Sicurezza e-mail Threat Defense: Autenticazione a più fattori e controlli degli accessi

Sommario

Introduzione

In questo documento vengono descritte le funzionalità che Cisco Email Threat Defense (ETD) offre per controllare l'accesso degli amministratori alla console di gestione.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di questi argomenti per configurare l'autenticazione ETD con Duo:

- Un abbonamento ETD Cisco
- Accesso a Cisco Security Cloud Control (SCC)
- Una soluzione di autenticazione per una sicurezza avanzata, in questo caso Cisco Duo.

Componenti usati

Il documento è limitato a Email Treat Defense e Secure Cloud Control.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

In questo documento viene illustrato come Cisco ETD utilizza Cisco SCC e si integra con Cisco Duo per garantire un'autenticazione sicura e un controllo granulare dell'accesso.

Nelle moderne soluzioni basate su cloud, il controllo dell'accesso è uno dei componenti più critici per garantire la sicurezza dei dati, la conformità alle normative e l'integrità operativa. Accesso non autorizzato, in particolare agli account dell'amministratore, può causare gravi conseguenze, ad esempio sistemi compromessi, perdite di dati e interruzioni del servizio.

Cisco offre solide funzionalità di sicurezza in tutto il suo portafoglio cloud, inclusa la tecnologia MFA (Multifactor Authentication), che è parte integrante di servizi come Cisco ETD. L'MFA aggiunge una fase di verifica critica al di là delle password tradizionali, richiedendo agli utenti di eseguire l'autenticazione tramite un fattore aggiuntivo, come l'approvazione di un'applicazione mobile, il token di sicurezza o la verifica biometrica.

Per semplificare e rafforzare il processo di autenticazione dell'amministratore, ETD sfrutta Cisco SCC, un servizio centralizzato di autenticazione e gestione delle policy.

Grazie a SCC, ETD può accedere a un'ampia gamma di funzioni di sicurezza, tra cui:

- Applicazione dell'MFA per ridurre i rischi di furto di credenziali.
- Integrazione con provider di identità di terze parti quali Cisco Duo, Microsoft Entra ID, Okta e altri per supportare flussi di lavoro di autenticazione flessibili e federazione delle identità aziendali.
- Amministrazione centralizzata delle policy, che consente l'applicazione di regole di accesso coerenti nei servizi cloud Cisco.

Cisco Duo, in particolare, estende queste funzionalità aggiungendo funzionalità avanzate di gestione degli accessi basate su policy. Utilizzando SCC come canale di integrazione, ETD può applicare direttamente i controlli granulari di Duo, come le restrizioni IP di origine, i controlli di integrità dei dispositivi e le regole basate sui gruppi di utenti per l'accesso dell'amministratore.

Ad esempio, le organizzazioni possono definire un criterio che consente l'accesso solo da intervalli di rete attendibili specifici. Tutti i tentativi di connessione eseguiti al di fuori dell'elenco di indirizzi IP autorizzati possono essere bloccati automaticamente, come mostrato negli schemi allegati. Questa combinazione di politiche contestuali di AMF + consente un approccio di difesa approfondito, garantendo che, anche se le credenziali sono compromesse, agli aggressori sia ancora impedito l'accesso al sistema a meno che non soddisfino anche criteri di sicurezza aggiuntivi.

Unendo Cisco ETD, Cisco SCC e Cisco Duo, le aziende possono implementare un modello di controllo dell'accesso sicuro, scalabile e di facile utilizzo, in linea con le best practice del settore, migliorando al contempo la protezione dei servizi cloud critici.

Scenari

Con ETD è possibile implementare diversi scenari di autenticazione e controllo dell'accesso per garantire l'accesso amministrativo:

1. MFA integrata: utilizzare la MFA integrata di Cisco o integrare la MFA Microsoft.
2. Cisco SCC con Cisco Duo - Combina l'autenticazione centralizzata di Cisco SCC con le funzionalità MFA avanzate di Duo.
3. Cisco SCC con un provider di identità esterno (ad esempio, Microsoft Entra ID): estensione dei criteri di autenticazione tramite l'integrazione con soluzioni di identità aziendali.

In questo documento viene descritta la procedura di configurazione per lo scenario 2: Cisco SCC con Cisco Duo, anche se il processo può essere adattato per altre tecnologie.

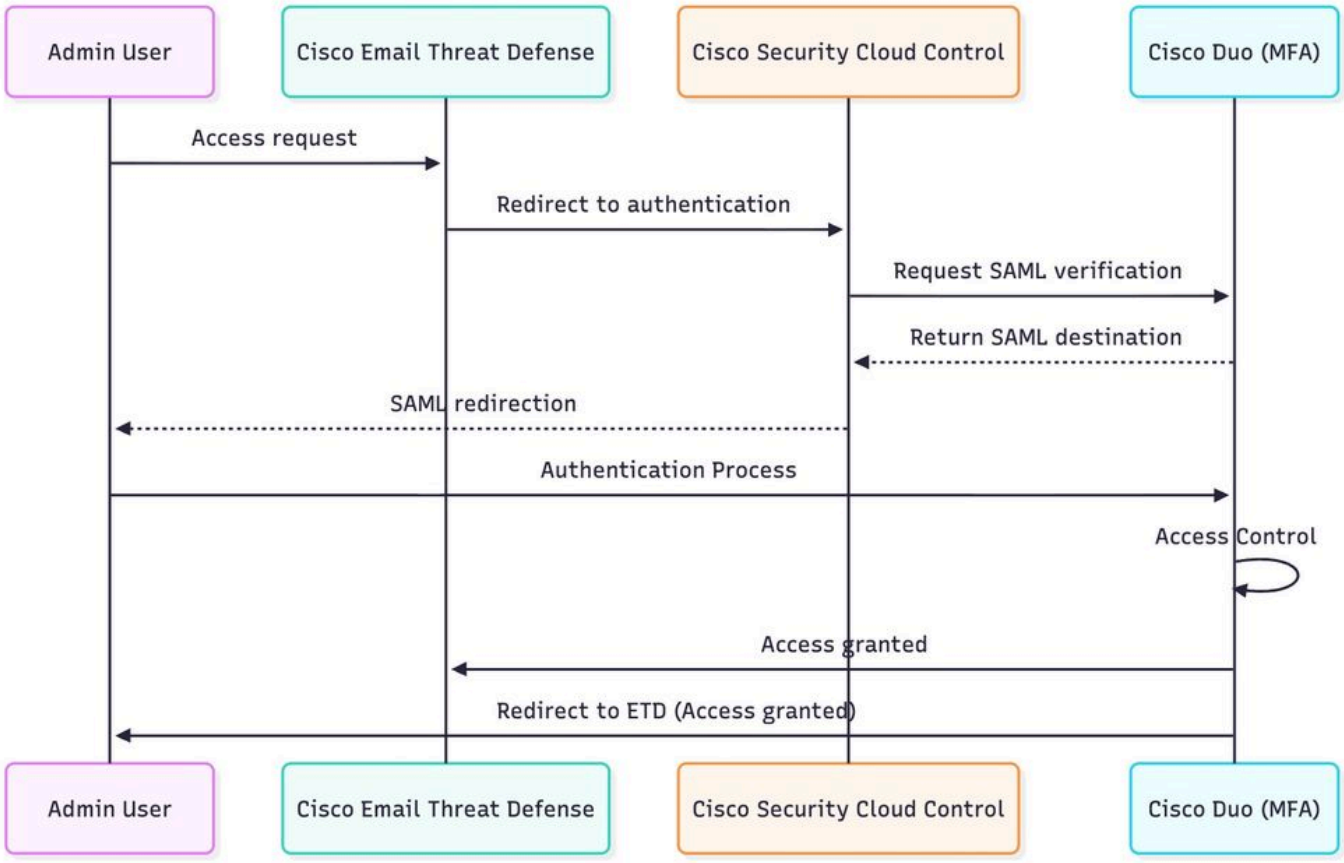
Nota: Questo documento offre una panoramica dei passaggi di base necessari per abilitare il controllo dell'accesso in Email Threat Defense (ETD) utilizzando le funzionalità di autenticazione a più fattori di Cisco Duo. L'implementazione dell'integrazione Duo consente di migliorare la sicurezza garantendo che solo gli utenti autorizzati possano accedere alla piattaforma. Per una guida completa, le opzioni di configurazione e gli scenari di distribuzione avanzati, fare riferimento alla documentazione ufficiale del prodotto:

- per la gestione centralizzata delle policy di sicurezza e degli accessi.

Cisco Duo: per istruzioni dettagliate sulla configurazione dell'autenticazione a più fattori e sulle best practice.

Cisco SCC Configuration

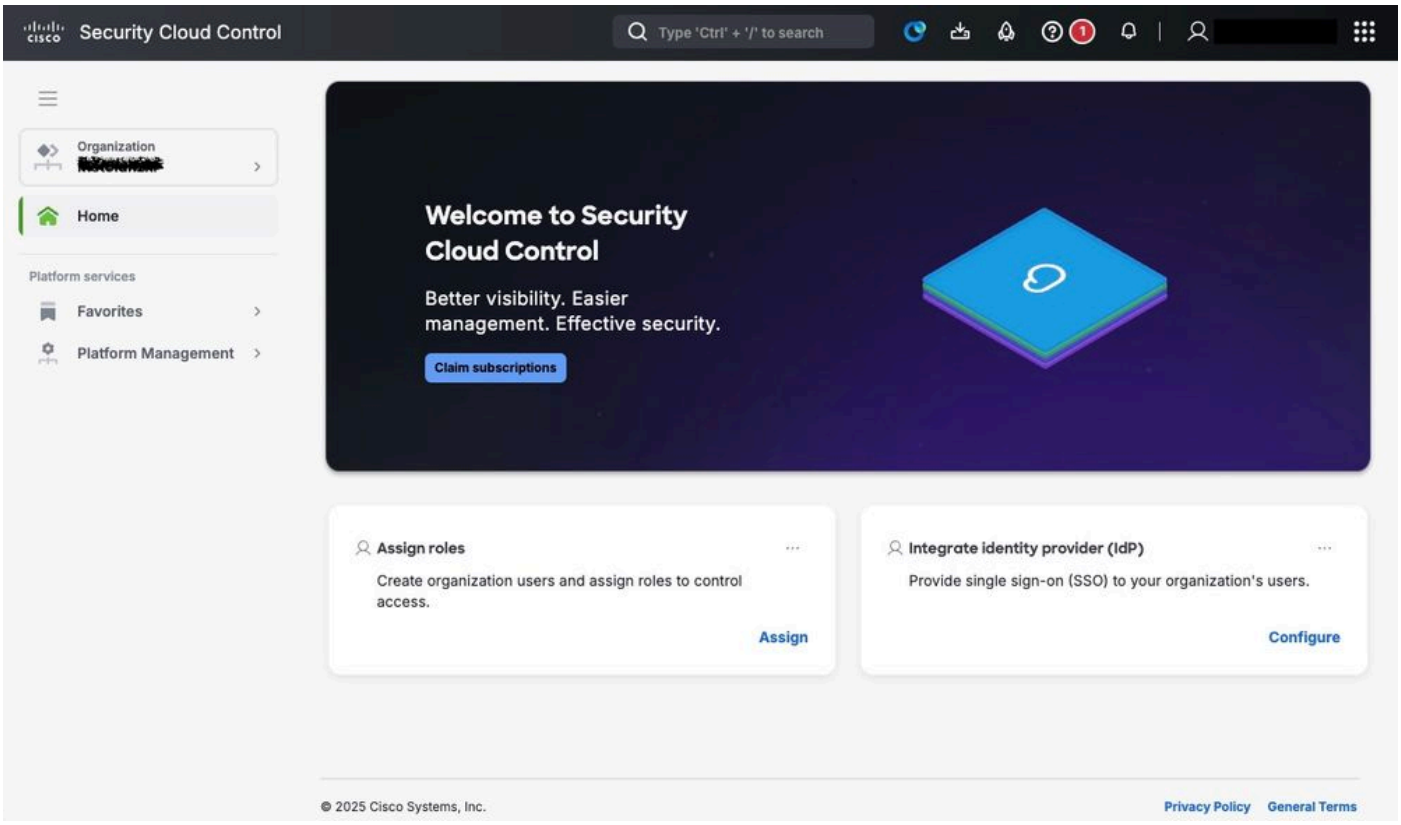
Per integrare Cisco ETD con Cisco Duo, il primo passaggio è configurare il dominio di autenticazione in Cisco SCC. Questo stabilisce la relazione di trust che consente a Cisco SCC di lavorare con identità esterne e fornitori MFA.



Diagramma

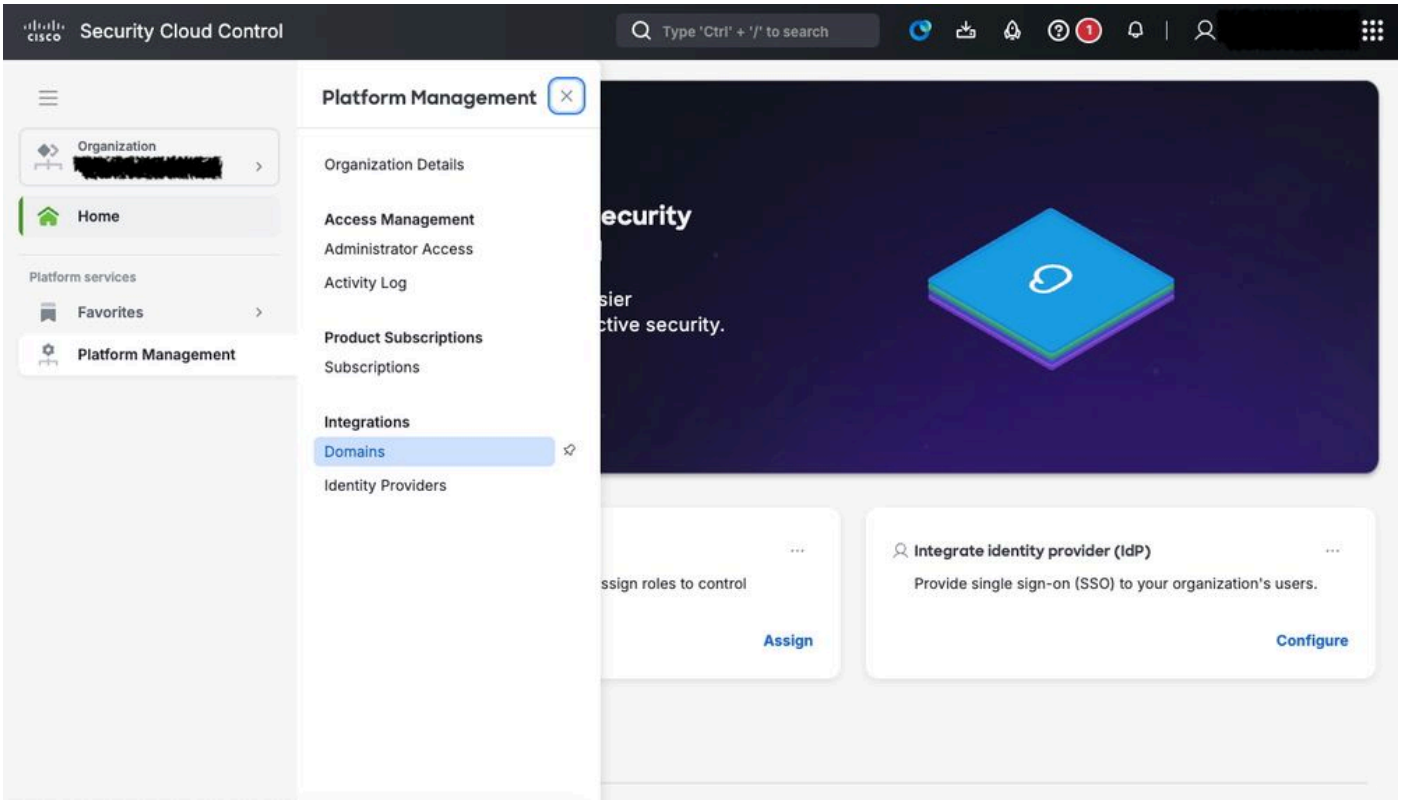
Passaggio 1. Accedere a Cisco SCC Console.

Accedere al portale Cisco SCC all'indirizzo https://security.cisco.com/.



Passaggio 2. Passare a Gestione dominio.

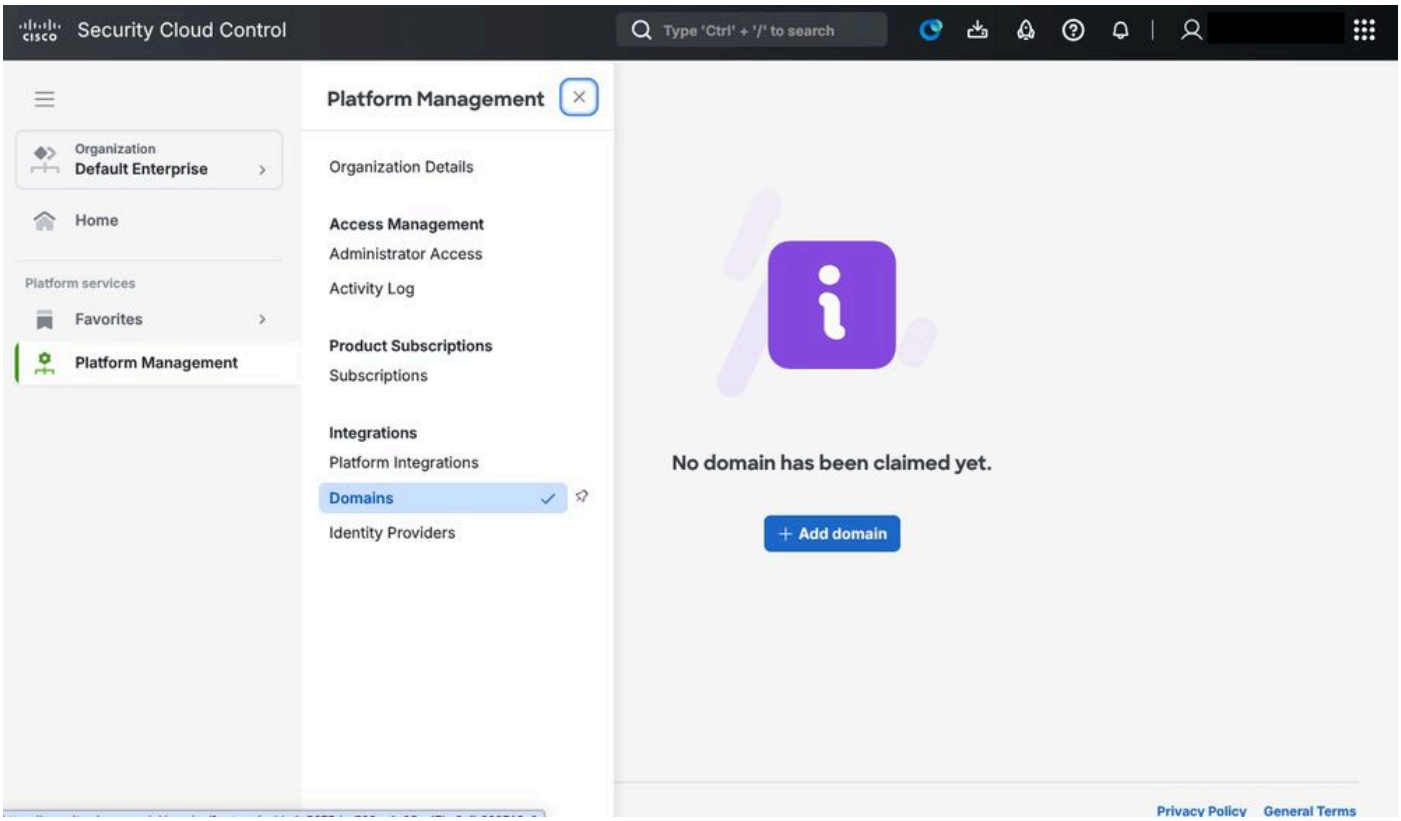
Dal menu principale, passare a Gestione piattaforma > Domini.



Configurazione Secure Cloud Control Domain

Passaggio 3. Aggiungere un nuovo dominio.

Fare clic su Add Domain (Aggiungi dominio) per avviare il processo di registrazione del dominio di autenticazione.

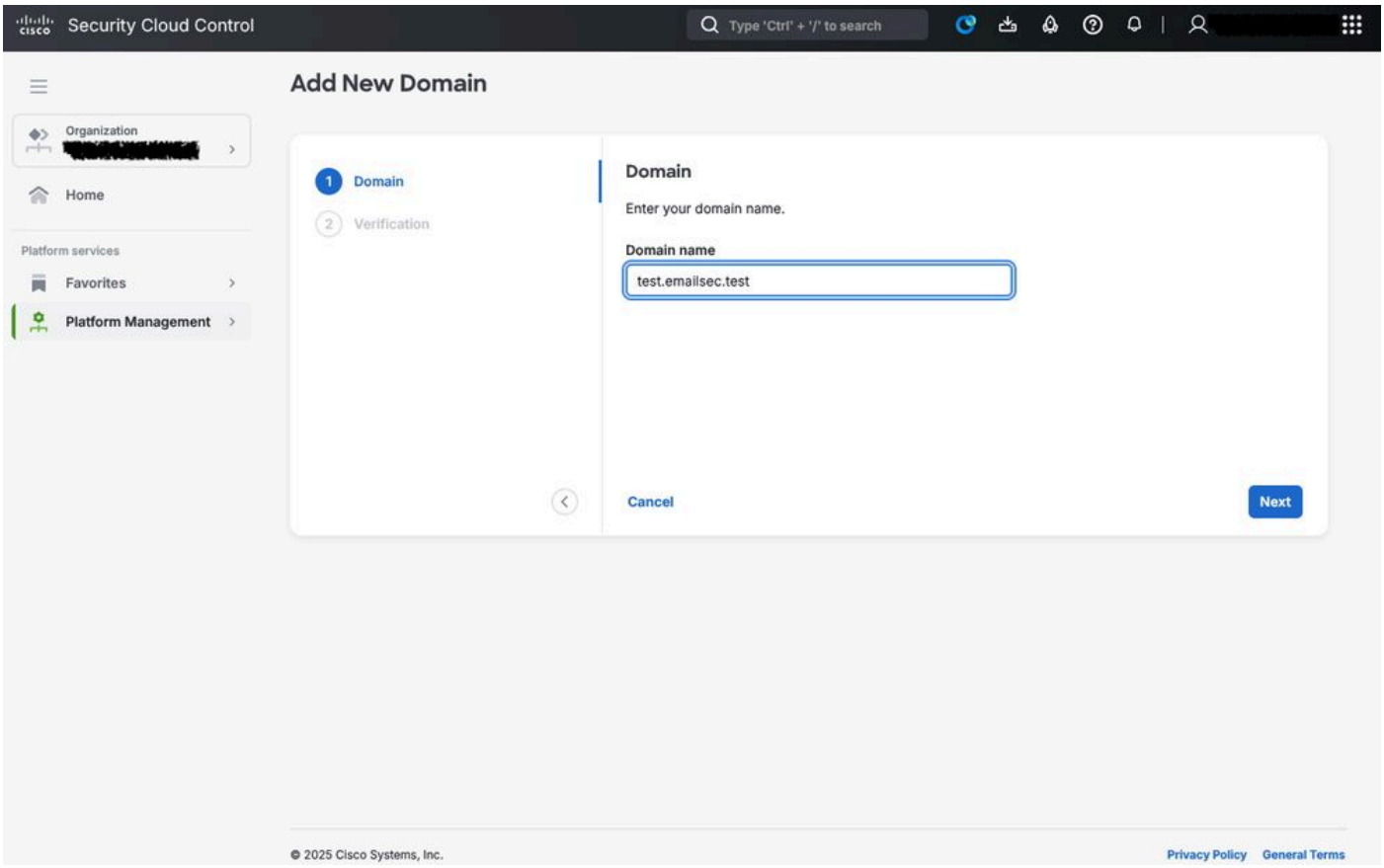


Controllo Security Cloud: Dominio

Passaggio 4. Fornire le informazioni sul dominio.

Completare il modulo con i dettagli del dominio utilizzato per l'autenticazione. Ciò include in genere:

- Il nome del dominio (ad esempio, test.emailsec.test)
- Informazioni di contatto (amministrative e tecniche)
- Parametri di autenticazione, a seconda del provider di identità scelto



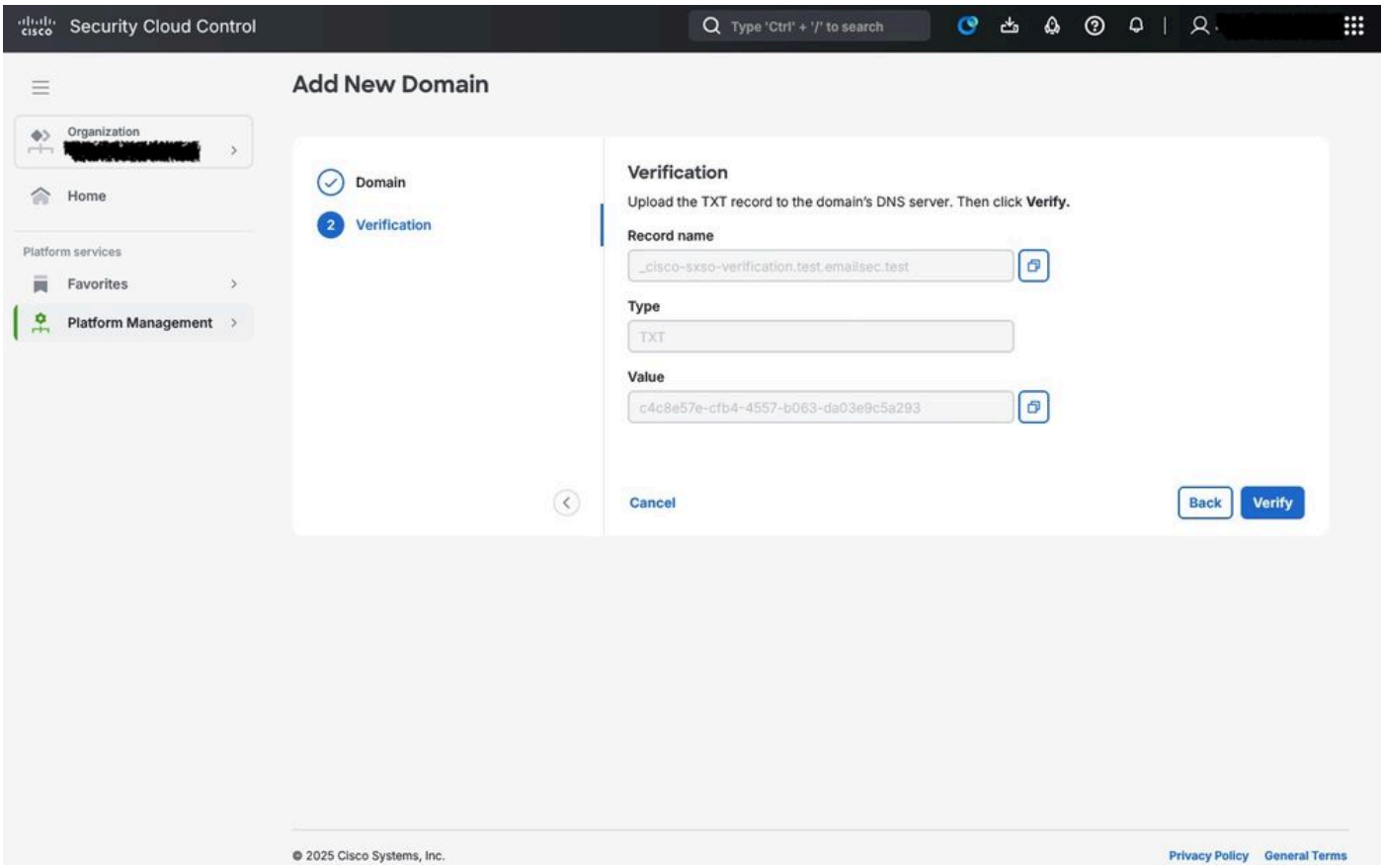
Passaggio 5. Verifica del dominio tramite DNS.

Dopo la registrazione del dominio, Cisco richiede una prova della proprietà.

- CSCC fornisce un record di verifica
- Questo record deve essere aggiunto alla configurazione DNS del dominio (in genere come record TXT)
- Cisco Secure Cloud convalida automaticamente la voce DNS per confermare che il dominio appartiene alla tua organizzazione

---

⚠ Attenzione: Il processo di verifica deve essere completato correttamente prima di poter procedere con l'integrazione. A seconda della propagazione DNS, la convalida richiede da alcuni minuti a alcune ore.



Collegamento di ETD a Cisco Duo tramite Cisco SCC

Una volta configurato correttamente il dominio dell'amministratore (che funge da base per l'applicazione di controlli di accesso e privilegi di gestione più rigorosi), il passo successivo consiste nell'integrare il servizio MFA sotto contratto.

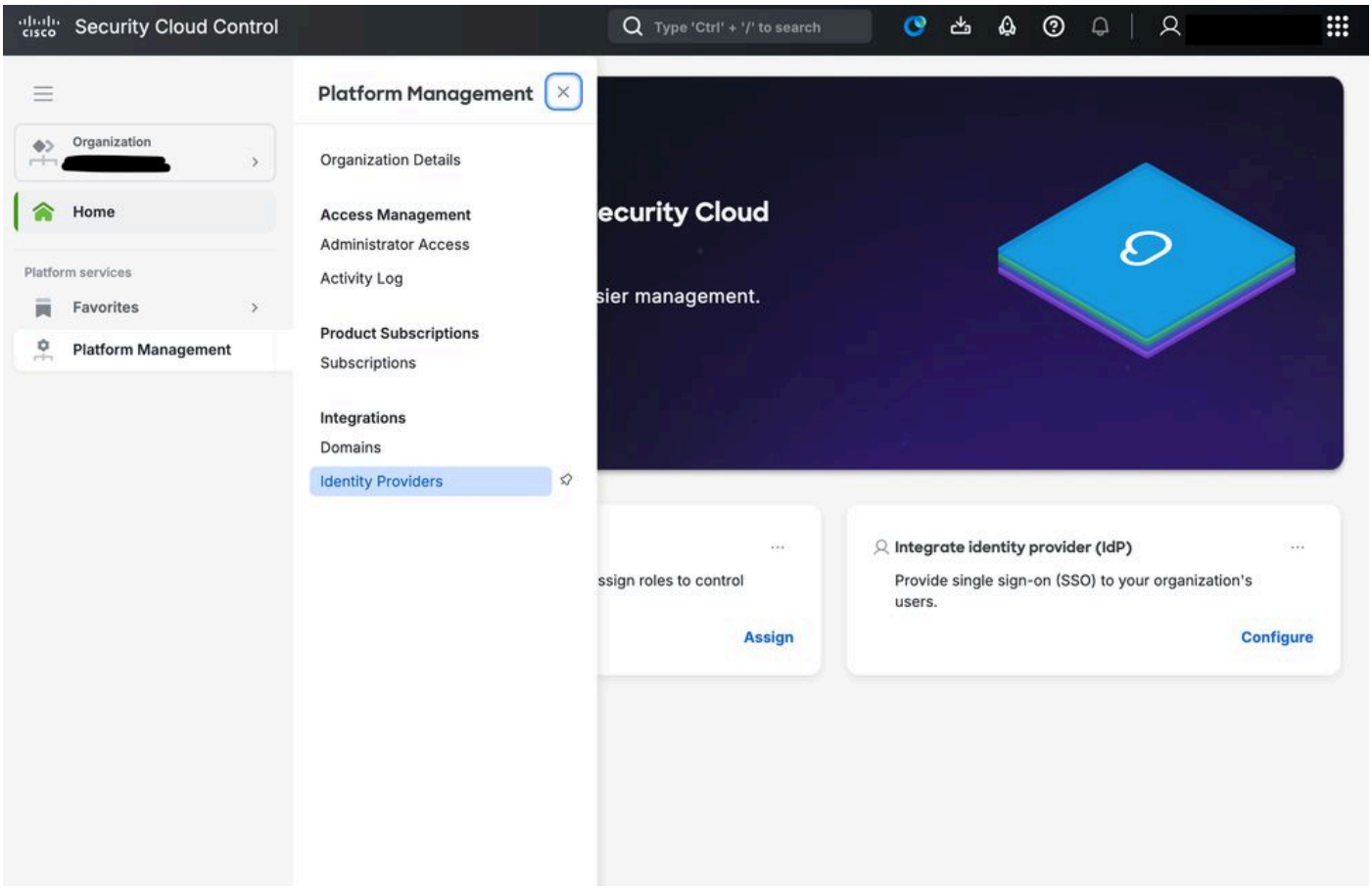
In questo scenario, Cisco Duo viene implementato come soluzione principale per il controllo degli accessi, l'accesso sicuro e la verifica MFA. Questa integrazione migliora la postura di sicurezza dell'ambiente richiedendo agli amministratori di autenticare la propria identità attraverso più passaggi di verifica, riducendo il rischio di accesso non autorizzato e garantendo la conformità alle policy di sicurezza aziendali.

CISCO Duo e Cisco Cloud Control Integration

Passaggio 1. Accesso alla Cisco SCC Console.

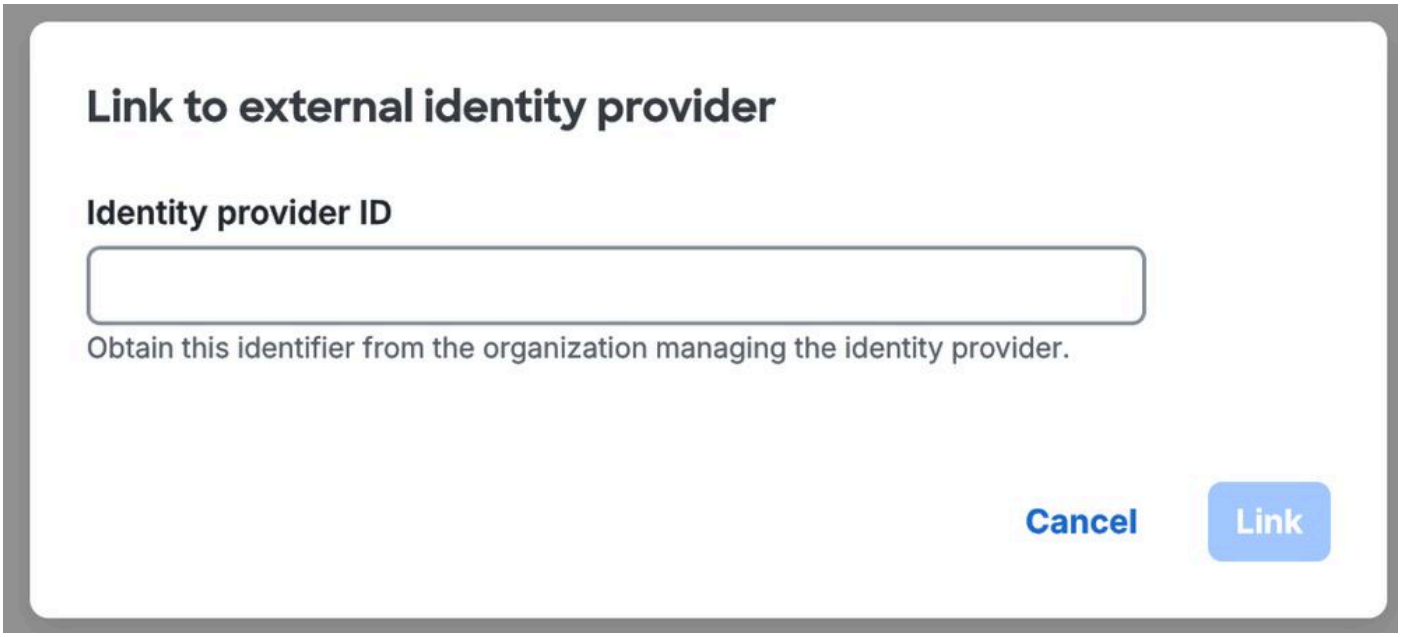
Accedere al portale Cisco Security Cloud Control https://security.cisco.com/.

Passare a Gestione piattaforma e fare clic su Provider di identità.



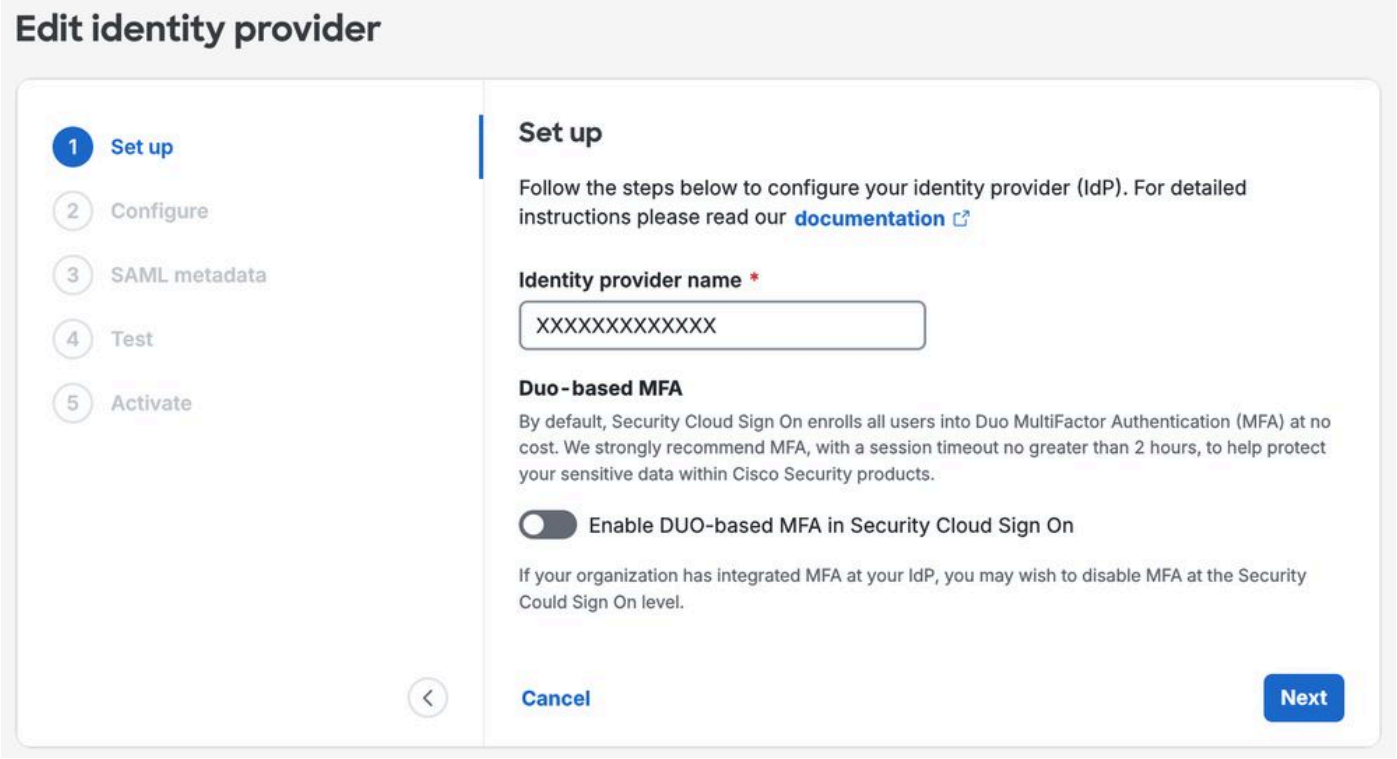
Configurazione IDP SCC

Utilizzare un nome personalizzato per identificare il provider di identità.



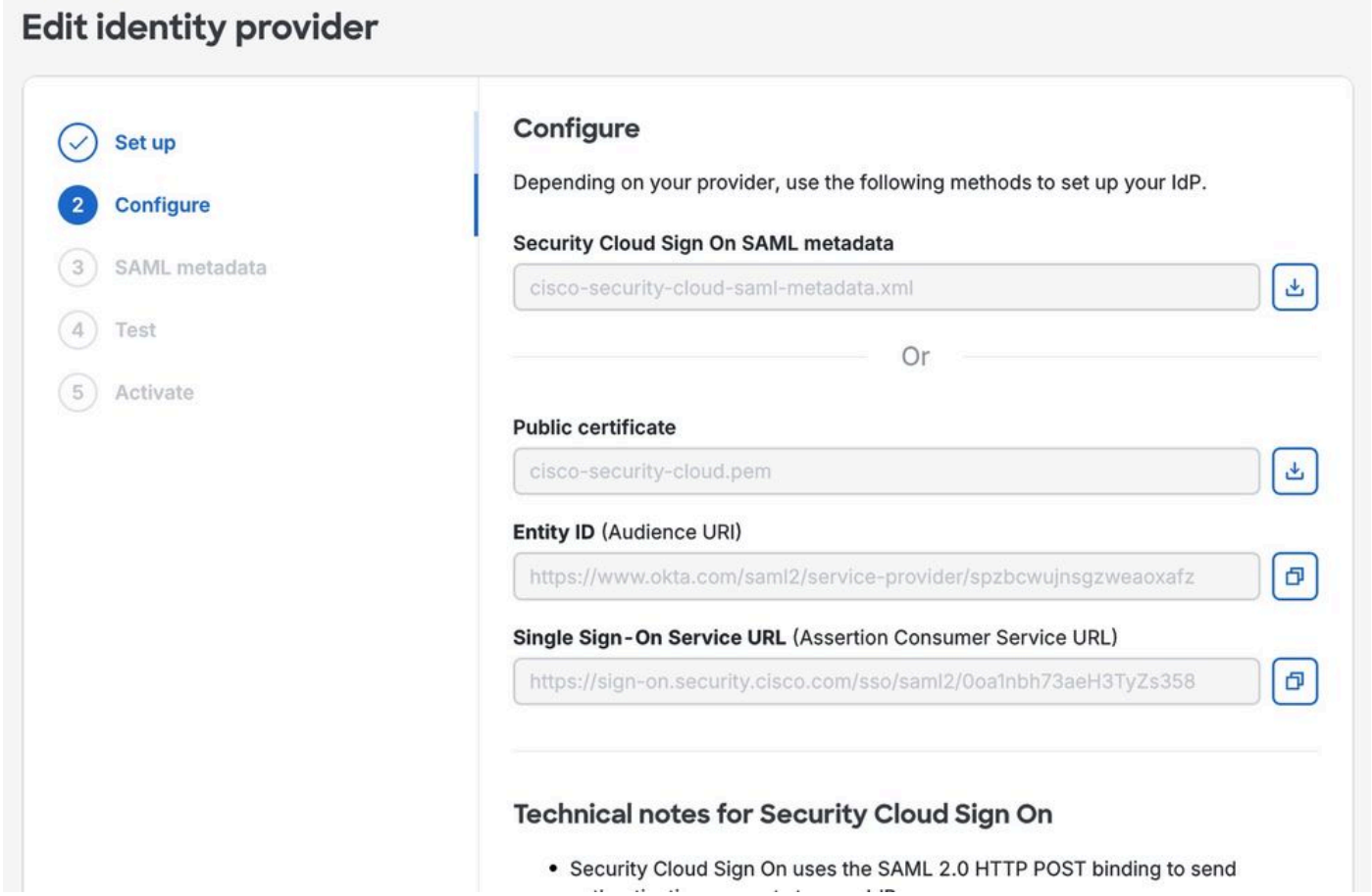
A questo punto viene avviata l'installazione. In questo momento, è possibile accedere a Cisco SCC e Cisco Duo.

Passaggio 2. In SCC, disabilitare l'abilitazione dell'autenticazione a più fattori basata su DUO in Security Cloud Sing On, come mostrato nella figura, e fare clic su Avanti.

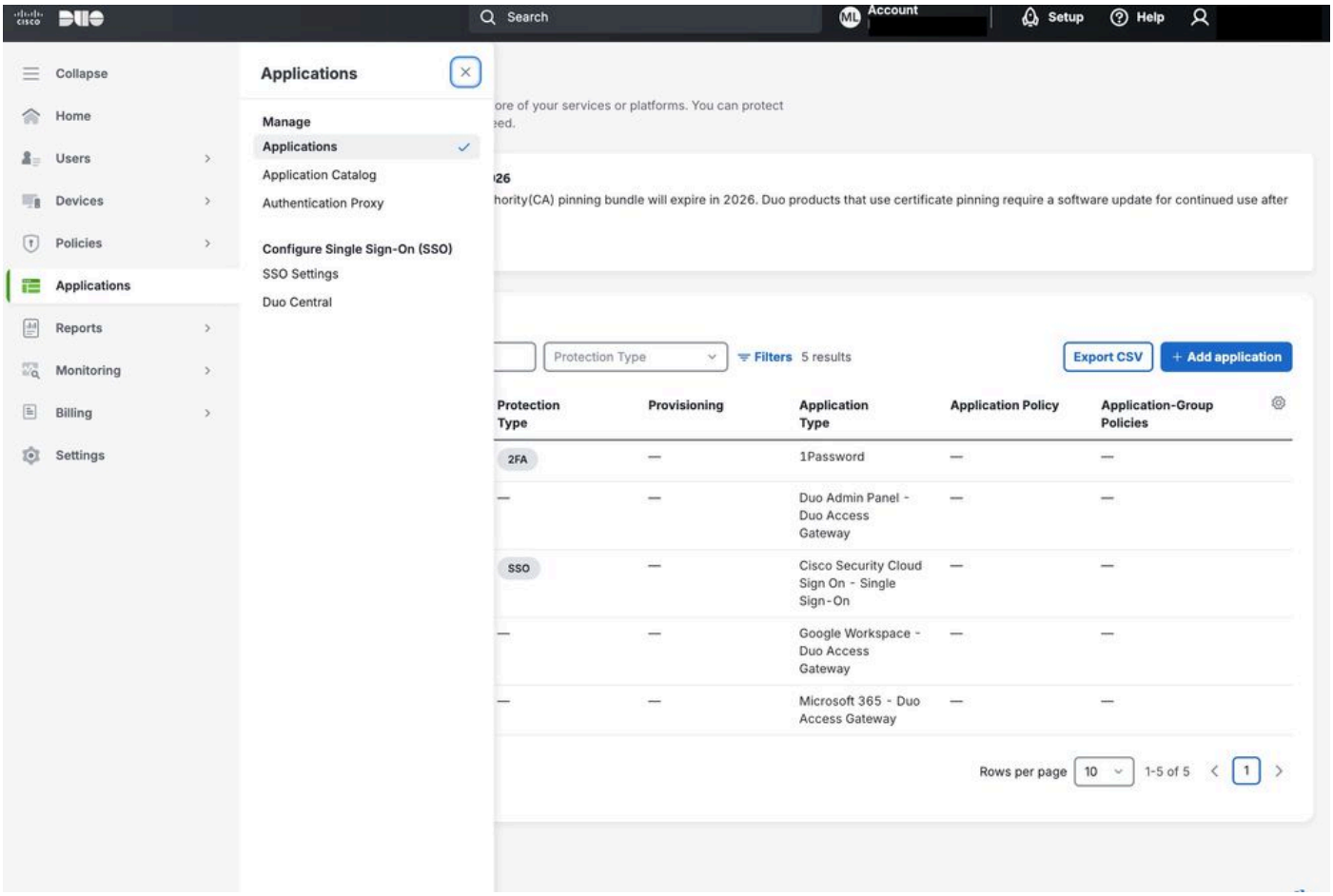


Configurazione provider di identità

Passaggio 3. I dati pertinenti vengono creati e utilizzati durante la configurazione di Cisco Duo. Assicurarsi di copiare tutti i valori richiesti e i dati associati e di archiviarli in un percorso sicuro. Questi dettagli sono essenziali per le future fasi di integrazione, in modo da garantire che siano accessibili solo al personale autorizzato e protetti in conformità con le politiche di sicurezza della vostra organizzazione.

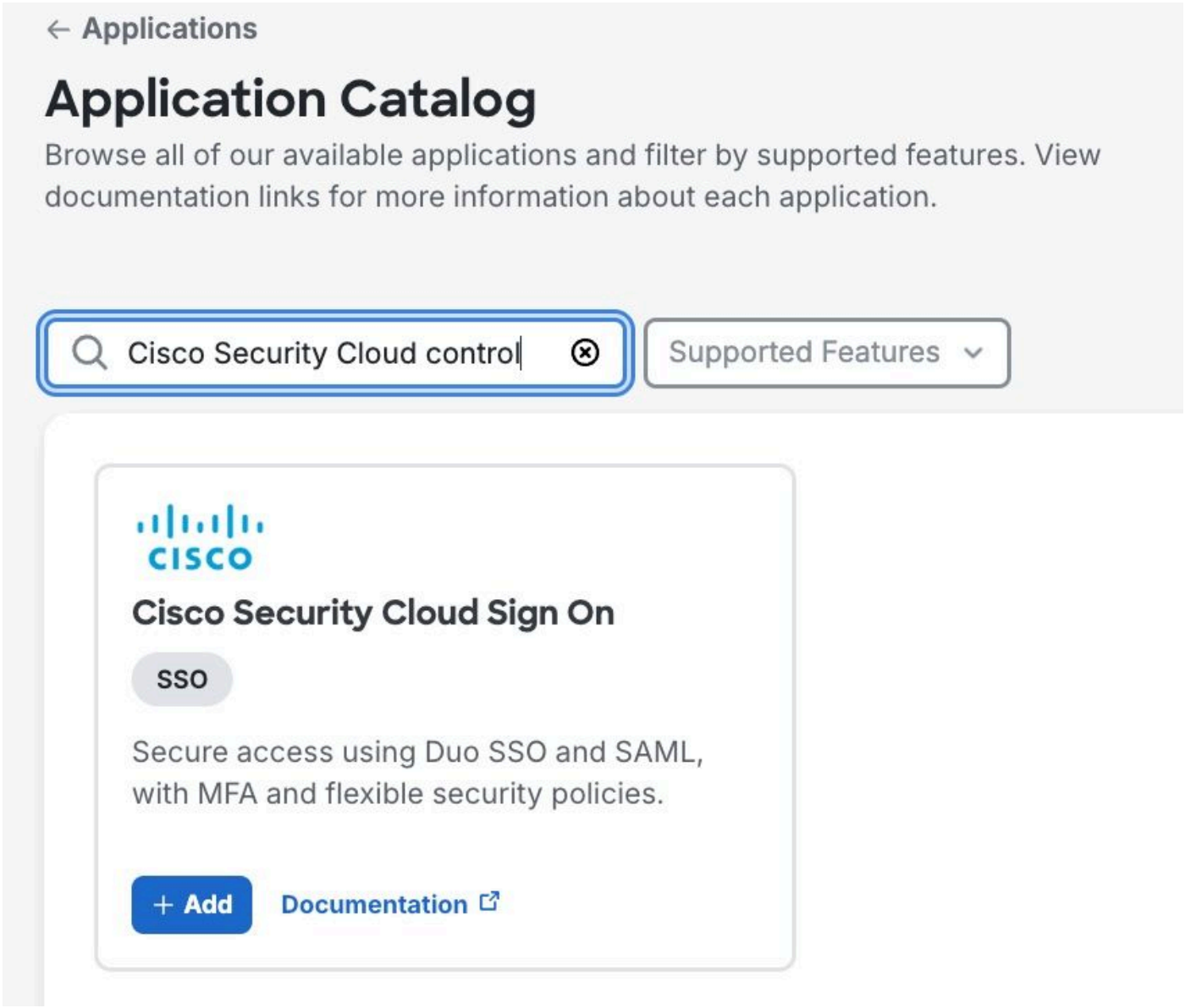


Passaggio 4. Aprire Cisco Duo, passare alla sezione Applicazioni e fare clic su Aggiungi applicazione.



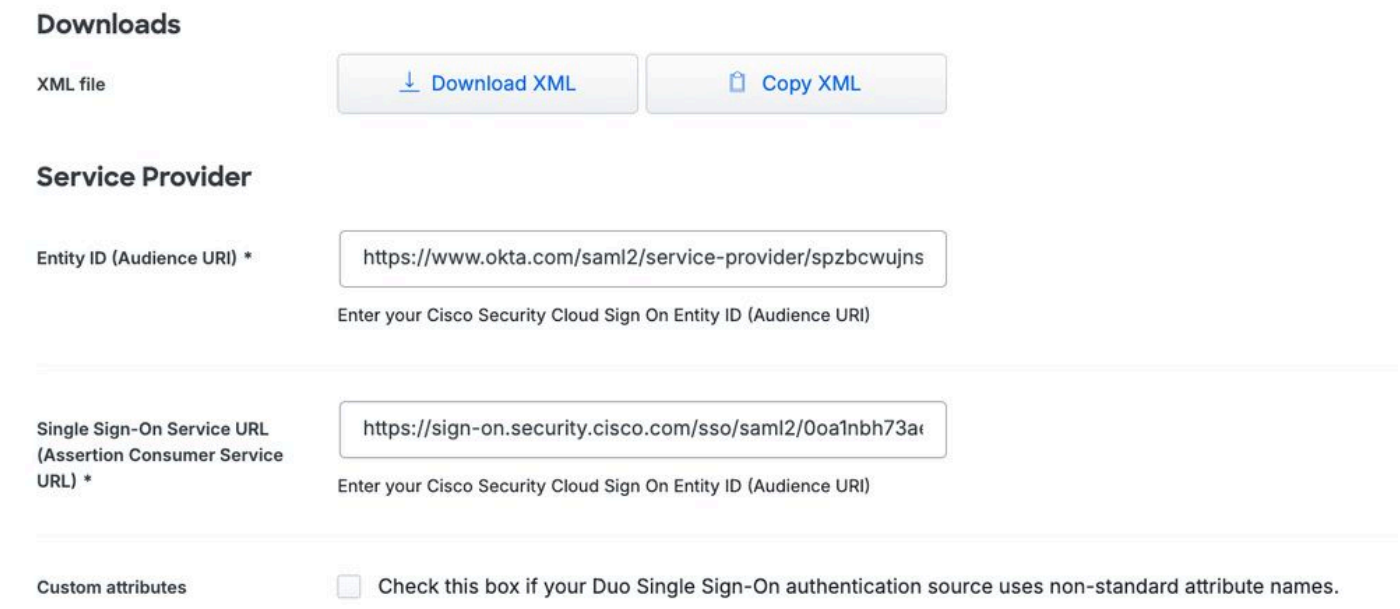
Applicazioni Cisco DUO

Nel menu, cercare Cisco Security Cloud e fare clic su Add (Aggiungi) per avviare l'integrazione.

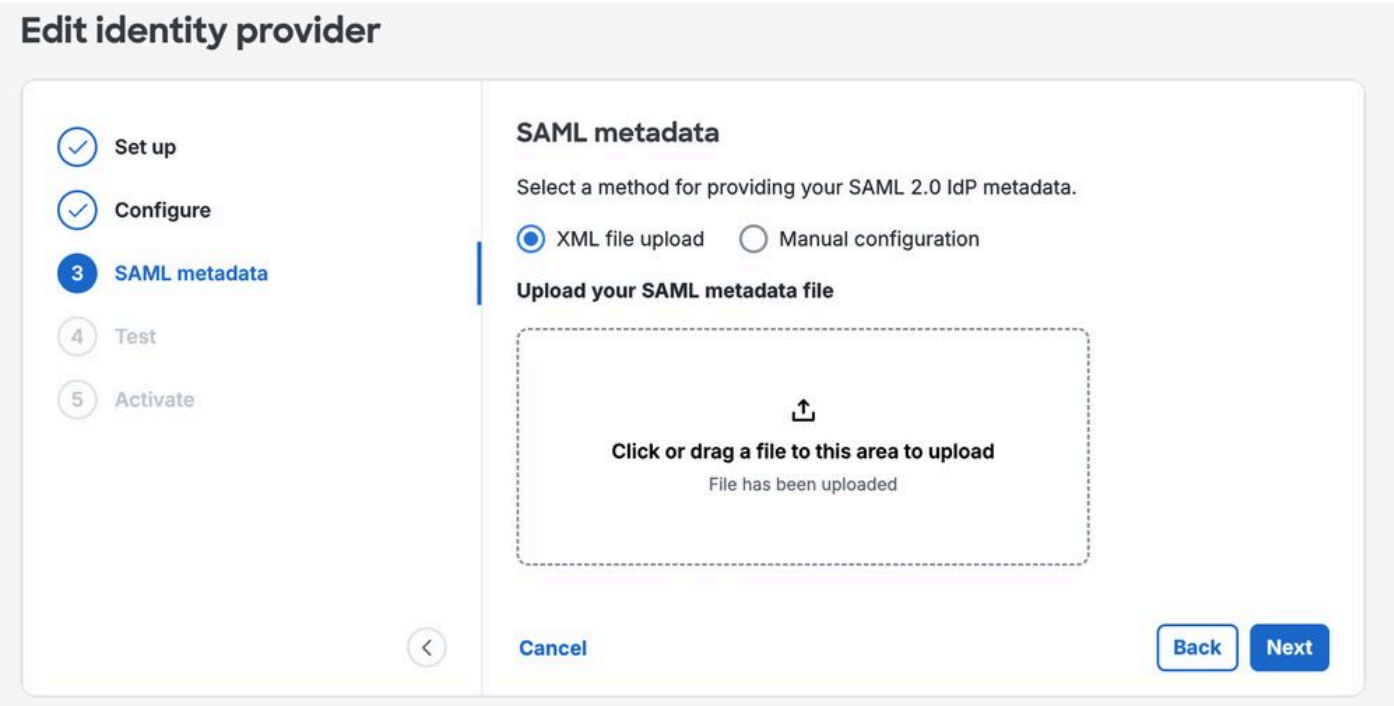


Passaggio 5. Configurare le informazioni pertinenti nell'applicazione Cisco Duo.

Copiare l'ID entità e l'URL del servizio Single Sign-On da Cisco SCC a Cisco Duo.



Passaggio 6. Scaricare l'XML e caricare il file in Cisco SCC.



Nota: Gli altri parametri che possono essere configurati nell'applicazione dalla console Cisco Duo devono essere regolati in base ai requisiti specifici dell'utente. Per una spiegazione dettagliata di ciascuna di queste impostazioni, consultare la documentazione ufficiale di Cisco Duo. Esempi di parametri configurabili includono il nome dell'applicazione assegnato, l'insieme di utenti a cui si applica il criterio e altre opzioni di personalizzazione che possono personalizzare i controlli di sicurezza per soddisfare le esigenze dell'organizzazione.

Configurazione dei criteri in Cisco Duo per Cisco ETD

In questa fase, tutti i componenti sono connessi e il passaggio successivo è configurare una policy da applicare al processo di autenticazione dell'amministratore nella console ETD di Cisco.

Nell'esempio, l'attenzione è focalizzata specificamente sul controllo dell'accesso basato sull'indirizzo IP. Tuttavia, Cisco Duo offre molte altre opzioni di controllo dell'accesso.

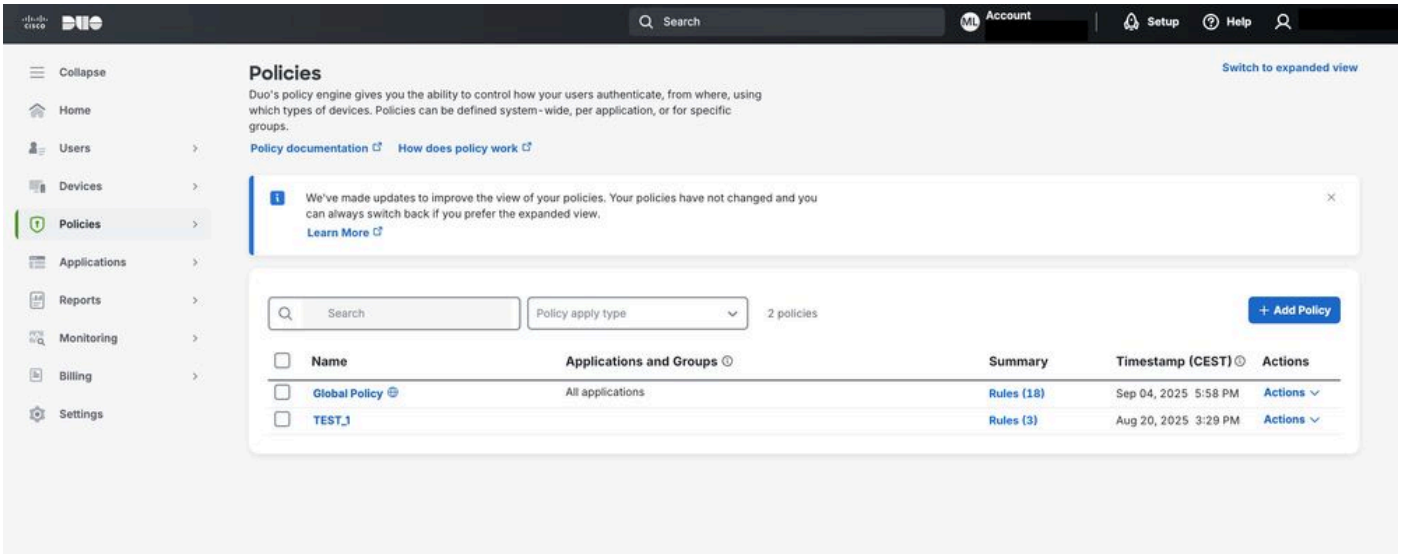
È possibile creare un nuovo criterio e assegnarlo all'applicazione, consentendo l'applicazione delle regole di autenticazione desiderate e delle restrizioni di sicurezza per gli accessi dell'amministratore.

Per informazioni più dettagliate su tutti i controlli e le opzioni di configurazione disponibili in Cisco Duo, consultare la documentazione ufficiale di Cisco Duo.

Questa risorsa fornisce una guida completa sull'installazione, la personalizzazione e le procedure ottimali per ottimizzare le policy di sicurezza.

Passando alla sezione Criteri di Cisco Duo, è possibile creare un criterio e assegnarlo alla connessione ETD di Cisco tramite Cisco Duo.

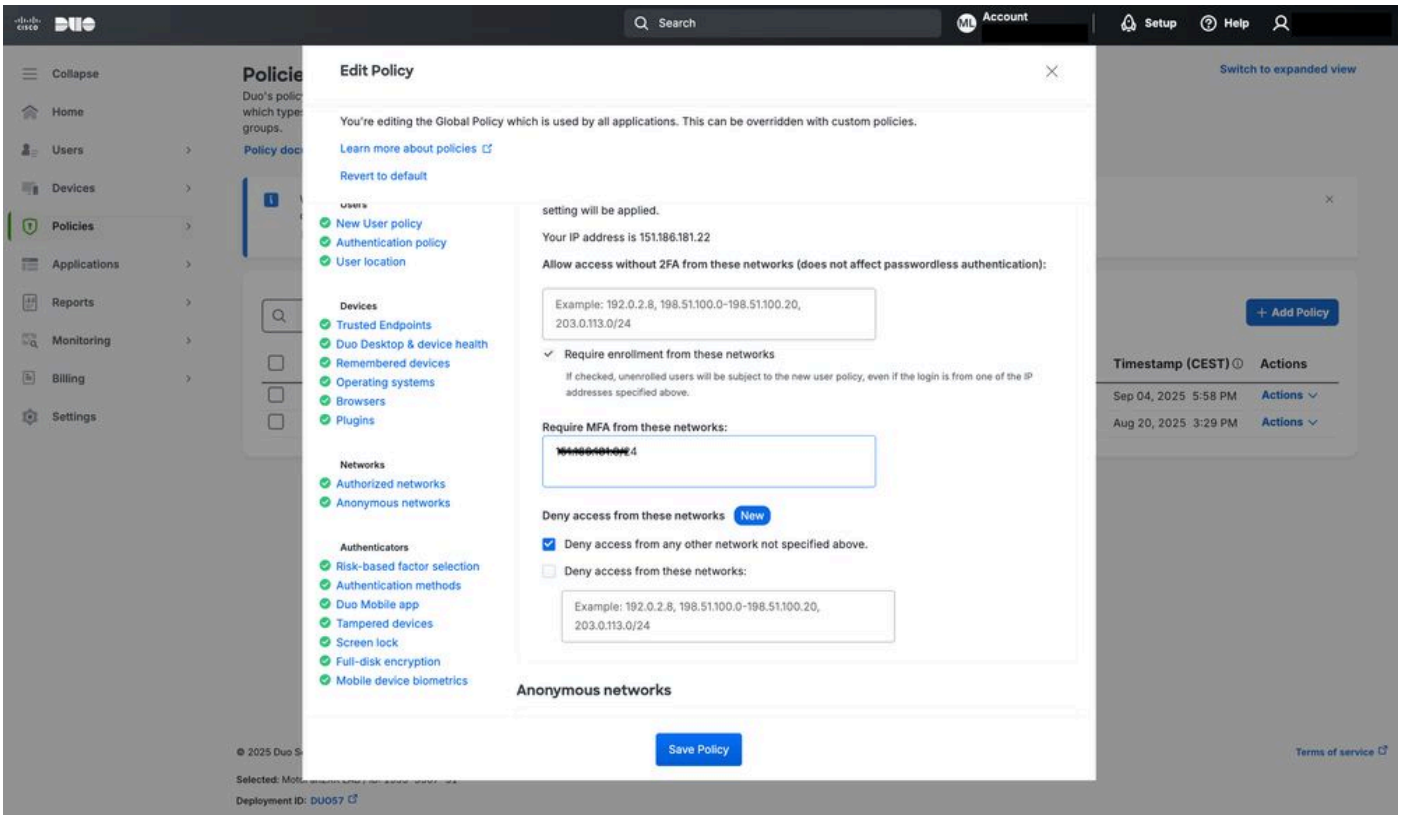
Questo criterio può essere applicato per utente o gruppo, a seconda dei requisiti di accesso.



Cisco Duo

In questo esempio, come mostrato nell'immagine, il controllo dell'accesso IP all'origine viene abilitato configurando la sezione Reti autorizzate.

Questa configurazione consente l'accesso solo da intervalli IP attendibili specificati, migliorando la sicurezza di Cisco ETD.



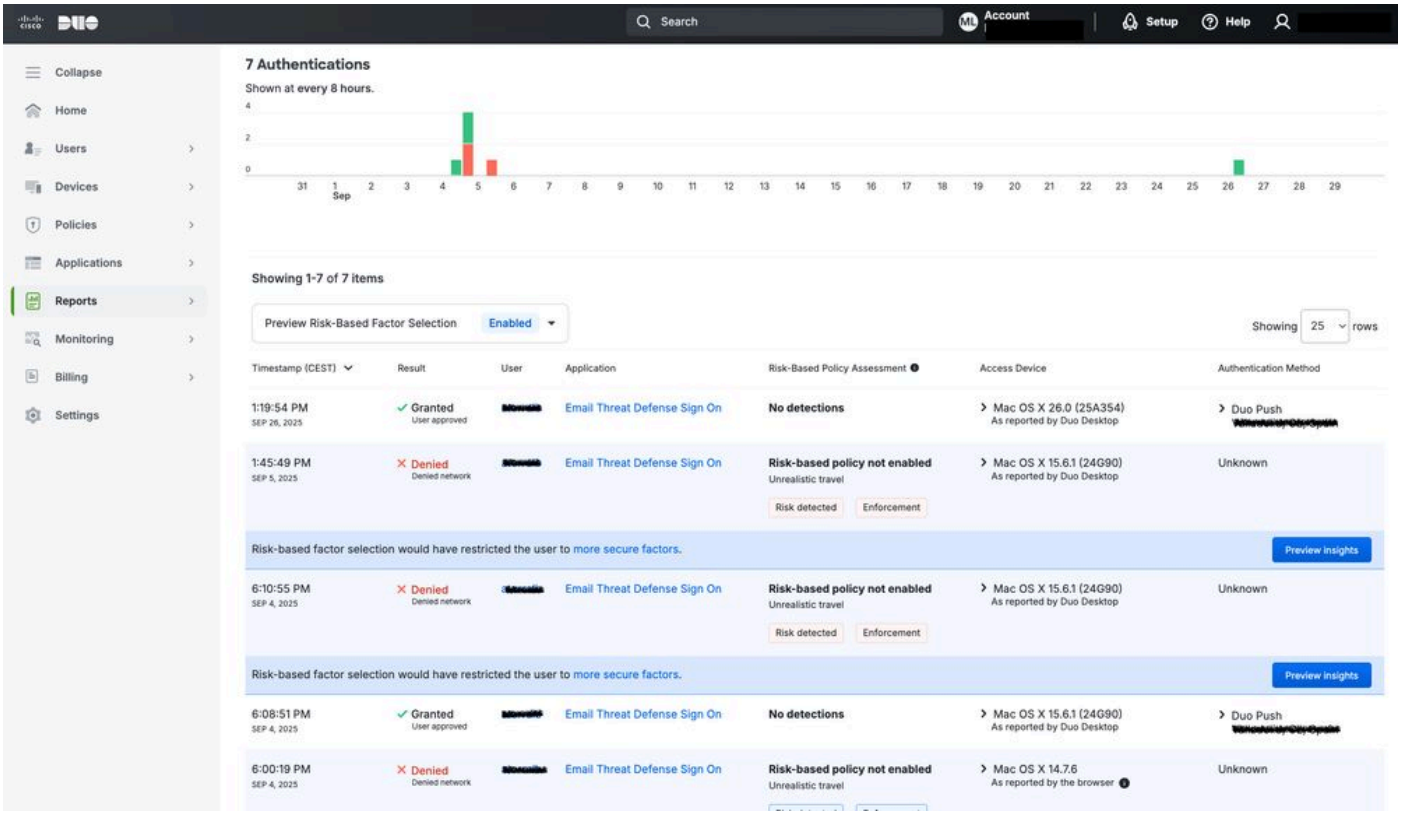
Configurazione criteri Cisco Duo

Conclusioni

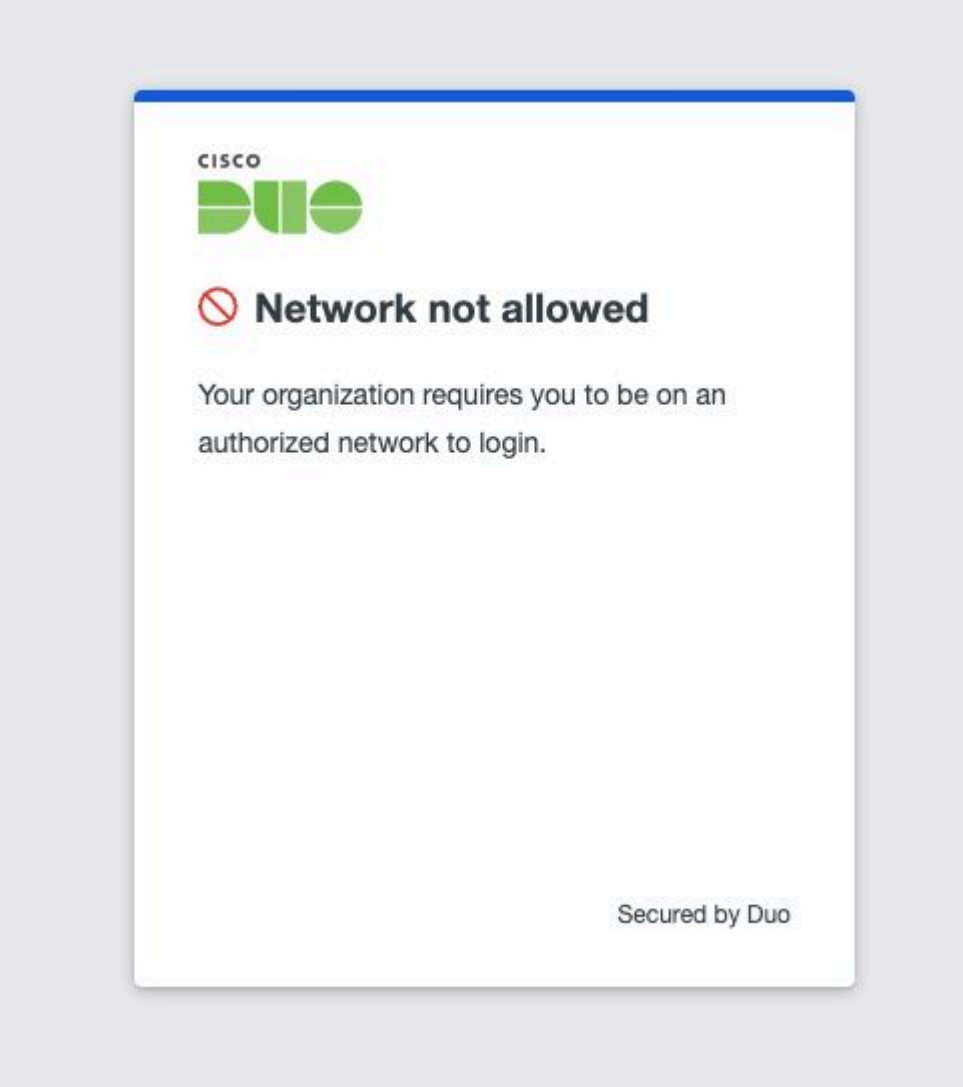
Cisco ETD offre opzioni flessibili per proteggere l'accesso degli amministratori tramite l'autenticazione a più fattori e l'integrazione con i provider di identità.
Combinando Cisco SCC con Cisco Duo, le organizzazioni possono implementare policy di autenticazione più efficaci, ridurre il rischio di accesso non autorizzato e allinearsi alle best practice del settore per una gestione sicura dei servizi cloud.

Oltre all'autenticazione a più fattori, gli amministratori possono utilizzare i controlli basati su policy di Cisco Duo per limitare l'accesso in base a criteri specifici, ad esempio l'indirizzo IP di origine. Ad esempio, come illustrato nell'immagine seguente, un tentativo di accesso da un indirizzo IP esterno all'intervallo autorizzato viene bloccato automaticamente dal sistema. Ciò garantisce che siano consentite solo le richieste provenienti da reti attendibili, aggiungendo un ulteriore livello di protezione contro potenziali attacchi.

Implementando il controllo degli accessi basato su IP insieme all'autenticazione a più fattori, le organizzazioni adottano un approccio di difesa approfondito, che combina la verifica dell'identità con la convalida della posizione di rete per salvaguardare le interfacce di gestione critiche nel cloud.



Report Cisco Duo



Risultato del controllo di rete

Avviso: È importante tenere presente che questa modifica influisce su tutte le applicazioni che utilizzano lo stesso dominio di autenticazione. non solo ETD, ma anche altri prodotti che si basano sullo stesso processo di autenticazione, ad esempio l'accesso alla console Cisco Secure Access.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).