Aprovisione Secure Firewall ASA a CSM

Contenido

Introducción

Prerequisites

- Requirements
- Componentes Utilizados

Antecedentes

Configurar

- Configuraciones
  - Configuración de ASA para la gestión de HTTPS
  - Aprovisione Secure Firewall ASA a CSM

Verificación

Introducción

En este documento se describe el proceso para aprovisionar el dispositivo de seguridad adaptable (ASA) de firewall seguro en Cisco Security Manager (CSM).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- ASA de firewall seguro
- CSM

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Secure Firewall ASA versión 9.18.3
- CSM versión 4.28

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

CSM ayuda a habilitar la aplicación de políticas uniformes y la rápida resolución de problemas de eventos de seguridad, ofreciendo informes resumidos a lo largo de la implementación de seguridad. Gracias a su interfaz centralizada, las organizaciones pueden ampliar de forma eficiente y gestionar una amplia gama de dispositivos de seguridad de Cisco con una visibilidad mejorada.

Configurar

En el siguiente ejemplo, se aprovisiona un ASA virtual a un CSM para una gestión centralizada.

Configuraciones

Configuración de ASA para la gestión de HTTPS

Paso 1. Cree un usuario con todos los privilegios.

Sintaxis de la línea de comandos (CLI):

```
configure terminal
username < user string > password < password > privilege < level number >
```

Esto se traduce en el siguiente ejemplo de comando, que tiene el usuario csm-user y la contraseña cisco123 de la siguiente manera:

```
ciscoasa# configure terminal
ciscoasa(config)# username csm-user password cisco123 privilege 15
```

Sugerencia: también se aceptan usuarios autenticados externamente para esta integración.

Paso 2. Habilitar servidor HTTP.

Sintaxis de la línea de comandos (CLI):

```
configure terminal
http server enable
```

Paso 3. Permitir el acceso HTTPS para la dirección IP del servidor CSM.

Sintaxis de la línea de comandos (CLI):

```
configure terminal
http < hostname > < netmask > < interface name >
```

Esto se traduce en el siguiente ejemplo de comando, que permite que cualquier red acceda al ASA a través de HTTPS en la interfaz externa (GigabitEthernet0/0):

```
ciscoasa# configure terminal
ciscoasa(config)# http 0.0.0.0 0.0.0.0 outside
```

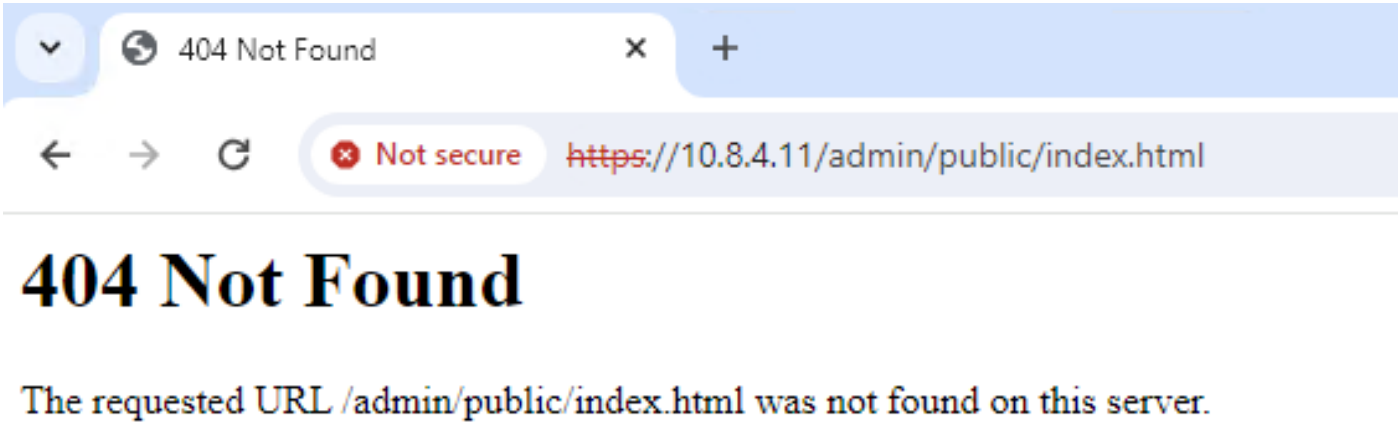
Paso 4. Valide que se puede alcanzar HTTPS desde el servidor CSM.

Abra cualquier explorador Web y escriba la siguiente sintaxis:

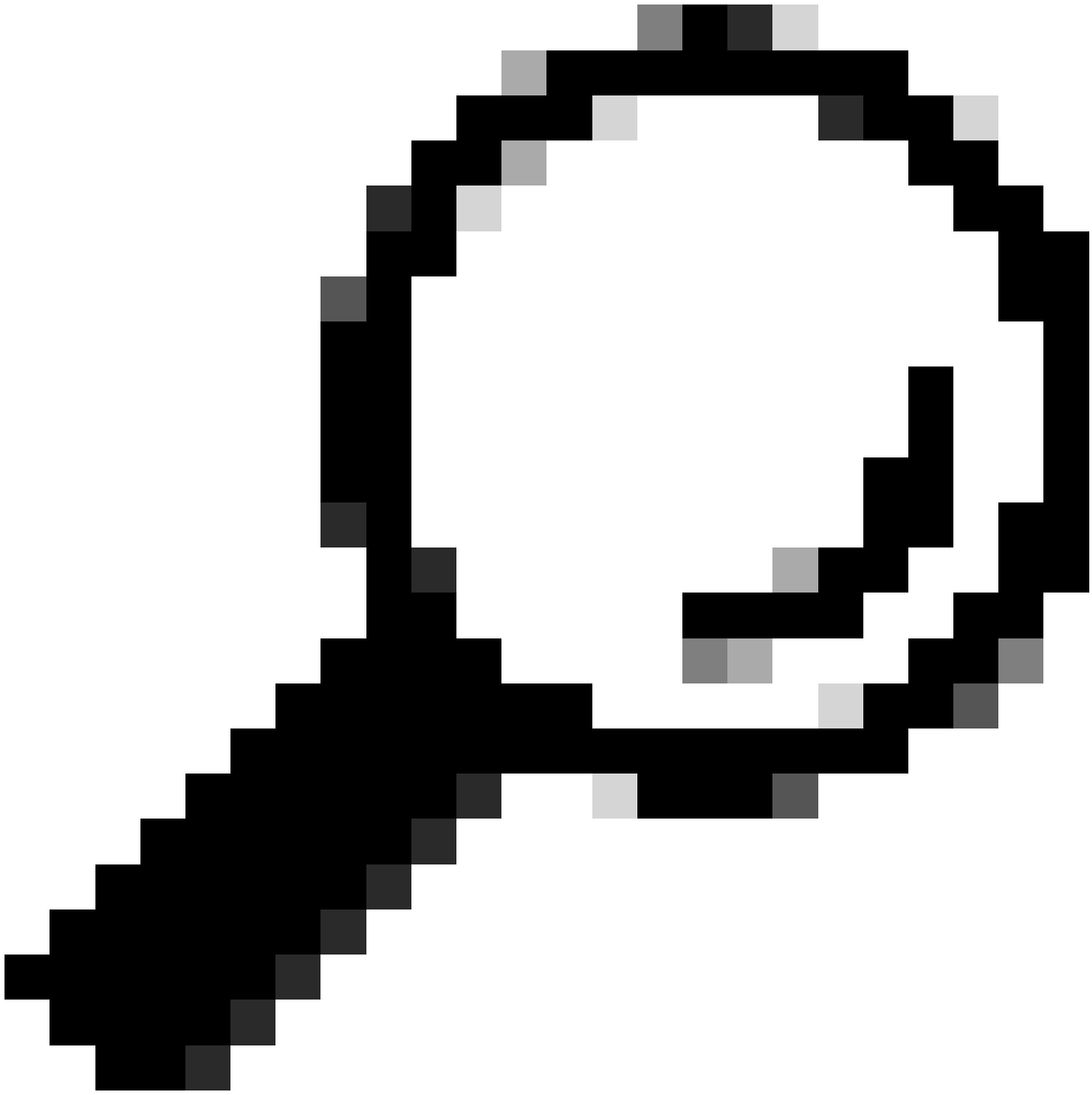
```
https://< ASA IP address >/
```

Esto se traduce en el siguiente ejemplo para la dirección IP de la interfaz externa que se permitió para el acceso HTTPS en el paso anterior:

```
https://10.8.4.11/
```



Respuesta HTTPS de ASA



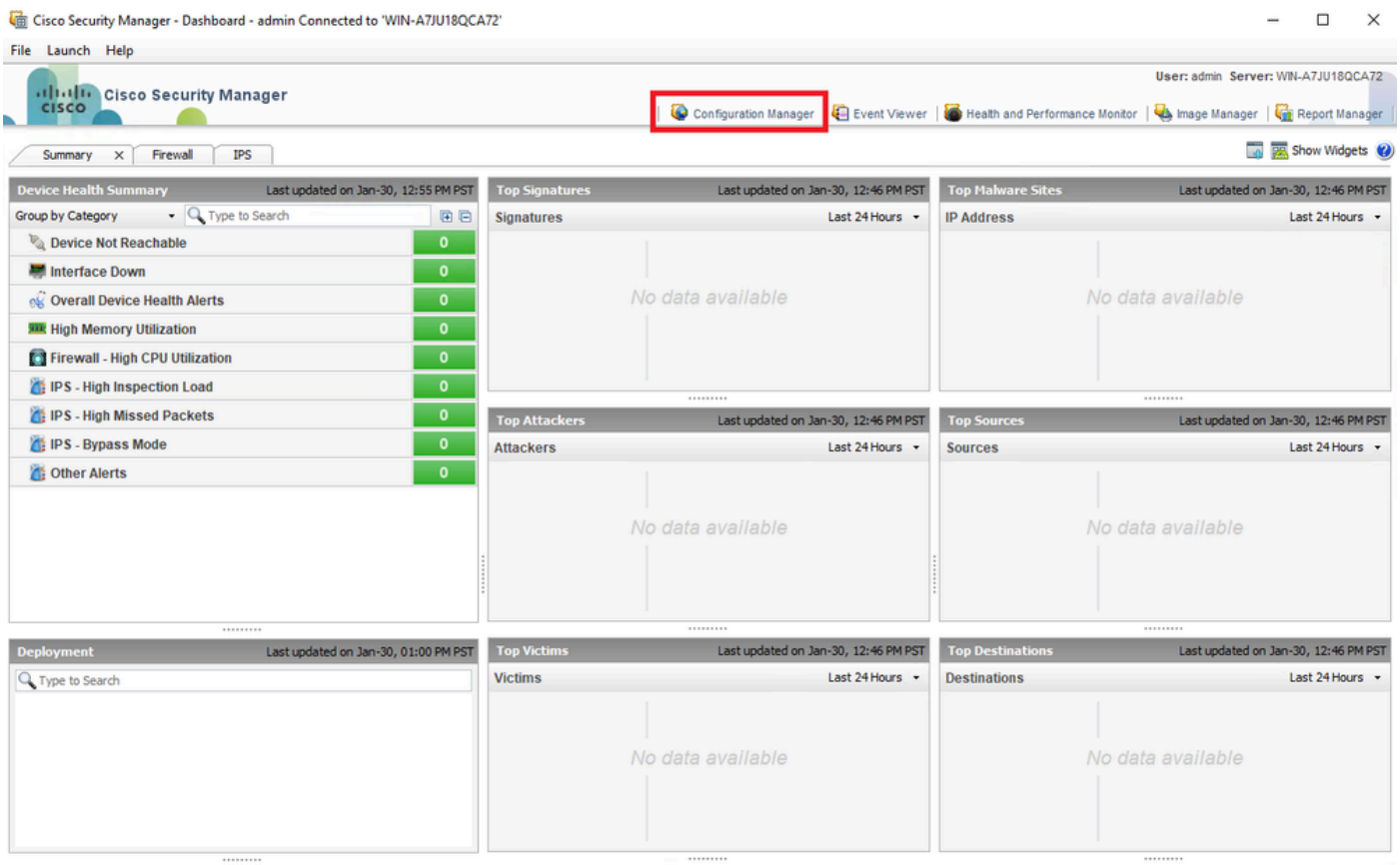
Consejo: Error 404 Not Found se espera en este paso, ya que este ASA no tiene el Cisco Adaptive Security Device Manager (ASDM) instalado, pero la respuesta HTTPS está ahí, ya que la página se redirige a la URL /admin/public/index.html.

Aprovisione Secure Firewall ASA a CSM

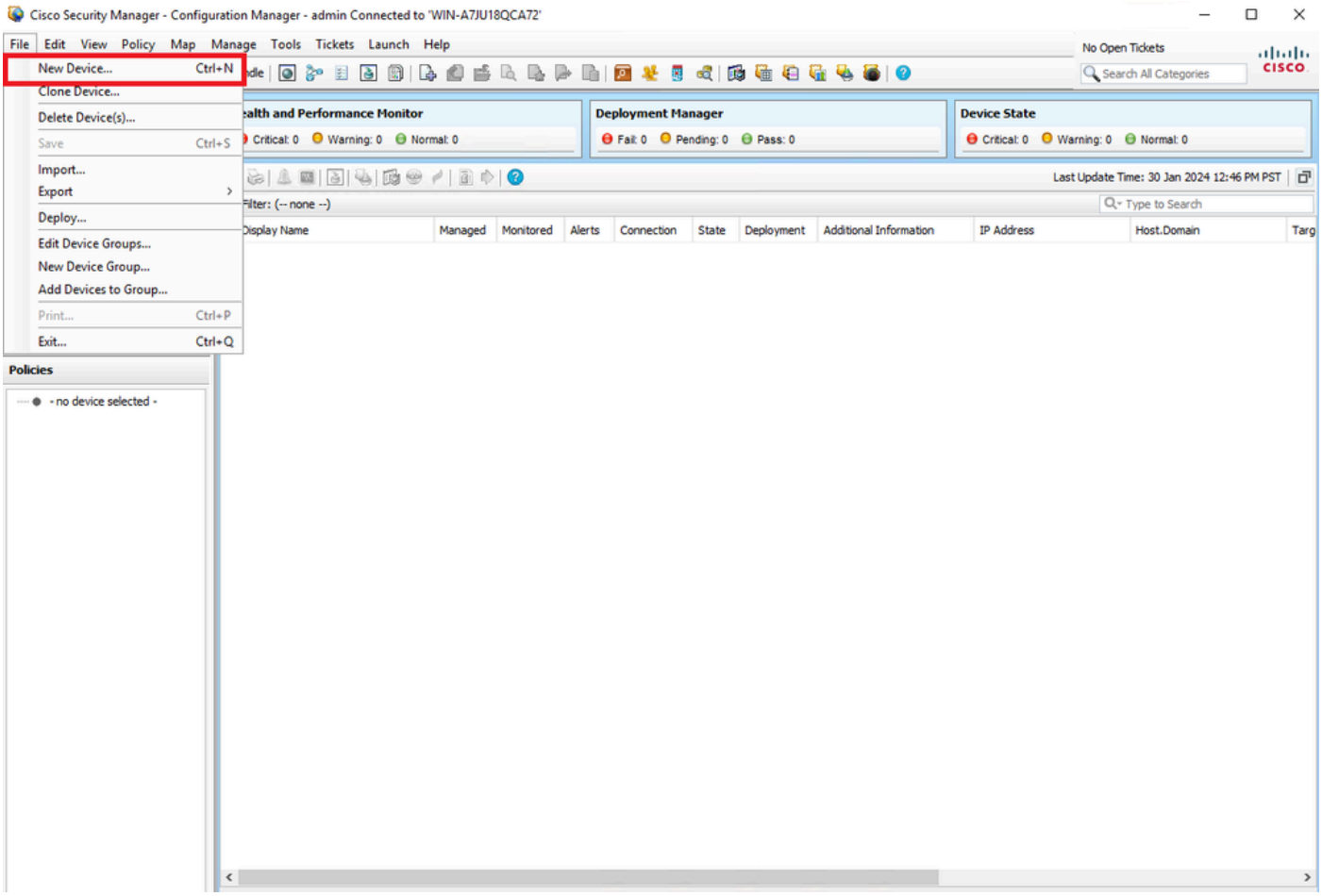
Paso 1. Abra e inicie sesión en el cliente CSM.

Inicio de sesión del cliente CSM

Paso 2. Abra el Administrador de configuración.

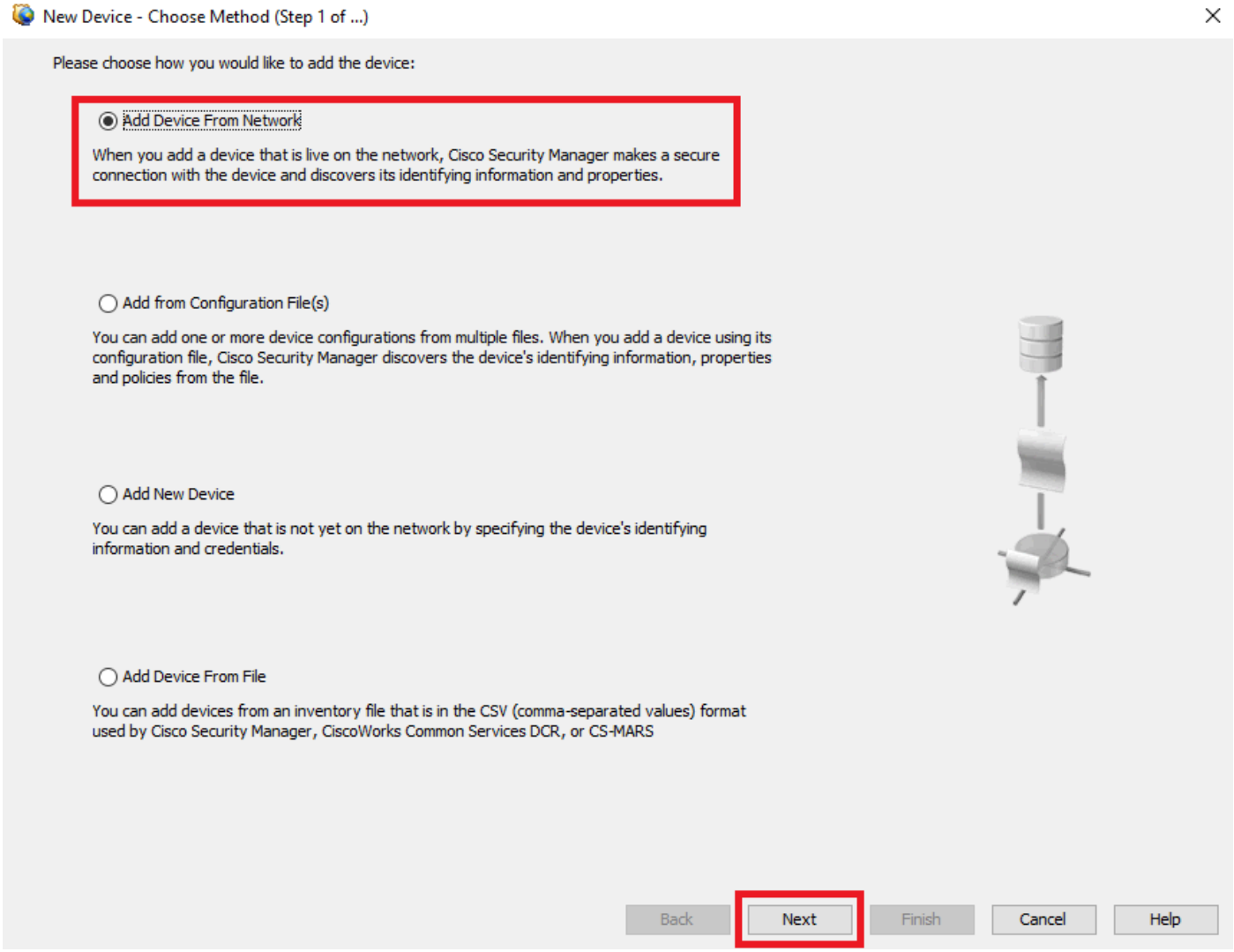


Paso 3. Vaya a Devices > New Device.



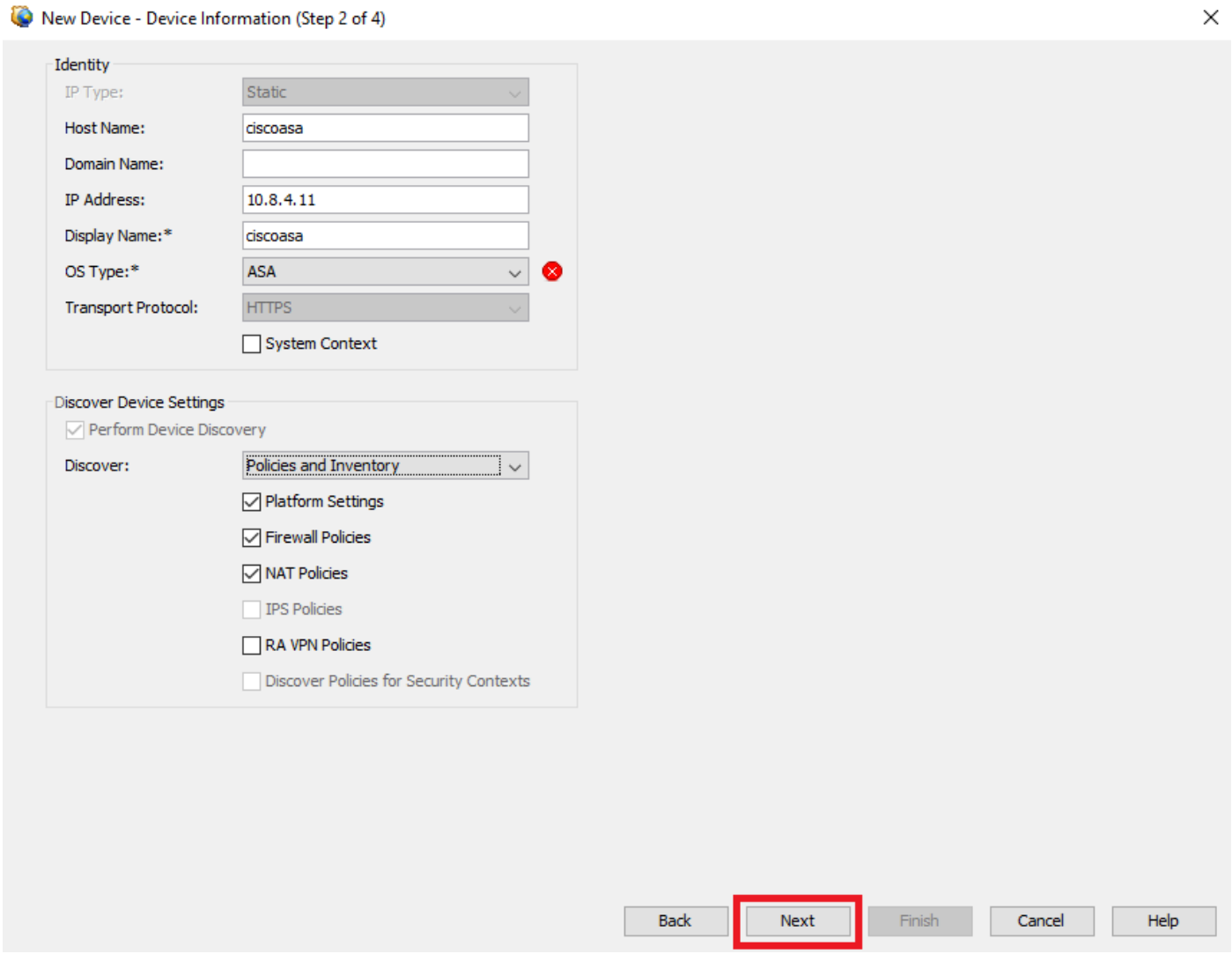
Administrador de configuración CSM

Paso 4. Seleccione la opción de adición que satisfaga el requisito según el resultado deseado. Como el ASA configurado ya está configurado en la red, la mejor opción para este ejemplo es **Add Device From Network** y haga clic en **Next**.



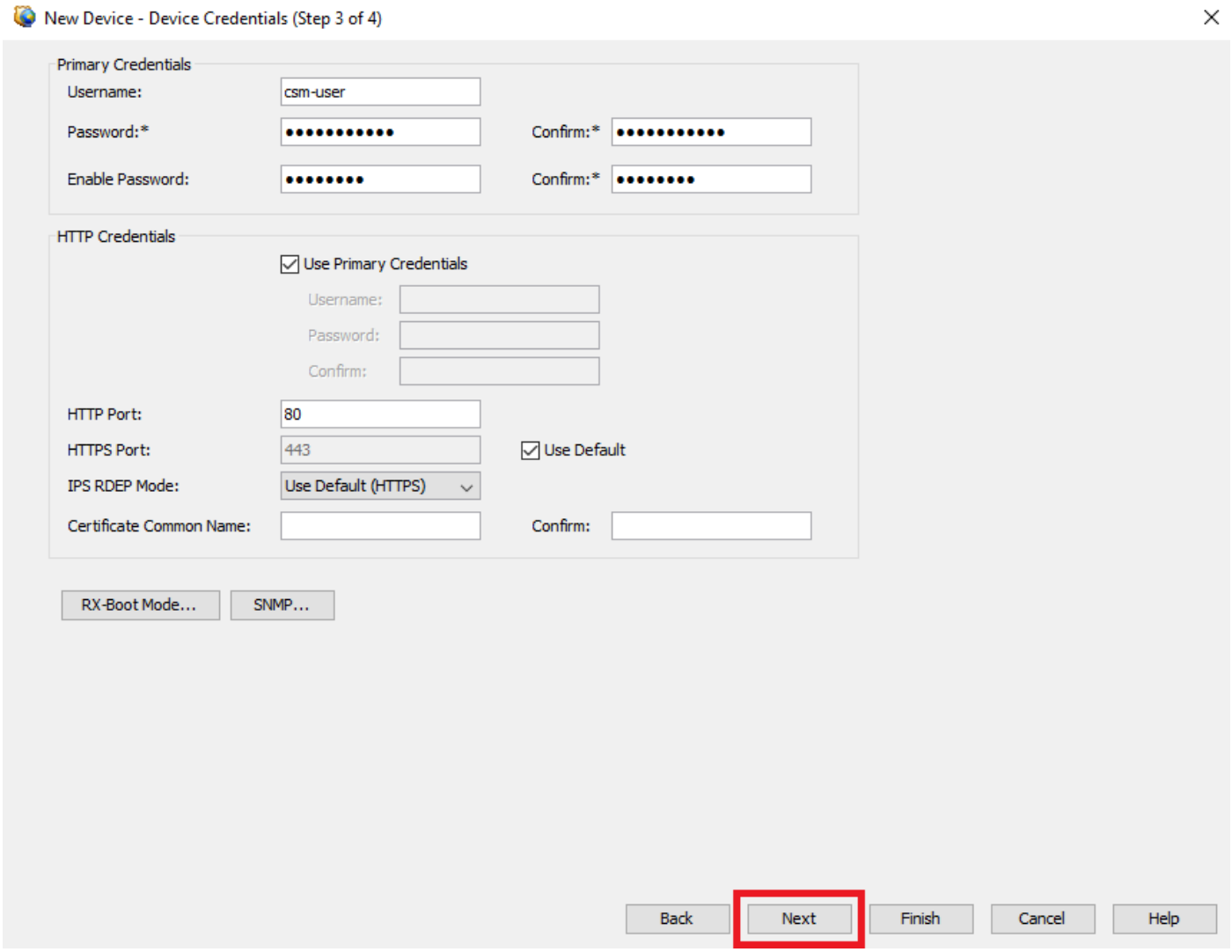
Método Device Add

Paso 5. Complete los datos necesarios según la configuración del ASA de firewall seguro y los parámetros de detección. A continuación, haga clic en **Next**.



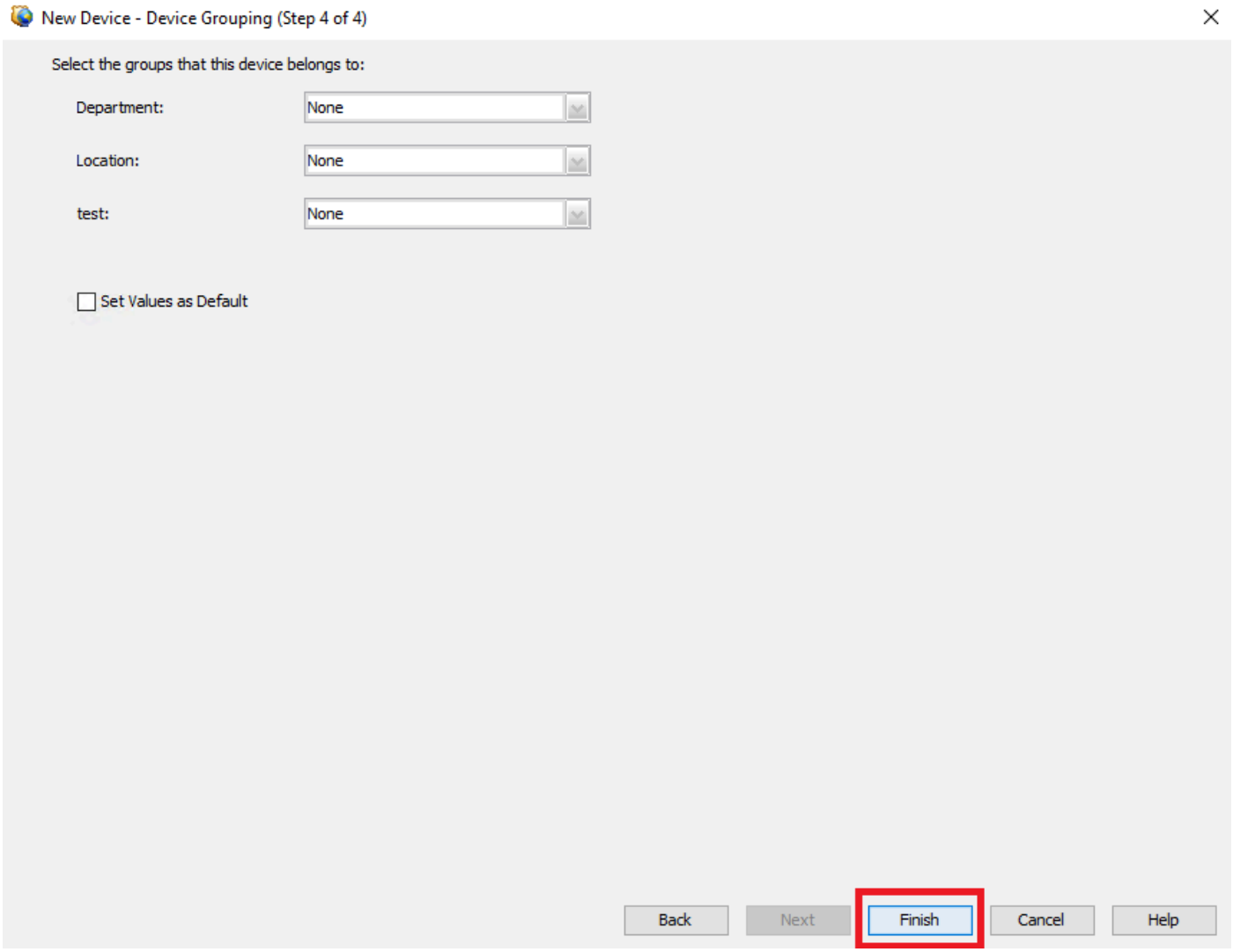
Configuración de ASA

Paso 6. Complete las credenciales requeridas del usuario CSM configurado en ASA y la contraseña **enable**.



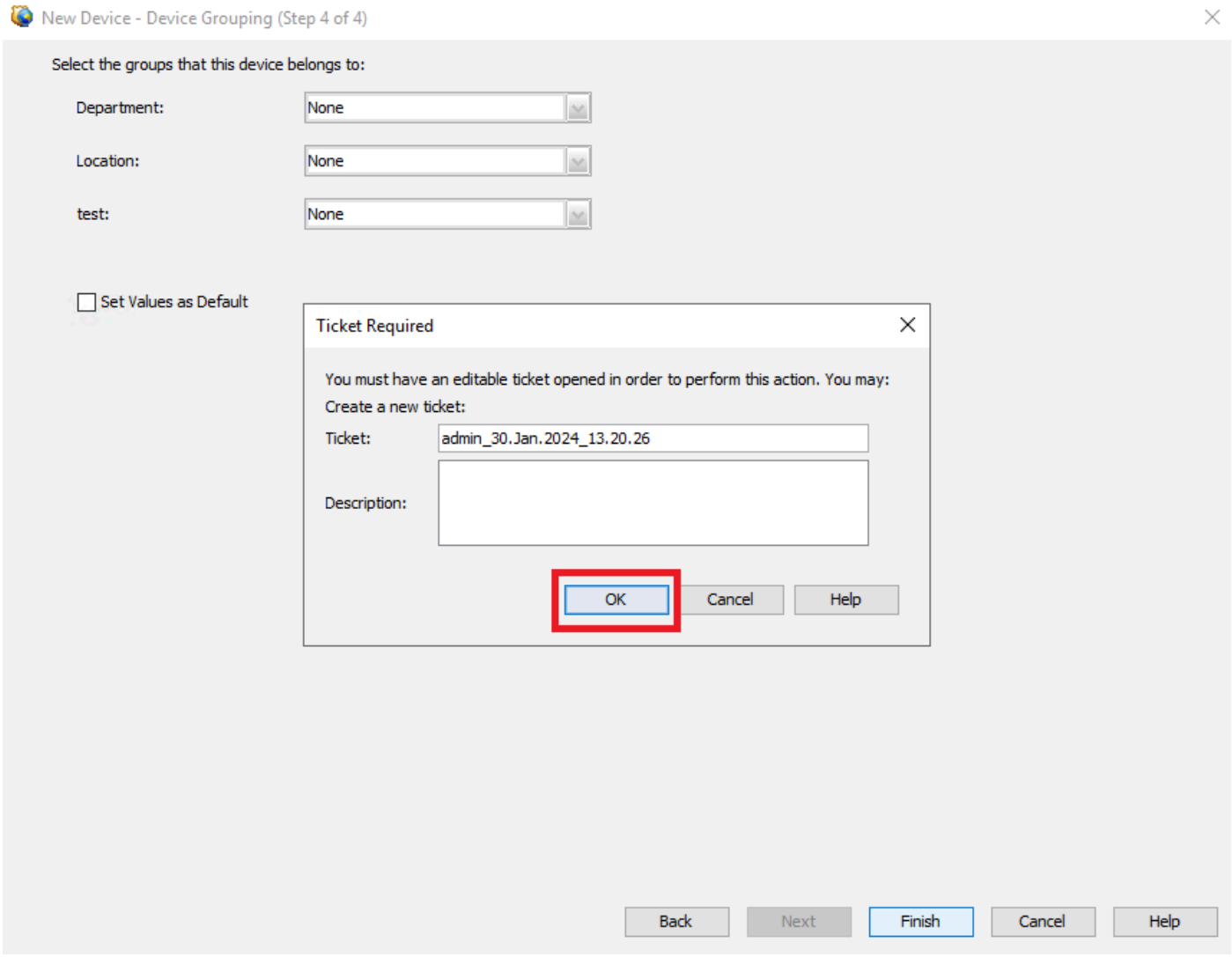
Credenciales de ASA

Paso 7. Seleccione los grupos que desee o omita este paso si no es necesario ninguno y haga clic en **Finish**.



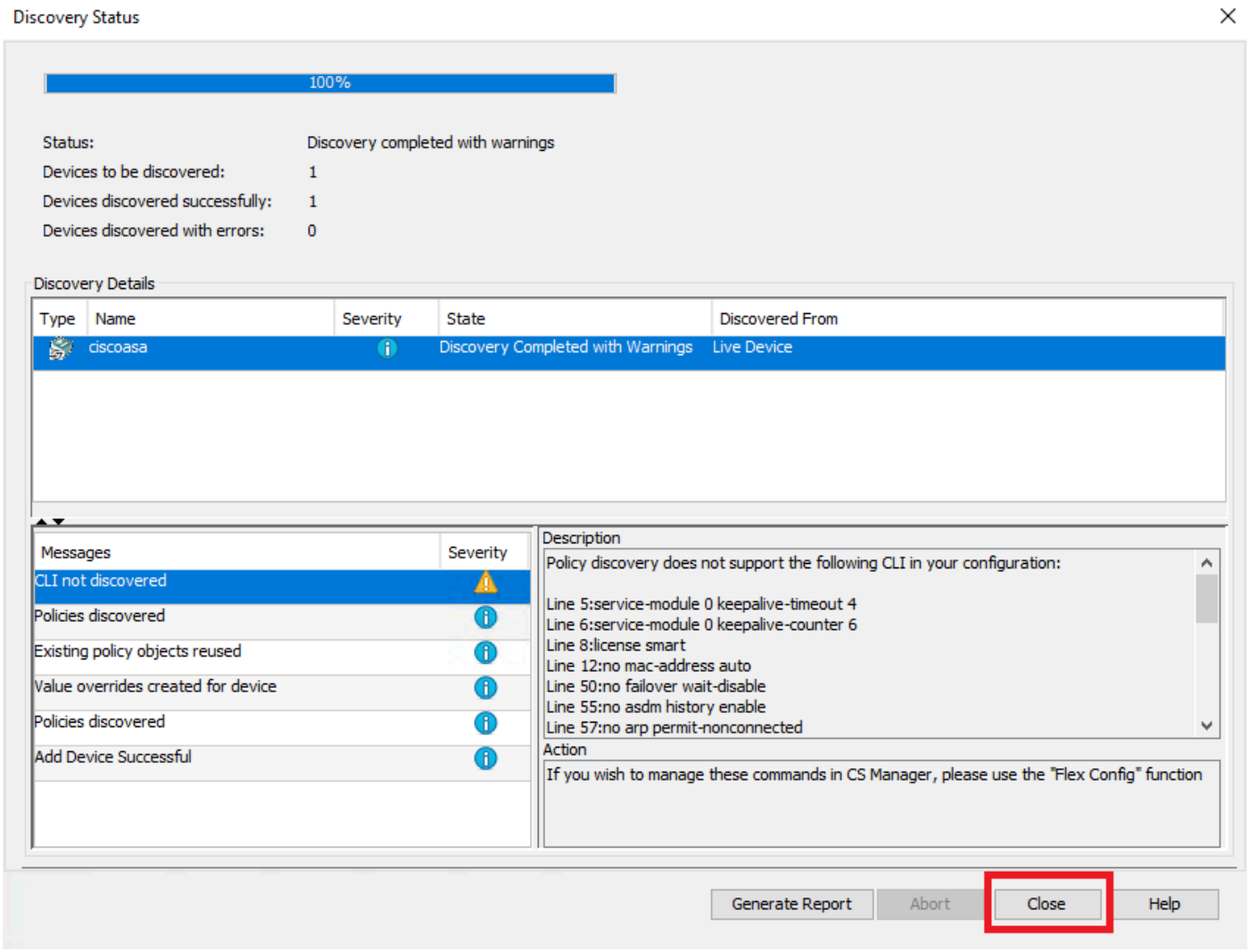
Selección de grupo CSM

Paso 8. Se genera una solicitud de ticket con fines de control, haga clic en **Aceptar**.

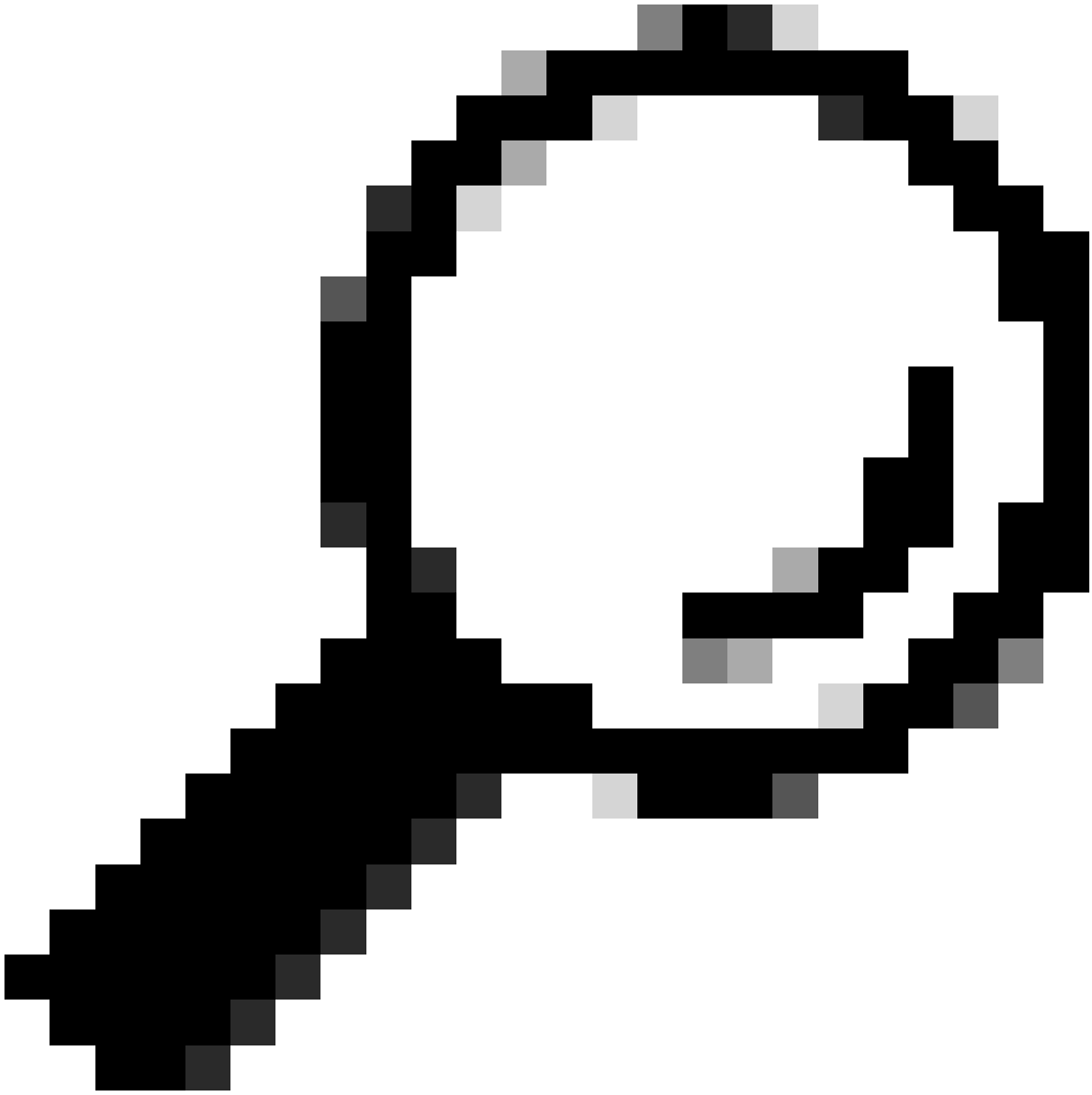


Creación de notificaciones CSM

Paso 9. Valide que la detección finalice sin errores y haga clic en **Cerrar**.

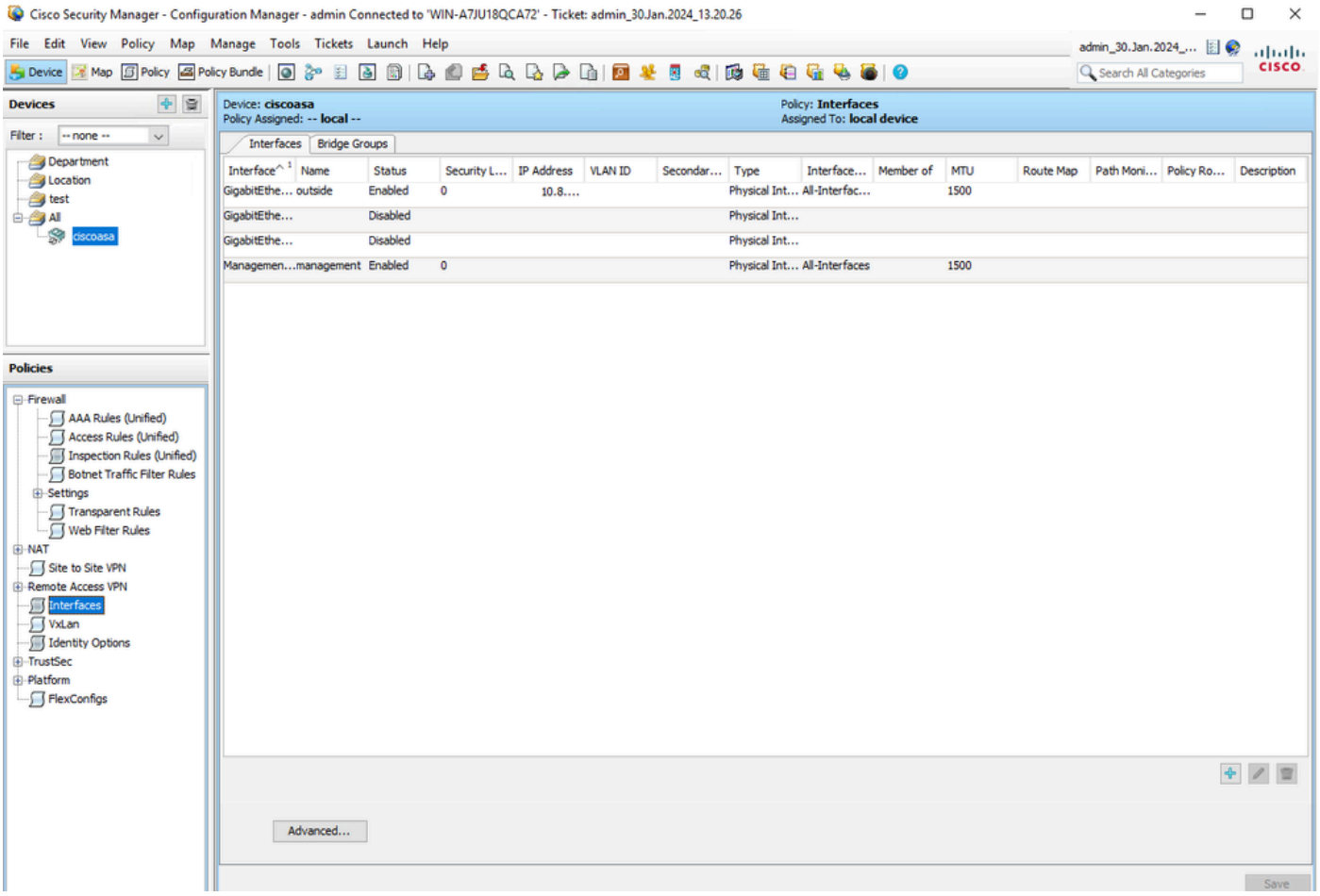


Detección de ASA



Sugerencia: se aceptan advertencias como resultado correcto, ya que no todas las funciones de ASA son compatibles con CSM.

Paso 10. Valide que ASA aparezca ahora como registrado en el cliente CSM y muestre la información correcta.



Información de ASA registrada

Verificación

Un debug HTTPS está disponible en ASA para fines de troubleshooting. Se utiliza el siguiente comando:

```
debug http
```

Este es un ejemplo de una depuración de registro CSM exitosa:

```
ciscoasa# debug http debug http enabled at level 1. ciscoasa# HTTP: processing handoff to legacy admin
```

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).