Protection contre les menaces : Authentification multifacteur et contrôles d'accès

Table des matières

Introduction

Ce document décrit les fonctionnalités offertes par Cisco Email Threat Defense (ETD) pour contrôler l'accès administrateur à la console de gestion.

Conditions préalables

Exigences

Cisco recommande que vous ayez connaissance de ces sujets afin de configurer l'authentification ETD avec Duo :

- Un abonnement Cisco ETD
- Accès à Cisco Security Cloud Control (SCC)
- Une solution d'authentification pour une sécurité renforcée, dans ce cas, Cisco Duo.

Composants utilisés

Ce document est limité à la défense contre les attaques par e-mail et au contrôle cloud sécurisé.

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 votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Ce document se concentre sur la façon dont Cisco ETD exploite Cisco SCC et s'intègre à Cisco Duo pour fournir une authentification sécurisée et un contrôle d'accès granulaire.

Dans les solutions cloud modernes, le contrôle d'accès est l'un des composants les plus essentiels pour garantir la sécurité des données, la conformité aux réglementations et l'intégrité opérationnelle. L'accès non autorisé, en particulier aux comptes d'administrateur, peut entraîner de graves conséquences telles que des systèmes compromis, des fuites de données et des interruptions de service.

Cisco propose des fonctionnalités de sécurité robustes dans l'ensemble de sa gamme de solutions cloud, notamment la technologie MFA (Multifactor Authentication), qui fait partie intégrante de services tels que Cisco ETD. MFA ajoute une étape de vérification critique au-delà des mots de passe traditionnels, exigeant que les utilisateurs s'authentifient via un facteur supplémentaire tel qu'une approbation d'application mobile, un jeton de sécurité ou une vérification biométrique.

Afin de rationaliser et de renforcer le processus d'authentification de l'administrateur, ETD s'appuie sur Cisco SCC, un service centralisé d'authentification et de gestion des politiques.

Grâce à SCC, ETD a accès à un large éventail de fonctions de sécurité, notamment :

- Application des AMF pour limiter les risques de vol d'informations d'identification.
- Intégration avec des fournisseurs d'identité tiers tels que Cisco Duo, Microsoft Entra ID, Okta et autres pour prendre en charge des workflows d'authentification flexibles et la fédération des identités d'entreprise.
- Administration centralisée des politiques, permettant des règles d'accès cohérentes sur l'ensemble des services cloud Cisco.

Cisco Duo, en particulier, étend ces fonctionnalités en ajoutant une gestion avancée des accès basée sur des politiques. En utilisant SCC comme canal d'intégration, ETD peut appliquer des contrôles granulaires de Duo tels que les restrictions IP source, les vérifications de l'état des périphériques et les règles basées sur les groupes d'utilisateurs directement à l'accès administrateur.

Par exemple, les organisations peuvent définir une politique qui autorise uniquement l'accès à partir de plages de réseaux sécurisés spécifiques. Toute tentative de connexion en dehors de la liste des adresses IP autorisées peut être automatiquement bloquée, comme illustré dans les schémas ci-joints. Cette combinaison de politiques MFA + contextuelles permet une approche de défense en profondeur, garantissant que même si les informations d'identification sont compromises, les pirates sont toujours empêchés d'accéder au système à moins qu'ils ne répondent également à des critères de sécurité supplémentaires.

En unifiant Cisco ETD, Cisco SCC et Cisco Duo, les entreprises peuvent mettre en oeuvre un modèle de contrôle d'accès sécurisé, évolutif et convivial, en s'alignant sur les meilleures pratiques du secteur tout en améliorant la protection des services cloud critiques.

Scénarios

Plusieurs scénarios d'authentification et de contrôle d'accès peuvent être mis en oeuvre avec ETD afin de sécuriser l'accès administratif :

1. AMF intégré : utilisez l'AMF intégré de Cisco ou intégrez l'AMF Microsoft.
2. Cisco SCC avec Cisco Duo : associez l'authentification centralisée de Cisco SCC aux fonctionnalités MFA avancées de Duo.
3. Cisco SCC avec un fournisseur d'identité externe (par exemple, Microsoft Entra ID) - Étendez les stratégies d'authentification en les intégrant aux solutions d'identité d'entreprise.

Ce document décrit les étapes de configuration du scénario 2 : Cisco SCC avec Cisco Duo, bien que le processus puisse être adapté à d'autres technologies.

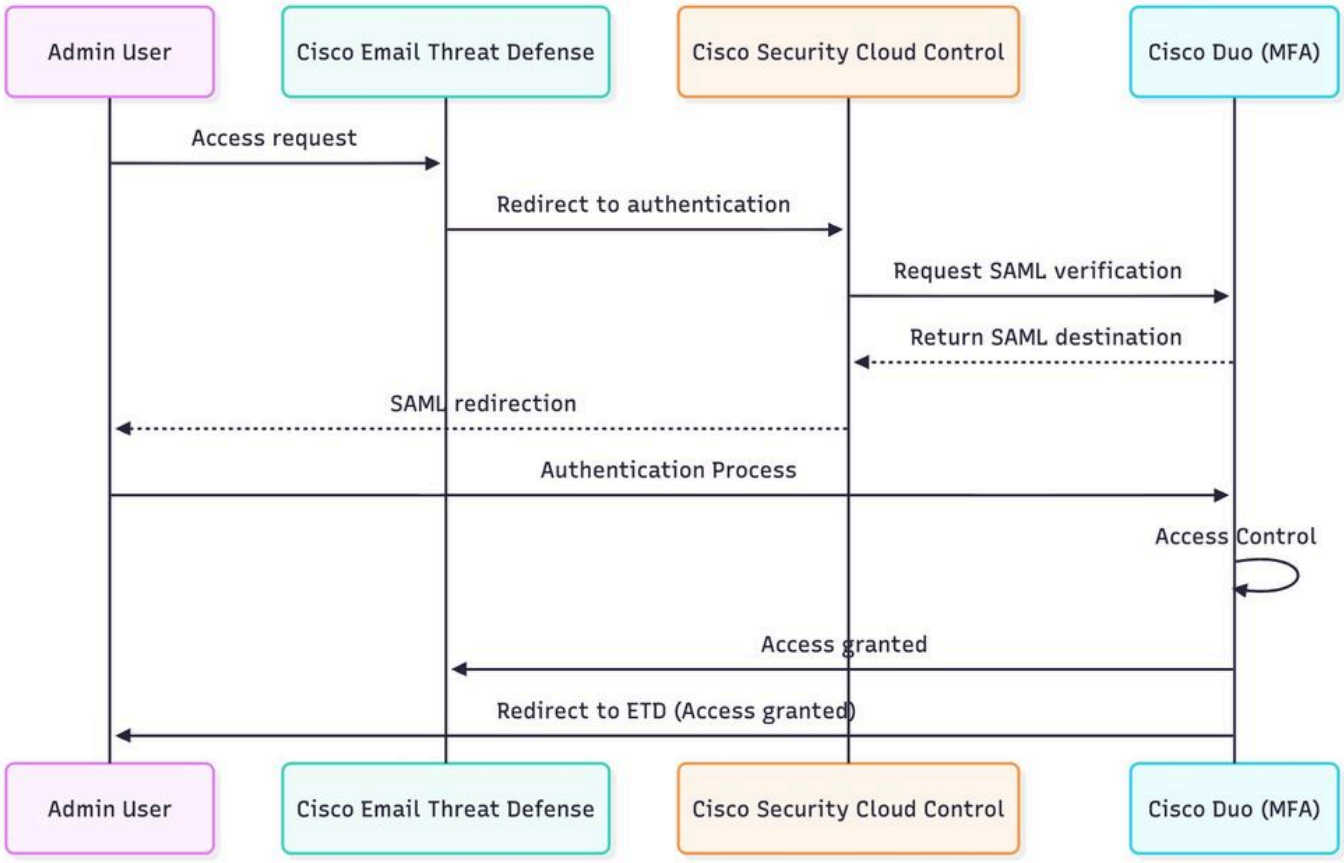
Remarque : Ce document présente les étapes de base requises pour activer le contrôle d'accès dans Email Threat Defense (ETD) à l'aide des fonctionnalités d'authentification multifacteur de Cisco Duo. La mise en oeuvre de l'intégration Duo permet d'améliorer la sécurité en garantissant que seuls les utilisateurs autorisés peuvent accéder à la plate-forme. Pour obtenir des conseils complets, des options de configuration et des scénarios de déploiement avancés, reportez-vous à la documentation officielle du produit :

- pour une gestion centralisée des accès et des politiques de sécurité.

Cisco Duo : pour obtenir des instructions détaillées sur la configuration de l'authentification multifacteur et les meilleures pratiques.

Configuration de Cisco SCC

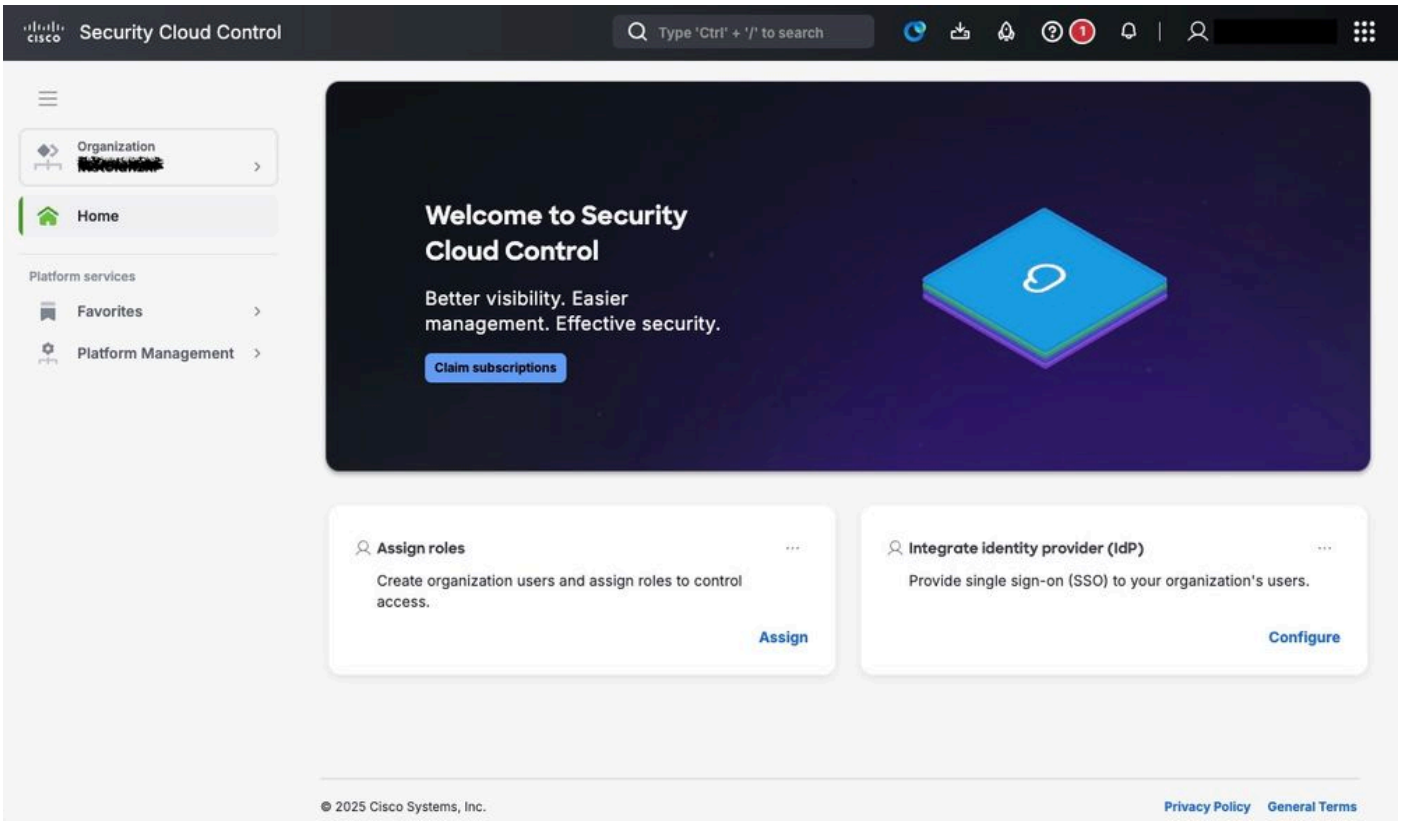
Afin d'intégrer Cisco ETD avec Cisco Duo, la première étape consiste à configurer le domaine d'authentification dans Cisco SCC. Cela établit la relation de confiance qui permet à Cisco SCC de travailler avec des fournisseurs d'identité et d'AMF externes.



Diagramme

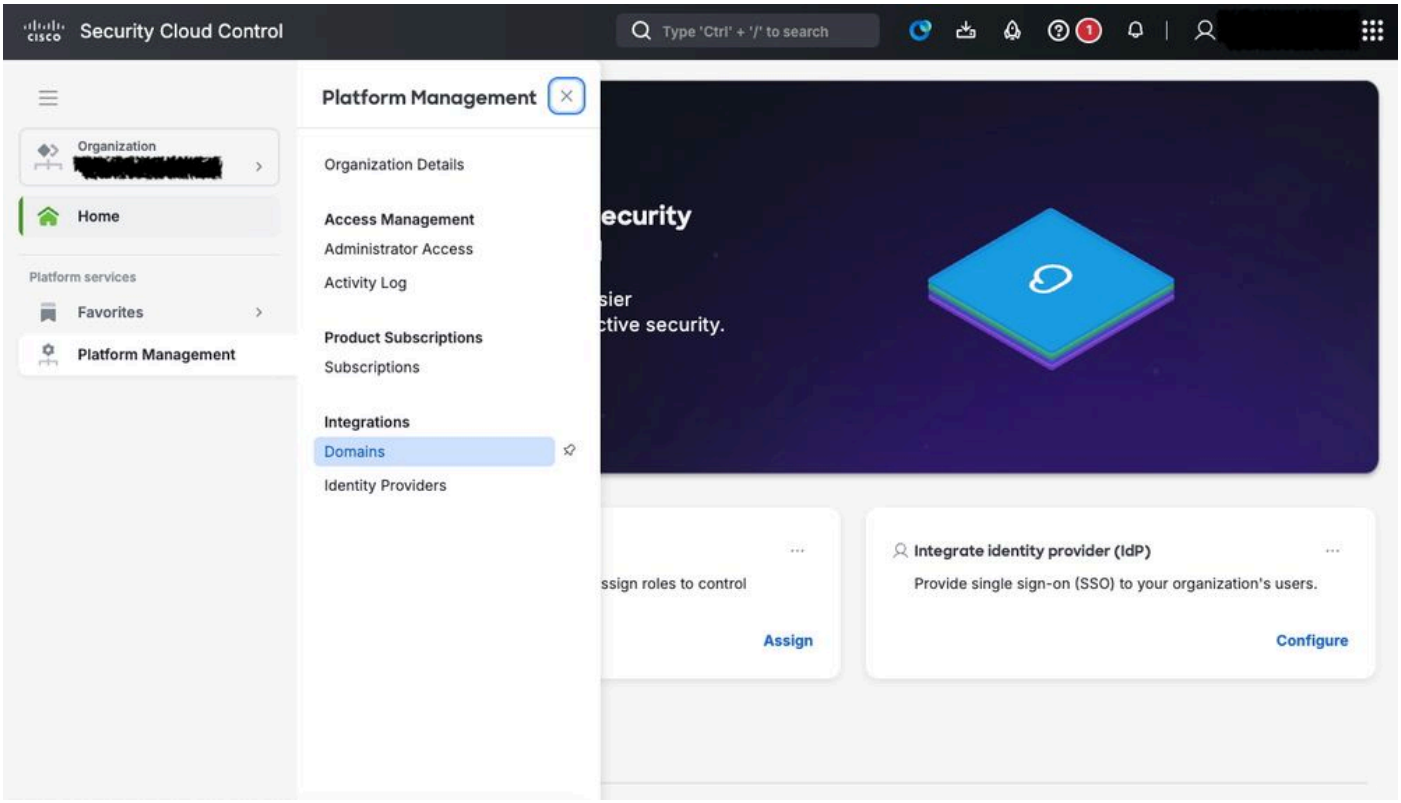
Étape 1 : accès à la console SCC de Cisco

Connectez-vous au portail Cisco SCC https://security.cisco.com/.



Étape 2. Accédez à Gestion du domaine.

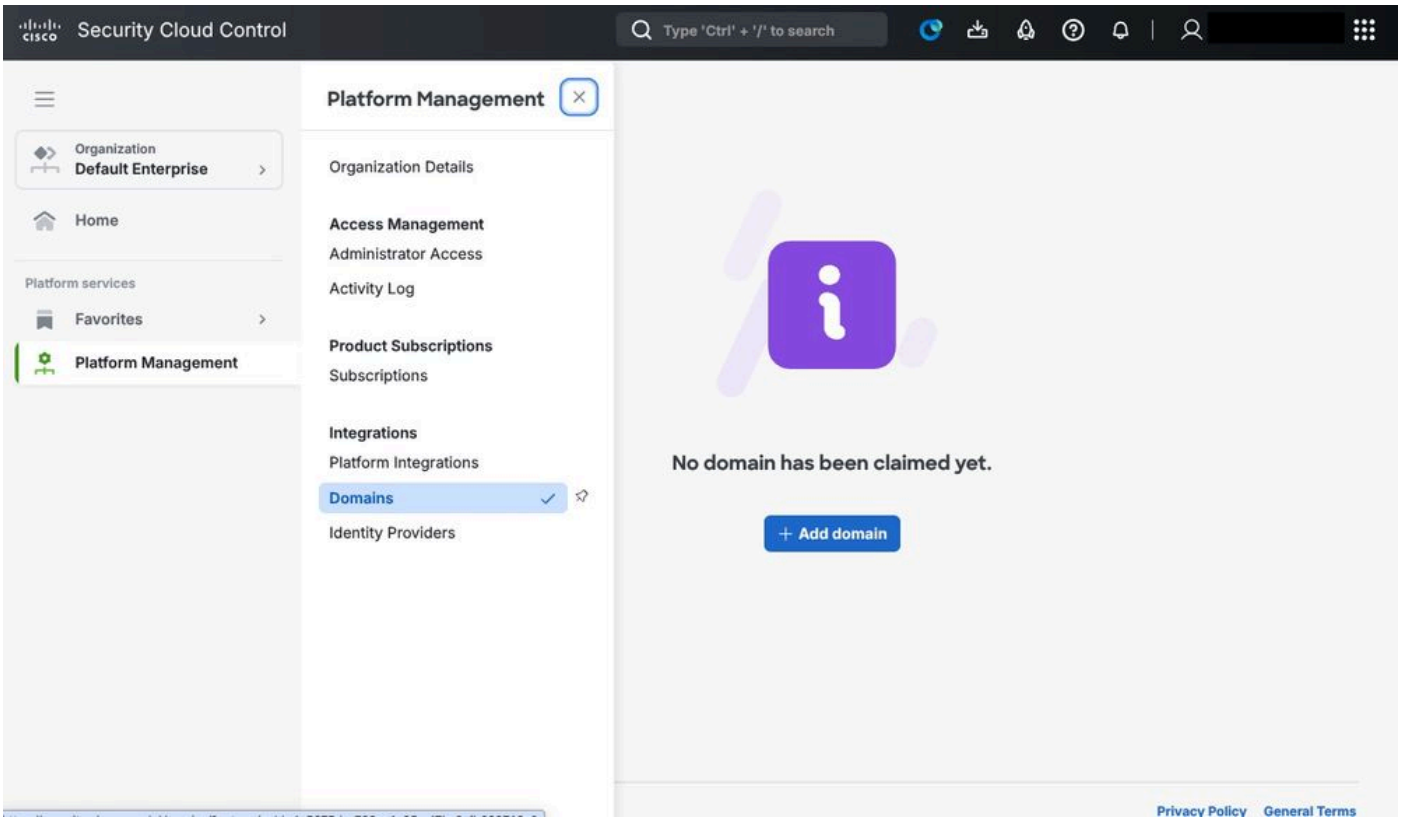
Dans le menu principal, accédez à Gestion de la plate-forme > Domaines.



Configuration du domaine de contrôle du cloud sécurisé

Étape 3. Ajout d'un nouveau domaine

Cliquez sur Add Domain afin de commencer le processus d'enregistrement de votre domaine d'authentification.

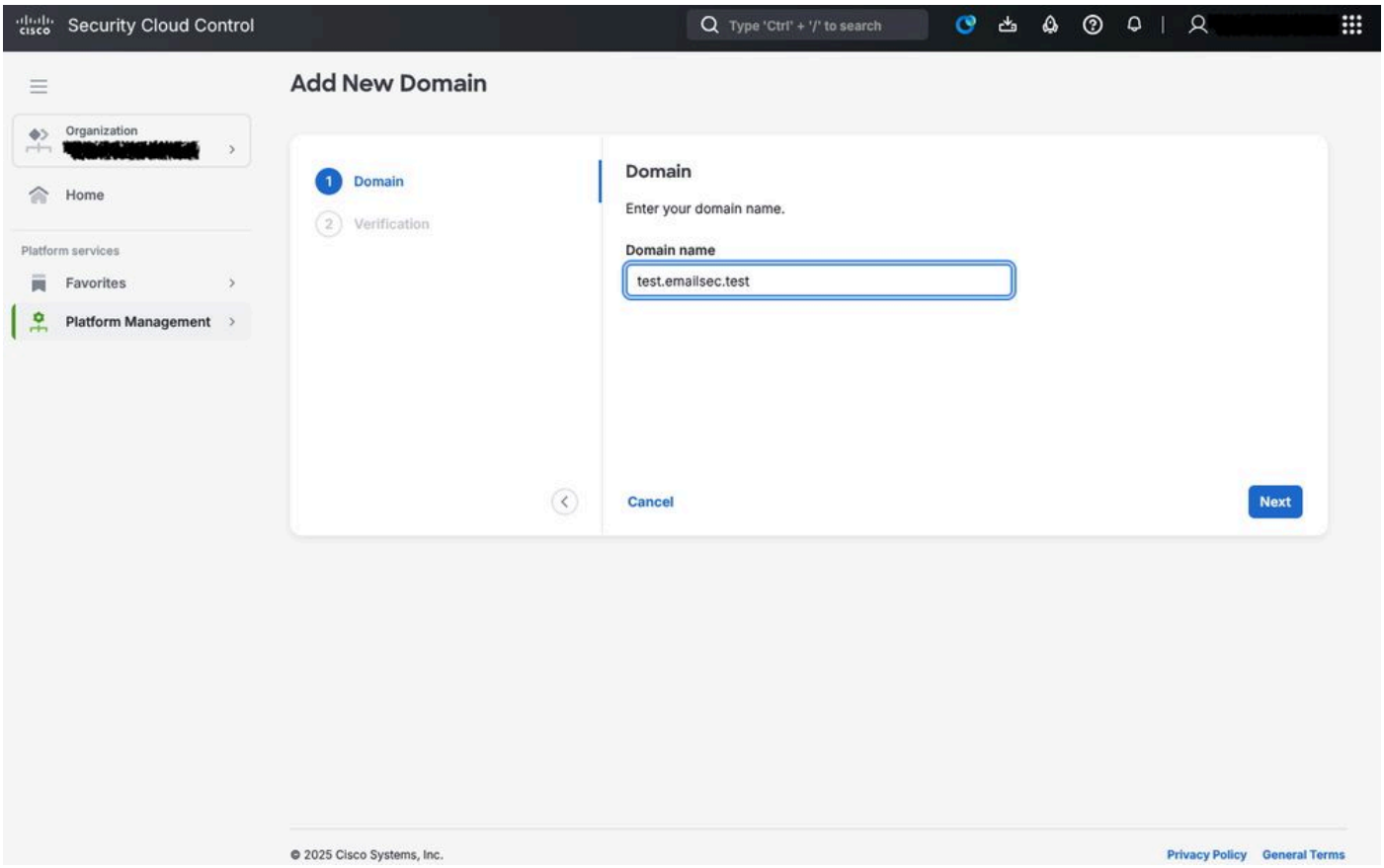


Contrôle du cloud de sécurité : Domaine

Étape 4. Fournissez les informations de domaine.

Remplissez le formulaire avec les détails du domaine utilisé pour l'authentification. Cela inclut généralement :

- Le nom de domaine (par exemple, test.emailsec.test)
- Coordonnées (administratives et techniques)
- Paramètres d'authentification, selon le fournisseur d'identité choisi



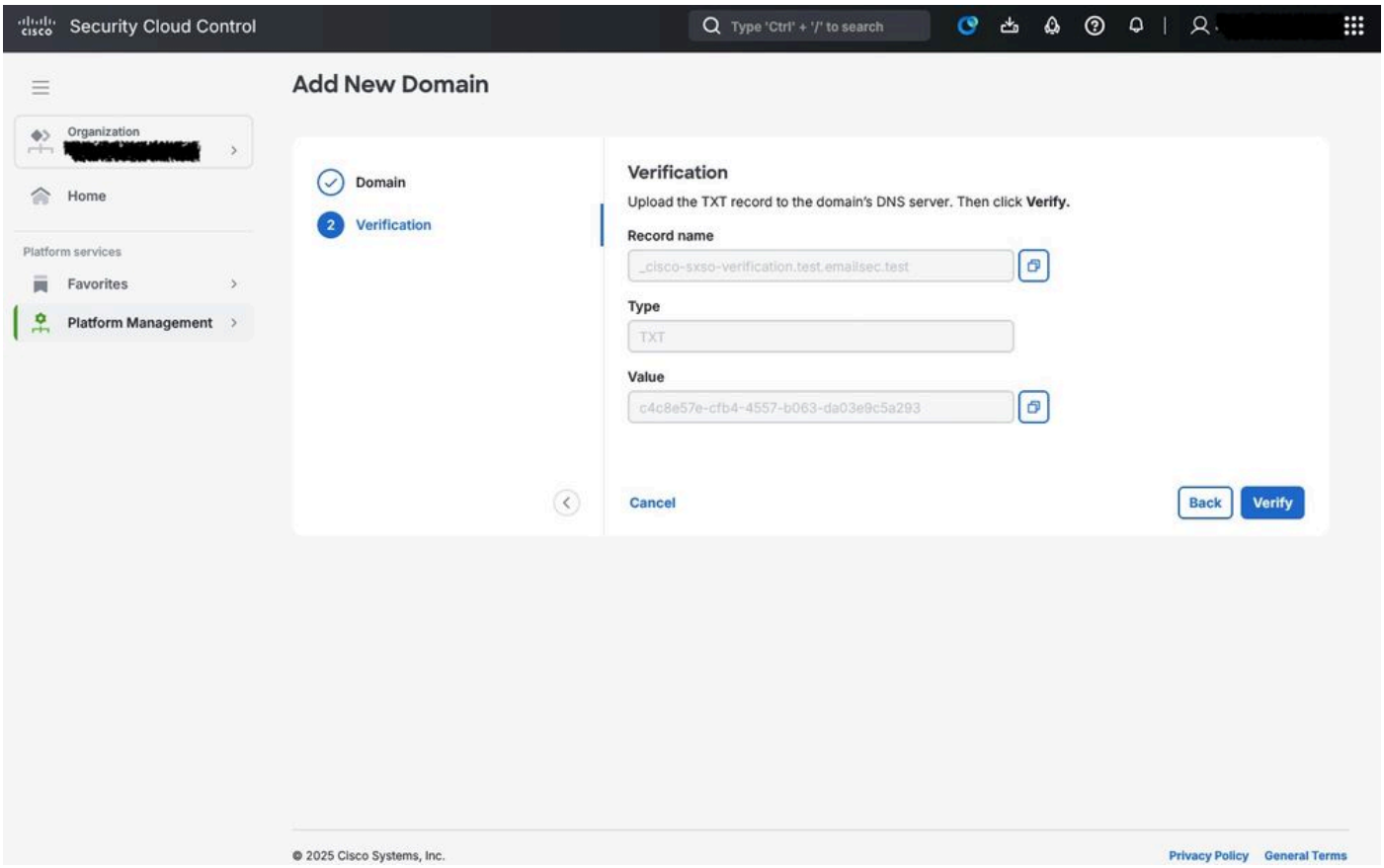
Étape 5. Vérification du domaine via DNS

Une fois le domaine enregistré, Cisco exige une preuve de propriété.

- Un enregistrement de vérification est fourni par CSCC
- Cet enregistrement doit être ajouté à votre configuration DNS de votre domaine (généralement sous la forme d'un enregistrement TXT)
- Cisco Secure Cloud valide automatiquement l'entrée DNS pour confirmer que le domaine appartient à votre organisation

---

⚠ Mise en garde : Le processus de vérification doit être terminé avant que vous puissiez poursuivre l'intégration. Selon la propagation DNS, la validation prend de quelques minutes à quelques heures.



Connexion d'ETD à Cisco Duo à l'aide de Cisco SCC

Une fois que le domaine de l'administrateur a été correctement configuré (ce qui sert de base à l'application de contrôles d'accès plus stricts et à la gestion des privilèges), l'étape suivante consiste à intégrer le service MFA sous contrat.

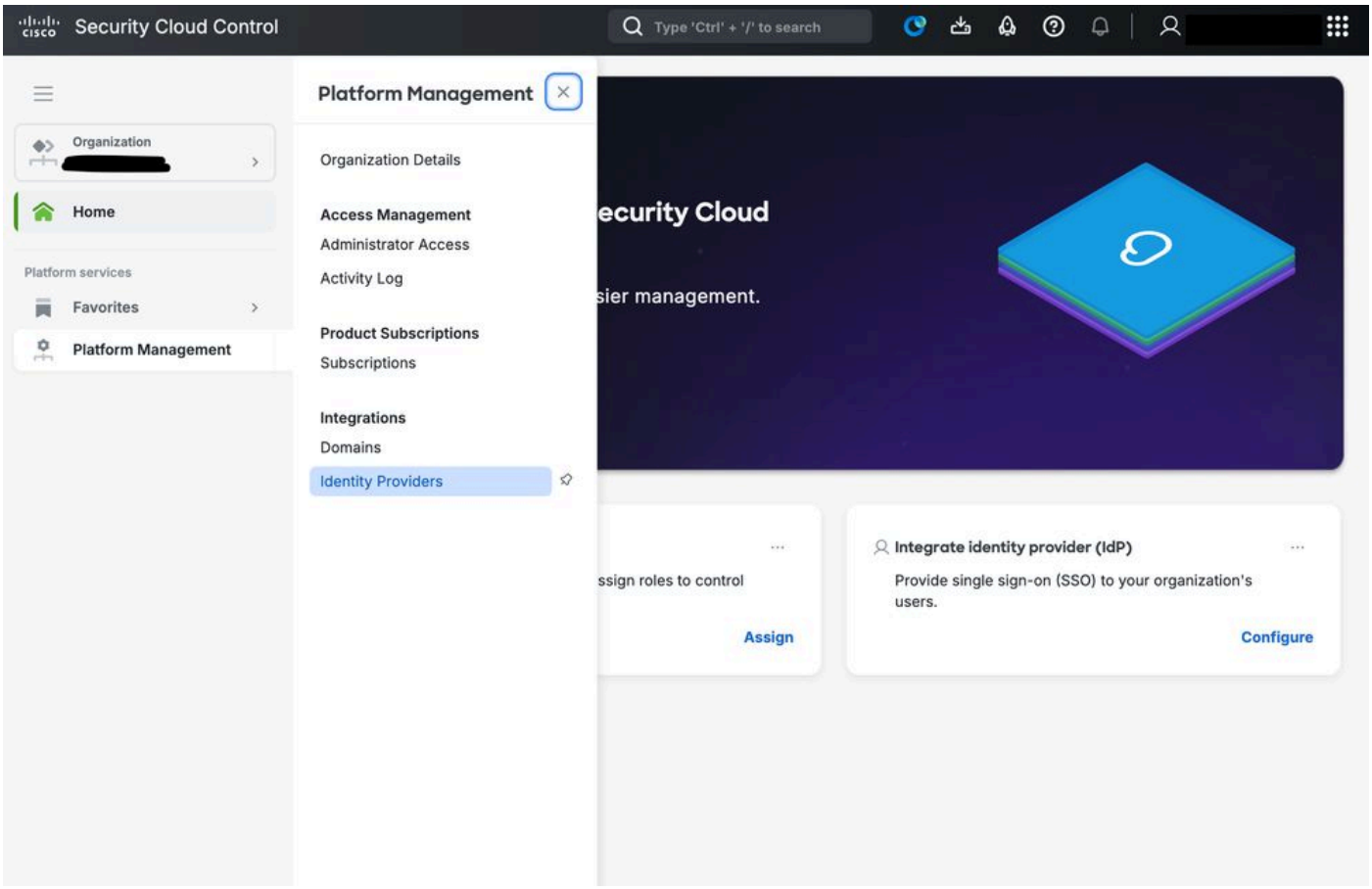
Dans ce scénario, Cisco Duo est mis en oeuvre en tant que solution principale pour le contrôle d'accès, la connexion sécurisée et la vérification de l'AMF. Cette intégration renforce la sécurité de l'environnement en demandant aux administrateurs d'authentifier leur identité par plusieurs étapes de vérification, réduisant ainsi le risque d'accès non autorisé et assurant la conformité avec les politiques de sécurité de l'entreprise.

Intégration de Cisco Duo et de Cisco Cloud Control

Étape 1. Accès à la console SCC de Cisco

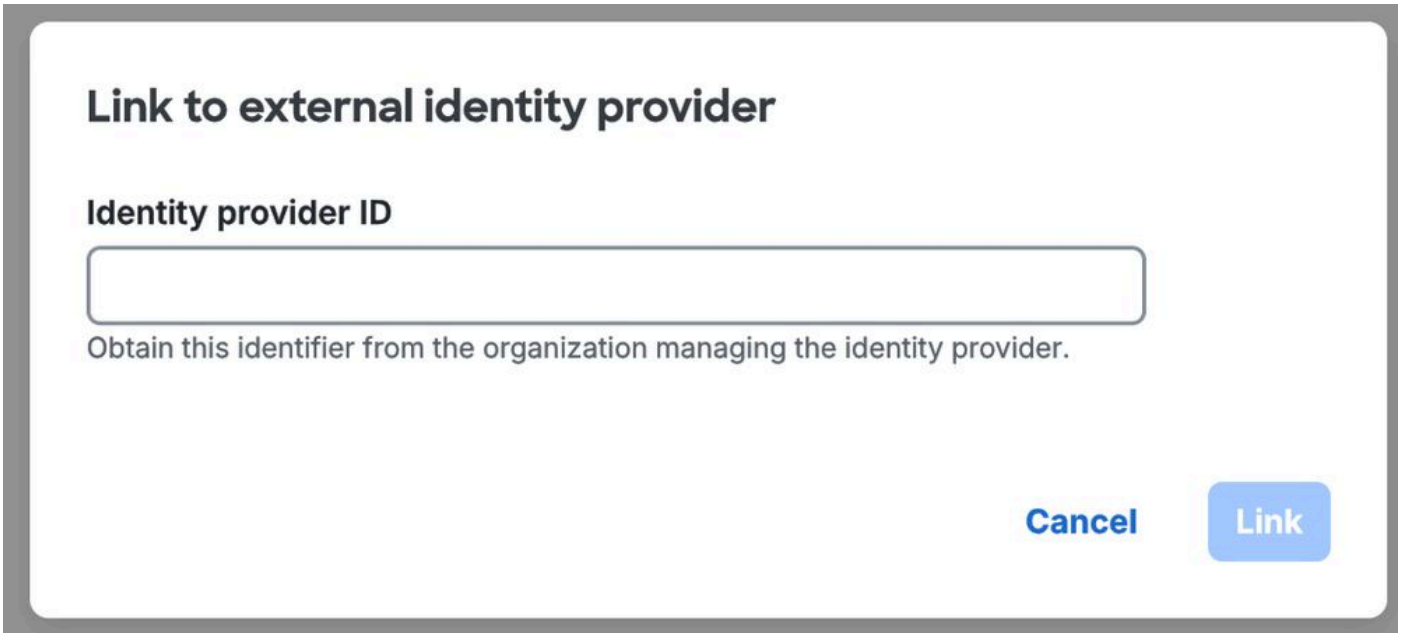
Connectez-vous au portail Cisco Security Cloud Control https://security.cisco.com/.

Accédez à Platform Management et cliquez sur Identity Providers.



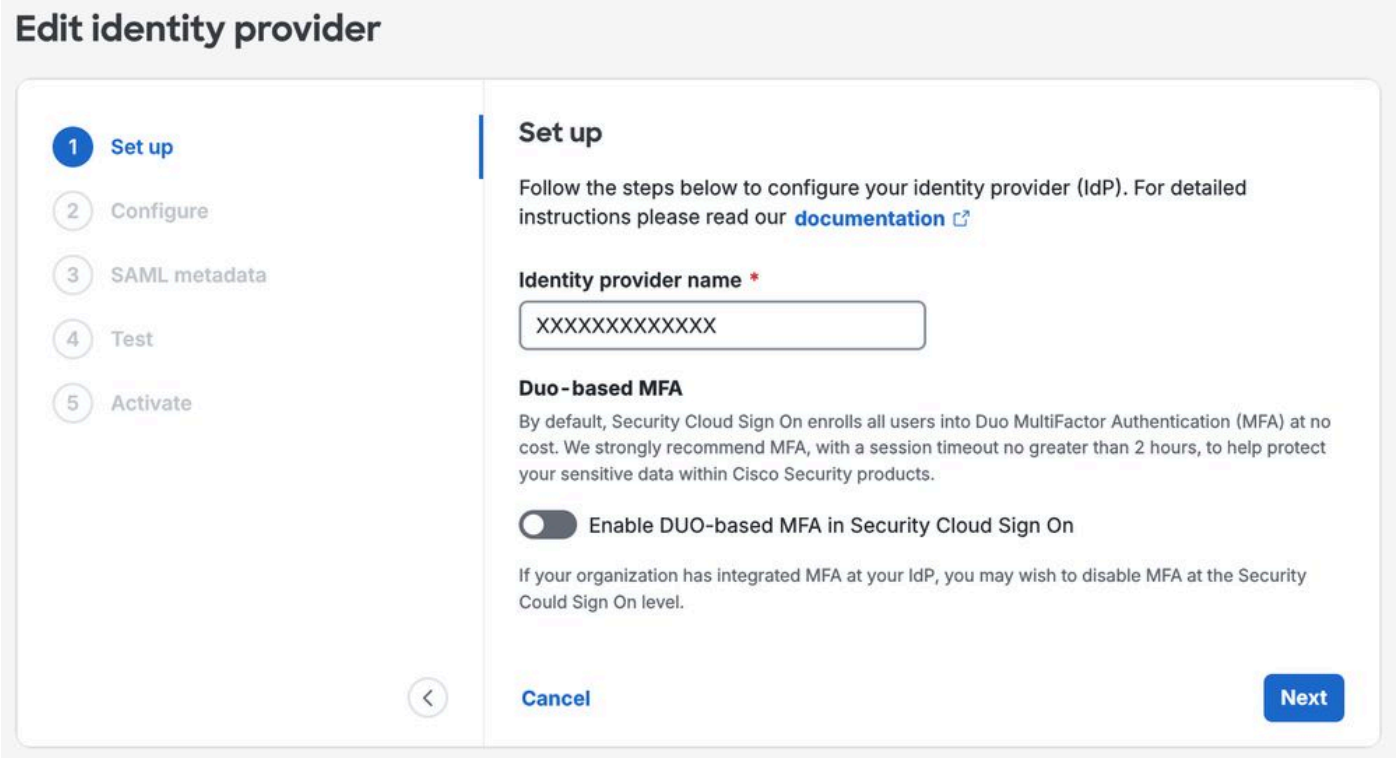
Configuration SCC IDP

Utilisez un nom personnalisé afin d'identifier le fournisseur d'identité.



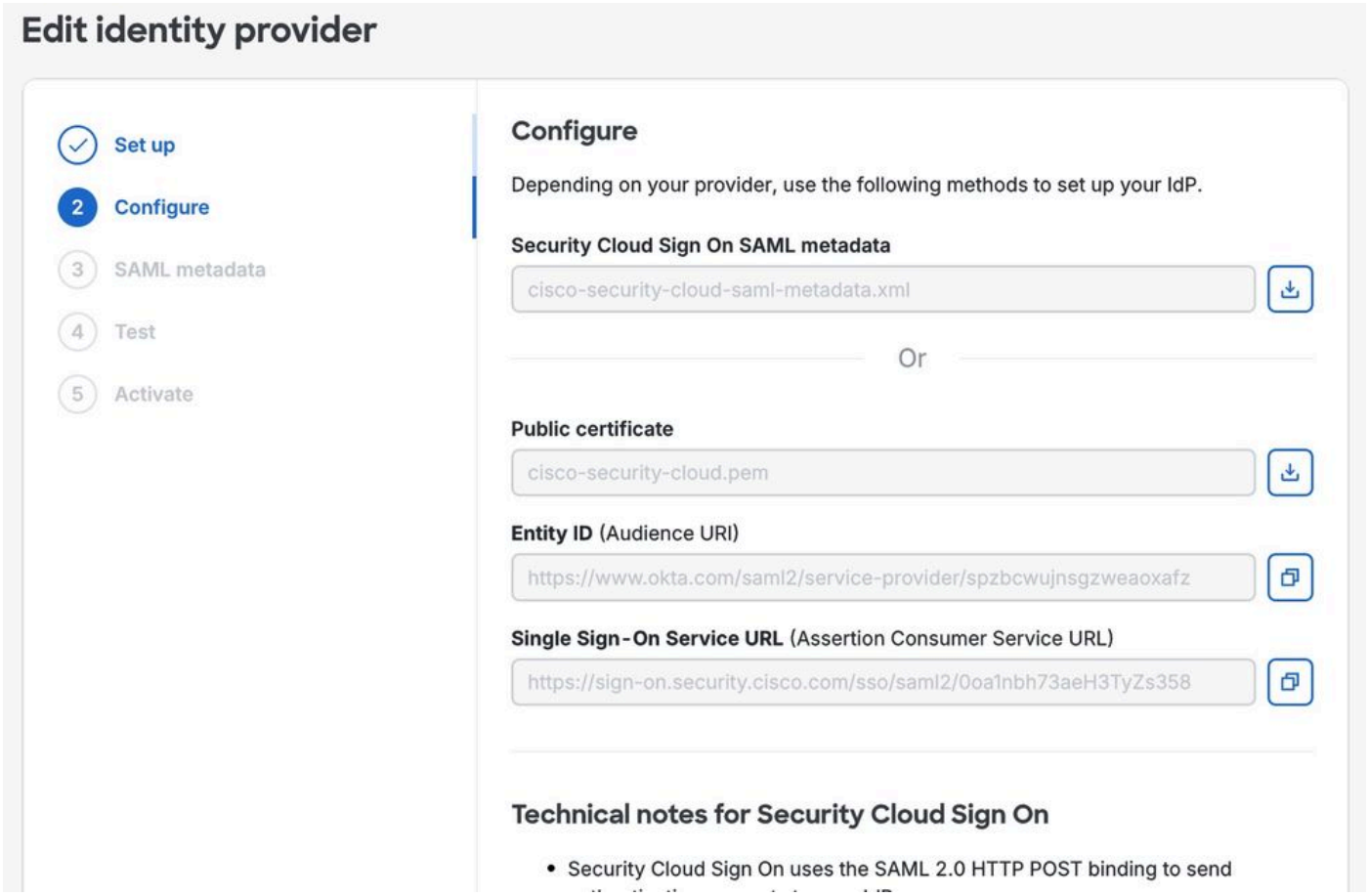
La configuration démarre. À ce stade, vous avez accès à Cisco SCC et à Cisco Duo.

Étape 2. Dans SCC, désactivez Enable DUO-based MFA in Security Cloud Sing On, comme illustré dans l'image, et cliquez sur Next.

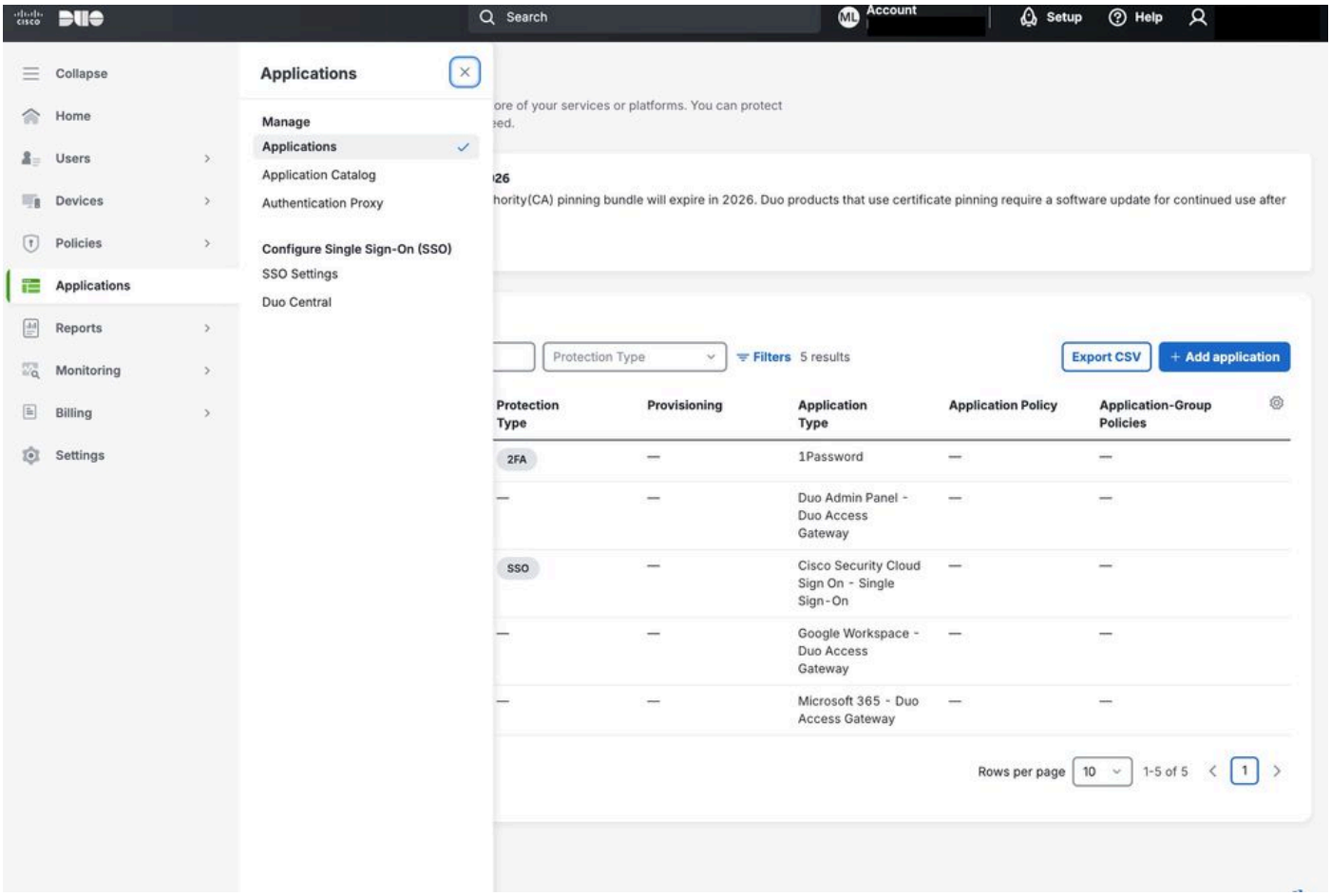


Configuration du fournisseur d'identité

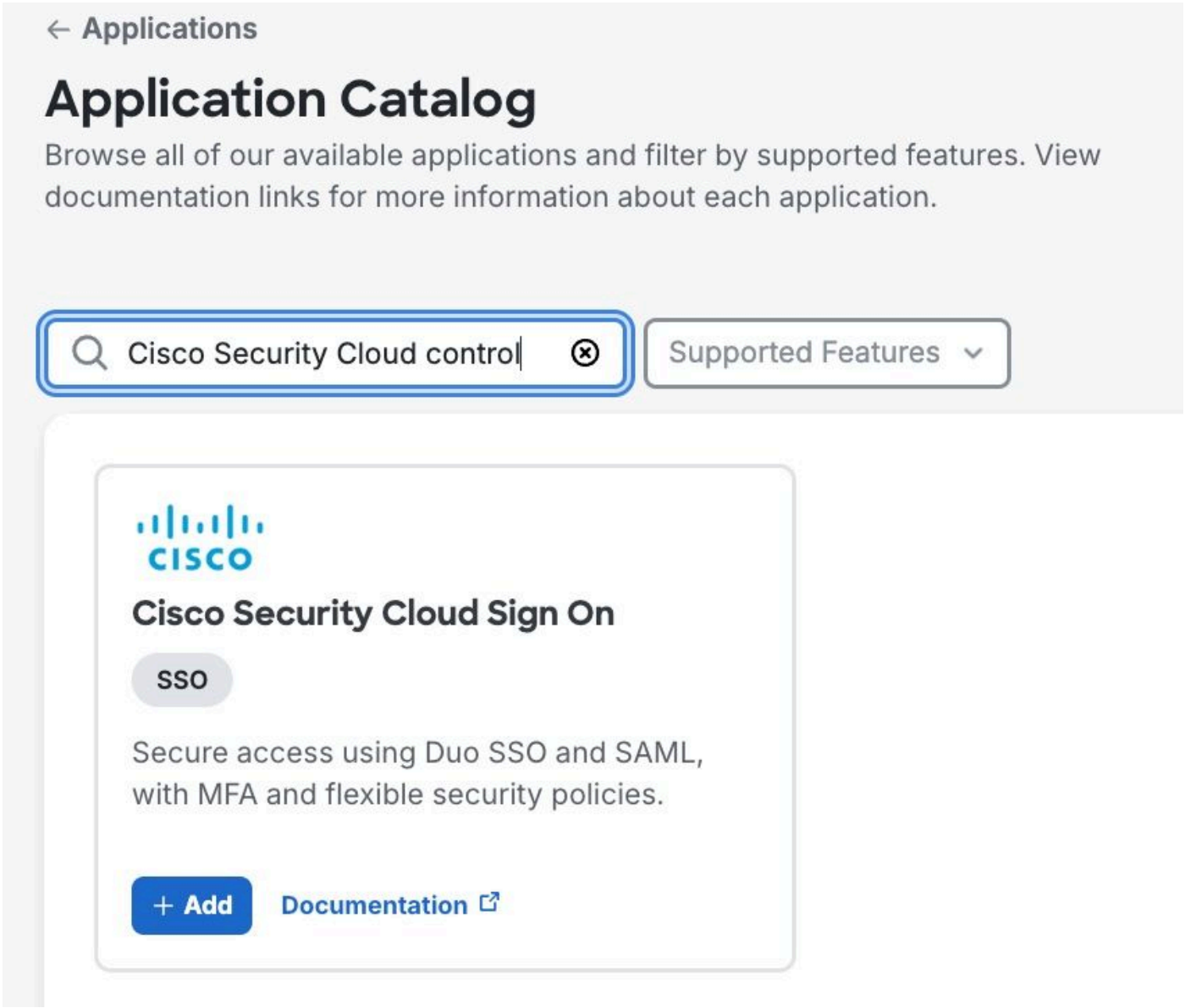
Étape 3. Les données pertinentes sont créées et utilisées lors de la configuration de Cisco Duo. Veillez à copier toutes les valeurs requises et les données associées, et à les stocker dans un emplacement sécurisé.
Ces détails sont essentiels pour les étapes d'intégration futures. Veillez donc à ce qu'ils soient accessibles uniquement au personnel autorisé et protégés conformément aux politiques de sécurité de votre organisation.



Étape 4. Ouvrez Cisco Duo, accédez à la section Applications et cliquez sur Add application.

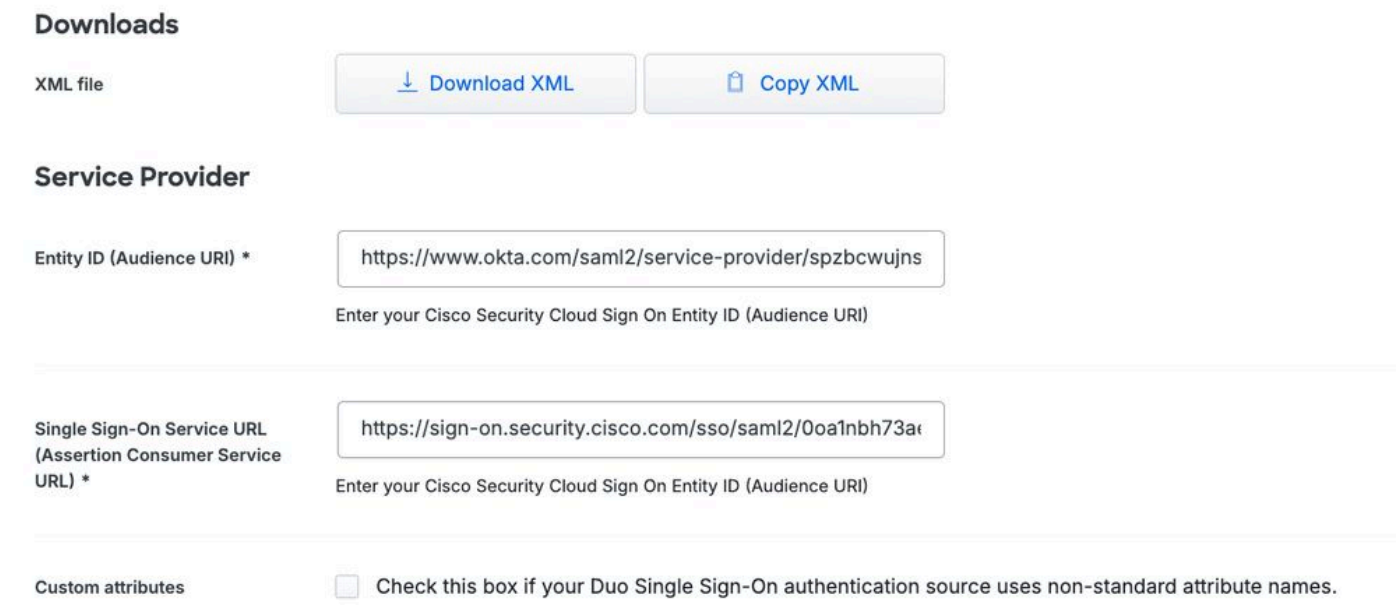


Dans le menu, recherchez Cisco Security Cloud et cliquez sur Add afin de démarrer l'intégration.

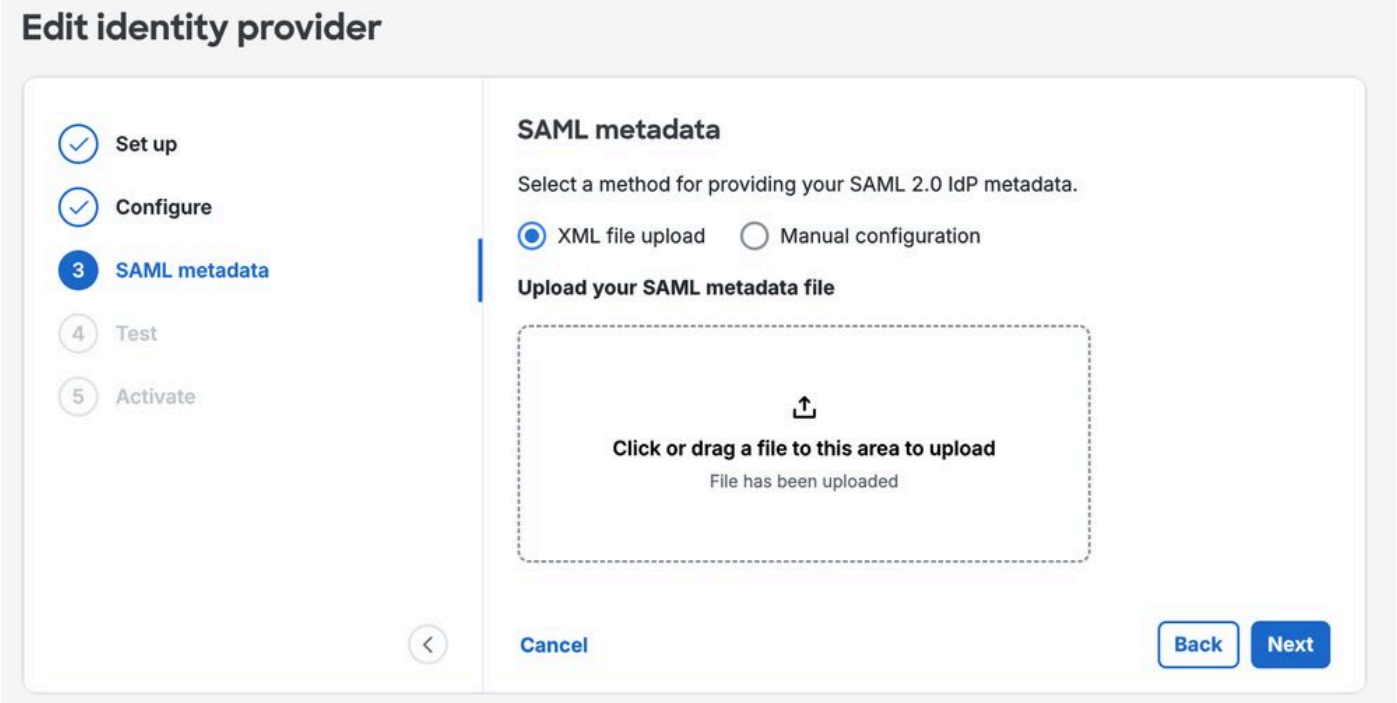


Étape 5 : configuration des informations pertinentes dans l’application Cisco Duo

Copiez l'ID d'entité et l'URL du service d'authentification unique de Cisco SCC dans Cisco Duo.



Étape 6. Téléchargez le fichier XML et téléchargez-le dans Cisco SCC.



Remarque : Les autres paramètres qui peuvent être configurés dans l'application à partir de la console Cisco Duo doivent être ajustés en fonction de vos besoins spécifiques. Vous trouverez des explications détaillées sur chacun de ces paramètres dans la documentation officielle de Cisco Duo. Les exemples de paramètres configurables incluent le nom de l'application attribuée, l'ensemble des utilisateurs auxquels la stratégie s'applique et d'autres options de personnalisation qui peuvent personnaliser les contrôles de sécurité afin de répondre aux besoins de votre organisation.

Configuration des politiques dans Cisco Duo pour Cisco ETD

À ce stade, tous les composants sont connectés et l'étape suivante consiste à configurer une stratégie qui s'applique au processus d'authentification de l'administrateur au sein de la console Cisco ETD.

Dans cet exemple, l'accent est mis sur le contrôle d'accès basé sur l'adresse IP. Cependant, Cisco Duo offre de nombreuses autres options de contrôle d'accès.

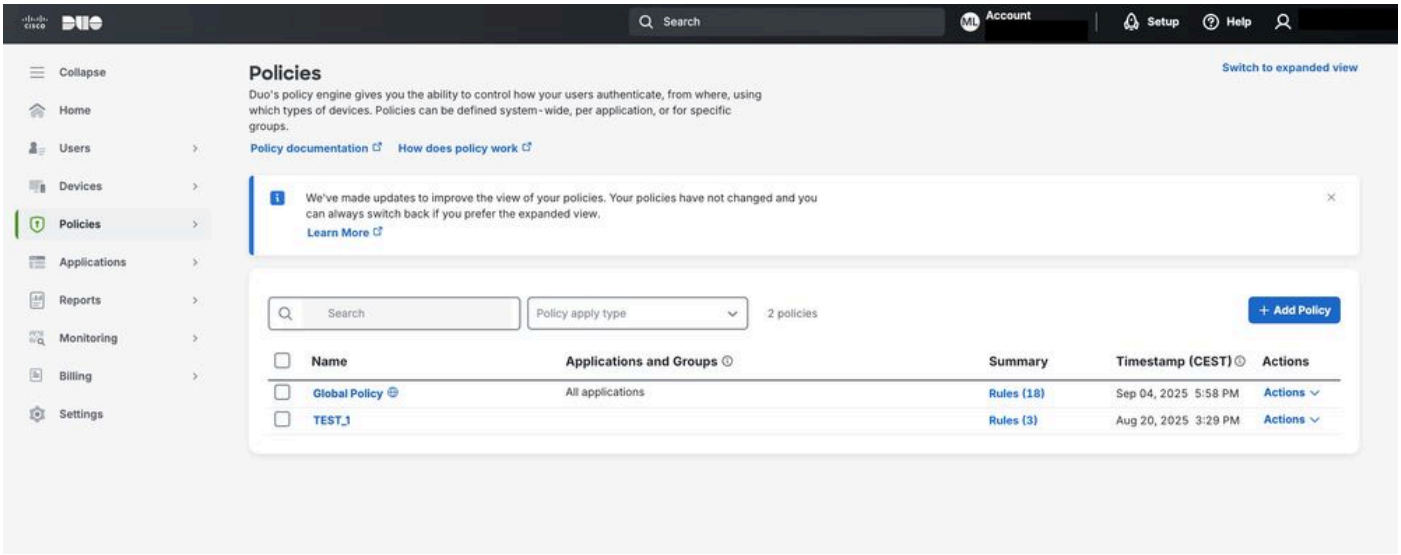
Une nouvelle stratégie peut être créée et attribuée à l'application, ce qui permet l'application des règles d'authentification et des restrictions de sécurité souhaitées pour les connexions administrateur.

Pour plus d'informations sur tous les contrôles et options de configuration disponibles dans Cisco Duo, reportez-vous à la documentation officielle de Cisco Duo.

Cette ressource fournit des conseils complets sur la configuration, la personnalisation et les meilleures pratiques afin d'optimiser les politiques de sécurité.

En naviguant jusqu'à la section Policies dans Cisco Duo, une politique peut être créée et attribuée à la connexion Cisco ETD par l'intermédiaire de Cisco Duo.

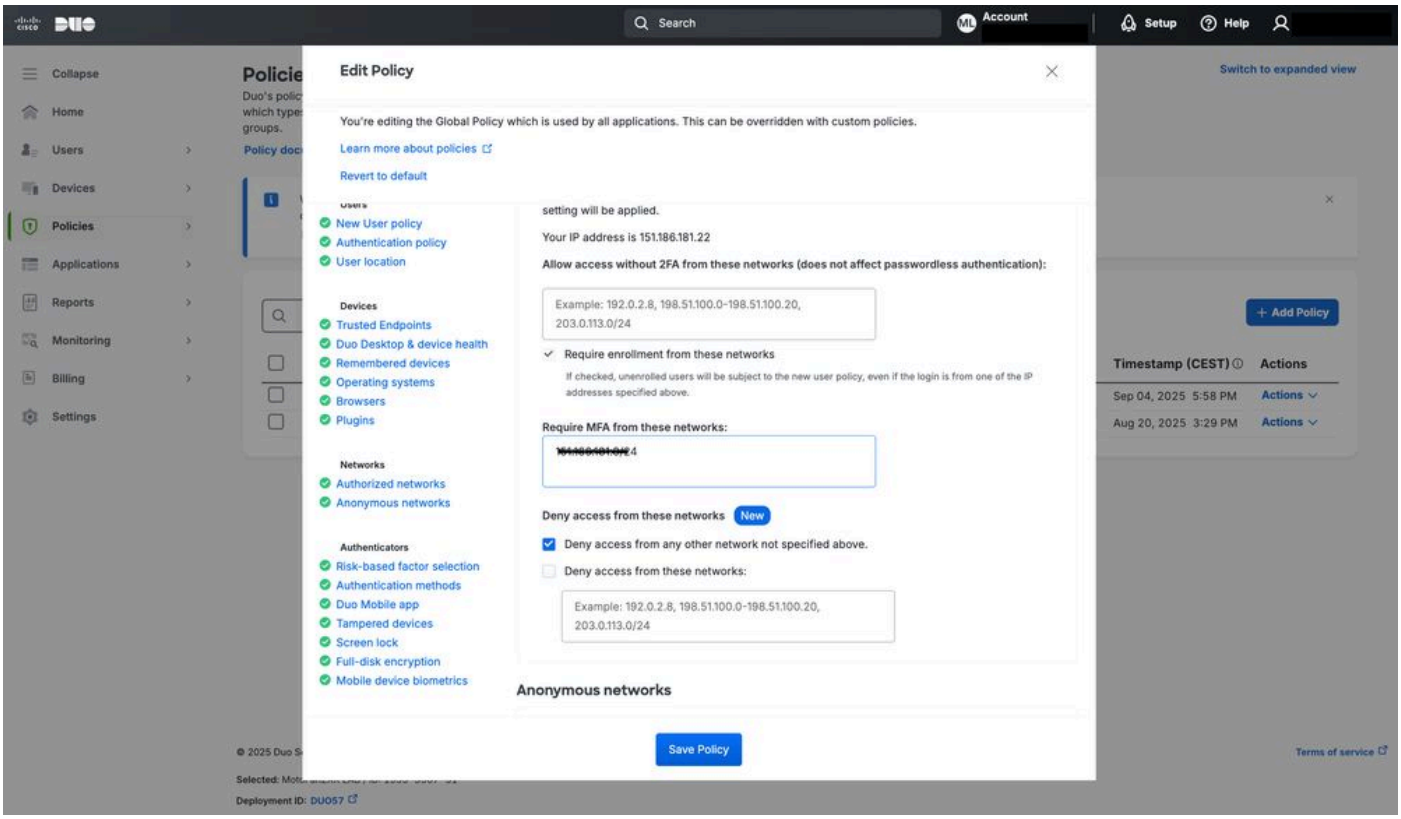
Cette stratégie peut être appliquée par utilisateur ou par groupe, en fonction des besoins d'accès.



Cisco Duo

Dans cet exemple, comme l'illustre l'image, le contrôle d'accès IP source est activé en configurant la section Authorized Networks.

Cette configuration autorise l'accès uniquement à partir des plages IP sécurisées spécifiées, ce qui renforce la sécurité de Cisco ETD.



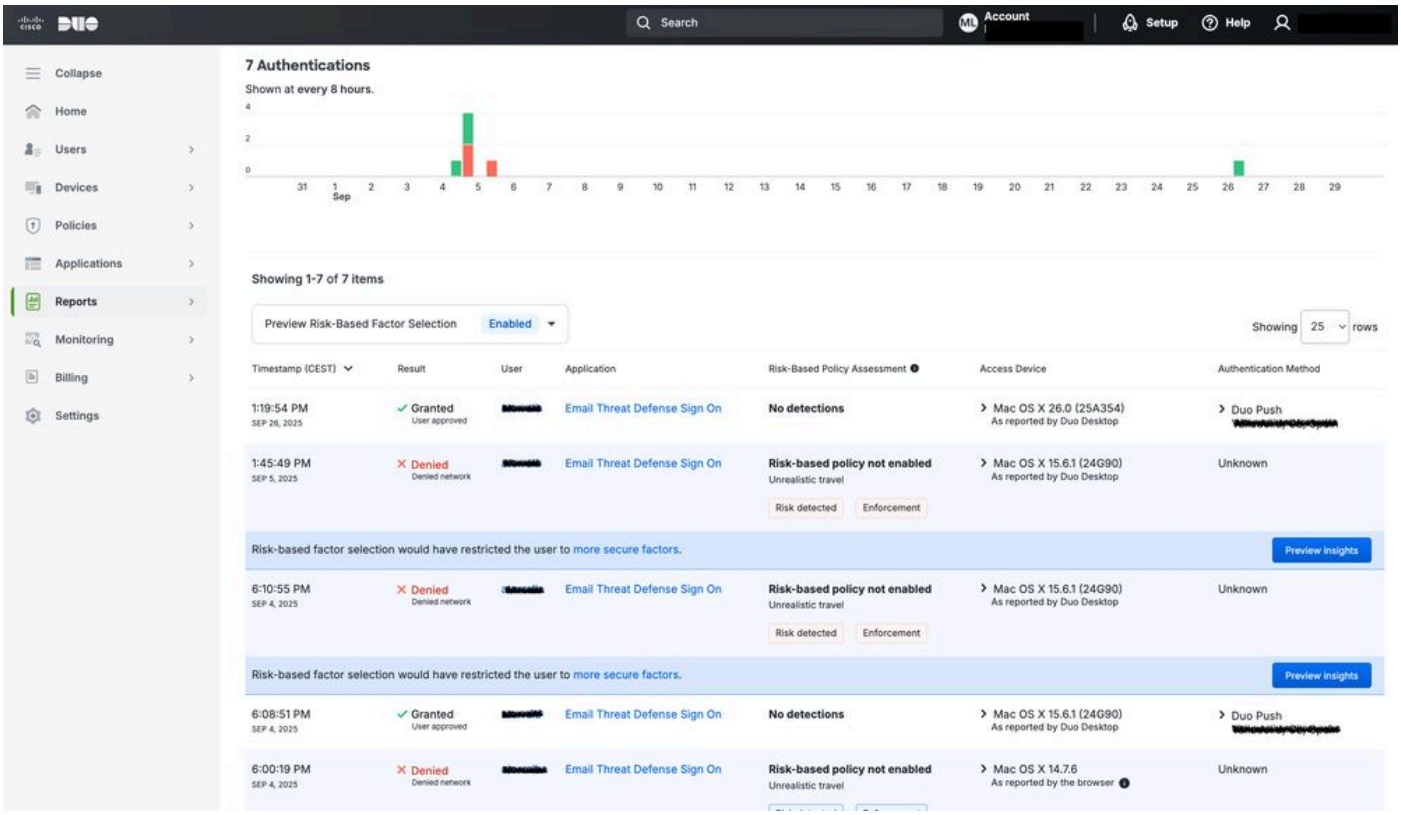
Configuration de la stratégie Cisco Duo

Conclusions

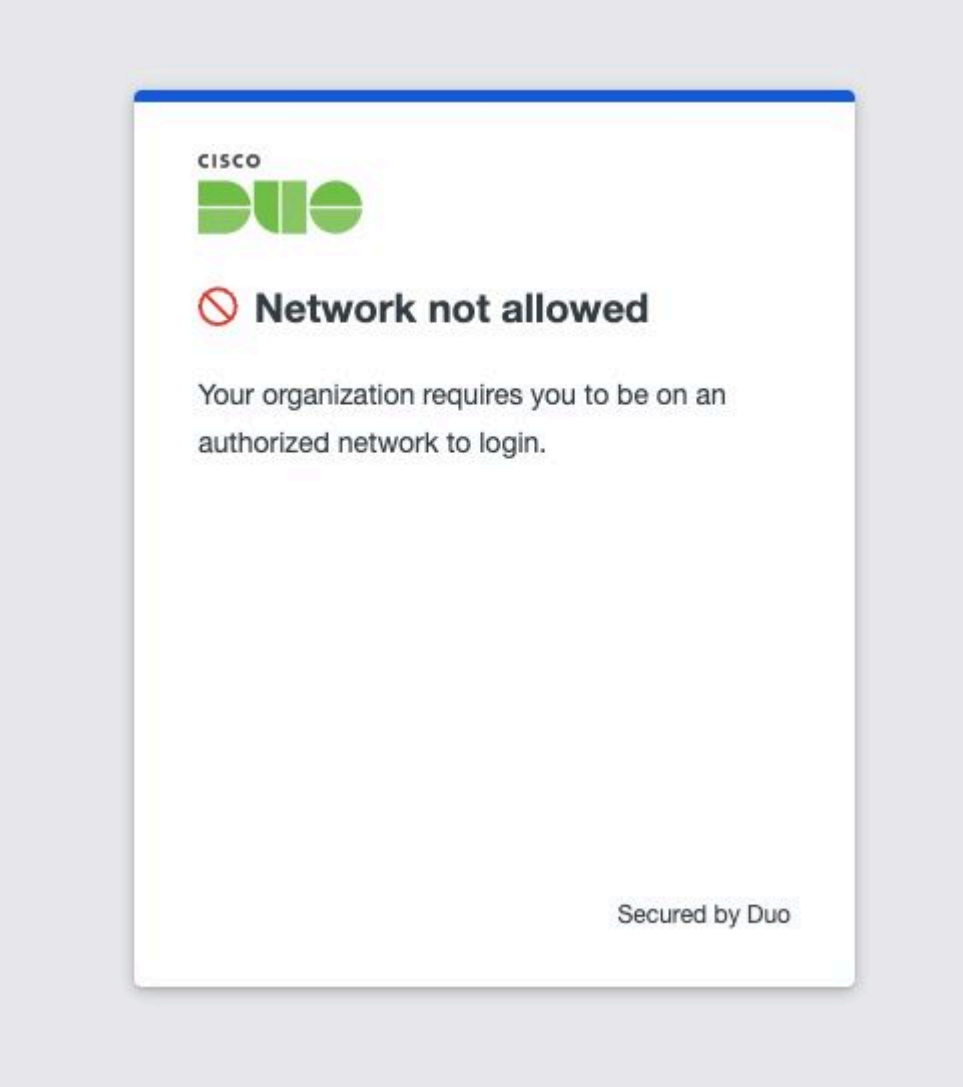
Cisco ETD offre des options flexibles afin de protéger l'accès administrateur via l'AMF et l'intégration avec les fournisseurs d'identité.
En combinant Cisco SCC et Cisco Duo, les entreprises peuvent mettre en oeuvre des politiques d'authentification plus strictes, réduire le risque d'accès non autorisé et s'aligner sur les meilleures pratiques du secteur en matière de gestion sécurisée des services cloud.

En plus de l'AMF, les administrateurs peuvent tirer parti des contrôles basés sur des politiques de Cisco Duo afin de restreindre l'accès en fonction de critères spécifiques, tels que l'adresse IP source. Par exemple, comme illustré dans l'image suivante, une tentative d'accès à partir d'une adresse IP en dehors de la plage autorisée est automatiquement bloquée par le système. Ainsi, seules les requêtes provenant de réseaux de confiance sont autorisées, ce qui ajoute une couche de protection supplémentaire contre les attaques potentielles.

En mettant en oeuvre un contrôle d'accès basé sur IP et une AMF, les entreprises adoptent une approche de défense en profondeur, combinant la vérification de l'identité à la validation de l'emplacement du réseau afin de protéger les interfaces de gestion critiques dans le cloud.



Rapports Cisco Duo



Résultat du contrôle du réseau

Avertissement : Il est important de comprendre que ce changement affecte toutes les applications qui utilisent le même domaine d'authentification ; non seulement ETD, mais également d'autres produits qui reposent sur le même processus d'authentification, comme l'accès à la console Cisco Secure Access.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.