Secure Email Threat Defense: Autenticação Multifator e Controles de Acesso

Contents

Introdução

Este documento descreve os recursos que o Cisco Email Threat Defense (ETD) fornece para controlar o acesso do administrador ao console de gerenciamento.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos para configurar a autenticação ETD com o Duo:

- Uma assinatura Cisco ETD
- Acesso ao Cisco Security Cloud Control (SCC)
- Uma solução de autenticação para maior segurança, neste caso, o Cisco Duo.

Componentes Utilizados

Este documento é restrito ao Email Treat Defense e ao Secure Cloud Control.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Este documento se concentra em como o Cisco ETD aproveita o Cisco SCC e se integra ao Cisco Duo para fornecer autenticação segura e controle de acesso granular.

Em soluções modernas baseadas em nuvem, o controle de acesso é um dos componentes mais críticos para garantir a segurança de dados, a conformidade regulamentar e a integridade operacional. Acesso não autorizado — especialmente para contas de administrador pode levar a graves consequências, como comprometimento de sistemas, vazamentos de dados e interrupções de serviço.

A Cisco oferece recursos de segurança robustos em todo o seu portfólio de nuvem, incluindo a tecnologia de Autenticação Multifator (MFA), que é parte integrante de serviços como o Cisco ETD. O MFA acrescenta uma etapa de verificação crítica além das senhas tradicionais, exigindo que os usuários se autentiquem por meio de um fator adicional, como uma aprovação de aplicativo móvel, token de segurança ou verificação biométrica.

Para simplificar e fortalecer o processo de autenticação do administrador, o ETD aproveita o Cisco SCC, um serviço centralizado de autenticação e gerenciamento de políticas.

Através do SCC, o ETD acessa um amplo conjunto de recursos de segurança, incluindo:

- Aplicação de MFA para reduzir os riscos de roubo de credenciais.
- Integração com provedores de identidade de terceiros, como Cisco Duo, Microsoft Entra ID, Okta e outros, para oferecer suporte a fluxos de trabalho de autenticação flexíveis e federação de identidade corporativa.
- Administração centralizada de políticas, permitindo regras de acesso consistentes nos serviços em nuvem da Cisco.

O Cisco Duo, em particular, amplia esses recursos adicionando gerenciamento de acesso baseado em políticas avançadas. Usando o SCC como o canal de integração, o ETD pode aplicar controles granulares do Duo, como restrições de IP de origem, verificações de integridade do dispositivo e regras baseadas em grupos de usuários, diretamente ao acesso do administrador.

Por exemplo, as organizações podem definir uma política que permita acesso apenas de intervalos de rede confiável específicos. Qualquer tentativa de conexão fora da lista de IPs autorizados pode ser automaticamente bloqueada, como ilustrado nos diagramas que acompanham. Essa combinação de MFA + políticas contextuais permite uma abordagem de defesa aprofundada, garantindo que, mesmo que as credenciais sejam comprometidas, os invasores ainda sejam impedidos de acessar o sistema, a menos que também atendam a critérios de segurança adicionais.

Ao unir o Cisco ETD, o Cisco SCC e o Cisco Duo, as empresas podem implementar um modelo de controle de acesso seguro, escalável e amigável, alinhado com as melhores práticas do setor ao mesmo tempo em que aprimoram a proteção para serviços de nuvem críticos.

Cenários

Vários cenários de autenticação e controle de acesso podem ser implementados com o ETD para proteger o acesso administrativo:

1. MFA integrado - Use o MFA integrado da Cisco ou integre o MFA da Microsoft.
2. Cisco SCC com Cisco Duo - Combine a autenticação centralizada do Cisco SCC com os recursos avançados de MFA do Duo.
3. Cisco SCC com um provedor de identidade externo (por exemplo, Microsoft Entra ID) - Estenda as políticas de autenticação integrando-se a soluções de identidade empresarial.

Este documento descreve as etapas de configuração para o Cenário 2: Cisco SCC com Cisco Duo, embora o processo possa ser adaptado para outras tecnologias.

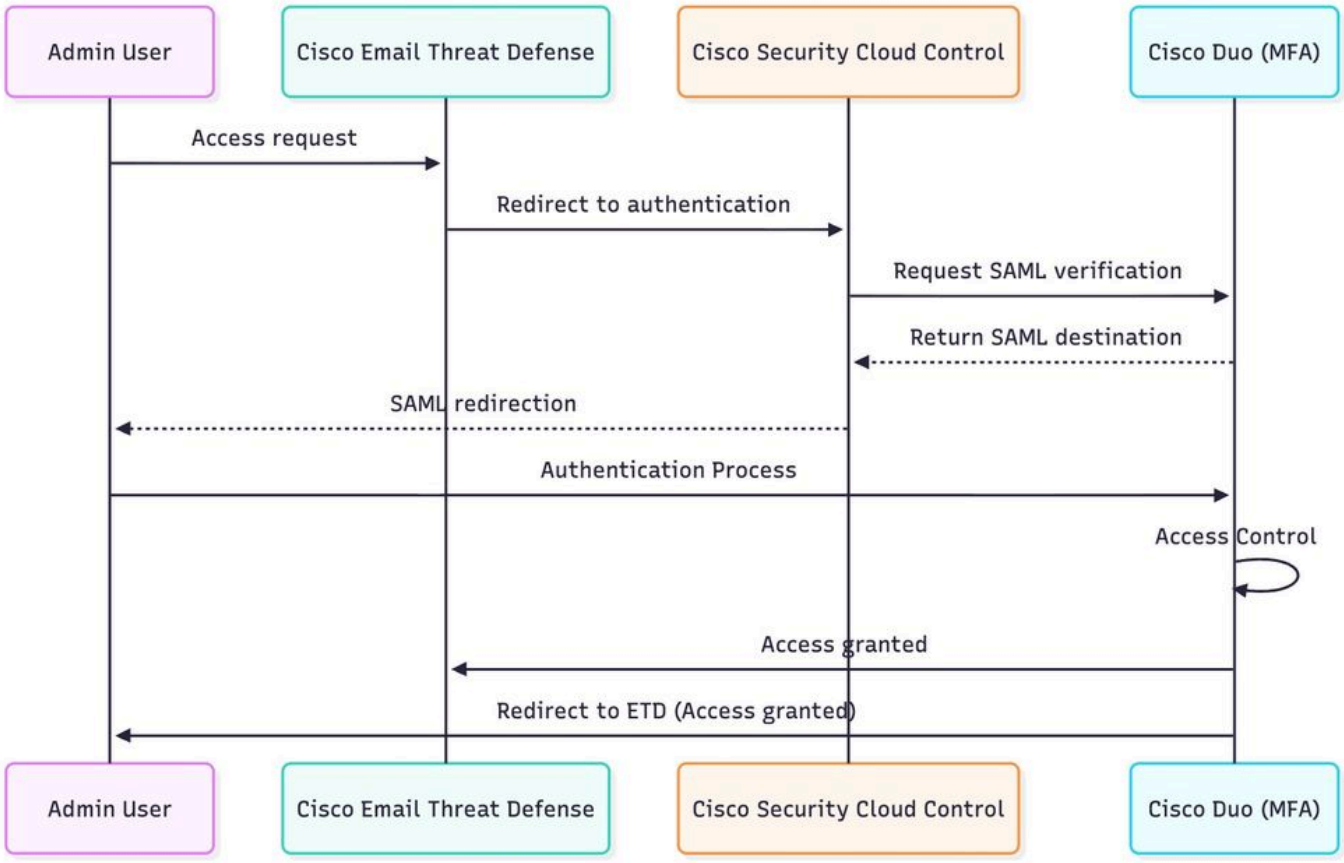
Note: Este documento fornece uma visão geral das etapas básicas necessárias para ativar o controle de acesso no Email Threat Defense (ETD) usando os recursos de autenticação de vários fatores do Cisco Duo. Implementar a integração Duo ajuda a aumentar a segurança, garantindo que apenas usuários autorizados possam acessar a plataforma. Para obter orientação abrangente, opções de configuração e cenários de implantação avançados, consulte a documentação oficial do produto:

- para gerenciamento centralizado de políticas de segurança e acesso.

Cisco Duo - para obter instruções detalhadas sobre a configuração da autenticação multifator e as práticas recomendadas.

Configuração do Cisco SCC

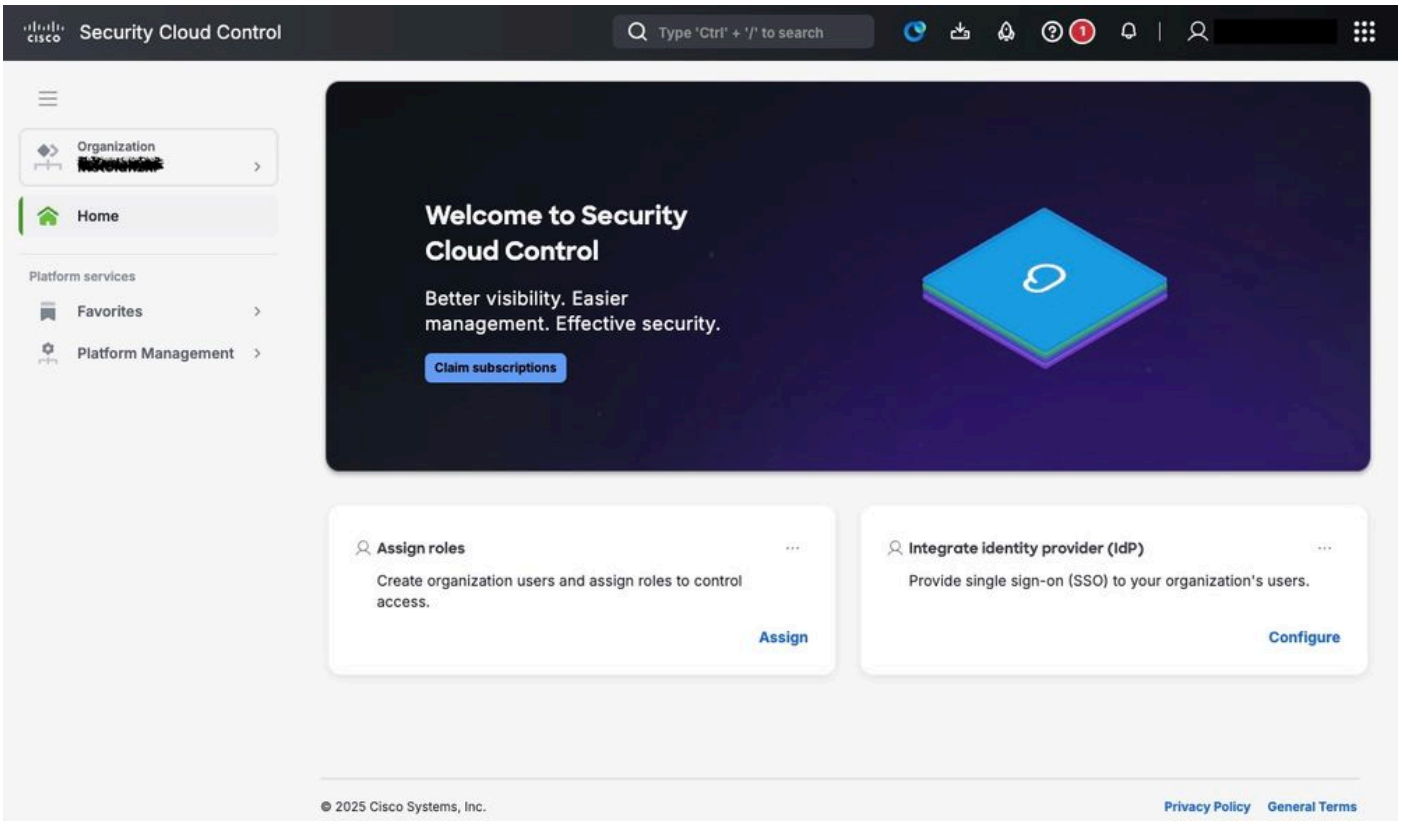
Para integrar o Cisco ETD com o Cisco Duo, a primeira etapa é configurar o domínio de autenticação no Cisco SCC. Isso estabelece a relação de confiança que permite que o Cisco SCC trabalhe com provedores de identidade externa e MFA.



Diagrama

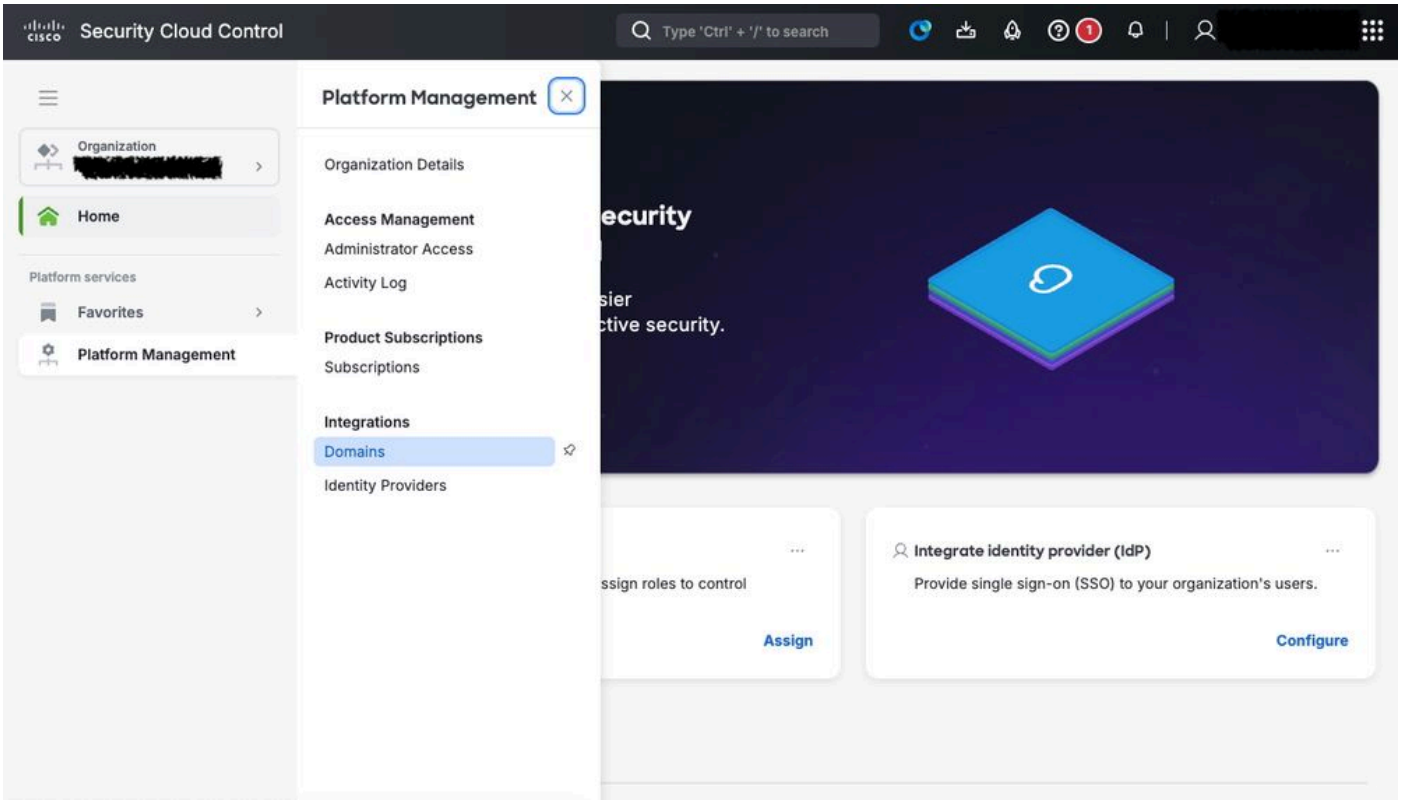
Etapa 1. Acessar o console Cisco SCC.

Faça login no portal Cisco SCC https://security.cisco.com/.



Etapa 2. Navegue até Gerenciamento de Domínio.

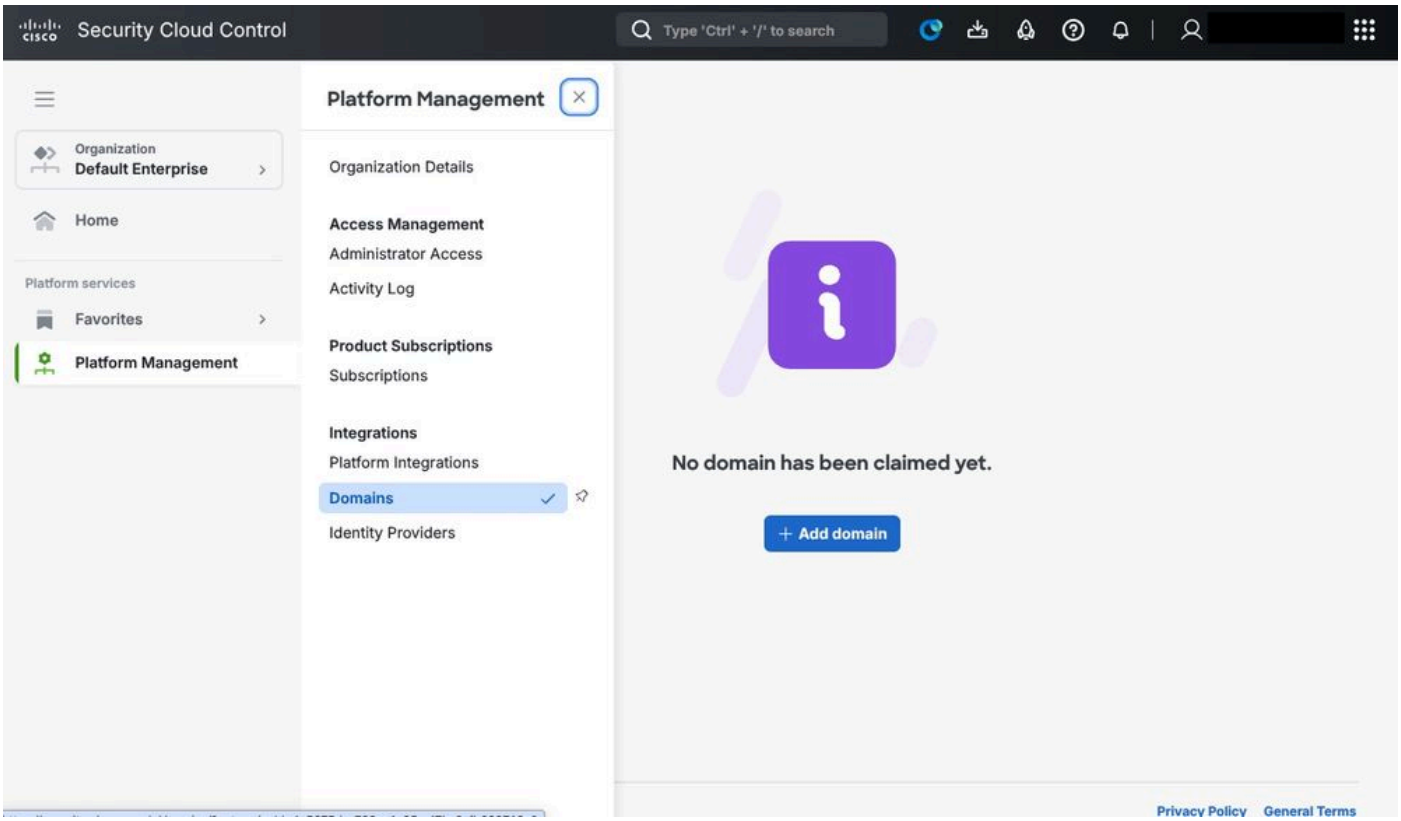
No menu principal, navegue para Gerenciamento de plataforma > Domínios.



Configuração segura do domínio de controle de nuvem

Etapa 3. Adicionar um novo domínio.

Clique em Add Domain para iniciar o processo de registro do domínio de autenticação.

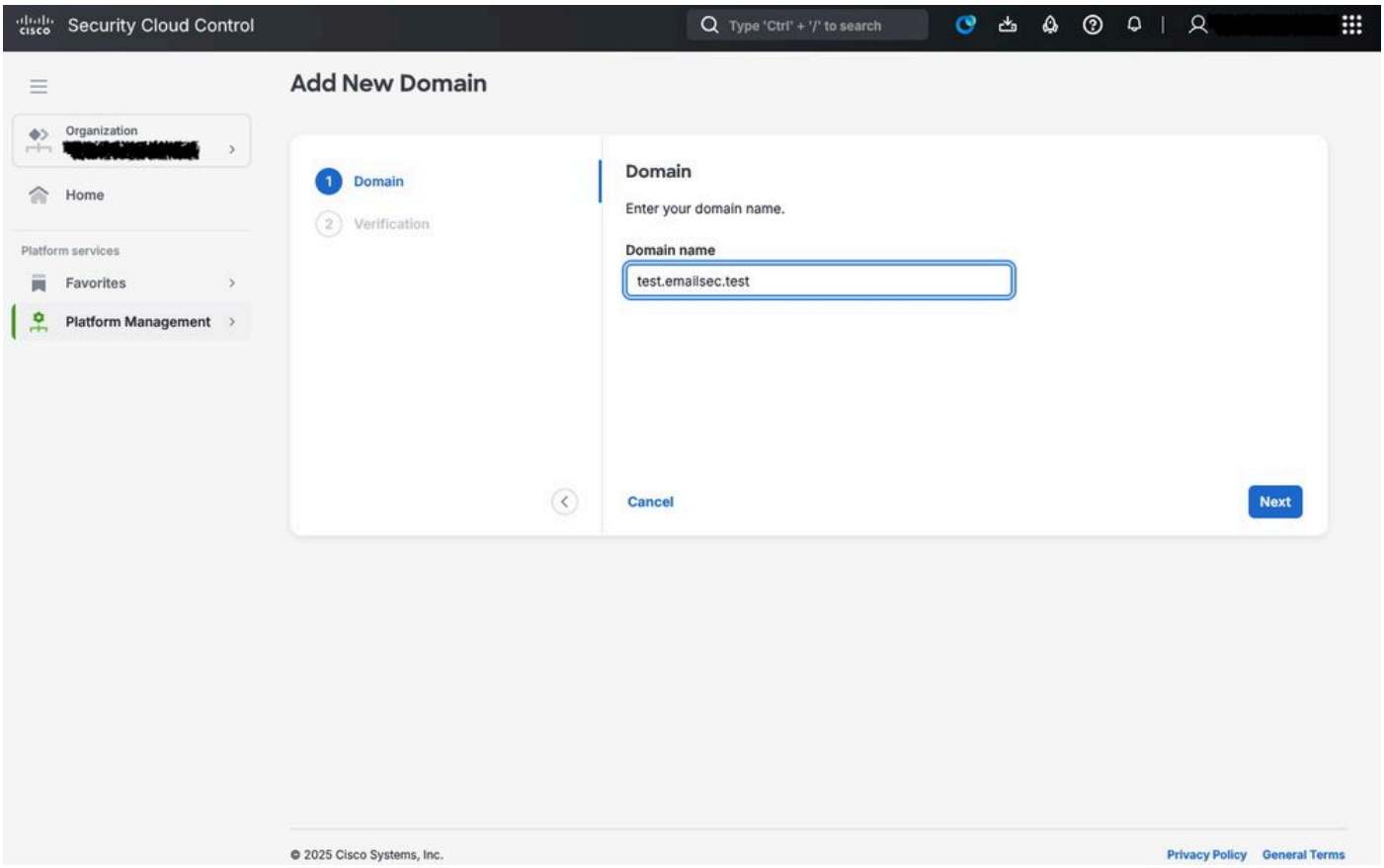


Controle de nuvem de segurança: domínio

Etapa 4. Fornecer as Informações do Domínio.

Preencha o formulário com os detalhes do domínio usado para autenticação. Isso normalmente inclui:

- O nome do domínio (por exemplo, test.emailsec.test)
- Informações de contato (administrativas e técnicas)
- Parâmetros de autenticação, dependendo do provedor de identidade escolhido



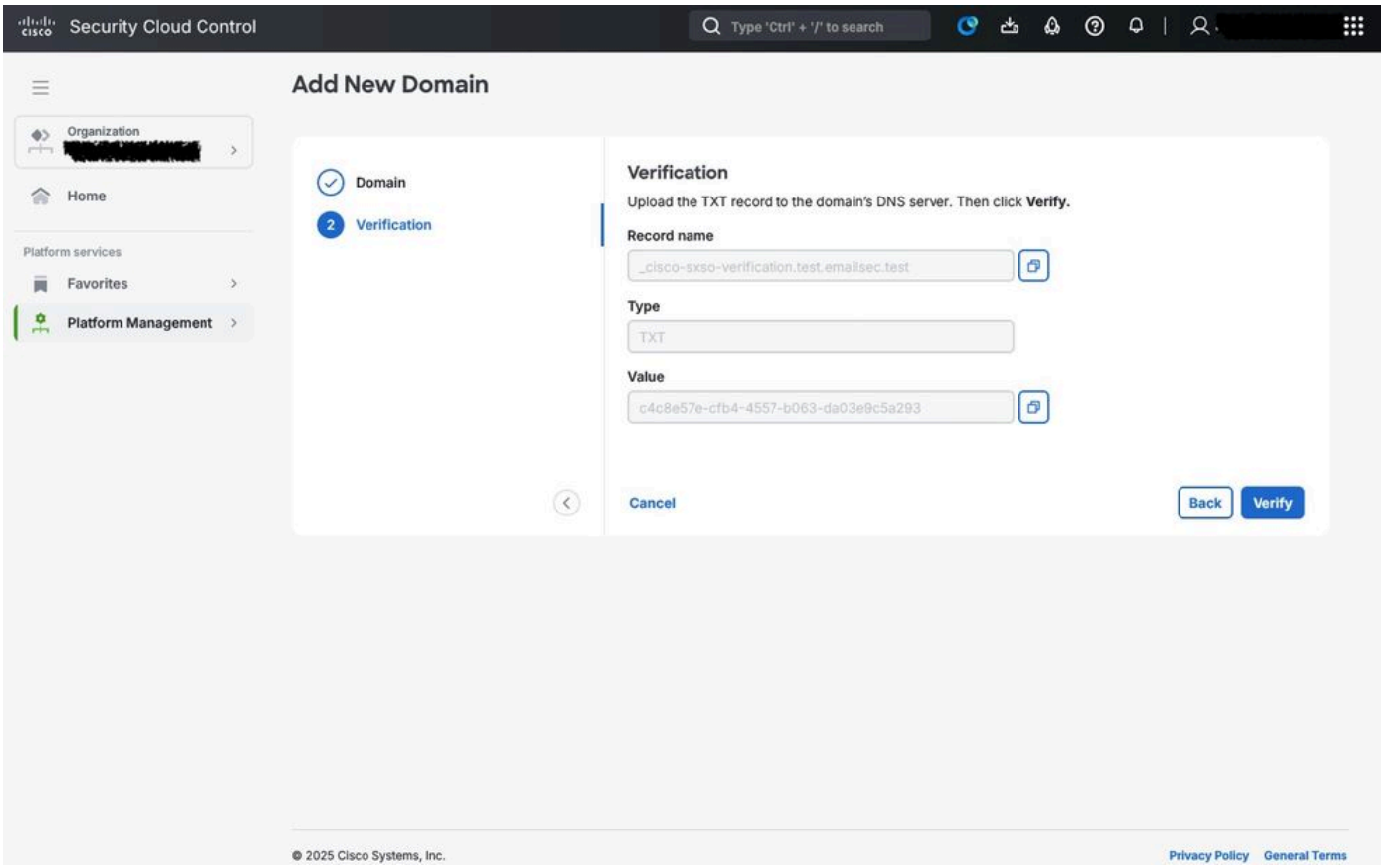
Etapa 5. Verificação de Domínio via DNS.

Depois que o domínio tiver sido registrado, a Cisco exigirá prova de propriedade.

- Um registro de verificação é fornecido pelo CSCC
- Esse registro deve ser adicionado à configuração DNS do domínio (geralmente como um registro TXT)
- O Cisco Secure Cloud valida automaticamente a entrada DNS para confirmar se o domínio pertence à sua organização

---

⚠ Caution: O processo de verificação deve ser concluído com êxito para que você possa prosseguir com a integração. Dependendo da propagação do DNS, a validação leva de vários minutos a algumas horas.



Como conectar o ETD ao Cisco Duo usando o Cisco SCC

Depois que o domínio do administrador tiver sido configurado com êxito (o que serve de base para aplicar controles de acesso mais rígidos e gerenciar privilégios), a próxima etapa é integrar o serviço MFA contratado.

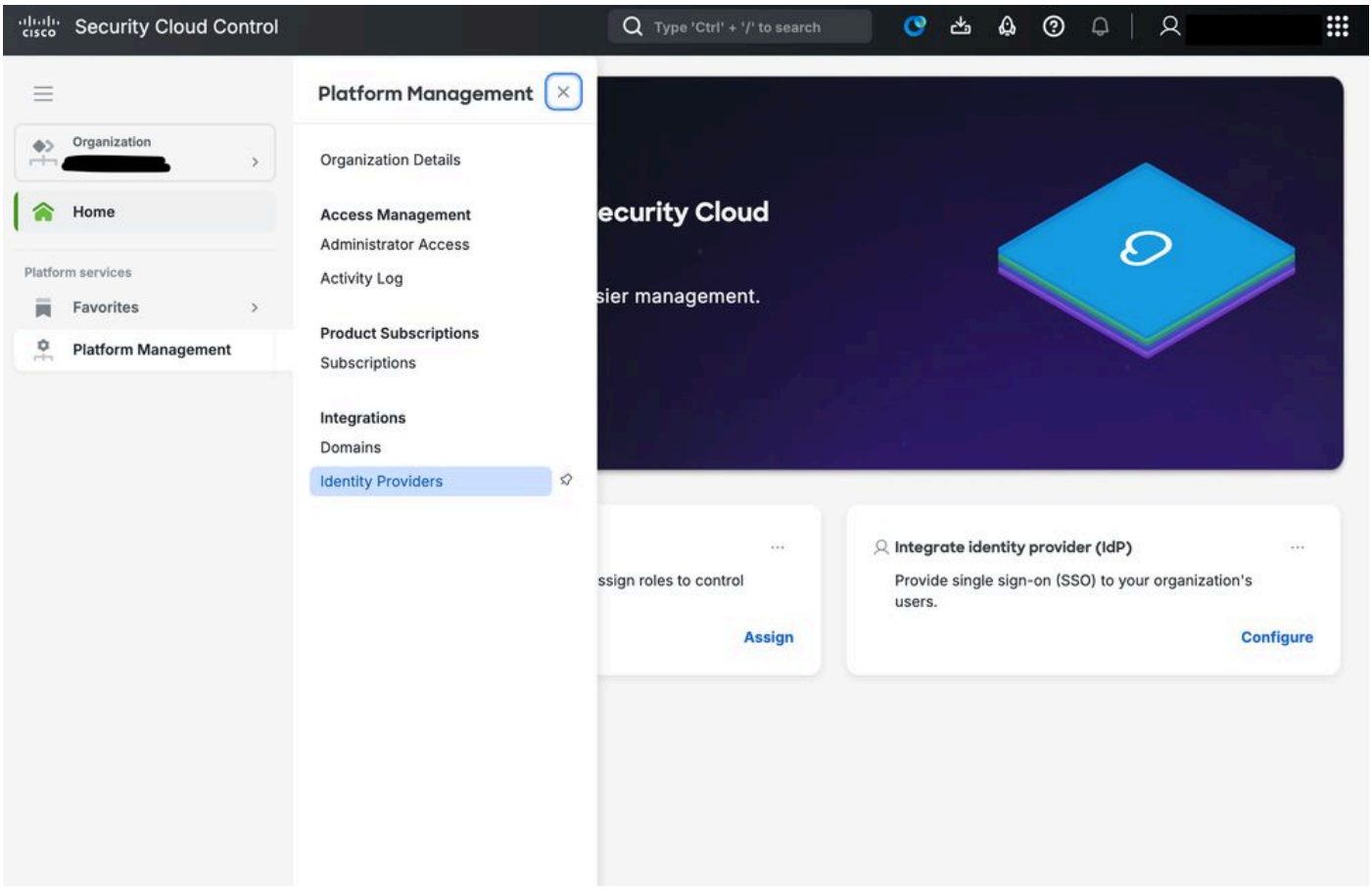
Neste cenário, o Cisco Duo é implementado como a solução primária para controle de acesso, login seguro e verificação de MFA. Essa integração aprimora a postura de segurança do ambiente exigindo que os administradores autentiquem sua identidade por meio de várias etapas de verificação, reduzindo o risco de acesso não autorizado e garantindo a conformidade com as políticas de segurança organizacionais.

Integração do Cisco Duo e do Cisco Cloud Control

Etapa 1. Acesso ao console Cisco SCC.

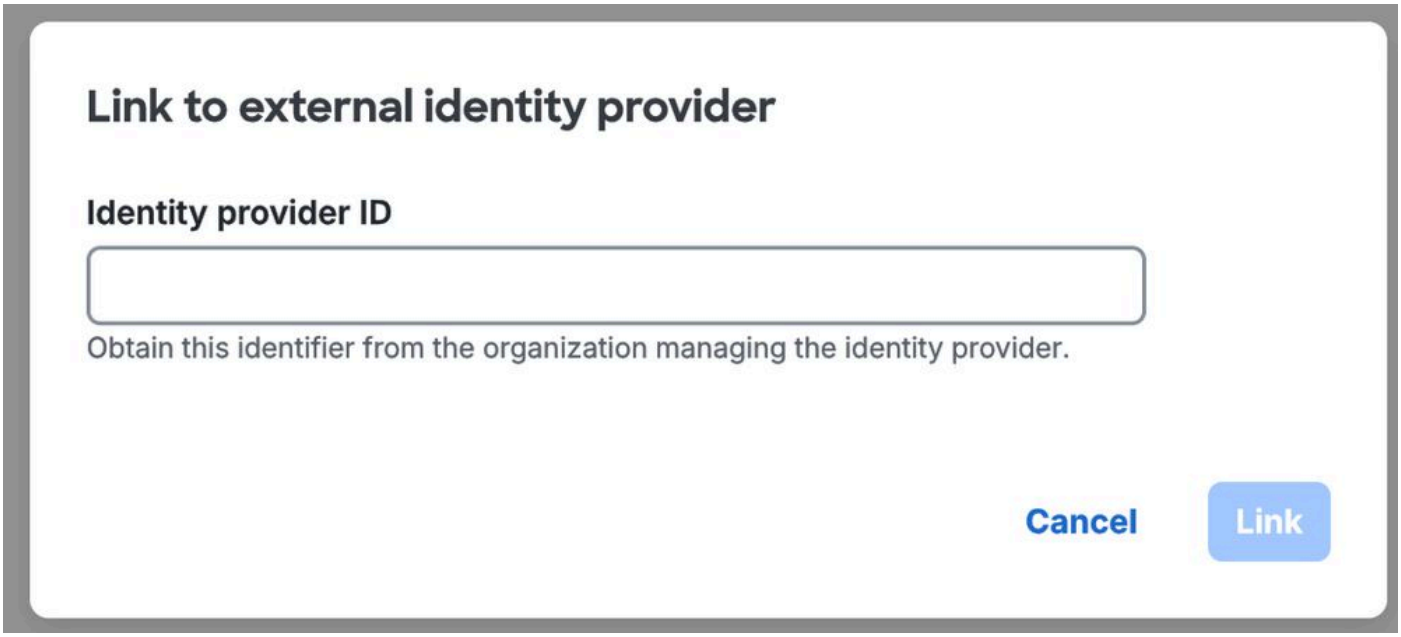
Faça login no portal Cisco Security Cloud Control https://security.cisco.com/.

Navegue até Gerenciamento de plataforma e clique em Provedores de identidade.



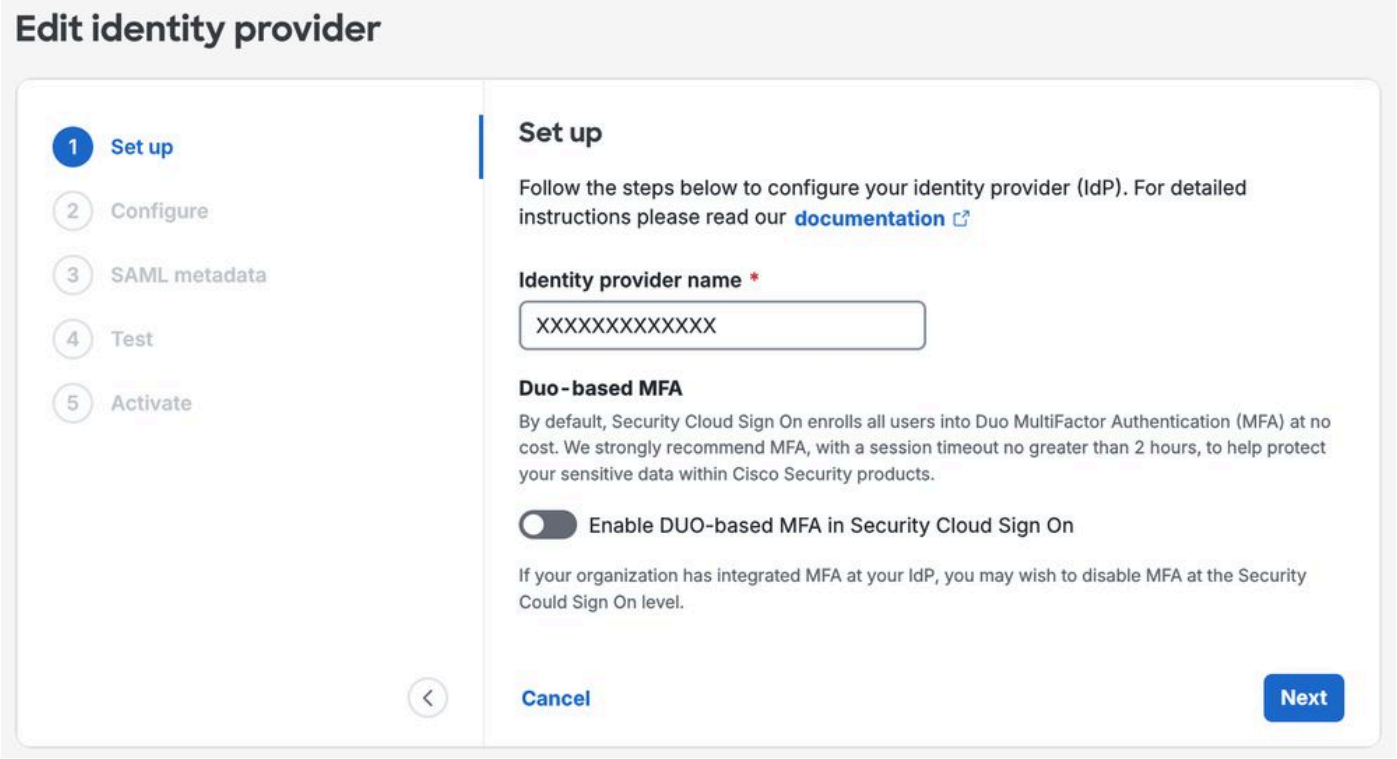
configuração SCC IDP

Use um nome personalizado para identificar o provedor de identidade.



Agora a configuração começa. Neste momento, você tem acesso ao Cisco SCC e ao Cisco Duo.

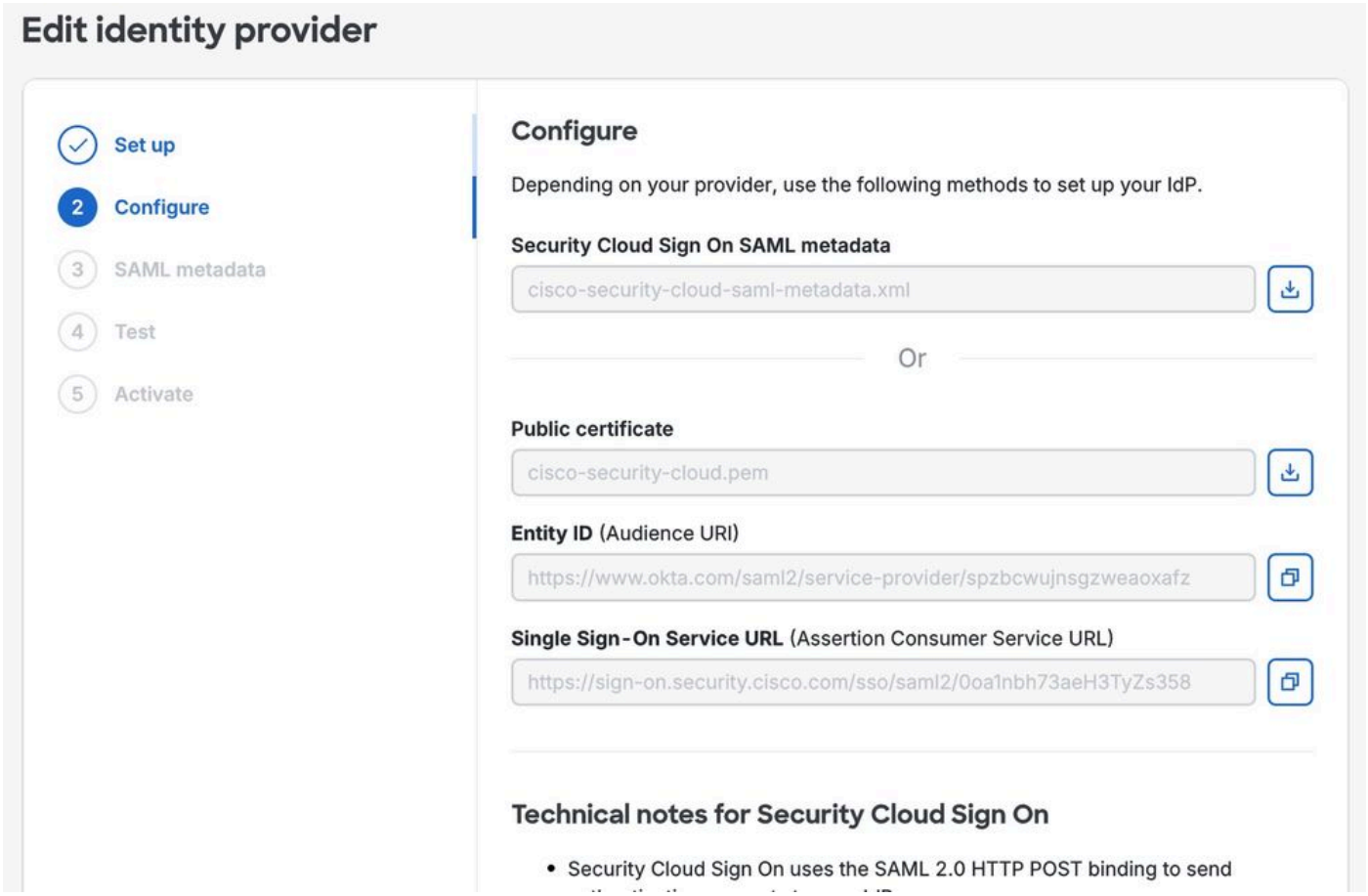
Etapa 2. No SCC, desabilite Habilitar MFA baseado em DUO em Segurança Cloud Sing On, como mostrado na imagem, e clique em Avançar.



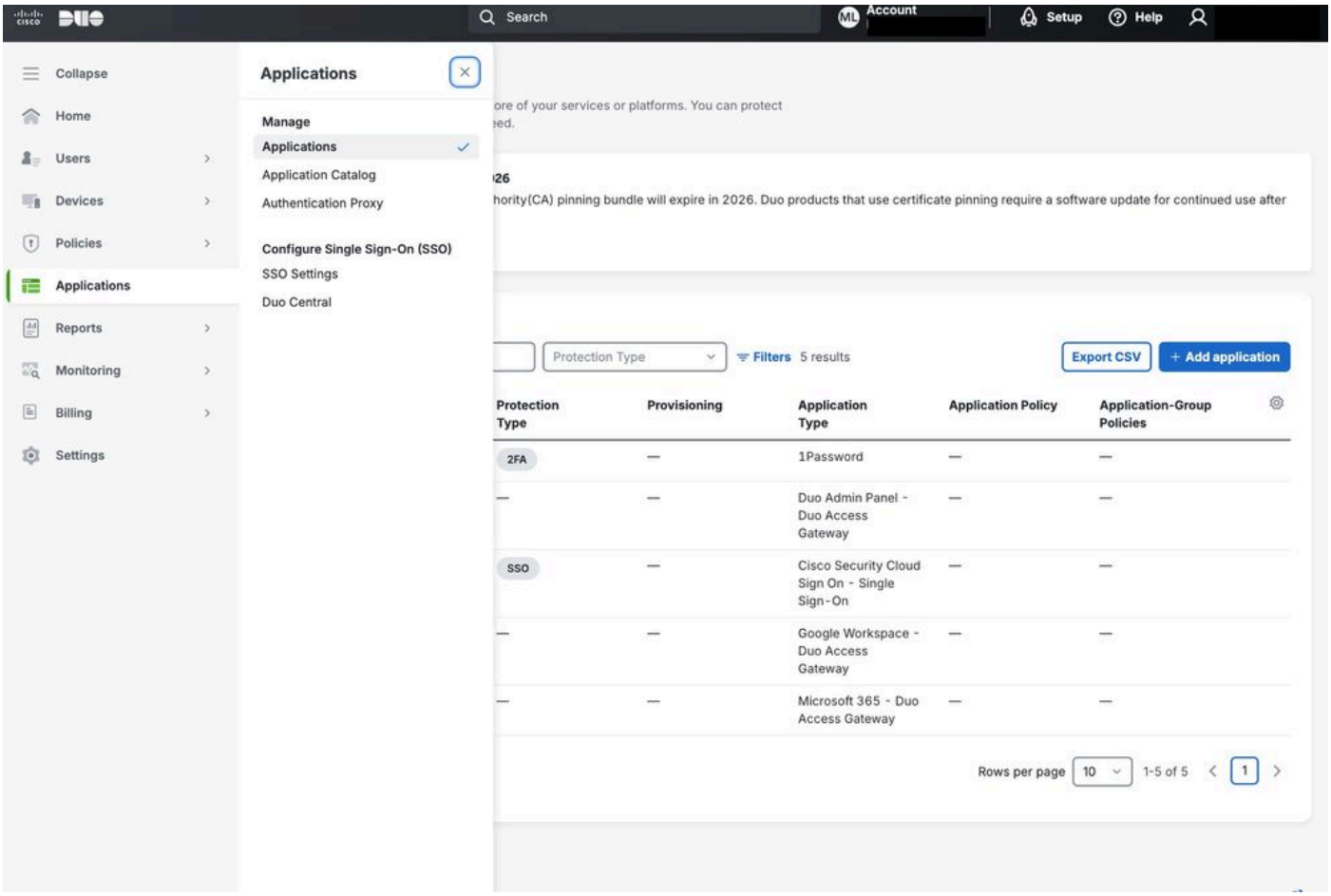
Configuração do provedor de identidade

Etapa 3. Os dados relevantes são criados e usados durante a configuração do Cisco Duo. Certifique-se de copiar todos os valores necessários e dados associados e armazená-los em um local seguro.

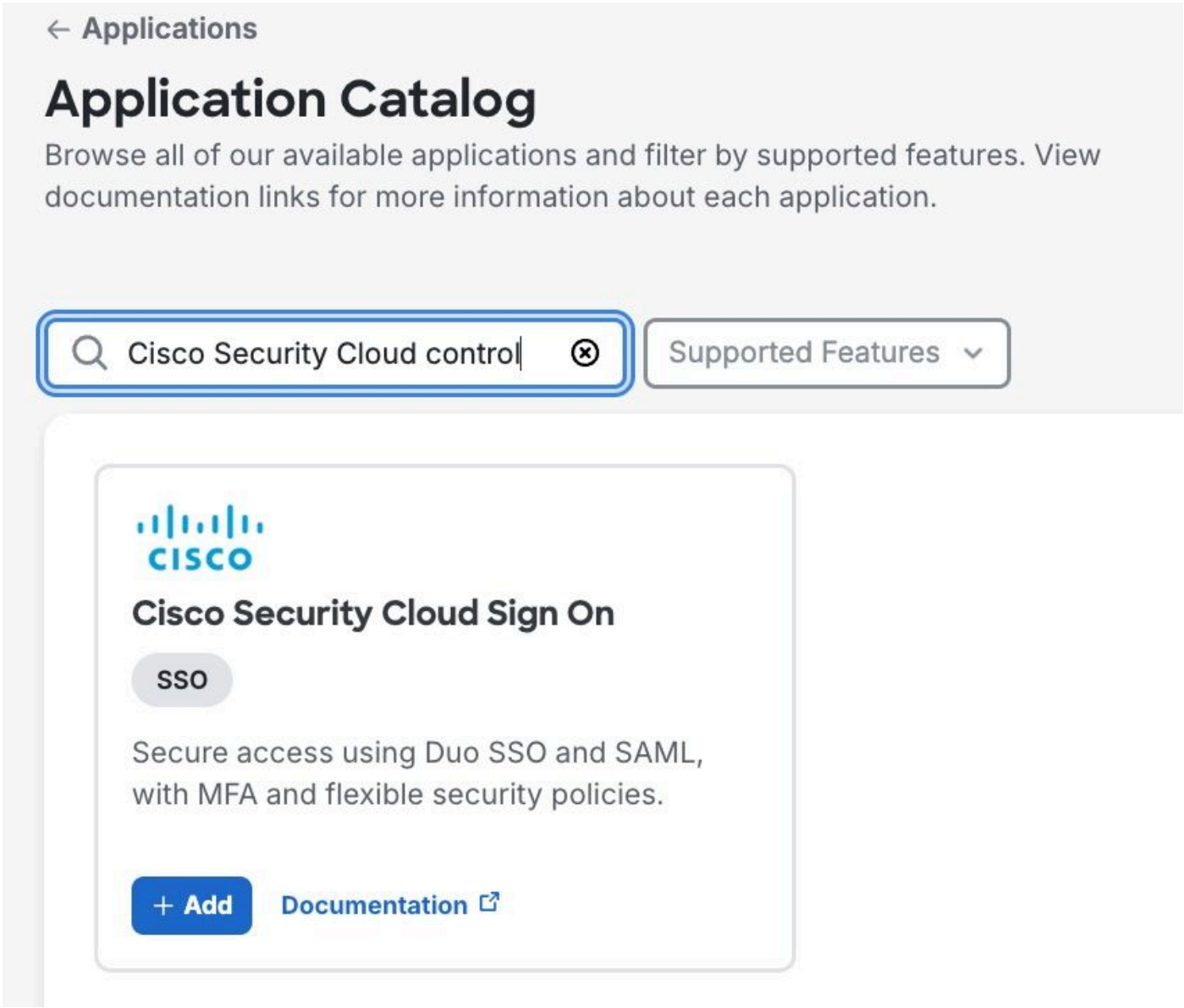
Esses detalhes são essenciais para etapas futuras de integração, portanto, certifique-se de que estejam acessíveis apenas para o pessoal autorizado e protegidos de acordo com as políticas de segurança da sua organização.



Etapa 4. Abra o Cisco Duo, navegue para a seção Aplicativos e clique em Adicionar aplicativo.

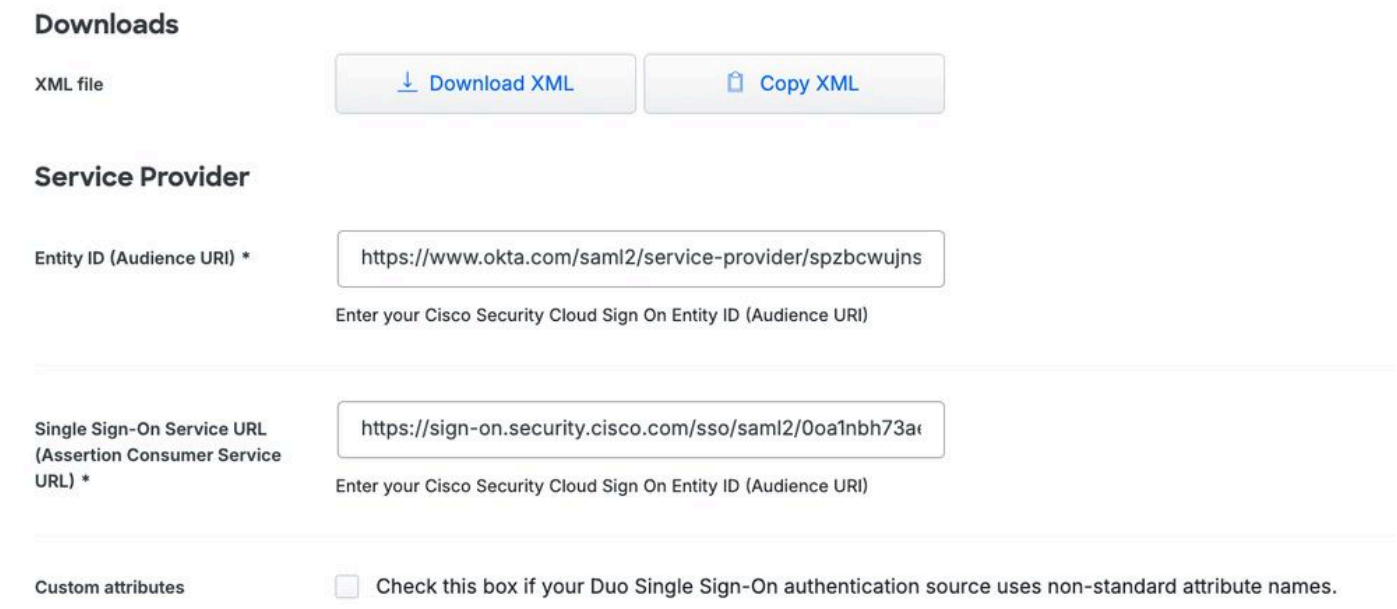


No menu, procure Cisco Security Cloud e clique em Add para iniciar a integração.

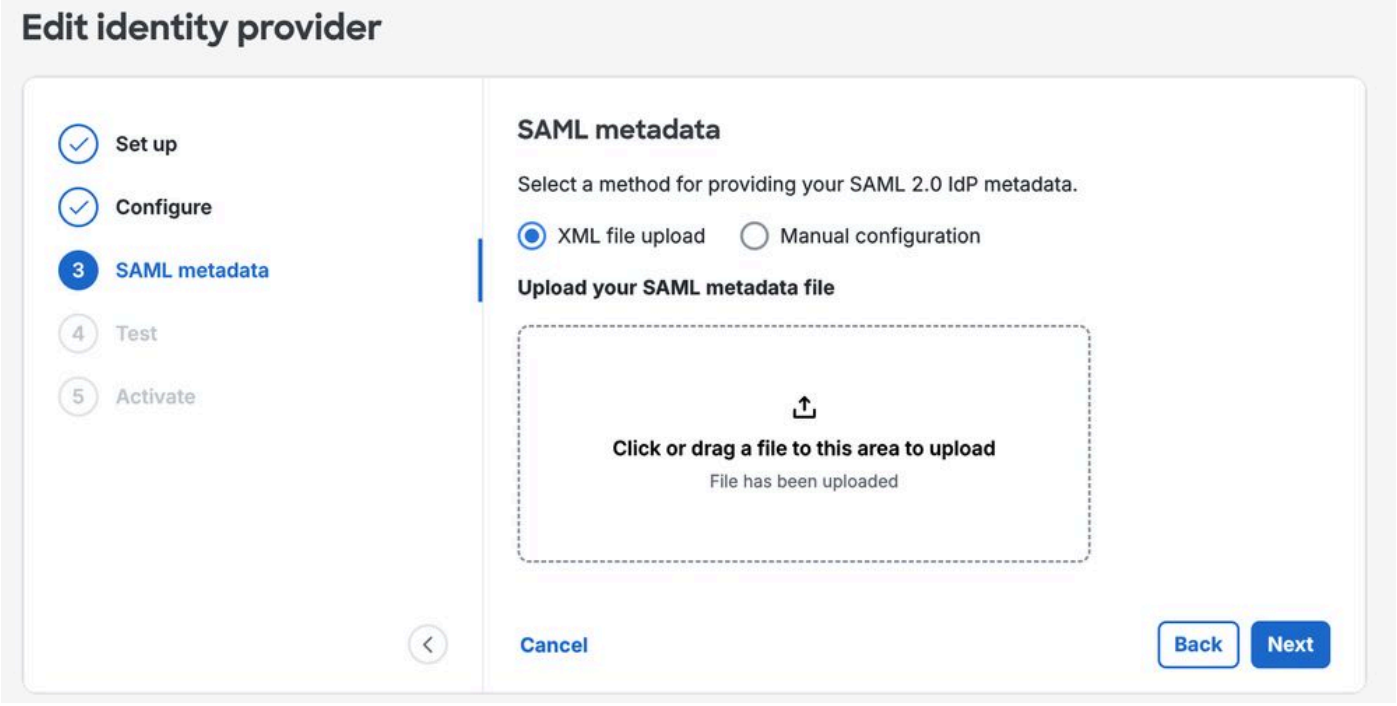


Etapa 5. Configurar as informações relevantes no aplicativo Cisco Duo.

Copie a ID da entidade e a URL do serviço de sign-on único do Cisco SCC para o Cisco Duo.



Etapa 6. Faça o download do XML e carregue o arquivo no Cisco SCC.



Note: Os parâmetros restantes que podem ser configurados no aplicativo a partir do console Cisco Duo devem ser ajustados de acordo com seus requisitos específicos. As explicações detalhadas para cada uma dessas configurações podem ser encontradas na documentação oficial do Cisco Duo. Exemplos de parâmetros configuráveis incluem o nome do aplicativo atribuído, o conjunto de usuários aos quais a política se aplica e outras opções de personalização que podem ajustar os controles de segurança para atender às necessidades da sua organização.

Configuração de política no Cisco Duo para Cisco ETD

Neste estágio, todos os componentes são conectados e a próxima etapa é configurar uma política que se aplica ao processo de autenticação do administrador no console Cisco ETD.

Neste exemplo, o foco está especificamente no controle de acesso com base no endereço IP. No entanto, o Cisco Duo oferece muitas outras opções de controle de acesso.

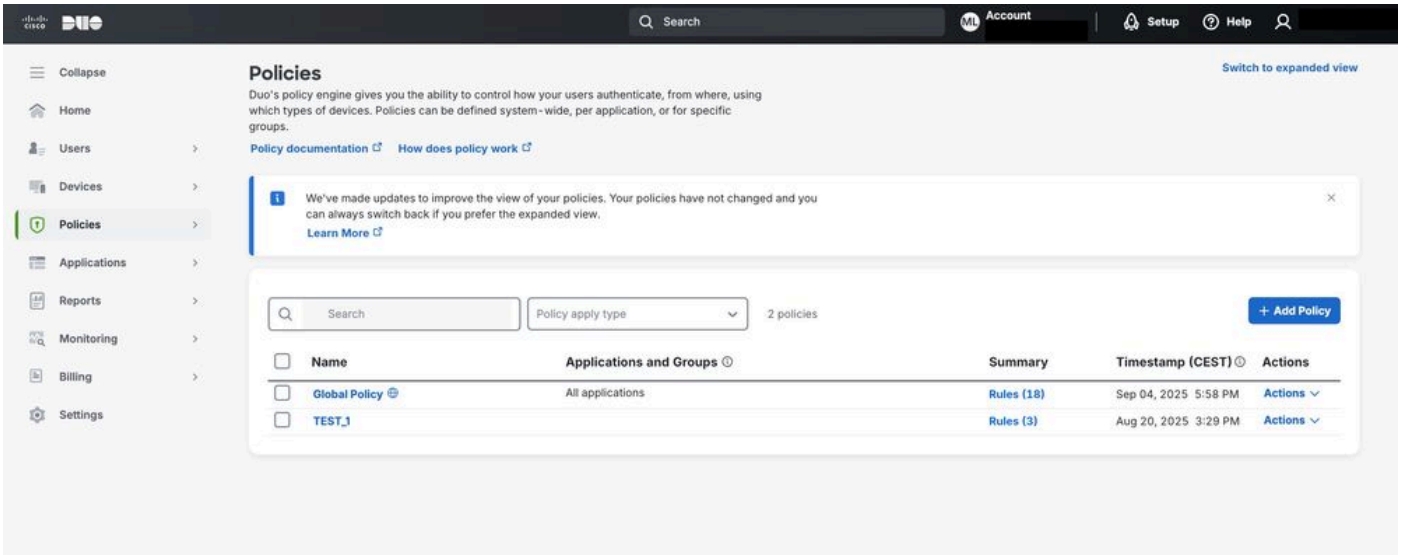
Uma nova política pode ser criada e atribuída ao aplicativo, permitindo a aplicação das regras de autenticação desejadas e restrições de segurança para logons do administrador.

Para obter informações mais detalhadas sobre todos os controles e opções de configuração disponíveis no Cisco Duo, consulte a documentação oficial do Cisco Duo.

Este recurso oferece orientação abrangente sobre configuração, personalização e práticas recomendadas para ajudar a otimizar as políticas de segurança.

Navegando para a seção Policies no Cisco Duo, uma política pode ser criada e atribuída à conexão Cisco ETD através do Cisco Duo.

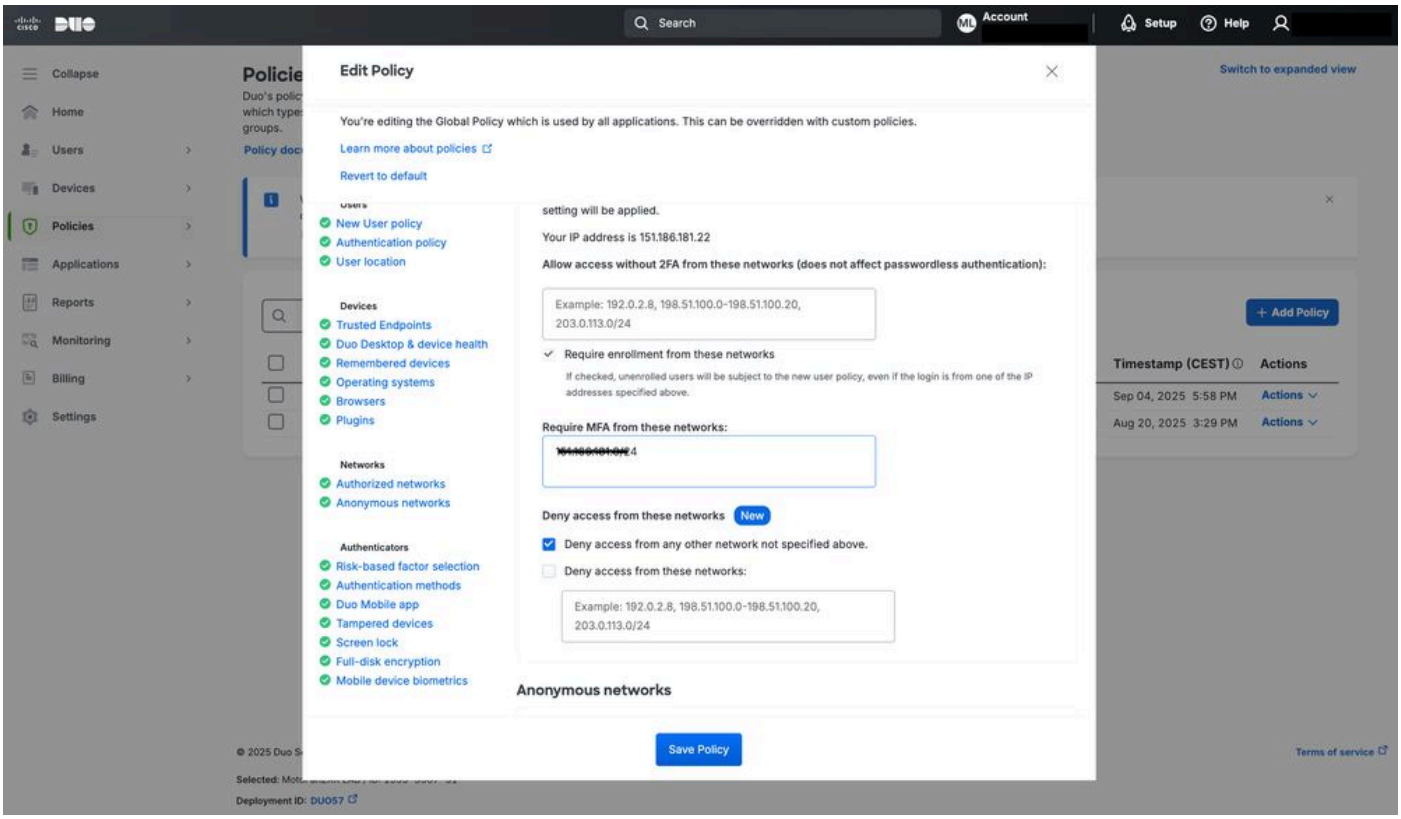
Essa política pode ser aplicada por usuário ou grupo, dependendo dos requisitos de acesso.



Cisco Duo

Neste exemplo, como mostrado na imagem, o controle de acesso do IP de origem é ativado pela configuração da seção Redes autorizadas.

Essa configuração permite acesso somente de intervalos de IP confiáveis especificados, aumentando a segurança do Cisco ETD.



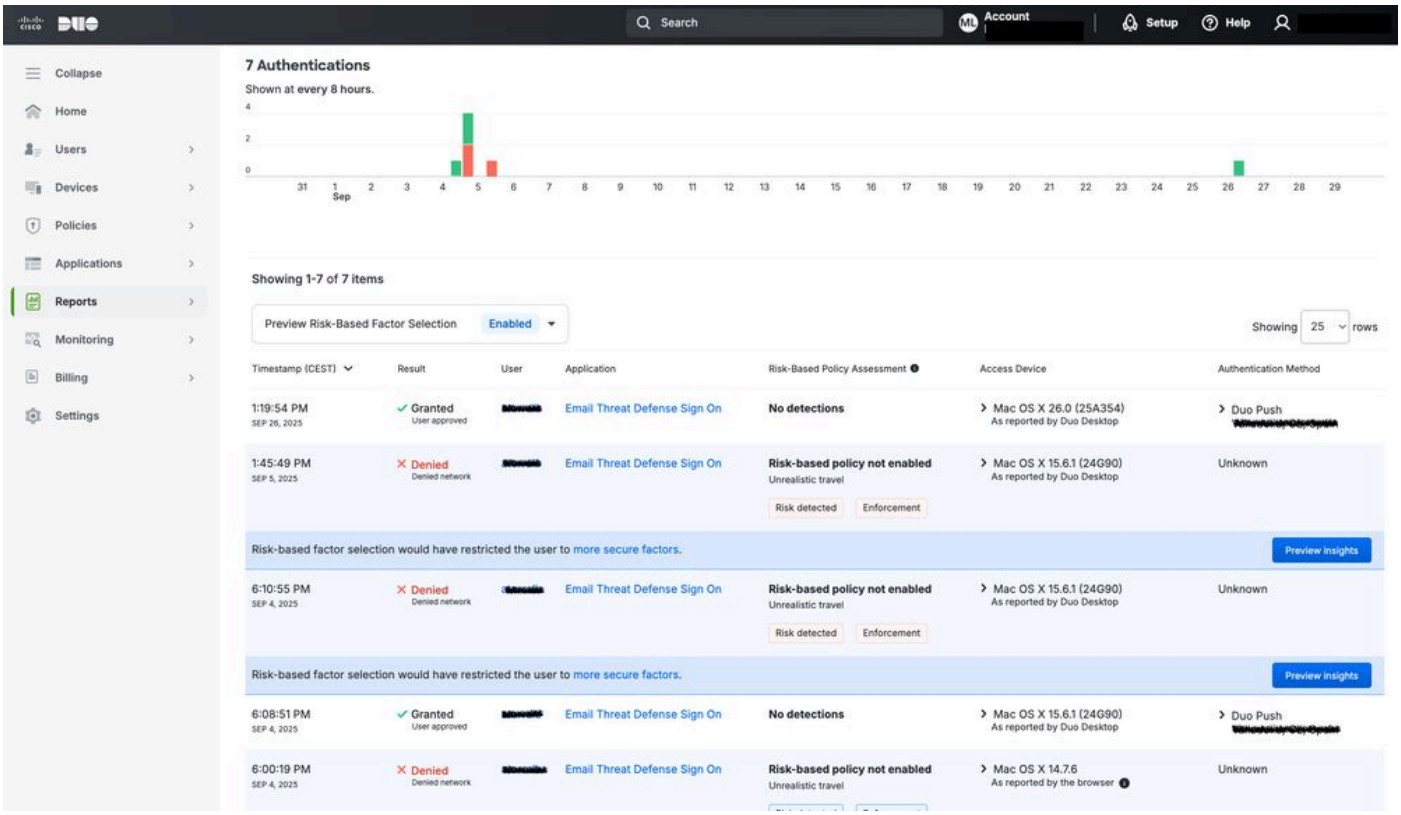
Configuração de política do Cisco Duo

Conclusões

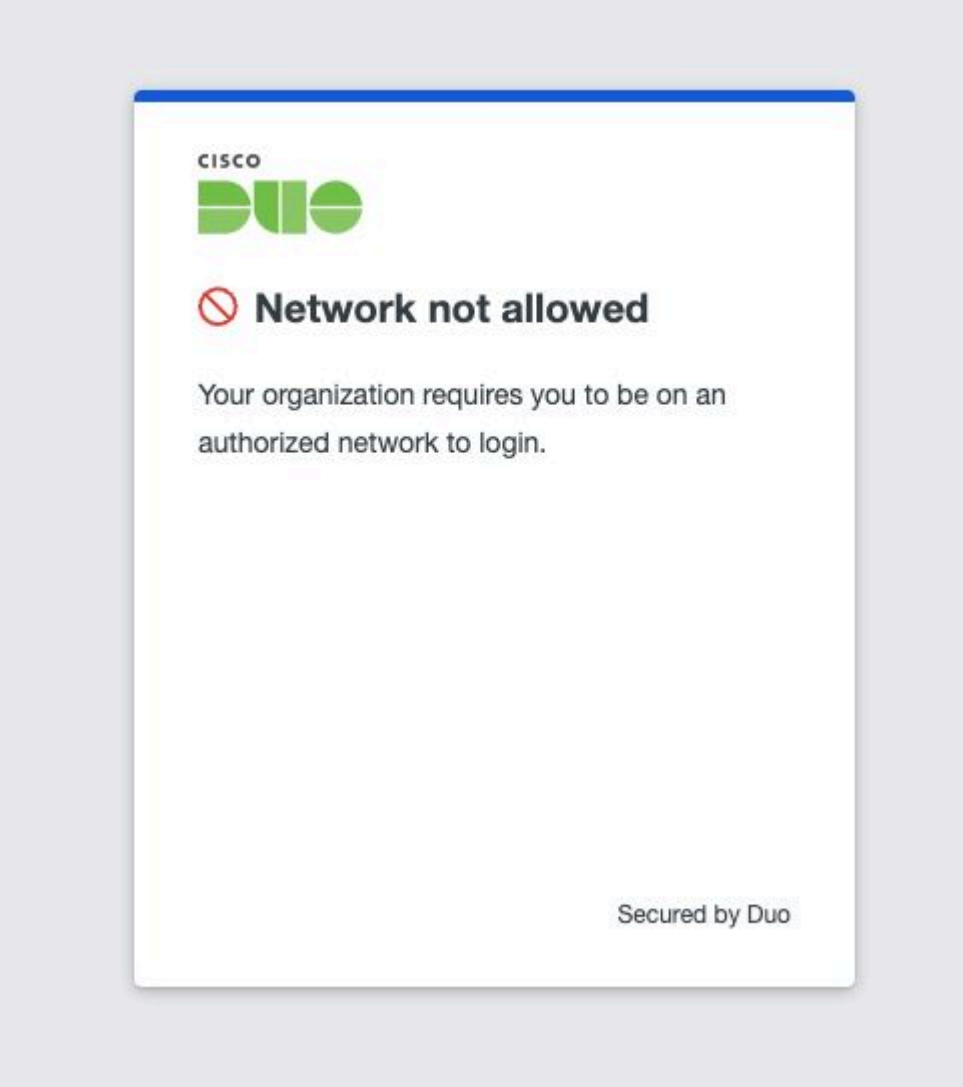
O Cisco ETD oferece opções flexíveis para proteger o acesso do administrador através do MFA e da integração com provedores de identidade.
Ao combinar o Cisco SCC com o Cisco Duo, as organizações podem implementar políticas de autenticação mais fortes, reduzir o risco de acesso não autorizado e alinhar-se com as práticas recomendadas do setor para gerenciamento seguro de serviços em nuvem.

Além do MFA, os administradores podem aproveitar os controles baseados em políticas do Cisco Duo para restringir o acesso com base em critérios específicos, como o endereço IP de origem. Por exemplo, como ilustrado na imagem a seguir, uma tentativa de acesso de um endereço IP fora do intervalo autorizado é automaticamente bloqueada pelo sistema. Isso garante que somente as solicitações originárias de redes confiáveis sejam permitidas, adicionando uma camada extra de proteção contra possíveis ataques.

Ao implementar o controle de acesso baseado em IP junto com o MFA, as empresas obtêm uma abordagem de defesa profunda, combinando verificação de identidade com validação de local de rede para proteger interfaces de gerenciamento críticas na nuvem.



Relatórios do Cisco Duo



Resultado do controle de rede

---

aviso: É importante entender que essa alteração afeta todos os aplicativos que usam o mesmo domínio de autenticação; não apenas ETD, mas também outros produtos que dependem do mesmo processo de autenticação, como o acesso ao console Cisco Secure Access.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.