Integre ISE y SecureX en las instalaciones mediante la orquestación

Contenido

[Introducción](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Configurar](#)
[Diagrama de la red](#)
[Configuraciones](#)
[Configuración de ISE PAN](#)
[Configurar e implementar servidor remoto](#)
[Configuración del destino en SecureX](#)
[Importar el flujo de trabajo desde Cisco Secure GitHub](#)
[Verificación](#)

Introducción

Este documento describe los pasos para integrar Identity Services Engine y SecureX mediante orquestación con un flujo de trabajo de Cisco Secure GitHub.

Prerequisites

Cisco recomienda que tenga conocimientos sobre estos temas:

- Experiencia con la configuración de Cisco ISE
- Conocimientos sobre la API de ISE
- Conocimientos sobre SecureX Orchestration

Requirements

Debe tener Cisco ISE implementado en la red y una cuenta SecureX activa. Los flujos de trabajo de orquestación se activan a través de la extensión del explorador SecureX.

En nuestro ejemplo, el flujo de trabajo que se va a utilizar se importó desde la página de Cisco Secure GitHub, este procedimiento se aplica también a un flujo de trabajo personalizado.

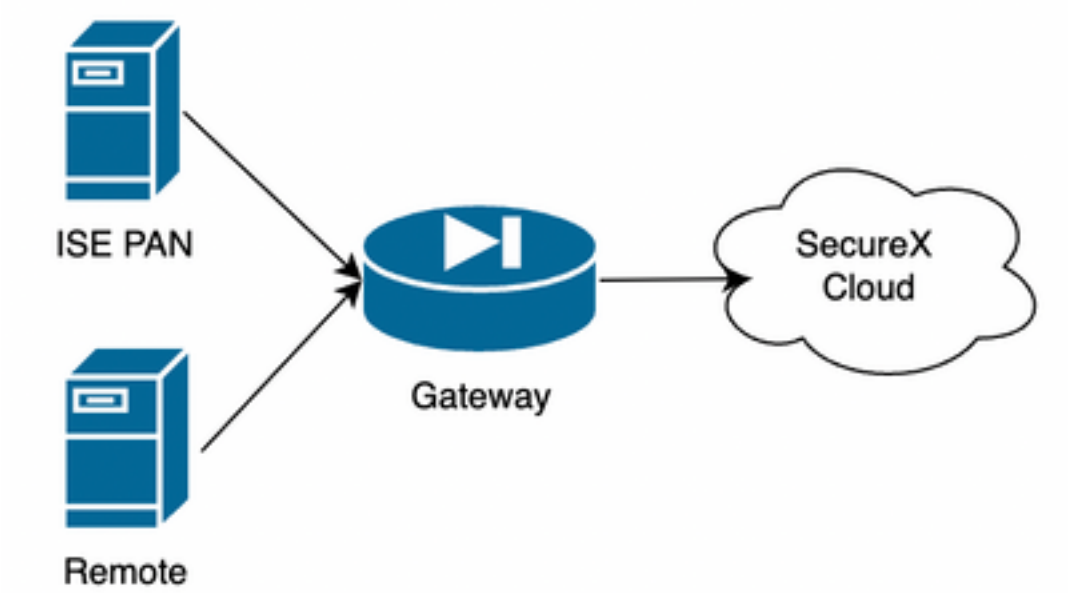
Componentes Utilizados

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

- Identity Services Engine ISE versión 3.1
- cuenta SecureX
- SXO Remote device versión 1.7

Configurar

Diagrama de la red



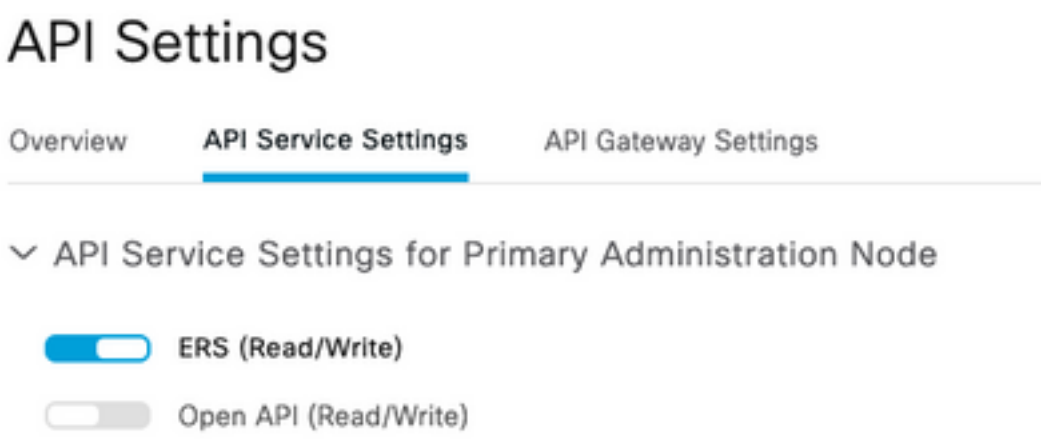
En nuestro ejemplo, ISE PAN y el servidor remoto se colocan en la misma subred para tener conectividad directa.

Dado que ISE es un dispositivo local, el servidor remoto debe estar en contacto con la nube Secure-X y reenviar la información al PAN de ISE

Configuraciones

Configuración de ISE PAN

1. Navegue hasta **Administración > Sistema > Configuración > Configuración de API >Configuración de servicio de API** y habilite **ERS (Lectura/Escritura)**

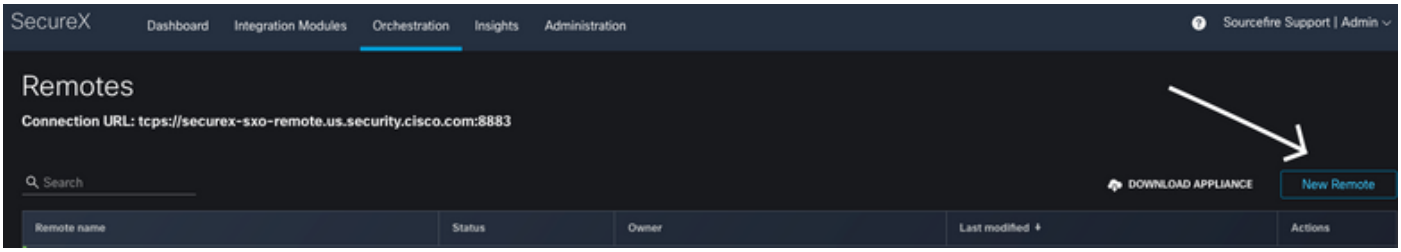


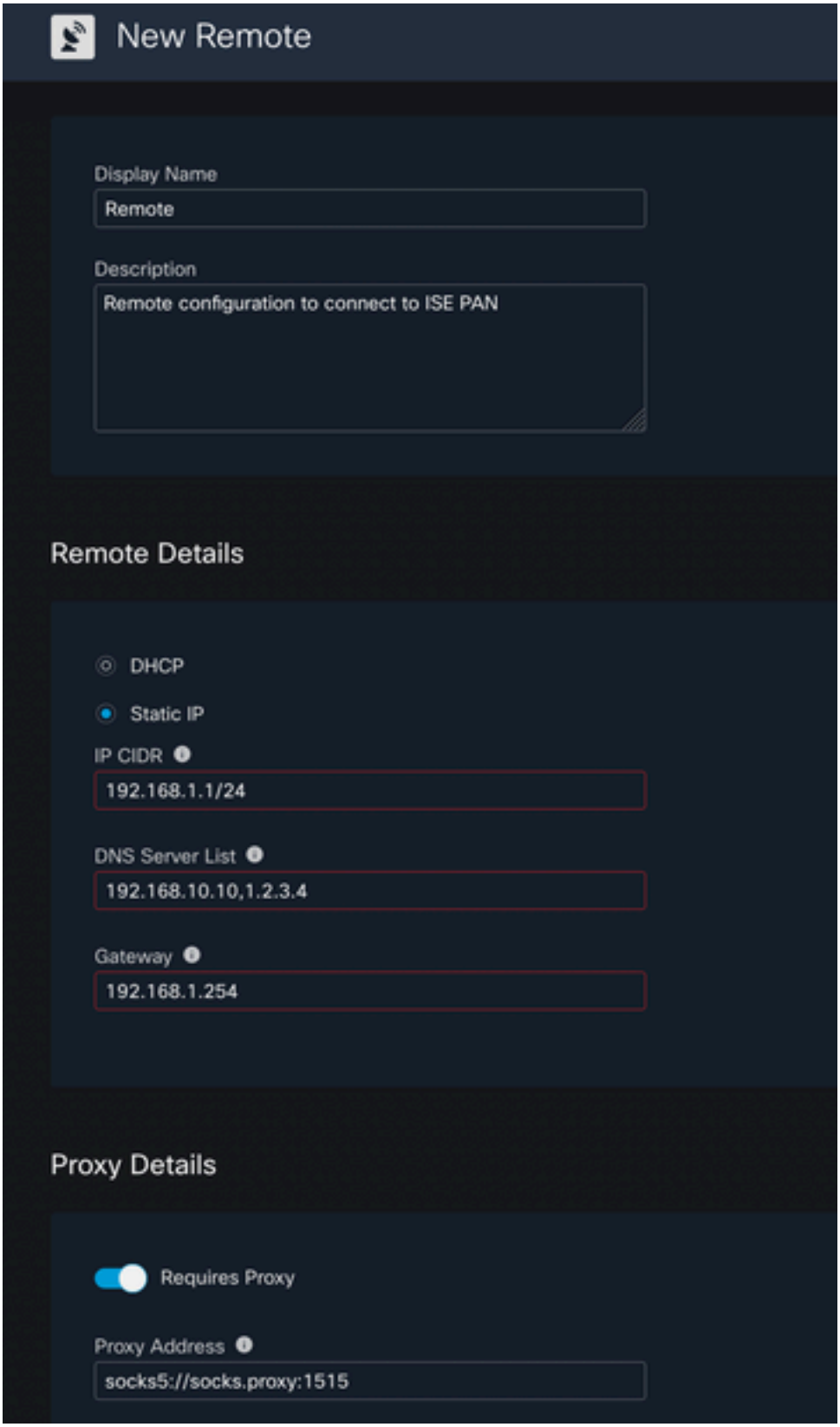
2. (Opcional) Cree un nuevo usuario para la conexión Secure-X, navegue hasta **Administration > System > Admin Access > Administrator > Admin Users** y cree un nuevo usuario, este nuevo usuario debe tener permisos "ERS Admin" o puede ser un superusuario admin.

Configurar e implementar servidor remoto

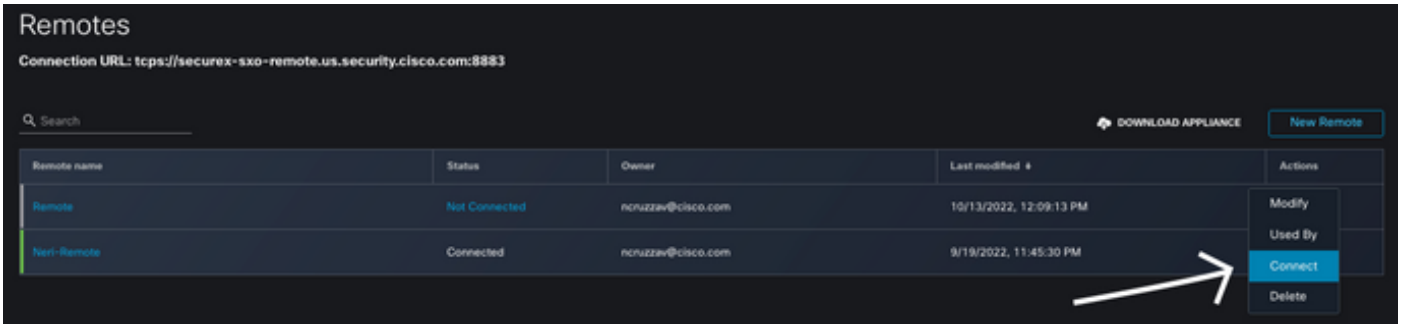
1. Configure el servidor remoto, en la consola Secure-X, navegue hasta **Orchestration > Admin > Remote Configuration** y seleccione la opción **New Remote**, la información de dirección IP es la que se utilizará cuando se cree la VM y debe estar en la misma subred en la que se implemente ISE PAN.

> **Nota:** Si la conexión a la nube se realiza a través de un proxy, actualmente solo se admite un proxy SOCKS5 para este fin.

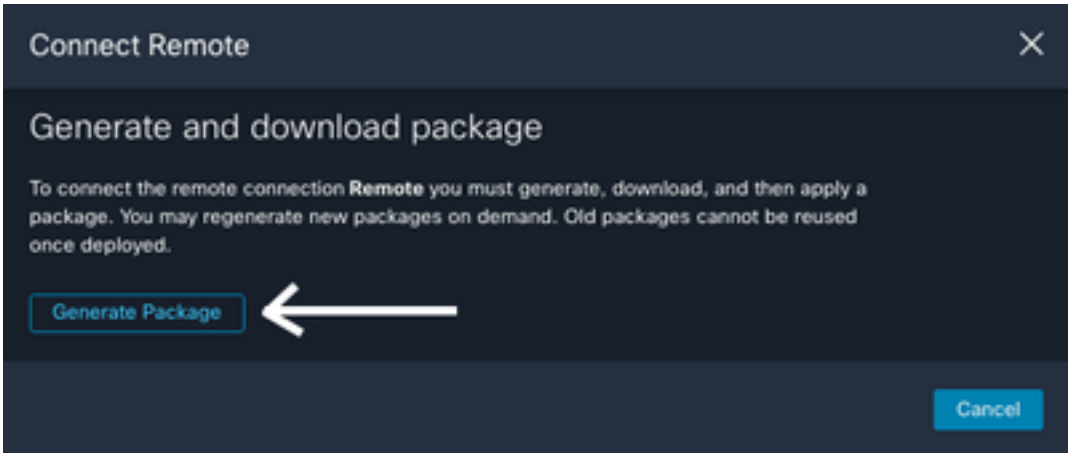




2. Descargue los parámetros configurados que se utilizarán para la implementación de VM. Una vez guardada la información, el mando aparecerá como "**No conectado**", desplácese por Acciones y seleccione **Conectar**



Seleccione **Generate Package,** esta acción descarga un archivo .zip que contiene la información que se acaba de configurar para utilizarse cuando se implementa la máquina virtual.

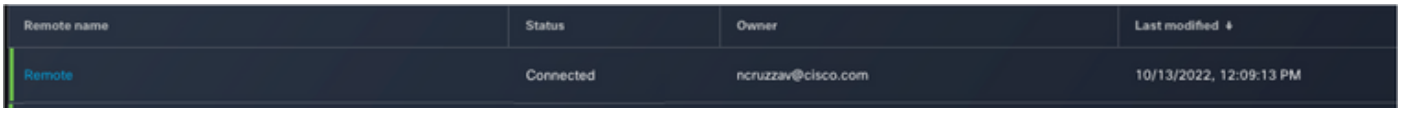


3. Descargue e instale la máquina virtual, junto a **New Remote** seleccione **DOWNLOAD APPLIANCE** esta acción descarga una imagen OVA que necesita utilizar para implementar el servidor remoto.

Para ver las especificaciones de la máquina virtual remota, consulte la guía de [configuración remota de SecureX]

La información descargada dentro del archivo ZIP se debe utilizar en los **datos de usuario codificados** cuando se crea la VM, esto llena la información remota configurada en el servidor una vez que se inicia.

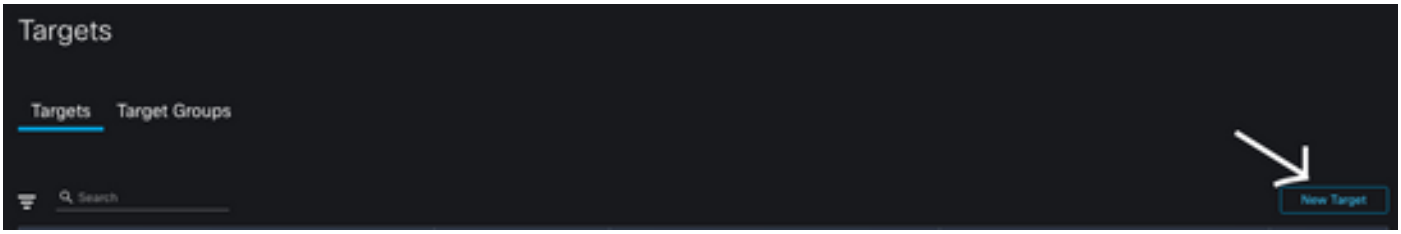
4. Una vez que la VM está activa, se conecta a la cuenta SecureX automáticamente, para verificar que la conexión está activa, bajo la configuración remota debe ver un cambio del estado a **"Conectado"**



Configuración del destino en SecureX

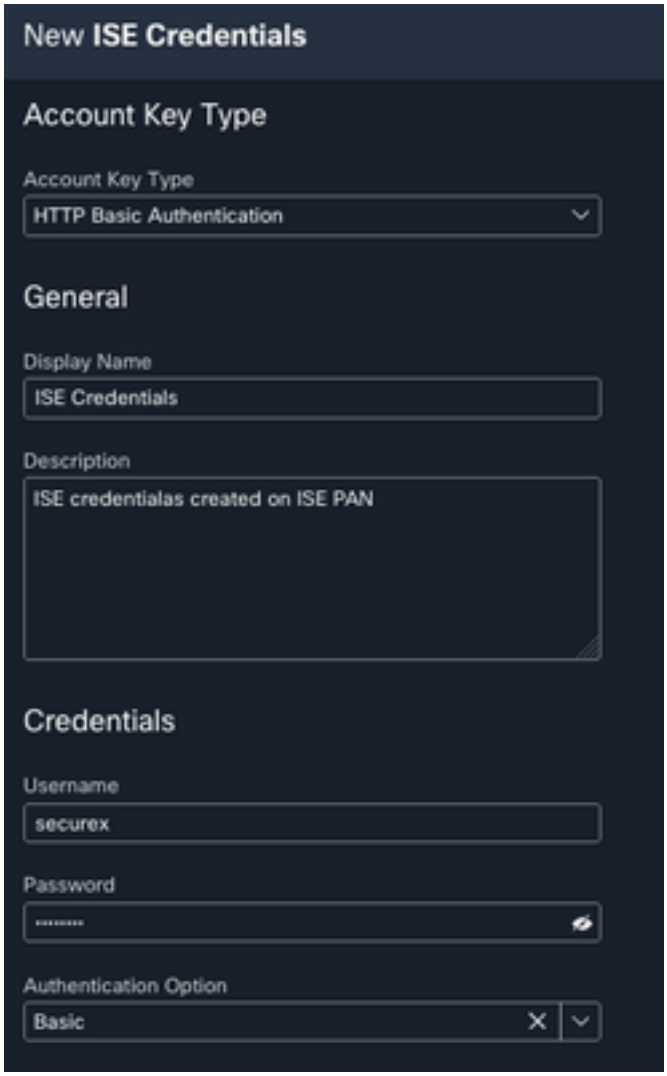
Para que la orquestación funcione con un dispositivo es importante configurar un **destino,** Secure X utiliza este destino para enviar las llamadas de API e interactuar con el dispositivo a través de la orquestación

1. Acceda a **Orquestación > Destinos > Nuevo Destino**

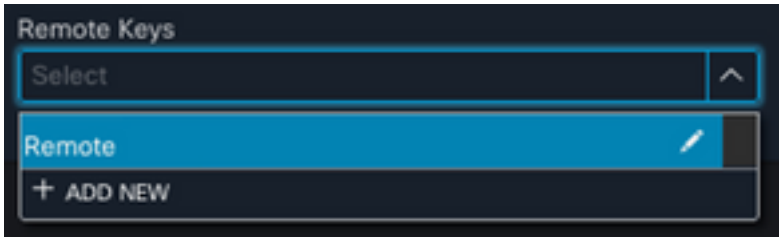


2. Rellene la información del objetivo con las siguientes directrices

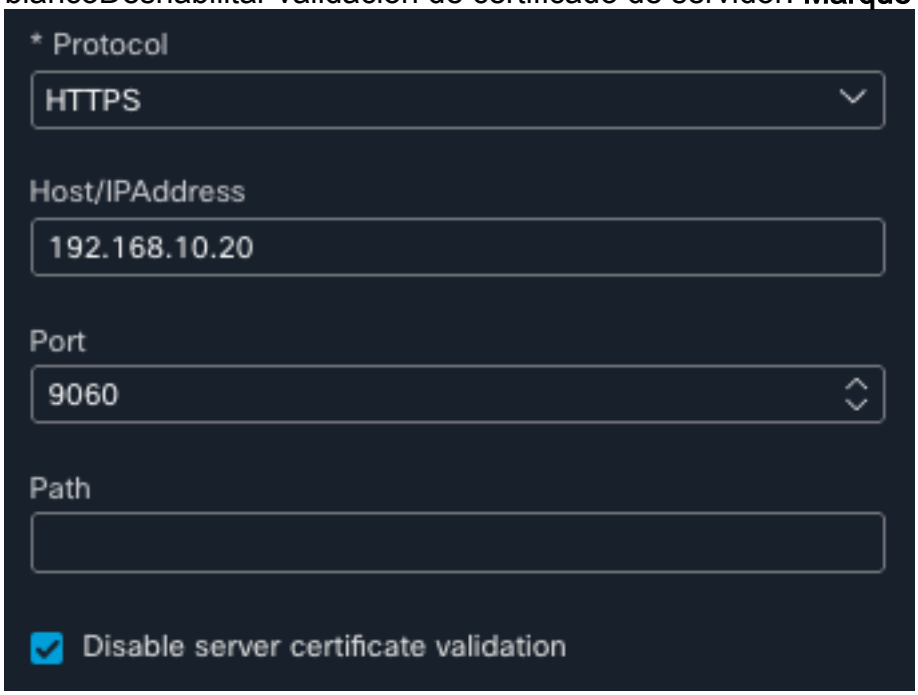
- Nombre para mostrar: Identificador de Destino
- Descripción: Una pequeña descripción para identificar el propósito del objetivo
- Claves de cuenta: Aquí debe configurar el usuario/contraseña para acceder a ISE a través de la API Sin claves de cuenta: **Falso**Claves de cuenta predeterminadas: Seleccione **Add New (Agregar nuevo).** Tipo de clave de cuenta: **Autenticación básica de HTTP**Nombre para mostrar: Identificador de clave de cuentaNombre de usuario: Usuario creado en **ISE PAN** como administrador ERSContraseña Contraseña para el usuario creado en **ISE PAN**Opción de autenticación: **Básico**



- Remoto: Aquí debe seleccionar la conexión remota configurada anteriormente
  Claves remotas: seleccione el mando a distancia en el menú desplegable



- HTTP: Aquí debe configurar la información de la API para el **ISE PAN** Protocolo: **HTTPS**Dirección IP/host: **IP privada de ISE PAN**Puerto: **9060**Ruta: Déjelo en blancoDeshabilitar validación de certificado de servidor: **Marque esta casilla**



- Proxy: Dado que la configuración de proxy se incluyó en la configuración remota, puede dejar esta sección en blanco
- Seleccione **Submit (Enviar).**

Importar el flujo de trabajo desde Cisco Secure GitHub

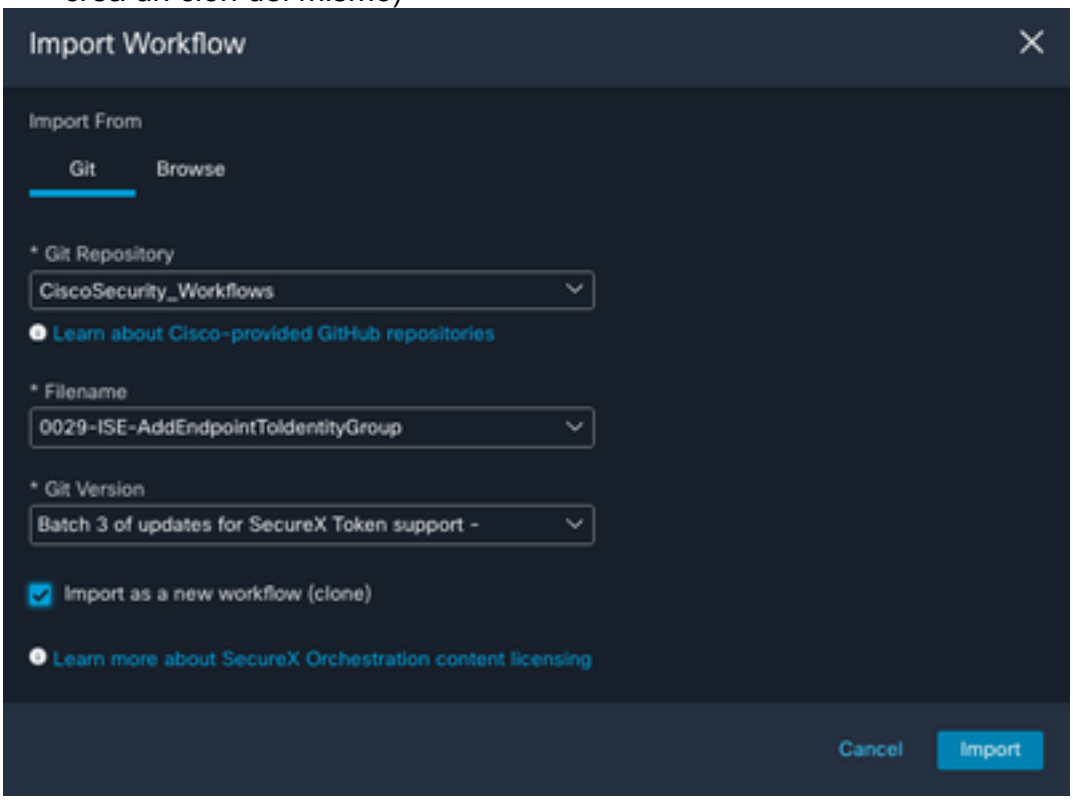
En este ejemplo, el flujo de trabajo que se debe utilizar es "Agregar terminal al grupo de identidad", puede utilizar cualquiera de los flujos de trabajo enumerados en la página Cisco Secure GitHub o puede crear un flujo de trabajo personalizado.

1. Vaya a **Orquestación > Mis flujos de trabajo > Importar flujo de trabajo**

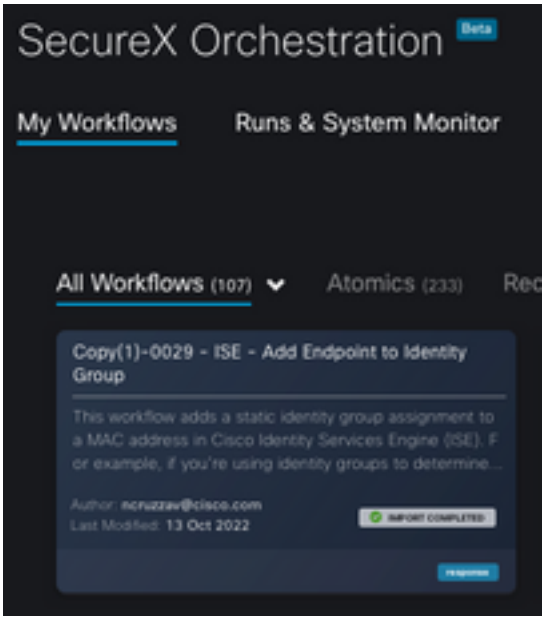
2. Para importar el flujo de trabajo, rellene la información de la siguiente manera y seleccione **Importar;** para identificar el flujo de trabajo que se va a importar, puede buscar por nombre o por número de flujo de trabajo

- Repositorio de Git: **CiscoSecurity_Workflows** (ubicación del flujo de trabajo)

- Nombre de Archivo: **0029-ISE-AddEndpointToIdentityGroup** (Seleccione el número de flujo de trabajo que desea utilizar)
- Versión de Git: **Lote 3 de actualizaciones para SecureX Token Support** (última versión)
- Importar como nuevo flujo de trabajo (clonar): **Comprobar** (se importa el flujo de trabajo y se crea un clon del mismo)

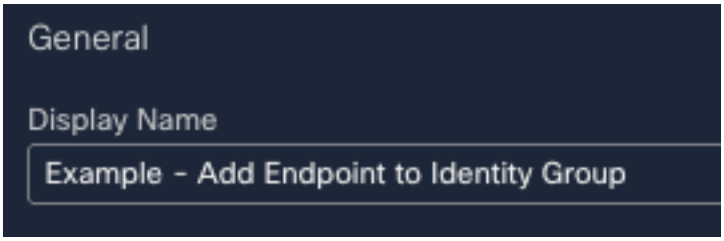


3. Una vez importada, la nueva plantilla aparece en **Mis flujos de trabajo,** seleccione el nuevo flujo de trabajo creado para editar los parámetros para que funcione con **ISE**

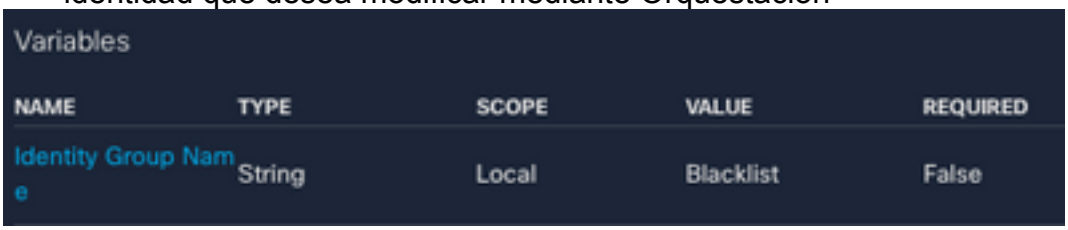


4. Puesto que se trata de un flujo de trabajo previo a la generación, sólo tiene que modificar tres secciones del flujo de trabajo:

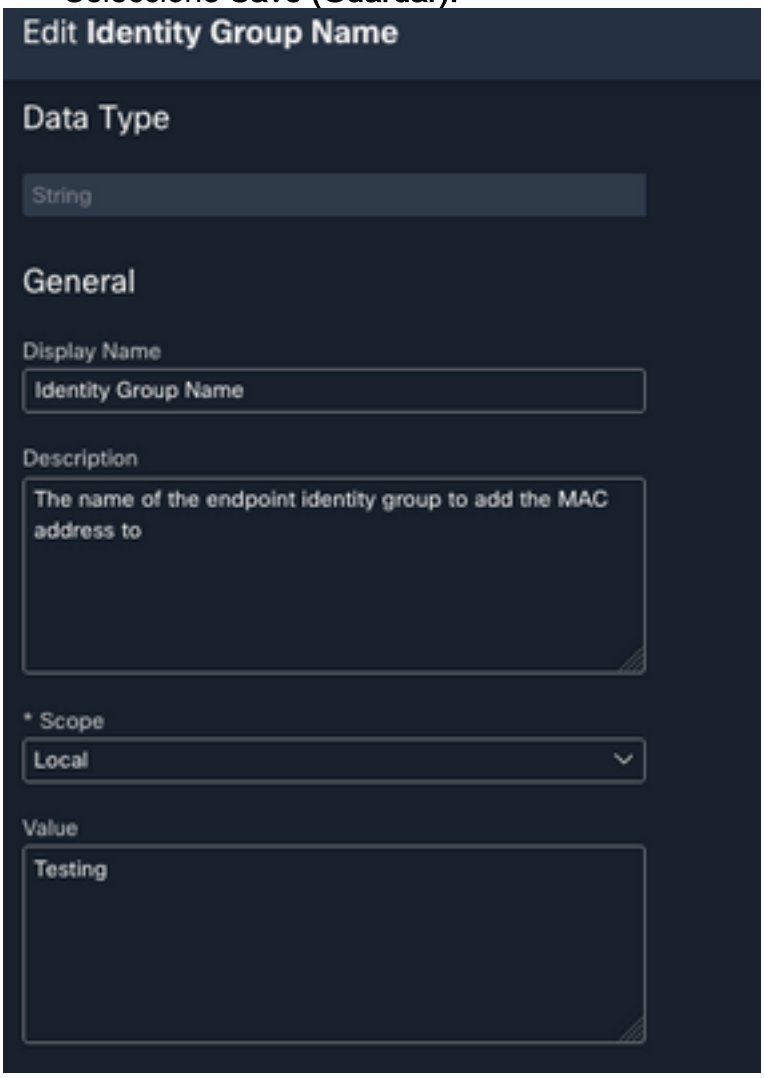
- Nombre: cambie el nombre para mostrar por un identificador mejor.



- Variable de grupo de identidad En Variables, edite la **Variable de grupo de identidad** de forma predeterminada es **Lista negra,** seleccione la variable y configure el nombre de grupo de identidad que desea modificar mediante Orquestación



- Seleccione **Save (Guardar).**



- Objetivo: Configure el **destino** configurado previamente Tipo de destino: **Extremo HTTP**Objetivo: **Nombre del destino configurado**

Verificación

Una vez configurado todo, es el momento de probar el flujo de trabajo

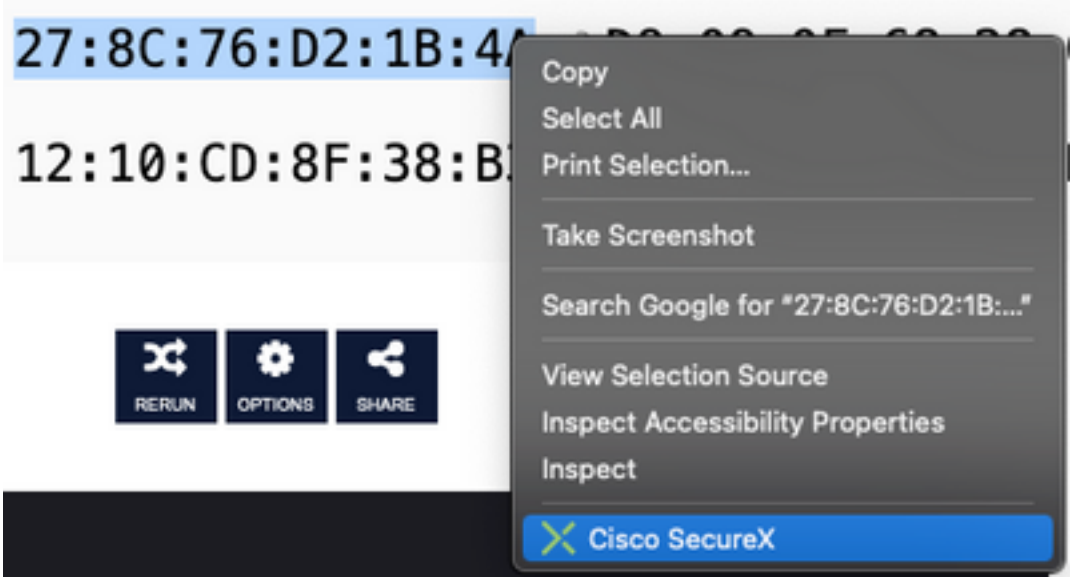
El flujo de trabajo de la prueba realiza esta acción: si encuentra una dirección MAC en una página web, podría estar en el propio ISE o en otra página web como Threat Response; a través de la extensión del explorador SecureX, el flujo de trabajo busca esa dirección MAC dentro de la base de datos de ISE a través de la API; si la dirección MAC no existe, el elemento observable se agrega al grupo de identidad de terminales sin necesidad de copiar el valor y el acceso a ISE.

Para demostrarlo, eche un vistazo al siguiente ejemplo:

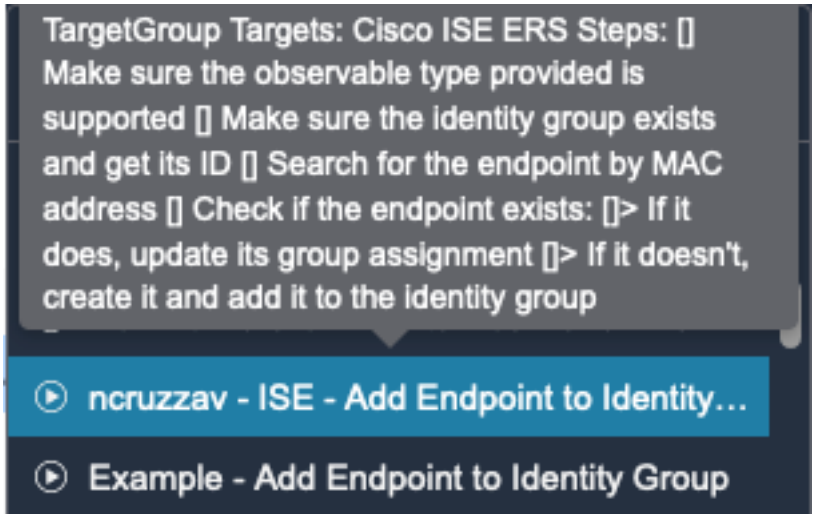
1. El flujo de trabajo seleccionado funciona con el tipo observable **"Dirección MAC"**

2. Busque una dirección MAC en una página web y haga clic con el botón derecho.

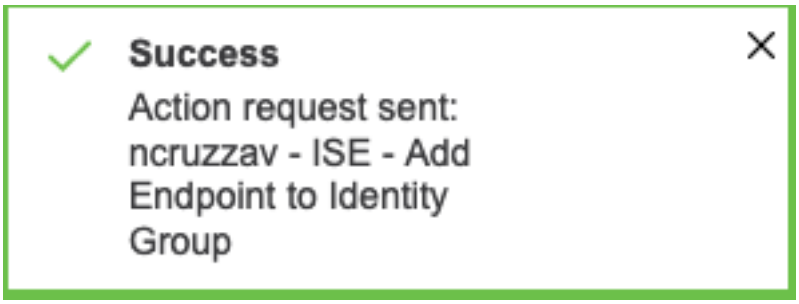
3. Seleccione la opción **SecureX**



4. Seleccione el **flujo de trabajo** creado antes de

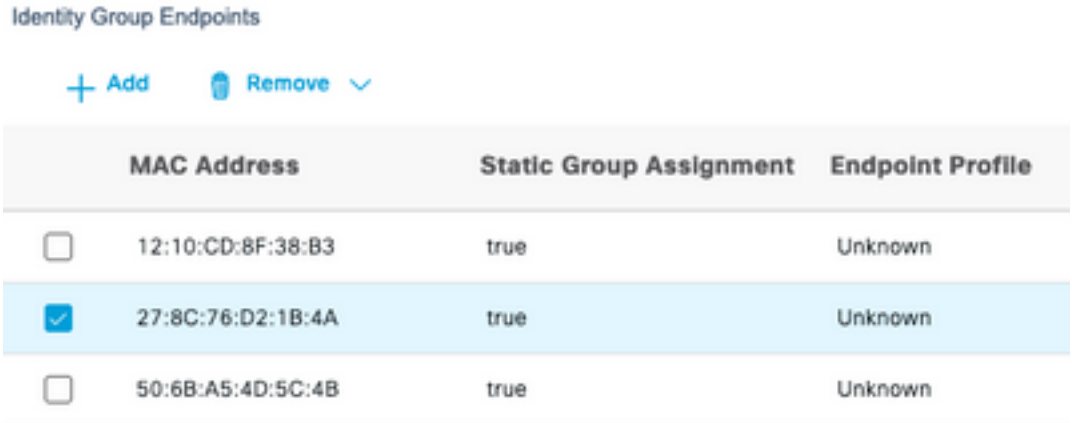


5. Confirme que la tarea se ha ejecutado correctamente



6. En **ISE PAN**, navegue hasta **Administration > Identity Management > Groups > Endpoint Identity Groups > (el grupo configurado en el flujo de trabajo)**

7. Abra el **Grupo de Identidad de Extremo** configurado en el flujo de trabajo y confirme que la dirección MAC seleccionada se agrega a la lista de direcciones MAC



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).