セキュアなEメール脅威に対する防御：多要素認証とアクセスコントロール

内容

はじめに

このドキュメントでは、Cisco Email Threat Defense(ETD)が管理コンソールへの管理者アクセスを制御するために提供する機能について説明します。

前提条件

要 件

Duoを使用してETD認証を設定するために、次の項目に関する知識があることが推奨されます。

- Cisco ETDサブスクリプション
- Cisco Security Cloud Control(SCC)へのアクセス
- セキュリティを強化するための認証ソリューション。この例ではCisco Duoです。

使用するコンポーネント

このドキュメントは、Eメール処理の防御とセキュアなクラウド制御に限定されています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

バックグラウンド情報

このドキュメントでは、Cisco ETDがどのようにCisco SCCを活用し、Cisco Duoと統合してセキュアな認証ときめ細かなアクセスコントロールを提供するかについて説明します。

最新のクラウドベースのソリューションでは、アクセスコントロールは、データセキュリティ、規制へのコンプライアンス、および運用の整合性を確保するうえで最も重要なコンポーネントの1つです。不正アクセス、特に管理者アカウントへの不正アクセスは、システムの侵害、データ漏洩、サービスの中断などの深刻な結果につながる可能性があります。

シスコは、Cisco ETDのようなサービスに不可欠なマルチファクタ認証(MFA)テクノロジーを含むクラウドポートフォリオ全体に、堅牢なセキュリティ機能を提供しています。MFAは、従来のパスワードの枠を超えて重要な検証手順を追加します。ユーザは、モバイルアプリケーションの承認、セキュリティトークン、生体認証の検証などの追加の要因によって認証を受ける必要があります。

管理者の認証プロセスを合理化および強化するために、ETDは中央集中型の認証およびポリシー管理サービスであるCisco SCCを利用します。

SCCを通じて、ETDは次のような幅広いセキュリティ機能にアクセスできます。

- クレデンシャル盗難のリスクを軽減するためのMFA適用
- Cisco Duo、Microsoft Entra ID、Oktaなどのサードパーティアイデンティティプロバイダーとの統合により、柔軟な認証ワークフローとエンタープライズアイデンティティフェデレーションをサポート。
- 一元化されたポリシー管理により、シスコクラウドサービス全体で一貫したアクセスルールを実現します。

特にCisco Duoは、高度なポリシーベースのアクセス管理を追加することで、これらの機能を拡張します。統合チャネルとしてSCCを使用すると、ETDは、送信元IP制限、デバイスのヘルスチェック、ユーザグループベースのルールなど、Duoのきめ細かい制御を管理者アクセスに直接適用できます。

たとえば、特定の信頼できるネットワーク範囲からのアクセスだけを許可するポリシーを定義できます。添付の図に示すように、許可されたIPリスト外での接続試行は自動的にブロックされる可能性があります。MFAとコンテキストに応じたポリシーを組み合わせることで、多層防御アプローチが可能になり、クレデンシャルが侵害されても、攻撃者は追加のセキュリティ基準を満たさない限りシステムへのアクセスを阻止できます。

Cisco ETD、Cisco SCC、およびCisco Duoを統合することにより、企業は安全性と拡張性が高く、使いやすいアクセス制御モデルを実装し、業界のベストプラクティスに合わせて、重要なクラウドサービスの保護を強化できます。

シナリオ

管理アクセスを保護するために、ETDでは次のような認証およびアクセスコントロールシナリオを実装できます。

1. 組み込みMFA：シスコの組み込みMFAを使用するか、Microsoft MFAを統合します。
2. Cisco SCCとCisco Duo - Cisco SCCの中央集中型の認証とDuoの高度なMFA機能を組み合わせます。
3. 外部アイデンティティプロバイダー（Microsoft Entra IDなど）を備えたCisco SCC – エンタープライズアイデンティティソリューションと統合することで、認証ポリシーを拡張します。

このドキュメントでは、「シナリオ2:Cisco SCCとCisco Duo」の設定手順について説明します。ただし、このプロセスは他のテクノロジーにも適用できます。

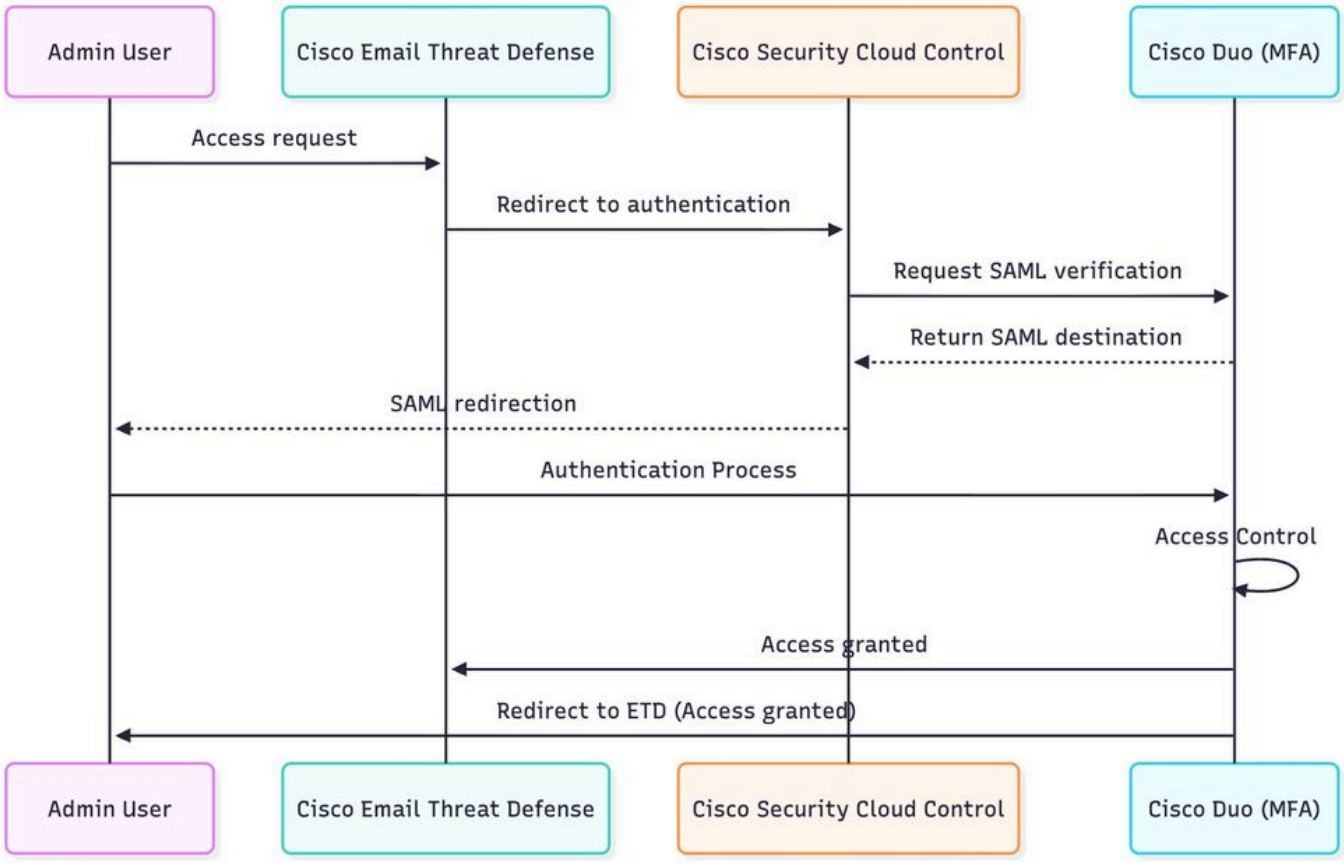
注：このドキュメントでは、Cisco Duoの多要素認証機能を使用してEmail Threat Defense(ETD)のアクセスコントロールを有効にするために必要な基本手順の概要について説明します。Duo統合を実装すると、許可されたユーザーのみがプラットフォームにアクセスできるようにすることで、セキュリティが強化されます。包括的なガイダンス、設定オプション、高度な導入シナリオについては、次の公式製品ドキュメントを参照してください。

– セキュリティポリシーとアクセス管理の一元化

Cisco Duo：多要素認証の設定とベストプラクティスに関する詳細な手順が記載されています。

Cisco SCCの設定

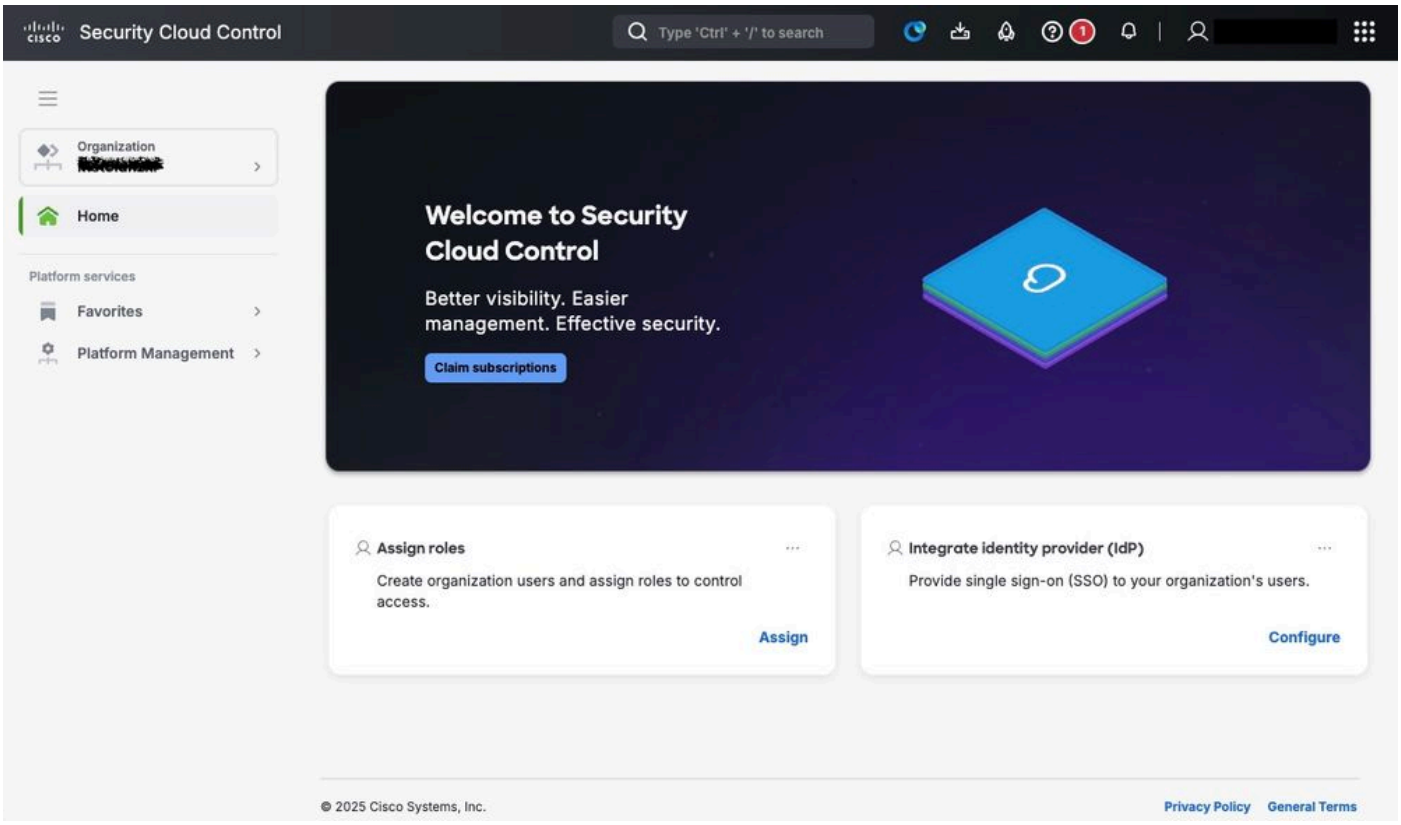
Cisco ETDをCisco Duoと統合するには、まずCisco SCCで認証ドメインを設定します。これにより、Cisco SCCが外部IDおよびMFAプロバイダーと連携できる信頼関係が確立されます。



図

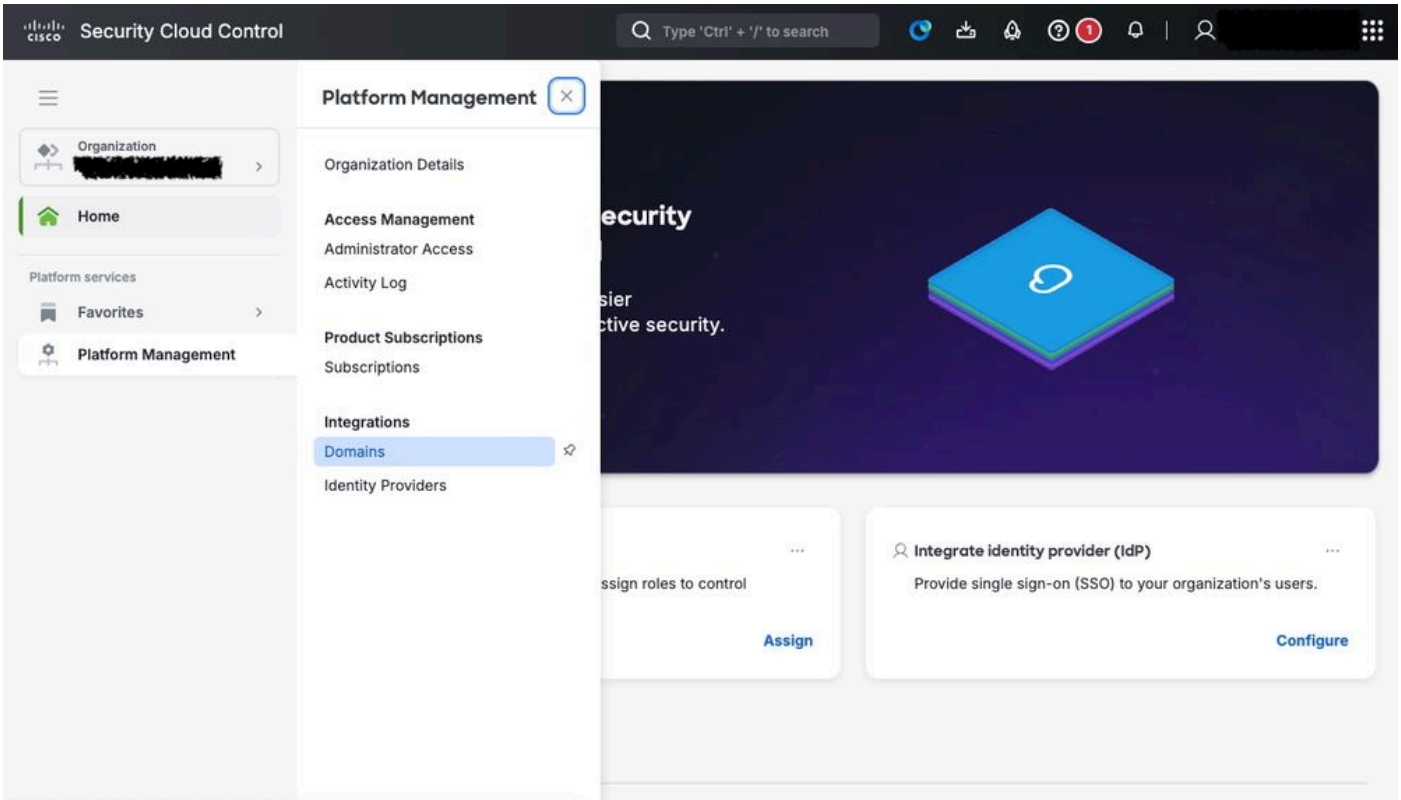
ステップ 1：Cisco SCCコンソールにアクセスします。

Cisco SCCポータルhttps://security.cisco.com/にログインします。



ステップ 2Domain Managementに移動します。

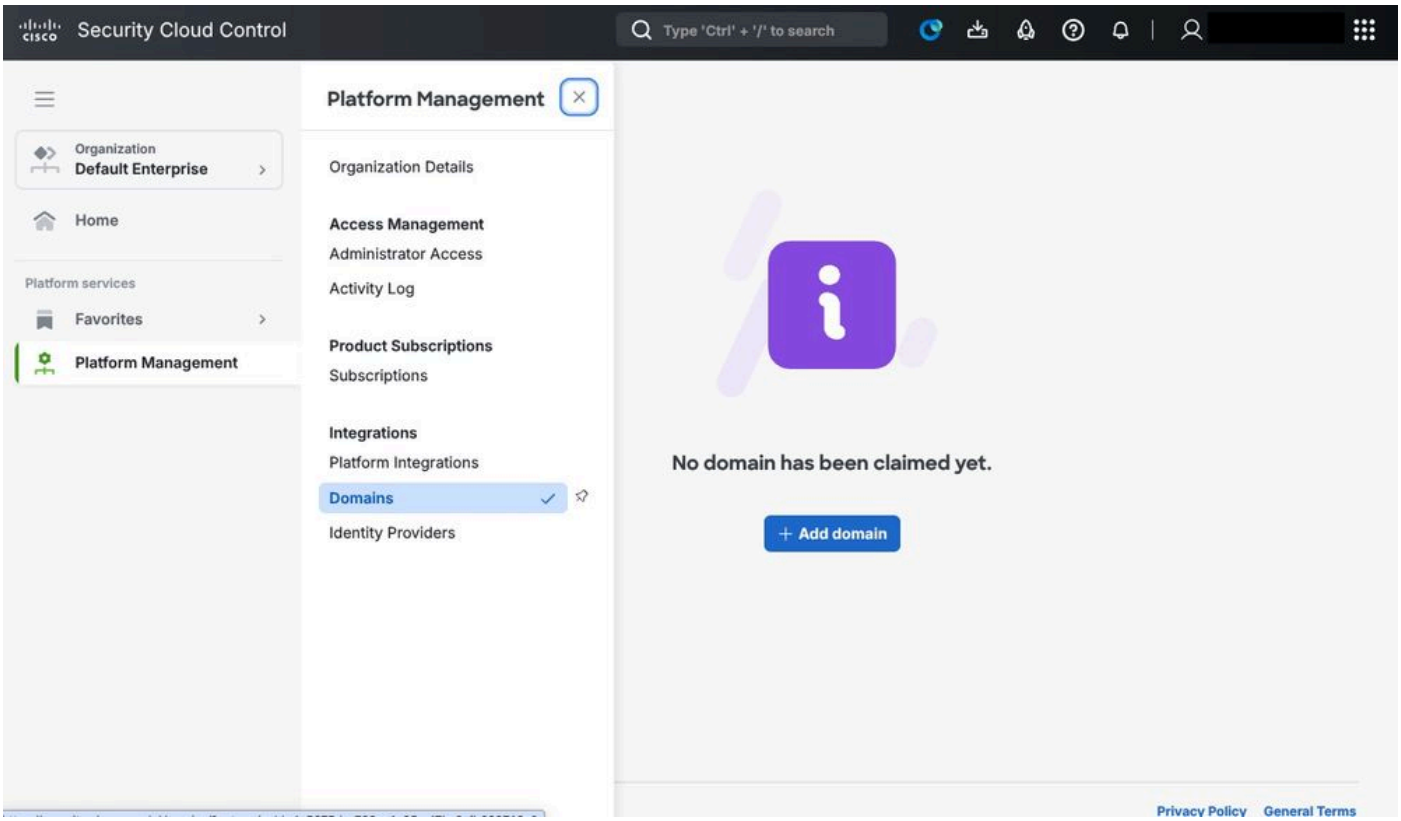
メインメニューから、Platform Management > Domainsの順に選択します。



Secure Cloud Control Domainの設定

ステップ 3新しいドメインを追加します。

Add Domainをクリックして、認証ドメインの登録プロセスを開始します。

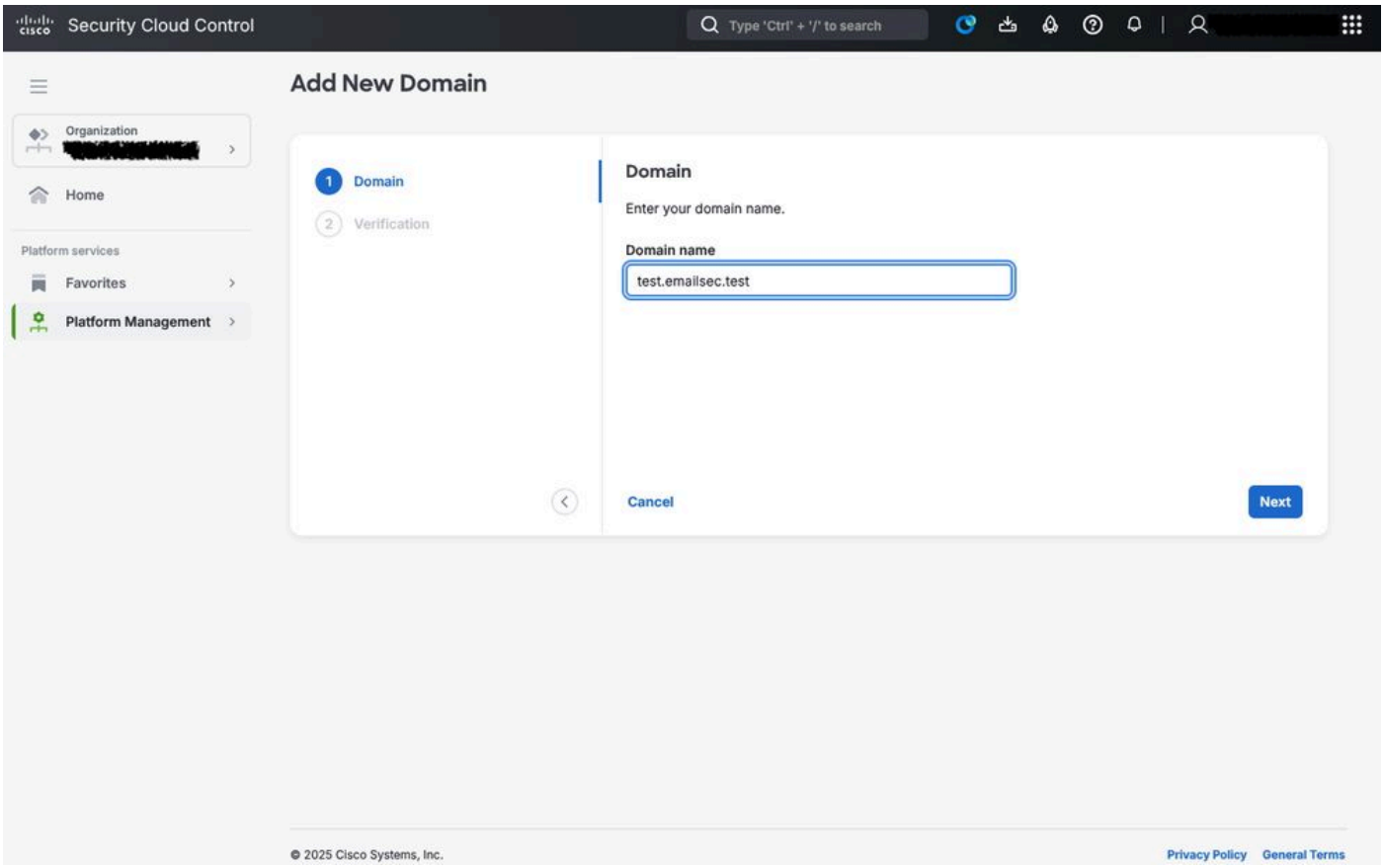


セキュリティクラウド制御：ドメイン

ステップ 4ドメイン情報を入力します。

フォームに、認証に使用するドメインの詳細を入力します。これには通常、次のものが含まれます。

- ドメイン名(test.emailsec.testなど)
- 連絡先情報（管理および技術）
- 選択したIDプロバイダーに応じた認証パラメータ

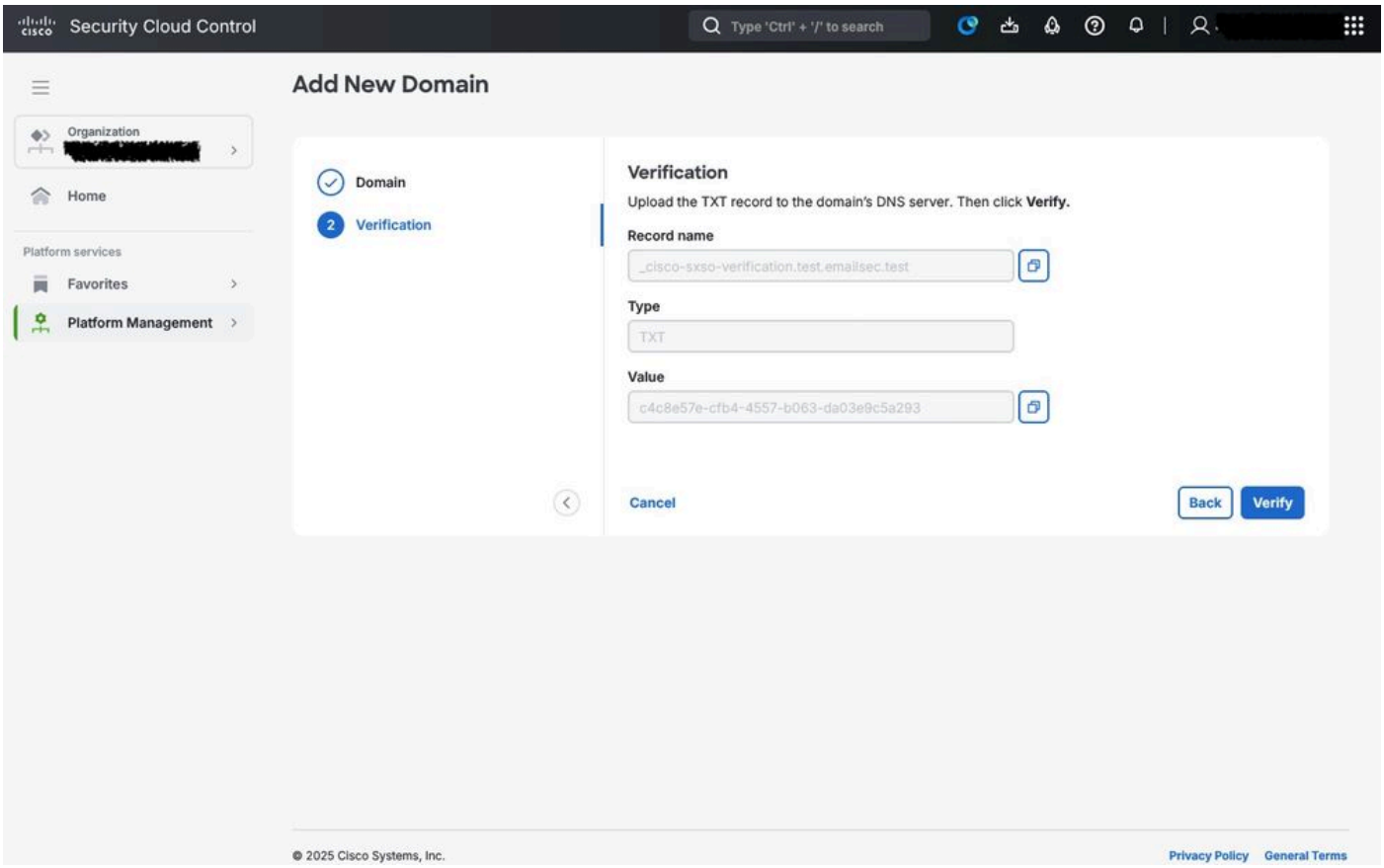


ステップ 5DNSによるドメインの検証

ドメインが登録されると、シスコは所有権の証明を要求します。

- 検証レコードはCSCCから提供されます
- このレコードは、ドメインのDNS設定に追加する必要があります（通常はTXTレコードとして）
- Cisco Secure CloudがDNSエントリを自動的に検証し、ドメインが組織に属していることを確認します

⚠ 注意：統合を進める前に、検証プロセスを正常に完了する必要があります。DNSの伝播によっては、検証に数分から数時間かかります。



Cisco SCCを使用したETDとCisco Duoの接続

管理者のドメインが正常に設定されたら（より厳密なアクセス制御を適用し、権限を管理するための基盤として機能します）、次の手順では、契約されたMFAサービスを統合します。

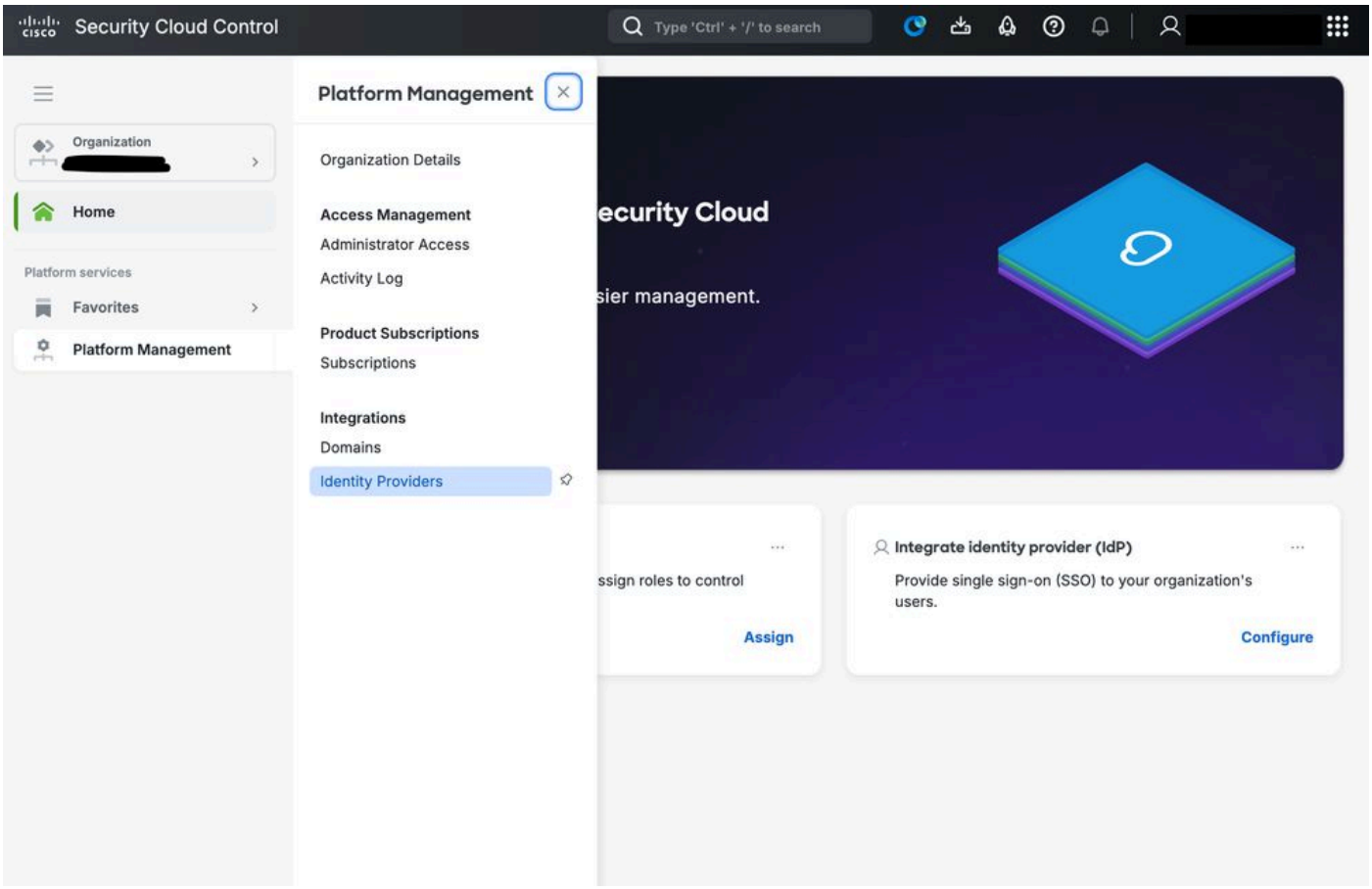
このシナリオでは、アクセスコントロール、セキュアログイン、およびMFA検証の主要なソリューションとしてCisco Duoが実装されます。この統合により、管理者が複数の認証手順を通じてIDを認証することが必要になるため、環境のセキュリティ体制が強化され、不正アクセスのリスクが軽減され、組織のセキュリティ・ポリシーへのコンプライアンスが確保されます。

Cisco DuoとCisco Cloud Controlの統合

ステップ 1： Cisco SCCコンソールへのアクセス

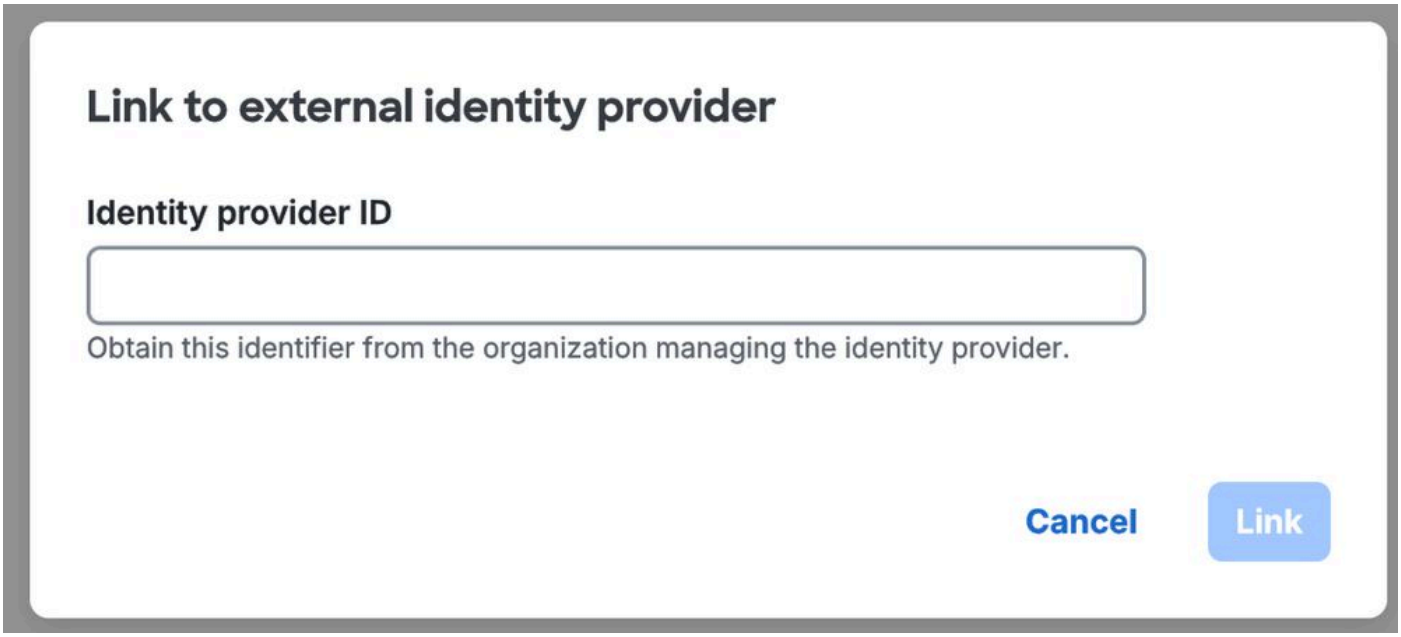
Cisco Security Cloud Controlポータルhttps://security.cisco.com/にログインします。

Platform Managementに移動し、Identity Providersをクリックします。



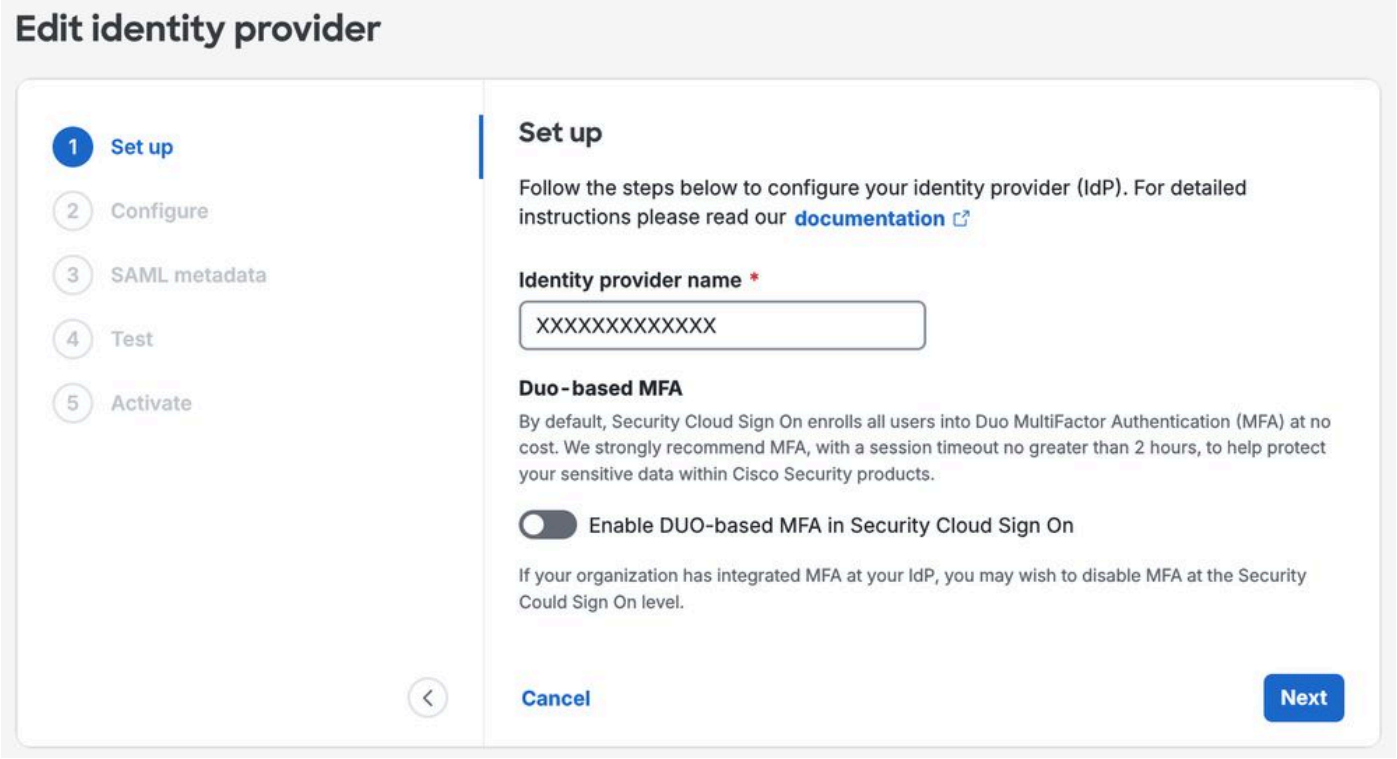
SCC IDPの設定

IDプロバイダーを識別するには、カスタム名を使用します。



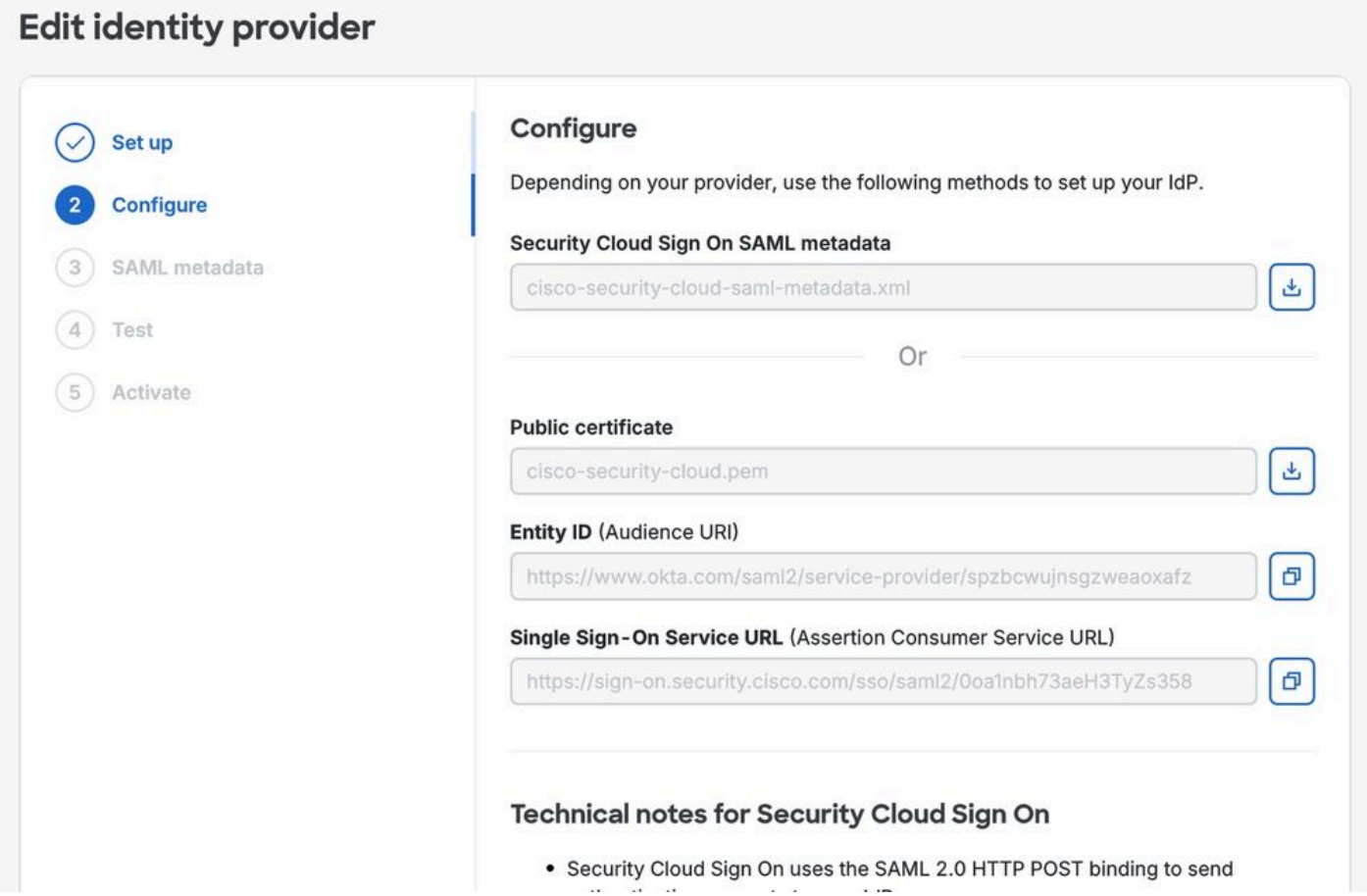
セットアップが開始されます。この時点で、Cisco SCCおよびCisco Duoにアクセスできます。

ステップ 2次の図に示すように、SCCでEnable DUO-based MFA in Security Cloud Sing Onを無効にして、Nextをクリックします。

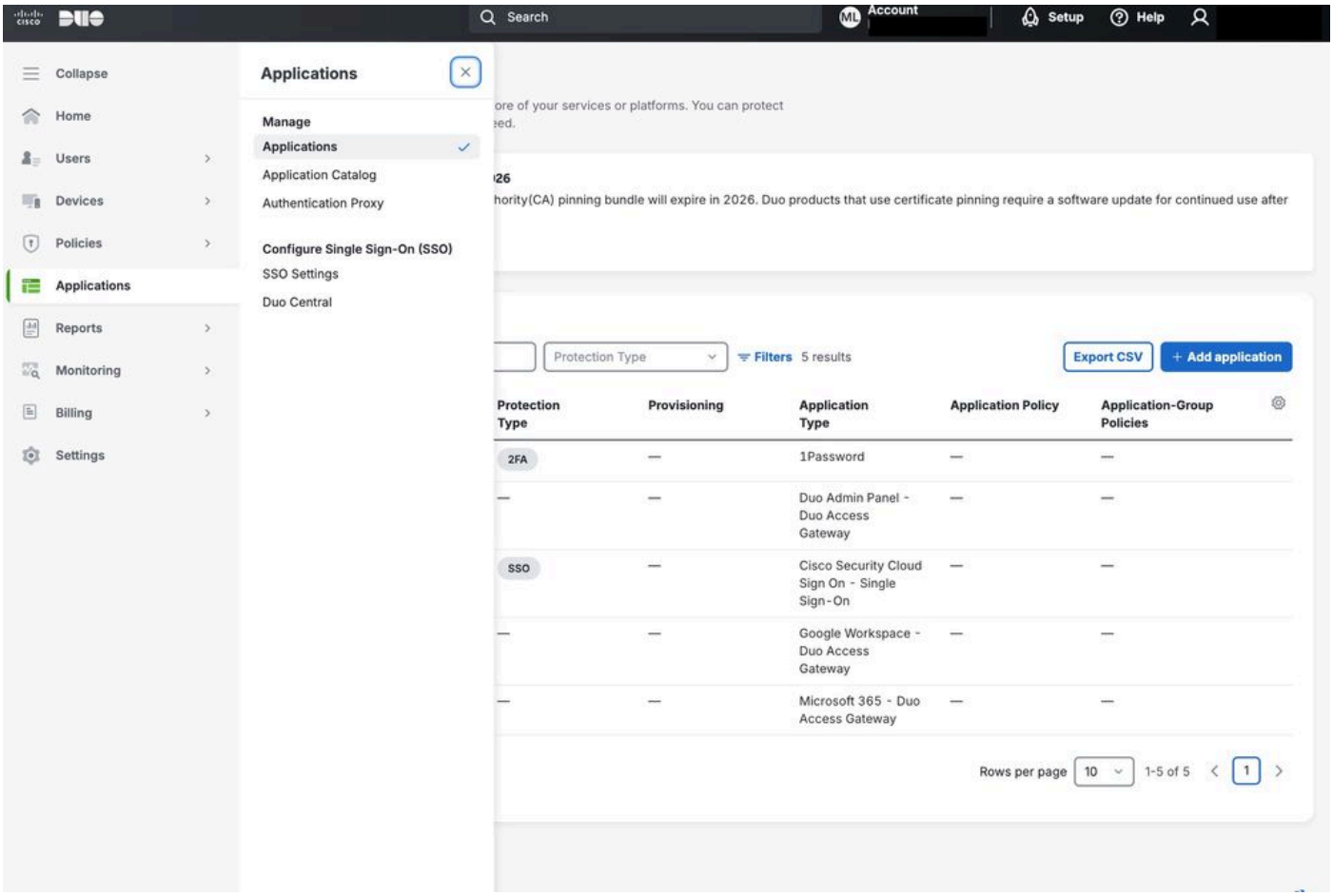


IDプロバイダーの設定

ステップ 3関連データが作成され、Cisco Duoの設定時に使用されます。
必要な値と関連データをすべてコピーし、安全な場所に保存してください。
これらの詳細は、今後の統合手順に不可欠です。そのため、許可された担当者のみがアクセスでき、組織のセキュリティポリシーに従って保護されていることを確認してください。

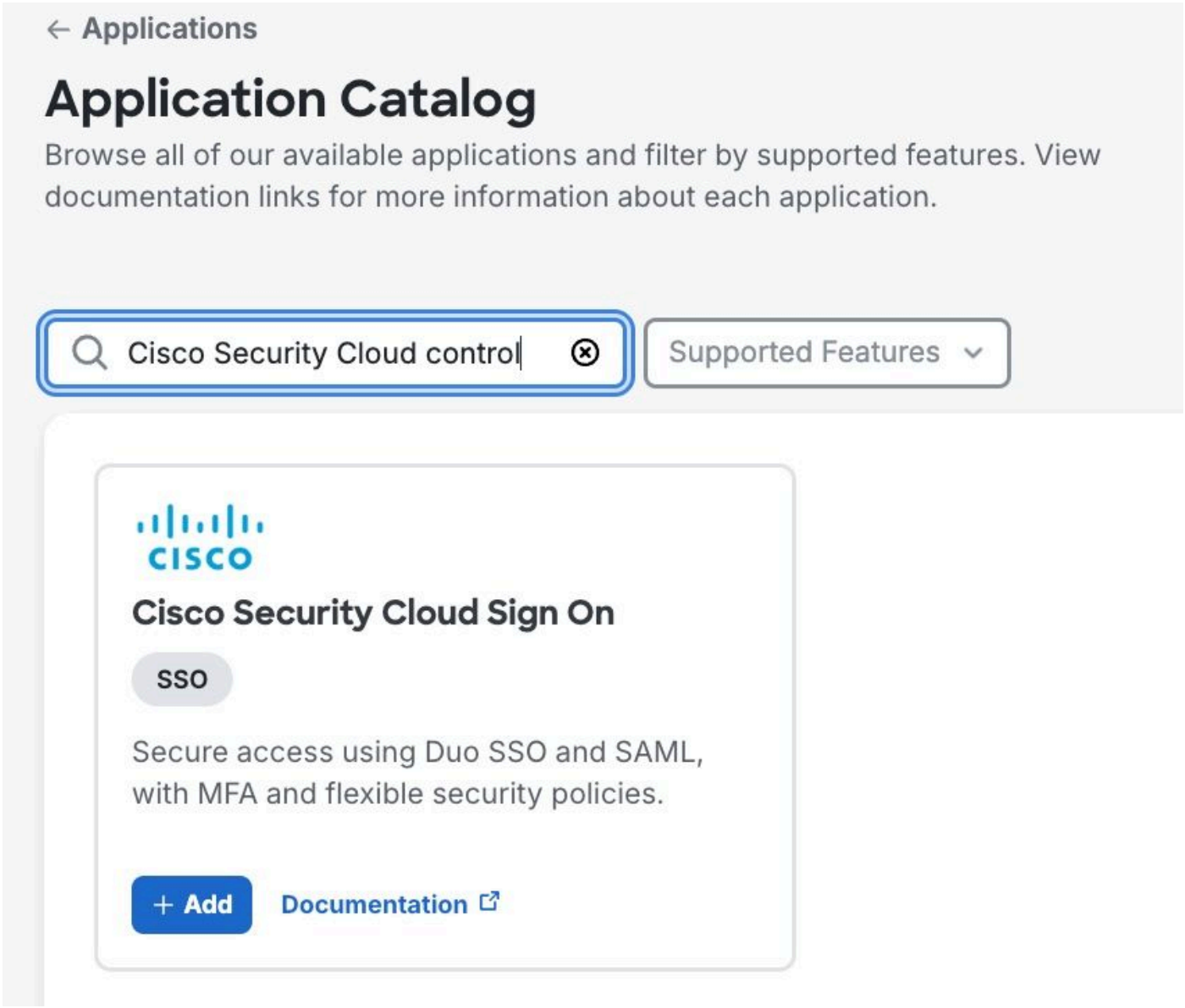


ステップ 4Cisco Duoを開き、Applicationsセクションに移動して、Add applicationをクリックします。



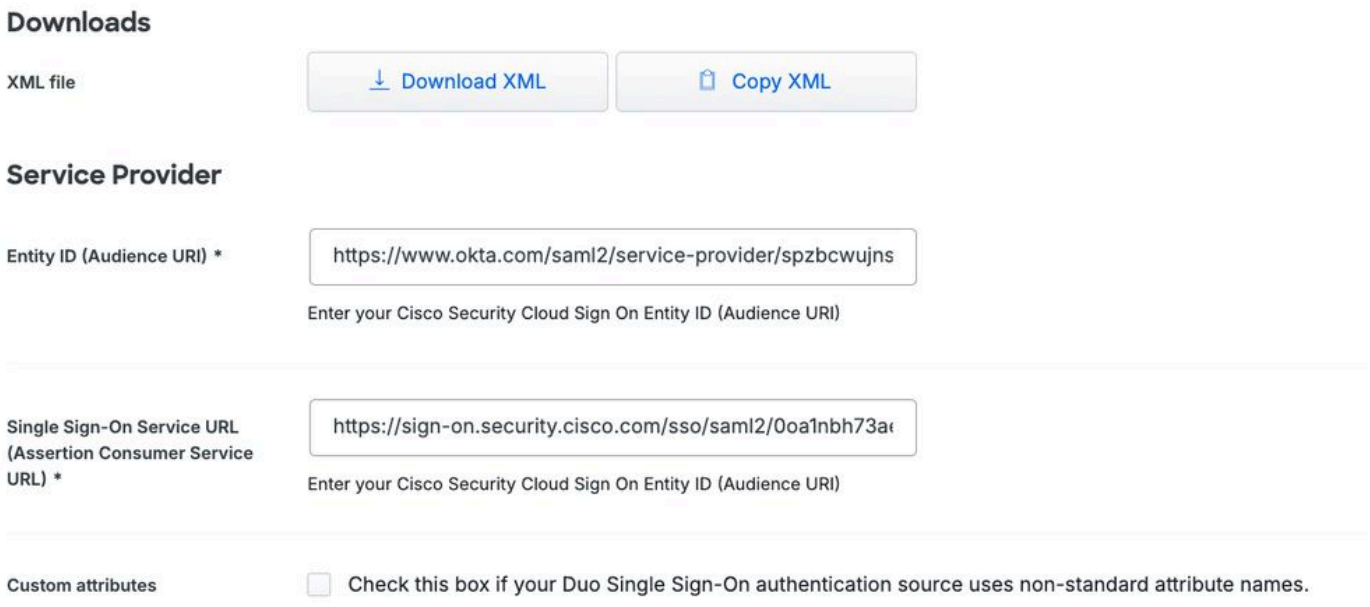
Cisco DUOアプリケーション

メニューでCisco Security Cloudを検索し、Addをクリックして統合を開始します。

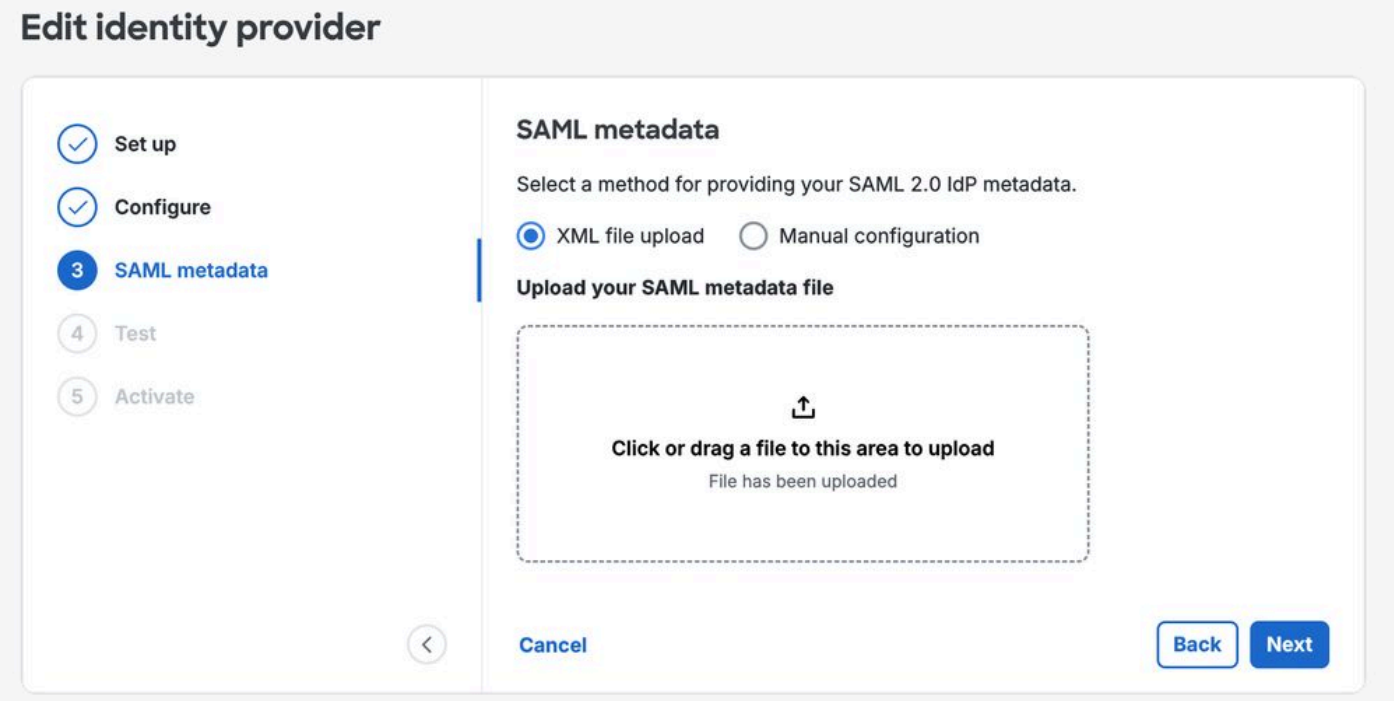


ステップ 5Cisco Duoアプリケーションで関連情報を設定します。

Cisco SCCからCisco Duoにエンティティ IDとシングルサインオンサービスURLをコピーします。



ステップ 6XMLをダウンロードし、Cisco SCCにファイルをアップロードします。



注:Cisco Duoコンソールからアプリケーションで設定できる残りのパラメータは、特定の要件に従って調整する必要があります。これらの各設定の詳細については、Cisco Duoの公式マニュアルを参照してください。設定可能なパラメータの例としては、割り当てられたアプリケーション名、ポリシーが適用されるユーザセット、組織のニーズに合わせてセキュリティ制御を調整できるその他のカスタマイズオプションなどがあります。

Cisco ETD用のCisco Duoでのポリシー設定

この段階ですべてのコンポーネントが接続されます。次に、Cisco ETDコンソール内で管理者の認証プロセスに適用されるポリシーを設定します。

この例では、特にIPアドレスに基づくアクセスコントロールに重点が置かれています。ただし、Cisco Duoには他にも多くのアクセスコントロールオプションがあります。

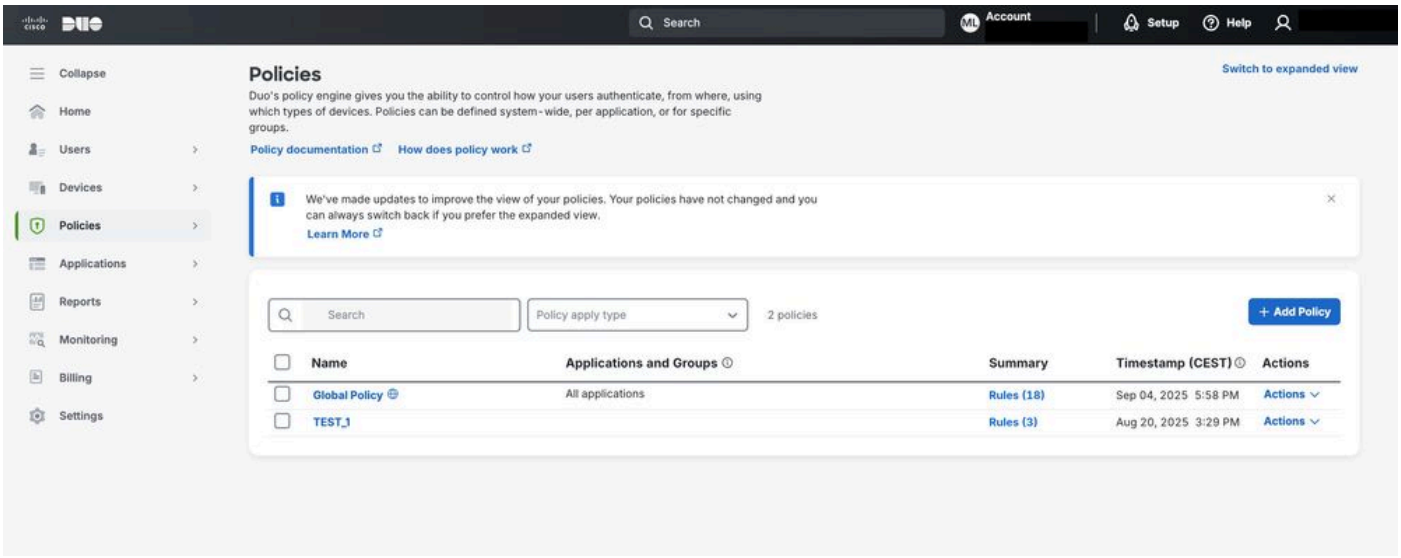
新しいポリシーを作成してアプリケーションに割り当てることにより、管理者ログインに対して必要な認証ルールとセキュリティ制限を適用できます。

Cisco Duoで使用可能なすべてのコントロールと設定オプションの詳細については、Cisco Duoの公式マニュアルを参照してください。

このリソースでは、セキュリティポリシーを最適化するための設定、カスタマイズ、およびベストプラクティスに関する包括的なガイダンスを提供します。

Cisco DuoでPoliciesセクションに移動すると、Cisco Duoを介してポリシーを作成し、Cisco ETD接続に割り当てることができます。

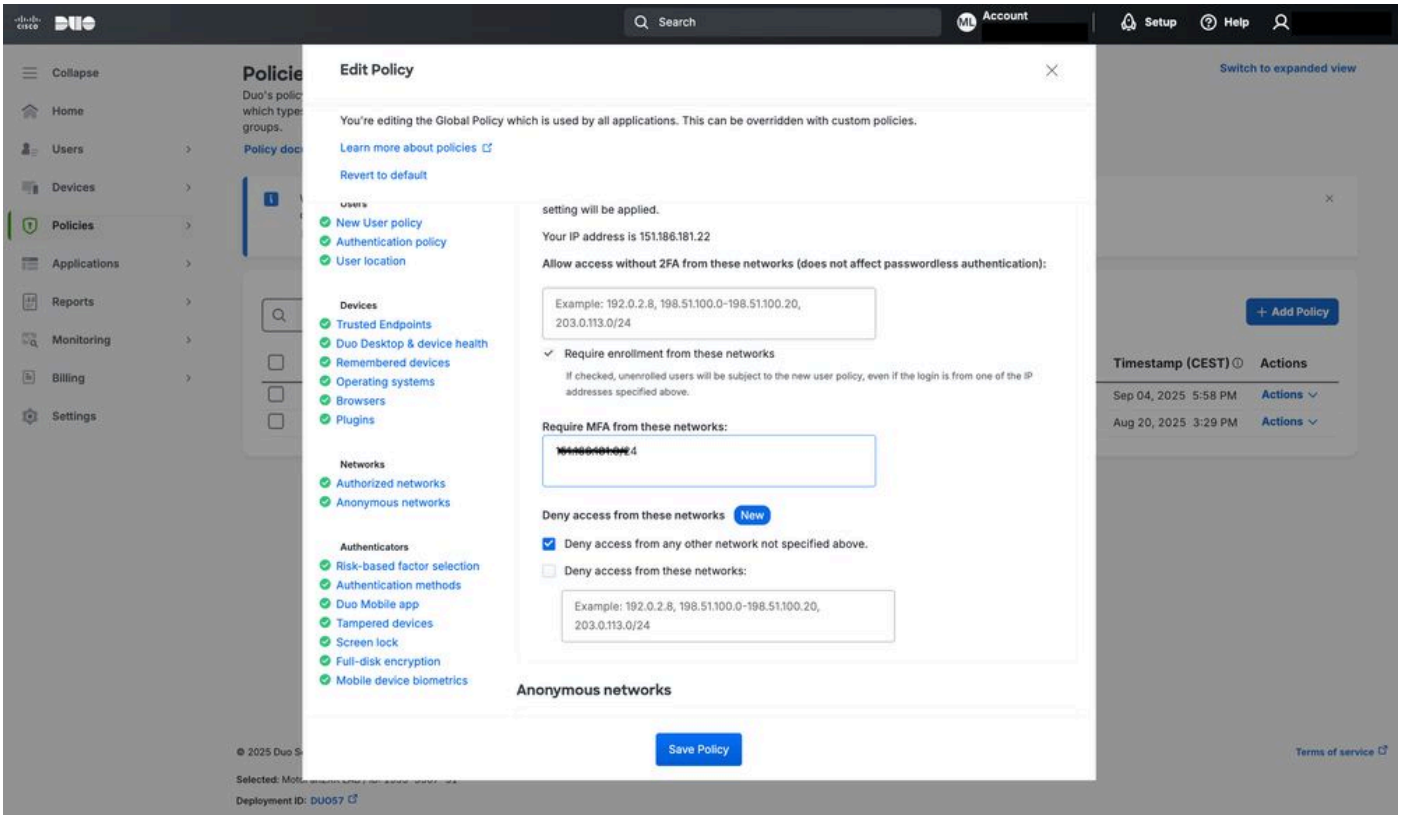
このポリシーは、アクセス要件に応じて、ユーザまたはグループごとに適用できます。



シスコDuo

この例では、図に示すように、送信元IPアクセスコントロールは、Authorized Networksセクションを設定することによって有効になります。

この設定では、指定された信頼できるIP範囲からのアクセスのみが許可され、Cisco ETDのセキュリティが強化されます。



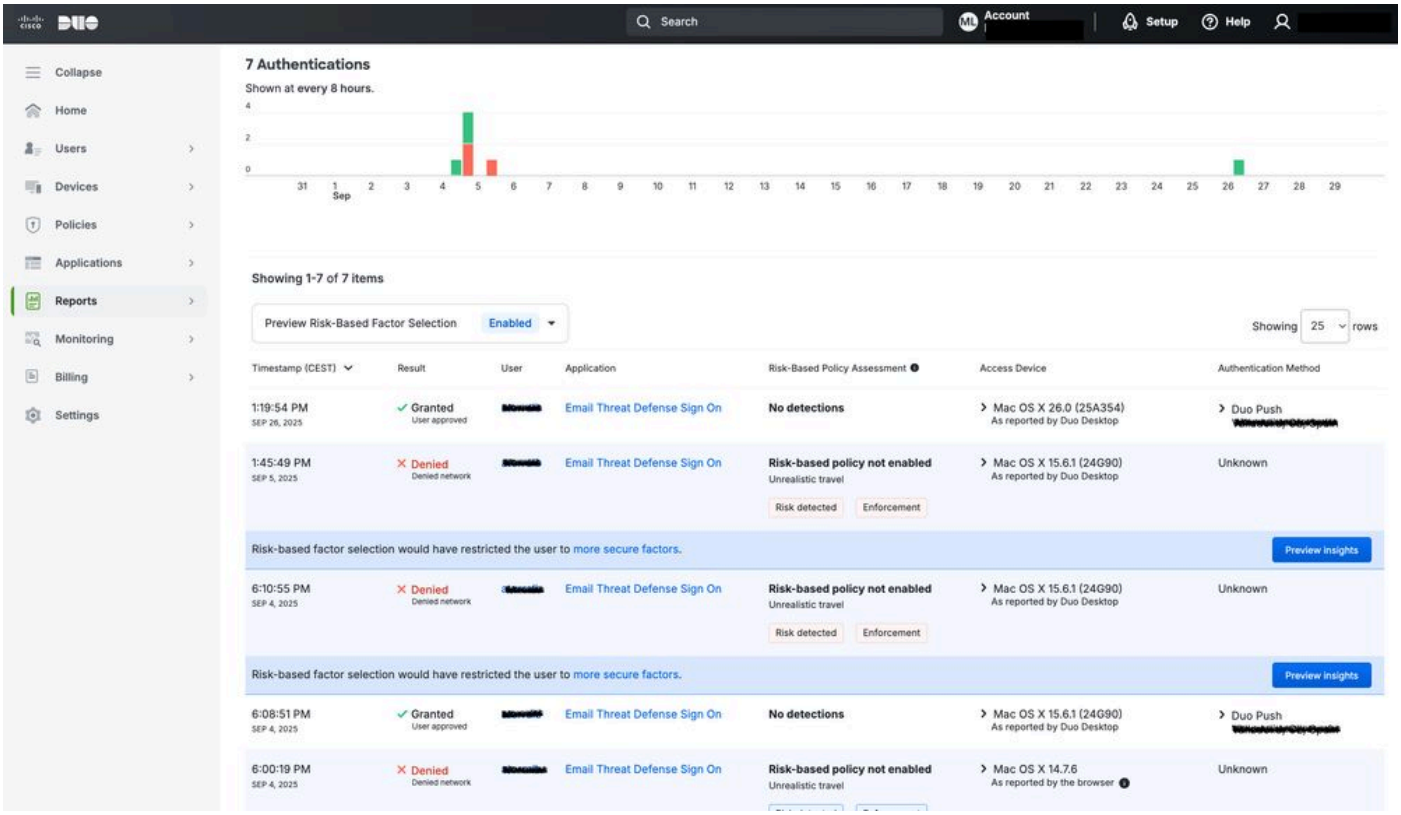
Cisco Duo Policyの設定

まとめ

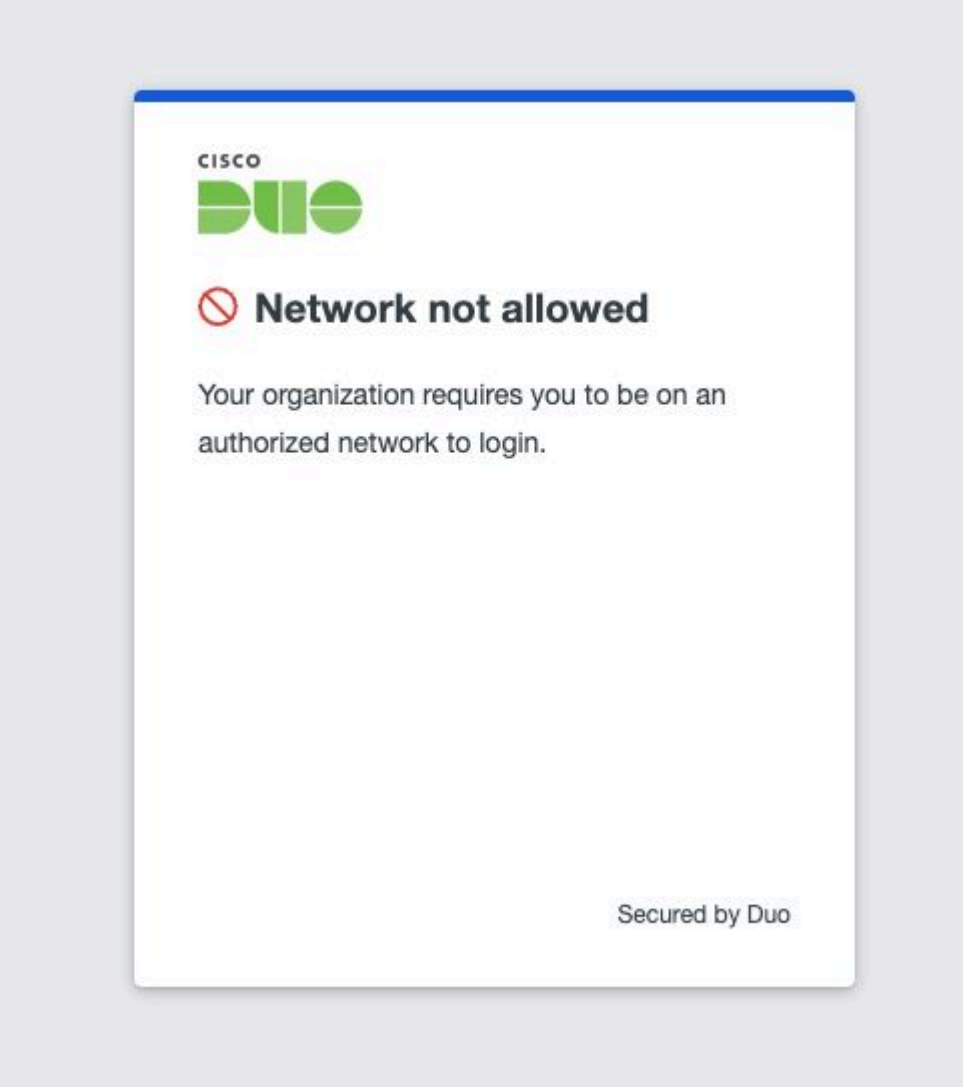
Cisco ETDは、MFAおよびアイデンティティプロバイダーとの統合を通じて管理者のアクセスを保護するための柔軟なオプションを提供します。
Cisco SCCとCisco Duoを組み合わせることで、組織はより強力な認証ポリシーを実装し、不正アクセスのリスクを軽減し、業界のベストプラクティスに合わせてセキュアなクラウドサービス管理を実現できます。

MFAに加えて、管理者はCisco Duoのポリシーベースの制御を活用して、送信元IPアドレスなどの特定の基準に基づいてアクセスを制限できます。たとえば、次の図に示すように、認可範囲外のIPアドレスからのアクセスの試みは、システムによって自動的にブロックされます。これにより、信頼できるネットワークから発信された要求だけが許可され、潜在的な攻撃に対する保護のレイヤが追加されます。

IPベースのアクセスコントロールをMFAとともに実装することで、組織は多層防御アプローチを実現できます。ID検証とネットワークロケーション検証を組み合わせて、クラウド内の重要な管理インターフェイスを保護します。



Cisco Duoレポート



ネットワーク制御結果

警告：この変更は、同じ認証ドメインを使用するすべてのアプリケーションに影響を与えることを理解しておくことが重要です。ETDだけでなく、Cisco Secure Accessコンソールへのアクセスなど、同じ認証プロセスに依存する他の製品にも影響を与えます。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。