates starting from initial delay: HH:MM:SS 11:38:27 every 2 hours

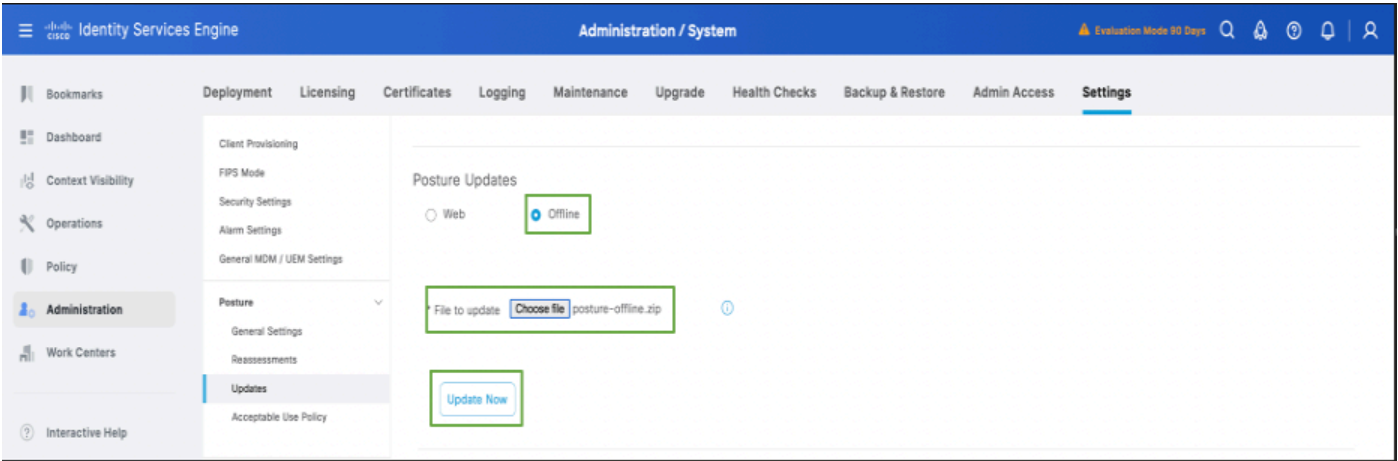
[Save](#) [Update Now](#) [Reset](#)

Update Information

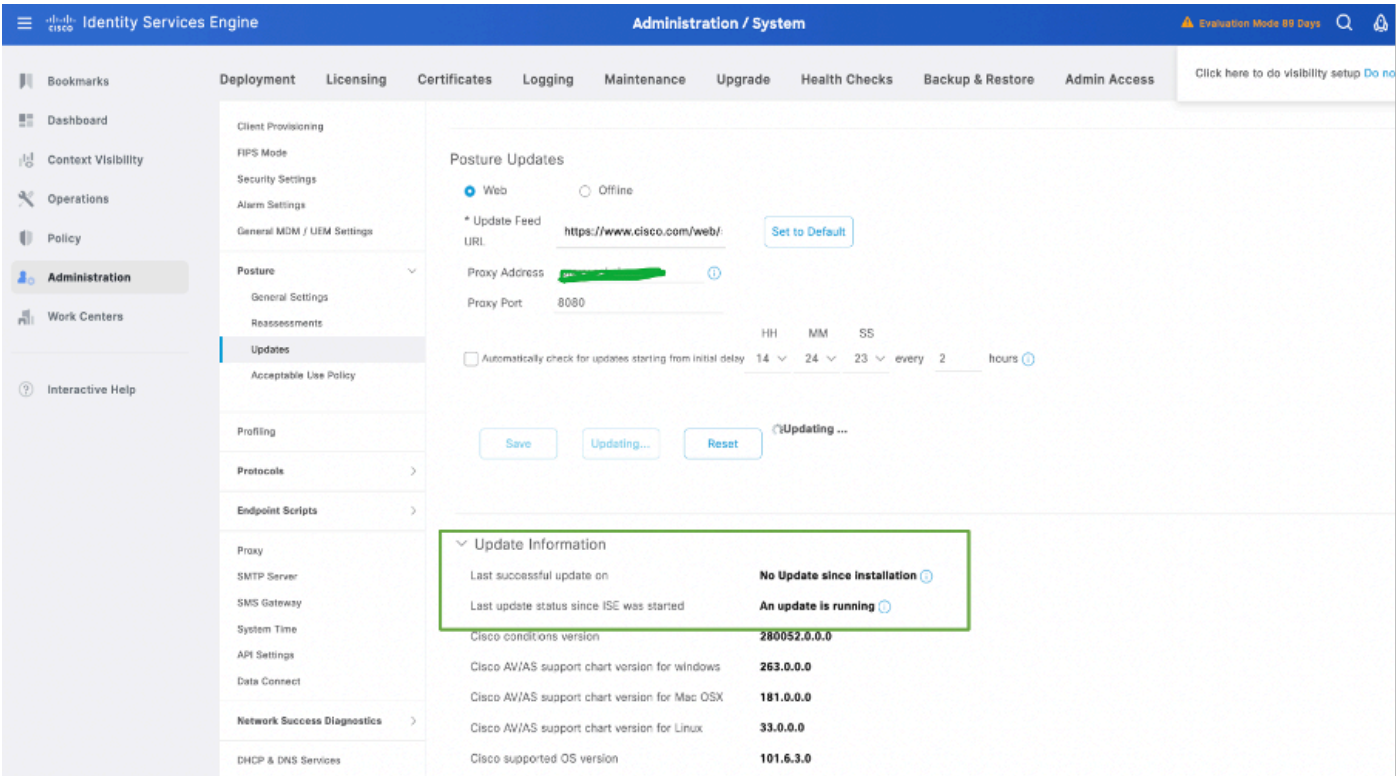
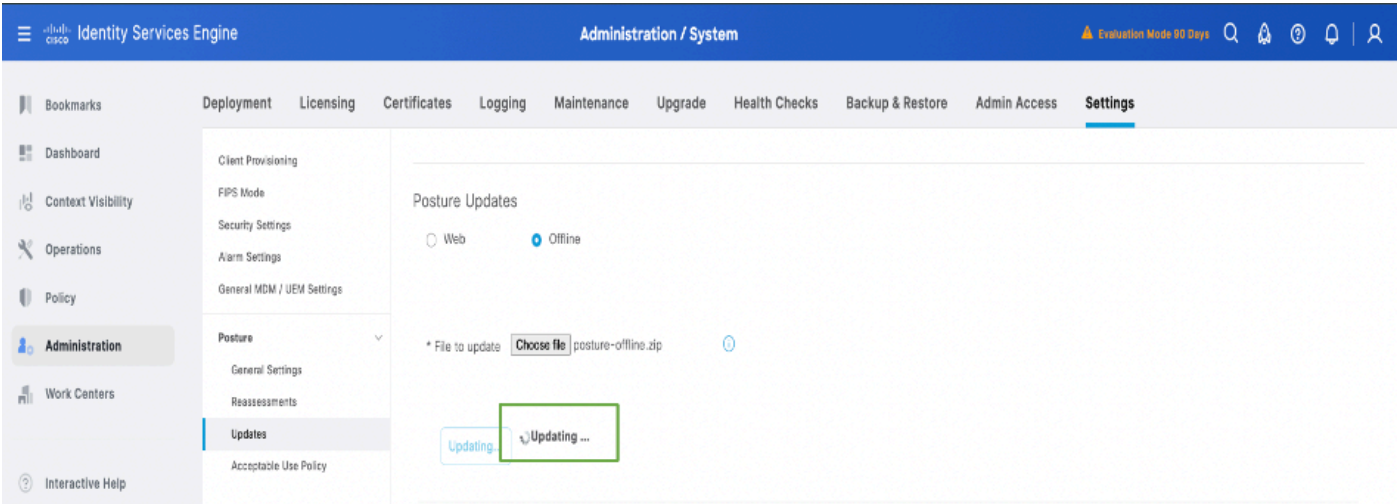
Last successful update on	No Update since installation
Last update status since ISE was started	No update since ISE was started.
Cisco conditions version	280052.0.0.0
Cisco AV/AS support chart version for windows	263.0.0.0
Cisco AV/AS support chart version for Mac OSX	181.0.0.0
Cisco AV/AS support chart version for Linux	33.0.0.0
Cisco supported OS version	84.6.2.0

2. Selecione a opção offline, procure e selecione a pasta posture-offline.zip que foi baixada para o

seu sistema local. Clique em Atualizar agora.



3. Quando as atualizações de postura começarem, o status será alterado para Atualizando.



4. O status das atualizações de postura pode ser verificado a partir das Informações de atualização conforme esta captura de tela:

The screenshot displays the Cisco Identity Services Engine (ISE) Administration / System interface. The left sidebar shows the navigation menu with 'Administration' selected. The main content area is titled 'Posture Updates' and includes the following sections:

- Posture Updates Configuration:**
 - Mode:** Web (selected) and Offline.
 - Update Feed URL:** <https://www.cisco.com/web/> (with a 'Set to Default' button).
 - Proxy Address:** [Redacted]
 - Proxy Port:** 8080
 - Automatic Check:** ☐ Automatically check for updates starting from initial delay. The delay is set to 14 hours, 51 minutes, and 55 seconds, with a frequency of every 2 hours.
 - Buttons:** Save, Update Now, and Reset.
- Update Information:** A table showing the status of updates.

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

Verificação

Faça login na GUI do nó Primary Admin -> Operations -> Troubleshooting -> Download Logs -> Debug Logs -> Application Logs -> isc-psc.log, clique em ise-psc.log e o log será baixado para o sistema local. Abra o arquivo baixado por meio do Bloco de Notas ou do editor de texto e filtre para download do OpSwat. Você deve ser capaz de encontrar as informações relacionadas às atualizações Posture que estão sendo executadas na implantação.

Você também pode controlar os logs efetuando login na CLI do nó Primary Admin usando o comando `show logging application ise-psc.log tail`.

O download do OpSwat, referente às atualizações de postura, foi iniciado:

```
2025-03-13 13:58:07,246 INFORMAÇÕES [admin-http-pool5][[]]
```

```
cisco.cpm.posture.download.DownloadManager -::admin::- Iniciando o download do opswat
```

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

```
cisco.cpm.posture.download.DownloadManager -::admin::- URI do arquivo de download offline :  
/opt/CSCOcpm/temp/cp/update/5c064701-a1ee-4a09-a190-3bf83c190af6/osgroupsV2.tar.gz
```

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

```
cisco.cpm.posture.download.DownloadManager -::admin::- URI do arquivo de download offline :  
/opt/CSCOcpm/temp/cp/update/5c064701-a1ee-4a09-a190-3bf83c190af6/osgroups.tar.gz
```

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

Concluído o download do Opswat, referindo-se a atualizações de postura são baixados e bem-sucedidos.

2025-03-13 14:24:50,796 INFO [pool-25534-thread-1][[]]

mnt.dbms.datadirect.impl.DatadirectServiceImpl -:::- Executando getStatus - datadirectSettings

2025-03-13 14:24:50,803 INFORMAÇÕES [admin-http-pool5][[]]

cisco.cpm.posture.download.DownloadManager -::admin::- Download do opswat concluído

2025-03-13 14:24:50,827 INFORMAÇÕES [admin-http-pool5][[]]

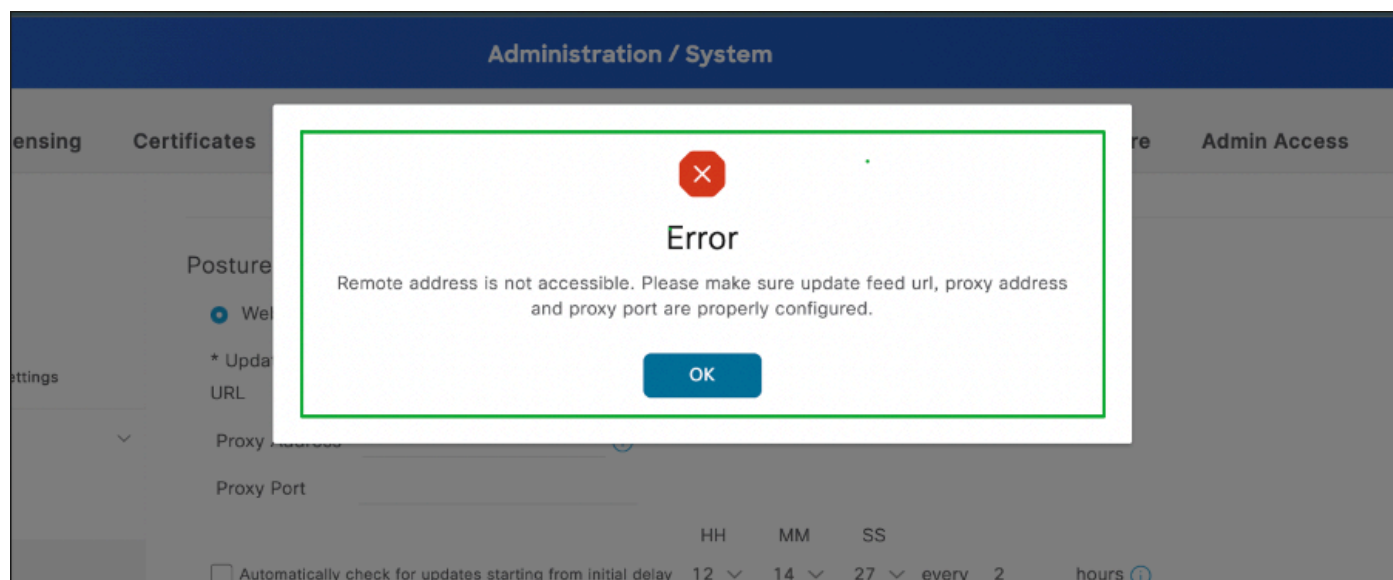
mnt.dbms.datadirect.impl.DatadirectServiceImpl -::admin::- Executando getStatus - datadirectSettings

Troubleshooting

Cenário

Falha nas Atualizações Online de Postura com o erro "O Endereço Remoto não está acessível. Verifique se a URL do feed de atualização, o endereço do proxy e a porta do proxy estão configurados corretamente".

Erro de exemplo:



Solução

1. Faça login na CLI do ISE, verifique se o ISE está acessível em cisco.com usando o comando "ping cisco.com".

isehostname/admin#ping cisco.com

Faça ping em cisco.com (72.163.4.161) 56(84) bytes de dados.

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

64 bytes de 72.163.4.161: icmp_seq=2 ttl=235 time=238 ms
64 bytes de 72.163.4.161: icmp_seq=3 ttl=235 time=239 ms
64 bytes de 72.163.4.161: icmp_seq=4 ttl=235 time=238 ms

— cisco.com ping statistics —

4 pacotes transmitidos, 4 recebidos, 0% de perda de pacotes, tempo 3004ms
rtt min/avg/max/mdev = 238,180/238,424/238,766/0,410 ms

2. Navegue até Administração -> Sistema -> Configurações -> O proxy está configurado com as portas apropriadas.

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. Verifique se as portas TCP 443, UDP 53 e UDP 123 são permitidas em todos os saltos para a Internet.

Defeitos conhecidos para problemas de atualização de postura

[ID de bug da Cisco 01523](#)

Referência

- [Guia do Administrador do Cisco Identity Services Engine, Versão 3.3](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.