通過LDAPS為安全網路分析管理器訪問配置外部身份驗證和授權

目錄

簡介

本檔案介紹安全網路分析管理員（前身為Stealthwatch管理中心）版本7.1或更高版本的基本設定，以使用外部驗證，並在7.2.1或更高版本中使用外部授權與LDAPS。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco Secure Network Analytics（前身為Stealthwatch）
- 常規LDAP和SSL操作
- 常規Microsoft Active Directory管理

採用元件

本檔案中的資訊是根據以下元件：

- 思科安全網路分析管理員（前身為SMC）版本7.3.2
- 配置為Active Directory域控制器的Windows Server 2016

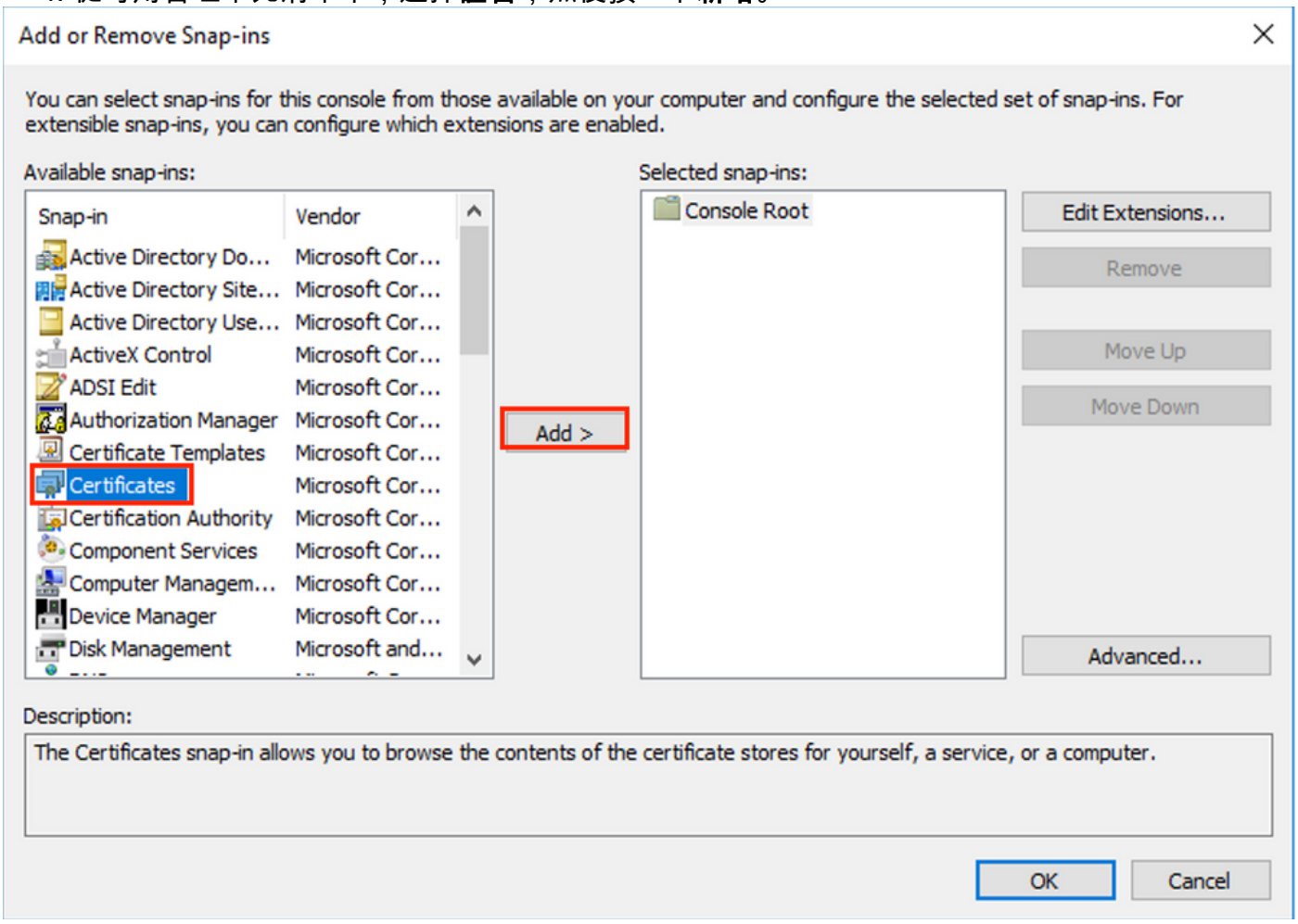
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設

）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。

設定

步驟A.登入到AD域控制器並匯出用於LDAP的SSL證書。

1. 對於Windows Server 2012或更高版本，從「開始」選單中選擇**運行**，然後輸入**certlm.msc**，然後繼續執行步驟8。
2. 對於較舊的Windows Server版本，從「開始」選單中選擇**「運行」**，然後輸入**mmc**。
3. 從「檔案」(File)選單中，選擇**「新增/刪除管理單元」(Add/Remove Snap In)**。
4. 從可用管理單元清單中，選擇**證書**，然後按一下**新增**。

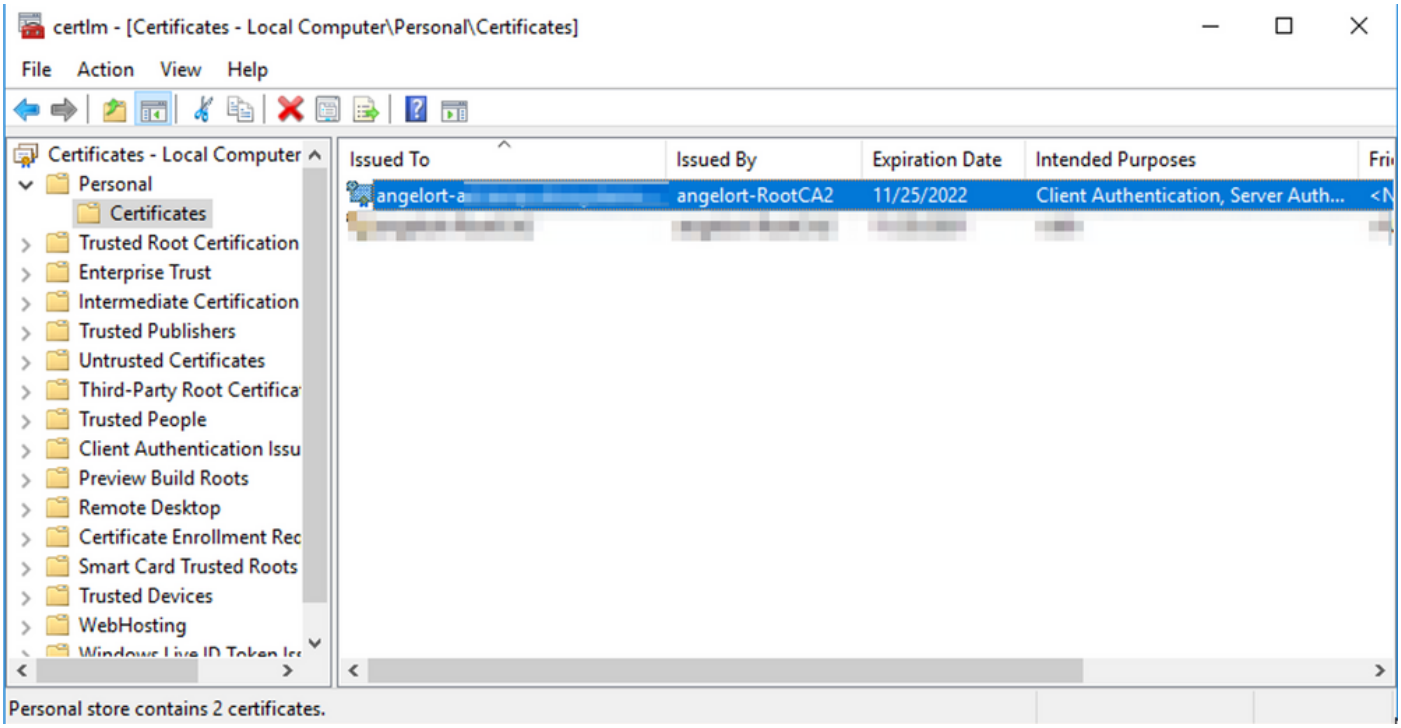


5.在**「證書」管理單元視窗**中，選擇**「電腦帳戶」**，然後選擇**「下一步」**。

6.保持選中**Local computer**，然後選擇**Finish**。

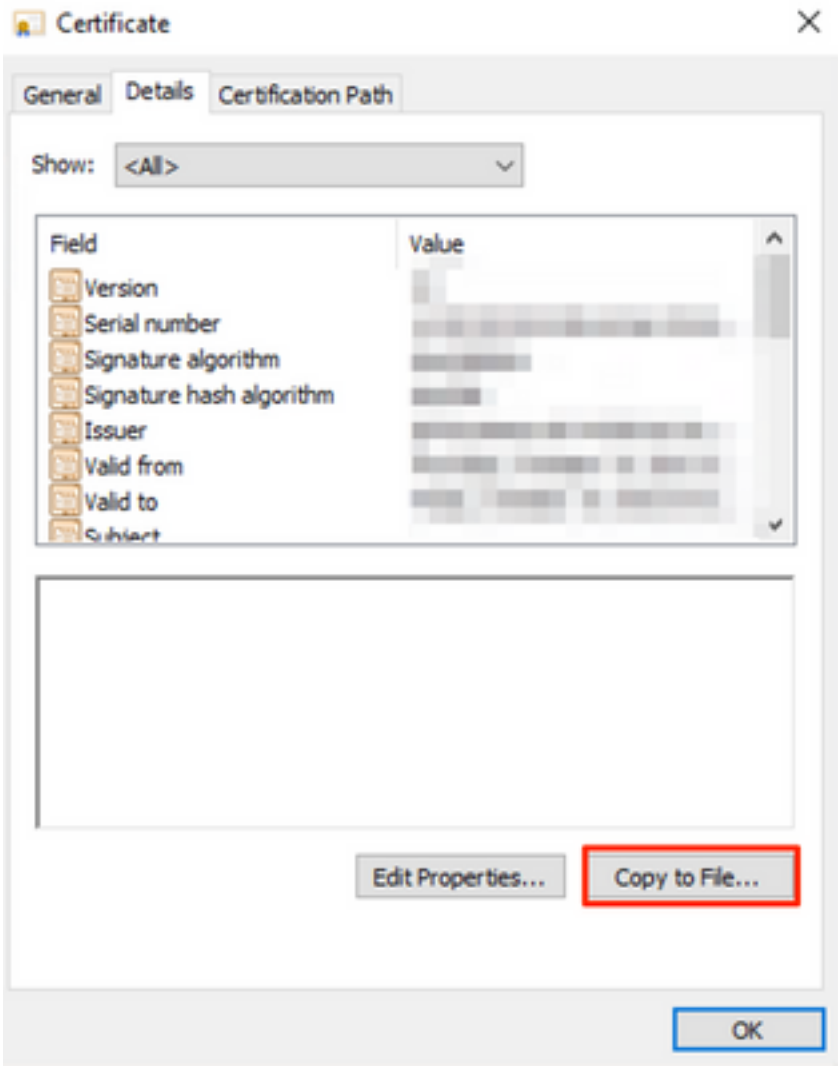
7.在「新增**或刪除管理單元」視窗中**，選擇**「確定」**。

8.導航到**證書（本地電腦）>個人>證書**



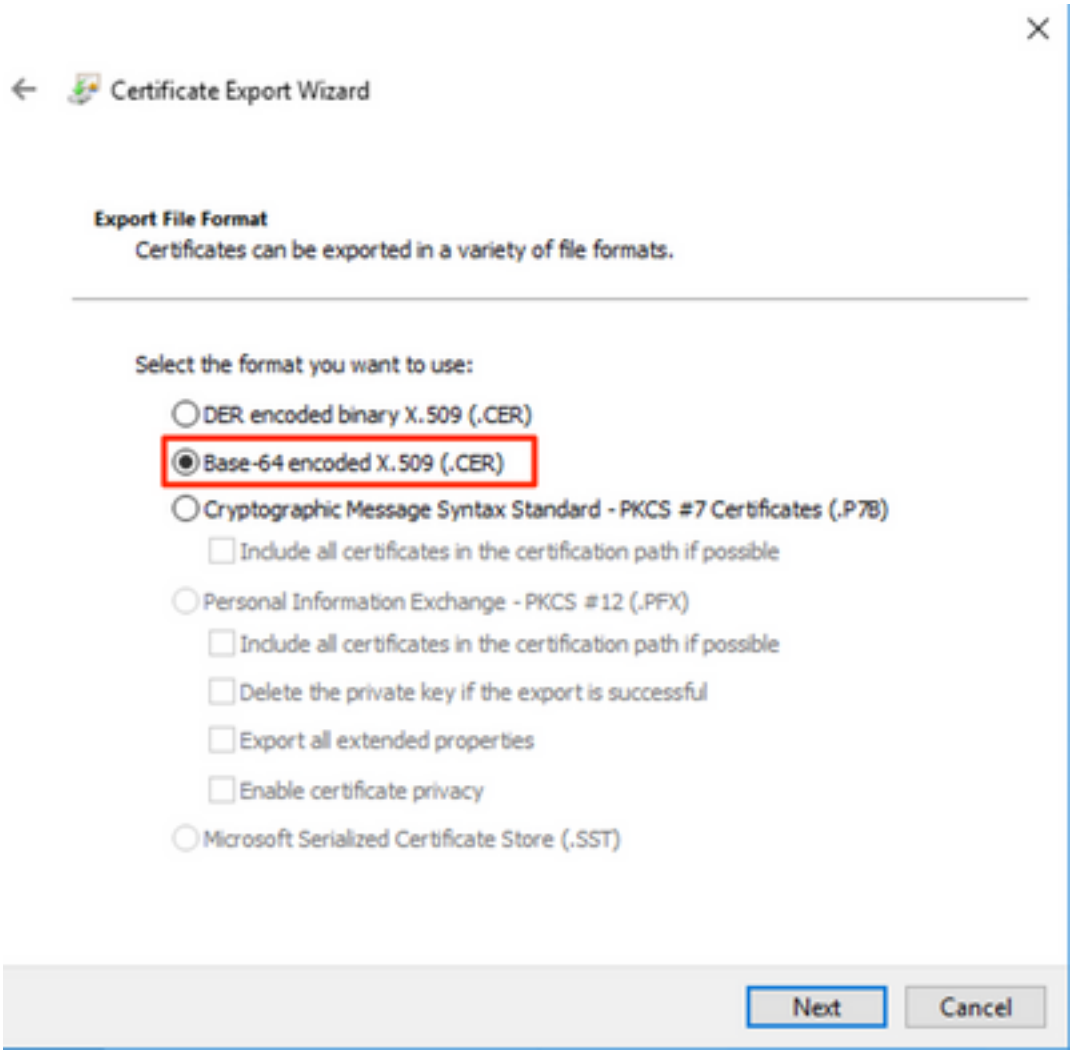
9.選擇並按一下右鍵域控制器上用於LDAPS身份驗證的SSL證書，然後按一下**開啟**。

10.定位至「詳細資訊」選**項卡**>按一下「複製**到檔案**」>「下一**步**」

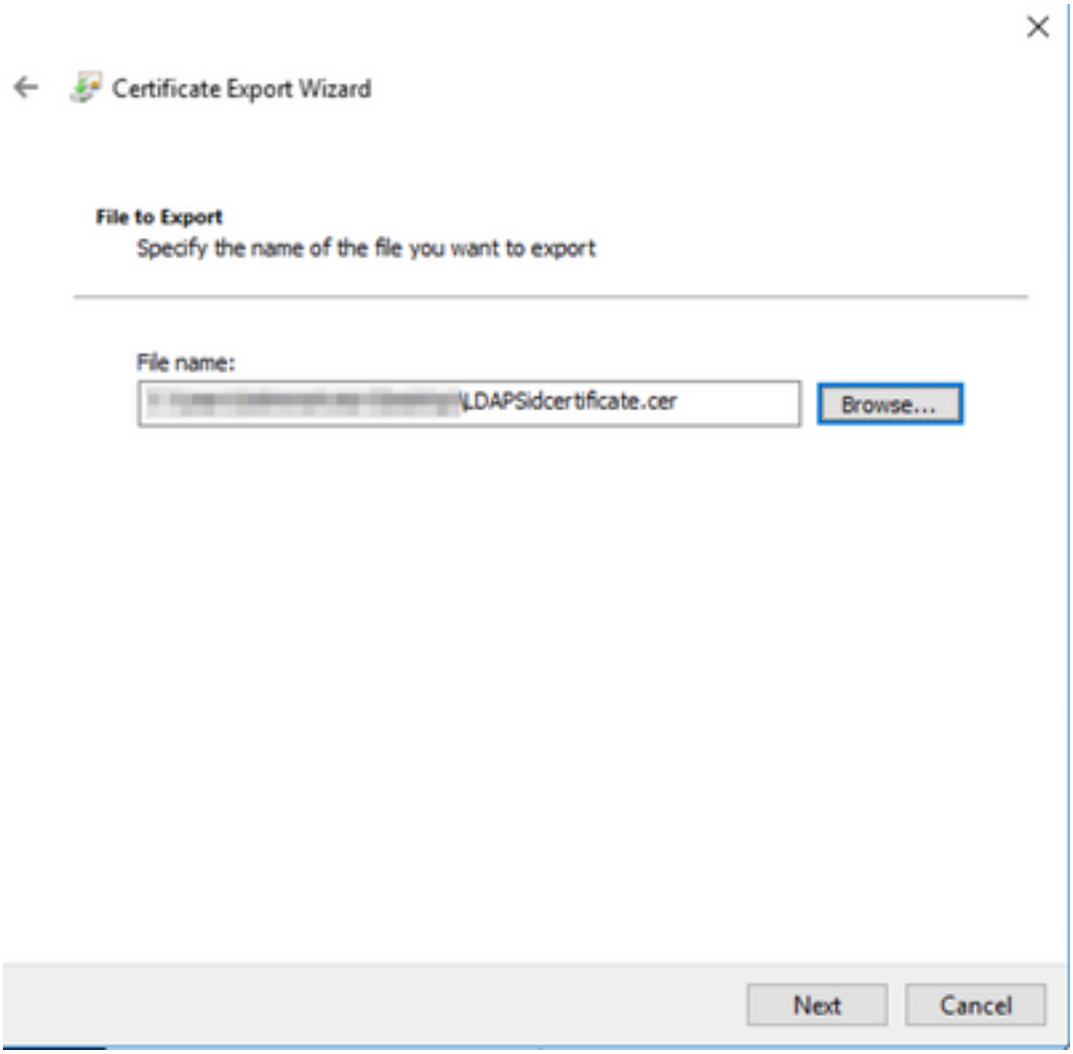


11.確保選中**No， do not export private key**，然後單擊**Next**

12.選擇**Base-64 encoded X.509** format，然後按一下**Next**。



13.選擇儲存證書的位置，命名檔案，然後按一下**下一步**。



14.按一下**Finish**，必須獲得「The export was successful」（匯出成功）。 消息。

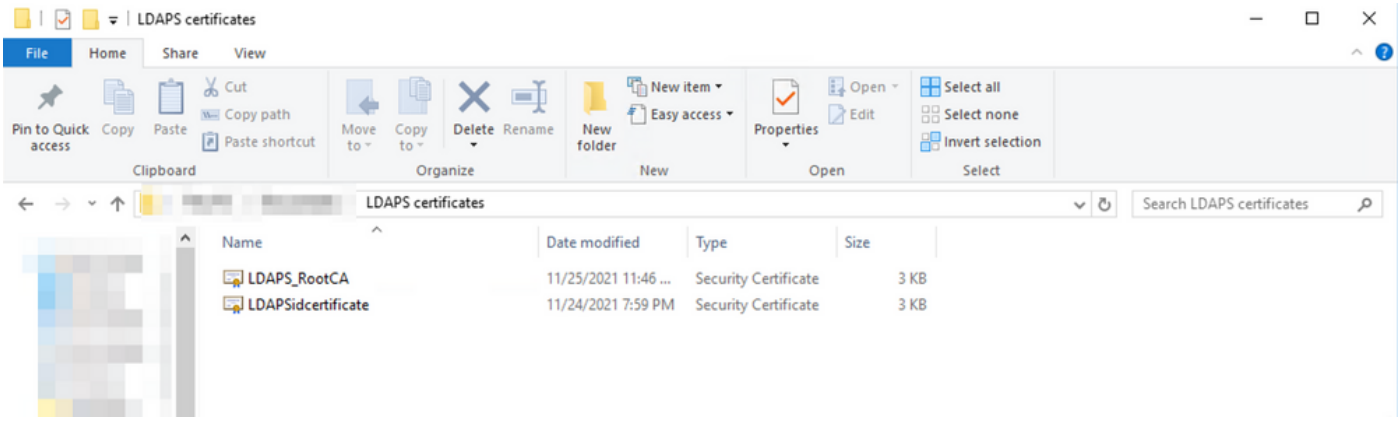
15.返回用於LDAPS的證書，然後選擇**Certification Path**頁籤。

16.選擇證書路徑頂部的根CA頒發者，然後按一下**View Certificate**。

17.重複步驟10-14以匯出對用於LDAPS身份驗證的證書進行簽名的根CA的證書。

> **附註**：您的部署可以具有多層CA層次結構，在這種情況下，您需要遵循相同的過程匯出信任鏈中的所有中間證書。

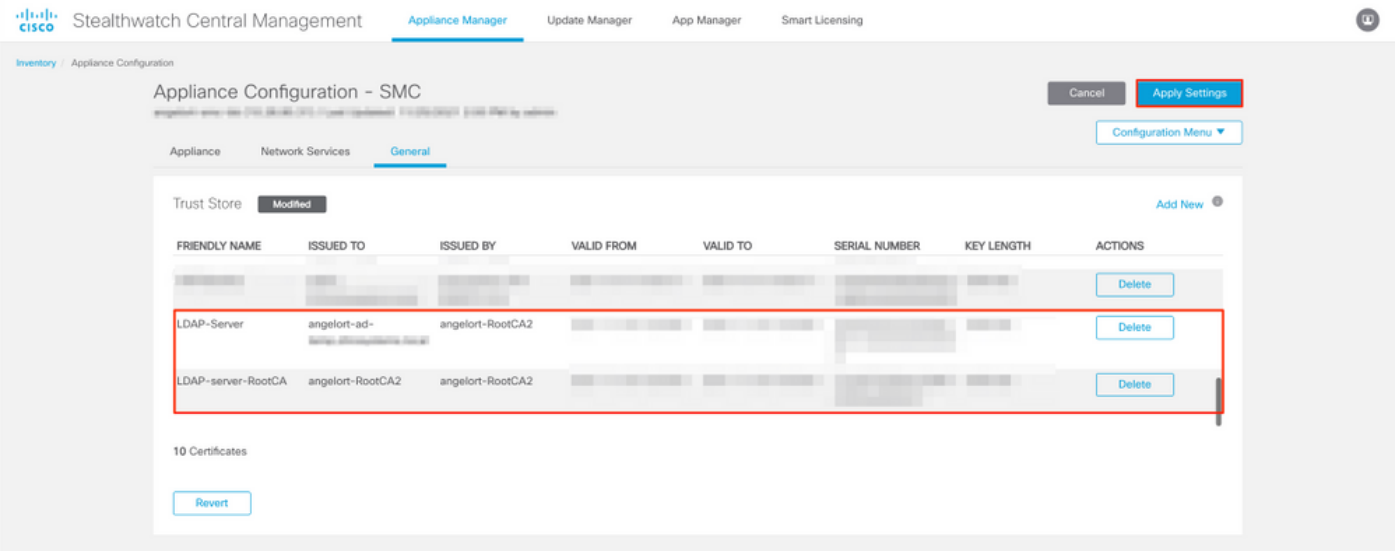
18.繼續之前，請確保LDAPS伺服器和證書路徑中的每個頒發機構都有一個證書檔案：根憑證和中間憑證（如果適用）。



步驟B.登入到SNA Manager以新增LDAP伺服器的證書和根鏈。

1. 導航到**Central Management** > Inventory。

2. 找到SNA Manager裝置，然後按一下**操作 > 編輯裝置配置**。
3. 在Appliance Configuration視窗中，導航至**Configuration Menu > Trust Store > Add New**。
4. 鍵入友好名稱，按一下**選擇檔案**並選擇LDAP伺服器的證書，然後按一下**新增證書**。
5. 重複上一步新增根CA證書和中間證書（如果適用）。
6. 確認上傳的憑證是否正確，然後按一下「**Apply Settings**」。

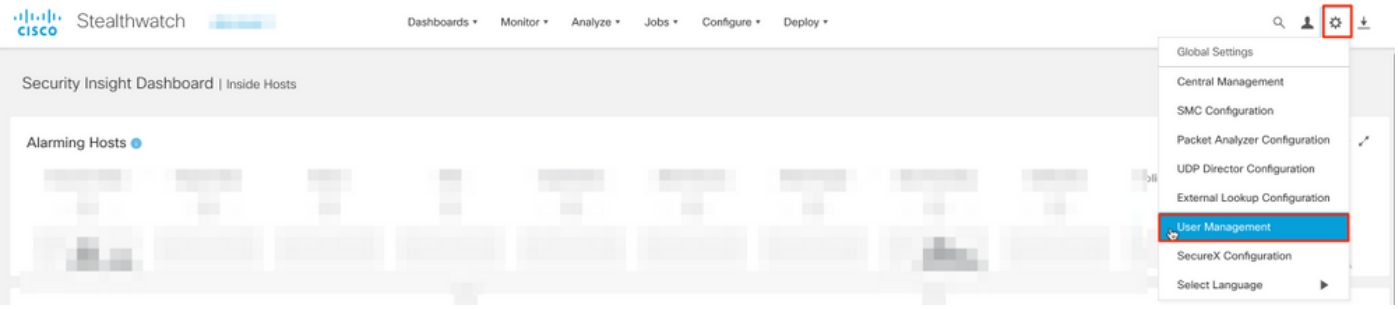


7.等待應用更改，並等待Manager狀態變為**Up**。

步驟C.新增LDAP外部服務配置。

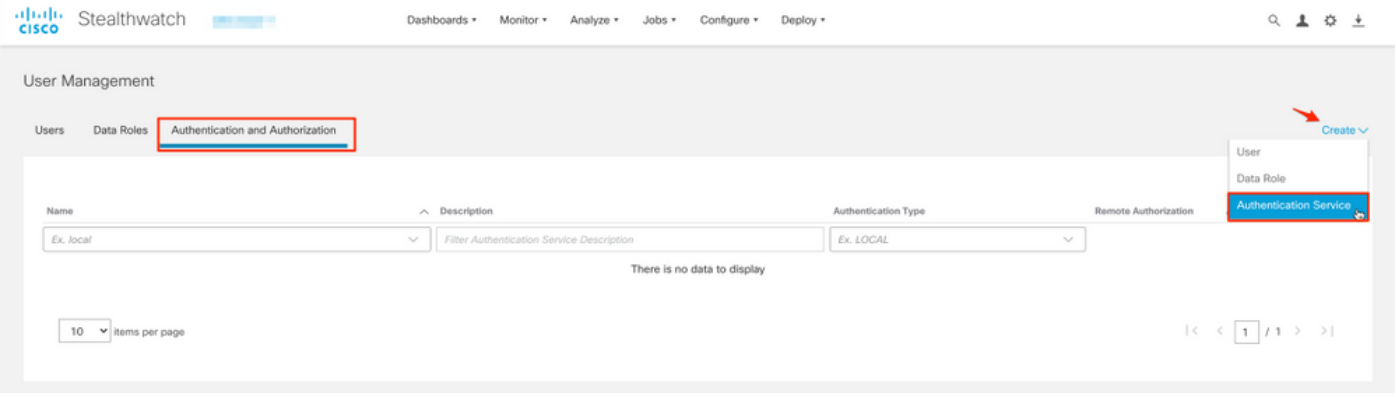
SNA 7.2或更高版本

1.開啟Manager主控制面板，然後導航至**全域性設定 > 使用者管理**。



2.在「使用者管理」視窗中，選擇**Authentication and Authorization選**項卡。

3.按一下**建立 > 身份驗證服務**。

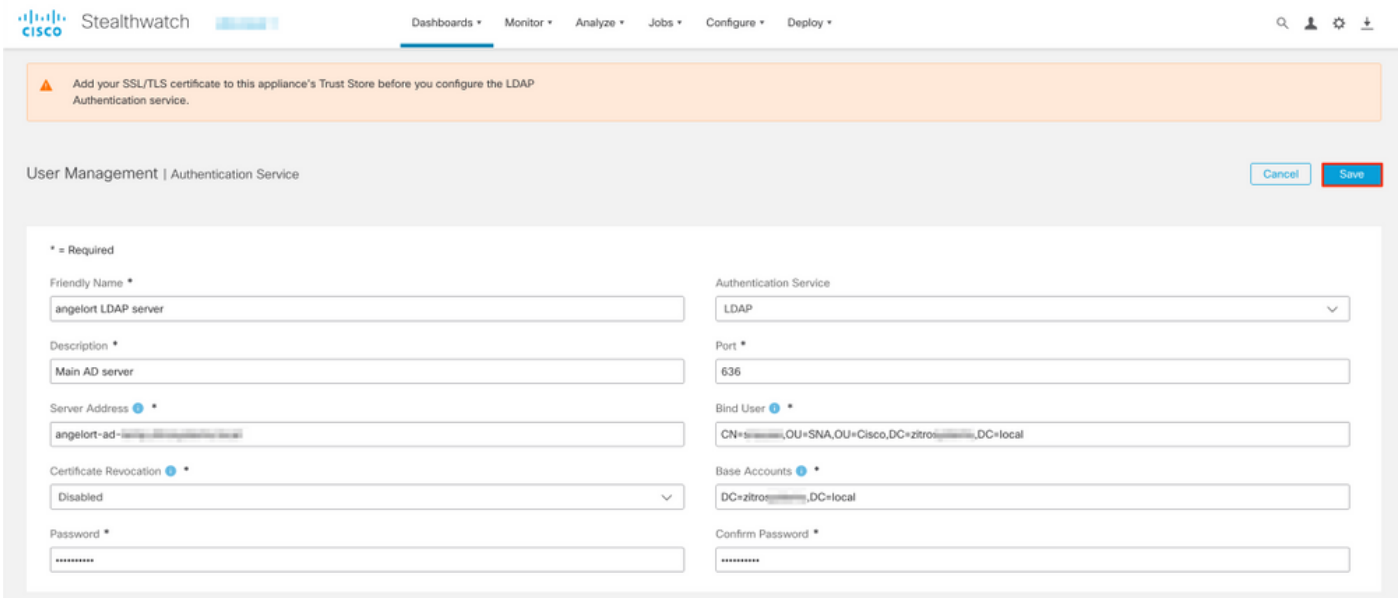


4.從**Authentication Service**下拉選單中選擇**LDAP**。

5.填寫必填欄位。

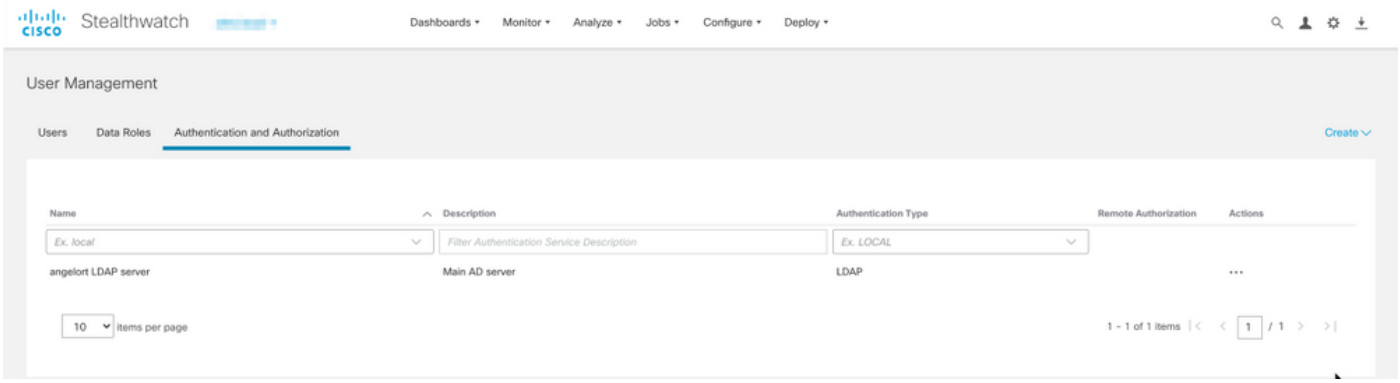
欄位	**備註**
友好名稱	輸入LDAP伺服器的名稱。
說明	輸入LDAP伺服器的說明。
伺服器位址	**輸入在LDAP伺服器證書的Subject Alternative Name(SAN)欄位中指定的完全限定的域名。** • 如果SAN欄位僅包含IPv4地址，請在Server Address欄位中輸入IPv4地址。 • 如果SAN欄位包含DNS名稱，請在Server Address欄位中輸入DNS名稱。 • 如果SAN欄位同時包含DNS和IPv4值，請使用的第一個值。
連接埠	輸入為安全LDAP通訊（通過TLS的LDAP）指定的LDAPS的公認TCP埠是636。
繫結使用者	輸入用於連線到LDAP伺服器的使用者ID。例如：CN=admin，OU=Corporate Users，DC=example，DC=com **附註**：如果將使用者新增到內建AD容器（例，「使用者」），則繫結使用者的繫結DN必規範名稱(CN)設定為內建資料夾（例如，CN=username， CN=Users， DC=domaiDC=com）。 但是，如果已將使用者新增到器，則繫結DN必須將組織單位(OU)設定為新名稱（例如，CN=username， OU=CorporatUsers， DC=domain， DC=com）。 **附註**：查詢繫結使用者的繫結DN的一個有用是查詢與Active Directory伺服器連線的WindoServer上的Active Directory。若要獲取此資訊，您可以開啟Windows命令提示符並鍵入命令**dsquery user dc=<distinguished>,dc=<name name <user>**。例如： **dsquery user dc=example，dc=com -name user1**。結果類CN=user1,OU=Corporate Users，DC=example，DC=com」
密碼	輸入用於連線到LDAP伺服器的繫結使用者密碼。
基本帳戶	輸入唯一判別名(DN)。 DN適用於必須開始搜尋使用者的目錄分支。它通常於目錄樹（您的域）的頂部，但是您也可以在目錄定子樹。「繫結使用者」和要進行身份驗證的使用須可從基本帳戶訪問。 例如：DC=example，DC=com

6.按一下**儲存**。



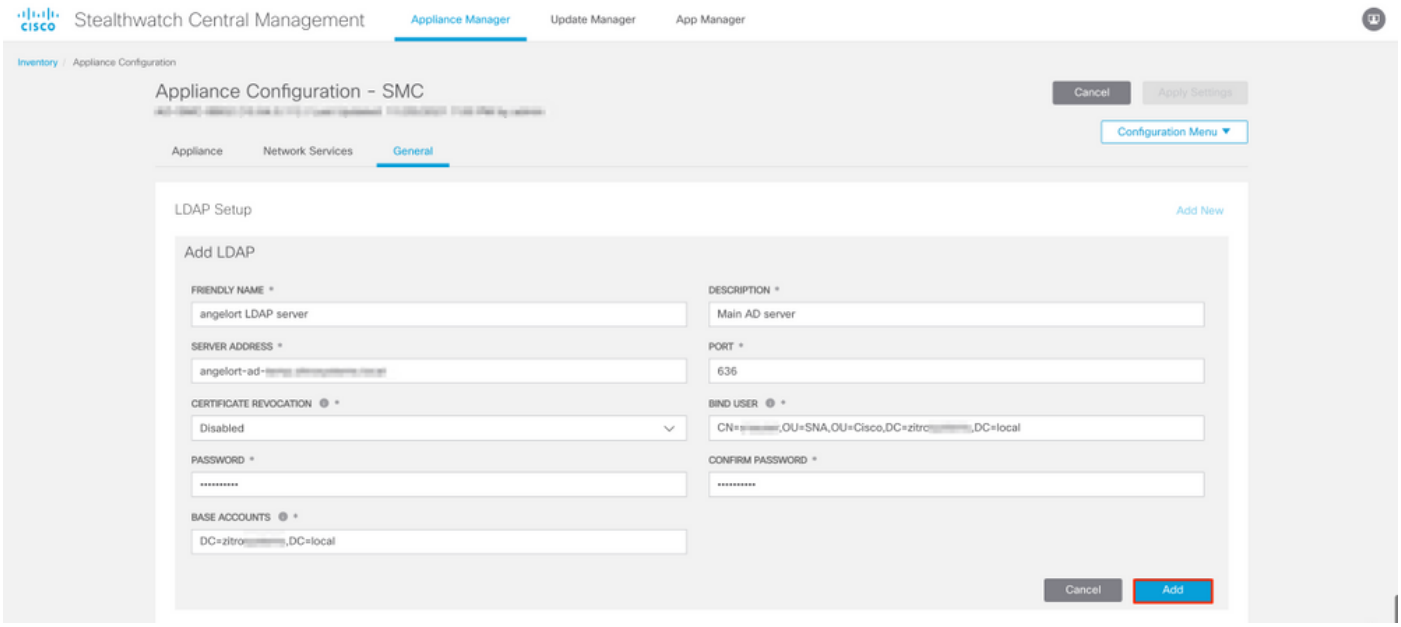
7.如果輸入的設定和新增到信任儲存的證書正確，您必須收到「您已成功儲存更改」的橫幅。

8.已配置的伺服器必須顯示在**User Management > Authentication and Authorization**下。



SNA版本7.1

1. 導航到**Central Management** > Inventory。
2. 找到SMC裝置，然後按一下**操作 > 編輯裝置配置**。
3. 在Appliance Configuration視窗中，導航到**Configuration Menu > LDAP Setup > Add New**。
4. 按照**SNA 7.2版或更高版本中的說明完成**必填欄位，步驟5。



5.按一下**Add**。

6.按一下**應用設定**。

7.一旦輸入的設定和新增到信任儲存的證書正確無誤，就會應用Manager上的更改，並且裝置狀態必須為**Up**。

步驟D.配置授權設定。

SNA同時支援通過LDAP進行的本地和遠端授權。通過此配置，AD伺服器的LDAP組對映到內建或自定義SNA角色。

通過LDAP支援SNA的身份驗證和授權方法有：

- 遠端身份驗證和本地授權
- 遠端身份驗證和遠端授權（僅支援SNA 7.2.1版或更高版本）

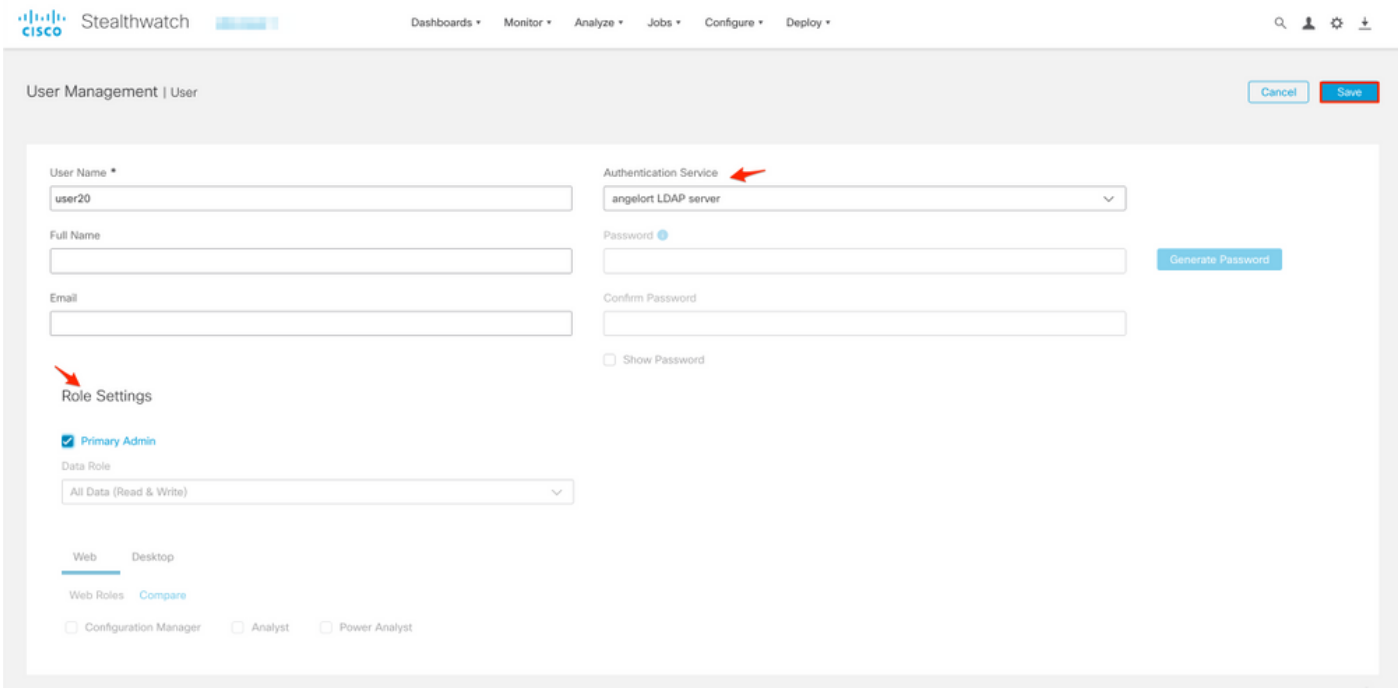
本地授權

在這種情況下，需要在本地定義使用者及其角色。為此，請按照以下步驟操作。

1.再次定位至**使用者管理**，按一下**使用者**標籤**> 建立 > 使用者**。

2.定義要使用LDAP伺服器進行身份驗證的使用者名稱，並從**Authentication Service**下拉選單中選擇配置的伺服器。

3.定義經LDAP伺服器驗證後，使用者對Manager必須擁有的許可權，然後按一下**Save**。



通過LDAP進行遠端授權

Secure Network Analytics 7.2.1版首次支援通過LDAP進行遠端身份驗證和授權。

> **附註**：7.1版不支援使用LDAP進行遠端授權。

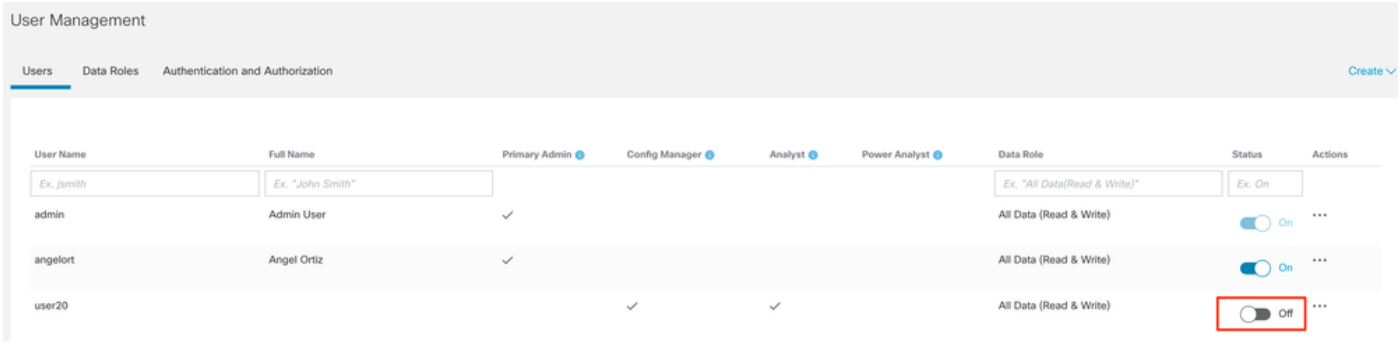
需要提及的是，如果使用者是在本地（在Manager中）定義和啟用的，則使用者是遠端身份驗證的，但在本地授權。使用者選擇過程如下：

1. 在Manager的歡迎頁上輸入憑據後，Manager將查詢具有指定名稱的本地使用者。
2. 如果找到本地使用者並啟用該使用者，則遠端驗證該使用者（如果之前配置了具有本地授權的LDAP遠端驗證），但使用本地設定進行授權。
3. 如果已配置和啟用遠端授權，且未在本地找到使用者（未配置或禁用），則遠端執行身份驗證和授權。

因此，成功配置遠端身份驗證的步驟是：

步驟D-1.禁用或刪除打算使用遠端授權但在本地定義的使用者。

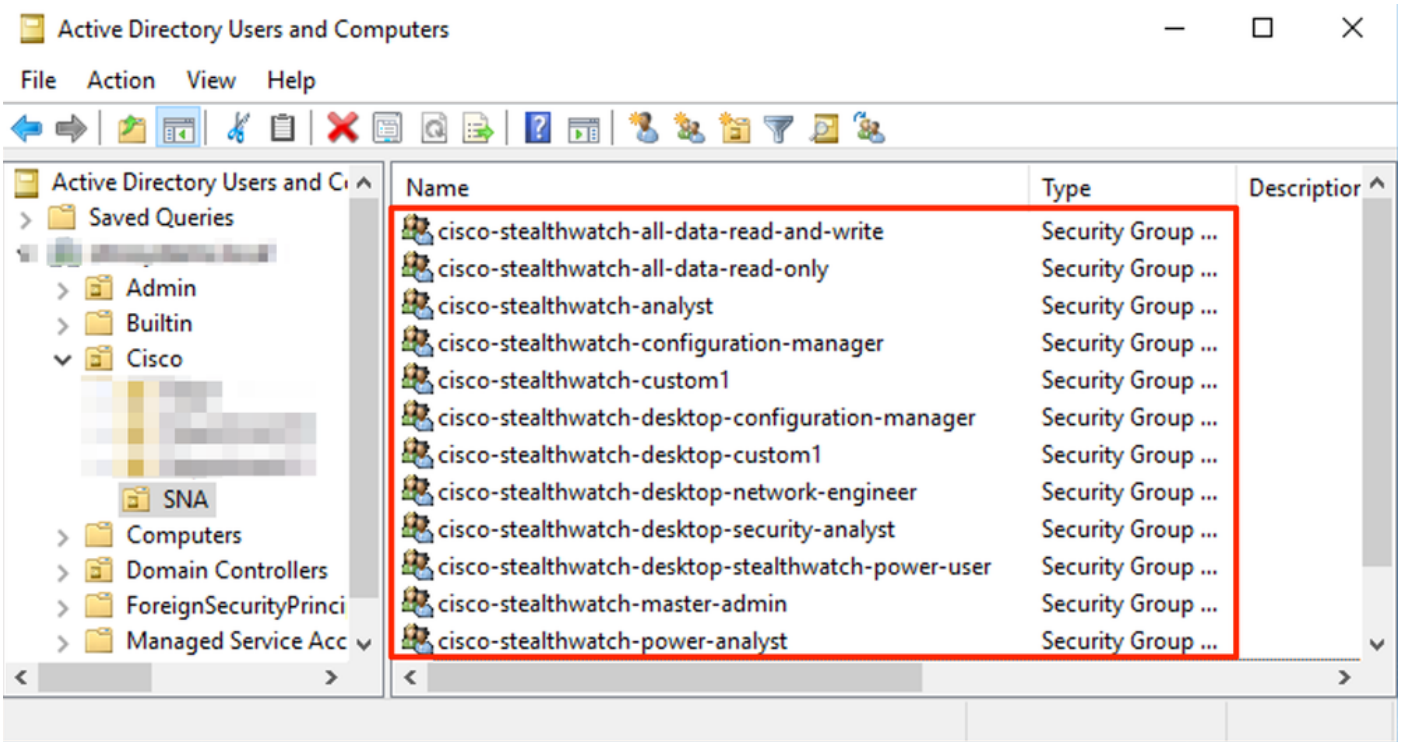
1. 開啟Manager主儀表板並導航到Global Settings > User Management。
2. 禁用或刪除通過LDAP使用遠端身份驗證和授權的使用者（如果存在），但是這些使用者是在本地配置的。



步驟D-2.在Microsoft AD伺服器中定義cisco-stealthwatch組。

對於通過LDAP使用者的外部身份驗證和授權，密碼和*cisco-stealthwatch*組在Microsoft Active Directory中遠端定義。要在AD伺服器中定義的*cisco-stealthwatch*組與SNA具有的不同角色相關，它們必須定義如下。

SNA角色	組名稱
主管理員	• cisco-stealthwatch-master-admin • cisco-stealthwatch-all-data-read-and-write • cisco-stealthwatch-all-data-read-only • cisco-stealthwatch-<custom>（可選） **附註**：確保自定義資料角色組以「cisco-stealthwatch —」開頭。
資料角色	
Web功能角色	• cisco-stealthwatch-configuration-manager • cisco-stealthwatch-power-analyst • cisco-stealthwatch-analyst • cisco-stealthwatch-desktop-stealthwatch-pow user • cisco-stealthwatch-desktop-configuration-ma • cisco-stealthwatch-desktop-network-enginee
案頭功能角色	• cisco-stealthwatch-desktop-security-analyst • cisco-stealthwatch-desktop-<custom>（可選 **附註**：確保自定義案頭功能角色組以「cisco-stealthwatch-desktop —」開頭。

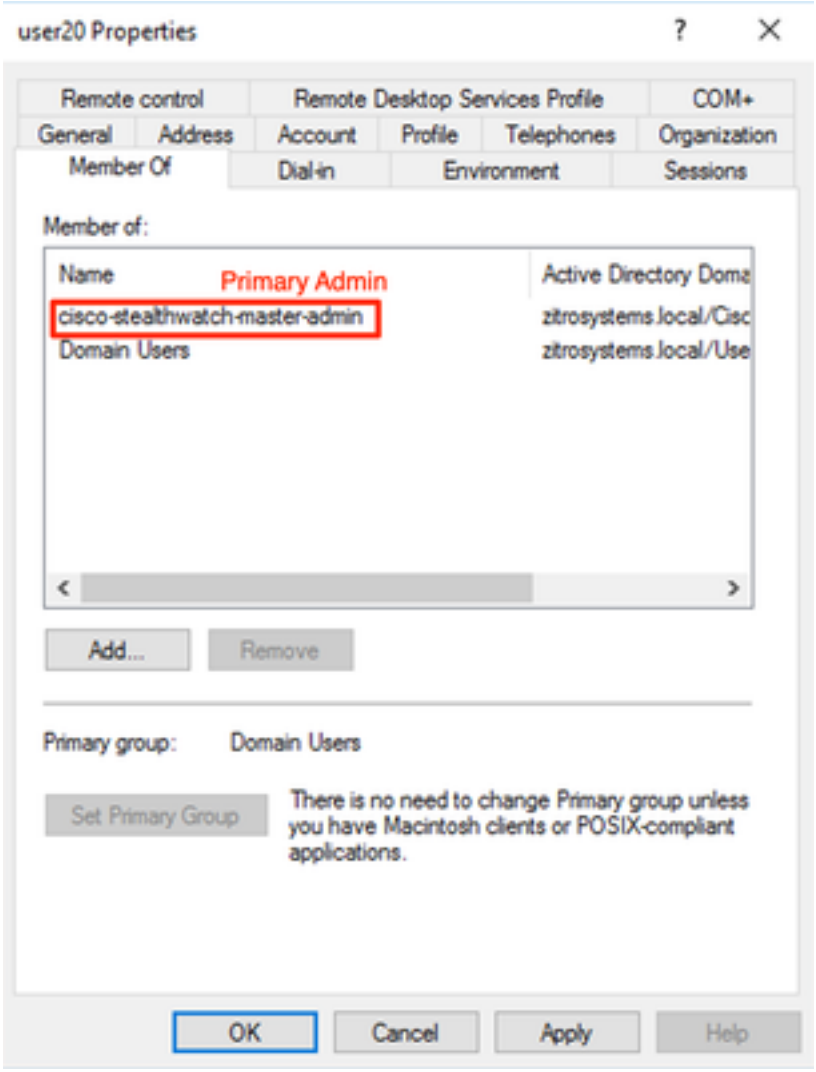


附註：如前所述，只要組名前面有正確的字串，則支援「資料角色」和「案頭功能角色」自定義組。必須在SNA Manager和Active Directory伺服器中定義這些自定義角色和組。例如，如果您在SNA Manager中為案頭客戶端角色定義自定義角色「custom1」，則必須將其對映到Active Directory中的cisco-stealthwatch-desktop-custom1。

步驟D-3.定義使用者的LDAP授權組對映。

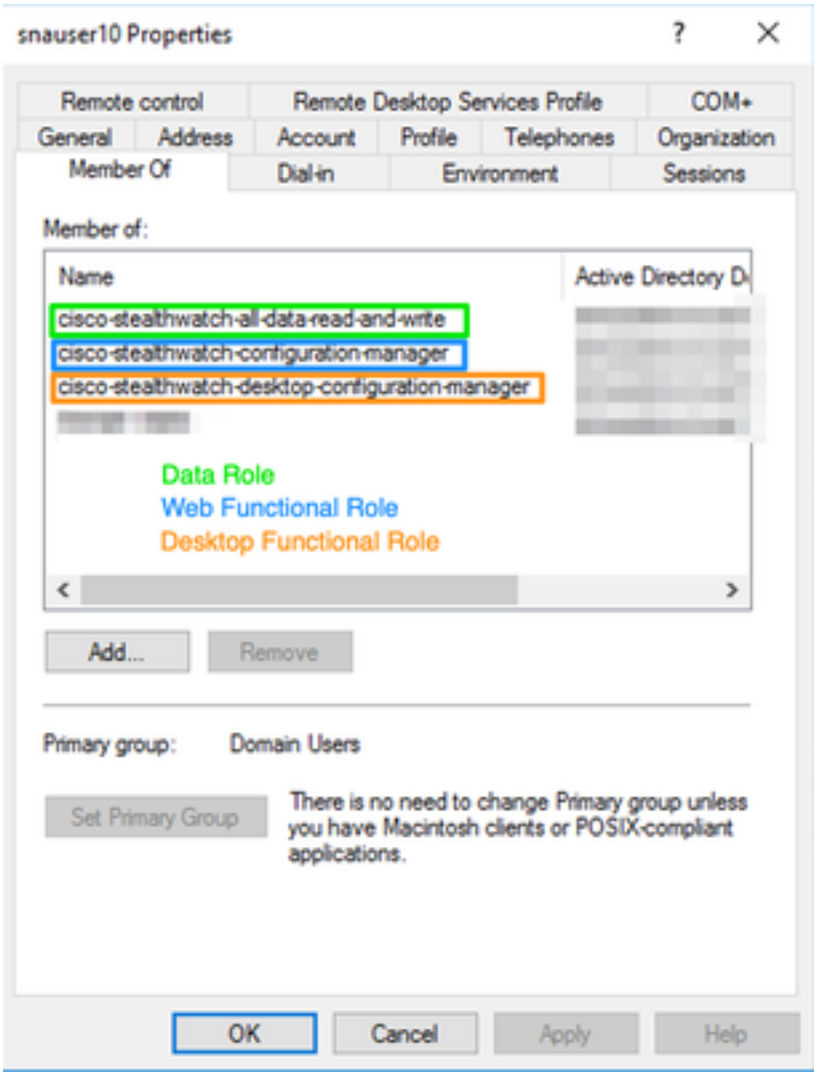
在AD伺服器中定義*cisco-stealthwatch*組後，我們可以將想要訪問SNA Manager的使用者對映到必要的組。必須按以下步驟操作。

- **Primary Admin**使用者必須分配給*cisco-stealthwatch-master-admin*組，且不能是任何其他*cisco-stealthwatch*組的成員。



- 除主管理員使用者以外的每個使用者都必須分配到具有下一個條件的每個角色組。

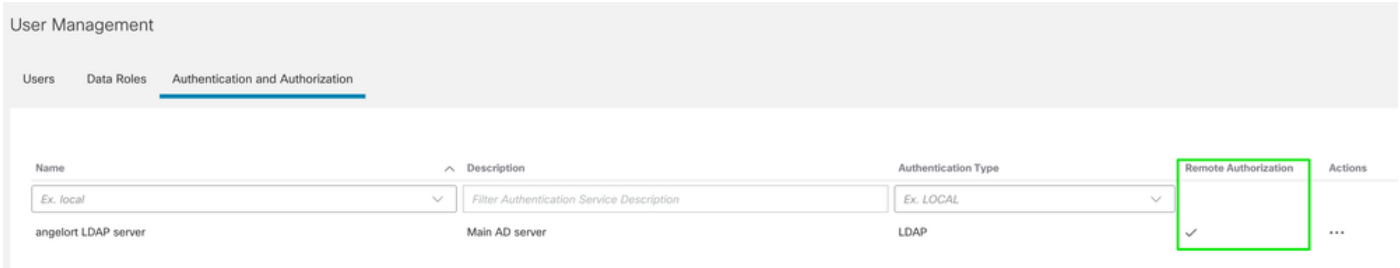
1. **資料角色**:使用者必須僅分配**到一個組**。
2. **Web功能角色**:必須將使用者分配至**至少一個組**。
3. **案頭功能角色**:必須將使用者分配至**至少一個組**。



步驟D-4.在SNA管理器上通過LDAP啟用遠端授權。

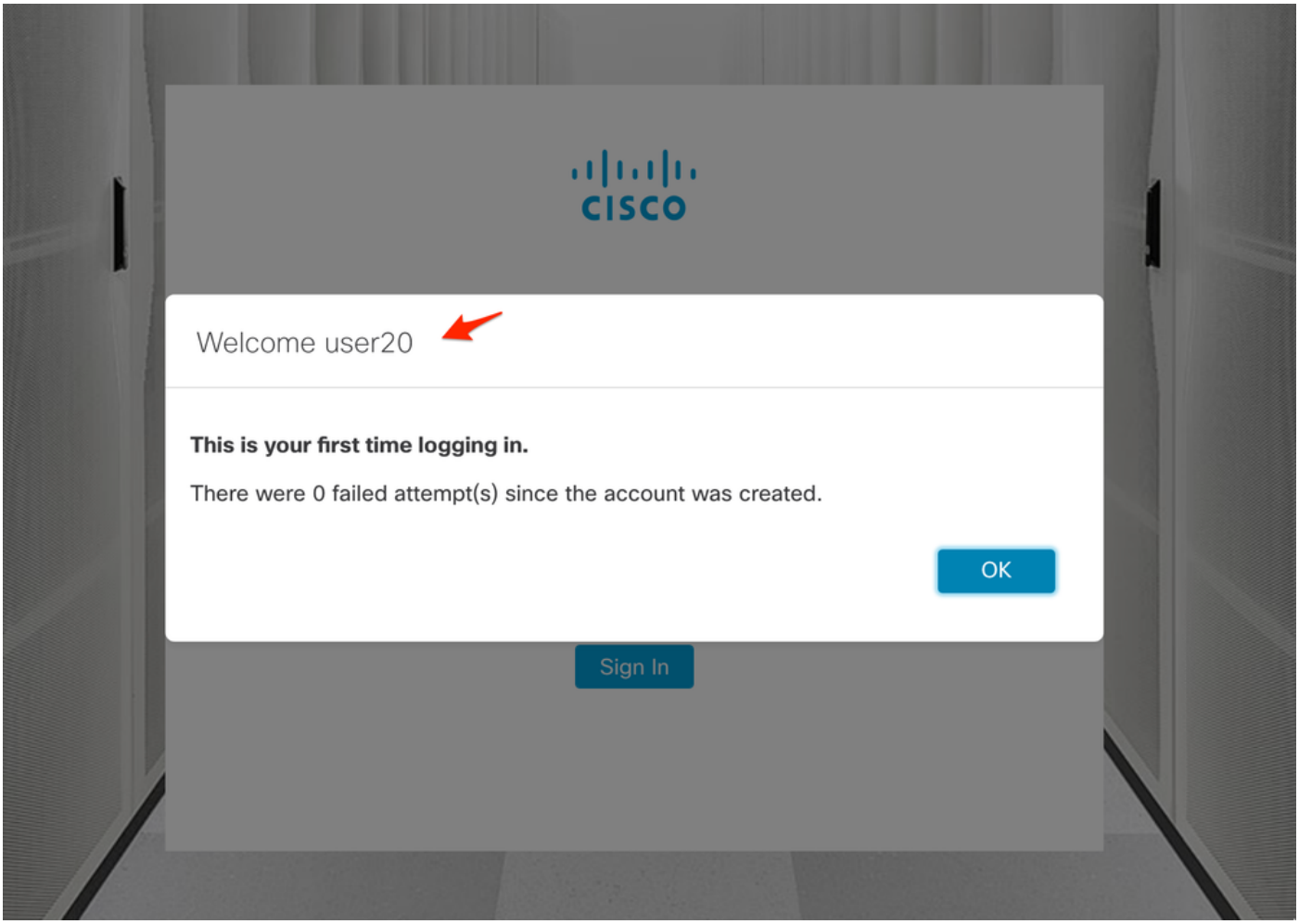
1. 開啟Manager主控制面板，然後導航至**全域性設定 > 使用者管理**。
2. 在**User Management**視窗中，選擇**Authentication and Authorization**頁籤。
3. 找到在步驟C中配置的LDAP身份**驗證服務**。
4. 按一下**Actions > Enable Remote Authorization**。

   附註：**一次只能使用一個外部授權服務。**如果另一個授權服務已在使用中，則會自動禁用該授權服務並啟用新的授權服務，但所有通過以前的外部服務獲得授權的使用者都將註銷。在任何操作發生之前都會顯示確認消息。

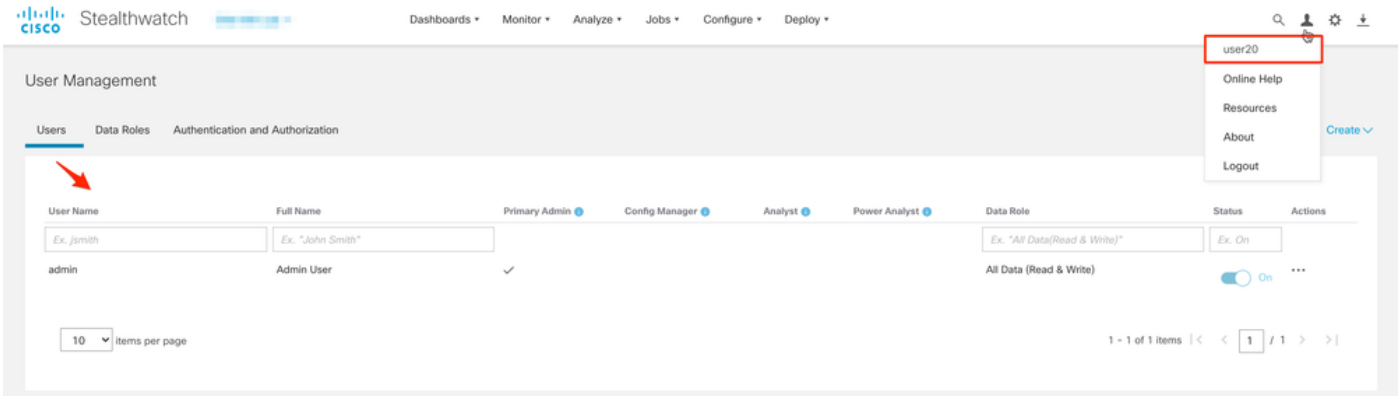


驗證

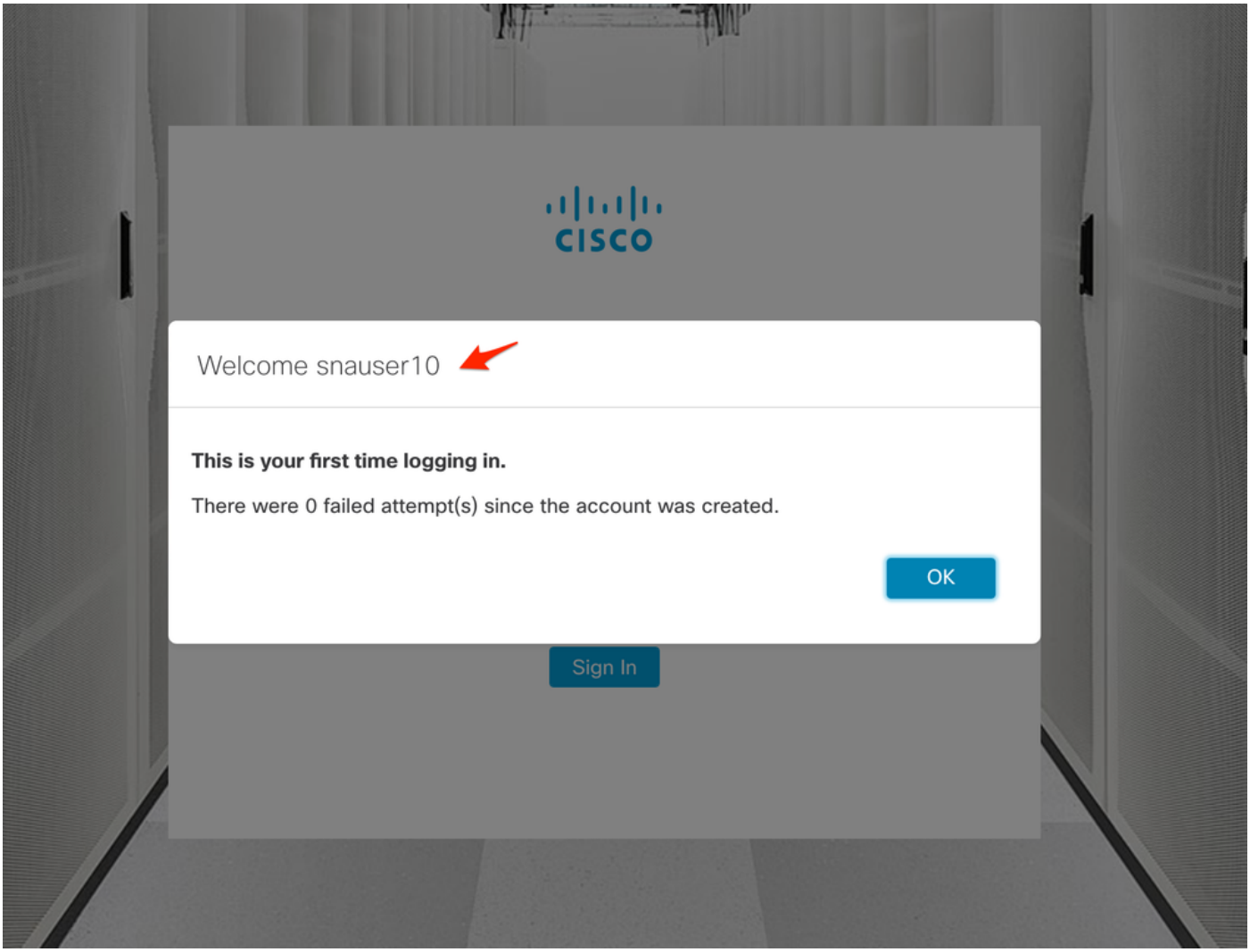
使用者可以使用在AD伺服器上定義的憑據登入。



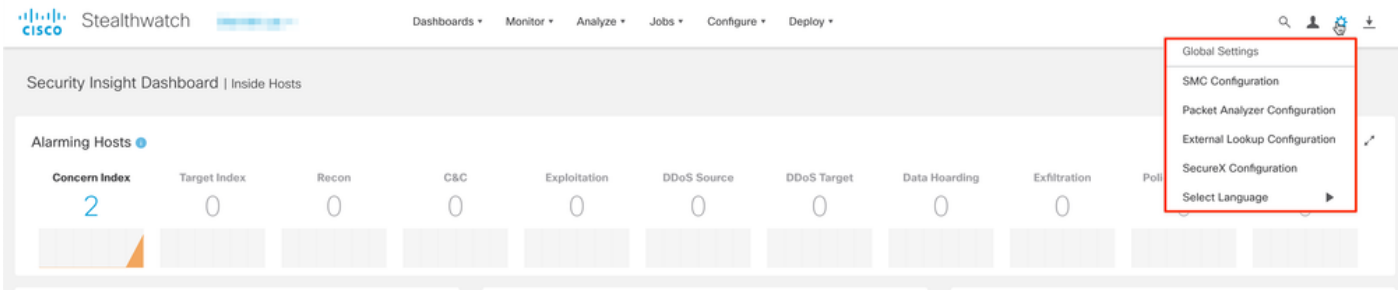
第二個驗證步驟與授權有關。在本例中，使用者「user20」成為AD伺服器中*cisco-stealthwatch-master-admin*組的成員，我們可以確認該使用者具有Primary Admin許可權。本地使用者中未定義使用者，因此我們可以確認Authorization屬性是由AD伺服器傳送的。



在本示例「snauser10」中對其他使用者執行相同的驗證。 我們可以使用AD伺服器上配置的憑據確認身份驗證成功。



對於授權驗證，由於此使用者不屬於主要管理員組，因此某些功能不可用。



疑難排解

如果無法成功儲存身份驗證服務的配置，請驗證：

1. 您已將LDAP伺服器的正確證書新增到Manager的信任儲存中。
2. 配置的**Server Address**在LDAP伺服器證書的Subject Alternative Name(SAN)欄位中指定。 如果SAN欄位僅包含IPv4地址，請在Server Address欄位中輸入IPv4地址。如果SAN欄位包含DNS名稱，請在Server Address欄位中輸入DNS名稱。如果SAN欄位同時包含DNS和IPv4值，請使用列出的第一個值。
3. 配置的**Bind User**和**Base Account**欄位正確，如AD域控制器所指定。

相關資訊

如需其他協助，請聯絡思科技術協助中心(TAC)。需要有效的支援合約： 思科全球支援聯絡人.