

安全電子郵件威脅防禦：多重驗證和存取控制

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[案例](#)

[Cisco SCC配置](#)

[使用Cisco SCC連線ETD與Cisco Duo](#)

[適用於Cisco ETD的Cisco Duo中的策略配置](#)

[結論](#)

簡介

本檔案介紹思科電子郵件威脅防禦(ETD)提供的功能，以控制管理員對管理控制檯的存取許可權。

必要條件

需求

思科建議您瞭解以下主題，以便使用Duo配置ETD身份驗證：

- [Cisco ETD訂用](#)
- [對思科安全雲控制\(SCC\)的訪問](#)
- [增強安全性的身份驗證解決方案，在本例中為Cisco Duo。](#)

採用元件

本文檔僅限於Email Treat Defense和Secure Cloud Control。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

本文檔重點介紹Cisco ETD如何利用Cisco SCC並與Cisco Duo整合以提供安全身份驗證和精細訪問控制。

在基於雲的現代解決方案中，訪問控制是確保資料安全性、合規性和操作完整性的最重要元件之一。

。未經授權的訪問 — 尤其是管理員帳戶的訪問 — 可能會導致嚴重的後果，如系統受損、資料洩露和服務中斷。

思科在其雲產品組合中提供強大的安全功能，包括多重身份驗證(MFA)技術，該技術是Cisco ETD等服務不可或缺的一部分。MFA在傳統密碼之外新增了一個關鍵驗證步驟，要求使用者通過附加因素（例如移動應用批准、安全令牌或生物特徵驗證）進行身份驗證。

為了簡化和加強管理員身份驗證流程，ETD利用Cisco SCC（一種集中式身份驗證和策略管理服務）。

通過SCC，ETD可獲得一系列安全功能，包括：

- 實施MFA以減輕憑證失竊風險。
- 與Cisco Duo、Microsoft Entra ID、Okta等第三方身份提供商整合，以支援靈活的身份驗證工作流程和企業身份聯合。
- 集中策略管理，允許跨思科雲服務執行一致的訪問規則。

特別是Cisco Duo，通過新增高級基於策略的訪問管理來擴展這些功能。使用SCC作為整合通道，ETD可以直接將Duo的粒度控制（如源IP限制、裝置運行狀況檢查和基於使用者組的規則）應用於管理員訪問。

例如，組織可以定義僅允許從特定受信任網路範圍進行訪問的策略。在授權IP清單之外進行的任何連線嘗試都會被自動阻止，如附圖所示。MFA和情景策略的組合支援深度防禦方法，確保即使證書受到危害，攻擊者仍然可以阻止其訪問系統，除非他們也滿足其他安全標準。

通過將Cisco ETD、Cisco SCC和Cisco Duo相結合，企業可以實施安全、可擴展且使用者友好的訪問控制模型，與行業最佳實踐保持一致，同時加強對關鍵雲服務的保護。

案例

通過ETD可以實施多種身份驗證和訪問控制方案，以保護管理訪問：

1. 嵌入式MFA — 使用Cisco的內建MFA或整合Microsoft MFA。
2. Cisco SCC與Cisco Duo — 將Cisco SCC的集中式身份驗證與Duo的高級MFA功能相結合。
3. 帶有外部身份提供商（例如，Microsoft Entra ID）的Cisco SCC — 通過與企業身份解決方案整合來擴展身份驗證策略。

本檔案介紹案例2的設定步驟：採用Cisco Duo的Cisco SCC，但此流程可以適用於其他技術。



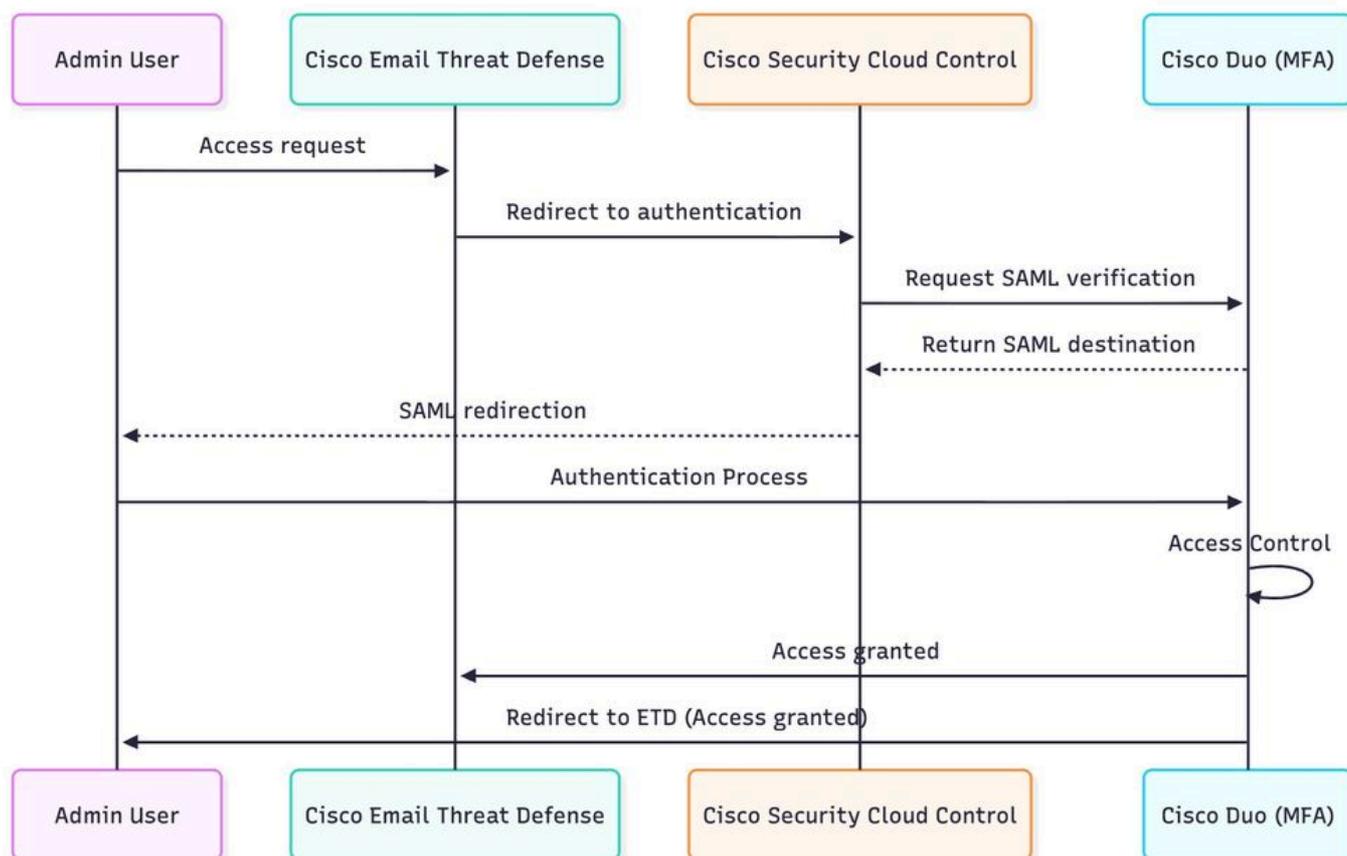
附註：本文檔概述了使用Cisco Duo的多重身份驗證功能在郵件威脅防禦(ETD)中啟用訪問控制所需的基本步驟。實施Duo整合可確保只有授權使用者才能訪問該平台，從而增強安全性。有關綜合指南、配置選項和高級部署方案，請參閱正式產品文檔：

— 用於集中式安全策略和訪問管理。

[Cisco Duo](#) - 瞭解有關多重身份驗證設定和最佳實踐的詳細說明。

Cisco SCC配置

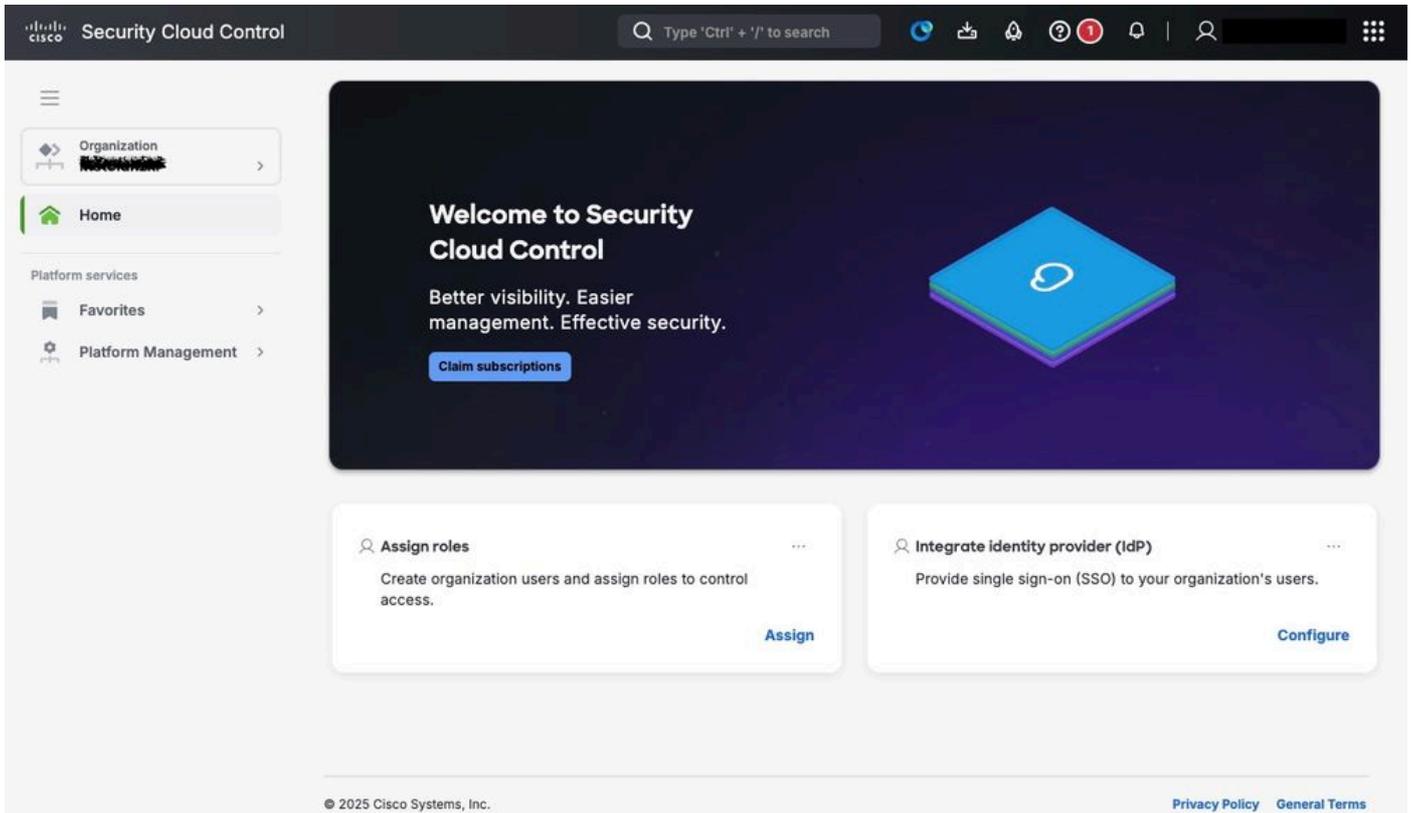
為了將Cisco ETD與Cisco Duo整合，第一步是在Cisco SCC中配置身份驗證域。這樣可建立信任關係，使思科SCC能夠與外部身份和MFA提供商合作。



圖表

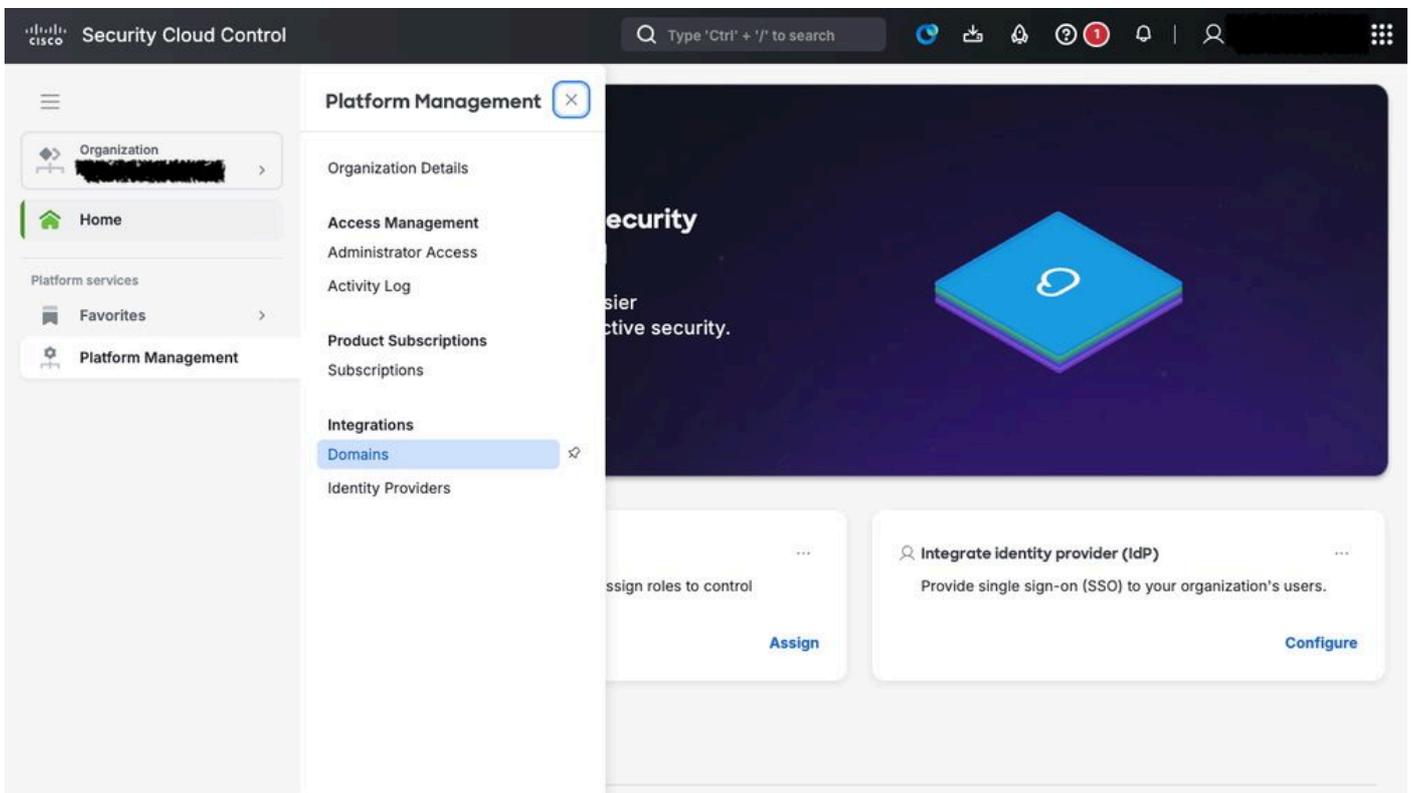
步驟1.訪問Cisco SCC控制檯。

登入到Cisco SCC門戶<https://security.cisco.com/>。



步驟2.導覽至Domain Management。

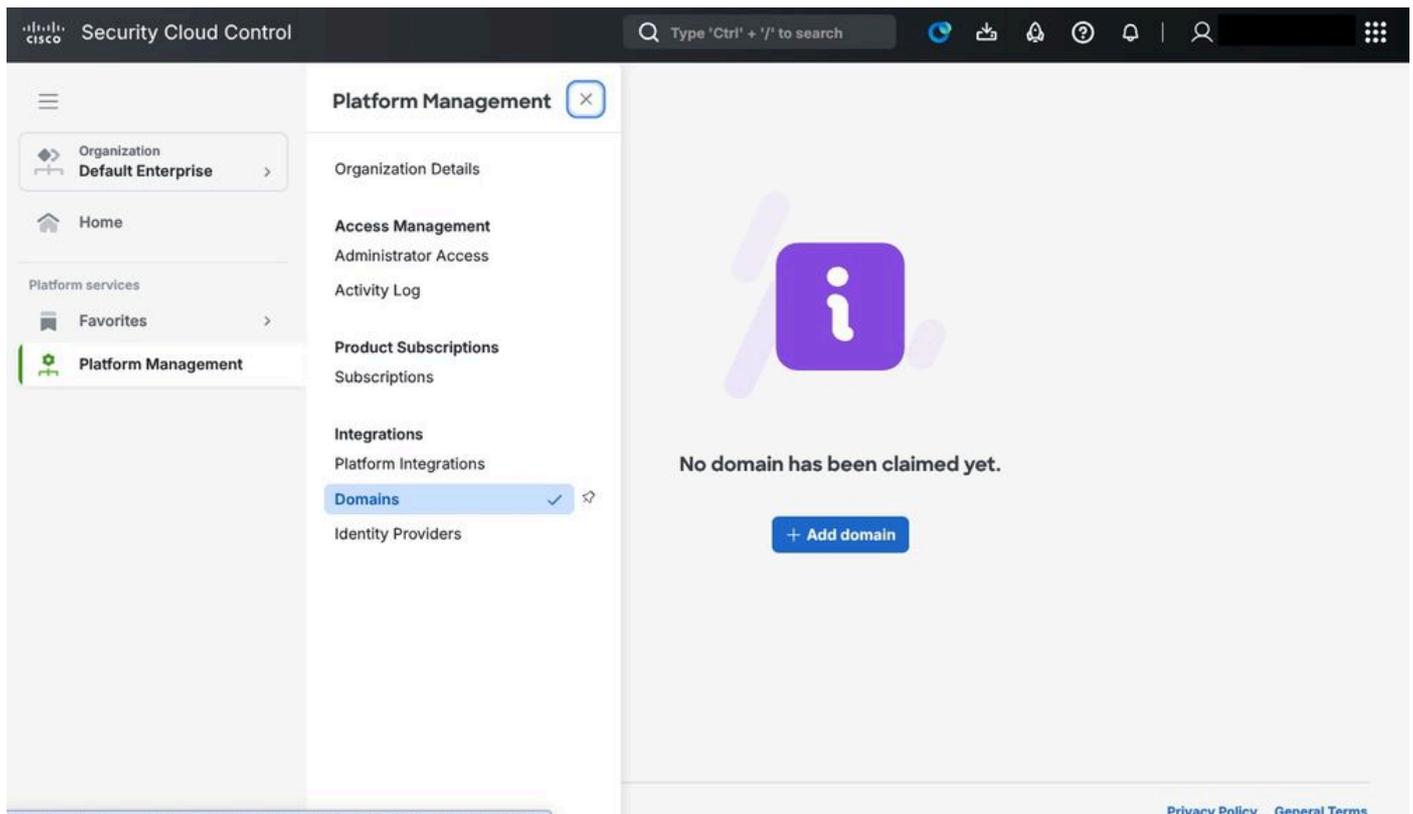
從主選單中，導航到Platform Management > Domains。



安全雲控制域配置

步驟3.新增新域。

按一下Add Domain以開始註冊身份驗證域的過程。

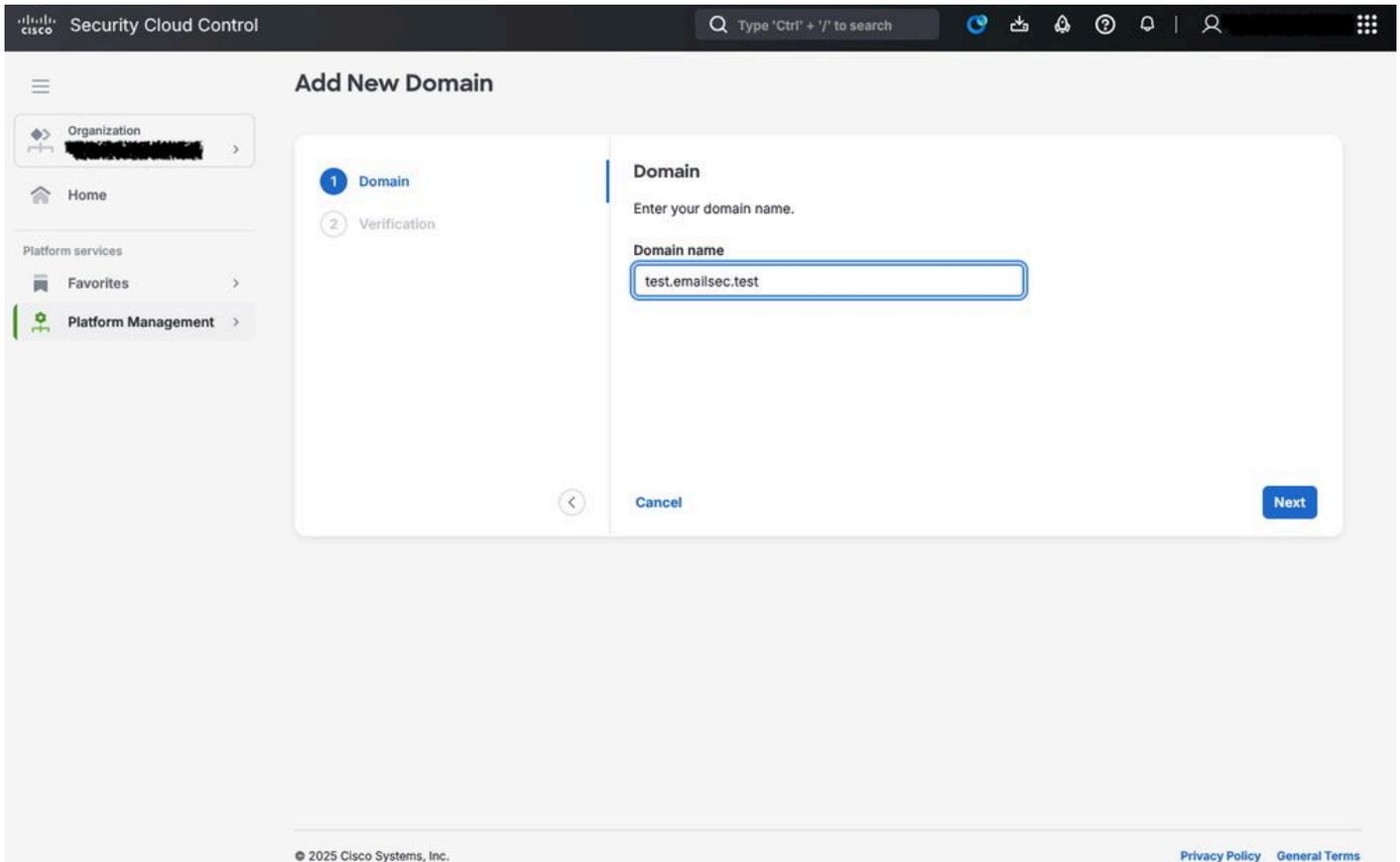


安全雲控制：域

步驟4.提供域資訊。

填寫包含用於身份驗證的域詳細資訊的表格。這通常包括：

- 域名(例如test.emailsec.test)
- 聯絡資訊 (行政和技術)
- 身份驗證引數，取決於所選的身份提供程式



步驟5.透過DNS進行網域驗證。

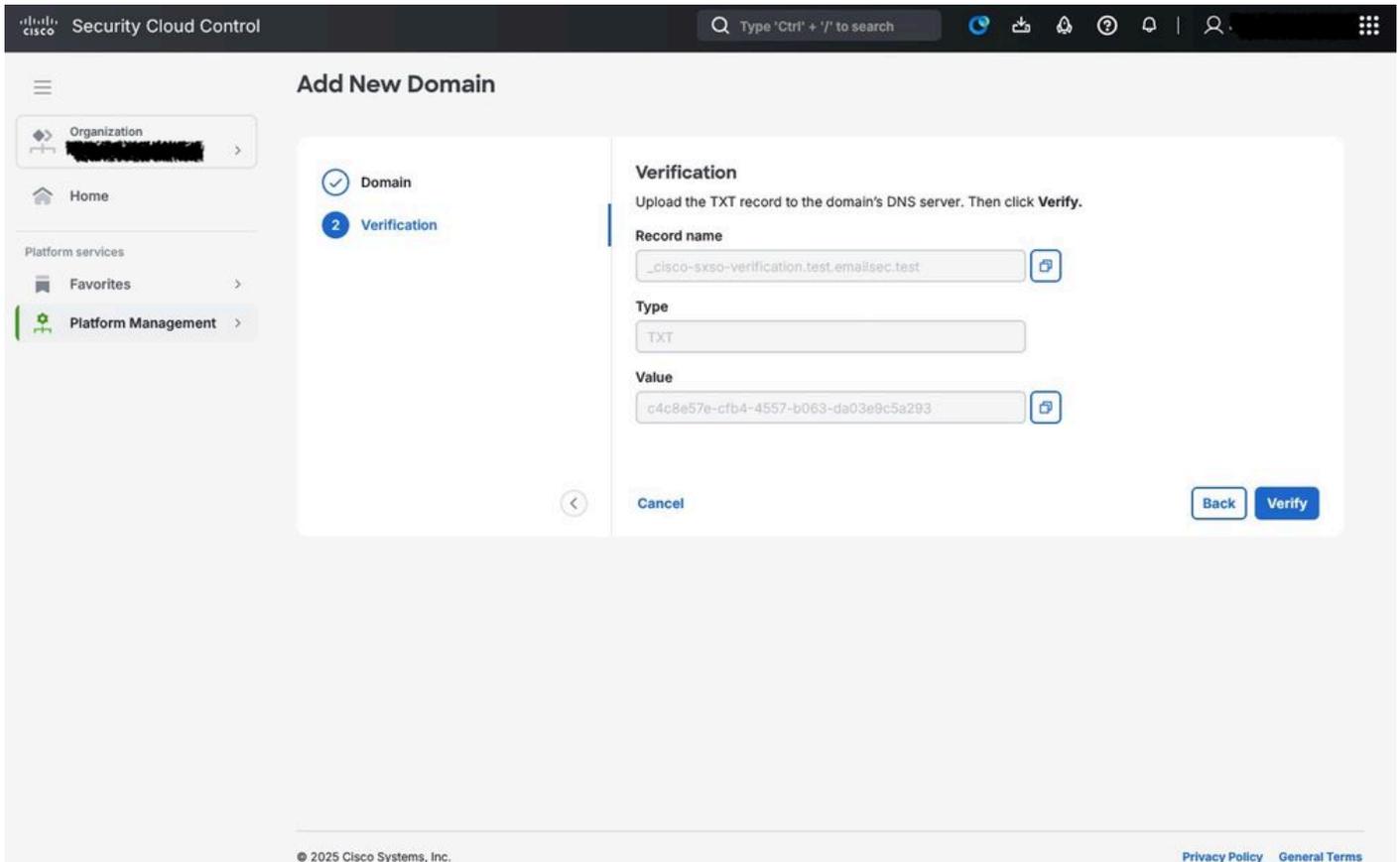
註冊域後，思科需要所有權證明。

- CSCC提供驗證記錄
- 此記錄必須新增到域的DNS配置中（通常作為TXT記錄）
- 思科安全雲會自動驗證DNS條目，以確認該域屬於您的組織



注意：驗證過程必須成功完成，才能繼續整合。根據DNS傳播，驗證需要幾分鐘到幾小時

。



使用Cisco SCC連線ETD與Cisco Duo

成功配置管理員的域（作為應用更嚴格的訪問控制和管理許可權的基礎）後，下一步是整合約定的MFA服務。

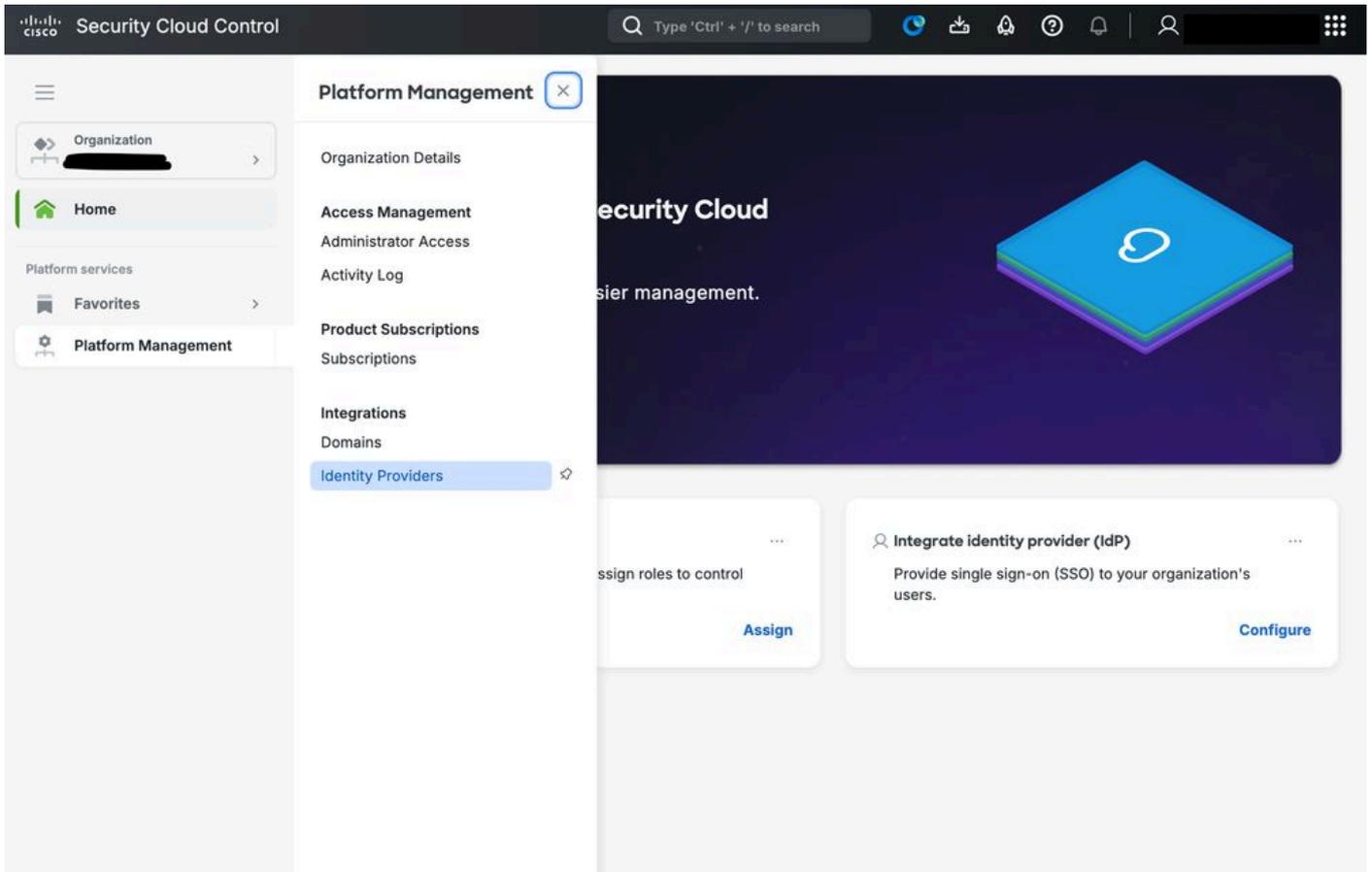
在此場景中，Cisco Duo被實施為訪問控制、安全登入和MFA驗證的主要解決方案。此整合要求管理員通過多個驗證步驟驗證其身份，從而增強環境的安全狀態，降低未經授權訪問的風險，並確保遵守組織安全策略。

Cisco Duo與Cisco Cloud Control Integration

步驟1.訪問Cisco SCC控制檯。

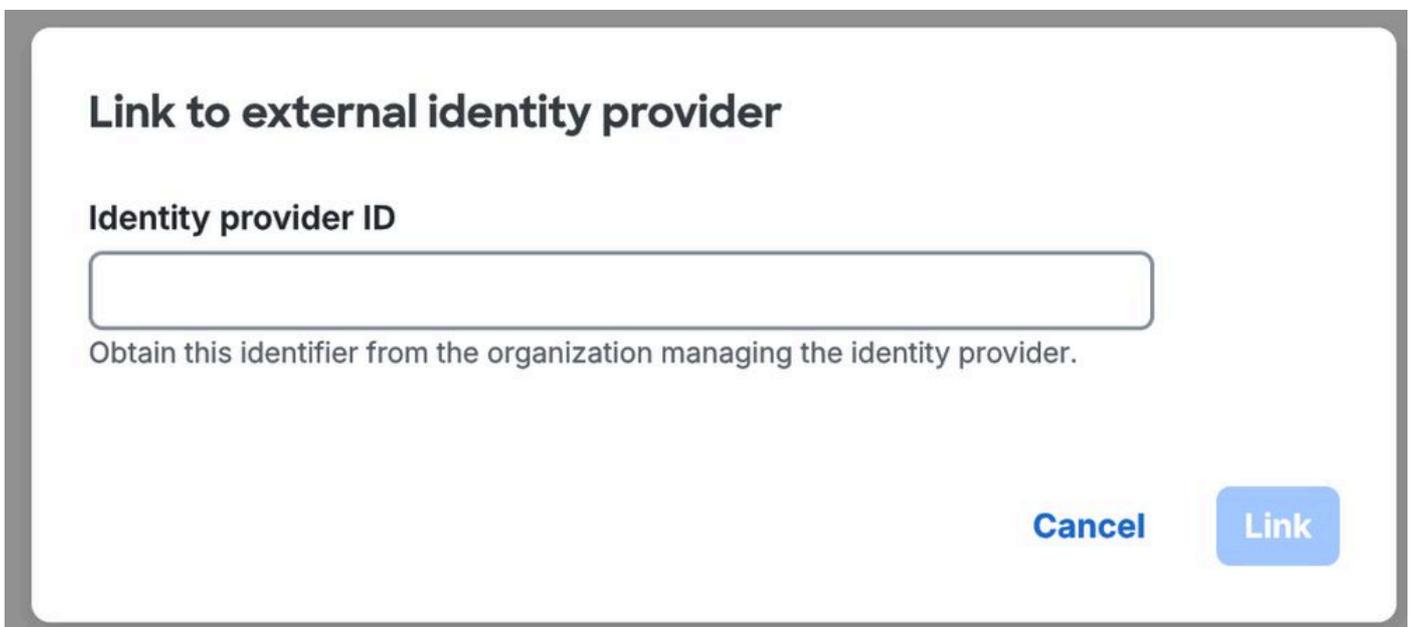
登入思科安全雲端控制入口網站<https://security.cisco.com/>。

導航到Platform Management，然後按一下Identity Providers。



SCC IDP配置

使用自定義名稱來標識身份提供程式。



現在開始安裝。現在，您可以訪問Cisco SCC和Cisco Duo。

步驟2.在SCC中，禁用Enable DUO-based MFA in Security Cloud Sing On（如圖所示），然後按一下Next。

Edit identity provider

- 1 Set up**
- 2 Configure
- 3 SAML metadata
- 4 Test
- 5 Activate

Set up

Follow the steps below to configure your identity provider (IdP). For detailed instructions please read our [documentation](#) 

Identity provider name *

Duo-based MFA

By default, Security Cloud Sign On enrolls all users into Duo MultiFactor Authentication (MFA) at no cost. We strongly recommend MFA, with a session timeout no greater than 2 hours, to help protect your sensitive data within Cisco Security products.

Enable DUO-based MFA in Security Cloud Sign On

If your organization has integrated MFA at your IdP, you may wish to disable MFA at the Security Cloud Sign On level.

[Cancel](#) [Next](#)

身份提供程式配置

步驟3. 建立相關資料，並在Cisco Duo配置過程中使用。

確保複製所有必需值和關聯資料，並將它們儲存在一個安全位置。

這些詳細資訊對於未來的整合步驟至關重要，因此請確保這些詳細資訊僅可供授權人員訪問，並且根據貴組織的安全策略得到保護。

Edit identity provider

- 1 Set up
- 2 Configure**
- 3 SAML metadata
- 4 Test
- 5 Activate

Configure

Depending on your provider, use the following methods to set up your IdP.

Security Cloud Sign On SAML metadata

cisco-security-cloud-saml-metadata.xml



Or

Public certificate

cisco-security-cloud.pem



Entity ID (Audience URI)

https://www.okta.com/saml2/service-provider/spzbcwujnsgzweaoxafz



Single Sign-On Service URL (Assertion Consumer Service URL)

https://sign-on.security.cisco.com/sso/saml2/0oa1nbh73aeH3TyZs358



Technical notes for Security Cloud Sign On

- Security Cloud Sign On uses the SAML 2.0 HTTP POST binding to send

步驟4.開啟[Cisco Duo](#)，導覽至Applications區段，然後按一下Add application。

Protection Type	Provisioning	Application Type	Application Policy	Application-Group Policies
2FA	—	1Password	—	—
—	—	Duo Admin Panel - Duo Access Gateway	—	—
SSO	—	Cisco Security Cloud Sign On - Single Sign-On	—	—
—	—	Google Workspace - Duo Access Gateway	—	—
—	—	Microsoft 365 - Duo Access Gateway	—	—

在功能表中，搜尋思科安全雲，然後按一下Add以開始整合。

← Applications

Application Catalog

Browse all of our available applications and filter by supported features. View documentation links for more information about each application.

🔍 Cisco Security Cloud control ✕ Supported Features ▾



Cisco Security Cloud Sign On

SSO

Secure access using Duo SSO and SAML, with MFA and flexible security policies.

[+ Add](#) [Documentation](#) ↗

步驟5. 在Cisco Duo應用程式中配置相關資訊。

將Entity ID和Singles Sign-On Service URL從Cisco SCC複製到Cisco Duo。

Downloads

XML file

Download XML

Copy XML

Service Provider

Entity ID (Audience URI) *

https://www.okta.com/saml2/service-provider/spzbcwujns

Enter your Cisco Security Cloud Sign On Entity ID (Audience URI)

Single Sign-On Service URL
(Assertion Consumer Service URL) *

https://sign-on.security.cisco.com/sso/saml2/00a1nbh73a

Enter your Cisco Security Cloud Sign On Entity ID (Audience URI)

Custom attributes

Check this box if your Duo Single Sign-On authentication source uses non-standard attribute names.

步驟6. 下載XML並將檔案上傳到Cisco SCC。

Edit identity provider

- ✓ Set up
- ✓ Configure
- 3 SAML metadata**
- 4 Test
- 5 Activate

SAML metadata

Select a method for providing your SAML 2.0 IdP metadata.

XML file upload Manual configuration

Upload your SAML metadata file

↑

Click or drag a file to this area to upload

File has been uploaded



Cancel

Back

Next



附註：應用程式中可從Cisco Duo控制檯配置的其餘引數必須根據您的特定要求進行調整。有關這些設定的詳細說明，請參閱官方[Cisco Duo文檔](#)。可配置引數的示例包括分配的應用程式名稱、應用該策略的使用者集，以及其他可以定製安全控制以滿足組織需求的可定製選項。

適用於Cisco ETD的Cisco Duo中的策略配置

在此階段，所有元件均已連線，下一步是配置適用於Cisco ETD控制檯內管理員身份驗證過程的策略。

在本示例中，重點特別放在基於IP地址的訪問控制上。但是，Cisco Duo提供了許多其他訪問控制選項。

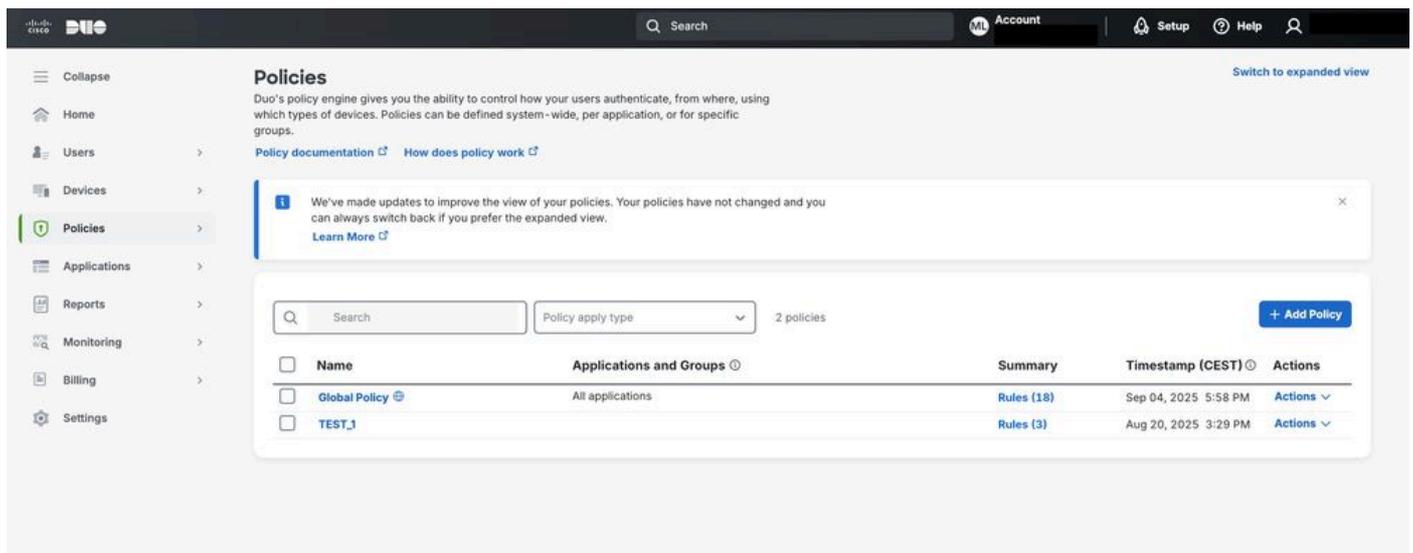
可以建立新的策略並分配給應用程式，從而實施管理員登入所需的身份驗證規則和安全限制。

有關Cisco Duo中所有可用控制元件和配置選項的更多詳細資訊，請參閱官方Cisco Duo文檔。

此資源提供有關設定、自定義和最佳實踐的全面指導，以幫助最佳化安全策略。

導航到Cisco Duo中的Policies部分，可以通過Cisco Duo建立策略並將其分配給Cisco ETD連線。

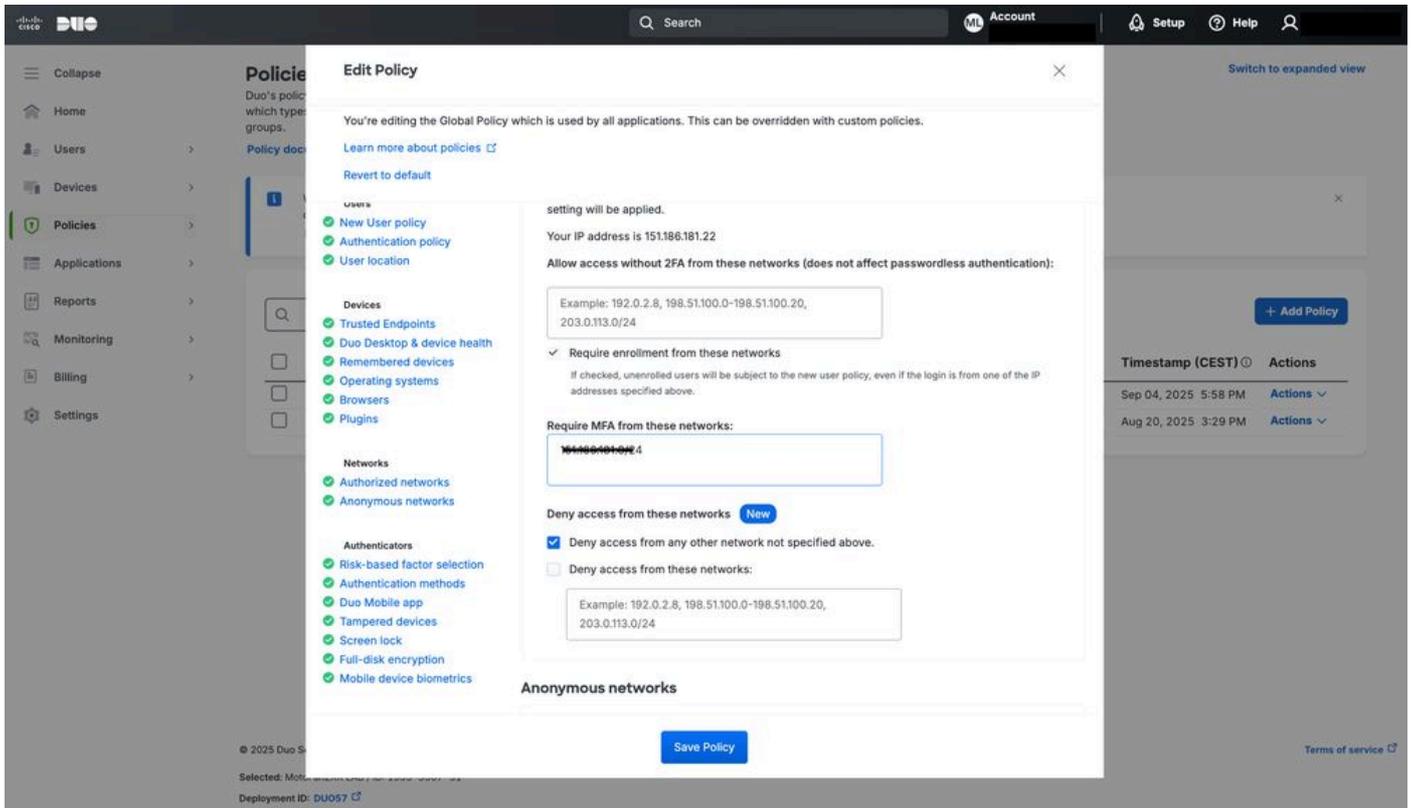
此策略可以根據訪問要求按使用者或組應用。



Cisco Duo

在此示例中，如圖所示，通過配置Authorized Networks部分啟用源IP訪問控制。

此配置僅允許從指定的受信任IP範圍進行訪問，從而增強了Cisco ETD的安全性。



Cisco Duo策略配置

結論

Cisco ETD提供靈活的選項，以便通過MFA以及與身份提供商的整合來保護管理員訪問。通過將Cisco SCC與Cisco Duo相結合，組織可以實施更強大的身份驗證策略，降低未經授權訪問的風險，並與行業最佳實踐保持一致，從而實現安全的雲服務管理。

除MFA外，管理員還可以利用Cisco Duo的基於策略的控制，以便根據特定條件（如源IP地址）限制訪問。例如，如下圖所示，系統會自動阻止從授權範圍之外的IP地址進行的訪問嘗試。這可以確保僅允許來自受信任網路的請求，從而增加一層額外保護，防止潛在攻擊。

通過與MFA一起實施基於IP的訪問控制，組織可以實現深度防禦方法 — 將身份驗證與網路位置驗證相結合，以保護雲中的關鍵管理介面。

- Collapse
- Home
- Users
- Devices
- Policies
- Applications
- Reports**
- Monitoring
- Billing
- Settings

7 Authentications

Shown at every 8 hours.



Showing 1-7 of 7 items

Preview Risk-Based Factor Selection **Enabled**

Showing 25 rows

Timestamp (CEST)	Result	User	Application	Risk-Based Policy Assessment	Access Device	Authentication Method
1:19:54 PM SEP 26, 2025	✓ Granted User approved	[Redacted]	Email Threat Defense Sign On	No detections	Mac OS X 26.0 (25A354) As reported by Duo Desktop	Duo Push [Redacted]
1:45:49 PM SEP 5, 2025	✗ Denied Denied network	[Redacted]	Email Threat Defense Sign On	Risk-based policy not enabled Unrealistic travel Risk detected Enforcement	Mac OS X 15.6.1 (24G90) As reported by Duo Desktop	Unknown
Risk-based factor selection would have restricted the user to more secure factors.						Preview Insights
6:10:55 PM SEP 4, 2025	✗ Denied Denied network	[Redacted]	Email Threat Defense Sign On	Risk-based policy not enabled Unrealistic travel Risk detected Enforcement	Mac OS X 15.6.1 (24G90) As reported by Duo Desktop	Unknown
Risk-based factor selection would have restricted the user to more secure factors.						Preview Insights
6:08:51 PM SEP 4, 2025	✓ Granted User approved	[Redacted]	Email Threat Defense Sign On	No detections	Mac OS X 15.6.1 (24G90) As reported by Duo Desktop	Duo Push [Redacted]
6:00:19 PM SEP 4, 2025	✗ Denied Denied network	[Redacted]	Email Threat Defense Sign On	Risk-based policy not enabled Unrealistic travel	Mac OS X 14.7.6 As reported by the browser	Unknown

CISCO



Network not allowed

Your organization requires you to be on an authorized network to login.

Secured by Duo

網路控制結果



警告：需要瞭解的是，此更改會影響使用相同身份驗證域的所有應用程式；不只限於 ETD，其他產品也依賴於相同的身份驗證過程，例如對思科安全訪問控制檯的訪問。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。