配置Umbrella以便遷移至安全訪問和安全雲控制

目錄

簡介

本檔案介紹如何使用安全雲控制(SCC)從Umbrella遷移至安全存取。

背景資訊

Umbrella客戶被鼓勵從Umbrella遷移到Secure Access，並需要使用Security Cloud Control管理其所有雲安全產品，作為這些更改的一部分。這樣，您就可以通過一個單一平台來管理其雲安全產品，包括思科安全訪問。

目前不支援多組織和MSSP（在本文建立時）。

必要條件

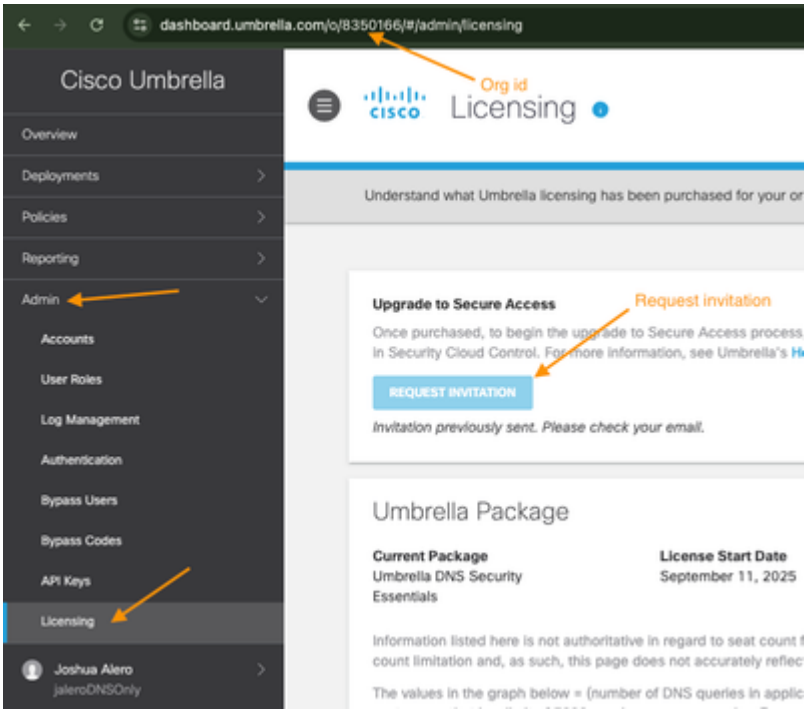
- 當前DNS或SIG訂閱
- 對Umbrella的完全管理員訪問許可權
- 訪問安全雲控制

準備階段

1.為遷移做準備

1. 確保您在Umbrella上具有DNS或SIG訂閱：

- 導航到Admin > Licensing進行驗證
- 升級至Secure Access必須顯示在頁面頂部：



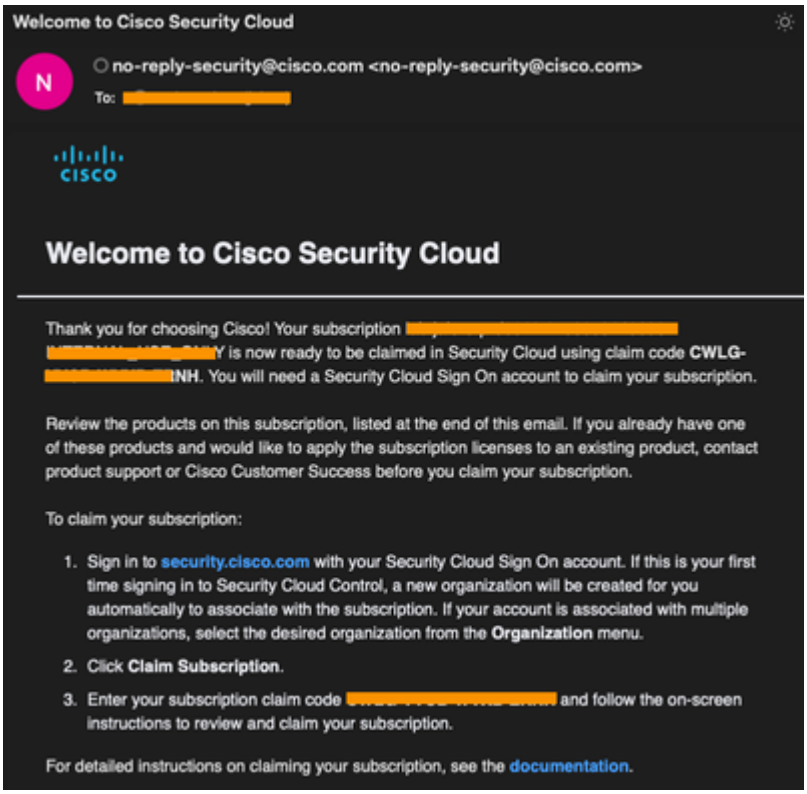
二。記下組織ID，在本例中為8350166。

三。在許可頁面上選擇Request Invitation選項。

重要:Request Invitation按鈕用作加入SCC的Umbrella租戶的邀請。它不會生成宣告代碼。完成安全訪問的訂單後，系統將向您提供索賠代碼。這是安全訪問的遷移過程的一部分。

附註：如果沒有Upgrade to Secure Access，請確保Umbrella軟體包是DNS或SIG（撰寫本文時當前不支援多組織或外掛）。

四。假設您已訂購Secure Access，請等待3-4個工作日，然後您必須收到一封包含訂閱宣告代碼的電子郵件(在從Umbrella租戶啟動請求邀請後)。 請在此處檢視示例電子郵件：



2.使用您現有的思科登入憑證登入到SCC

i.導覽至Security Cloud Control portal，然後使用您的思科登入憑證登入。

附註：用於訪問您的Umbrella控制面板的相同思科登入憑證。

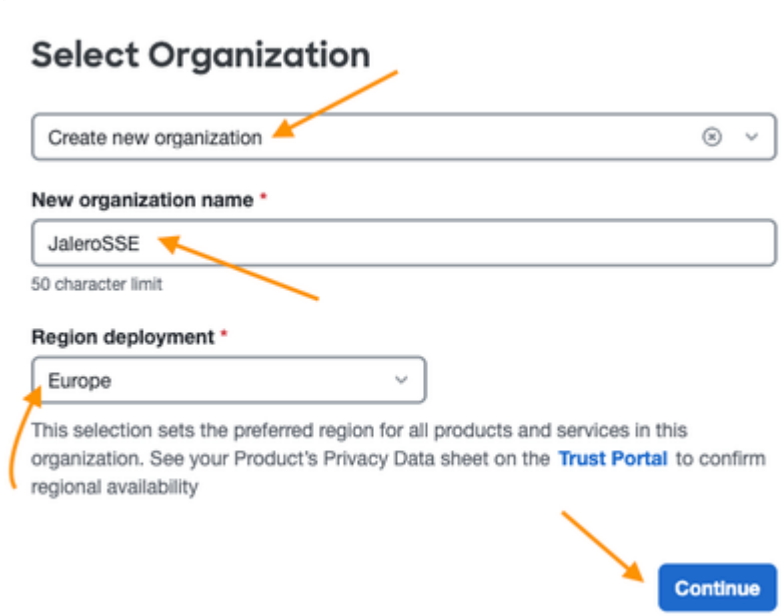
二。選擇建立新組織（如果您沒有現有組織）。

三。在「新組織名稱」(New Organization name)欄位中輸入新組織名稱。

四。從Region deployment下拉選單中選擇適當的區域。

注意：這必須是您的租戶將部署到的基本區域。

示例如下：



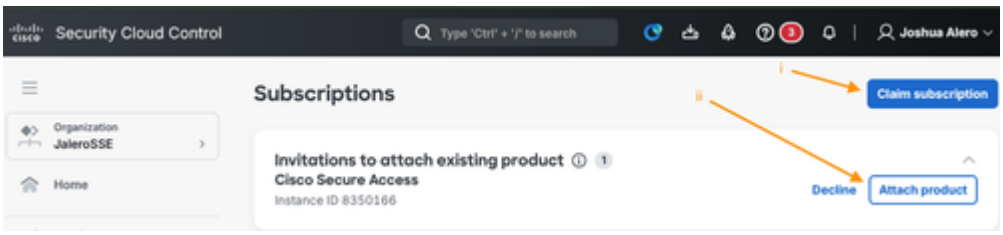
v.然後選擇繼續以完成組織建立。

3.將Umbrella組織連結到SCC並申請訂閱

i.選擇Claim subscription按鈕以使用上面第1步中提供的代碼進行索賠。

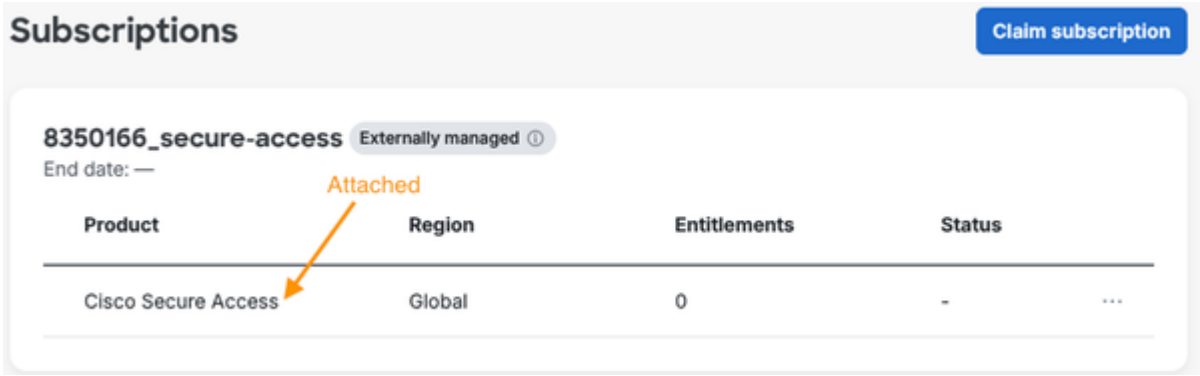
二。必須在訂用頁面中看到您的Umbrella組織ID，以及將其附加到SCC的邀請。

附註：Umberla控制面板上的Umberla組織ID必須相同。這對遷移和確保SCC和Umbrella連結都很重要。

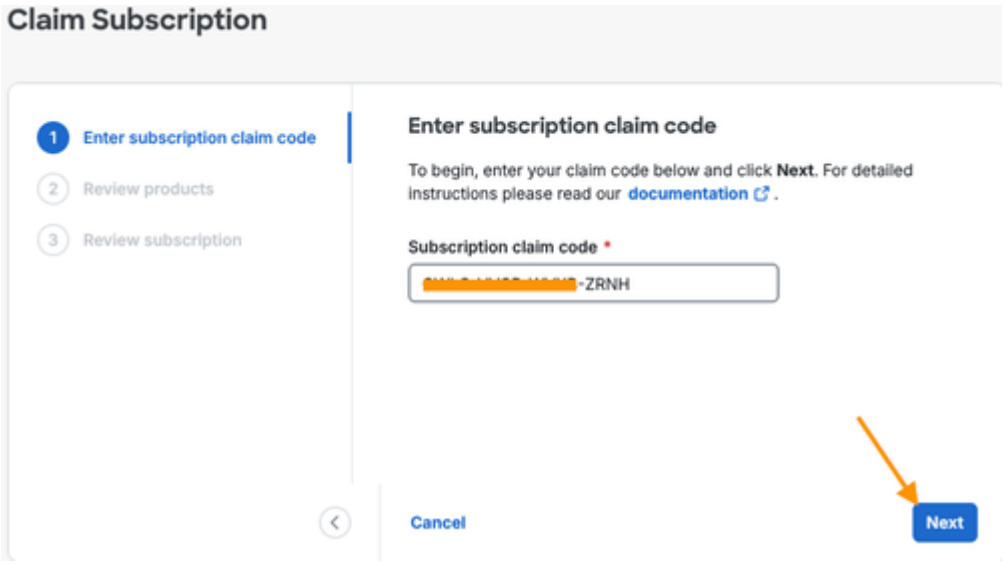


— 選擇Attach product，將您的Umbrella組織附加到SCC。

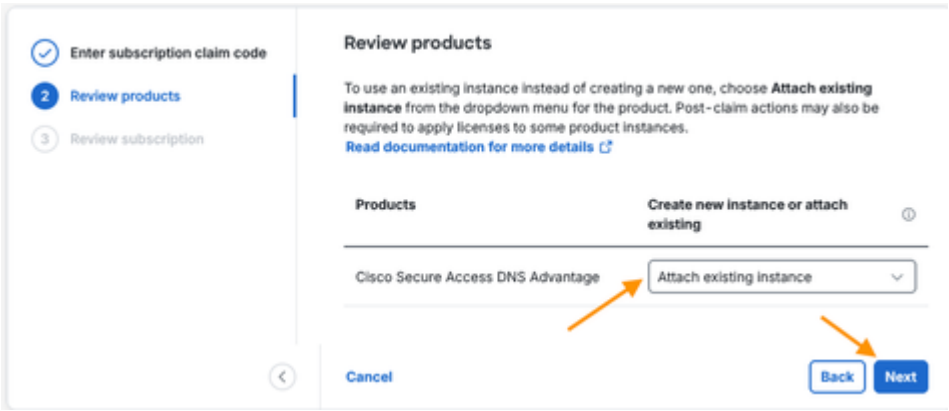
— 附加時，您必須在同一頁面中看到Cisco Secure Access產品，如以下示例所示：



三。輸入領款申請代碼並選擇下一步:

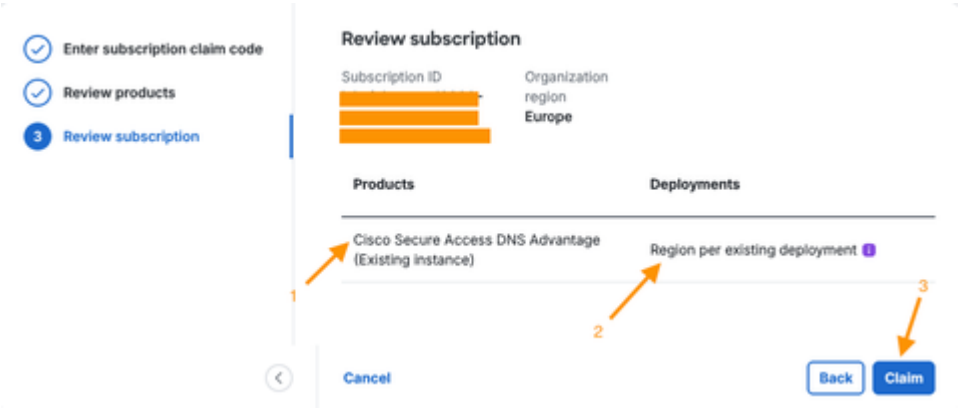


四。從Create new instance or attach existing下拉選單中選擇Attach existing instance:

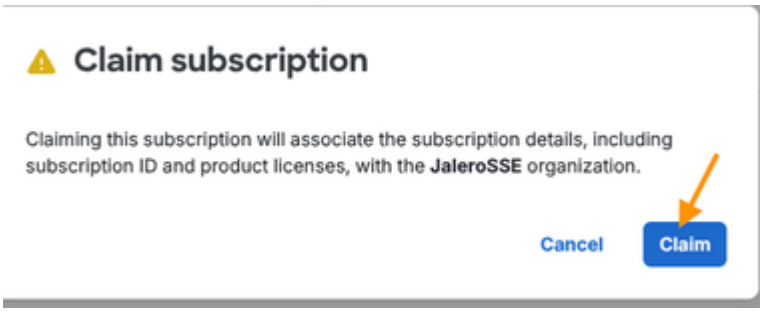


v.檢查設定：

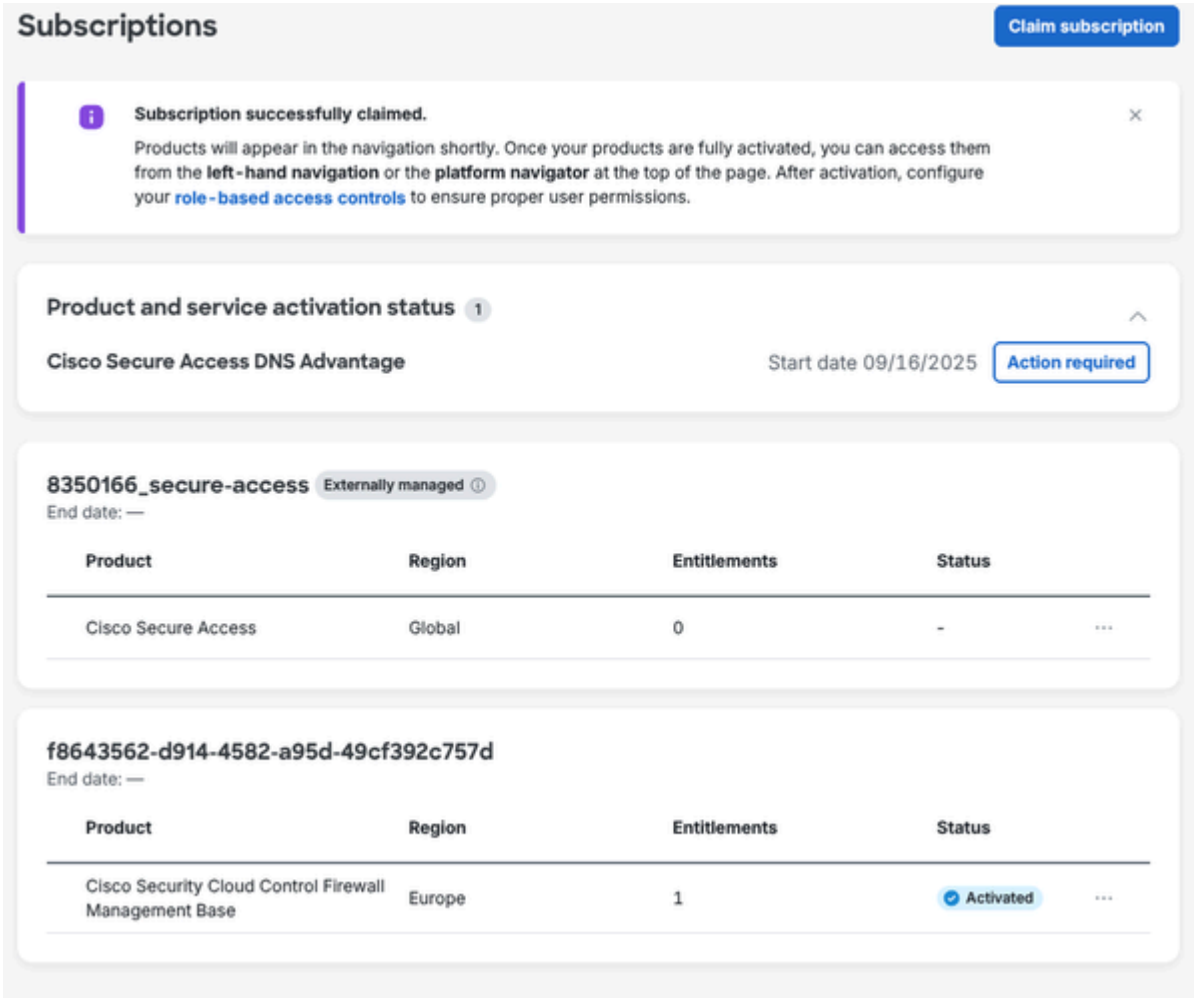
- 確保(Existing instance)是產品名稱的一部分
- 必須將區域設定為所連線的Secure Access例項的現有區域
- 選擇Claim move以移至下一頁



- 確認訂閱宣告：

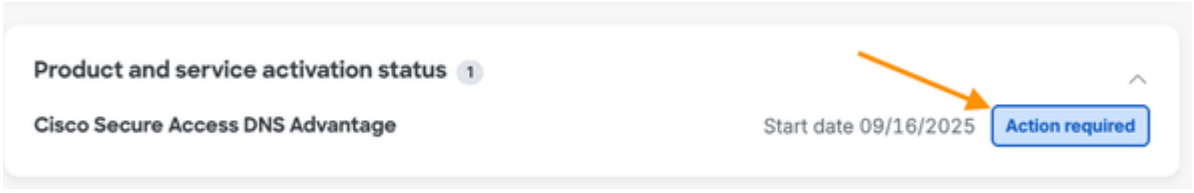


- 成功申請和調配後，您必須獲得一個類似於此處的Subscriptions頁面，其中顯示您所有已啟用的產品：

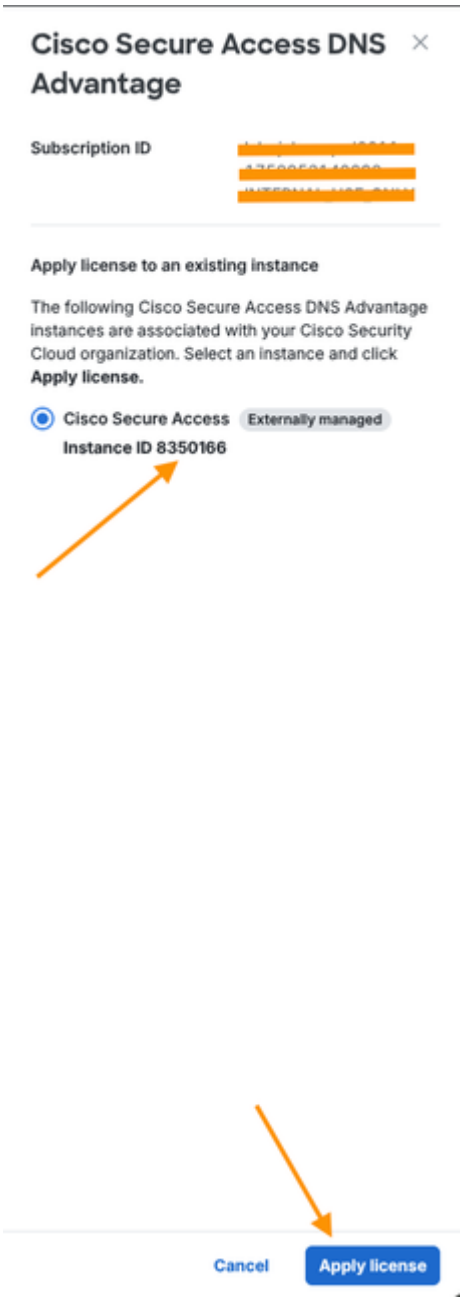


4.將許可證應用於安全訪問例項

i.選擇Action required選項：



二。選擇App license:

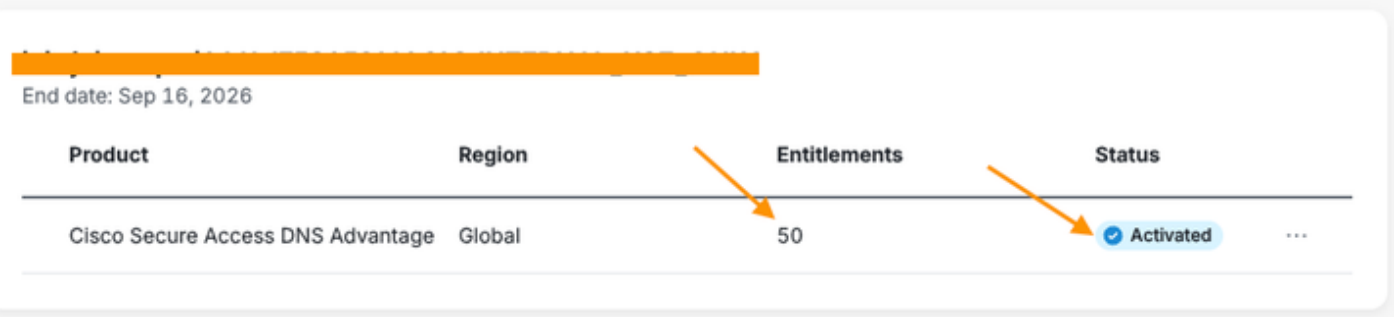


驗證到SCC的安全訪問鏈路

使用此部分驗證您的Secure Access租戶是否已連結到SCC。

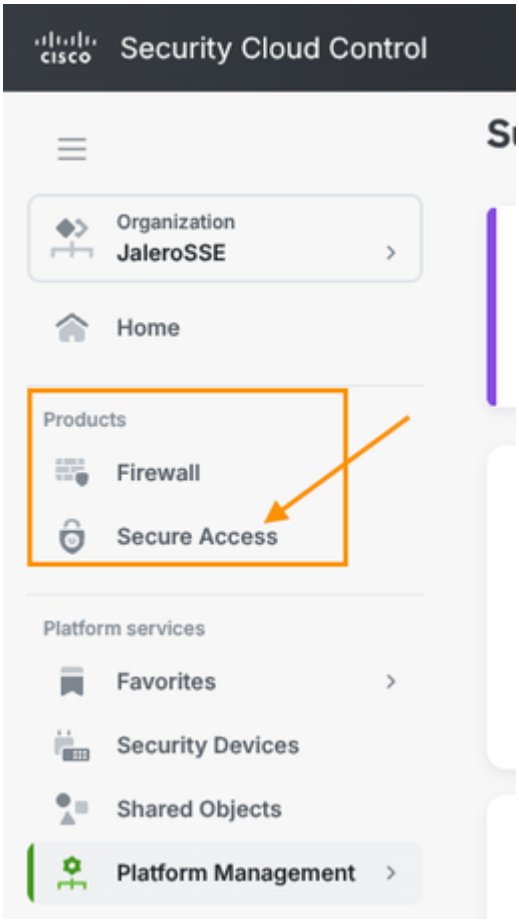
1.訂閱中的產品啟用狀態

驗證Cisco Secure Access <License Type>產品例項是否已啟用：



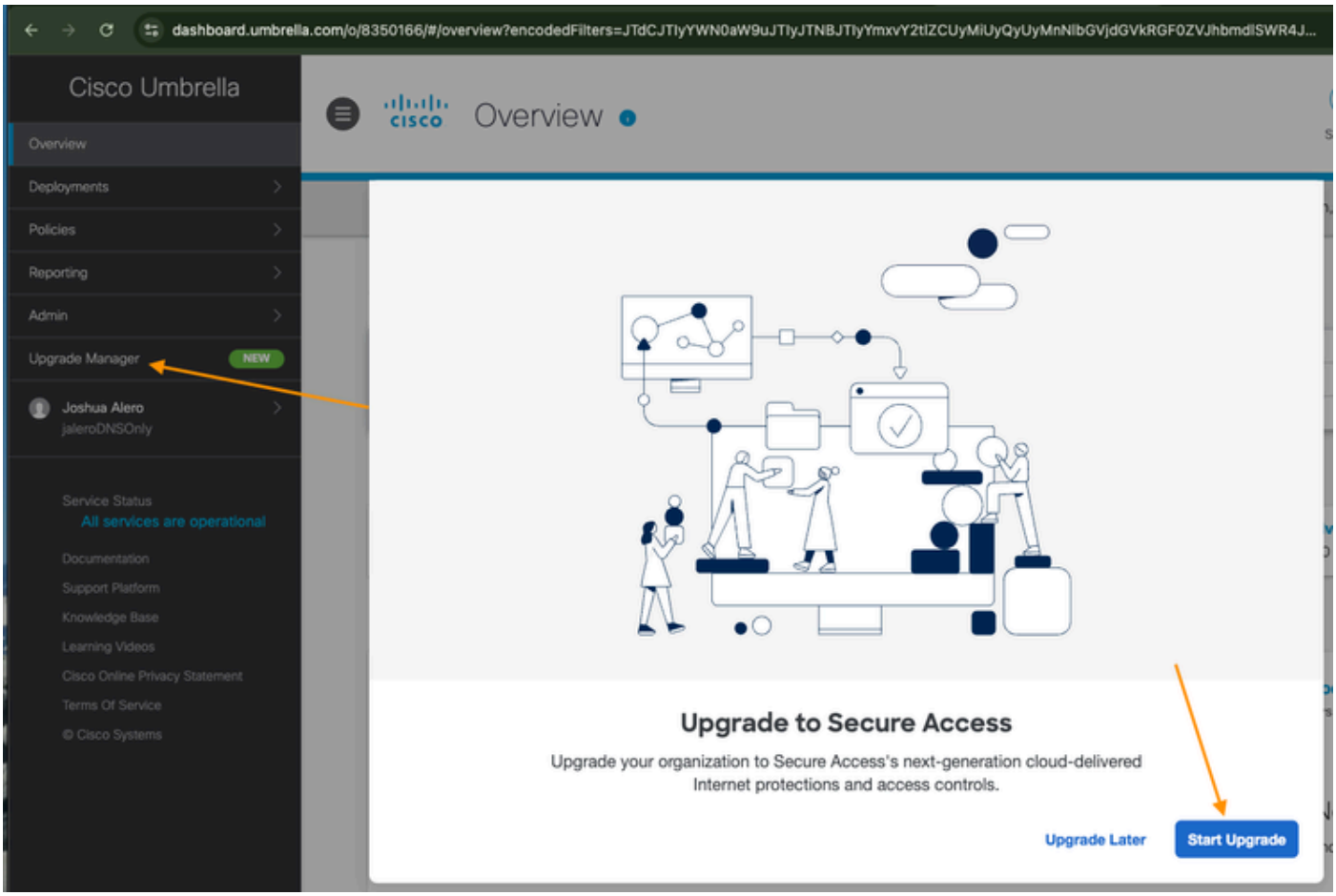
2.產品清單中的安全訪問

安全訪問現在還必須列在產品下：

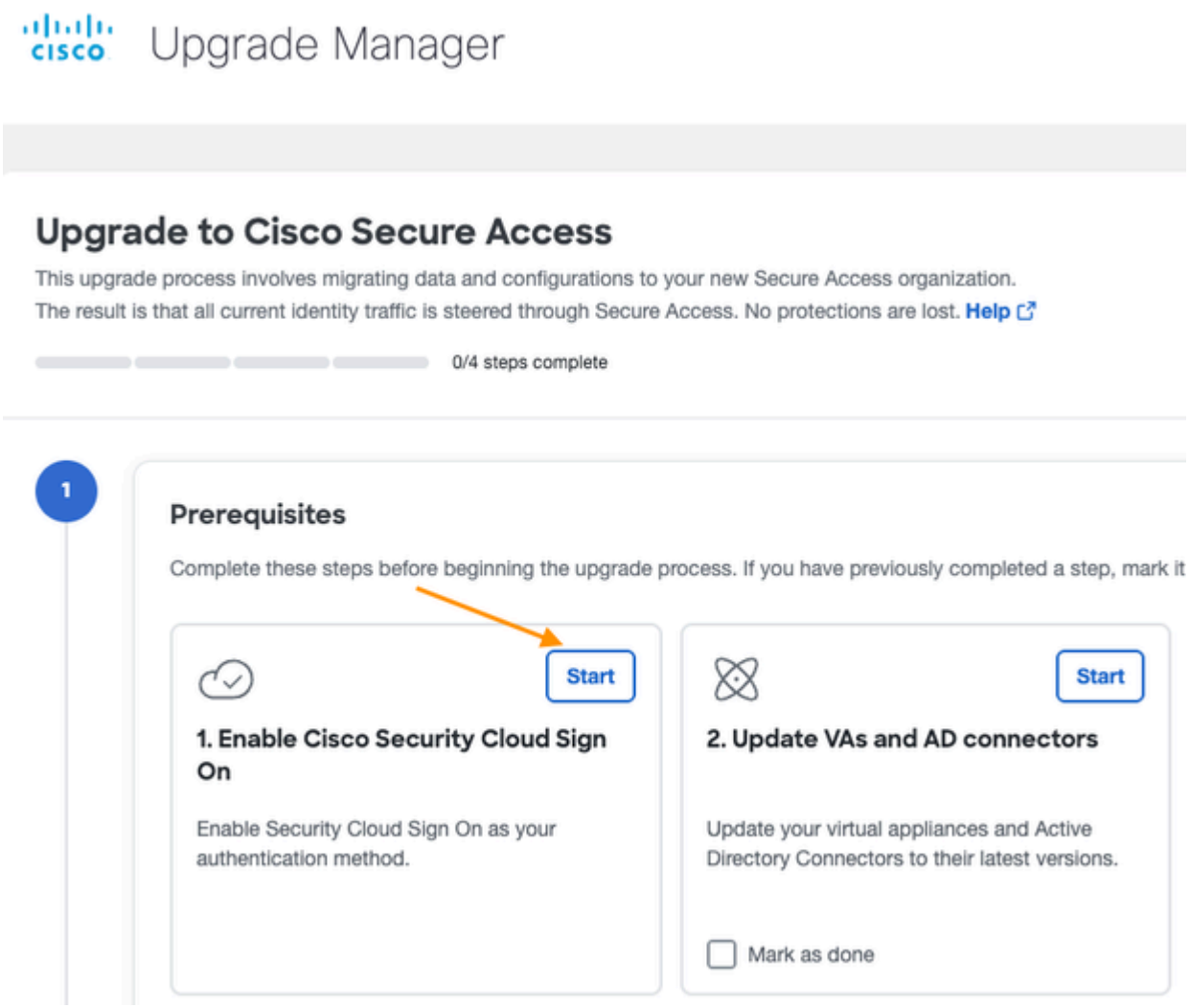


從Umbrella遷移至安全訪問

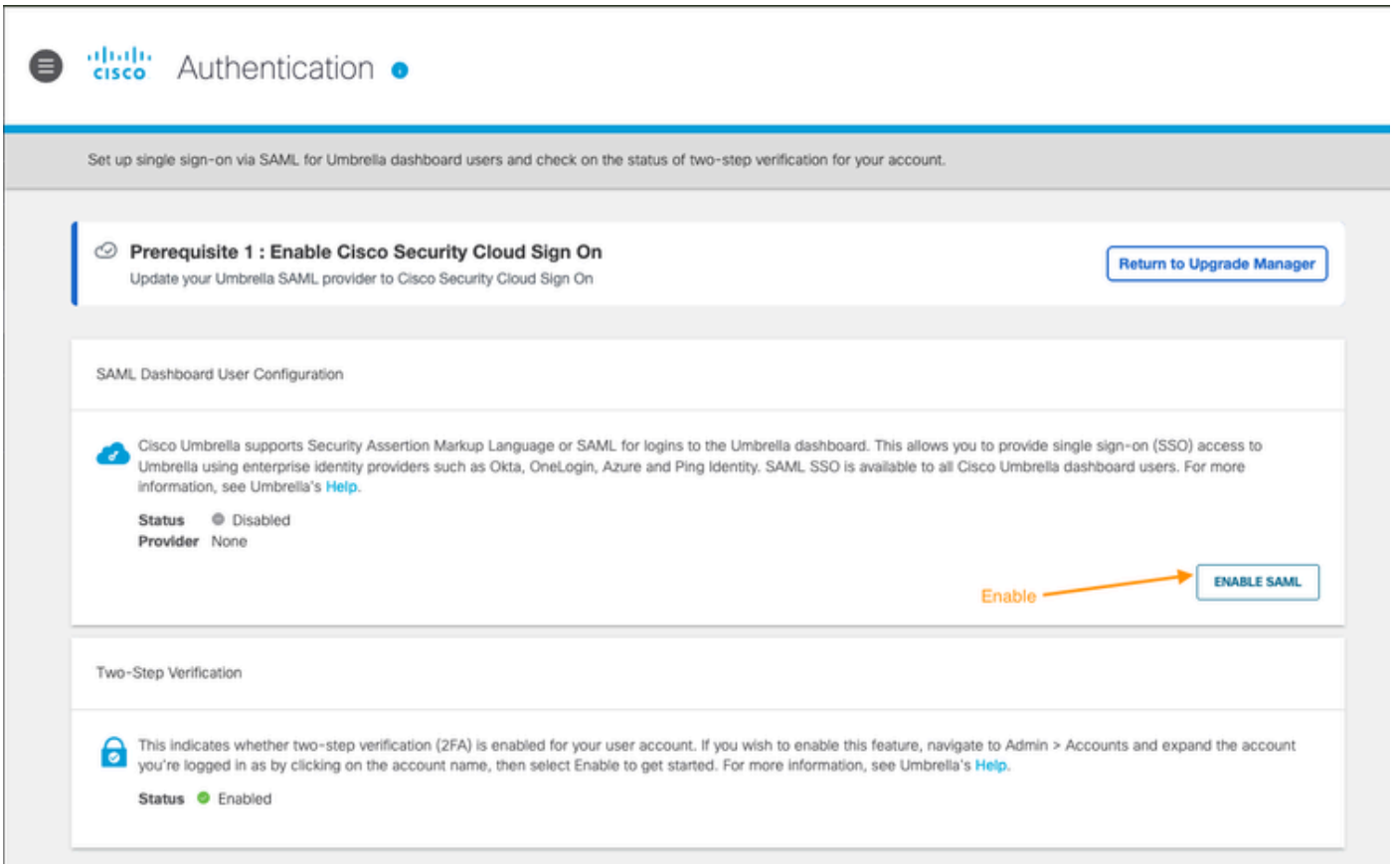
1. 使用與上面相同的帳戶重新登入到Umbrella。
2. 導航到新選單項Upgrade Manager:



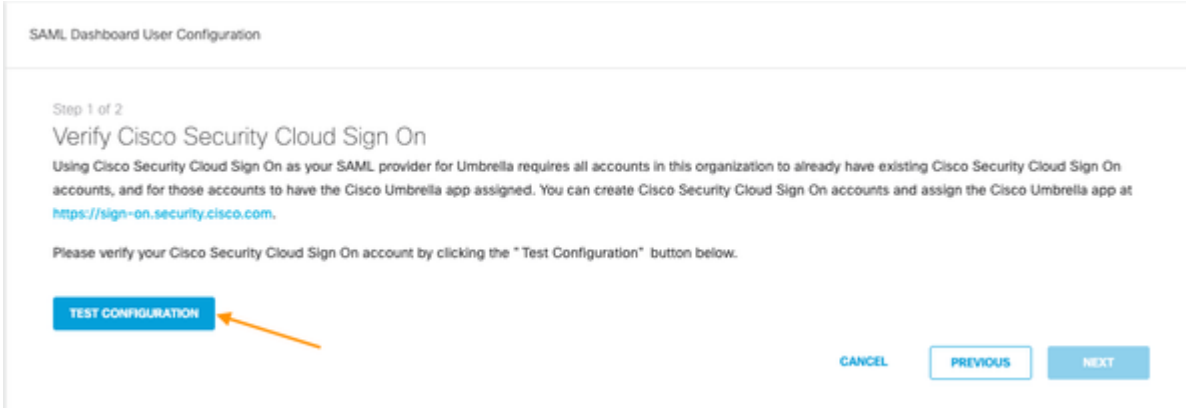
3.在Upgrade Manager頁面中，選擇Enable Cisco Security Cloud Sign on下的Start



4.在SAML儀表板使用者配置下選擇啟用SAML，以將SCC作為SAML提供程式連結以進行儀表板登入：

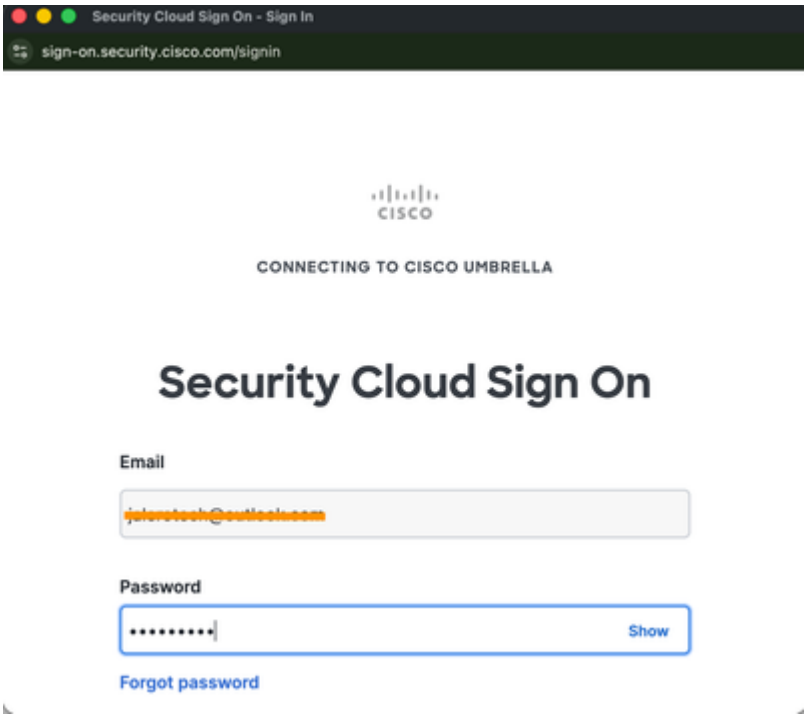


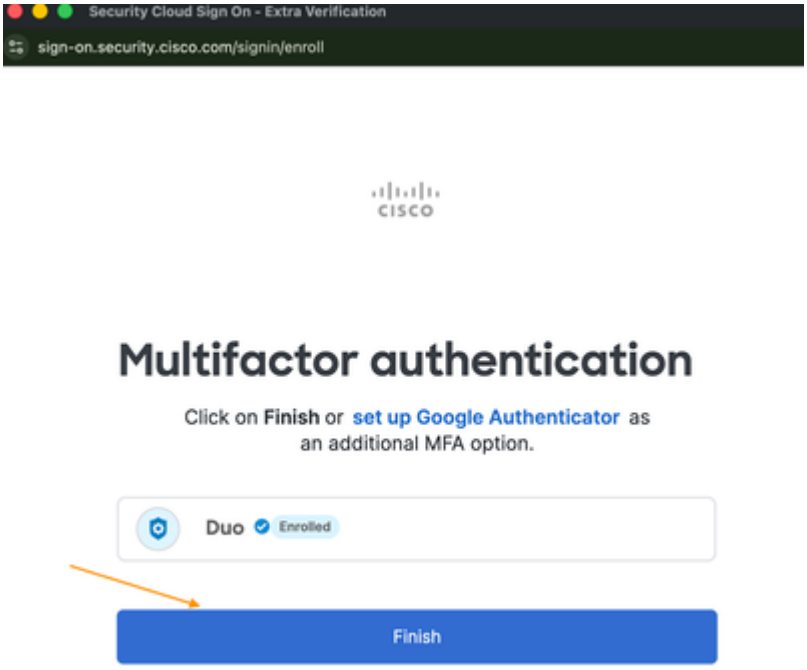
5.使用TEST CONFIGURATION選項測試SAML配置：



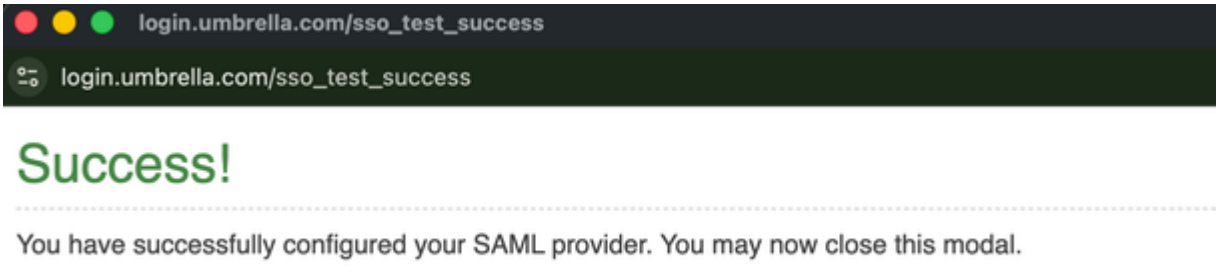
6. SCC的登入頁面必須出現在另一個彈出視窗中（確保已禁用彈出視窗阻止程式）：

出現提示時，使用您的SCC憑證登入。



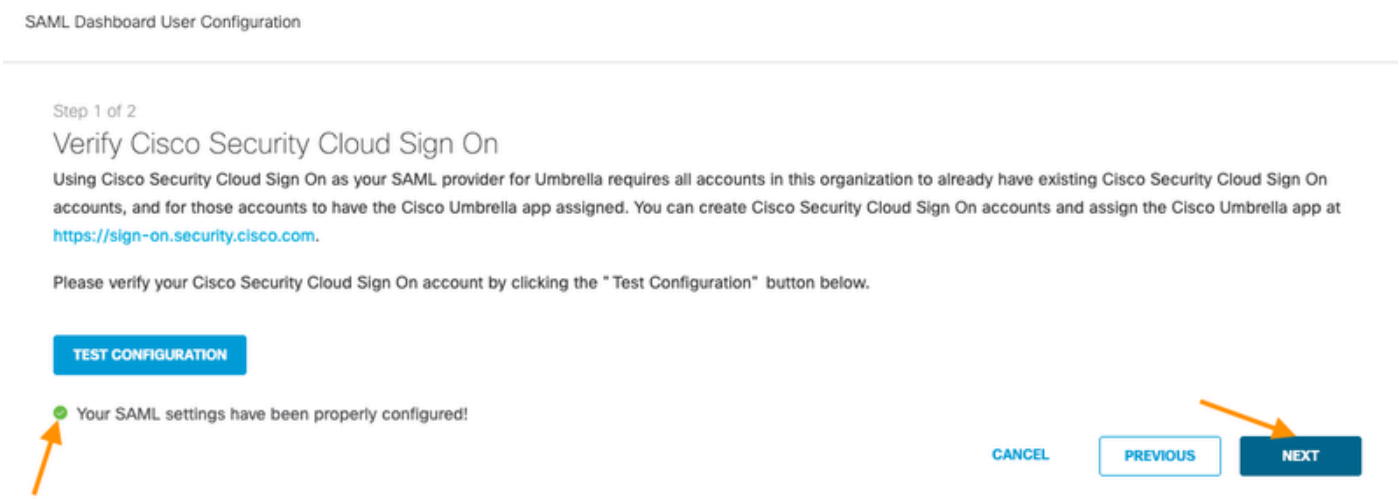


驗證登入後，您必須在此處獲取消息，並進行確認。此時SAML部分幾乎完成：

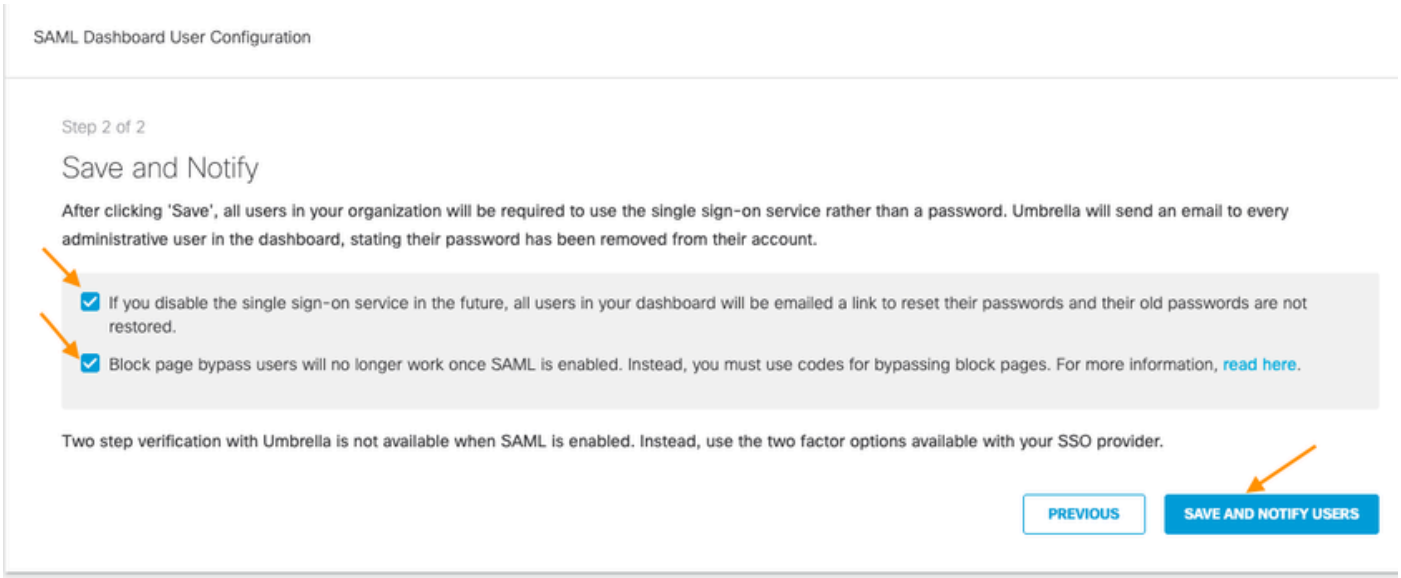


然後，必須再次返回到SAML儀表板使用者配置部分：

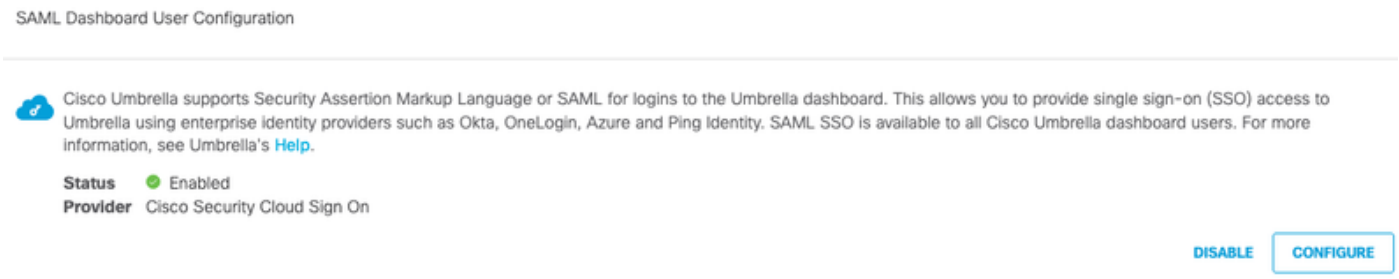
- 綠色勾選顯示已正確配置SAML設定
- 選擇NEXT繼續



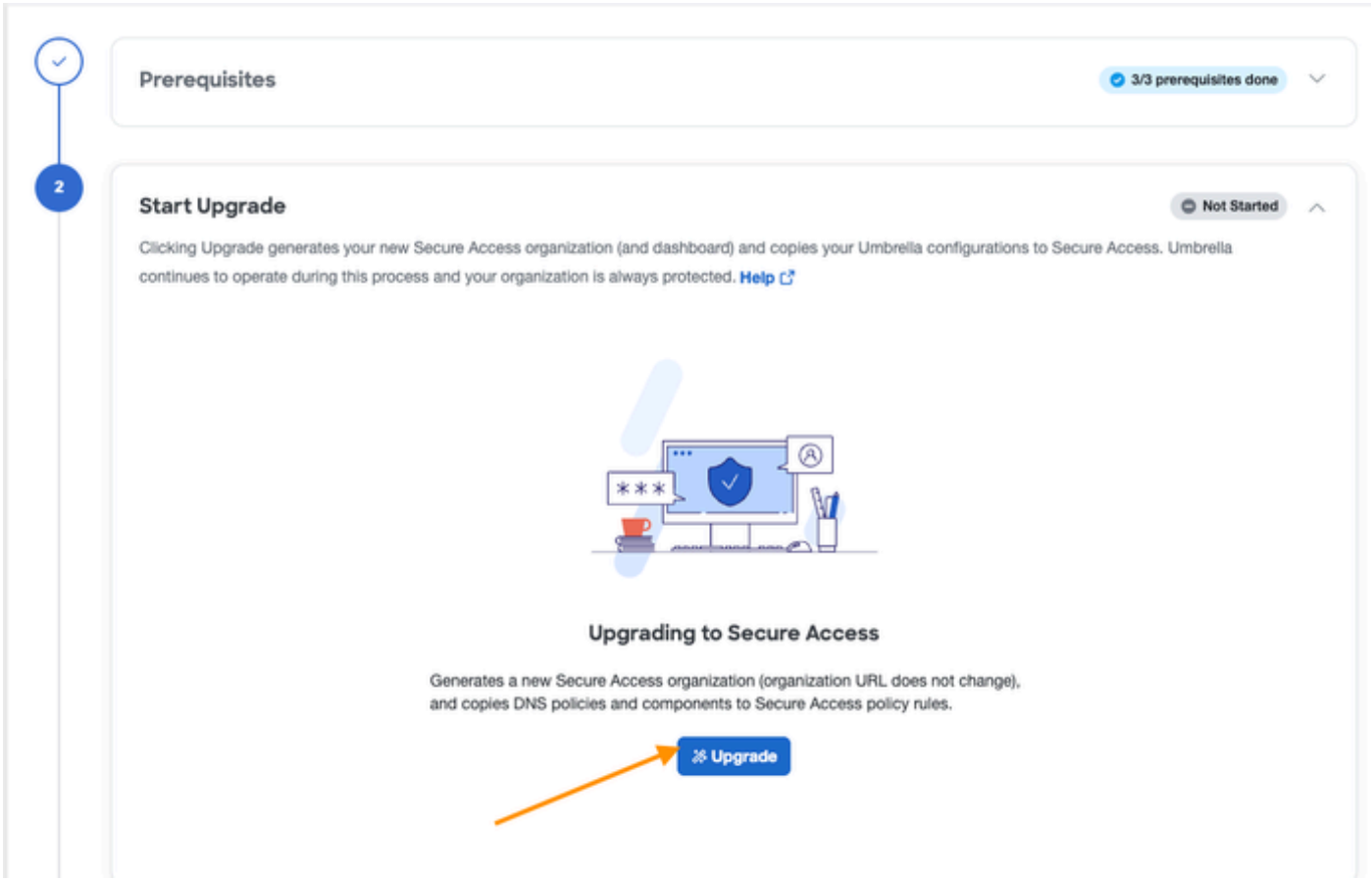
儲存更改並通知使用者：



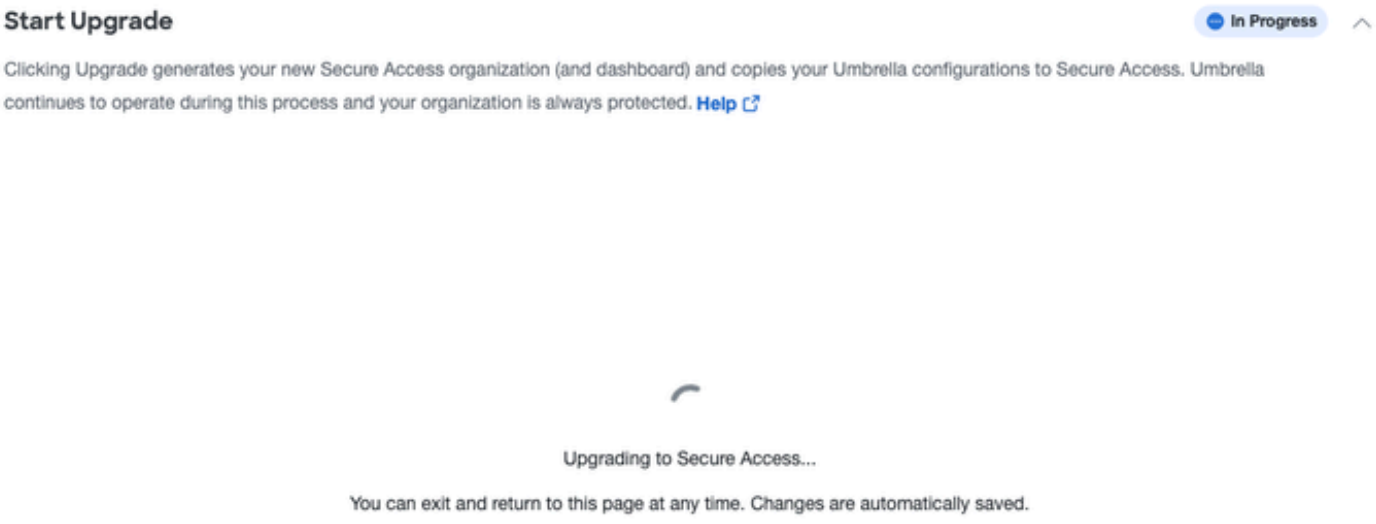
SAML配置已完成：



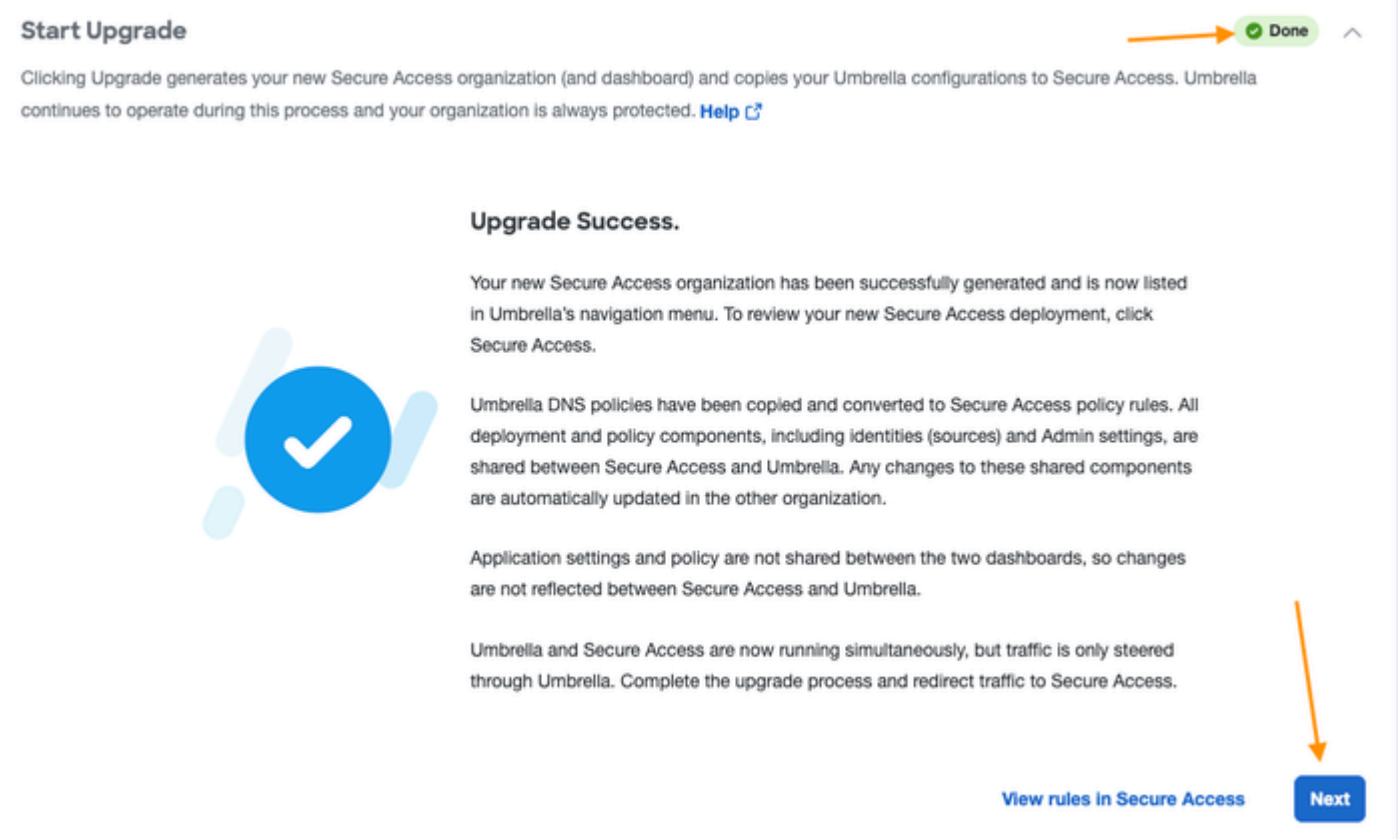
7.在開始升級部分中選擇升級，以升級到安全訪問：



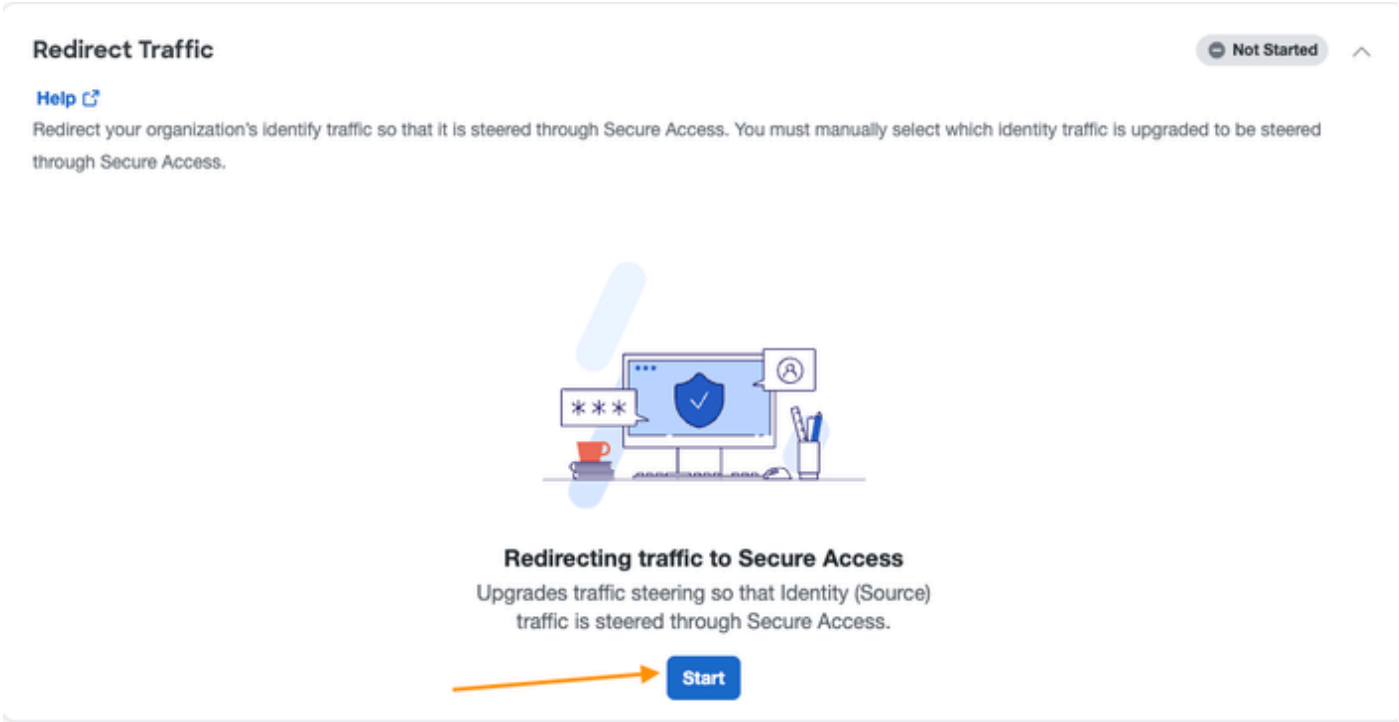
- 允許升級繼續：



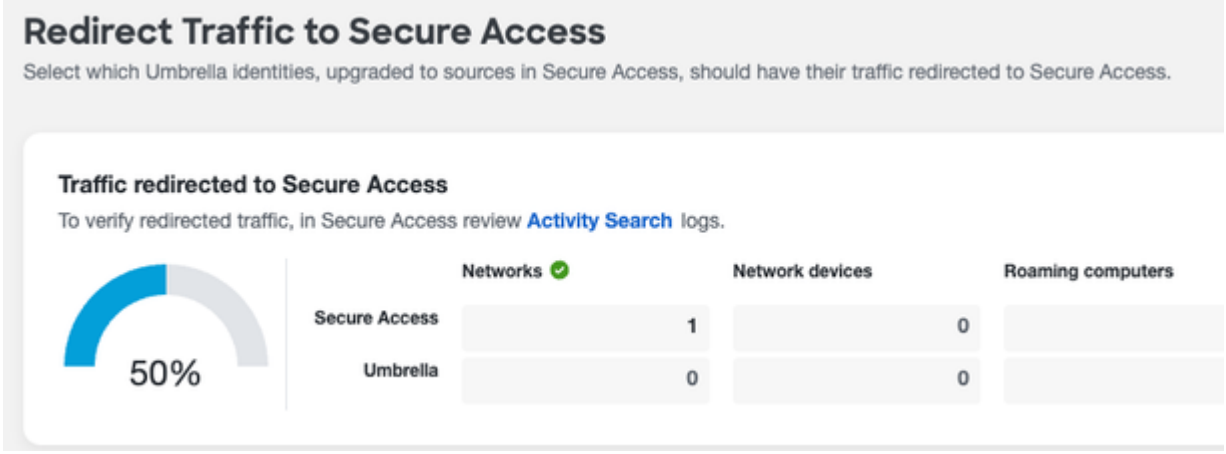
- 完成後，您必須在以下影象上獲得一個這樣的頁面：



8.將流量重定向到安全訪問



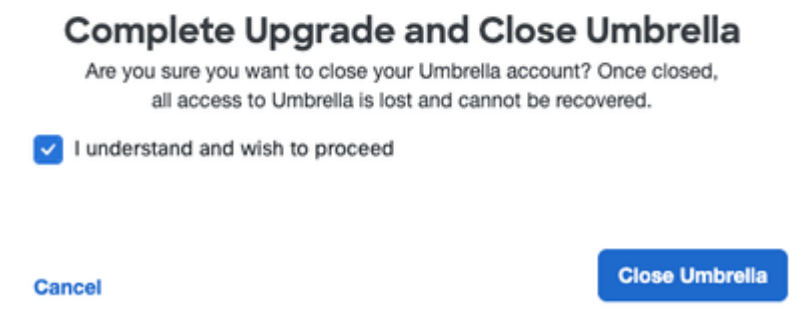
- 確認重新導向已完成。在示例中，只有網路身份從Umbrella遷移到Secure Access:



9.完成向Secure Access的升級和遷移

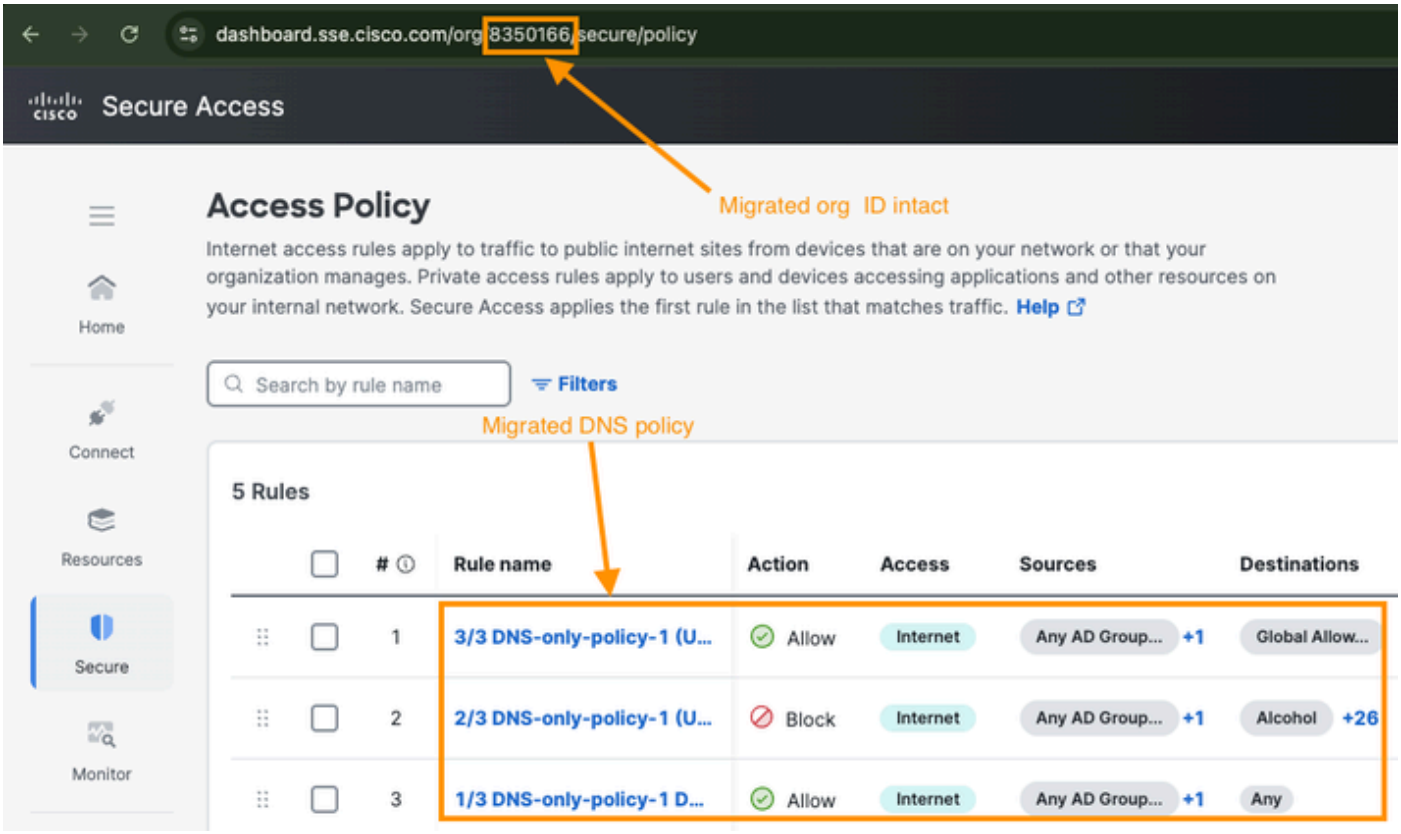
⚠ 注意：這將完全刪除您的Umbrella組織，並且不可撤銷，因此在執行此步驟之前，請確保所有專案都已完全遷移。

- 當您在此處的影象上選擇Close Umbrella時，您將在umbrella組織被刪除時失去對其的訪問許可權：



驗證遷移

1. 使用登入憑據登入Secure Access
2. 導航到安全>訪問策略以顯示遷移的規則，如下面的示例所示。組織ID必須與上面準備遷移部分的相同。



相關資訊

- Umbrella檔案
- 技術支援與文件 - Cisco Systems

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）。