Sicherer Schutz vor E-Mail-Bedrohungen: Mehrstufige Authentifizierung und Zugriffskontrollen

Inhalt

Einleitung

In diesem Dokument werden die Funktionen beschrieben, die Cisco Email Threat Defense (ETD) zur Kontrolle des Administratorzugriffs auf die Managementkonsole bereitstellt.

Voraussetzungen

Anforderungen

Cisco empfiehlt zur Konfiguration der ETD-Authentifizierung mit Duo, dass Sie über die folgenden Themen informiert sind:

- Ein Cisco ETD-Abonnement
- Zugriff auf Cisco Security Cloud Control (SCC)
- Eine Authentifizierungslösung für erhöhte Sicherheit, in diesem Fall Cisco Duo.

Verwendete Komponenten

Dieses Dokument ist auf den Schutz vor E-Mail-Angriffen und die sichere Cloud-Kontrolle beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer

gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

In diesem Dokument wird erläutert, wie Cisco ETD das Cisco SCC nutzt und mit Cisco Duo integriert werden kann, um eine sichere Authentifizierung und eine präzise Zugriffskontrolle zu ermöglichen.

Bei modernen Cloud-basierten Lösungen ist die Zugriffskontrolle eine der wichtigsten Komponenten für die Gewährleistung der Datensicherheit, der Erfüllung gesetzlicher Auflagen und der betrieblichen Integrität. Nicht autorisierter Zugriff - insbesondere auf Administratorkonten - kann schwerwiegende Folgen haben, wie z. B. Systemgefährdungen, Datenlecks und Serviceunterbrechungen.

Cisco bietet robuste Sicherheitsfunktionen für sein gesamtes Cloud-Portfolio, darunter die Multifactor Authentication-Technologie (MFA), die einen integralen Bestandteil von Services wie Cisco ETD darstellt. MFA fügt einen wichtigen Verifizierungsschritt hinzu, der über herkömmliche Passwörter hinausgeht, sodass sich Benutzer über einen zusätzlichen Faktor authentifizieren müssen, z. B. eine Genehmigung mobiler Anwendungen, ein Sicherheitstoken oder eine biometrische Verifizierung.

Um den Authentifizierungsprozess für Administratoren zu optimieren und zu optimieren, nutzt ETD Cisco SCC, einen zentralisierten Authentifizierungs- und Richtlinienmanagement-Service.

Über SCC erhält ETD Zugang zu einer breiten Palette von Sicherheitsfunktionen, darunter:

- Durchsetzung von Makrofinanzhilfen zur Minderung des Risikos des Diebstahls von Anmeldeinformationen.
- Integration mit Identitätsanbietern von Drittanbietern wie Cisco Duo, Microsoft Entra ID, Okta und anderen zur Unterstützung flexibler Authentifizierungs-Workflows und des Unternehmens-Identitätsverbunds
- Zentralisierte Richtlinienverwaltung, die einheitliche Zugriffsregeln für alle Cisco Cloud-Services ermöglicht

Cisco Duo erweitert diese Funktionen durch ein erweitertes richtlinienbasiertes Zugriffsmanagement. Mithilfe von SCC als Integrationskanal kann ETD detaillierte Kontrollen von Duo wie Quell-IP-Beschränkungen, Gerätezustandsprüfungen und benutzergruppenbasierte Regeln direkt auf den Administratorzugriff anwenden.

Organisationen können beispielsweise eine Richtlinie definieren, die nur den Zugriff aus bestimmten vertrauenswürdigen Netzwerkbereichen zulässt. Jeder Verbindungsversuch außerhalb der autorisierten IP-Liste kann automatisch blockiert werden, wie in den beigefügten Diagrammen dargestellt. Diese Kombination aus MFA und kontextbezogenen Richtlinien ermöglicht einen tief greifenden Abwehransatz, der sicherstellt, dass Angreifer auch dann nicht auf das System zugreifen können, wenn die Anmeldeinformationen gefährdet sind, es sei denn, sie erfüllen zusätzliche Sicherheitskriterien.

Durch die Kombination von Cisco ETD, Cisco SCC und Cisco Duo können Unternehmen ein sicheres, skalierbares und benutzerfreundliches Zugriffskontrollmodell implementieren, das sich an branchenübliche Best Practices anpasst und gleichzeitig den Schutz für wichtige Cloud-Services verbessert.

Szenarien

Mehrere Authentifizierungs- und Zugriffskontrollszenarien können mit ETD implementiert werden, um den Administratorzugriff zu sichern:

1. Integrierte MFA: Verwenden Sie die integrierte MFA von Cisco, oder integrieren Sie Microsoft MFA.
2. Cisco SCC mit Cisco Duo - Kombinieren Sie die zentralisierte Authentifizierung von Cisco SCC mit den erweiterten MFA-Funktionen von Duo.
3. Cisco SCC mit externem Identitätsanbieter (z. B. Microsoft Entra ID) - Erweiterung der Authentifizierungsrichtlinien durch die Integration in Enterprise Identity-Lösungen

In diesem Dokument werden die Konfigurationsschritte für Szenario 2 beschrieben: Cisco SCC mit Cisco Duo, der Prozess kann jedoch für andere Technologien angepasst werden.

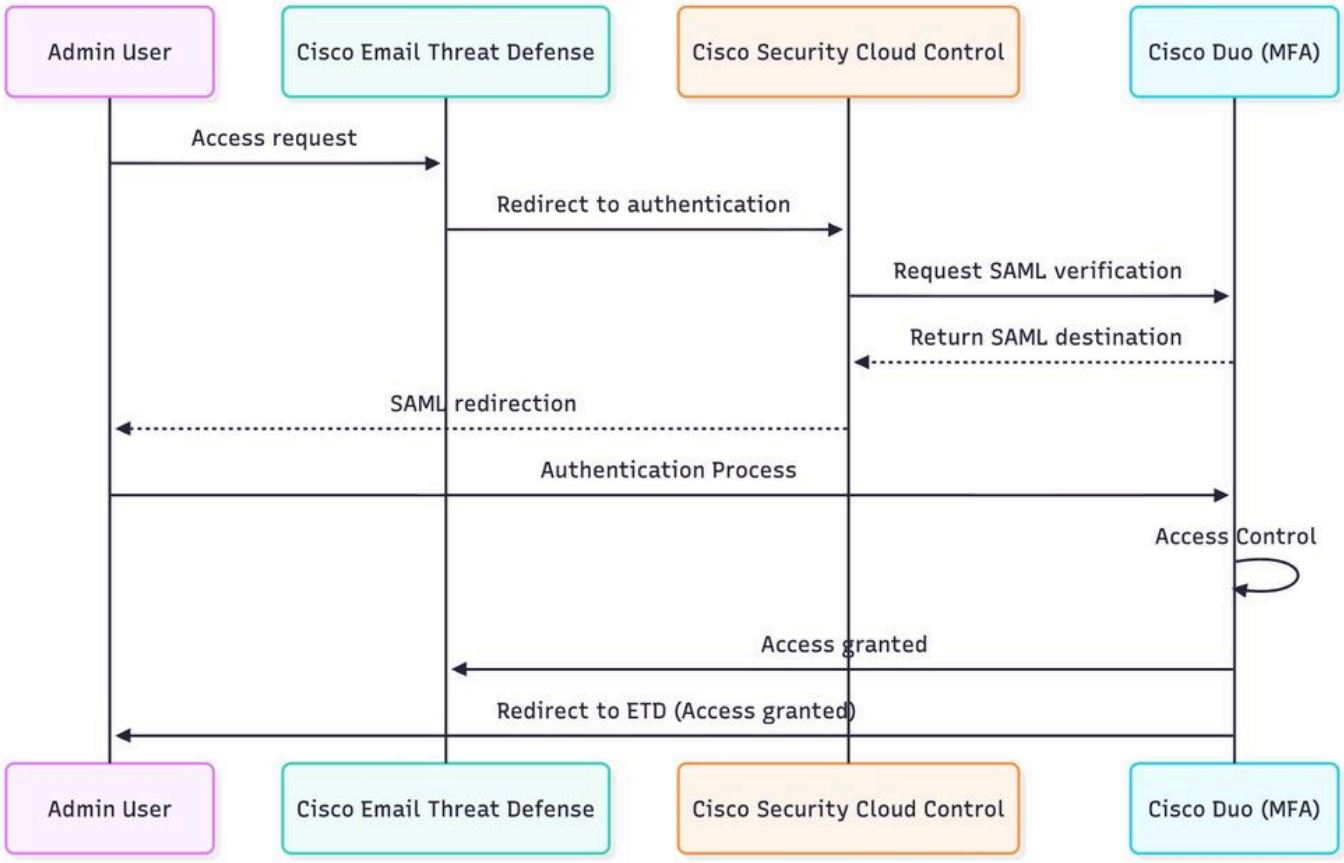
Anmerkung: Dieses Dokument bietet eine Übersicht über die grundlegenden Schritte, die erforderlich sind, um die Zugriffskontrolle in Email Threat Defense (ETD) mithilfe der Multifaktor-Authentifizierungsfunktionen von Cisco Duo zu aktivieren. Durch die Implementierung der Duo-Integration wird die Sicherheit erhöht, da nur autorisierte Benutzer auf die Plattform zugreifen können. Umfassende Anleitungen, Konfigurationsoptionen und erweiterte Bereitstellungsszenarien finden Sie in der offiziellen Produktdokumentation:

- für zentralisierte Sicherheitsrichtlinien und Zugriffsverwaltung.

Cisco Duo: Hier finden Sie detaillierte Anweisungen zur Multifaktor-Authentifizierungskonfiguration und Best Practices.

Cisco SCC-Konfiguration

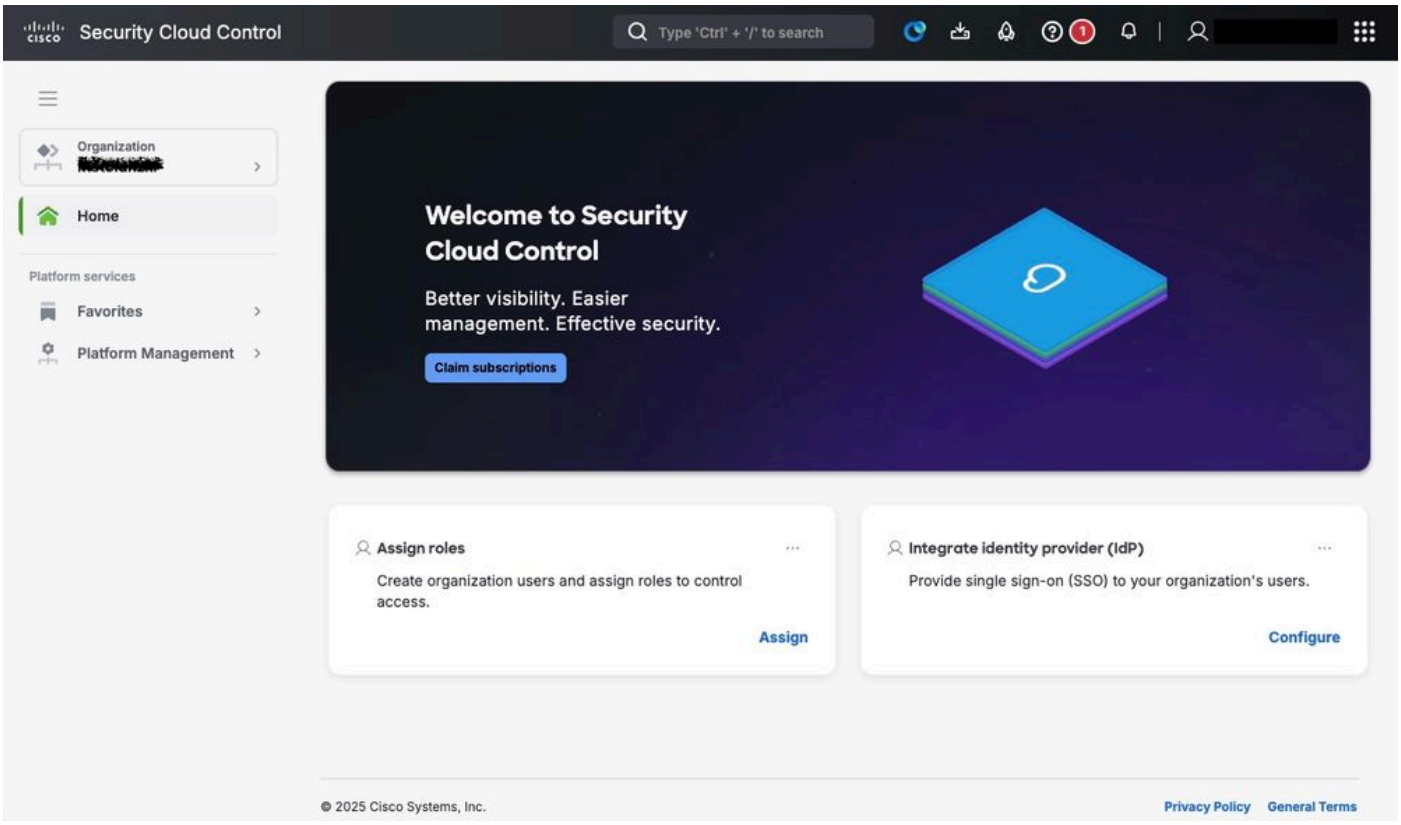
Für die Integration von Cisco ETD mit Cisco Duo ist der erste Schritt die Konfiguration der Authentifizierungsdomäne im Cisco SCC. Auf diese Weise wird die Vertrauensbeziehung hergestellt, die die Zusammenarbeit von Cisco SCC mit externen Identitäts- und MFA-Anbietern ermöglicht.



Diagramm

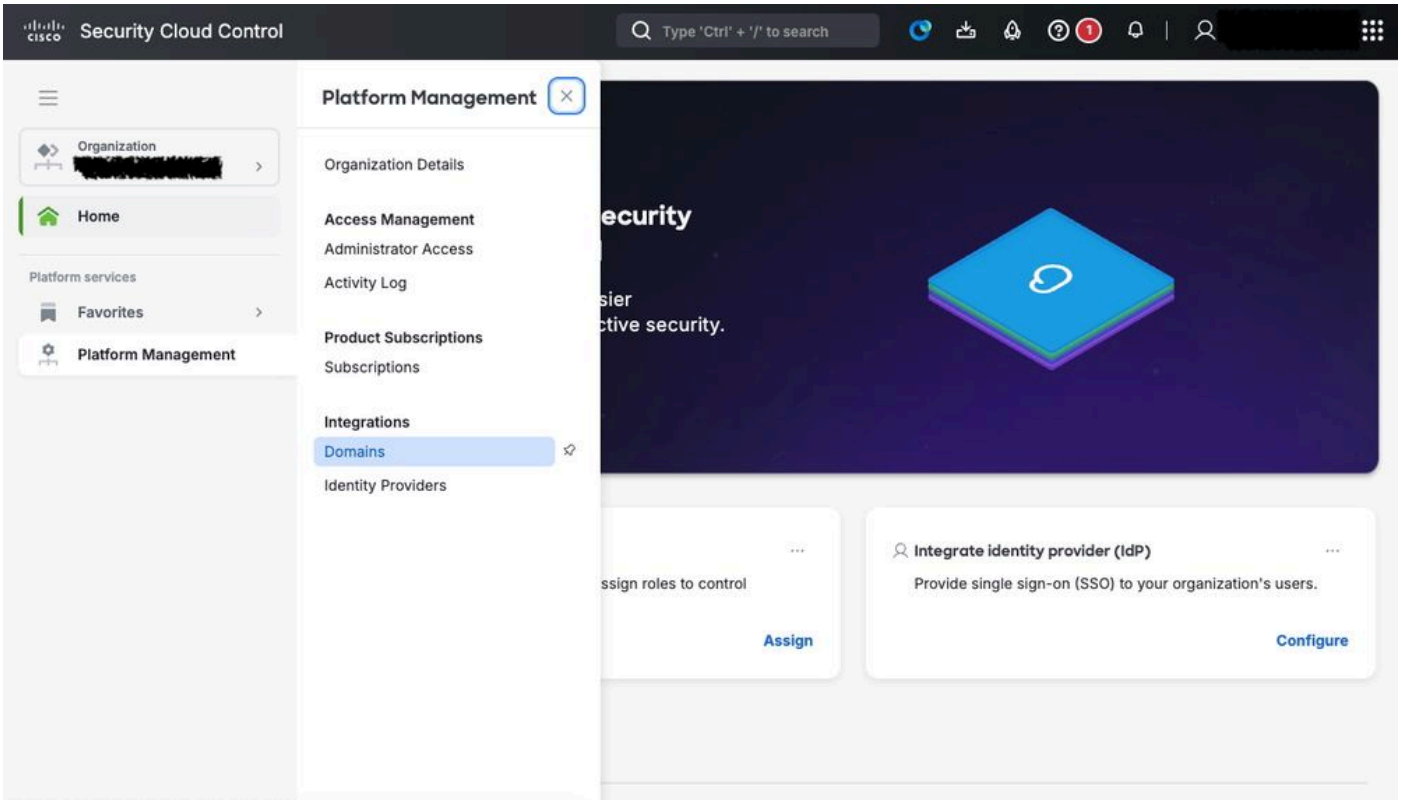
Schritt 1: Zugriff auf die Cisco SCC-Konsole

Melden Sie sich beim Cisco SCC-Portal an https://security.cisco.com/.



Schritt 2: Navigieren Sie zu Domänenmanagement.

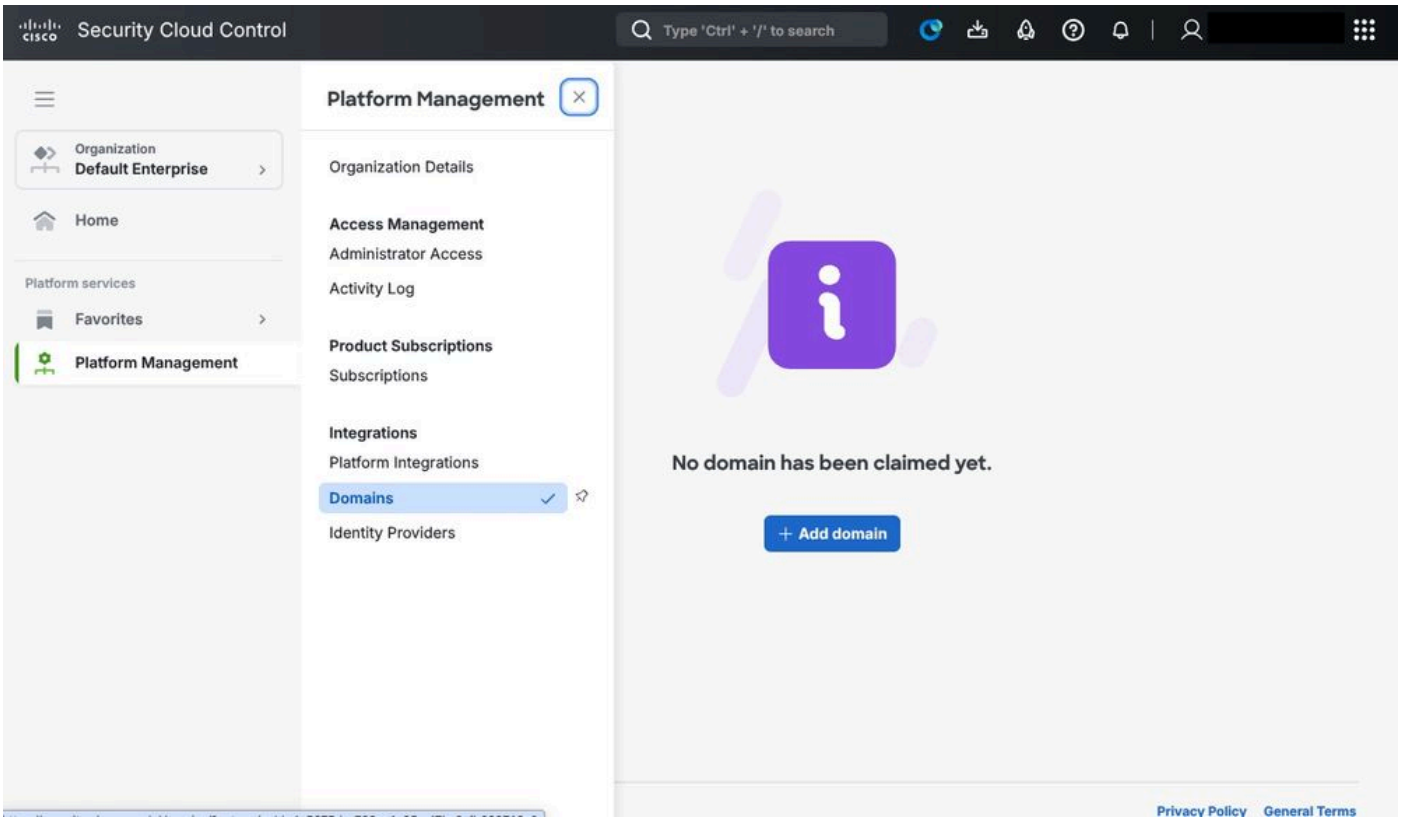
Navigieren Sie im Hauptmenü zu Platform Management > Domains (Plattformverwaltung > Domänen).



Konfiguration der sicheren Cloud-Kontrolldomäne

Schritt 3: Hinzufügen einer neuen Domäne

Klicken Sie auf Add Domain (Domäne hinzufügen), um mit der Registrierung der Authentifizierungsdomäne zu beginnen.

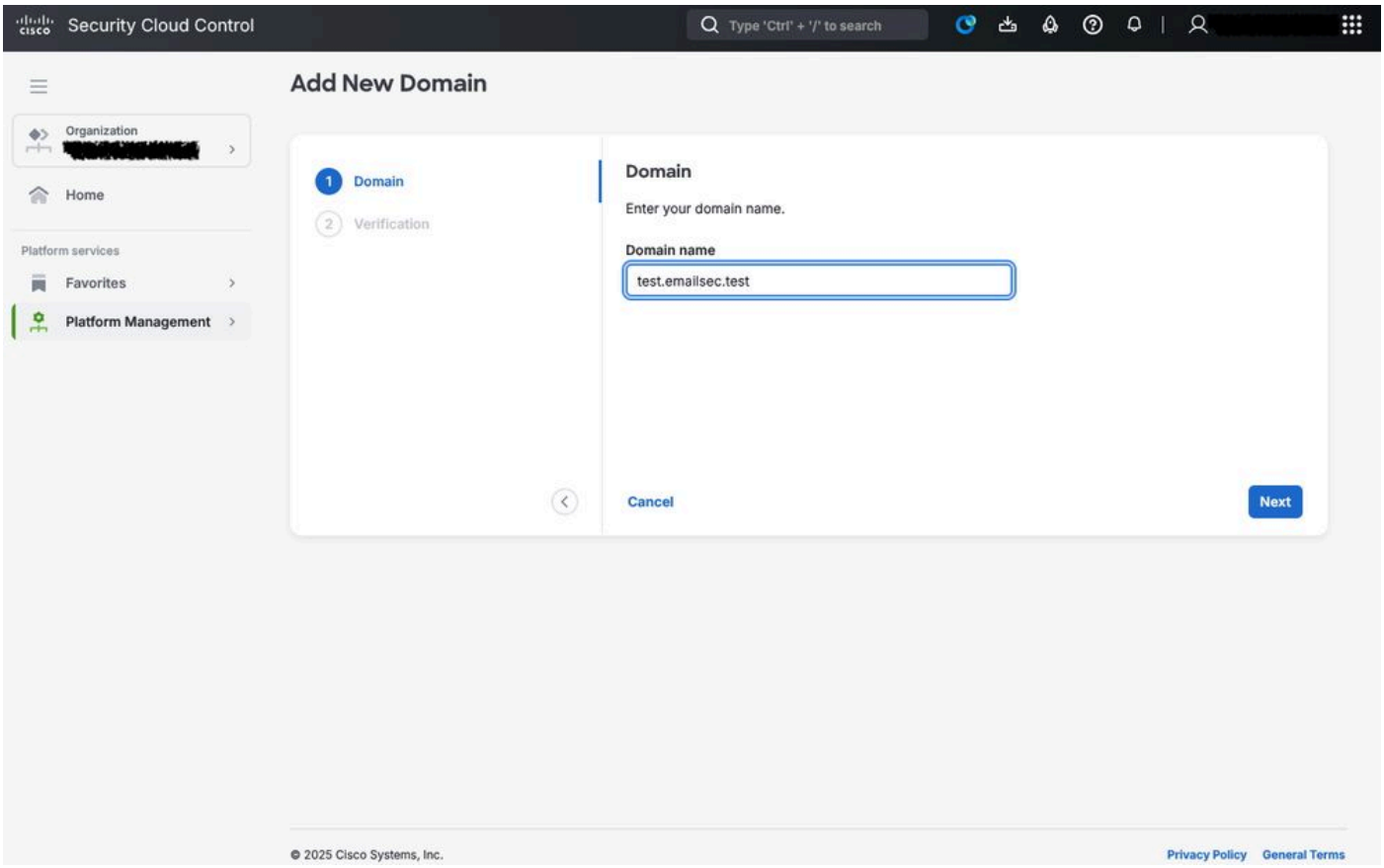


Cloud-Sicherheitskontrolle: Domäne

Schritt 4: Geben Sie die Domäneninformationen an.

Füllen Sie das Formular mit den Details der Domäne aus, die für die Authentifizierung verwendet wird. Dazu gehören in der Regel:

- Der Domänenname (z. B. test.emailsec.test)
- Kontaktinformationen (administrativ und technisch)
- Authentifizierungsparameter, abhängig vom gewählten Identitätsanbieter

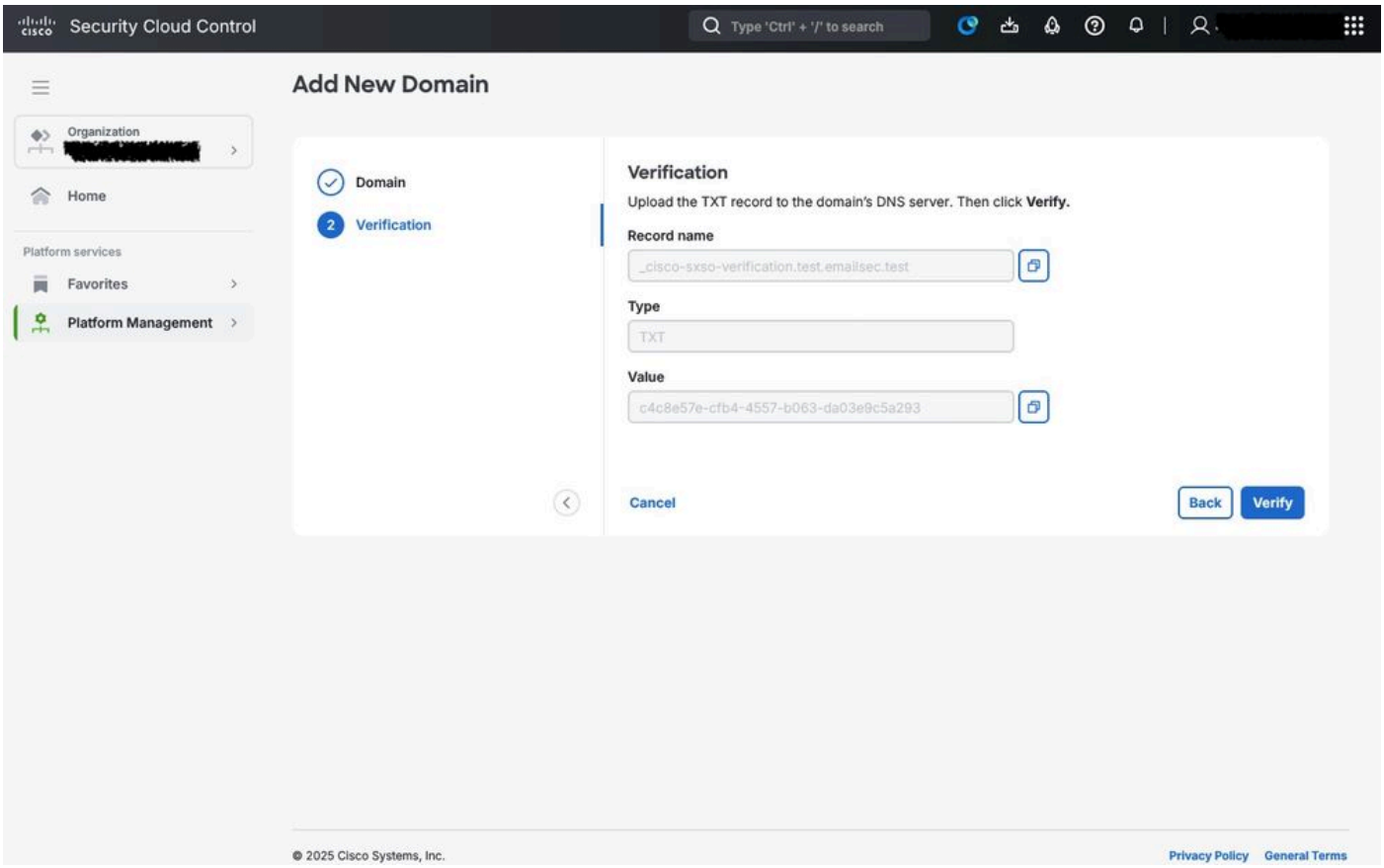


Schritt 5: Domain Verification via DNS.

Nach der Registrierung der Domäne benötigt Cisco einen Besitznachweis.

- Ein Verifizierungsdatensatz wird vom CSCC bereitgestellt.
- Dieser Eintrag muss Ihrer DNS-Konfiguration Ihrer Domäne hinzugefügt werden (in der Regel als TXT-Eintrag)
- Cisco Secure Cloud validiert automatisch den DNS-Eintrag, um sicherzustellen, dass die Domäne zu Ihrer Organisation gehört.

⚠ Vorsicht: Der Verifizierungsprozess muss erfolgreich abgeschlossen werden, bevor Sie mit der Integration fortfahren können. Je nach DNS-Propagierung dauert die Validierung mehrere Minuten bis einige Stunden.



Verbindung von ETD mit Cisco Duo mithilfe von Cisco SCC

Nach der erfolgreichen Konfiguration der Domäne des Administrators (die als Grundlage für strengere Zugriffskontrollen und zur Verwaltung von Berechtigungen dient), besteht der nächste Schritt in der Integration des vertraglich vereinbarten MFA-Services.

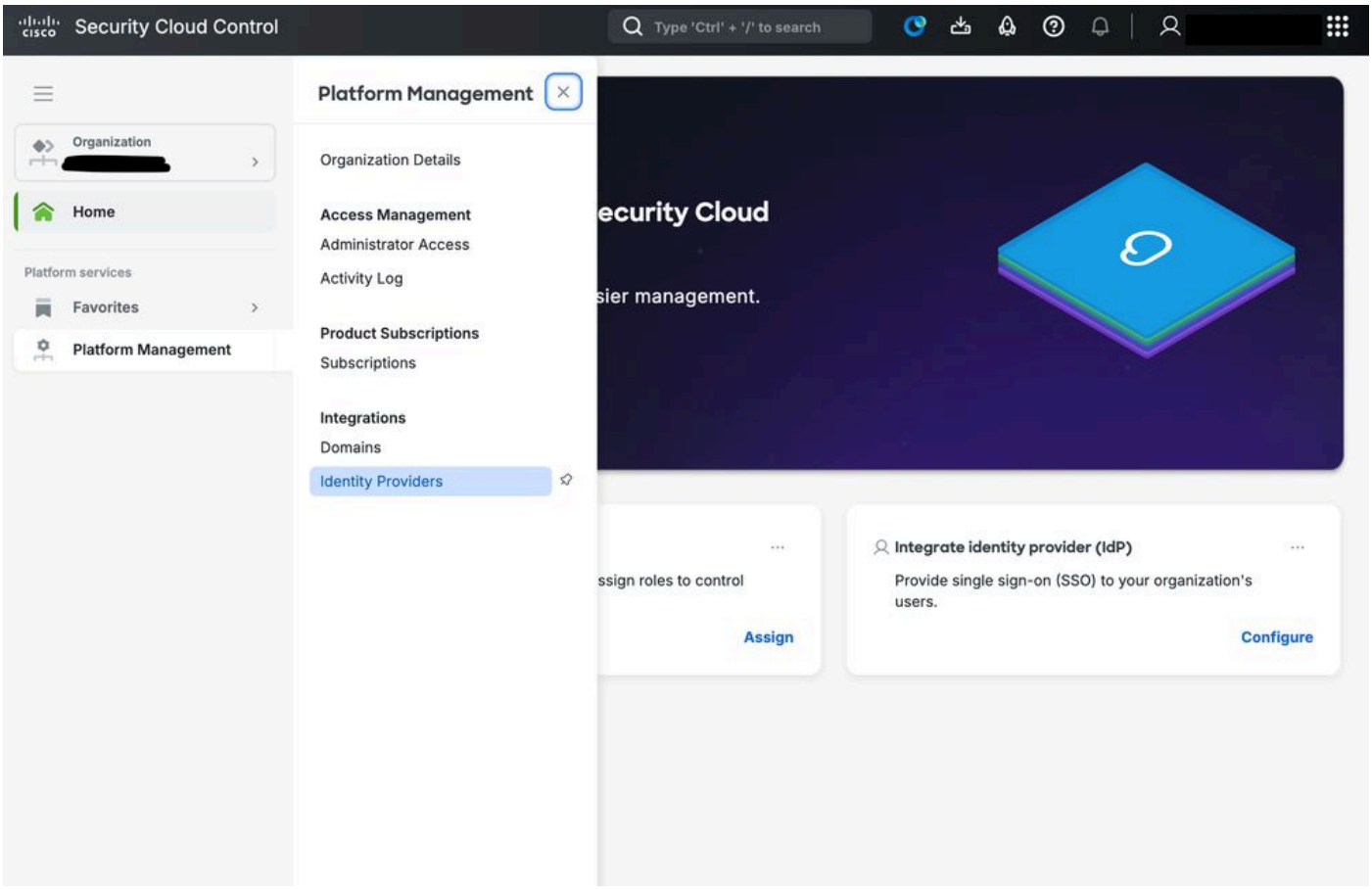
In diesem Szenario wird Cisco Duo als primäre Lösung für die Zugriffskontrolle, sichere Anmeldung und MFA-Verifizierung implementiert. Durch diese Integration wird der Sicherheitsstatus der Umgebung verbessert, da Administratoren ihre Identität in mehreren Überprüfungsschritten authentifizieren müssen. Dadurch wird das Risiko nicht autorisierter Zugriffe reduziert und die Einhaltung der Sicherheitsrichtlinien gewährleistet.

Integration von Cisco Duo und Cisco Cloud Control

Schritt 1: Zugriff auf die Cisco SCC-Konsole

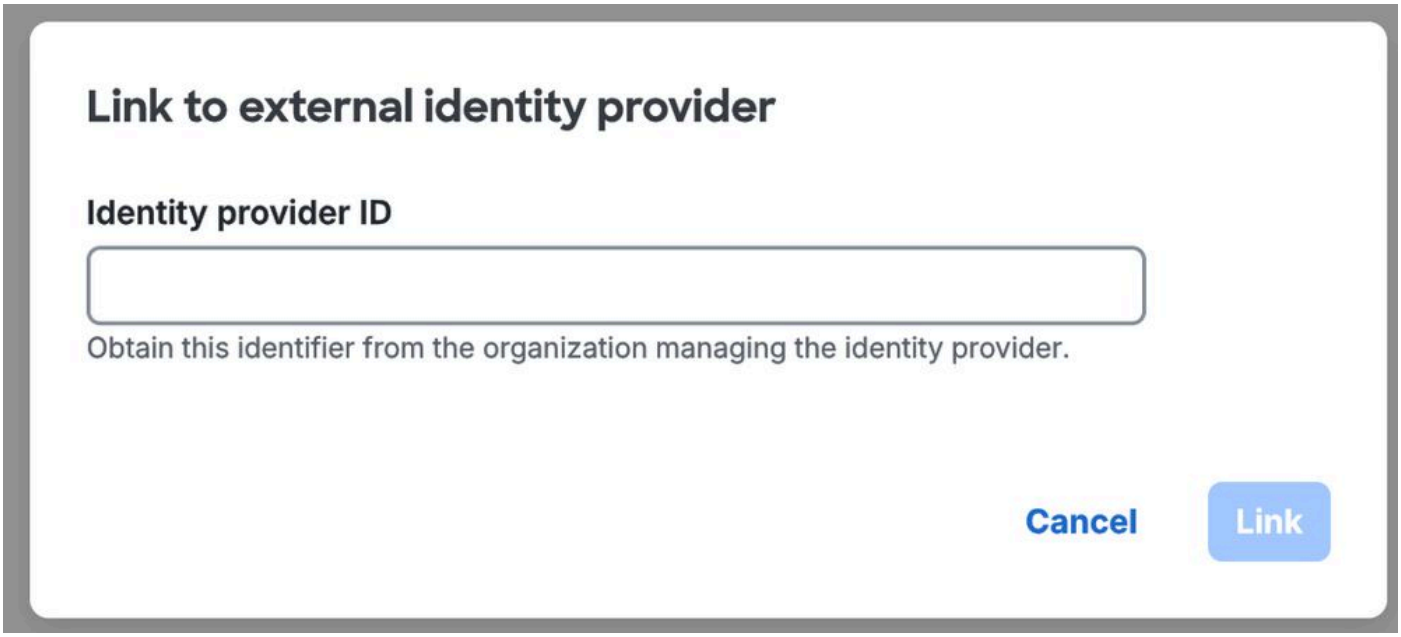
Melden Sie sich beim Cisco Security Cloud Control-Portal unter https://security.cisco.com/ an.

Navigieren Sie zu Plattformverwaltung, und klicken Sie auf Identitätsanbieter.



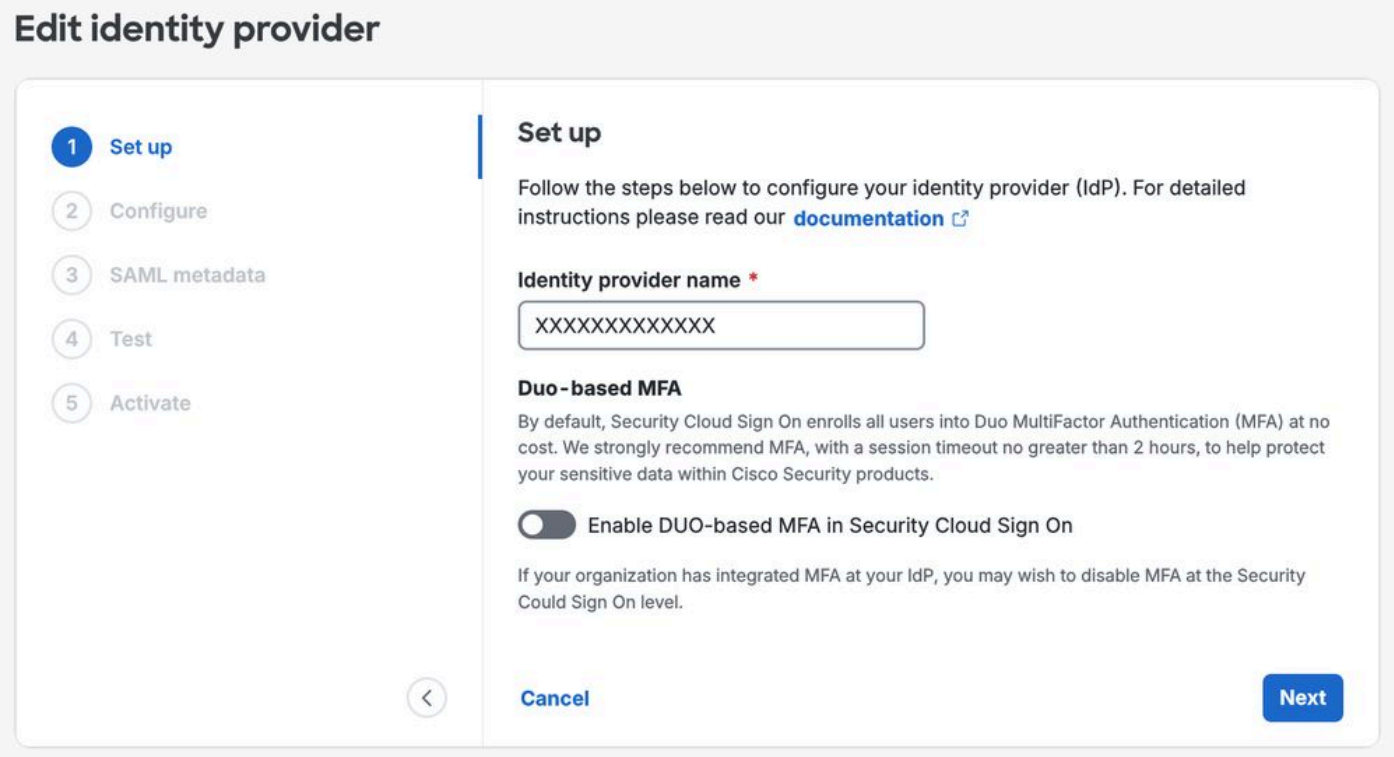
SCC IDP-Konfiguration

Verwenden Sie einen benutzerdefinierten Namen, um den Identitätsanbieter zu identifizieren.



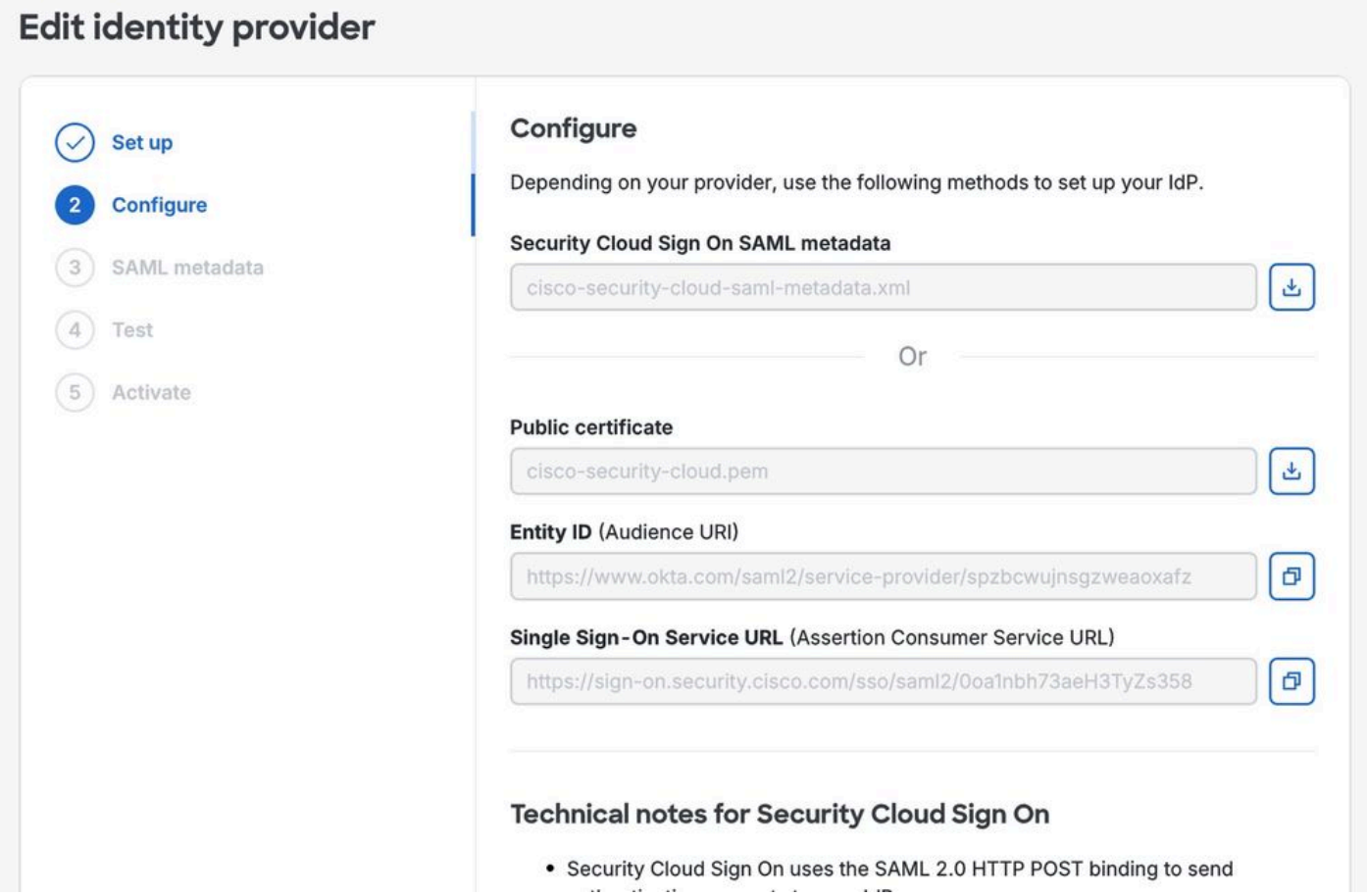
Nun startet das Setup. Sie haben jetzt Zugriff auf Cisco SCC und Cisco Duo.

Schritt 2: Deaktivieren Sie in SCC Enable DUO-based MFA in Security Cloud Sing On, wie in dargestellt, und klicken Sie auf Weiter.

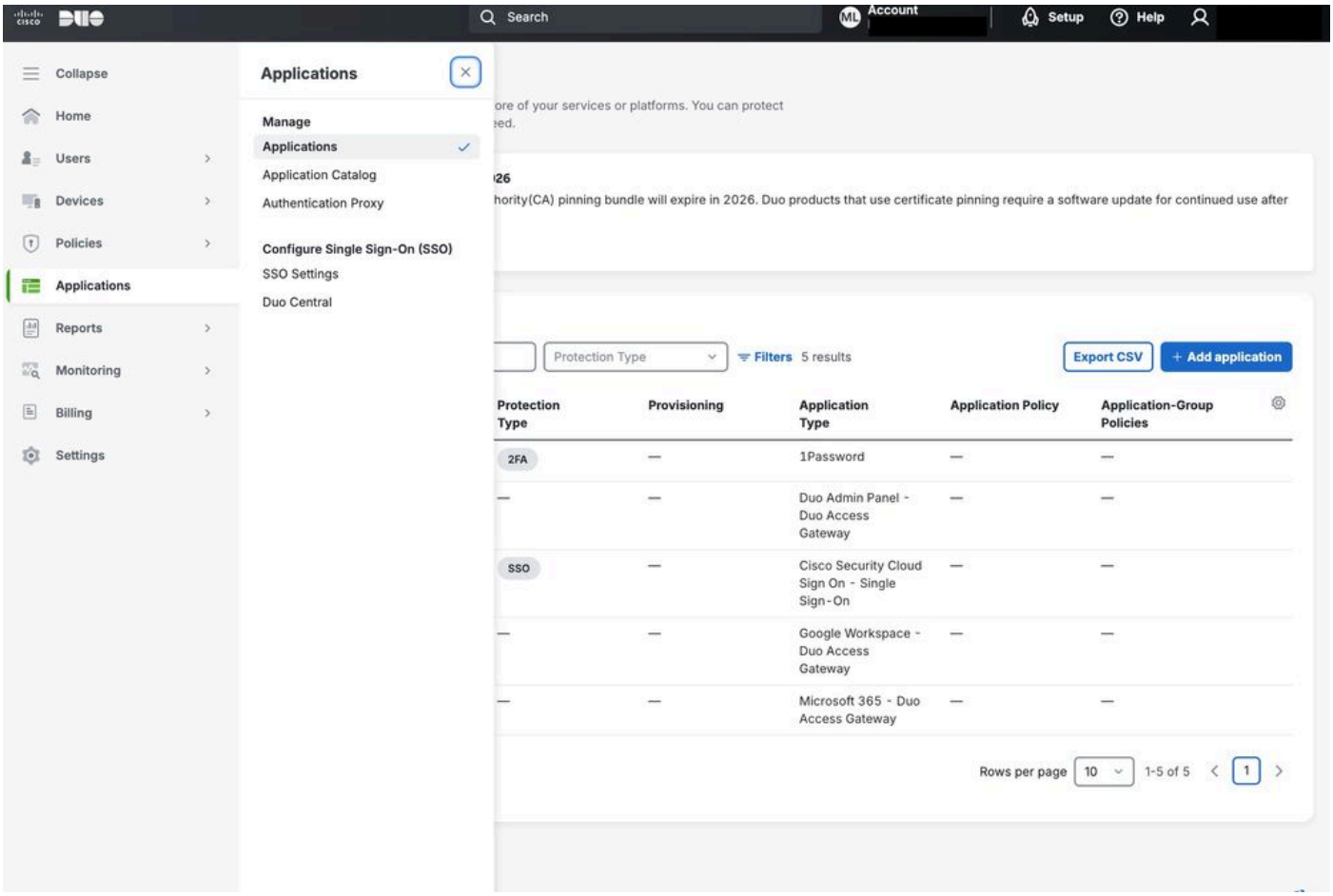


Identity Provider-Konfiguration

Schritt 3: Die relevanten Daten werden erstellt und während der Cisco Duo-Konfiguration verwendet.
Stellen Sie sicher, dass Sie alle erforderlichen Werte und zugehörigen Daten kopieren und an einem sicheren Ort speichern.
Diese Angaben sind für zukünftige Integrationsschritte unerlässlich. Stellen Sie daher sicher, dass nur autorisiertes Personal auf sie zugreifen kann und dass sie entsprechend den Sicherheitsrichtlinien Ihres Unternehmens geschützt sind.

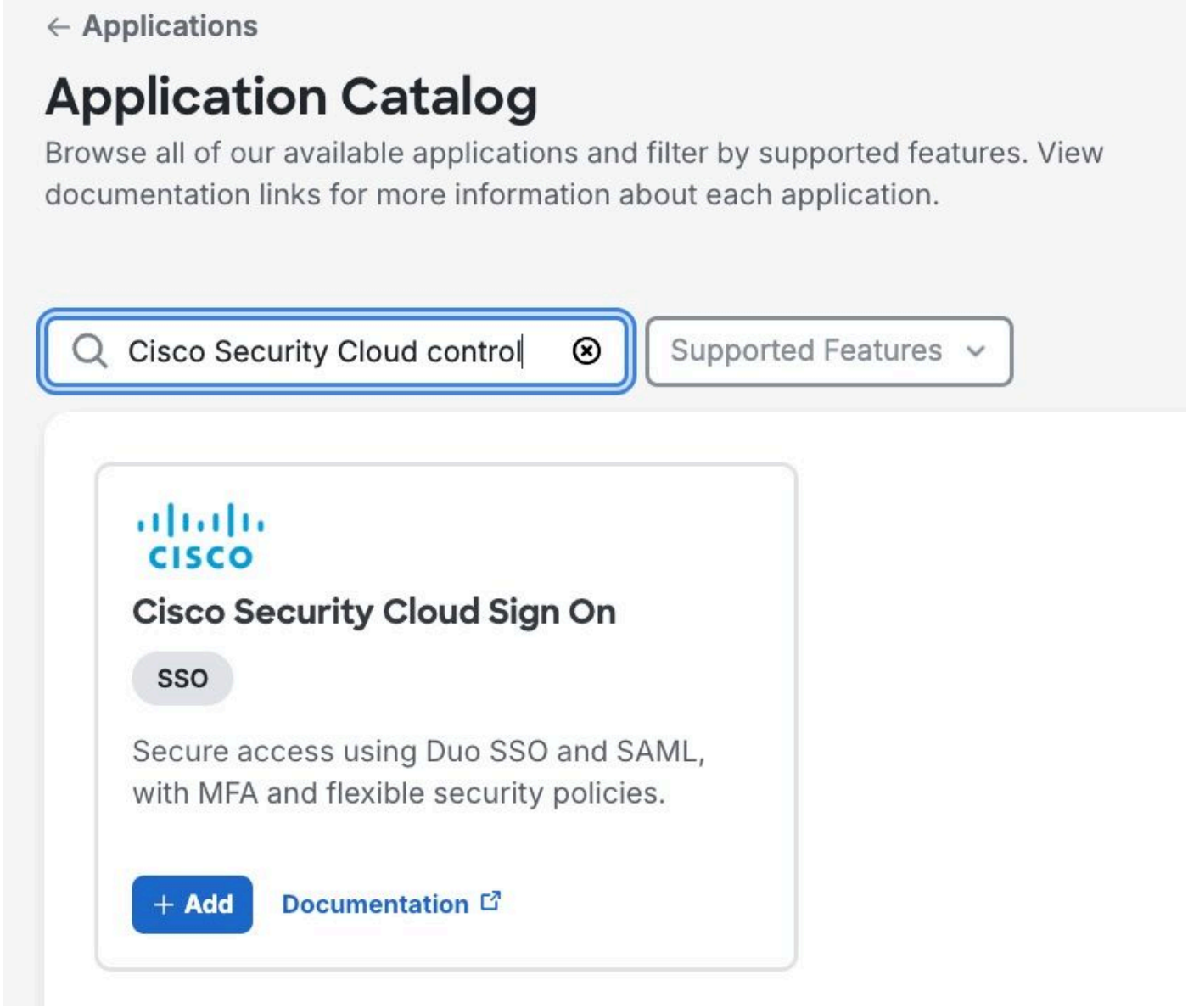


Schritt 4: Öffnen Sie Cisco Duo, navigieren Sie zum Abschnitt Applications (Anwendungen), und klicken Sie auf Add application (Anwendung hinzufügen).



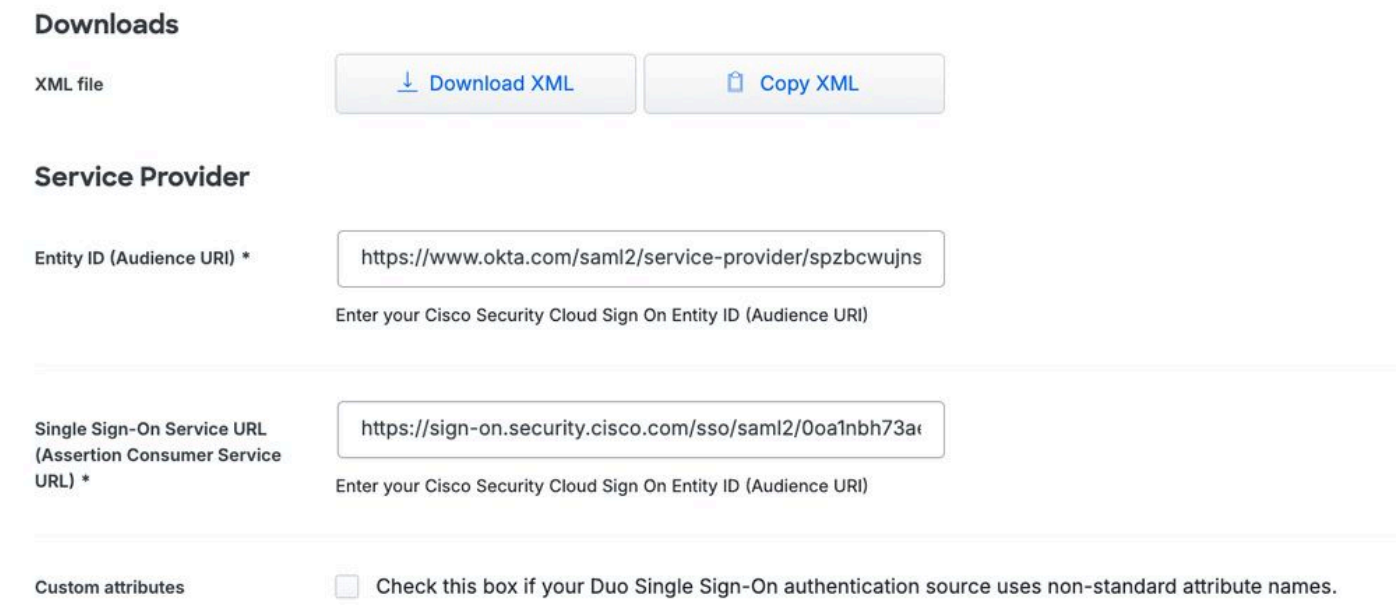
Cisco DUO-Anwendungen

Suchen Sie im Menü nach Cisco Security Cloud, und klicken Sie auf Hinzufügen, um die Integration zu starten.

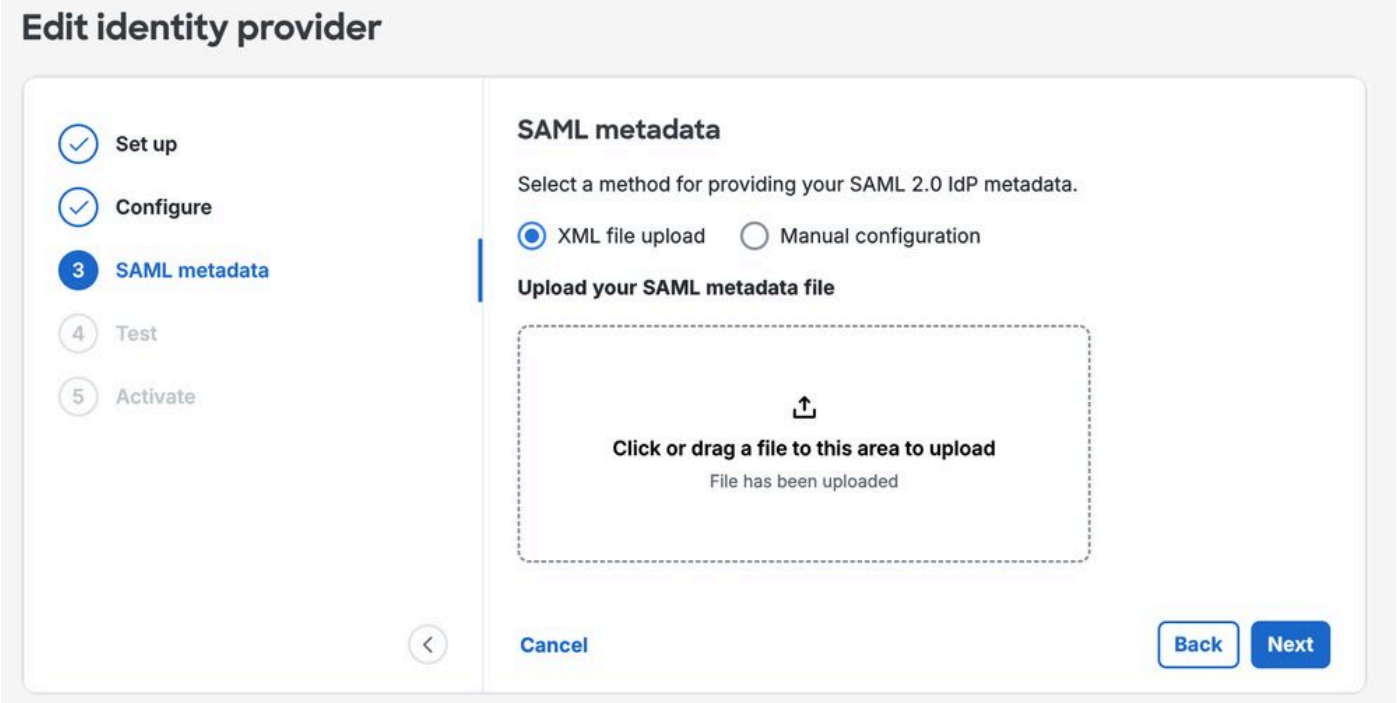


Schritt 5: Konfigurieren Sie die relevanten Informationen in der Cisco Duo-Anwendung.

Kopieren Sie die Entitäts-ID und die URL des Single Sign-On-Service aus dem Cisco SCC in Cisco Duo.



Schritt 6: Laden Sie die XML-Datei herunter, und laden Sie sie in Cisco SCC hoch.



Anmerkung: Die übrigen Parameter, die in der Anwendung über die Cisco Duo Konsole konfiguriert werden können, müssen Ihren spezifischen Anforderungen entsprechend angepasst werden. Ausführliche Erläuterungen zu den einzelnen Einstellungen finden Sie in der offiziellen Cisco Duo-Dokumentation. Beispiele für konfigurierbare Parameter sind der zugewiesene Anwendungsname, die Gruppe von Benutzern, auf die die Richtlinie angewendet wird, und andere Anpassungsoptionen, mit denen die Sicherheitskontrollen an die Anforderungen Ihres Unternehmens angepasst werden können.

Richtlinienkonfiguration in Cisco Duo für Cisco ETD

Zu diesem Zeitpunkt sind alle Komponenten verbunden. Der nächste Schritt besteht in der Konfiguration einer Richtlinie, die für den Authentifizierungsprozess des Administrators in der Cisco ETD-Konsole gilt.

In diesem Beispiel liegt der Schwerpunkt auf der Zugriffskontrolle auf Basis der IP-Adresse. Cisco Duo bietet jedoch noch viele weitere Zugriffskontrolloptionen.

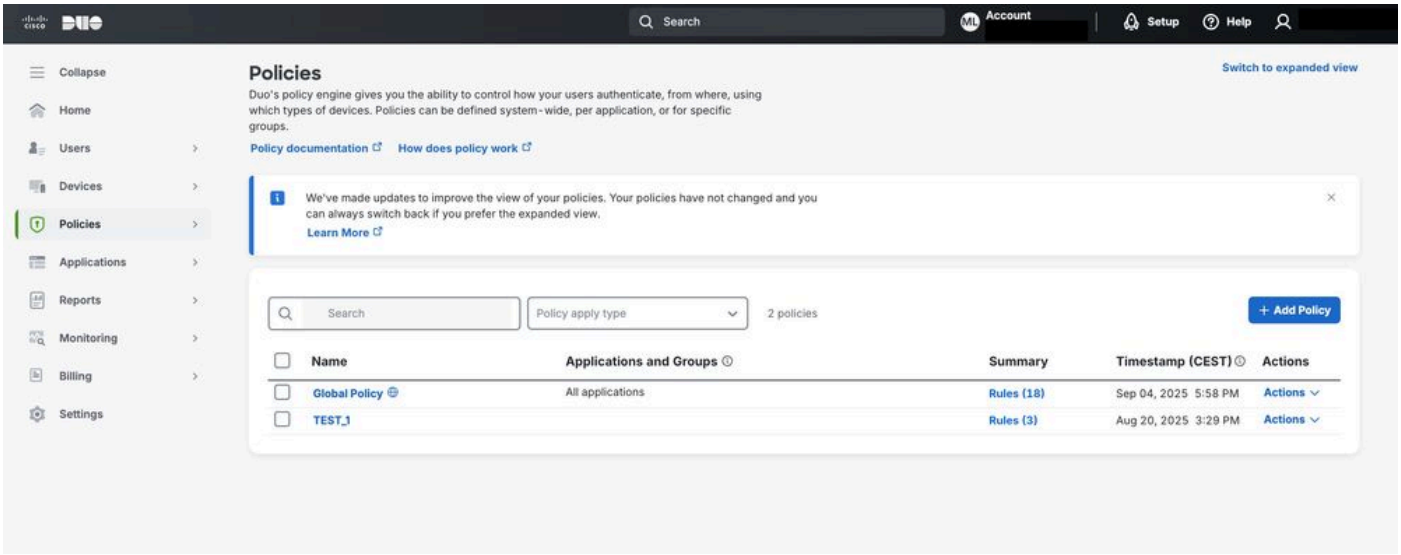
Eine neue Richtlinie kann erstellt und der Anwendung zugewiesen werden, sodass die gewünschten Authentifizierungsregeln und Sicherheitseinschränkungen für Administratoranmeldungen durchgesetzt werden können.

Detaillierte Informationen zu allen in Cisco Duo verfügbaren Steuerungen und Konfigurationsoptionen finden Sie in der offiziellen Cisco Duo Dokumentation.

Diese Ressource bietet umfassende Anleitungen zur Einrichtung, Anpassung und zu Best Practices, um Sicherheitsrichtlinien zu optimieren.

Navigieren Sie in Cisco Duo zum Abschnitt Policies (Richtlinien), und erstellen Sie über Cisco Duo eine Richtlinie, die der Cisco ETD-Verbindung zugewiesen wird.

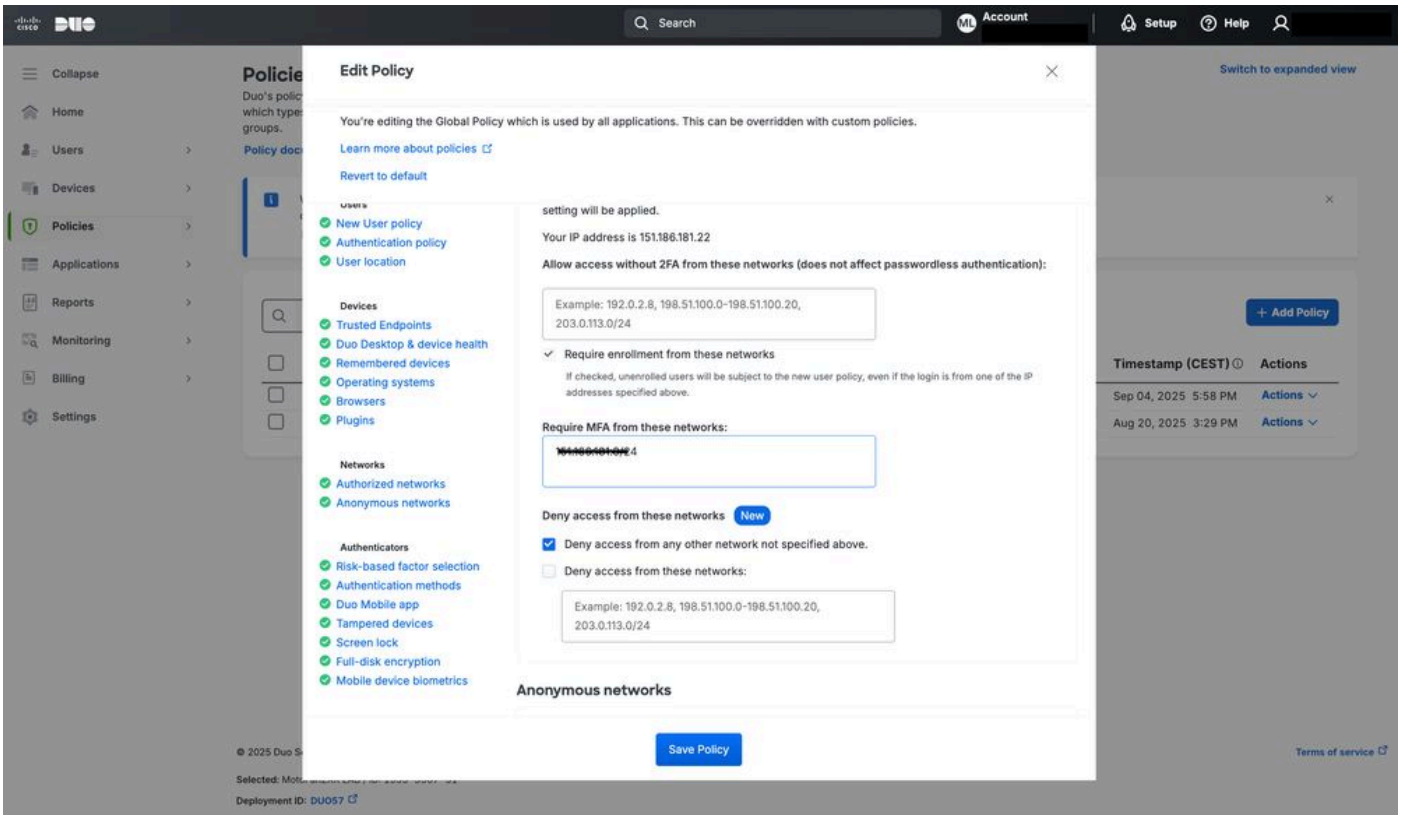
Diese Richtlinie kann je nach Zugriffsanforderungen für jeden Benutzer oder jede Gruppe angewendet werden.



Cisco Duo

In diesem Beispiel wird, wie im Bild gezeigt, die Quell-IP-Zugriffskontrolle aktiviert, indem der Abschnitt "Autorisierte Netzwerke" konfiguriert wird.

Diese Konfiguration ermöglicht den Zugriff nur aus bestimmten vertrauenswürdigen IP-Bereichen und erhöht so die Sicherheit für Cisco ETD.



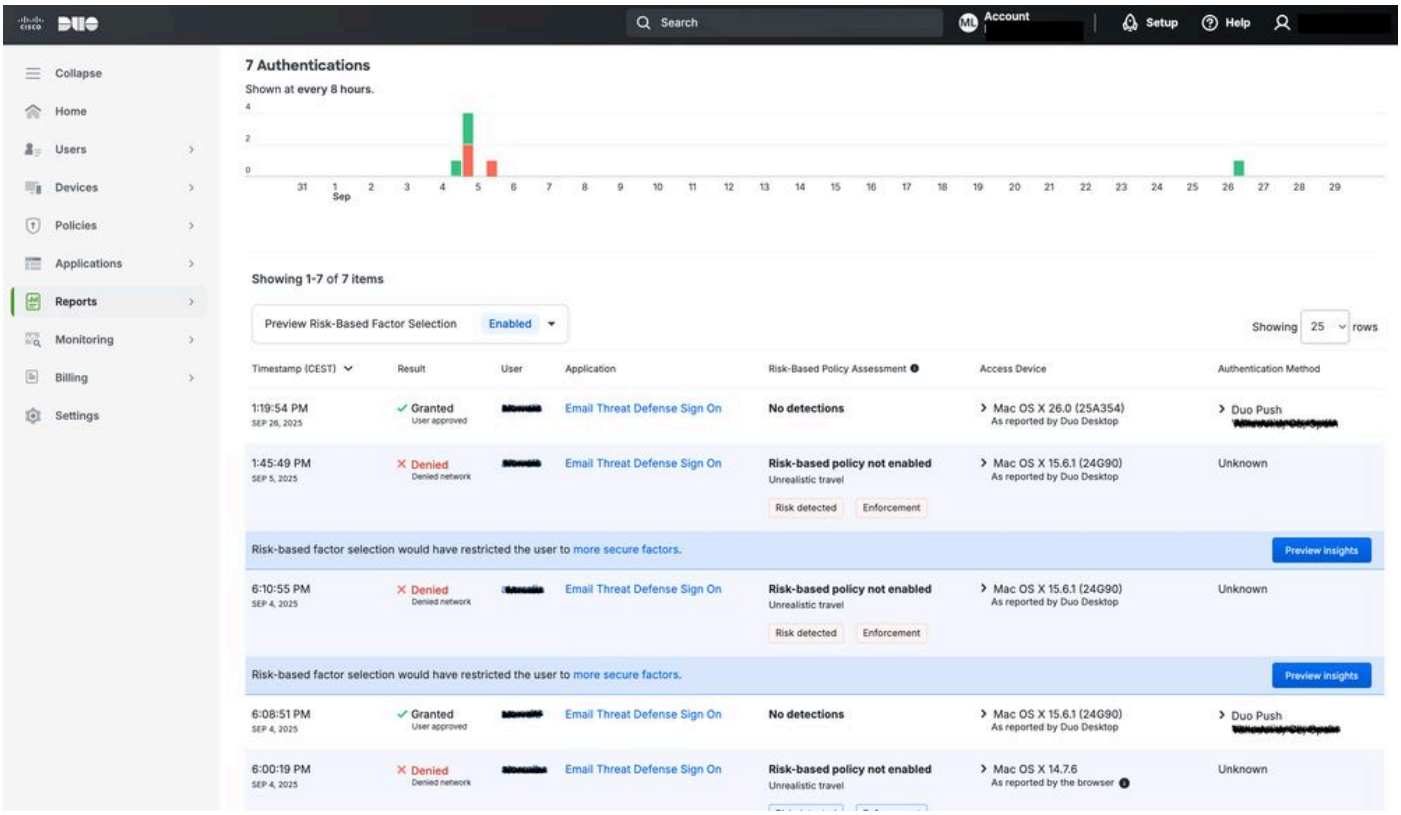
Konfiguration der Cisco Duo Richtlinien

Schlussfolgerungen

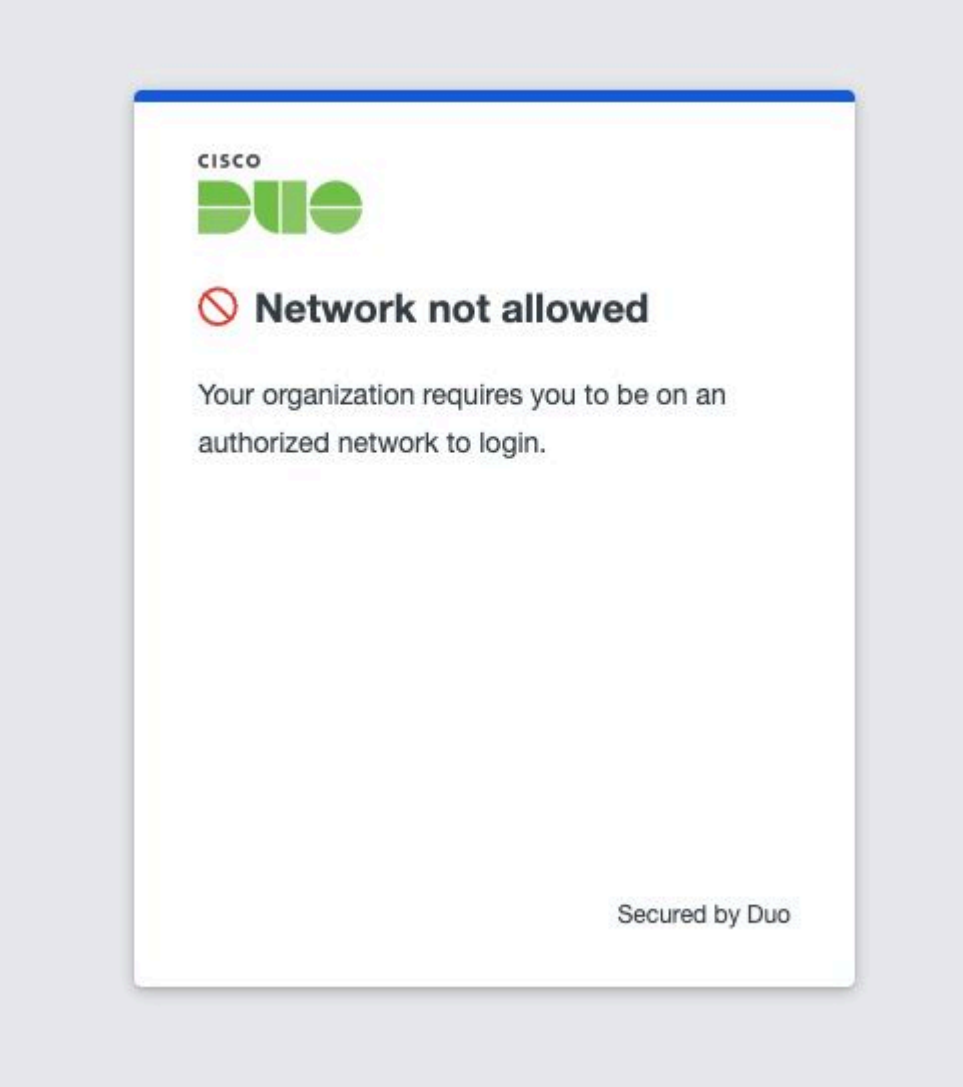
Cisco ETD bietet flexible Optionen zum Schutz des Administratorzugriffs über MFA und zur Integration mit Identitätsanbietern.
Durch die Kombination von Cisco SCC mit Cisco Duo können Unternehmen strengere Authentifizierungsrichtlinien implementieren, das Risiko nicht autorisierter Zugriffe reduzieren und die branchenspezifischen Best Practices für ein sicheres Cloud-Service-Management einhalten.

Zusätzlich zu MFA können Administratoren richtlinienbasierte Kontrollen von Cisco Duo nutzen, um den Zugriff anhand bestimmter Kriterien wie der Quell-IP-Adresse einzuschränken. Wie im nächsten Bild gezeigt, wird beispielsweise ein Zugriffsversuch von einer IP-Adresse außerhalb des autorisierten Bereichs automatisch vom System blockiert. So wird sichergestellt, dass nur Anfragen aus vertrauenswürdigen Netzwerken zugelassen werden. Dies erhöht den Schutz vor potenziellen Angriffen.

Durch die Implementierung einer IP-basierten Zugriffskontrolle in Verbindung mit MFA profitieren Unternehmen von einem tief greifenden Ansatz, bei dem Identitätsüberprüfung mit Standortüberprüfung des Netzwerks kombiniert wird, um wichtige Managementschnittstellen in der Cloud zu schützen.



Cisco Duo-Berichte



Ergebnis der Netzwerkkontrolle

Warnung: Es ist wichtig zu verstehen, dass diese Änderung alle Anwendungen betrifft, die dieselbe Authentifizierungsdomäne verwenden. nicht nur ETD, sondern auch andere Produkte, die auf den gleichen Authentifizierungsprozess angewiesen sind, wie z. B. der Zugriff auf die Cisco Secure Access-Konsole.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.