在ISE中执行状态更新离线和在线

目录

简介

本文档介绍如何在思科身份服务引擎®(ISE)中执行状态更新。

先决条件

要求

思科建议您了解安全评估流程。

使用的组件

本文档中的信息基于这些硬件与软件版本。

- 思科身份服务引擎3.2及更高版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

安全状态更新包括一组预定义的检查、规则和支持图表，用于防病毒和反间谍软件的Windows和MacOS操作系统，以及思科支持的操作系统信息。

当您首次在网络中部署思科ISE时，您可以从网络下载终端安全评估更新。此过程通常需要大约20分钟。在初始下载后，您可以配置Cisco ISE验证和下载增量更新自动发生。

思科ISE仅在初始状态更新期间创建一次默认状态策略、要求和补救。如果删除它们，思科ISE不会在后续手动或计划更新期间再次创建它们。

您可以执行两种状态更新：

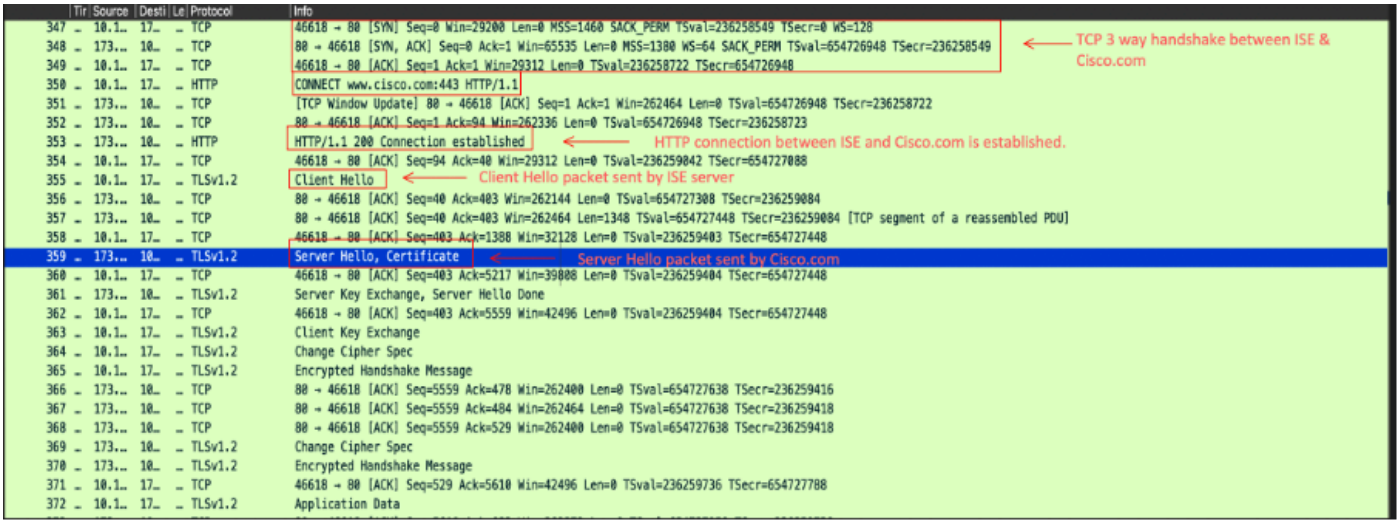
- 在线状态更新。
- 离线状态更新。

在线状态更新

Web Posture Update/Online Posture Update会从思科云或服务器存储库检索最新状态更新。这包括直接从思科服务器下载最新的策略、定义和签名。ISE需要连接到思科云服务器或更新存储库，以检索最新的终端安全评估定义、策略和其他关联文件。

网络或在线状态更新期间会发生什么情况？

身份服务引擎(ISE)使用HTTP通过代理或直接互联网连接访问思科网站，与www.cisco.com建立连接。在此过程中，将发生客户端hello和服务器hello交换，服务器提供其证书以验证其合法性和确认客户端信任。完成客户端hello和服务器hello后，客户端密钥交换发生，服务器启动状态更新。以下数据包捕获演示在线状态更新期间ISE服务器与Cisco.com之间的通信。



- 在Server Hello期间，Cisco.com会将这些证书发送到客户端以确认客户端信任。

<#root>

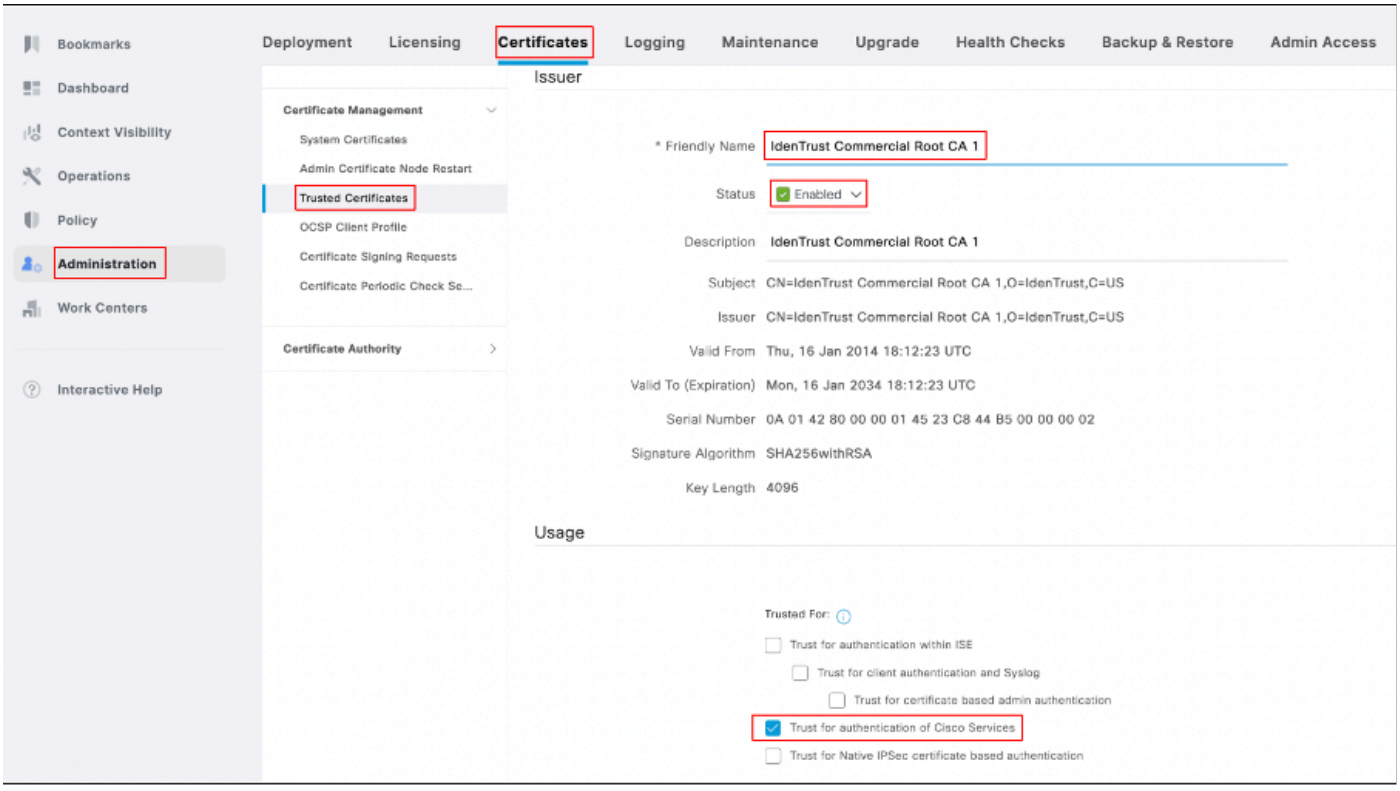
```
Certificates Length: 5083
Certificates (5083 bytes)
Certificate Length: 1940
Certificate: 3082079030820678a003020102021040019 1d1f3c7ec4ea73b301be3e06a90300d06092a… (id-at-commonNam
Certificate Length: 1754
Certificate: 308206d6308204bea003020102021040016efb0a205cfaebe18f71d73abb78300d06092a… (id-at-commonNam
Certificate Length: 1380
Certificate: 3082056030820348a00302010202100a0142800000014523c844b500000002300d06092a… (id-at-commonNam
```

IdenTrust Commercial Root CA

1

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

- 在ISE GUI中，必须确保启用服务器证书IdenTrust Commercial Root CA 1，并信任对思科服务进行身份验证，以建立与Cisco.com的连接。默认情况下，此证书包含在ISE中，并选中“Trust for authenticating Cisco services”，但建议进行验证。
- 通过转至ISE GUI > Administration > Certificates > Trusted Certificates检查证书状态和受信任的使用情况。按名称IdenTrust Commercial Root CA 1过滤，选择证书，然后编辑证书以验证信任用法，如下屏幕截图所示：



- 安全评估更新可以包括新的或修改的安全评估策略、新的防病毒/防恶意软件定义和其他安全相关标准。

- 此方法需要活动的互联网连接，通常在ISE系统配置为使用基于云的存储库进行状态更新时执行。

适用场合

当您希望确保安全评估策略、安全定义和条件与思科提供的最新可用版本保持一致时，可使用在线安全评估更新。

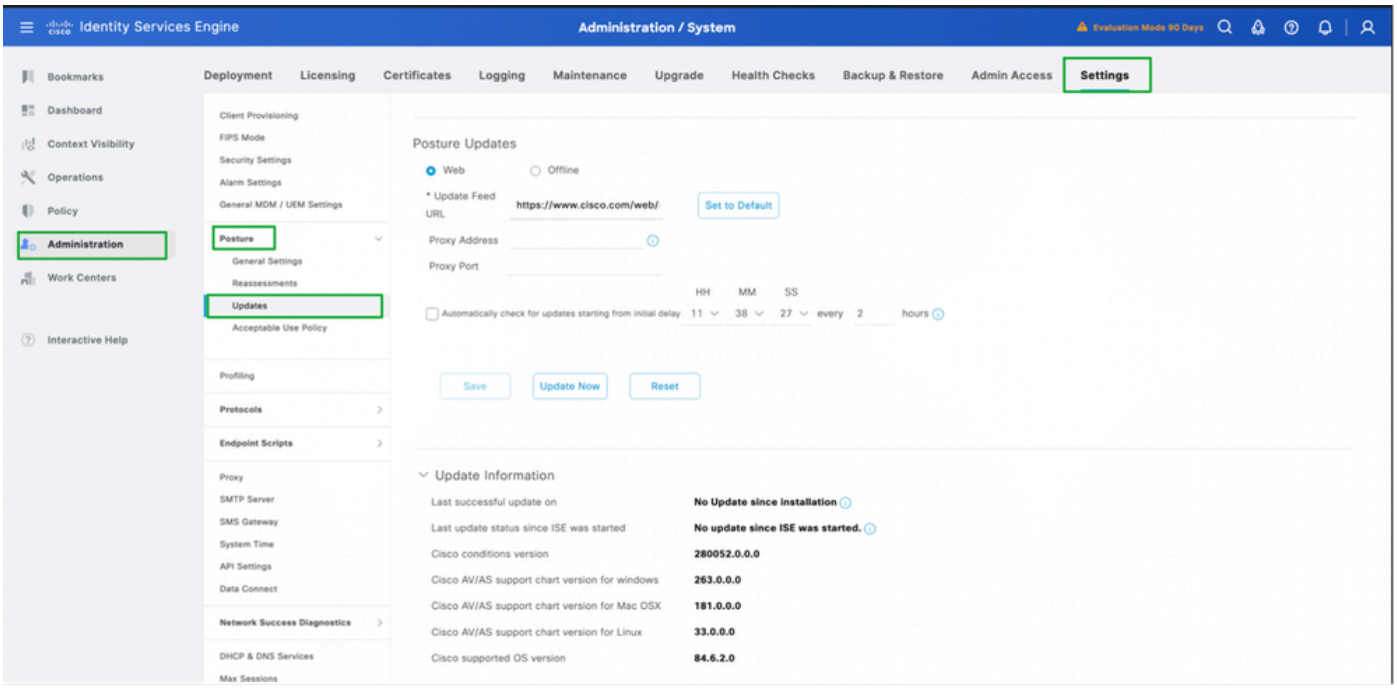
用于在线状态更新的端口

要确保ISE系统可以成功到达思科云服务器以下载终端安全评估更新，必须在防火墙中打开这些端口并允许从ISE到互联网的出站通信：

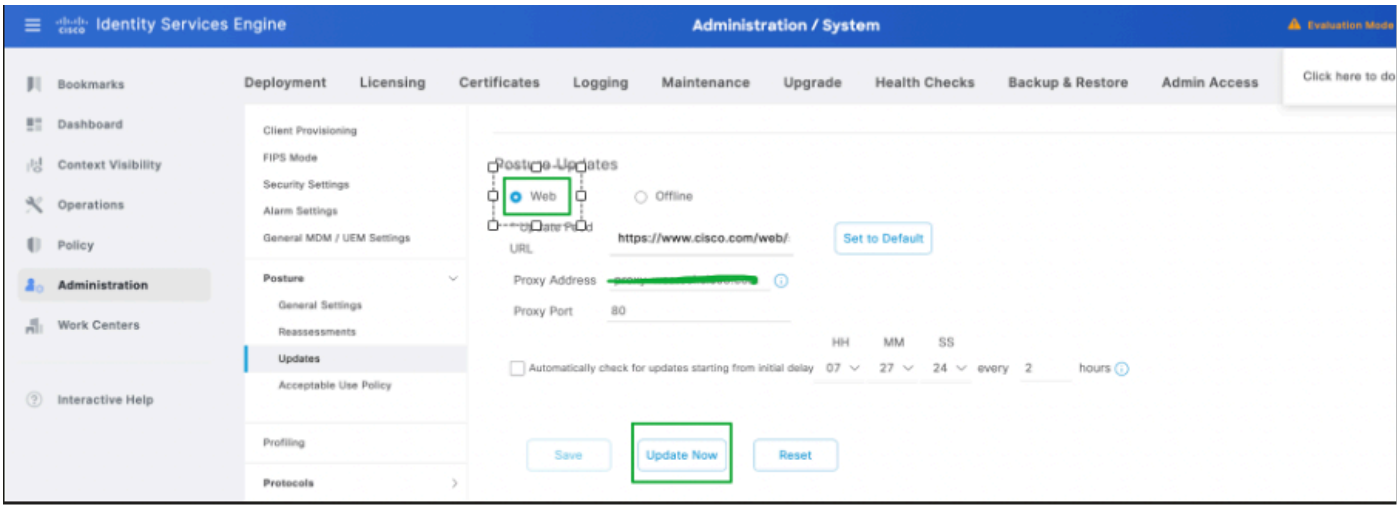
1. HTTPS(TCP 443):
   - ISE通过安全连接(TLS/SSL)访问思科云服务器和下载更新的主端口。
   - 这是基于Web的状态更新进程的最关键端口。
2. DNS(UDP 53):
   - ISE必须能够执行DNS查找来解析更新服务器的主机名。
   - 确保ISE系统可以访问DNS服务器并解析域名。
3. NTP(UDP 123):
   - ISE使用NTP进行时间同步。这对于确保更新过程的时间戳正确以及ISE系统在同步的时区运行非常重要。
   - 在许多情况下，还需要通过UDP 123访问NTP服务器。

执行在线状态更新的程序

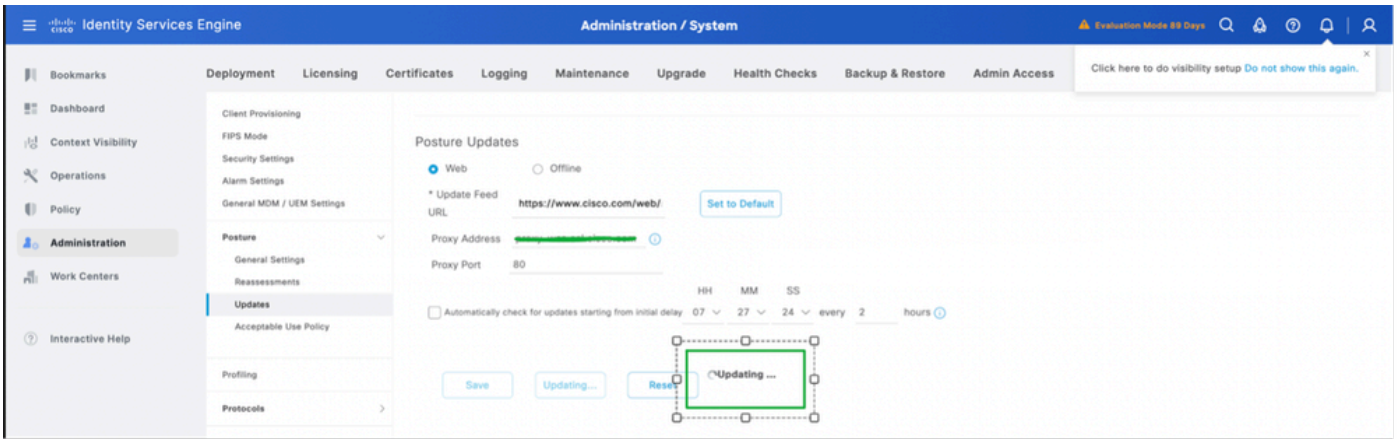
1. 登录GUI -> Administration -> System -> Settings -> Posture -> Updates。



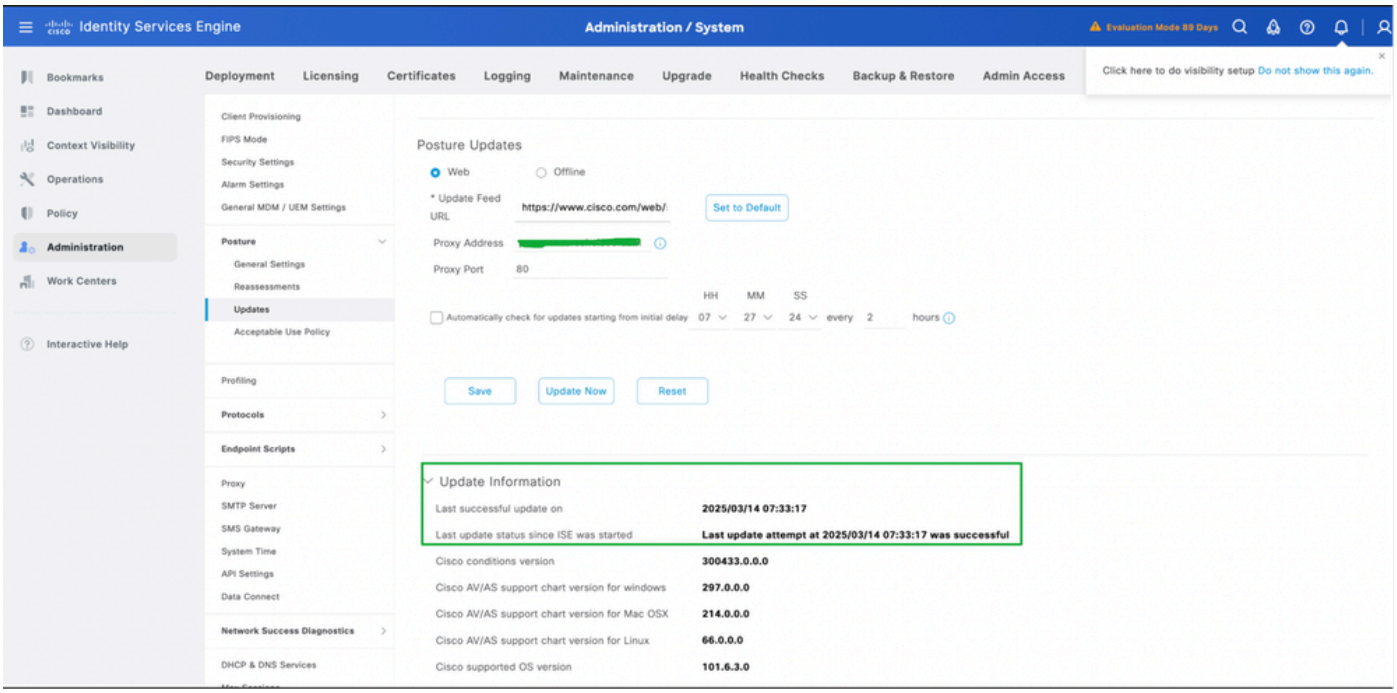
2.选择方法作为Web进行在线状态更新，然后单击Update Now。



3.状态更新开始后，状态将更改为更新。



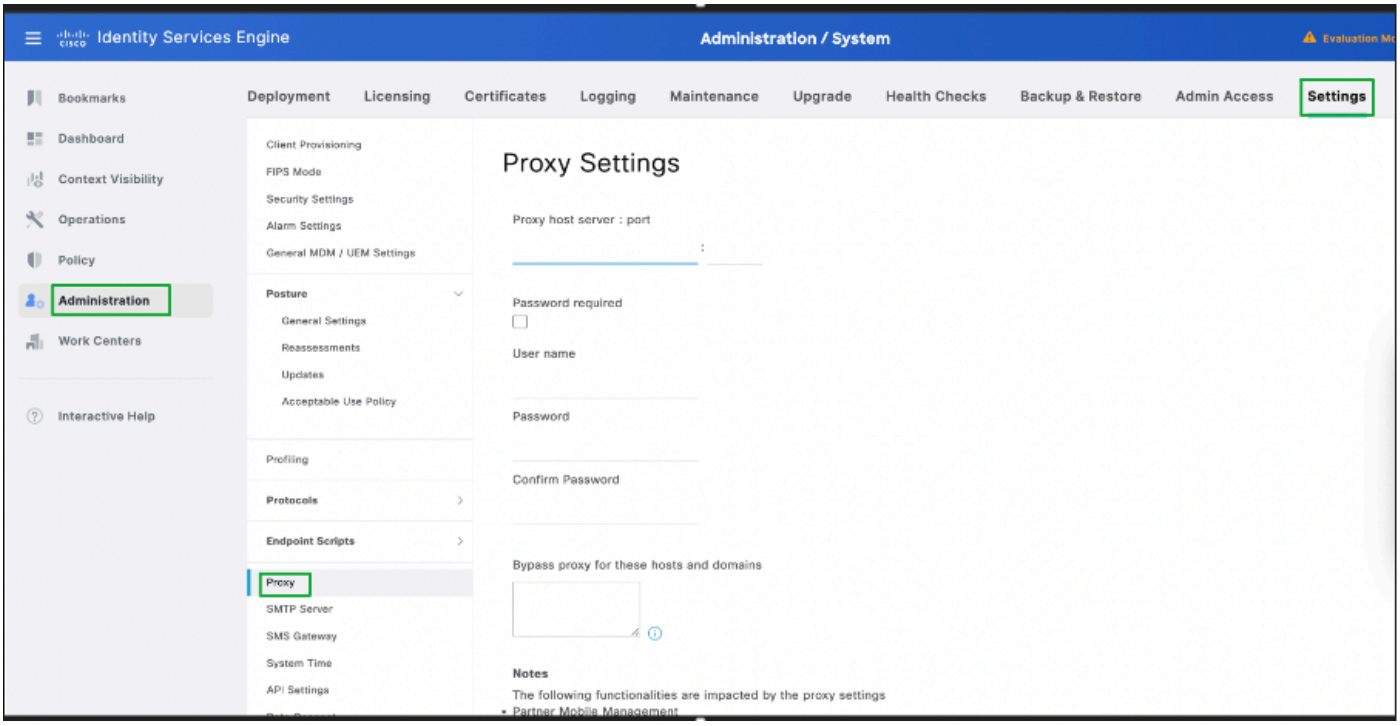
4.根据此屏幕截图，可从更新信息验证终端安全评估更新的状态：



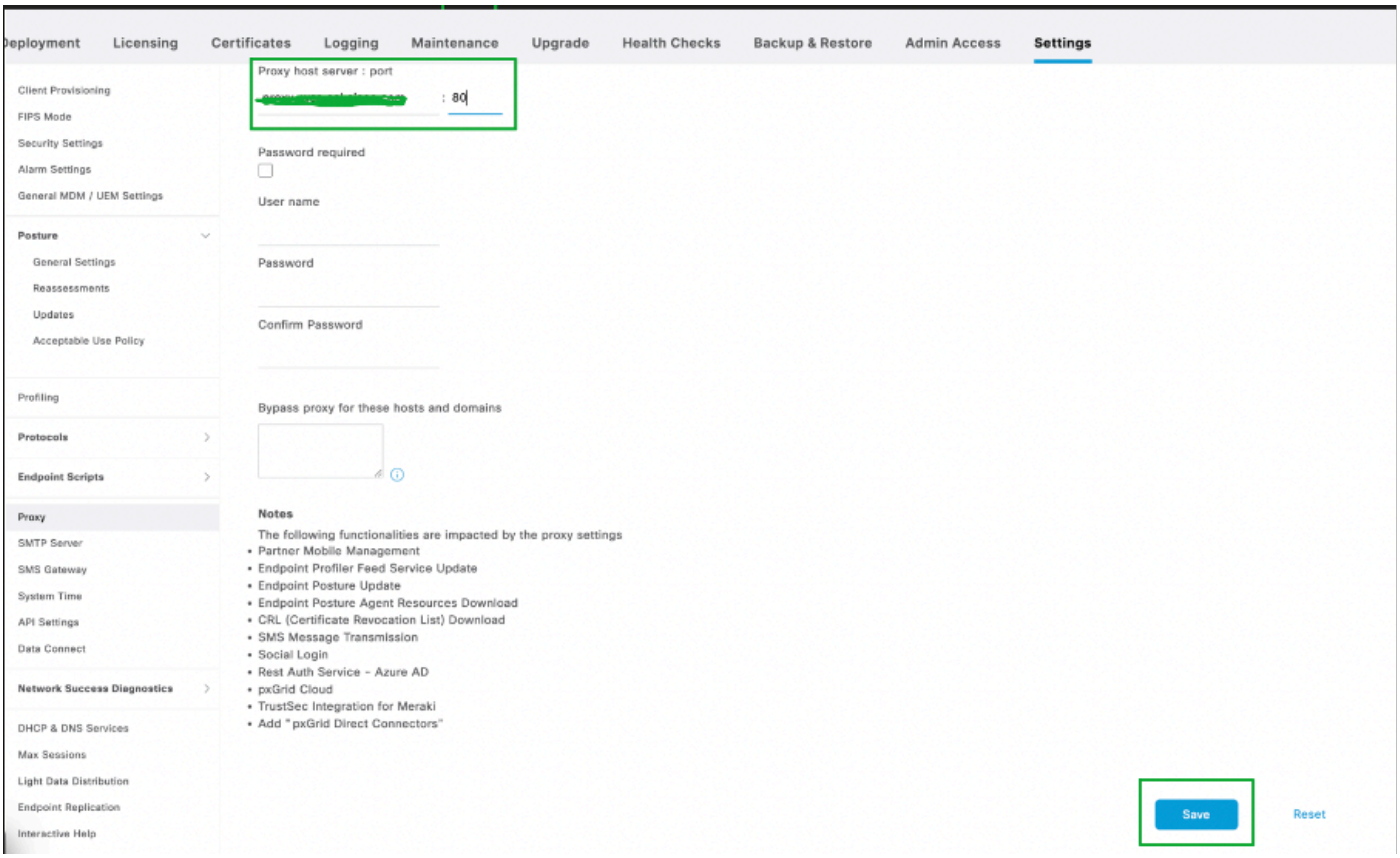
在线状态更新的代理配置

在状况更新字段URL不可访问的受限环境中，在这种情况下，需要代理配置。请参阅在ISE中配置代理。

1. 导航到管理(Administration)->系统(System)->设置(Settings)->代理(Proxy)。



2.配置代理详细信息，单击保存。



3.执行在线状态更新时，ISE会自动获取代理的详细信息。

离线状态更新

Offline Posture Update允许您手动将状态更新文件（以.zip或其他支持的文件格式）上传到ISE。

当您执行离线状态更新时，会发生什么情况？

- 您手动上传更新的状况文件。
- ISE处理和应用这些文件，其中包括更新的策略、防病毒定义、安全状态评估以及其他类型的文件。
- 离线更新不需要Internet连接，通常用于具有严格安全或网络策略，防止直接访问外部服务器的环境。

适用场合

此方法通常用于系统与Internet隔离的环境中，或者当您拥有由Cisco或您的安全团队提供的特定脱机更新文件时。

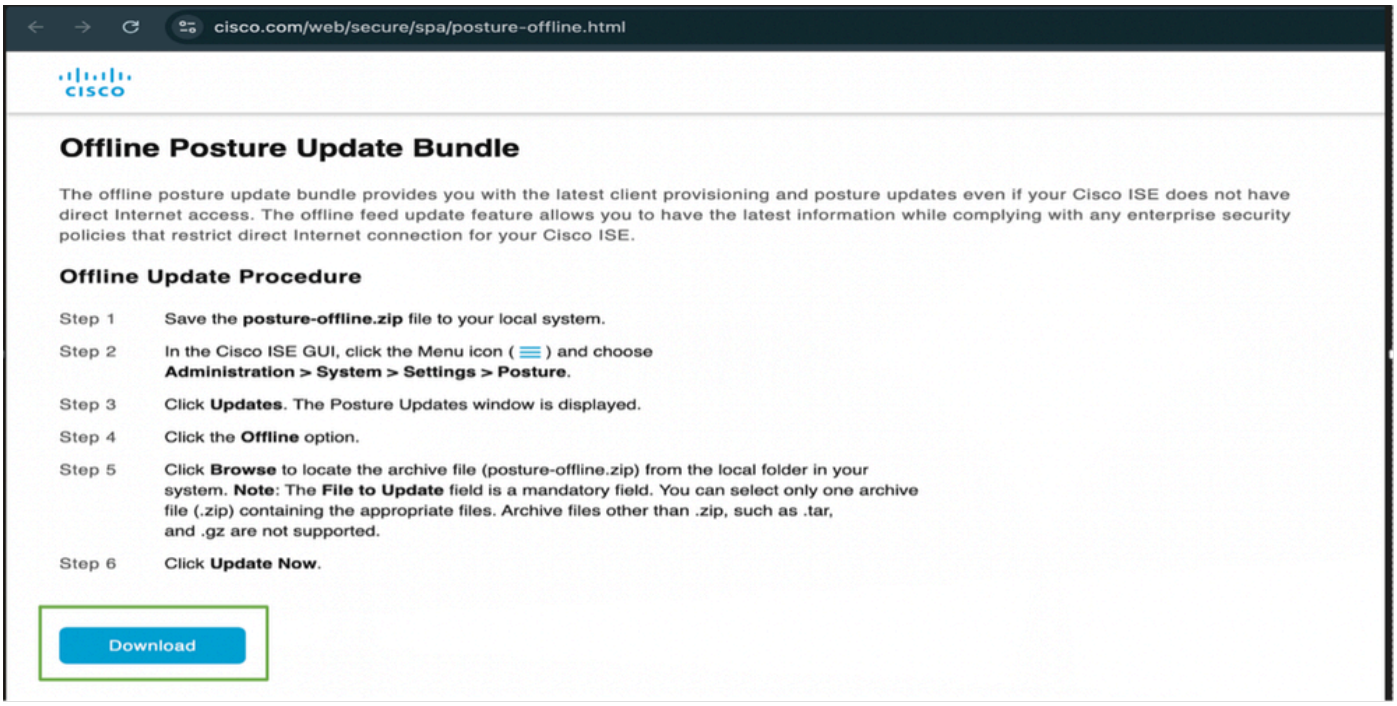
用于离线状态更新的端口

对于与ISE服务器的一般通信（在更新过程中），在许多情况下，这些端口是相关的：

1. 管理访问（端口22、443）：
   - SSH(TCP 22):如果您使用SSH访问ISE系统以进行故障排除或手动上传。
   - HTTPS(TCP 443):如果使用GUI（Web界面）进行更新上传。
2. 文件传输（SFTP或SCP）：
   - 如果需要通过SFTP或SCP手动将文件上传到ISE，请确保在ISE系统上打开相应端口（通常为SSH/SFTP的端口22）。
3. 本地网络访问:
   - 确保您上传更新的系统（例如，管理工作站或服务器）可以通过管理访问所需的端口与ISE通信，但是同样，脱机状态更新不需要任何外部端口，因为文件是手动提供的。

在哪里查找文件以进行离线状态更新？

1. 导航至URL:https://www.cisco.com/web/secure/spa/posture-offline.html，点击Download并将posture-offline.zip文件下载到您的本地系统。

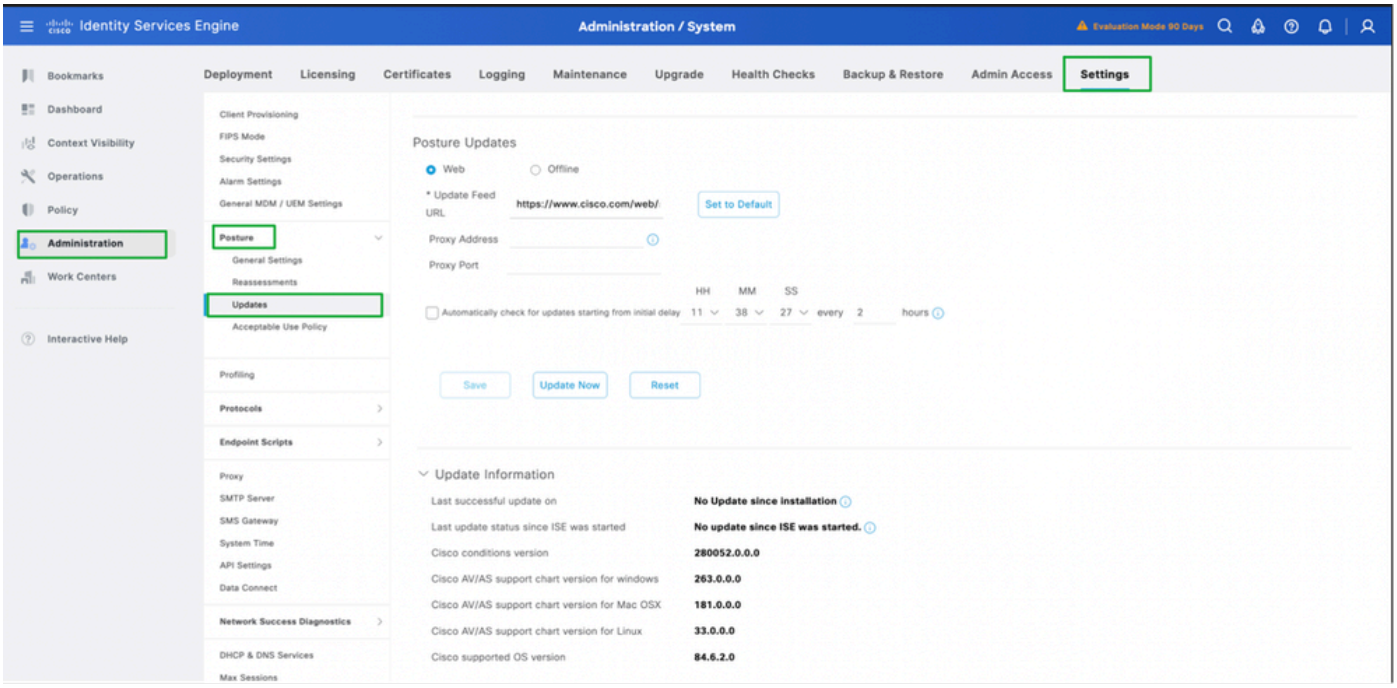


离线状态更新文件包括

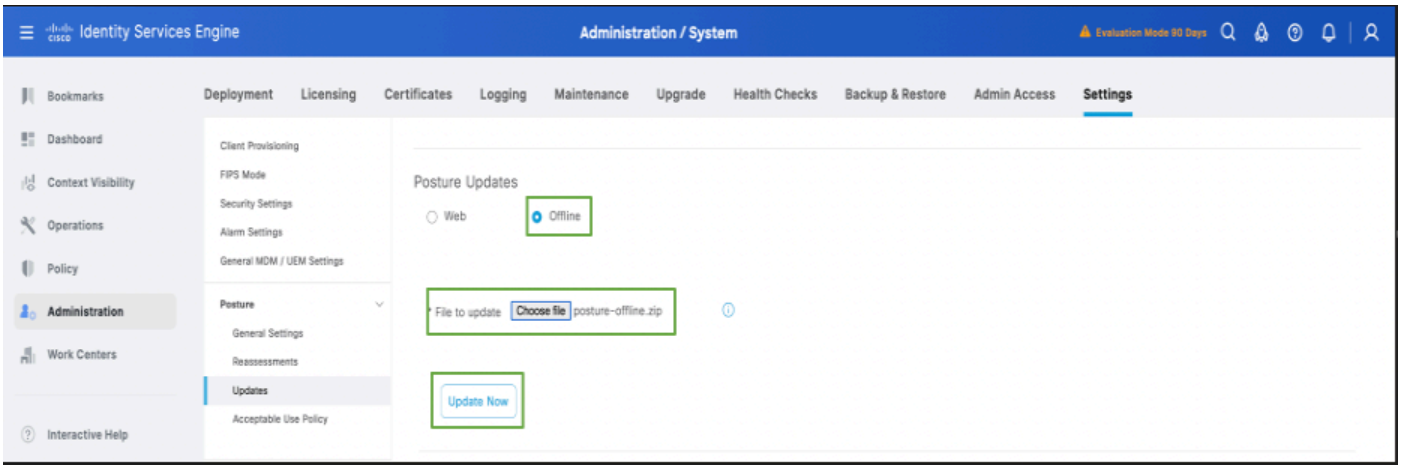
- 防病毒定义（签名）。
- 状况策略和规则。
- 安全评估和其他状态评估配置文件。

执行离线状态更新的过程

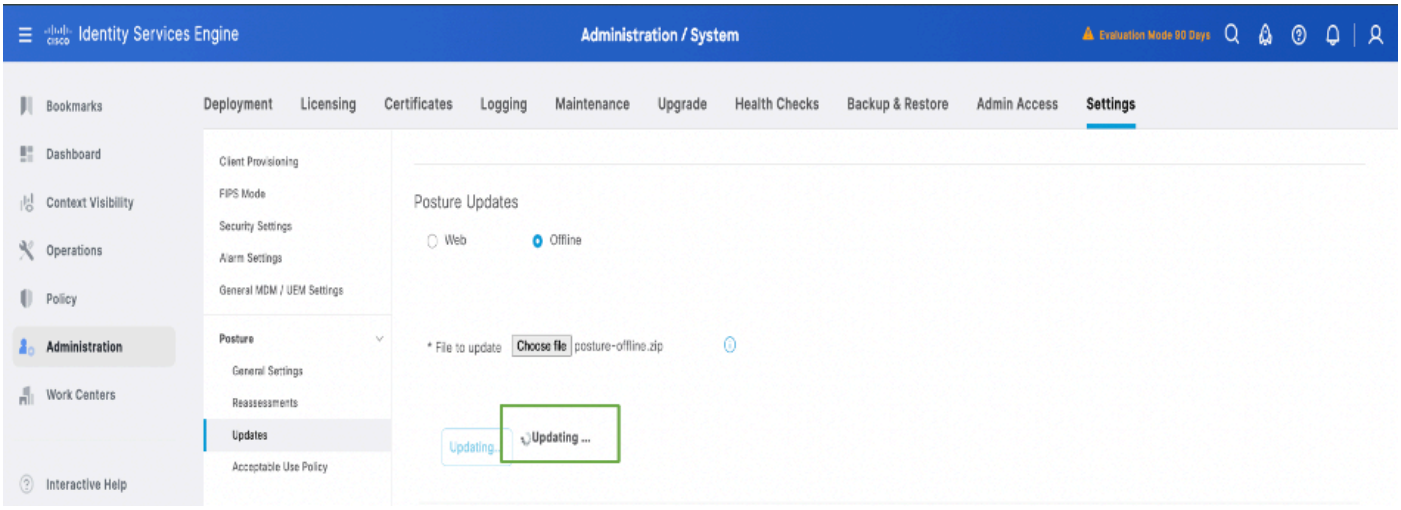
1. 登录ISE GUI -> Administration -> System -> Settings -> Posture -> Updates。

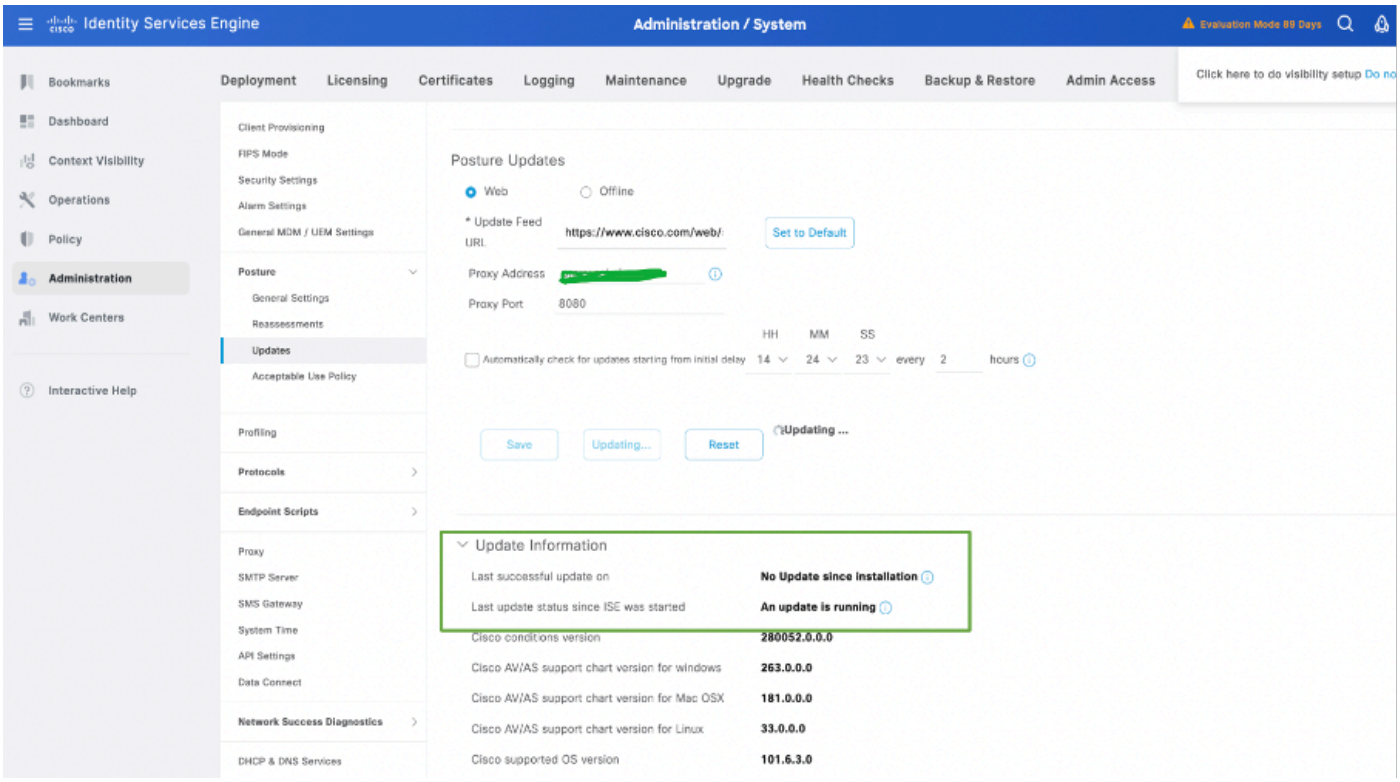


2.选择offline选项，浏览并选择已下载到本地系统的posture-offline.zip文件夹。单击Update Now。

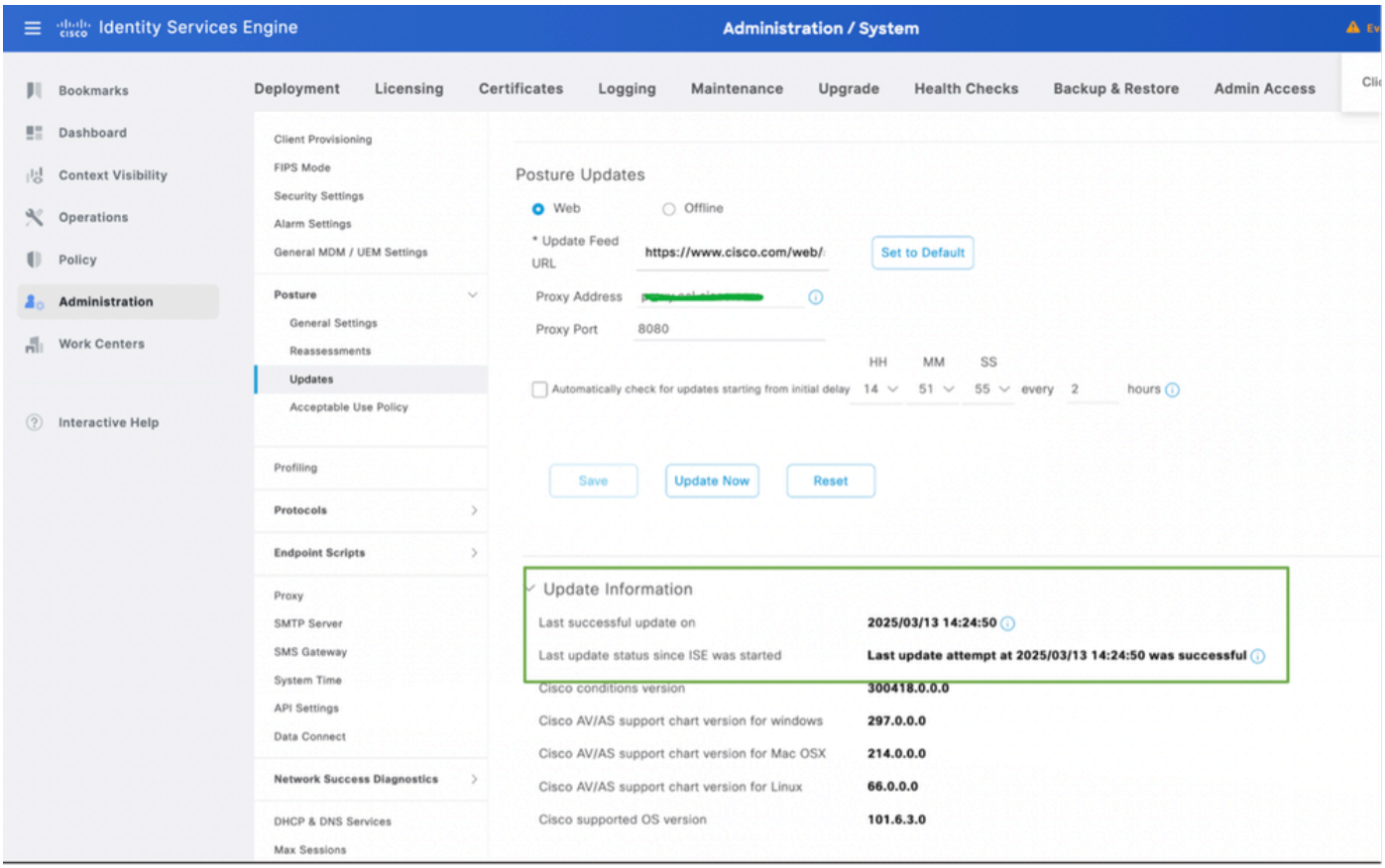


3.状态更新开始后，状态将更改为更新。





4.根据此屏幕截图，可从更新信息验证终端安全评估更新的状态：



确认

登录到Primary Admin节点的GUI -> Operations -> Troubleshooting -> Download Logs -> Debug logs -> Application logs -> isc-psc.log ，单击ise-psc.log，日志会下载到您的本地系统。通过记事本或文本编辑器打开已下载的文件，并过滤Opswat下载。您必须能够找到与在部署中执行的状态更新相关的信息。

您还可以使用show logging application ise-psc.log tail命令登录到主管理节点的CLI，从而跟踪日志。

Opswat下载（指安全评估更新）已启动：

2025-03-13 13:58:07,246 INFO [admin-http-pool5][[]] cisco.cpm.posture.download.DownloadManager -::admin::: — 正在启动opswat下载

2025-03-13 13:58:07,251 INFO [admin-http-pool5][[]] cisco.cpm.posture.download.DownloadManager -::admin::: — 脱机下载文件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::: — 脱机下载文件URI :/opt/CSCOcpm/temp/cp/update/5c064701-a1ee-4a09-a190-3bf83c190af6/osgroups.tar.gz

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

已完成Opswat下载，表示状态更新已下载并成功。

2025-03-13 14:24:50,796 INFO [pool-25534-thread-1][[]]
mnt.dbms.datadirect.impl.DatadirectServiceImpl -::: — 正在执行getStatus - datadirectSettings

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

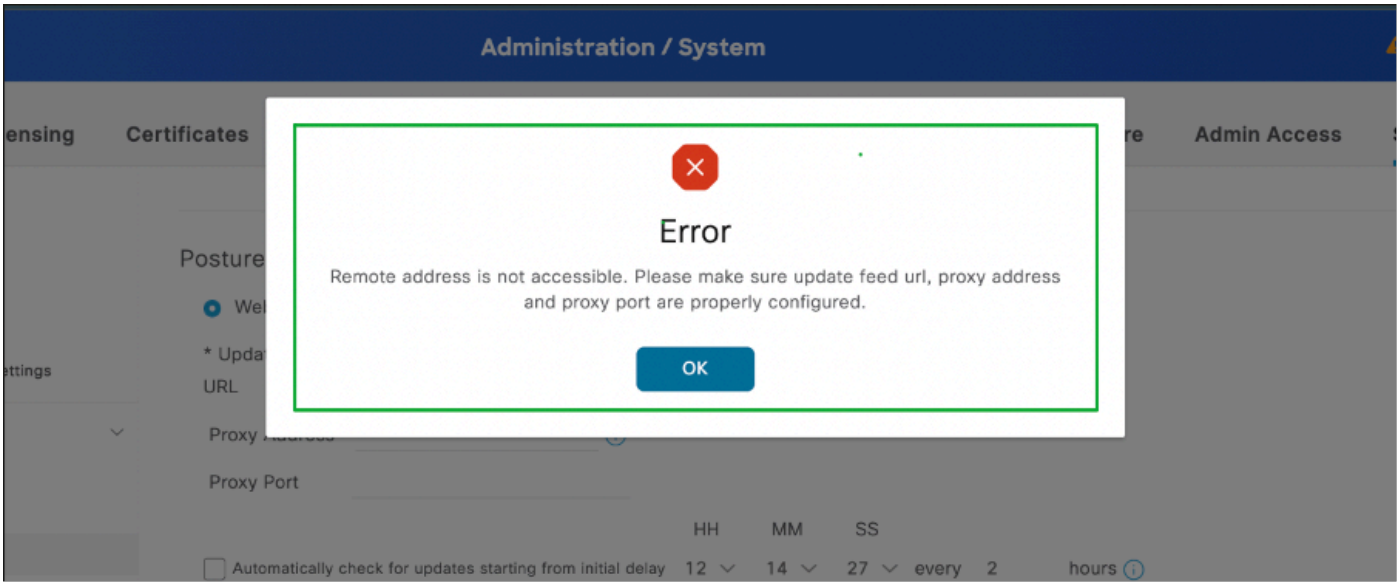
2025-03-13 14:24:50,827 INFO [admin-http-pool5][[]]
mnt.dbms.datadirect.impl.DatadirectServiceImpl -::admin:: — 正在执行getStatus - datadirectSettings

故障排除

场景

在线状态更新失败，错误为“远程地址不可访问。请确保更新源URR、代理地址和代理端口配置正确”。

示例错误：



解决方案

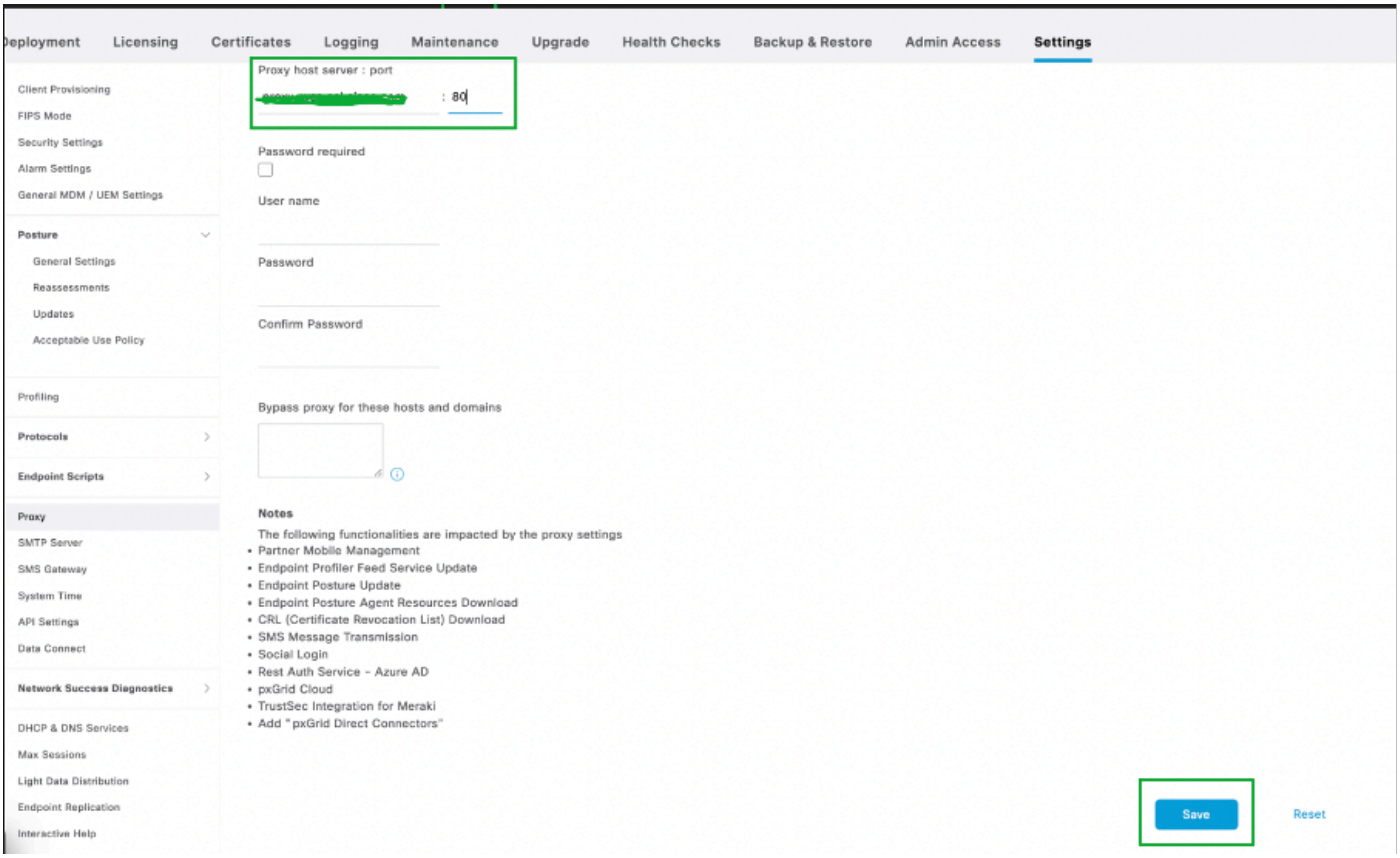
1.登录ISE的CLI，使用命令“ping cisco.com”验证ISE可以访问cisco.com。

isehostname/admin#ping cisco.com
PING cisco.com(72.163.4.161)56(84)字节的数据。
从72.163.4.161开始的64个字节：icmp_seq=1 ttl=235 time=238 ms
从72.163.4.161开始的64个字节：icmp_seq=2 ttl=235 time=238 ms
从72.163.4.161开始的64个字节：icmp_seq=3 ttl=235 time=239 ms
从72.163.4.161开始的64个字节：icmp_seq=4 ttl=235 time=238 ms

— cisco.com ping统计信息 —
4个数据包已传输，4个已接收，0%数据包丢失，时间3004ms

rtt min/avg/max/mdev = 238.180/238.424/238.766/0.410毫秒

2.导航至管理 — >系统 — >设置 — >代理配置了正确的端口。



3.验证通往Internet的所有跳上是否允许端口TCP 443、UDP 53和UDP 123。

状态更新问题的已知缺陷

思科漏洞ID 01523

参考

- 思科身份服务引擎管理员指南，版本3.3

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。