Protección frente a amenazas de correo electrónico seguro: Autenticación multifactor y controles de acceso

Contenido

Introducción

Este documento describe las capacidades que Cisco Email Threat Defence (ETD) proporciona para controlar el acceso del administrador a la consola de gestión.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento de estos temas para configurar la autenticación ETD con Duo:

- Una suscripción a Cisco ETD
- Acceso a Cisco Security Cloud Control (SCC)
- Una solución de autenticación para una seguridad mejorada, en este caso, Cisco Duo.

Componentes Utilizados

Este documento se limita a Email Treat Defence y Secure Cloud Control.

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

Este documento se centra en cómo Cisco ETD aprovecha Cisco SCC y se integra con Cisco Duo para ofrecer autenticación segura y control de acceso granular.

En las soluciones modernas basadas en la nube, el control de acceso es uno de los componentes más importantes para garantizar la seguridad de los datos, el cumplimiento de las normas y la integridad operativa. El acceso no autorizado, especialmente a las cuentas de administrador, puede conllevar graves consecuencias, como sistemas en riesgo, filtraciones de datos e interrupciones del servicio.

Cisco ofrece sólidas funciones de seguridad en su cartera de nube, incluida la tecnología de autenticación multifactor (MFA), que es una parte integral de servicios como Cisco ETD. MFA agrega un paso de verificación crítico más allá de las contraseñas tradicionales, que requiere que los usuarios se autentiquen a través de un factor adicional como la aprobación de una aplicación móvil, token de seguridad o verificación biométrica.

Para optimizar y fortalecer el proceso de autenticación del administrador, ETD aprovecha Cisco SCC, un servicio de administración de políticas y autenticación centralizado.

A través de SCC, ETD obtiene acceso a un amplio conjunto de funciones de seguridad, entre las que se incluyen:

- Aplicación de MFA para mitigar los riesgos de robo de credenciales.
- Integración con proveedores de identidad de terceros como Cisco Duo, Microsoft Entra ID, Okta y otros para admitir flujos de trabajo de autenticación flexibles y federación de identidades empresariales.
- Administración centralizada de políticas, lo que permite unas reglas de acceso uniformes en los servicios en la nube de Cisco.

Cisco Duo, en concreto, amplía estas capacidades añadiendo gestión de acceso avanzada basada en políticas. Utilizando SCC como canal de integración, ETD puede aplicar controles granulares de Duo, como restricciones de IP de origen, comprobaciones del estado de los dispositivos y reglas basadas en grupos de usuarios directamente al acceso del administrador.

Por ejemplo, las organizaciones pueden definir una política que solo permita el acceso desde rangos de redes de confianza específicos. Cualquier intento de conexión fuera de la lista de IP autorizadas se puede bloquear automáticamente, como se muestra en los diagramas adjuntos. Esta combinación de MFA + políticas contextuales permite un enfoque de defensa en profundidad, lo que garantiza que, incluso si las credenciales están en peligro, los atacantes no podrán acceder al sistema a menos que también cumplan criterios de seguridad adicionales.

Al combinar Cisco ETD, Cisco SCC y Cisco Duo, las empresas pueden implementar un modelo de control de acceso seguro, escalable y fácil de usar, alineándose con las prácticas recomendadas del sector y mejorando al mismo tiempo la protección de los servicios críticos en la nube.

Escenarios

Se pueden implementar varios escenarios de autenticación y control de acceso con ETD para asegurar el acceso administrativo:

1. MFA integrado: utilice el MFA integrado de Cisco o integre Microsoft MFA.
2. Cisco SCC con Cisco Duo: combine la autenticación centralizada de Cisco SCC con las funciones avanzadas de MFA de Duo.
3. Cisco SCC con un proveedor de identidad externo (por ejemplo, Microsoft Entra ID): amplíe las políticas de autenticación mediante la integración con soluciones de identidad empresarial.

Este documento describe los pasos de configuración para el Escenario 2: Cisco SCC con Cisco Duo, aunque el proceso se puede adaptar para otras tecnologías.

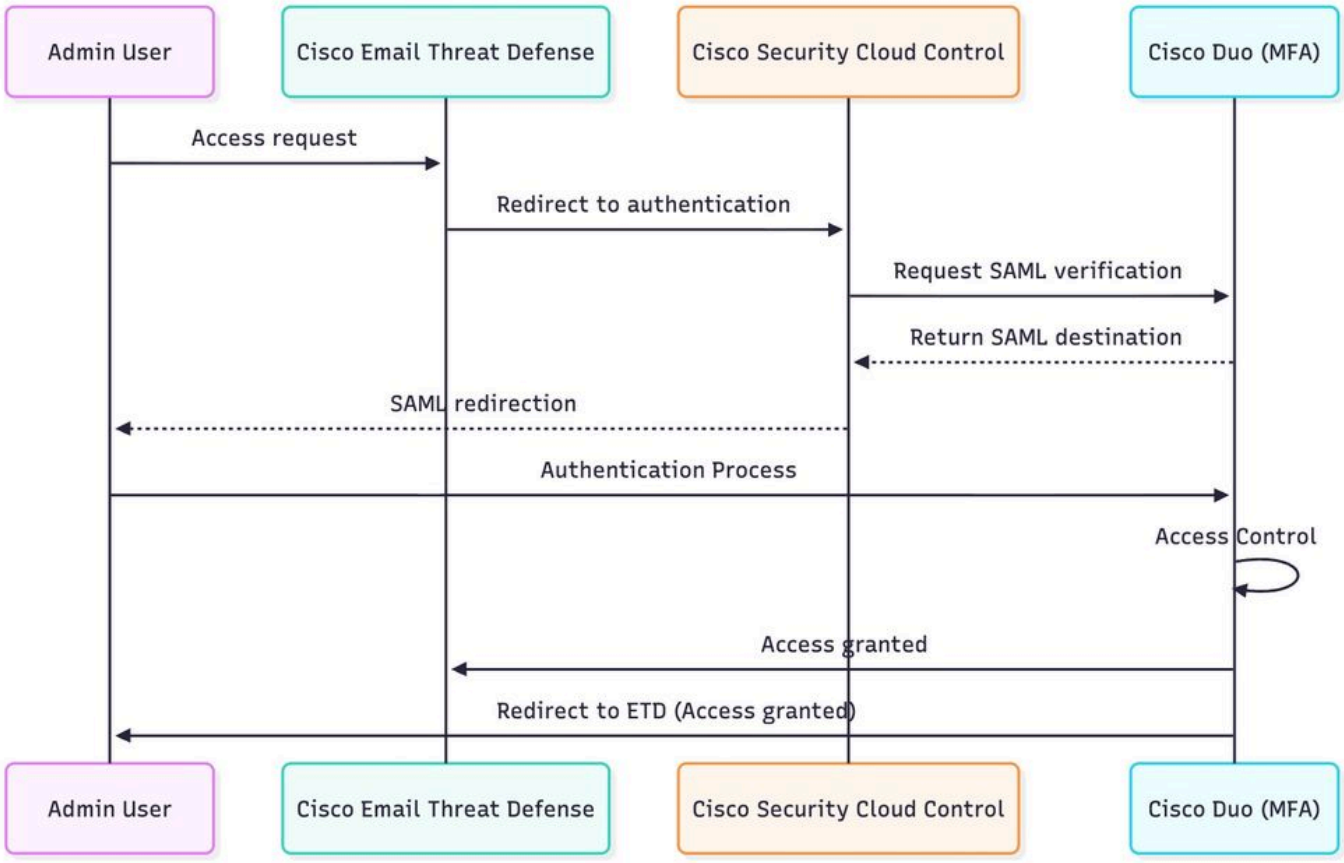
Nota: Este documento proporciona una descripción general de los pasos básicos necesarios para habilitar el control de acceso en Email Threat Defence (ETD) mediante las capacidades de autenticación multifactor de Cisco Duo. La implementación de la integración Duo ayuda a mejorar la seguridad al garantizar que solo los usuarios autorizados puedan acceder a la plataforma. Para obtener una guía completa, opciones de configuración y escenarios de implementación avanzados, consulte la documentación oficial del producto:

- para una política de seguridad y una gestión de acceso centralizadas.

Cisco Duo: para obtener instrucciones detalladas sobre la configuración de la autenticación multifactor y las prácticas recomendadas.

Configuración de Cisco SCC

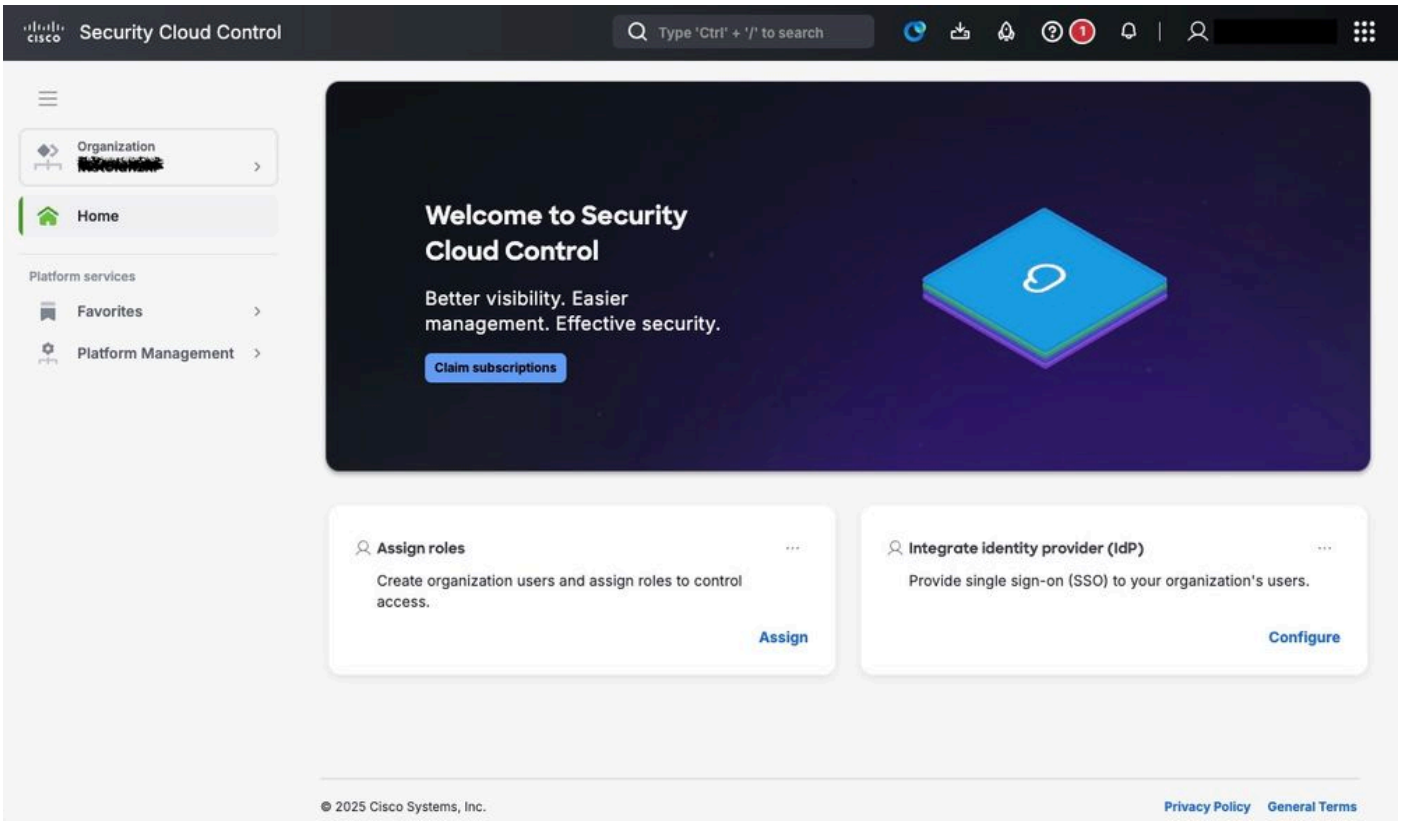
Para integrar Cisco ETD con Cisco Duo, el primer paso es configurar el dominio de autenticación en Cisco SCC. Esto establece la relación de confianza que permite a Cisco SCC trabajar con proveedores de identidades externas y AMF.



Diagrama

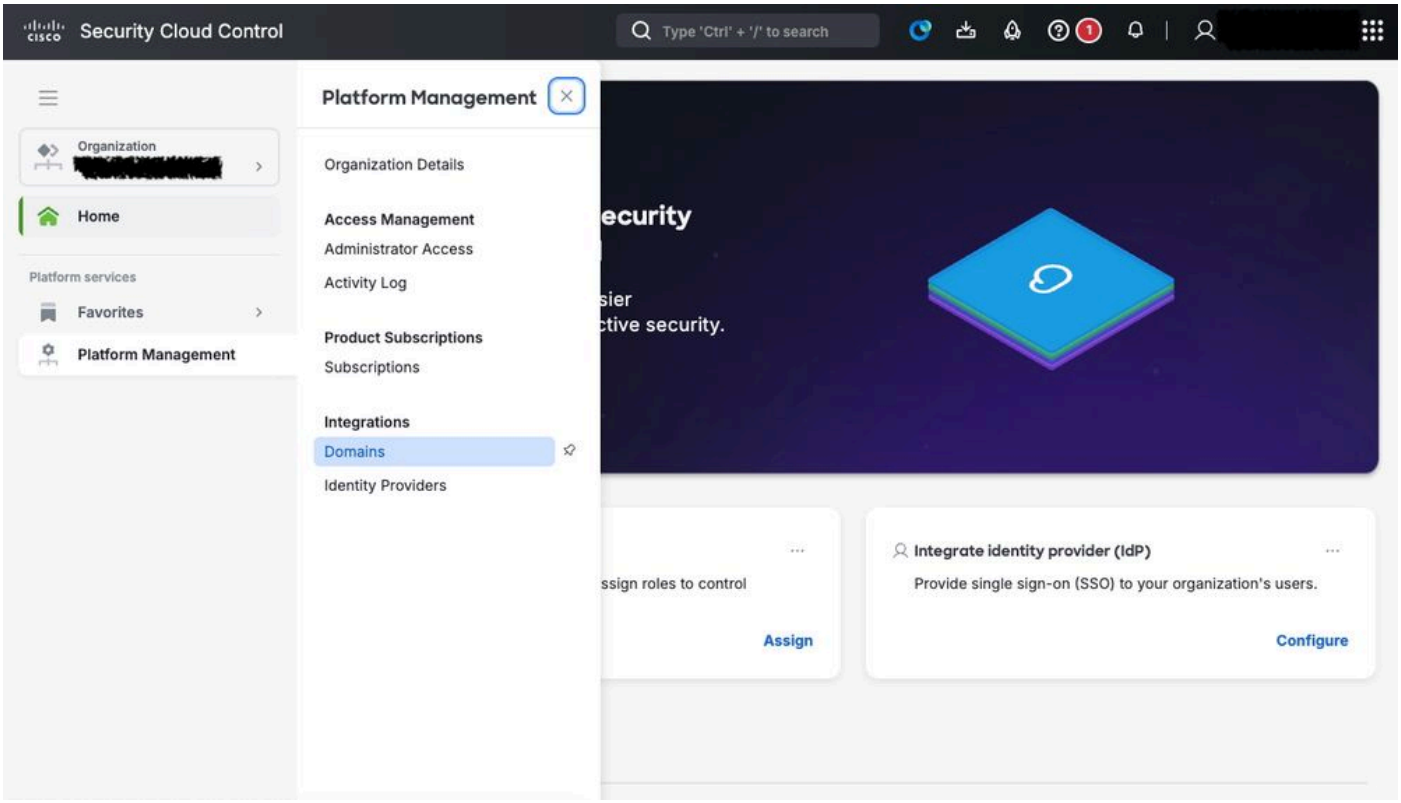
Paso 1. Acceda a la consola de Cisco SCC.

Inicie sesión en el portal de Cisco SCC https://security.cisco.com/.



Paso 2. Navegue hasta Administración de dominios.

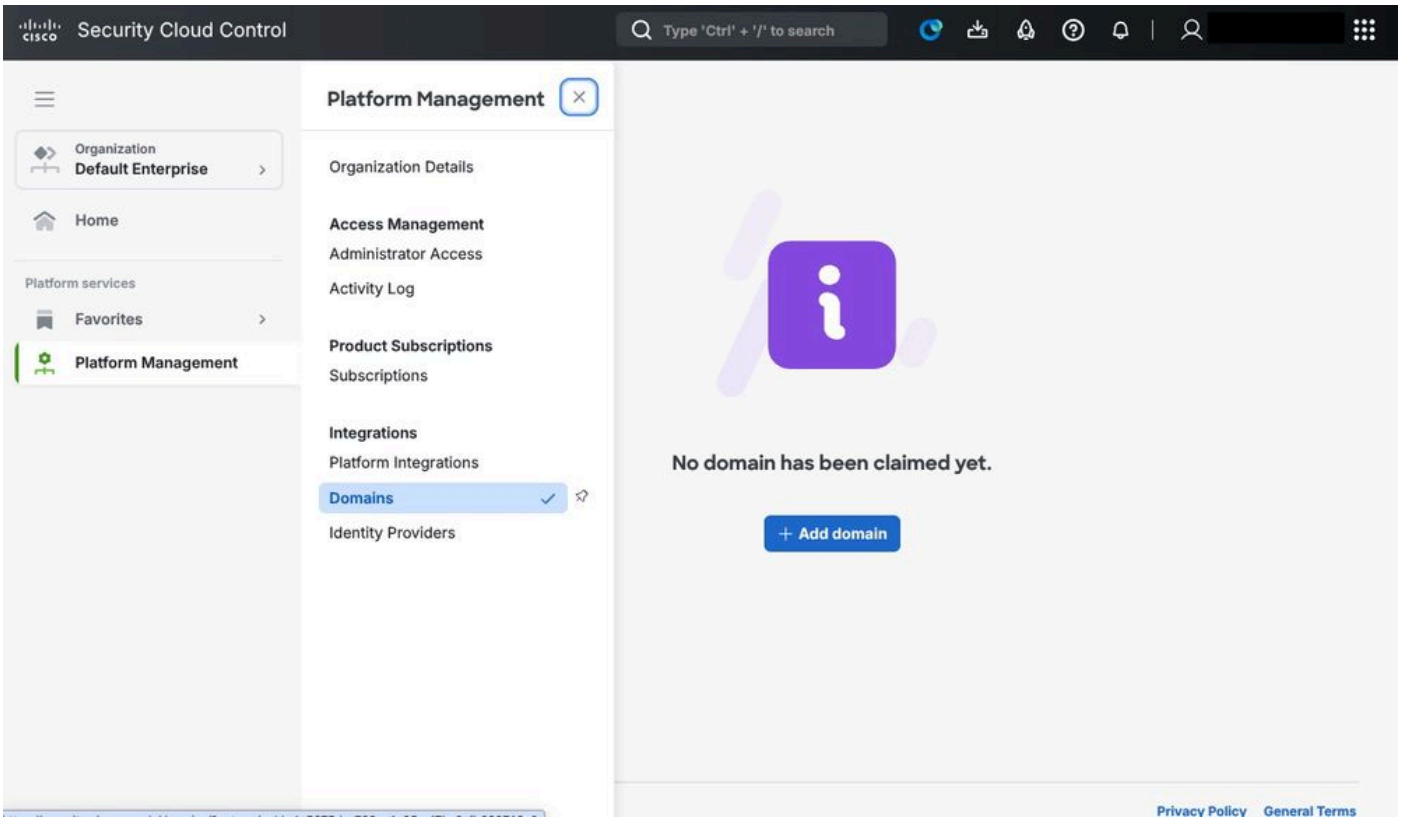
En el menú principal, navegue hasta Administración de la plataforma > Dominios.



Configuración de Secure Cloud Control Domain

Paso 3. Agregar un nuevo dominio.

Haga clic en Agregar dominio para comenzar el proceso de registro de su dominio de autenticación.

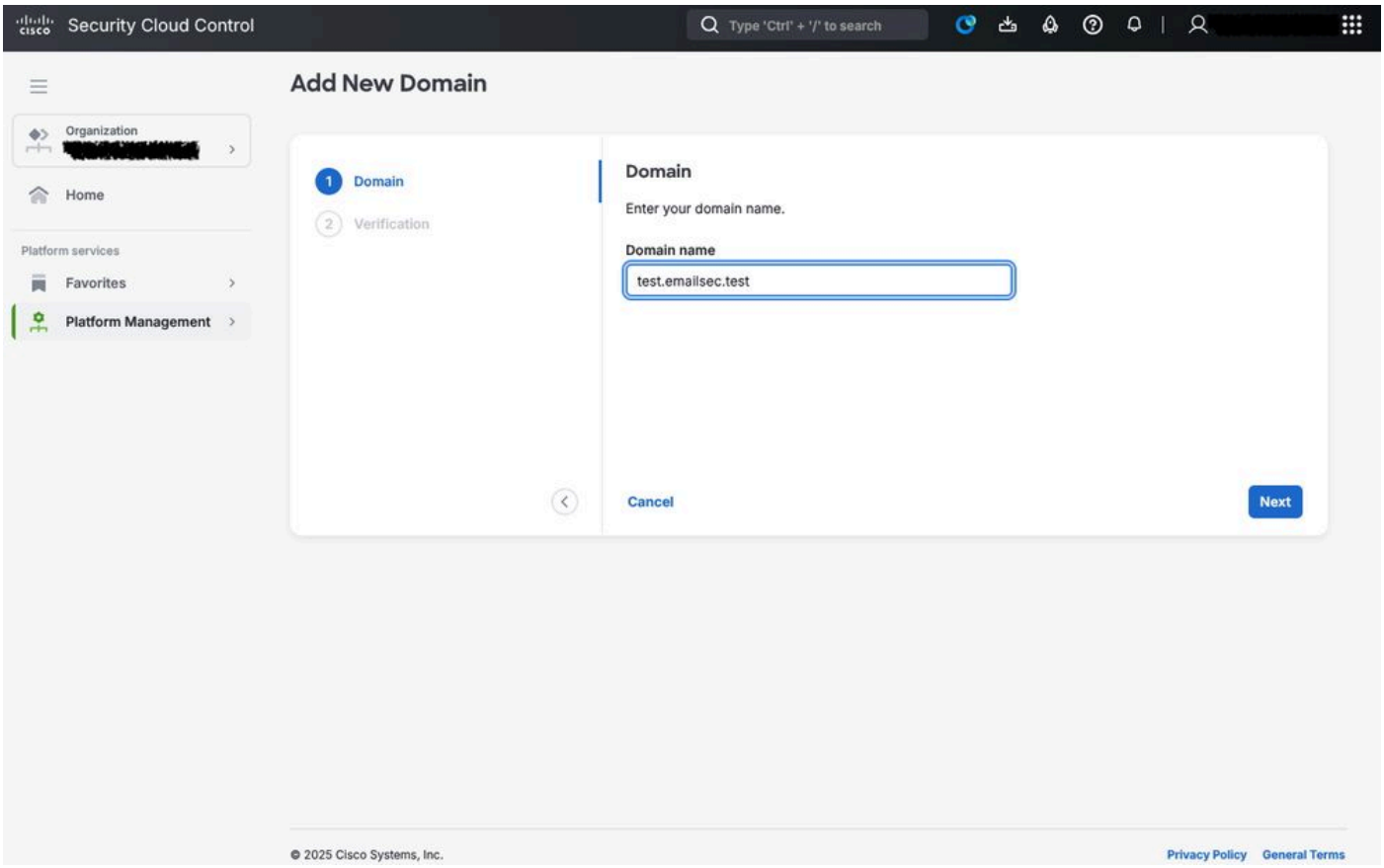


Seguridad Control de la nube: Dominio

Paso 4. Proporcione la información de dominio.

Complete el formulario con los detalles del dominio que se utiliza para la autenticación. Esto incluye normalmente:

- El nombre de dominio (por ejemplo, test.emailsec.test)
- Información de contacto (administrativa y técnica)
- Parámetros de autenticación, en función del proveedor de identidad seleccionado



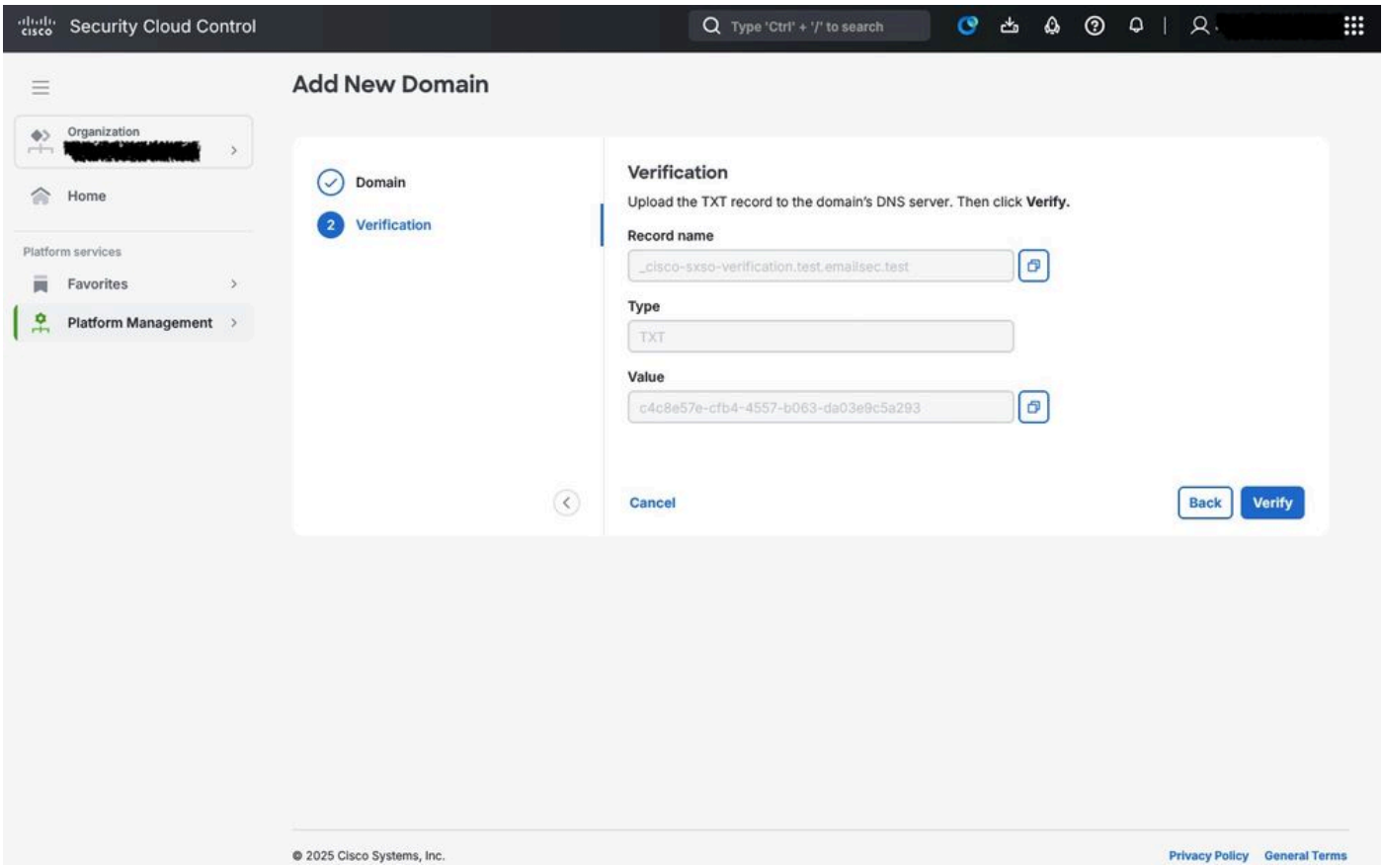
Paso 5. Verificación de dominio vía DNS.

Una vez registrado el dominio, Cisco necesita una prueba de propiedad.

- CSCC proporciona un registro de verificación
- Este registro debe agregarse a la configuración de DNS del dominio (normalmente como un registro TXT)
- Cisco Secure Cloud valida automáticamente la entrada DNS para confirmar que el dominio pertenece a su organización

---

⚠ Precaución: El proceso de verificación debe completarse correctamente para poder continuar con la integración. En función de la propagación de DNS, la validación tarda de varios minutos a unas pocas horas.



Conexión de ETD con Cisco Duo mediante Cisco SCC

Una vez configurado correctamente el dominio del administrador (que sirve de base para aplicar controles de acceso y privilegios de gestión más estrictos), el siguiente paso consiste en integrar el servicio de AMF contratado.

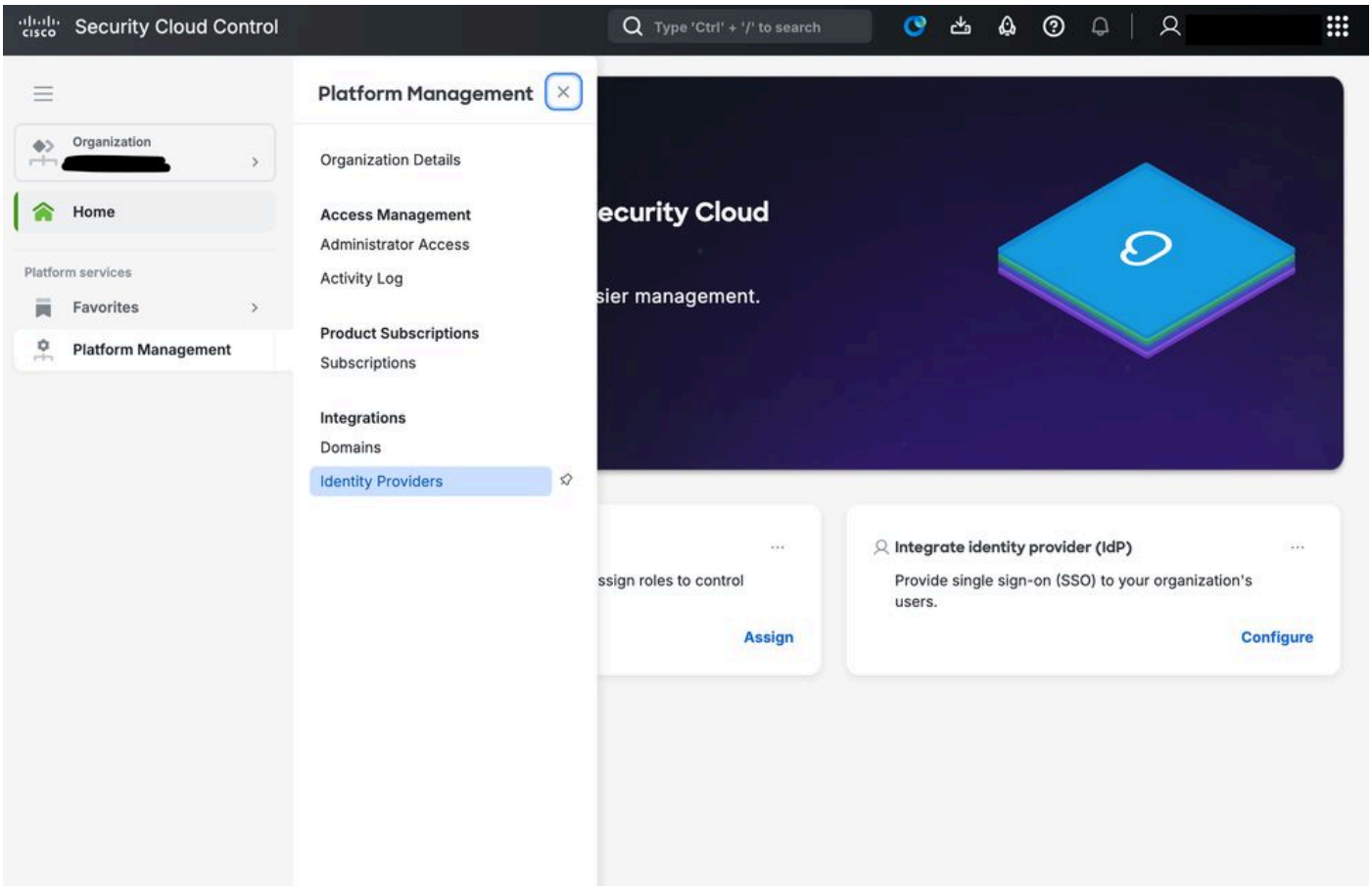
En esta situación, Cisco Duo se implementa como la solución principal para el control de acceso, el inicio de sesión seguro y la verificación de MFA. Esta integración mejora el estado de seguridad del entorno, ya que requiere que los administradores autentiquen su identidad a través de varios pasos de verificación, lo que reduce el riesgo de acceso no autorizado y garantiza el cumplimiento de las políticas de seguridad de la organización.

Integración de Cisco Duo y Cisco Cloud Control

Paso 1. Acceso a Cisco SCC Console.

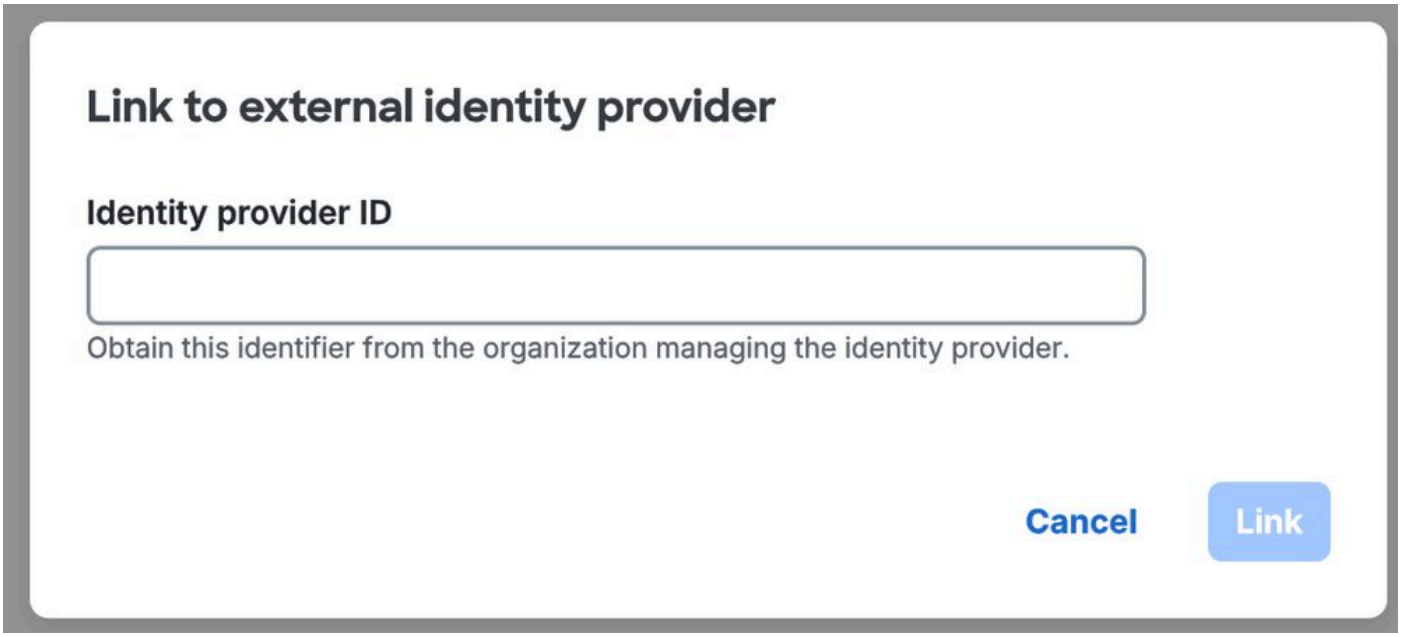
Inicie sesión en el portal de Cisco Security Cloud Control https://security.cisco.com/.

Navegue hasta Administración de la plataforma y haga clic en Proveedores de identidad.



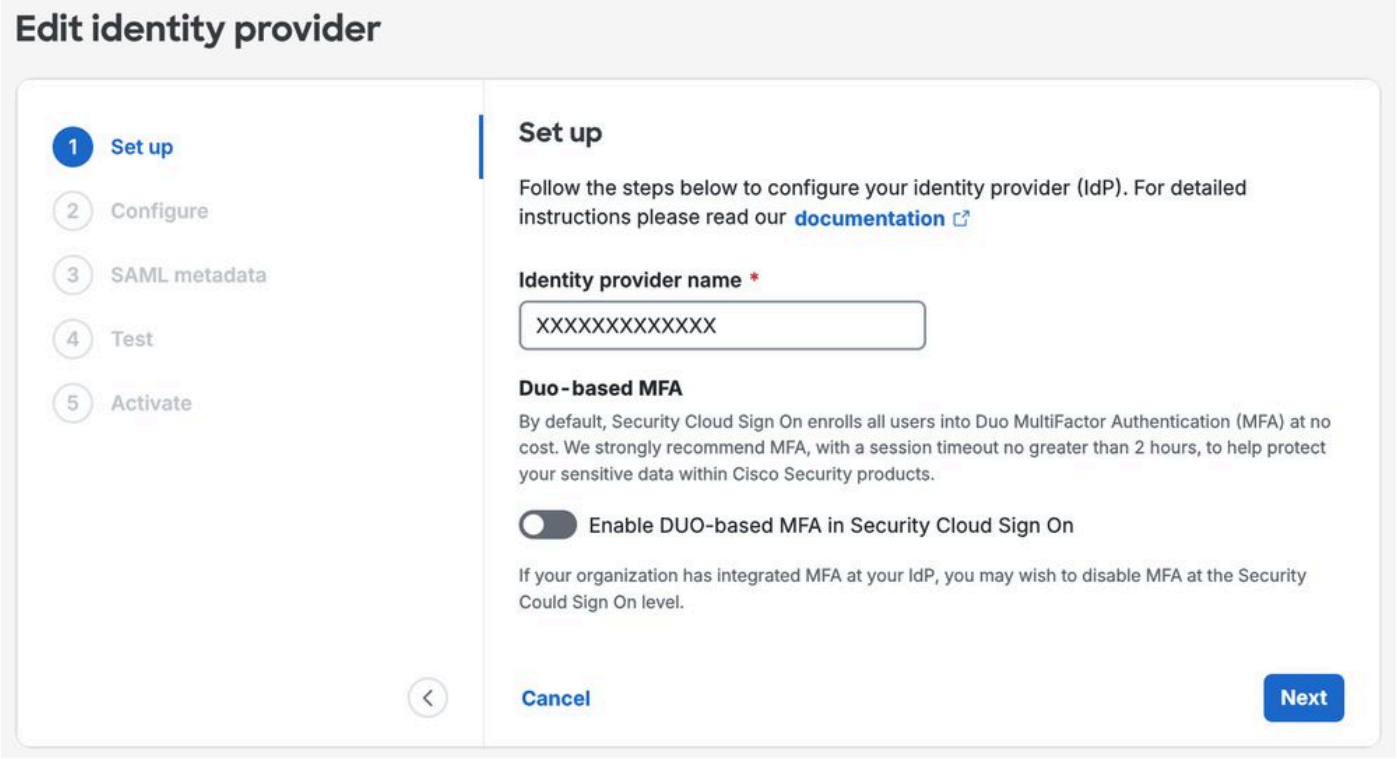
configuración de SCC IDP

Utilice un nombre personalizado para identificar al proveedor de identidad.



Ahora comienza la configuración. En este momento, tendrá acceso a Cisco SCC y Cisco Duo.

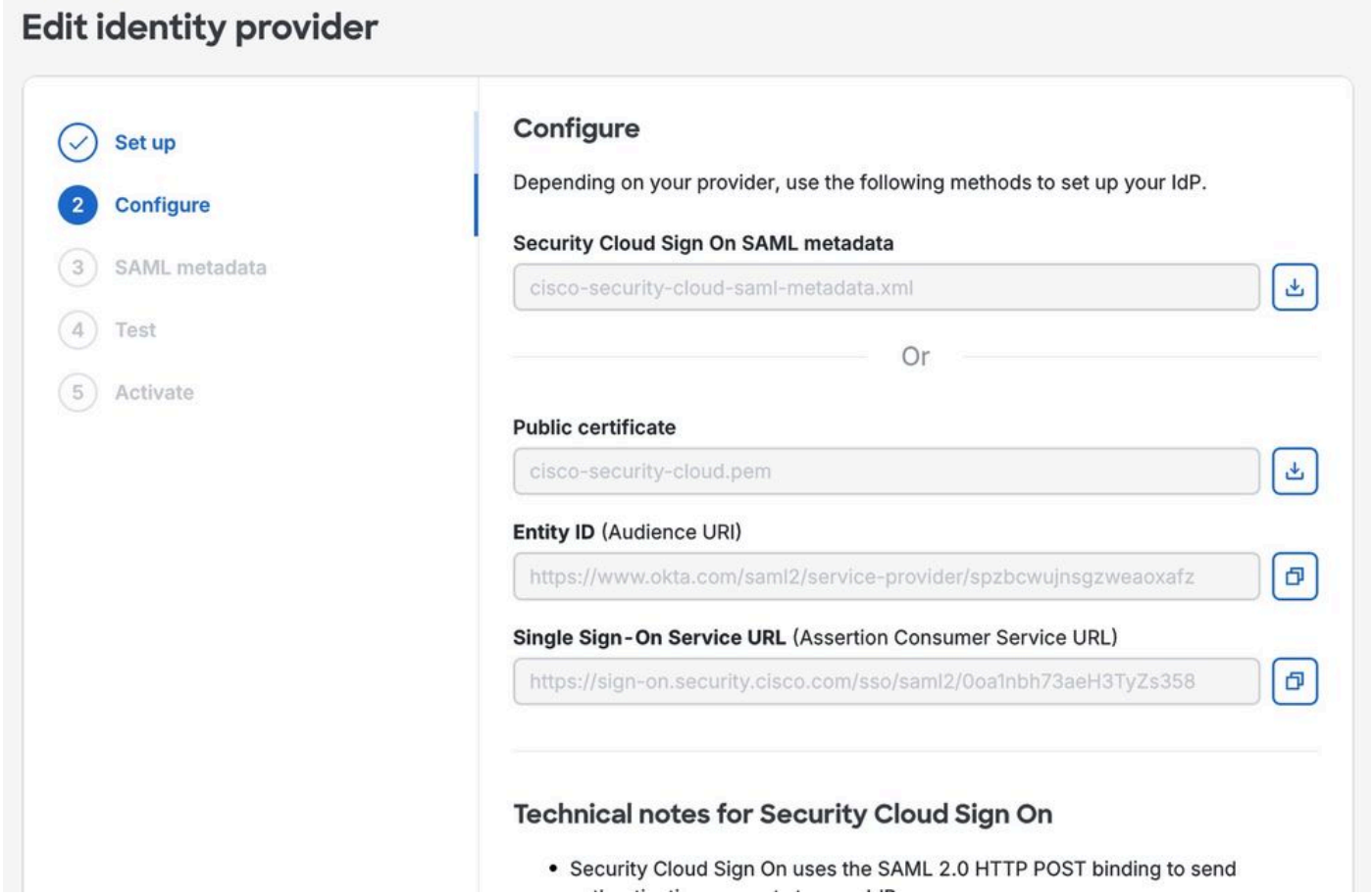
Paso 2. En SCC, inhabilite Enable DUO-based MFA in Security Cloud Sing On, como se muestra en la imagen, y haga clic en Next.



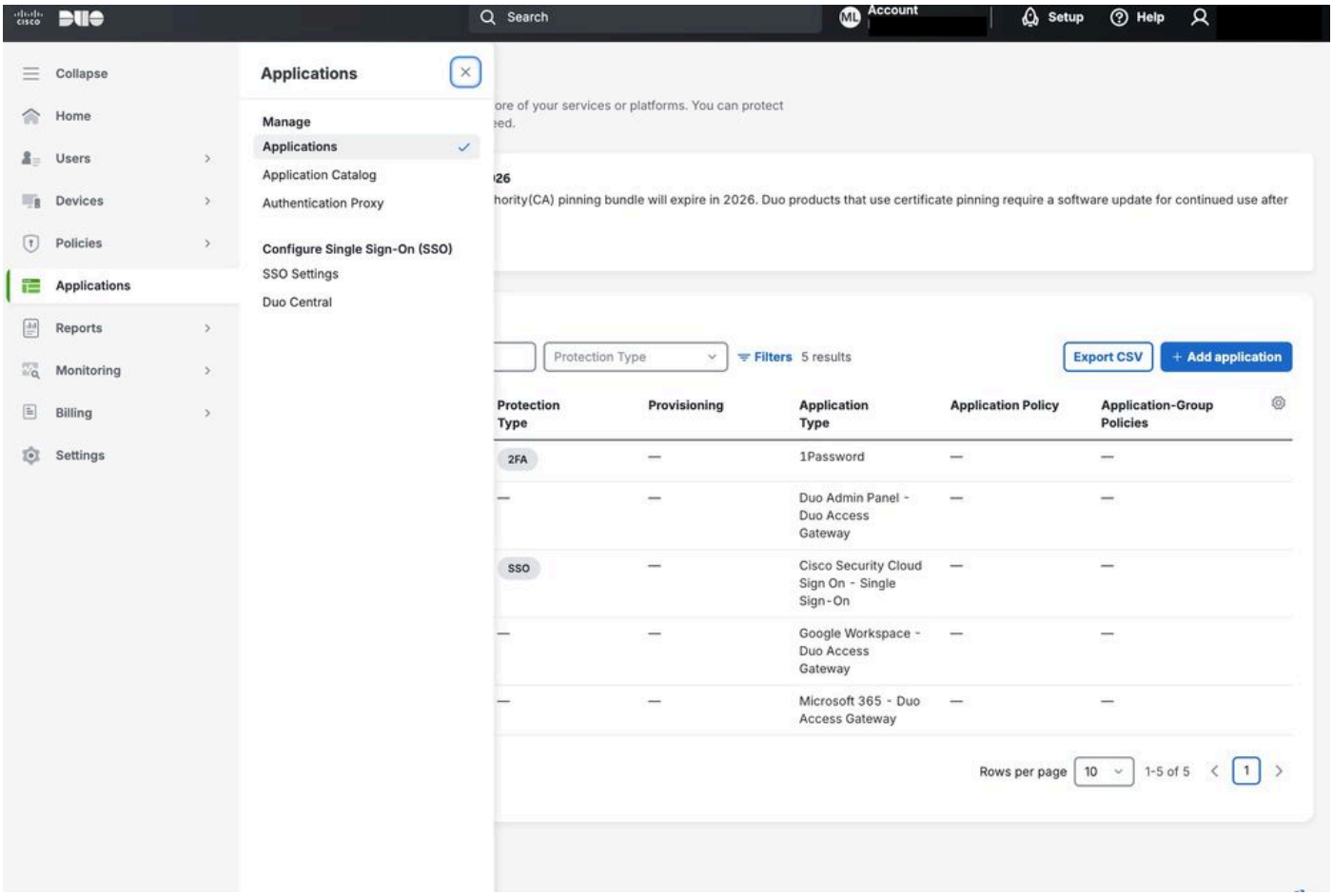
Configuración del proveedor de identidad

Paso 3. Se crean los datos relevantes y se utilizan durante la configuración de Cisco Duo. Asegúrese de copiar todos los valores necesarios y los datos asociados, y almacenarlos en una ubicación segura.

Estos datos son esenciales para futuros pasos de integración, por lo que debe asegurarse de que solo sean accesibles para el personal autorizado y estén protegidos de acuerdo con las políticas de seguridad de su organización.

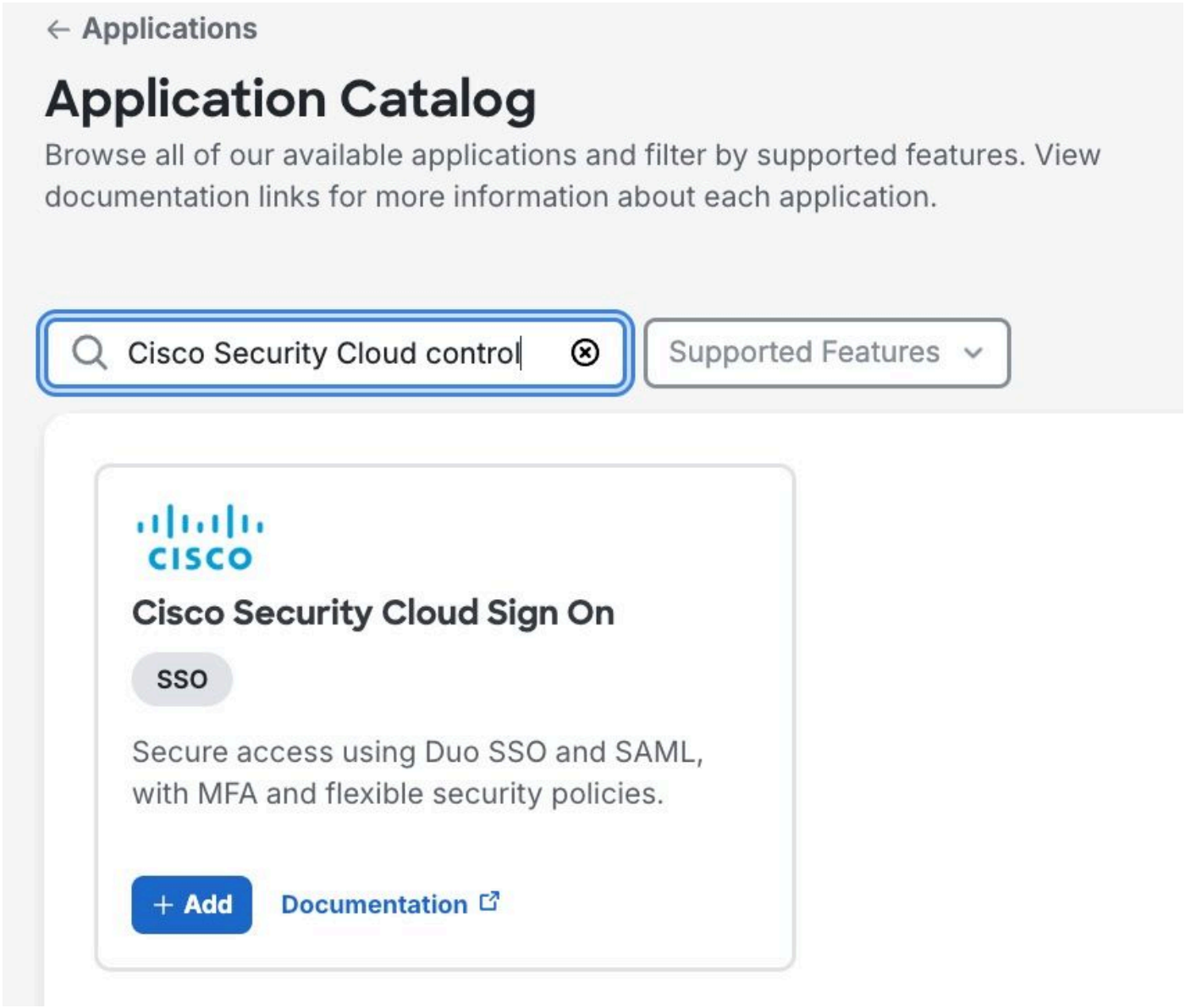


Paso 4. Abra Cisco Duo, navegue hasta la sección Aplicaciones y haga clic en Agregar aplicación.



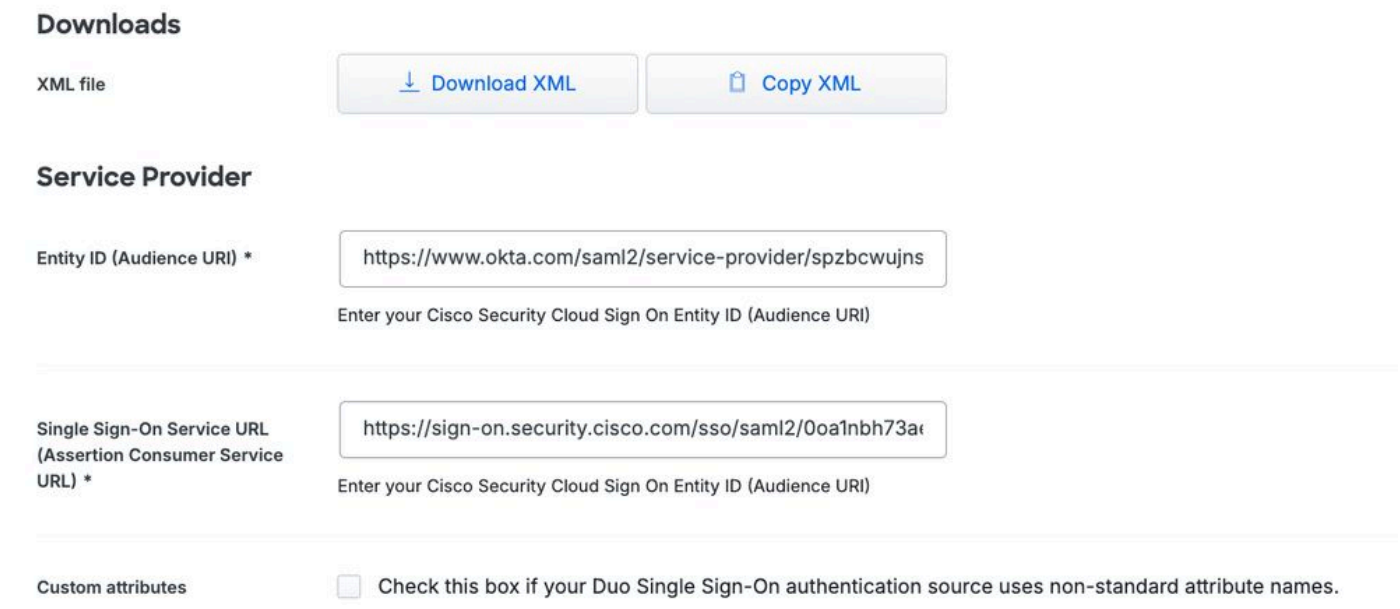
Aplicaciones Cisco DUO

En el menú, busque Cisco Security Cloud y haga clic en Agregar para iniciar la integración.

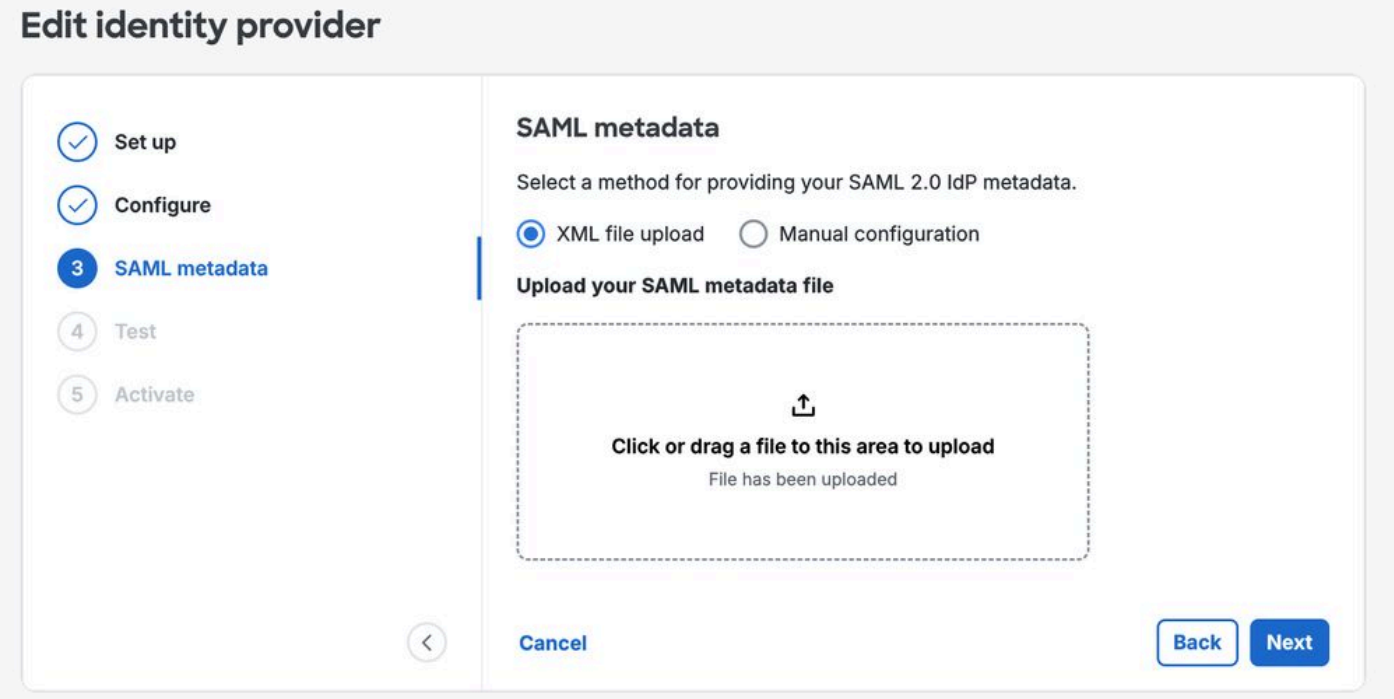


Paso 5. Configure la información relevante en la aplicación Cisco Duo.

Copie la ID de entidad y la URL del servicio de inicio de sesión único de Cisco SCC en Cisco Duo.



Paso 6. Descargue el XML y cargue el archivo en Cisco SCC.



Nota: El resto de los parámetros que se pueden configurar en la aplicación desde la consola de Cisco Duo se deben ajustar según sus requisitos específicos. En la documentación oficial de Cisco Duo se pueden encontrar explicaciones detalladas para cada una de estas configuraciones. Entre los ejemplos de parámetros configurables se incluyen el nombre de aplicación asignado, el conjunto de usuarios a los que se aplica la directiva y otras opciones de personalización que pueden personalizar los controles de seguridad para satisfacer las necesidades de su organización.

Configuración de políticas en Cisco Duo para Cisco ETD

En esta etapa, todos los componentes están conectados, y el siguiente paso es configurar una política que se aplique al proceso de autenticación del administrador dentro de la consola Cisco ETD.

En este ejemplo, el enfoque se centra específicamente en el control de acceso basado en la dirección IP. Sin embargo, Cisco Duo ofrece muchas otras opciones de control de acceso.

Se puede crear una nueva directiva y asignarla a la aplicación, lo que permite la aplicación de las reglas de autenticación deseadas y las restricciones de seguridad para los inicios de sesión de los administradores.

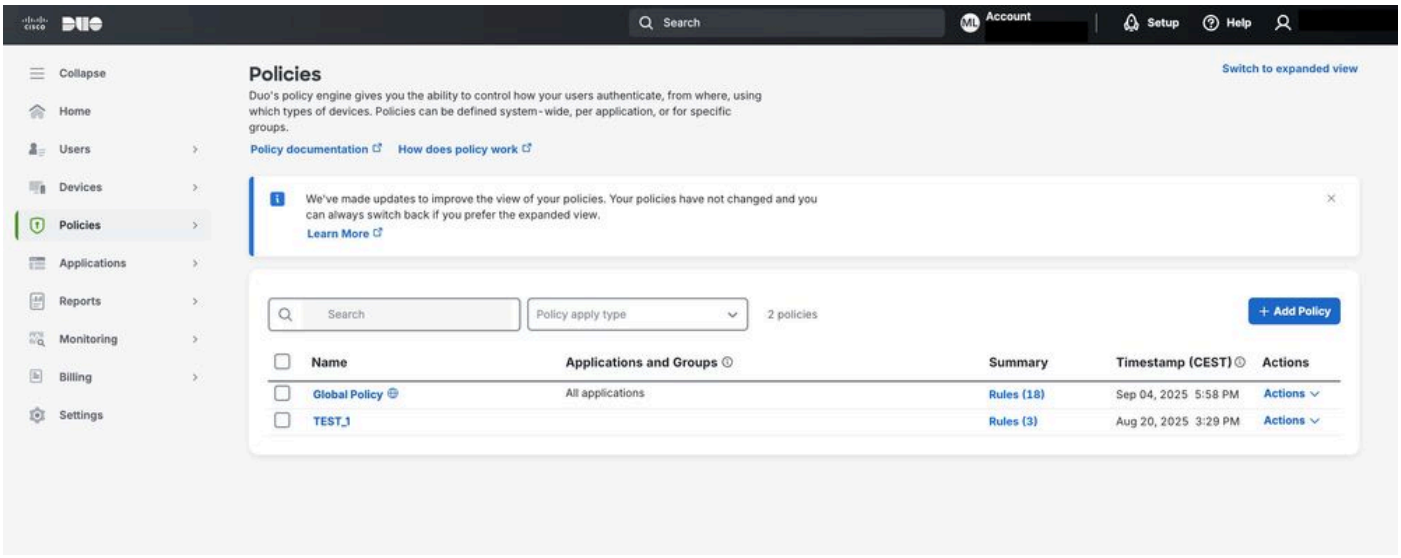
Para obtener información más detallada sobre todos los controles y opciones de configuración disponibles en Cisco Duo, consulte la documentación oficial de Cisco Duo.

Este recurso proporciona una guía completa sobre la configuración, personalización y prácticas

recomendadas para ayudar a optimizar las políticas de seguridad.

Al navegar a la sección Políticas en Cisco Duo, se puede crear una política y asignarla a la conexión Cisco ETD a través de Cisco Duo.

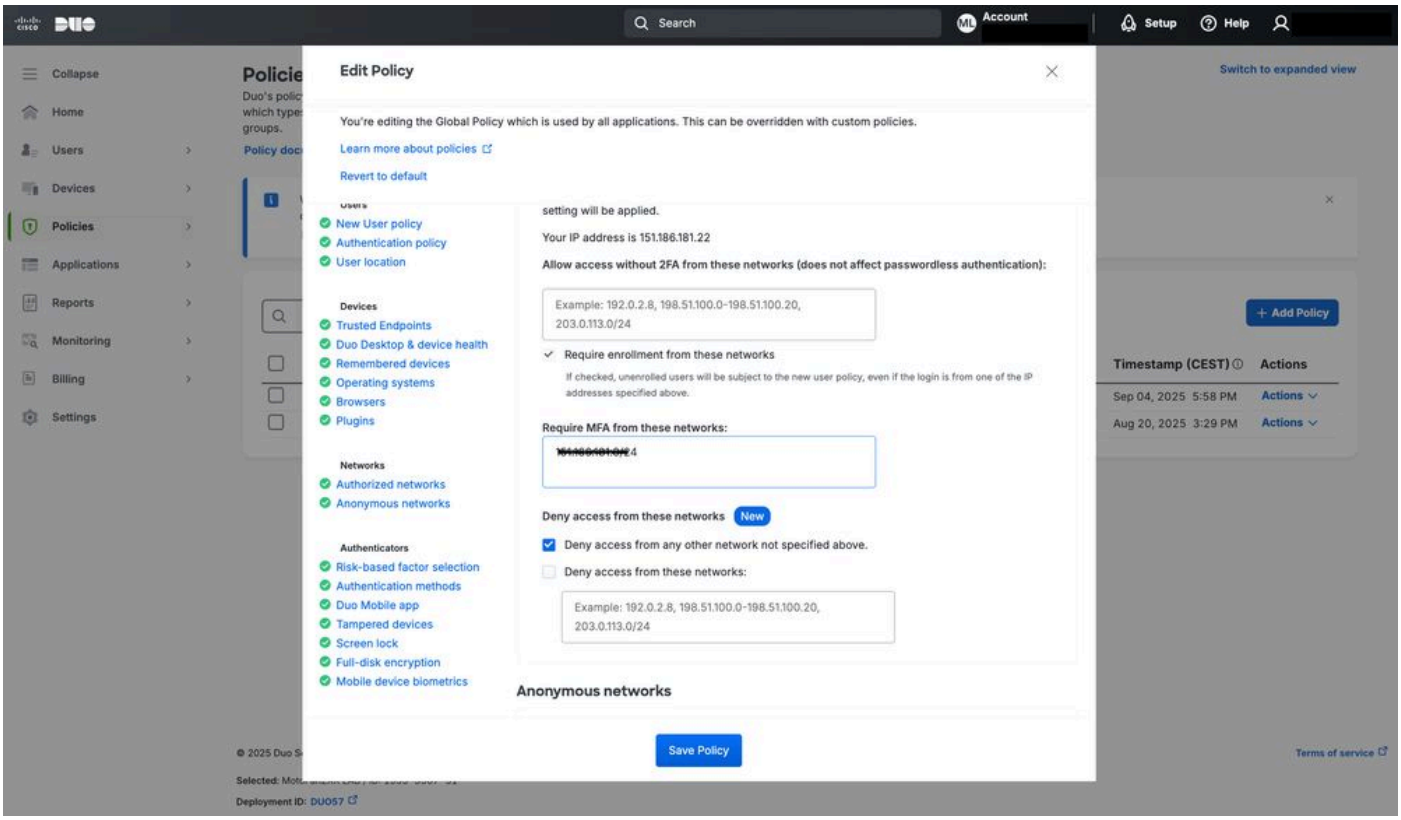
Esta política se puede aplicar por usuario o grupo, en función de los requisitos de acceso.



Cisco Duo

En este ejemplo, como se muestra en la imagen, el control de acceso IP de origen se habilita mediante la configuración de la sección Redes autorizadas.

Esta configuración solo permite el acceso desde intervalos de IP de confianza especificados, lo que mejora la seguridad de Cisco ETD.

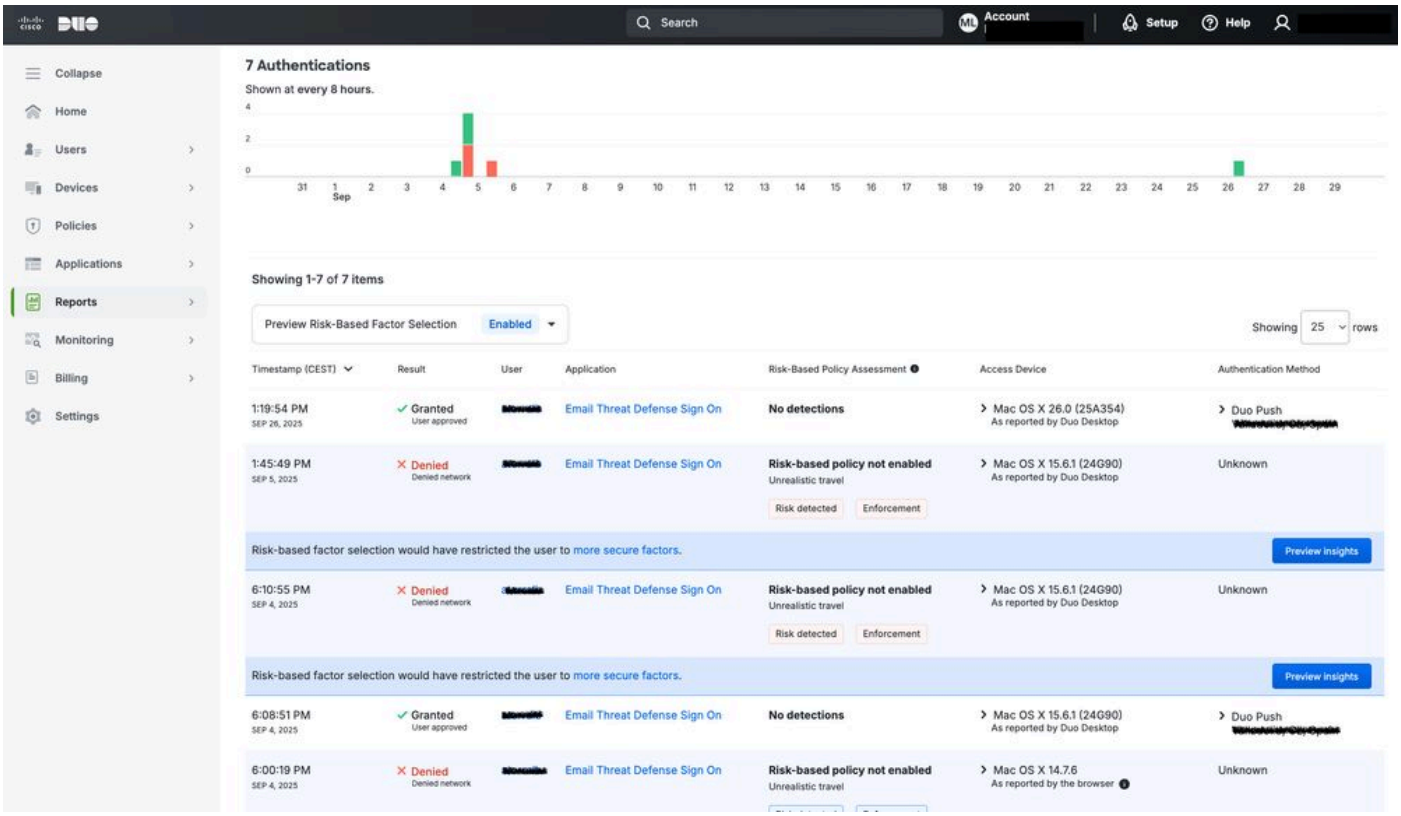


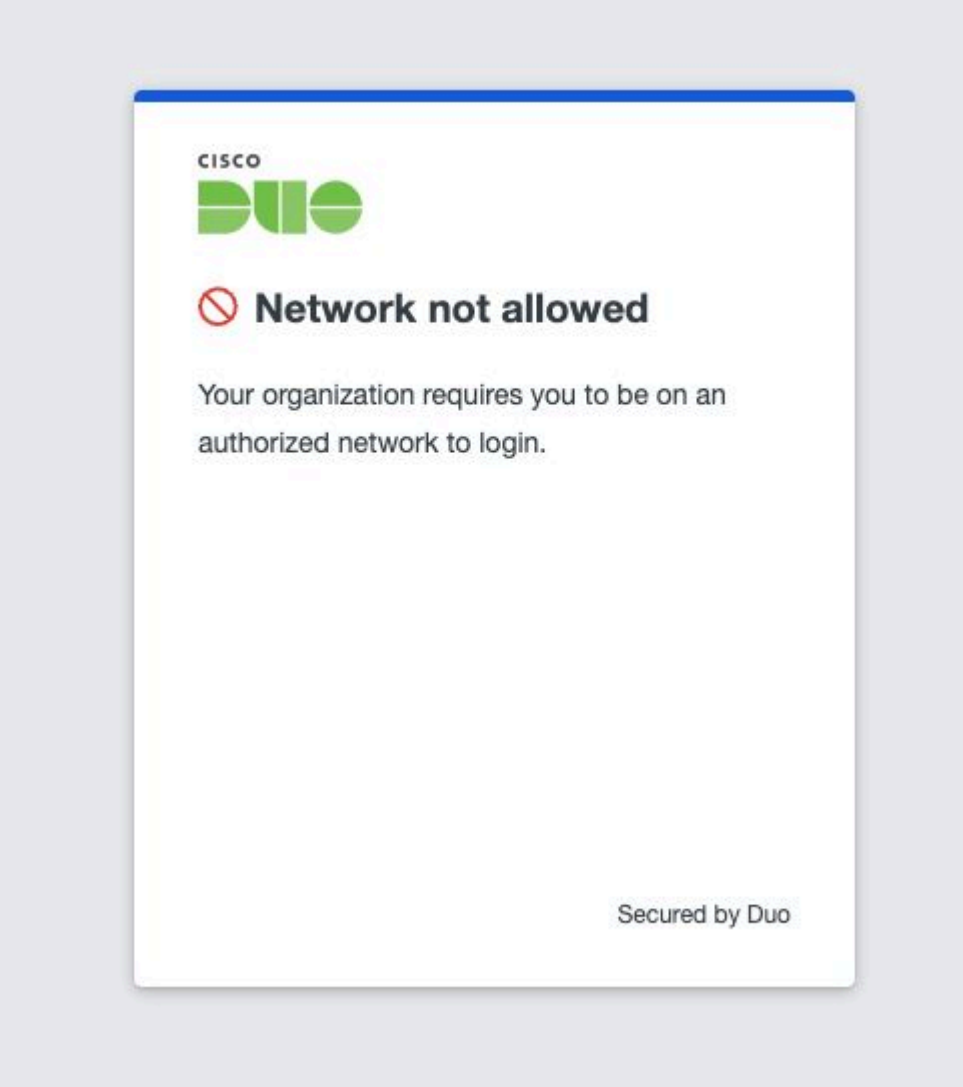
Conclusiones

Cisco ETD ofrece opciones flexibles para proteger el acceso de los administradores a través de MFA y la integración con los proveedores de identidad.
Al combinar Cisco SCC con Cisco Duo, las organizaciones pueden implementar políticas de autenticación más estrictas, reducir el riesgo de acceso no autorizado y adaptarse a las prácticas recomendadas del sector para una gestión segura de los servicios en la nube.

Además de MFA, los administradores pueden aprovechar los controles basados en políticas de Cisco Duo para restringir el acceso en función de criterios específicos, como la dirección IP de origen. Por ejemplo, como se muestra en la siguiente imagen, el sistema bloquea automáticamente un intento de acceso desde una dirección IP que se encuentre fuera del intervalo autorizado. Esto garantiza que solo se permiten las solicitudes que se originan en redes de confianza, lo que añade una capa adicional de protección frente a posibles ataques.

Al implementar el control de acceso basado en IP junto con MFA, las organizaciones logran un enfoque de defensa en profundidad que combina la verificación de identidad con la validación de la ubicación de la red para proteger las interfaces de gestión críticas en la nube.





Resultado de control de red

Advertencia: Es importante comprender que este cambio afecta a todas las aplicaciones que utilizan el mismo dominio de autenticación; no solo ETD, sino también otros productos que dependen del mismo proceso de autenticación, como el acceso a la consola de Cisco Secure Access.

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).