Realizar actualizaciones de estado en ISE sin conexión y en línea

Contenido

- Introducción
- Prerequisites
  - Requirements
  - Componentes Utilizados
- Antecedentes
- Actualizaciones de estado online
  - ¿Qué ocurre durante las actualizaciones de estado en línea o en la Web?
    - Cuándo se debe utilizar
  - Puertos utilizados para la actualización de estado en línea
  - Procedimiento para realizar actualizaciones de estado en línea
- Configuración de proxy para actualizaciones de estado en línea
- Actualizaciones de estado sin conexión
  - ¿Qué ocurre cuando se realiza una actualización de estado sin conexión?
    - Cuándo se debe utilizar
  - Puertos utilizados para actualizaciones de estado sin conexión
  - ¿Dónde buscar archivos para actualizaciones de estado sin conexión?
  - Incluir archivos de actualización de estado sin conexión
  - Procedimiento para realizar actualizaciones de estado sin conexión
- Verificación
- Troubleshoot
  - Situación
  - Solución
  - Defectos conocidos para problemas de actualización de estado
- Referencia

Introducción

Este documento describe cómo realizar actualizaciones de estado en Cisco Identity Services Engine® (ISE).

Prerequisites

Requirements

Cisco recomienda que tenga conocimientos sobre el flujo de estado.

Componentes Utilizados

La información de este documento se basa en estas versiones de hardware y software.

- Cisco Identity Services Engine 3.2 y versiones posteriores.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Las actualizaciones de estado incluyen un conjunto de comprobaciones predefinidas, reglas y gráficos de compatibilidad para antivirus y anti spyware para sistemas operativos Windows y MacOS, así como información de sistemas operativos compatibles con Cisco.

Al implementar Cisco ISE en la red por primera vez, puede descargar actualizaciones de estado desde la Web. Este proceso suele tardar aproximadamente 20 minutos. Después de la descarga inicial, puede configurar Cisco ISE para que verifique y descargue las actualizaciones incrementales para que se realicen automáticamente.

Cisco ISE crea políticas de estado, requisitos y soluciones predeterminadas solo una vez durante una actualización de estado inicial. Si los elimina, Cisco ISE no los volverá a crear durante las siguientes actualizaciones manuales o programadas.

Existen dos tipos de actualizaciones de estado que puede realizar:

- Actualizaciones de estado en línea.
- Actualizaciones de estado sin conexión.

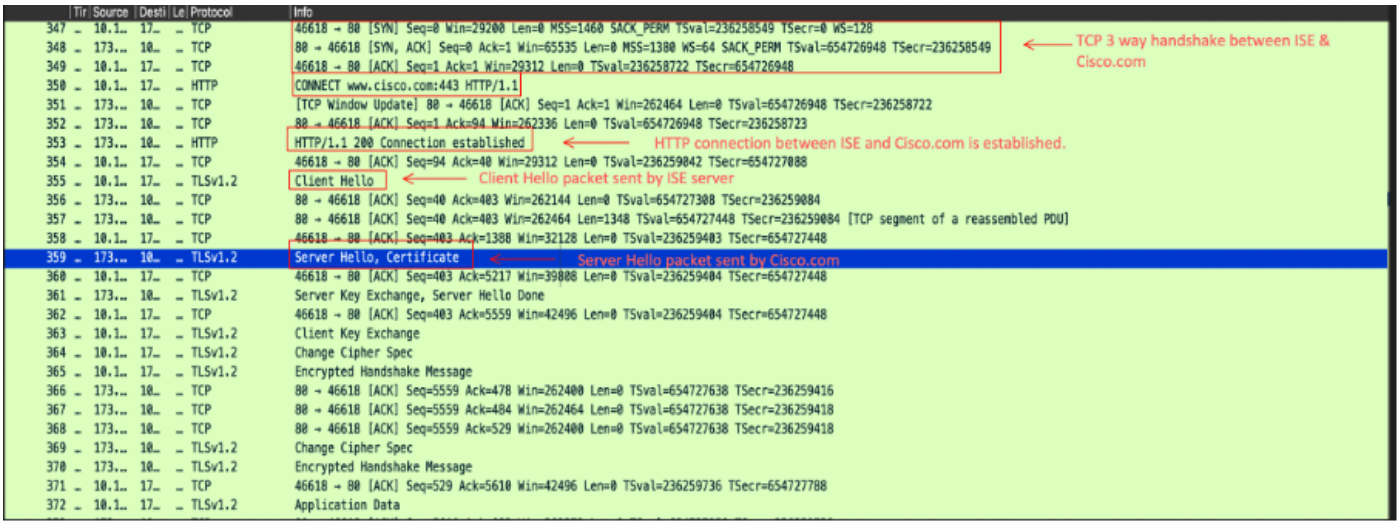
Actualizaciones de estado online

Una Actualización de estado web/Actualización de estado en línea recupera las últimas actualizaciones de estado de los repositorios del servidor o de la nube de Cisco. Esto implica descargar las últimas políticas, definiciones y firmas directamente desde los servidores de Cisco. ISE debe conectarse a los servidores en la nube de Cisco o actualizar los repositorios para recuperar las definiciones de estado, las políticas y otros archivos asociados más recientes.

¿Qué ocurre durante las actualizaciones de estado en línea o en la Web?

El Identity Services Engine (ISE) accede al sitio web de Cisco a través de un proxy o de una conexión directa a Internet mediante HTTP, estableciendo una conexión con www.cisco.com. Durante este proceso, se produce el intercambio de saludo del cliente y saludo del servidor, y el servidor proporciona su certificado para verificar su legitimidad y confirmar la confianza del lado del cliente. Una vez que se completan el saludo del cliente y el saludo del servidor, tiene lugar el intercambio de claves del cliente y el servidor inicia las actualizaciones de estado. Esta es la

captura de paquetes que demuestra la comunicación entre el servidor ISE y Cisco.com durante las actualizaciones de estado en línea.



- Durante el saludo del servidor, Cisco.com envía estos certificados al cliente para confirmar la confianza del lado del cliente.

<#root>

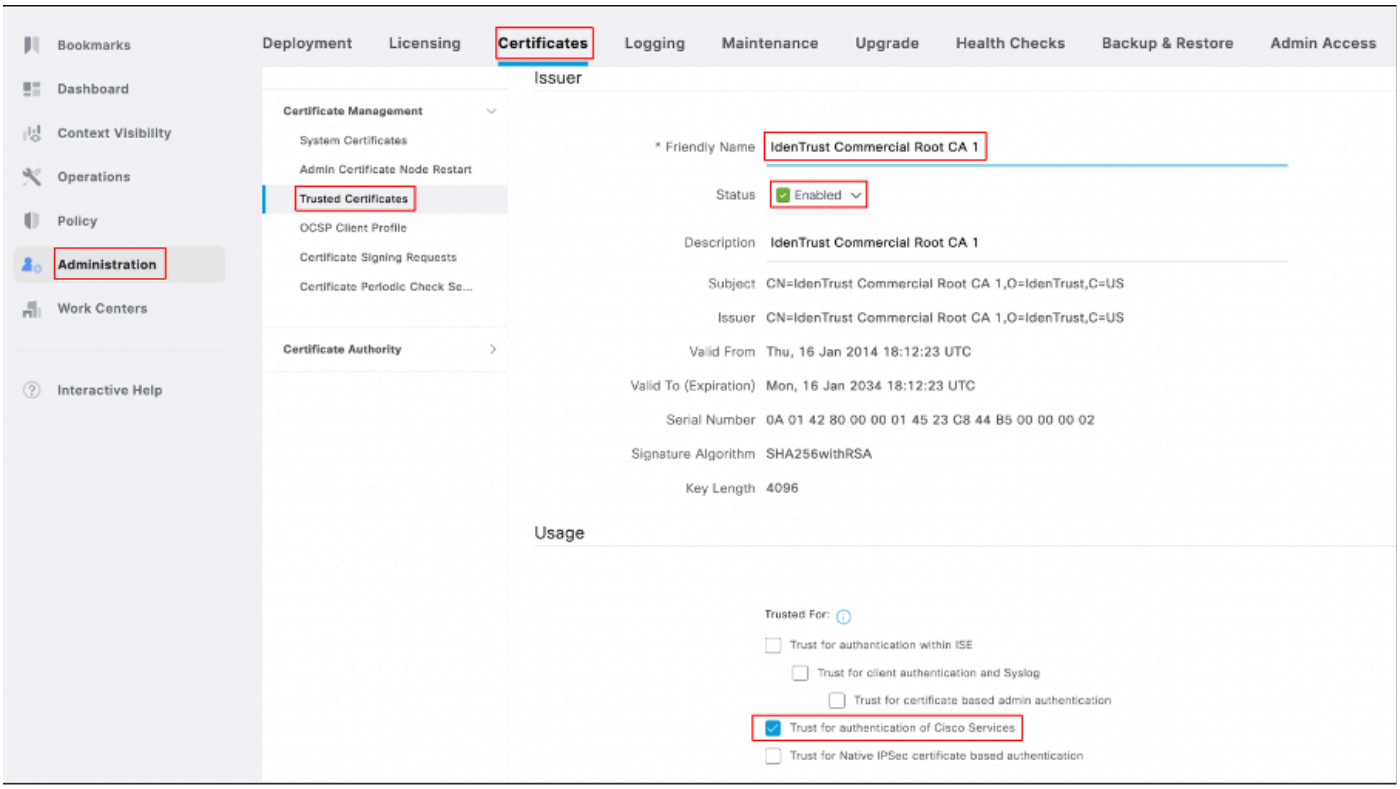
```
Certificates Length: 5083
Certificates (5083 bytes)
Certificate Length: 1940
Certificate: 3082079030820678a003020102021040191d1f3c7ec4ea73b301be3e06a90300d06092a… (id-at-commonNam
Certificate Length: 1754
Certificate: 308206d6308204bea003020102021040016efb0a205cfaebe18f71d73abb78300d06092a… (id-at-commonNam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

IdenTrust Commercial Root CA

1

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

- En la GUI de ISE, es importante asegurarse de que el certificado de servidor IdenTrust Commercial Root CA 1 esté habilitado y Trust para autenticar los servicios de Cisco para establecer la conectividad con Cisco.com. De forma predeterminada, este certificado se incluye en ISE y la opción "Confianza para autenticar los servicios de Cisco" está activada, pero se recomienda la verificación.
- Verifique el estado del certificado y el uso confiable en la GUI de ISE > Administración > Certificados > Certificados confiables. Filtre por el nombre IdenTrust Commercial Root CA 1, seleccione el certificado y edítelo para verificar el uso de confianza, como se muestra en esta captura de pantalla:



- Las actualizaciones de estado pueden incluir políticas de estado nuevas o revisadas, nuevas definiciones de antivirus/antimalware y otros criterios relacionados con la seguridad para las evaluaciones de estado.
- Este método requiere una conexión a Internet activa y se suele realizar cuando el sistema ISE está configurado para utilizar repositorios basados en la nube para actualizaciones de estado.

Cuándo se debe utilizar

Las actualizaciones de estado online se utilizan cuando se desea garantizar que las políticas de estado, las definiciones de seguridad y los criterios están actualizados con las últimas versiones disponibles proporcionadas por Cisco.

Puertos utilizados para la actualización de estado en línea

Para garantizar que el sistema ISE pueda acceder correctamente a los servidores en la nube de Cisco para descargar las actualizaciones de estado, estos puertos deben estar abiertos en el firewall y permitir la comunicación saliente de ISE a Internet:

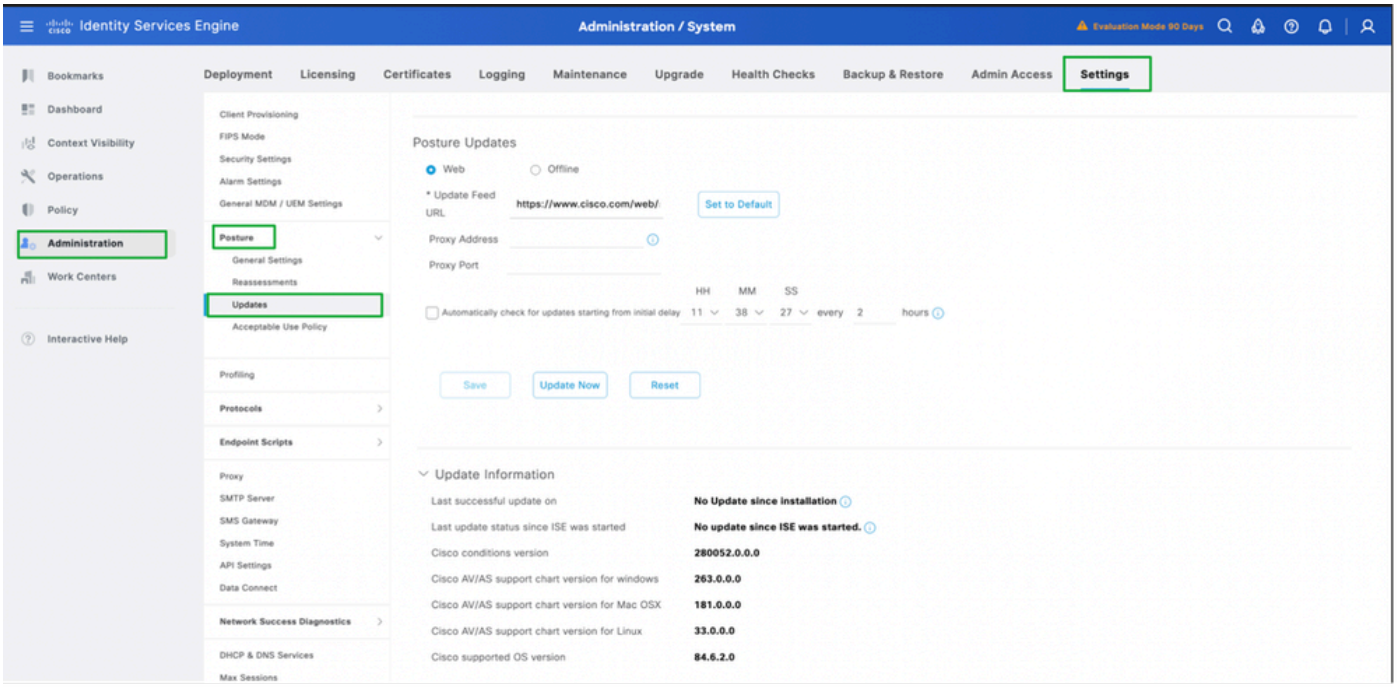
1. HTTPS (TCP 443):
    - Puerto principal para que ISE llegue a los servidores en la nube de Cisco y descargue actualizaciones a través de una conexión segura (TLS/SSL).
    - Este es el puerto más importante para el proceso de actualización de estado basado en Web.
2. DNS (UDP 53):
    - ISE debe poder realizar búsquedas DNS para resolver los nombres de host de los servidores de actualización.

- Asegúrese de que su sistema ISE puede alcanzar los servidores DNS y resolver los nombres de dominio.

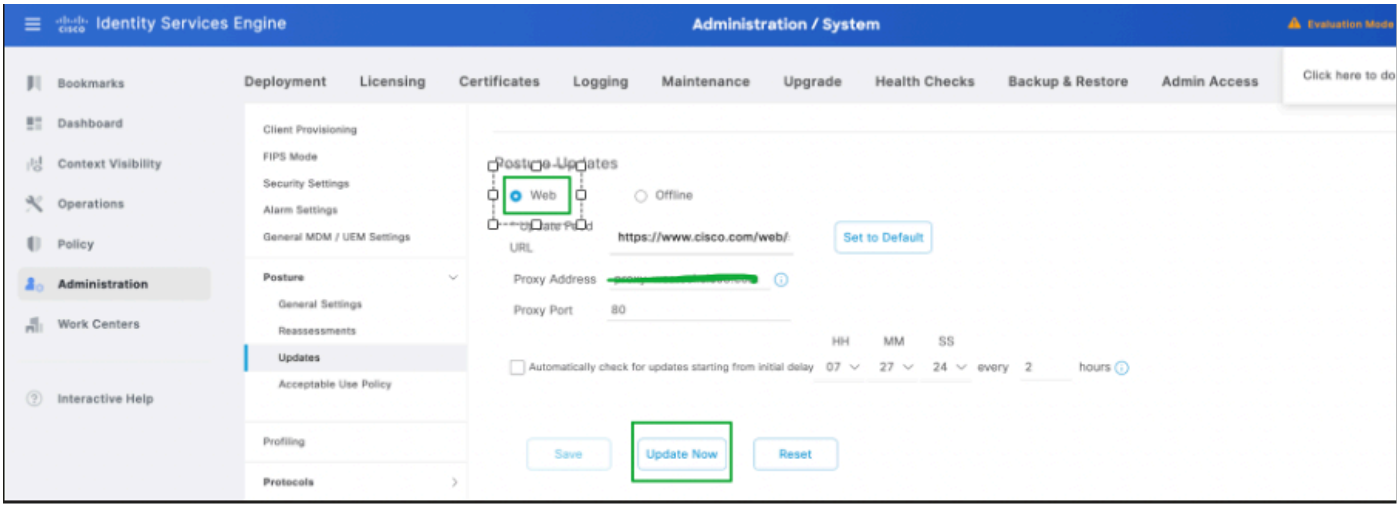
3. NTP (UDP 123):
   - ISE utiliza NTP para la sincronización horaria. Esto es importante para garantizar que el proceso de actualización tiene la marca de tiempo correcta y que el sistema ISE funciona en una zona horaria sincronizada.
   - En muchos casos, los servidores NTP también deben ser accesibles a través de UDP 123.

Procedimiento para realizar actualizaciones de estado en línea

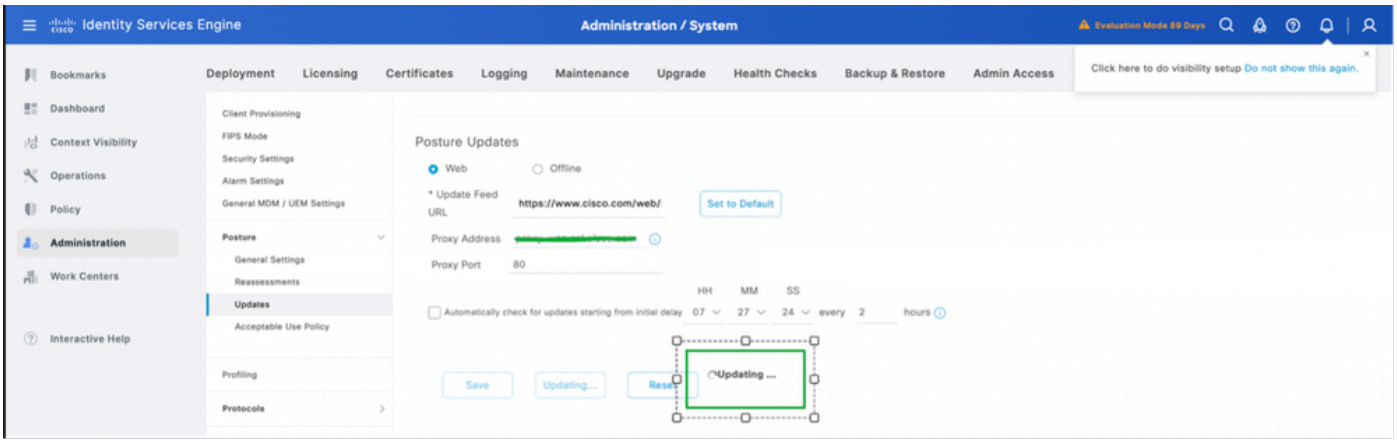
1. Inicie sesión en la GUI -> Administration -> System -> Settings -> Posture -> Updates (GUI -> Administration -> System -> Settings -> Posture -> Updates (Configuración -> Estado -> Actualizaciones).



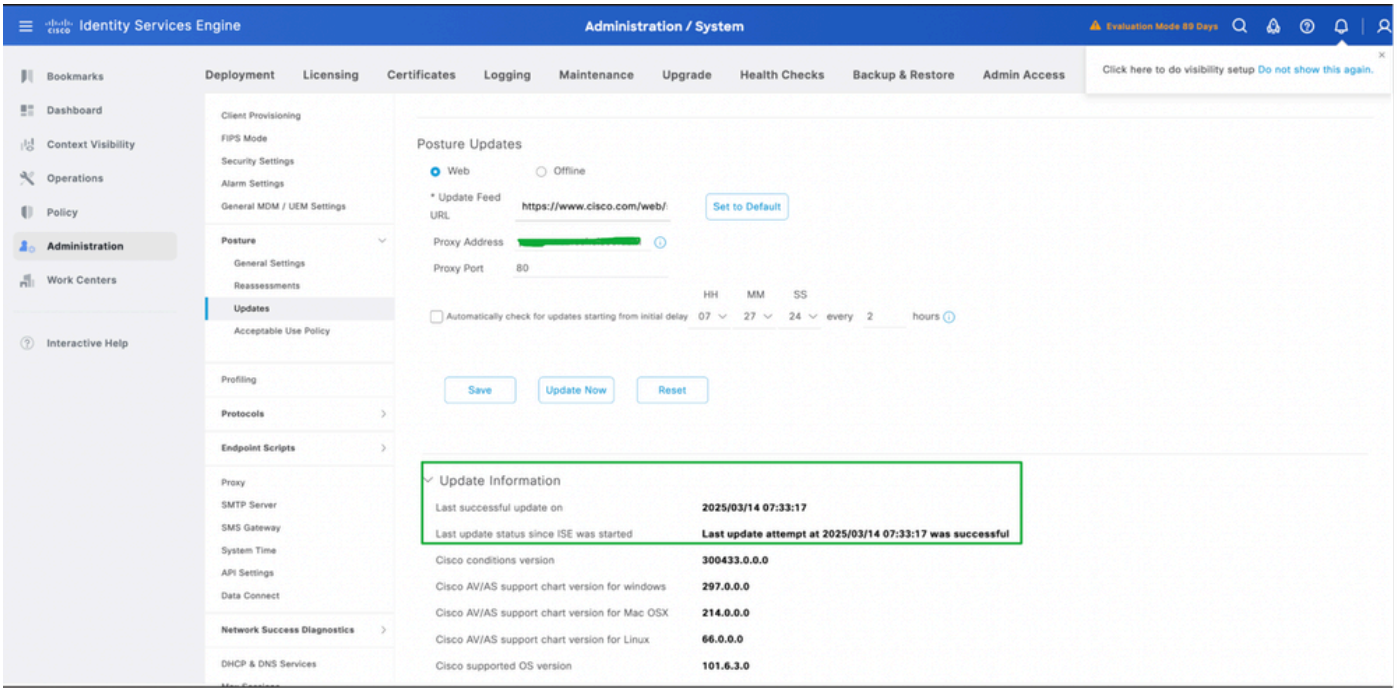
2. Seleccione el método como Web para las actualizaciones de estado en línea, haga clic en Actualizar ahora.



3. Una vez iniciadas las actualizaciones de estado, el estado cambiaría a Actualización.



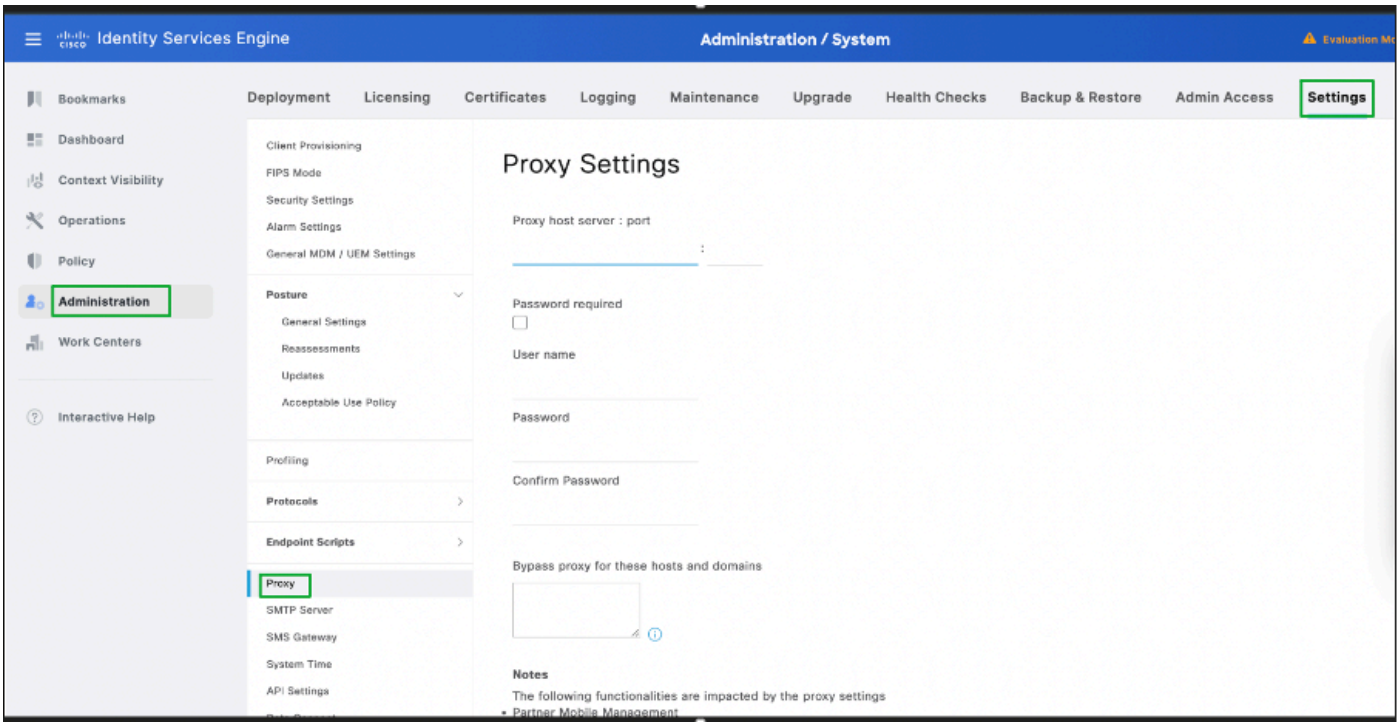
4. El estado de las actualizaciones de postura se puede verificar desde la información de actualización según esta captura de pantalla:



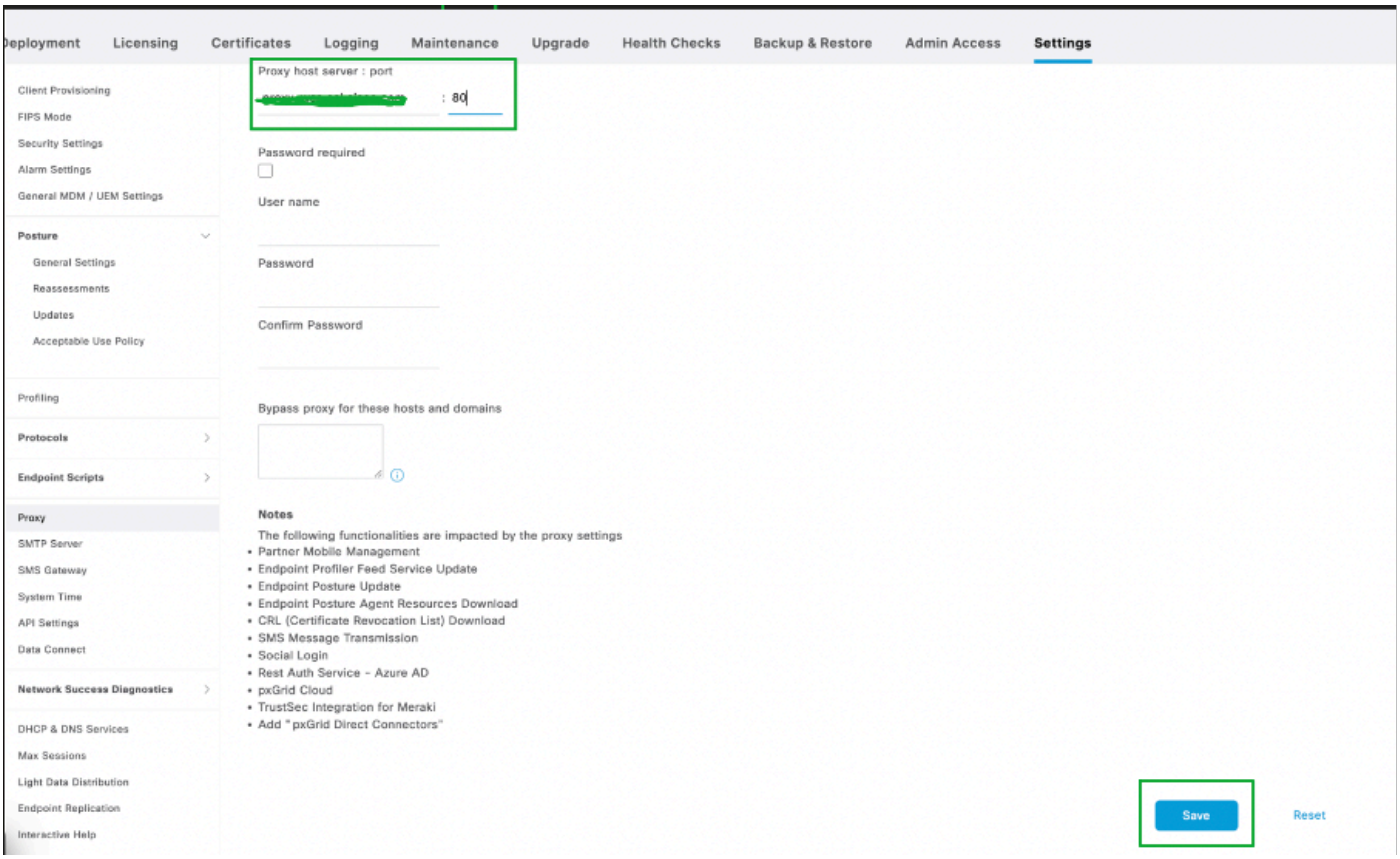
Configuración de proxy para actualizaciones de estado en línea

En un entorno restringido en el que no se puede acceder a la URL del campo Actualización de estado, en ese caso se requiere la configuración de proxy. Consulte Configuración de proxy en ISE.

1. Vaya a Administración -> Sistema -> Configuración -> Proxy.



2. Configure los detalles del proxy y haga clic en Guardar.



3. ISE recuperará automáticamente los detalles del proxy cuando se realicen las actualizaciones de estado en línea.

Actualizaciones de estado sin conexión

Una actualización de estado sin conexión permite cargar manualmente archivos de actualización de estado (en forma de .zip u otro formato de archivo compatible) en ISE.

¿Qué ocurre cuando se realiza una actualización de estado sin conexión?

- Los archivos de estado actualizados se cargan manualmente.
- ISE procesa y aplica estos archivos, que pueden incluir políticas actualizadas, definiciones de antivirus, evaluaciones de estado, entre otros tipos de archivos.
- La actualización sin conexión no requiere conectividad a Internet y se suele utilizar en entornos con políticas de red o de seguridad estrictas que impiden el acceso directo a servidores externos.

Cuándo se debe utilizar

Este método se utiliza a menudo en entornos en los que el sistema está aislado de Internet o cuando tiene archivos de actualización sin conexión específicos proporcionados por Cisco o su equipo de seguridad.

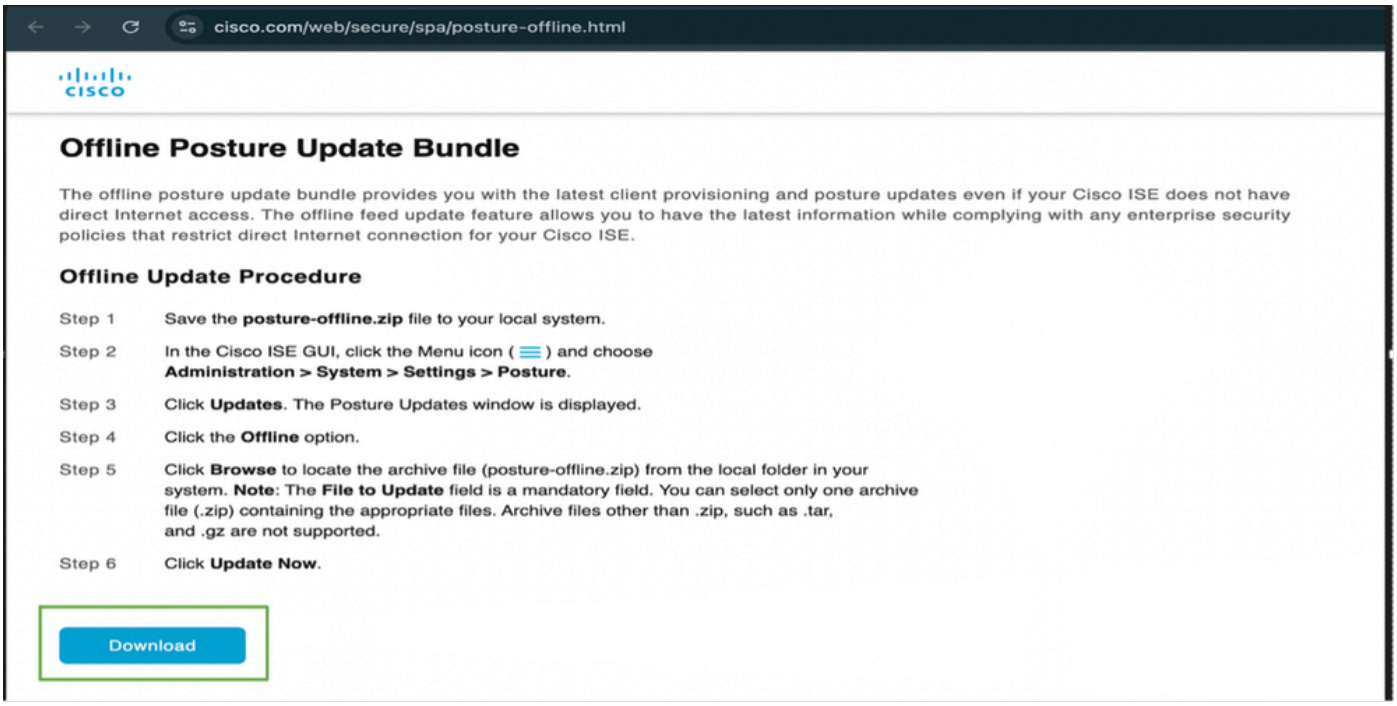
Puertos utilizados para actualizaciones de estado sin conexión

Para la comunicación general con el servidor ISE (durante el proceso de actualización), en muchos casos, estos puertos son relevantes:

1. Acceso a la gestión (puertos 22 y 443):
    - SSH (TCP 2): Si utiliza SSH para acceder al sistema ISE para la resolución de problemas o la carga manual.
    - HTTPS (TCP 443): Si utiliza la GUI (interfaz web) para la carga de la actualización.
2. Transferencia de archivos (SFTP o SCP):
    - Si necesita cargar archivos manualmente en ISE a través de SFTP o SCP, asegúrese de que los puertos correspondientes (normalmente el puerto 22 para SSH/SFTP) estén abiertos en el sistema ISE.
3. Acceso a red local:
    - Asegúrese de que el sistema desde el que está cargando la actualización (por ejemplo, una estación de trabajo de administración o un servidor) pueda comunicarse con ISE a través de los puertos necesarios para el acceso a la gestión, pero, de nuevo, las actualizaciones de estado sin conexión no requieren ningún puerto externo, ya que los archivos se proporcionan manualmente.

¿Dónde buscar archivos para actualizaciones de estado sin conexión?

1. Vaya a la URL: https://www.cisco.com/web/secure/spa/posture-offline.html , haga clic en Descargar y el archivo posture-offline.zip se descargará en su sistema local.

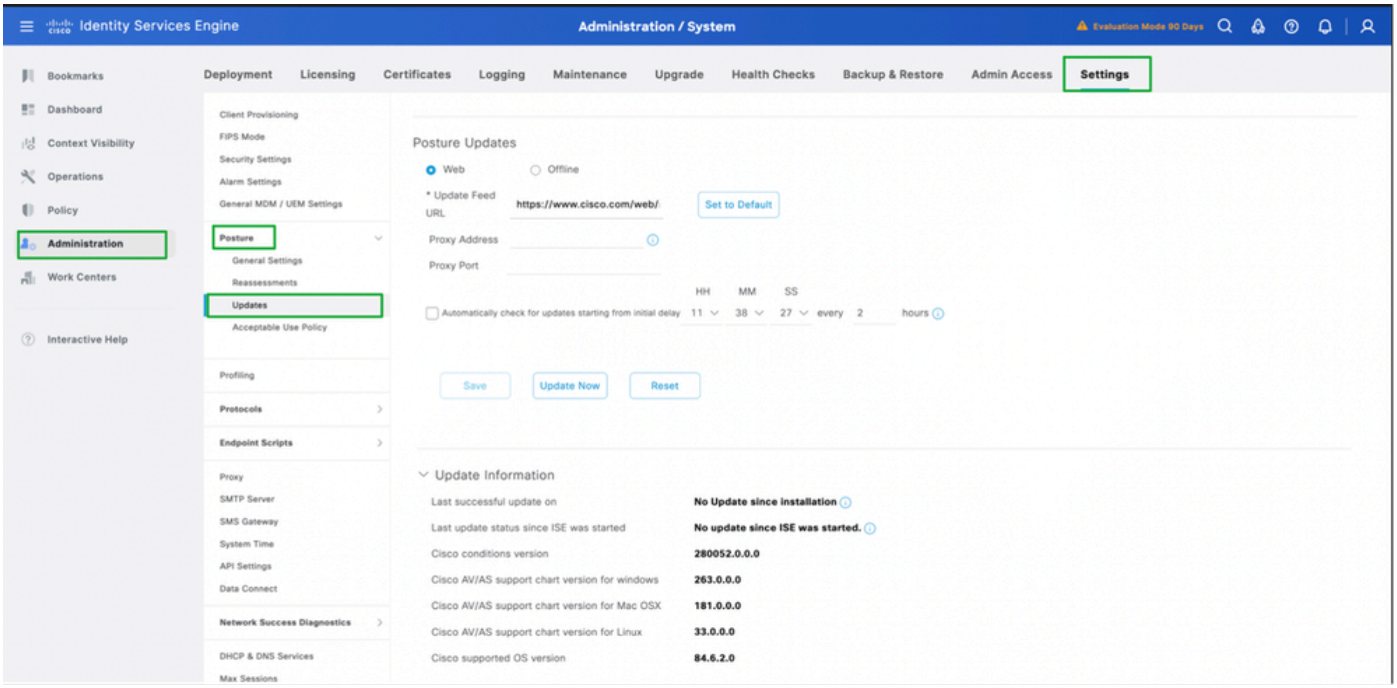


Incluir archivos de actualización de estado sin conexión

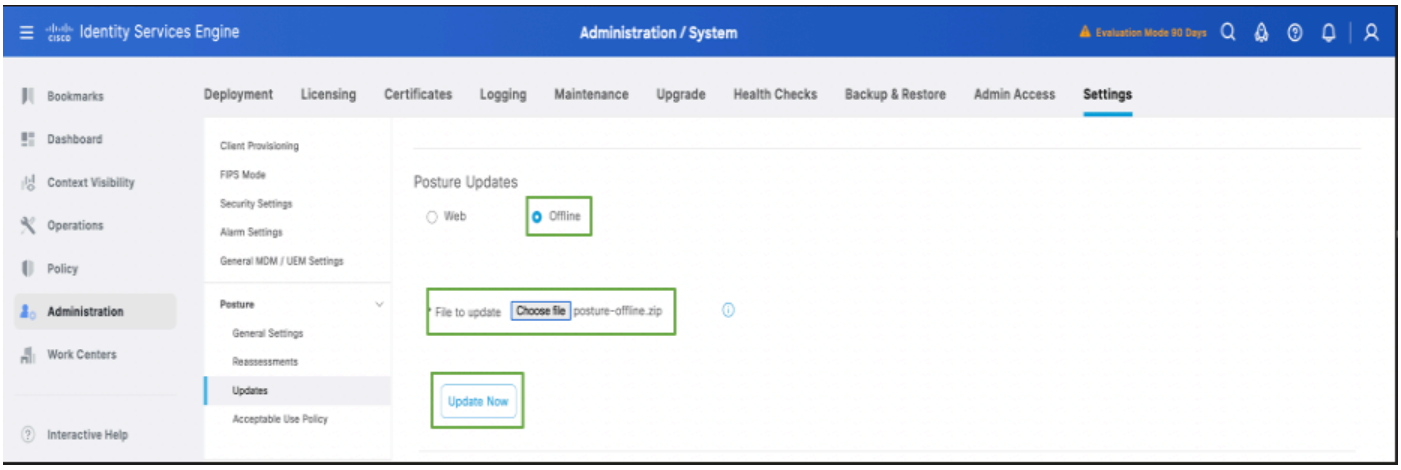
- Definiciones de antivirus (firmas).
- Políticas y reglas de estado.
- Evaluaciones de seguridad y otros archivos de configuración para la evaluación del estado.

Procedimiento para realizar actualizaciones de estado sin conexión

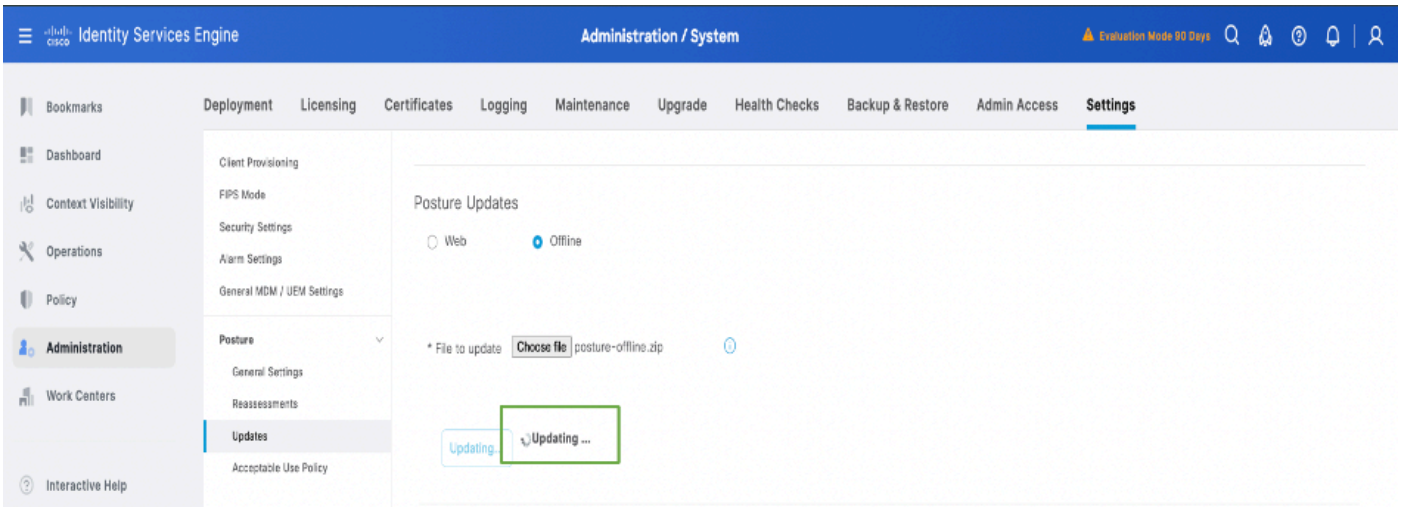
1. Inicie sesión en la GUI de ISE -> Administración -> Sistema -> Configuración -> Estado -> Actualizaciones.

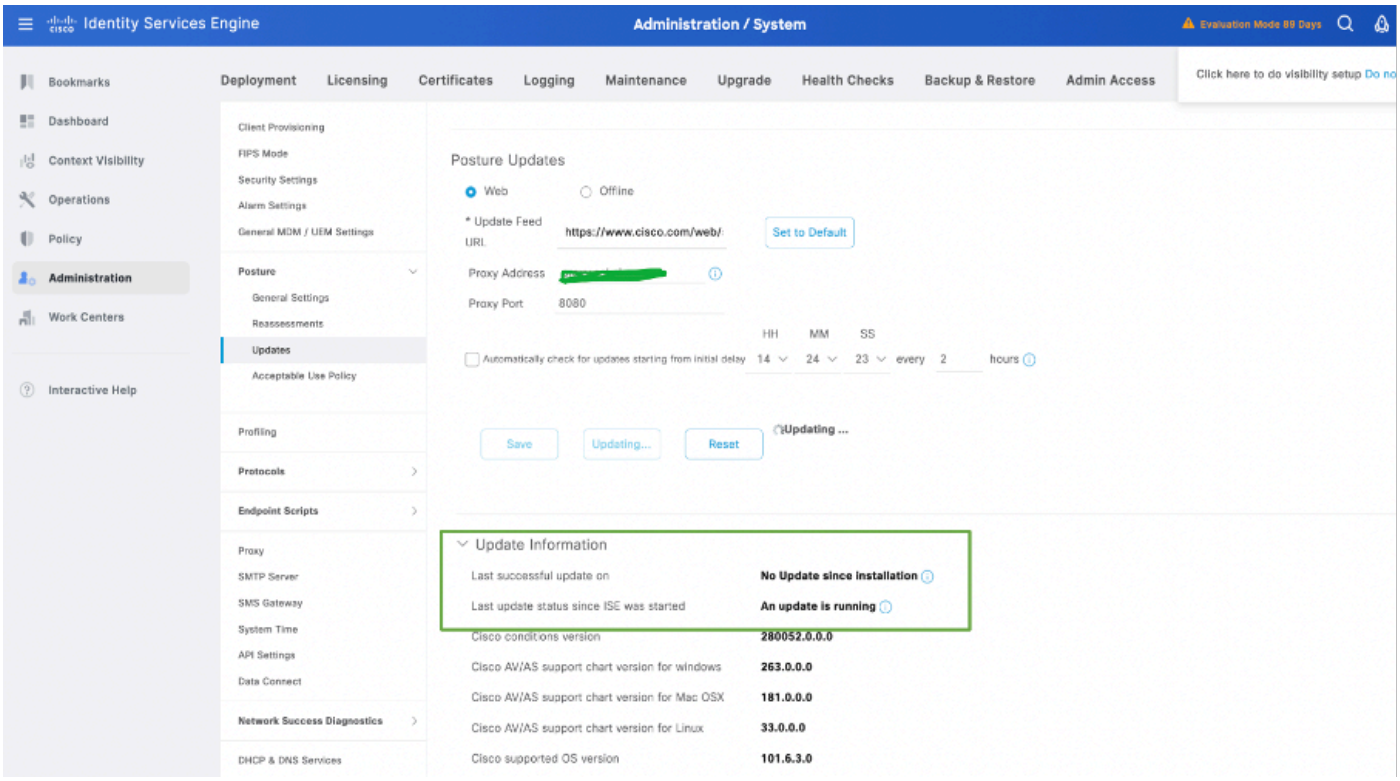


2. Seleccione la opción offline, navegue y seleccione la carpeta posture-offline.zip que se descargó a su sistema local. Haga clic en Update Now.

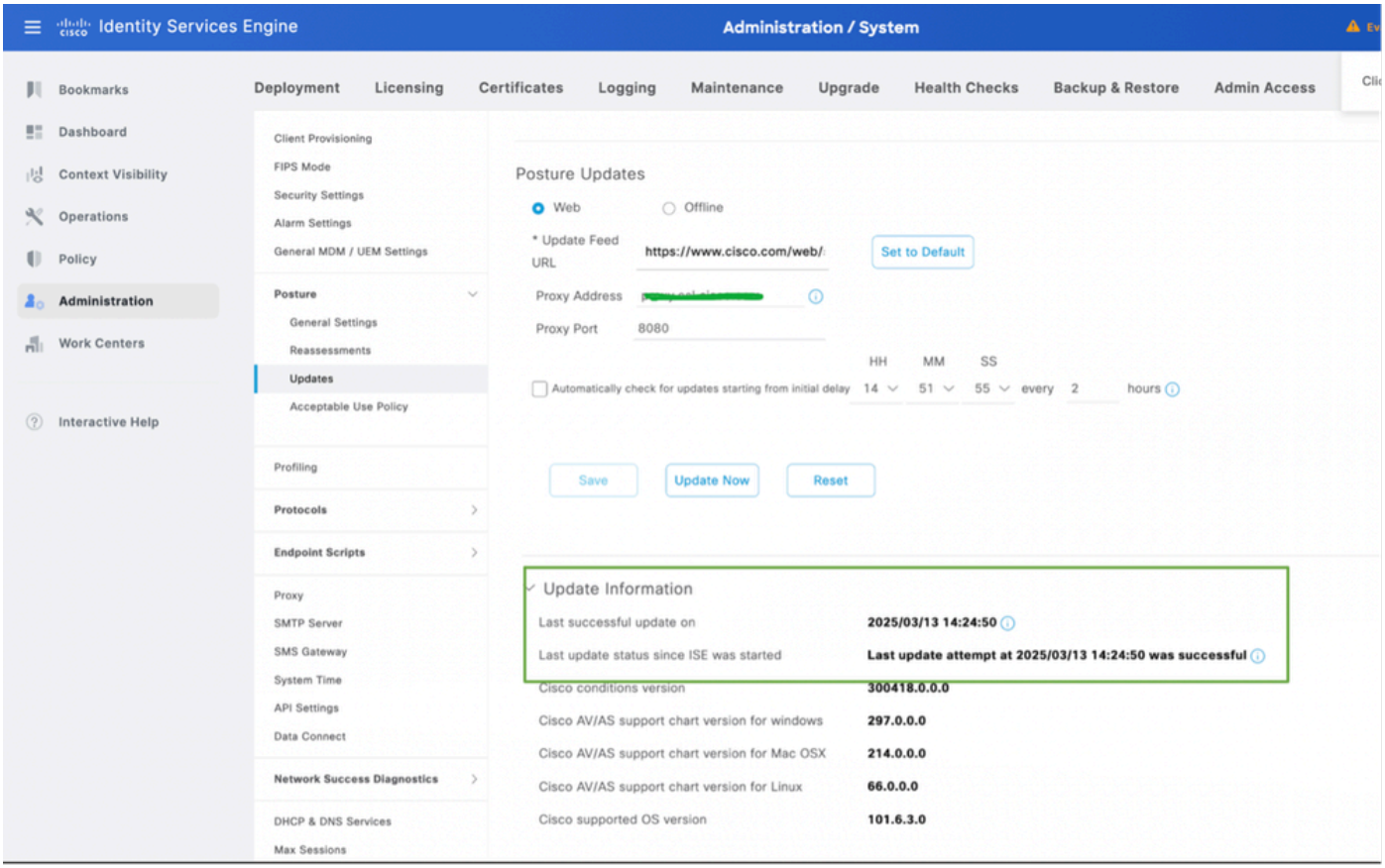


3. Una vez iniciadas las actualizaciones de estado, el estado cambiaría a Actualización.





4. El estado de las actualizaciones de postura se puede verificar desde la información de actualización según esta captura de pantalla:



Verificación

Inicie sesión en la GUI del nodo de administración principal -> Operaciones -> Resolución de problemas -> Registros de descarga -> Registros de depuración -> Registros de aplicación -> isc-psc.log , haga clic en ise-psc.log y el registro se descargará al sistema local. Abra el archivo descargado a través del Bloc de notas o el editor de texto, y filtre para la descarga de Opswat. Debe poder encontrar la información relacionada con las actualizaciones de estado que se están realizando en la implementación.

También puede seguir los registros registrándolos en la CLI del nodo de administración principal mediante el comando show logging application ise-psc.log tail.

Se inicia la descarga de Opswat, que hace referencia a las actualizaciones de estado:

2025-03-13 13:58:07,246 INFO [admin-http-pool5][[]] cisco.cpm.posture.download.DownloadManager -::admin:::- Iniciando descarga de opswat

2025-03-13 13:58:07,251 INFO [admin-http-pool5][[]] cisco.cpm.posture.download.DownloadManager -::admin:::- URI de archivo de descarga sin conexión : /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 de archivo de descarga sin conexión : /opt/CSCOcpm/temp/cp/update/5c064701-a1ee-4a09-a190-3bf83c190af6/osgroups.tar.gz

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

Se ha completado la descarga de Opswat, refiriéndose a que las actualizaciones de estado se descargan y se realizan correctamente.

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

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

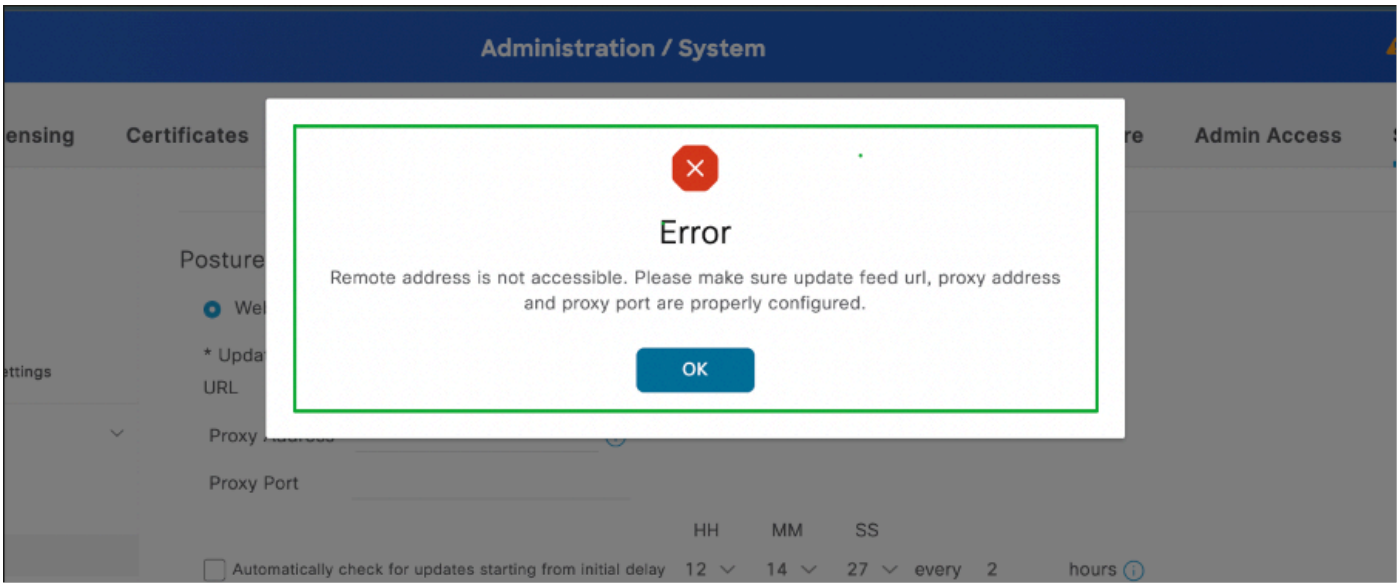
2025-03-13 14:24:50,827 INFO [admin-http-pool5][[]] mnt.dbms.datadirect.impl.DatadirectServiceImpl -::admin::- Ejecución de getStatus - datadirectSettings

Troubleshoot

Situación

Error en las actualizaciones de estado en línea: "No se puede acceder a la dirección remota. Asegúrese de que la dirección URL de la fuente de actualización, la dirección proxy y el puerto proxy están configurados correctamente."

Ejemplo de error:



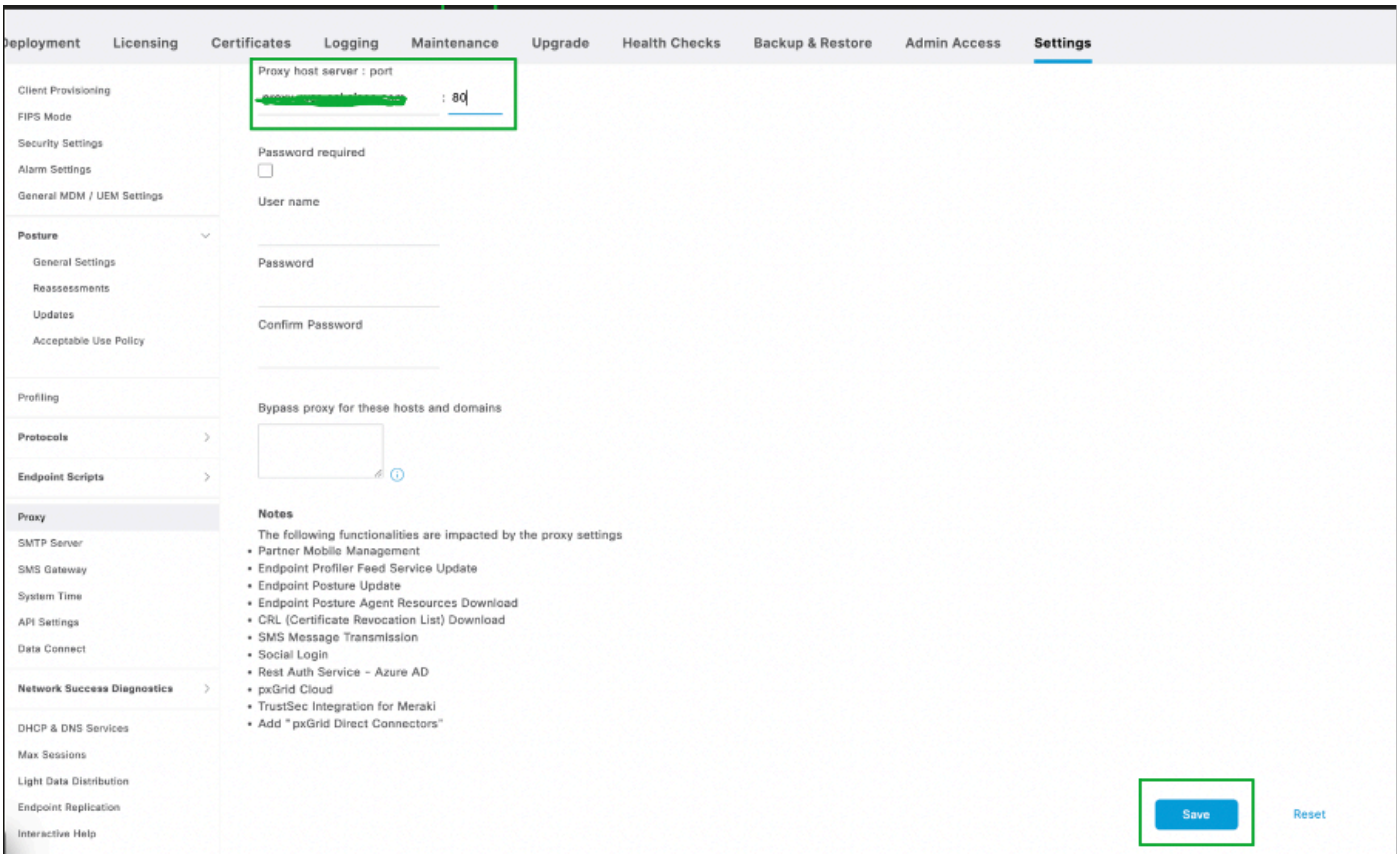
Solución

1. Inicie sesión en la CLI de ISE y compruebe que ISE está disponible en cisco.com mediante el comando "ping cisco.com".

isehostname/admin#ping cisco.com
PING cisco.com (72.163.4.161) 56(84) bytes de datos.
64 bytes de 72.163.4.161: icmp_seq=1 ttl=235 tiempo=238 ms
64 bytes de 72.163.4.161: icmp_seq=2 ttl=235 tiempo=238 ms
64 bytes de 72.163.4.161: icmp_seq=3 ttl=235 tiempo=239 ms
64 bytes de 72.163.4.161: icmp_seq=4 ttl=235 tiempo=238 ms

— cisco.com ping statistics —
4 paquetes transmitidos, 4 recibidos, 0% de pérdida de paquetes, tiempo 3004 ms
rtt min/avg/max/mdev = 238,180/238,424/238,766/0,410 ms

2. Vaya a Administration -> System -> Settings -> El proxy está configurado con los puertos adecuados.



3. Verifique si los puertos TCP 443, UDP 53 y UDP 123 están permitidos en todos los saltos a Internet.

Defectos conocidos para problemas de actualización de estado

ID de bug de Cisco 01523

Referencia

- Guía del administrador de Cisco Identity Services Engine, versión 3.3

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).