通过LDAPS配置外部身份验证和授权以访问安全网络分析管理器

目录

简介

本文档介绍安全网络分析管理器（以前称为Stealthwatch管理中心）7.1版或更高版本的基本配置，以使用外部身份验证，以及在7.2.1版或更高版本中使用LDAPS的外部授权。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科安全网络分析（以前称为Stealthwatch）
- 常规LDAP和SSL操作
- 常规Microsoft Active Directory管理

使用的组件

本文档中的信息基于以下组件：

- 思科安全网络分析管理器（以前称为SMC）7.3.2版
- Windows Server 2016配置为Active Directory域控制器

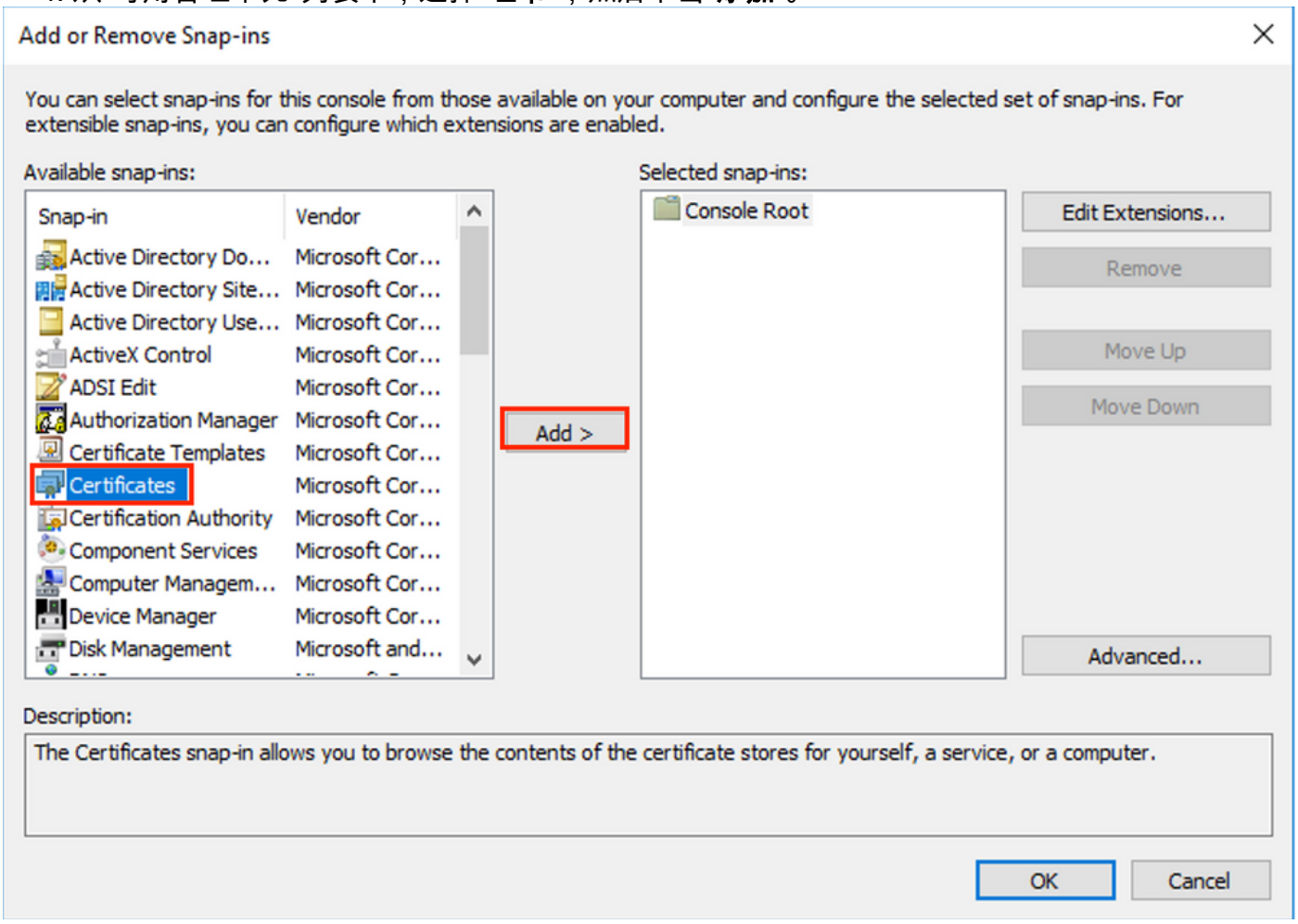
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

步骤A.登录AD域控制器并导出用于LDAP的SSL证书。

1. 对于Windows Server 2012或更高版本，从“开始”**菜单**中选择“运行”，然后输入**certlm.msc**，然后继续执行第**8步**。
2. 对于较旧的Windows Server版本，请**从“**开始”菜单中选择“运行”，然后输**入mmc**。
3. 从“文件”菜单中，选**择“添加/删除管理单元**”。
4. 从“可用管理单元”列表中，选择“证**书”**，然后单击“**添加”**。

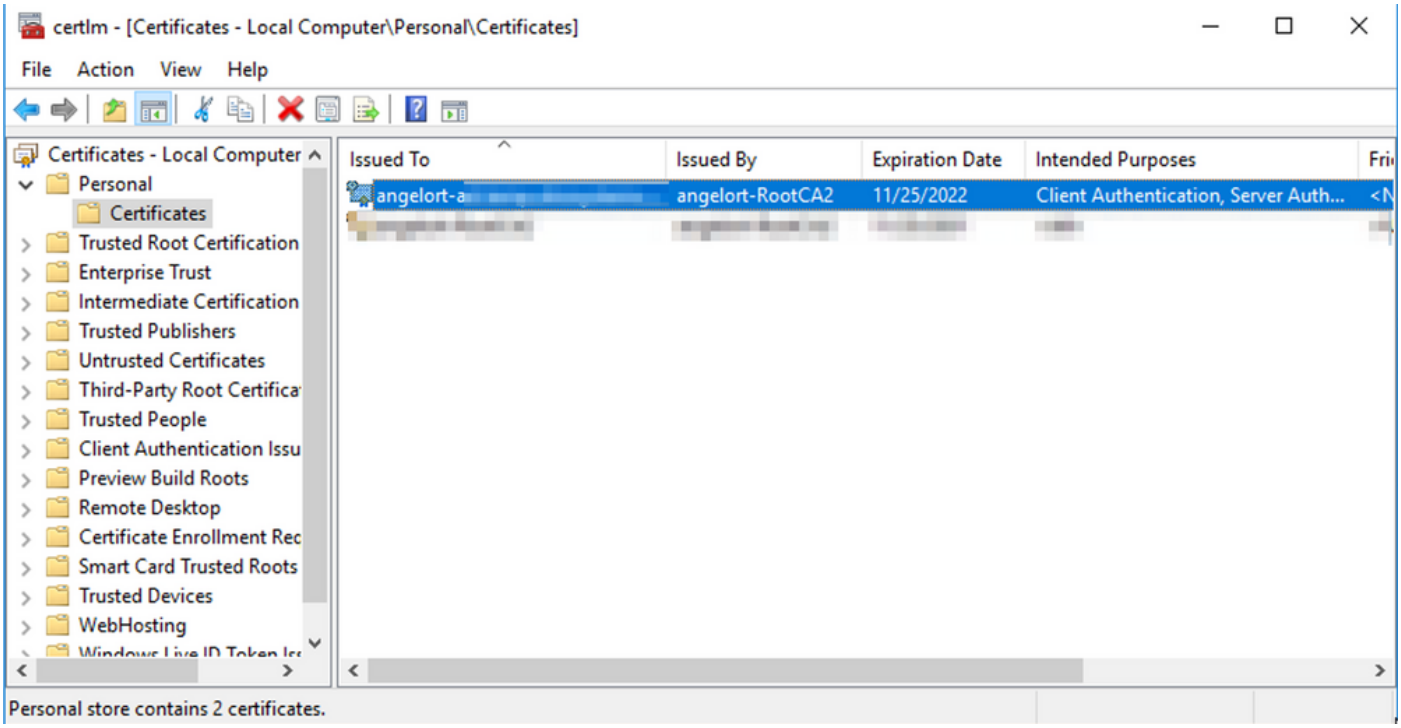


5.在“证**书”管理单**元窗口中，**选择“**计算机帐户”，然**后选择**“

6.保留“本**地计算机”**为选中状态，然后选择“**完成”**。

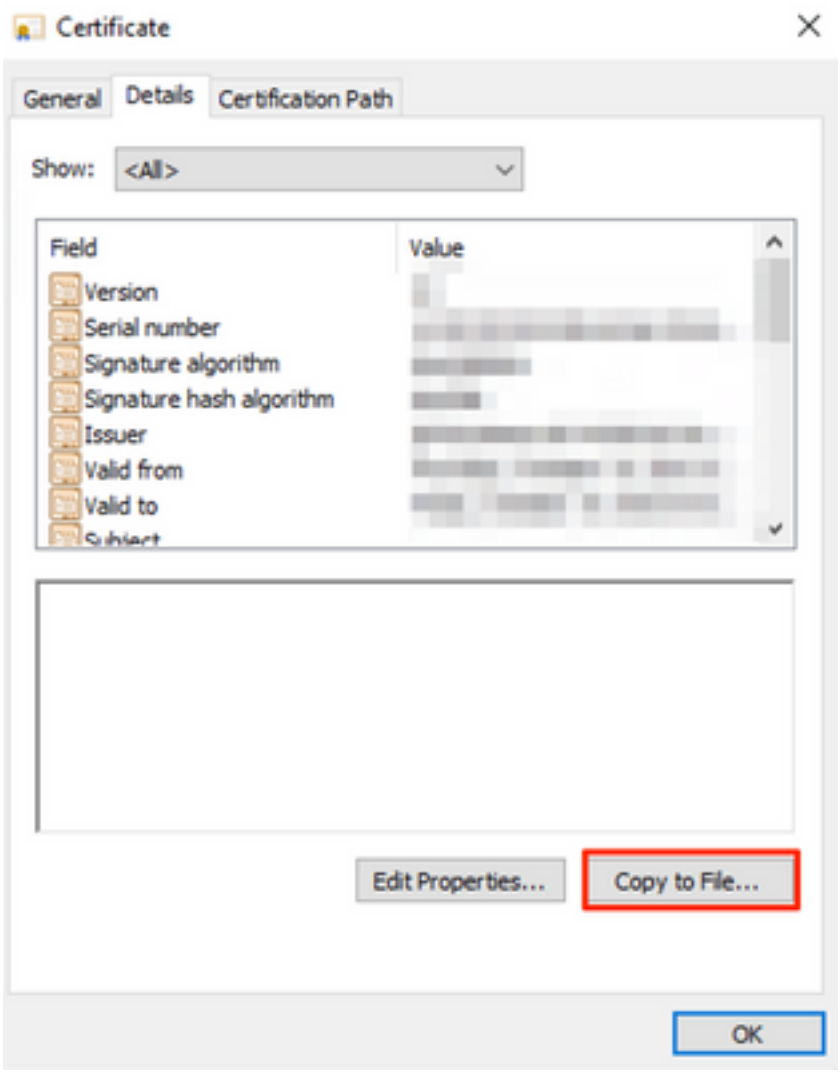
7.在“添加**或删除管理单元”窗**口中，选**择确定**。

8.导航至“证**书（本地计算机）”>“个人”>“证书”**



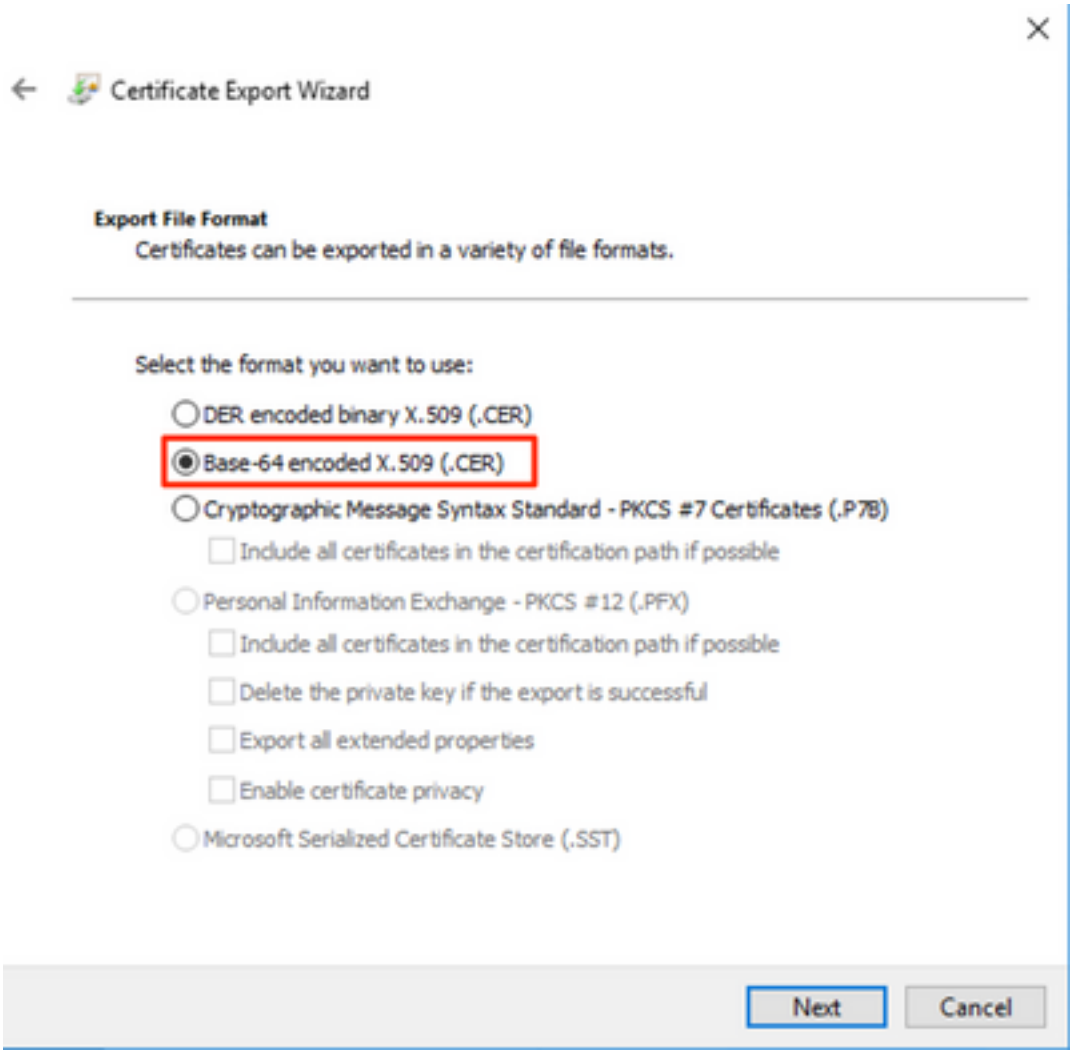
9.在域控制器上选择并右键单击用于LDAPS身份验证的SSL证书，然后单击**Open**。

10.导航至“详细信**息**”选项卡>单击“**复制到文件**”>“下**一步**”

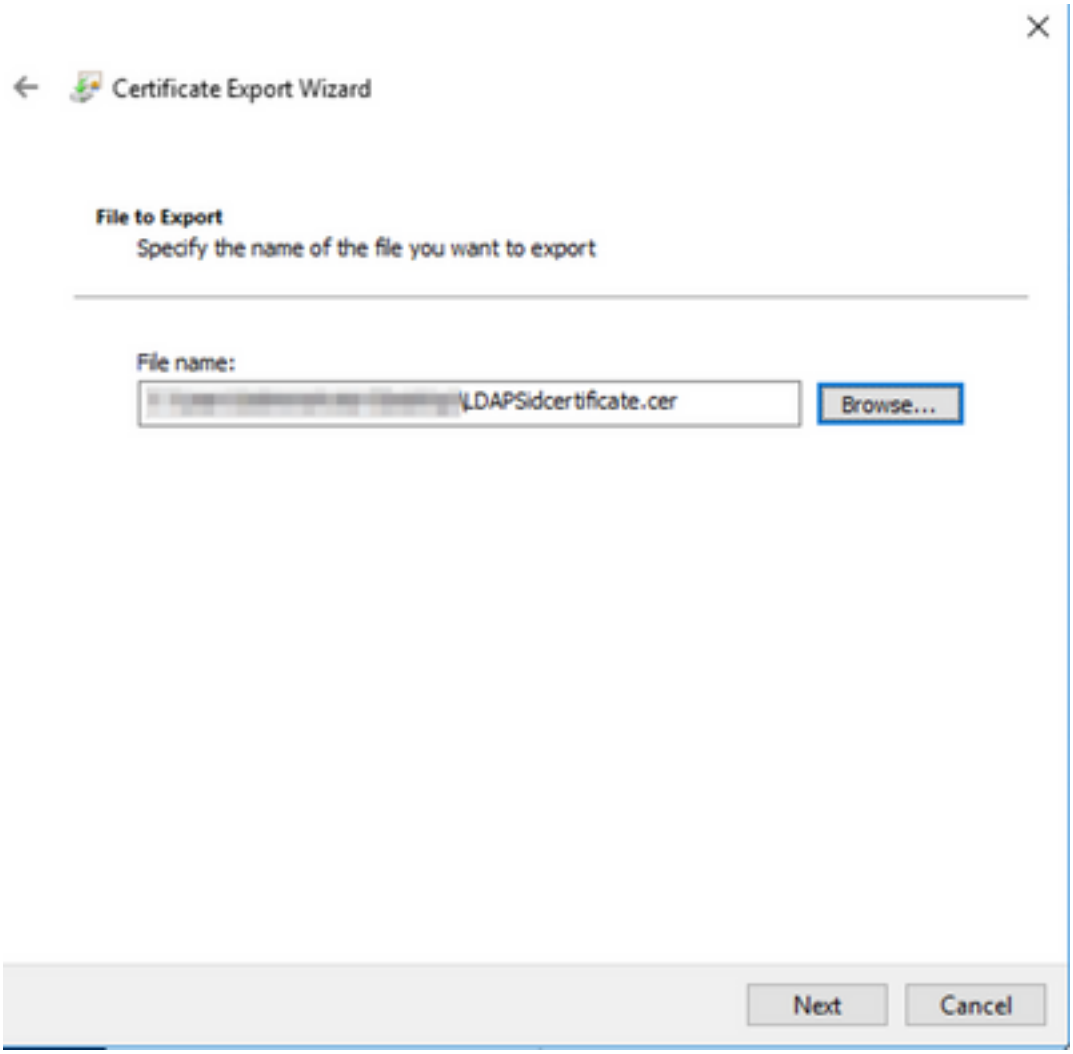


11.确保选**择“否，不导出私钥”**，然后单击“下**一步**”

12.选择**Base-64编码的X.509格式，然**后单击“下**一步”**。



13.选择存储证书的位置，命名文件，然后单击“下一**步”**。



14.单击“完**成”**，您必须看到“导出成功”。 邮件.

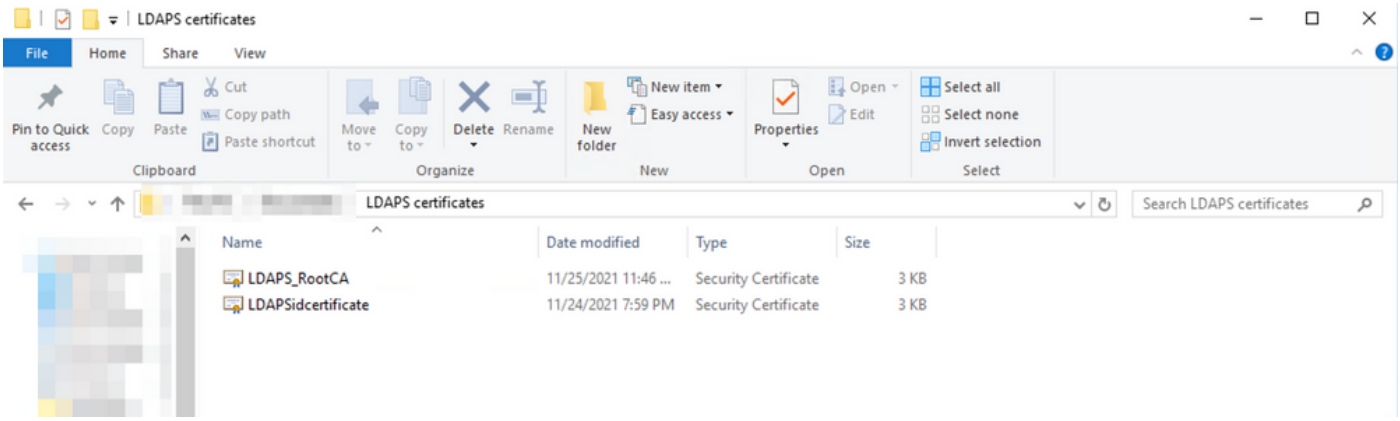
15.返回到用于LDAPS的证书，然后选择“认证路**径”选**项卡。

16.选择证书路径顶部的根CA颁发者，然后单击“查看证**书”**。

17.重复步骤10-14，以导出签署用于LDAPS身份验证的证书的根CA的证书。

> **注意：**部署可以有多层CA层次结构，在这种情况下，您需要遵循相同的步骤导出信任链中的所有中间证书。

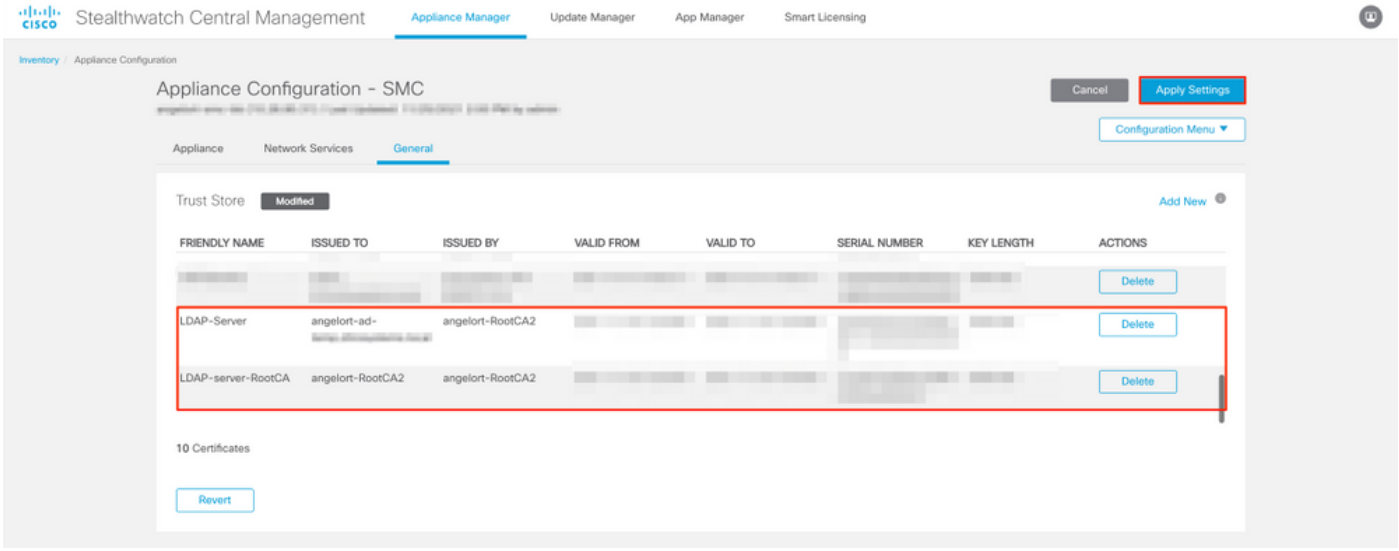
18.在继续之前，请确保在证书路径中为LDAPS服务器和每个颁发机构提供一个证书文件：根证书和中间证书（如果适用）。



步骤B.登录SNA Manager以添加LDAP服务器和根链的证书。

1. 导航至**Central Management >** Inventory。

2. 找到SNA Manager设备，然后单击“操作”**>“编辑设备配置”**。
3. 在“装置配置”(Appliance Configuration)窗口中，导航**至“配置”**(Configuration)菜单**>“信任存储”(Trust Store)>**“添**加新建”(Add New)**。
4. 键入友好名称，单击**选择文**件并选择LDAP服务器的证书，然后单击**添加证书。**
5. 重复上一步，添加根CA证书和中间证书（如果适用）。
6. 验证上传的证书是否正确，然后单击“Apply Settings(应**用设置)**”。

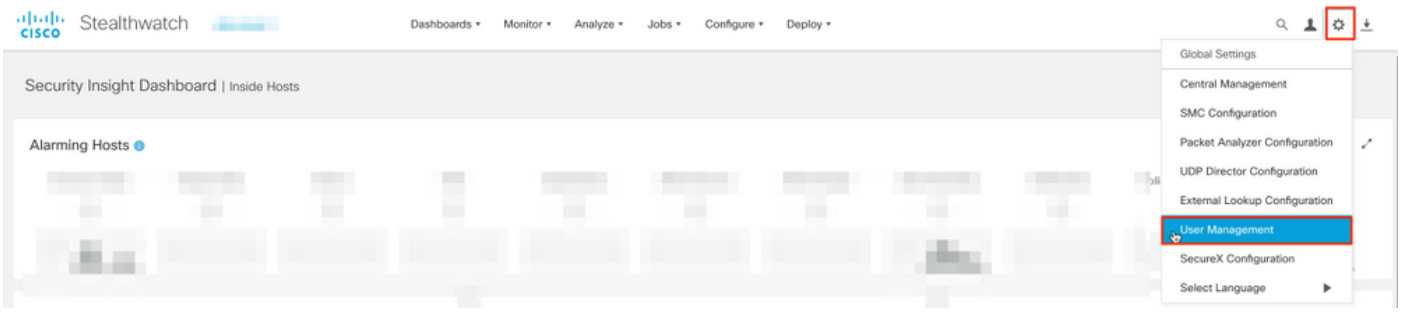


7.等待应用更改，并等待Manager状态**为Up。**

步骤C.添加LDAP外部服务配置。

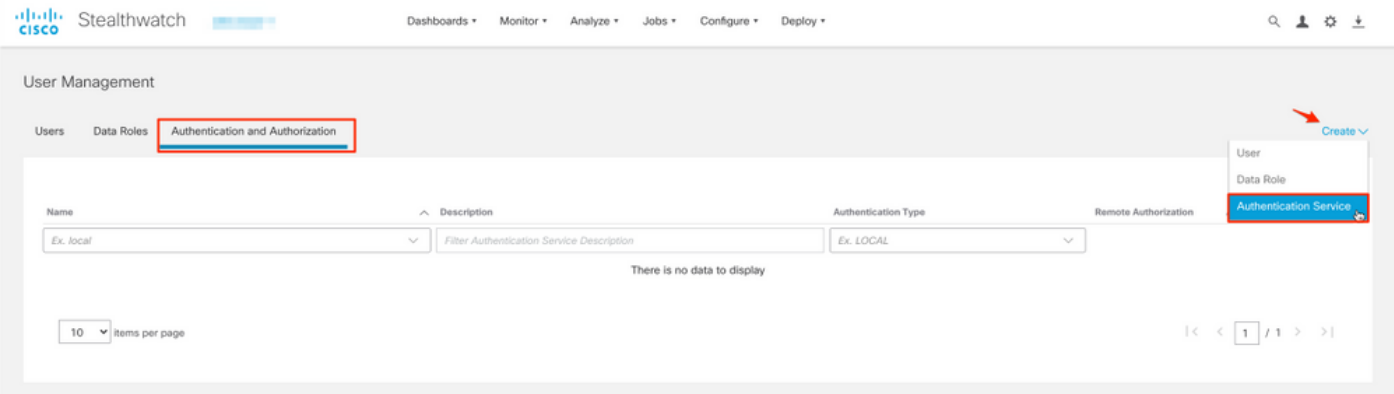
SNA版本7.2或更高版本

1.打开Manager主控制面板并导航至“全局设**置”>**“用户**管理”。**



2.在“用户管理”窗口中，选择“身份验**证和授权”**选项卡。

3.单击“创**建”>“身份验证服务**”。



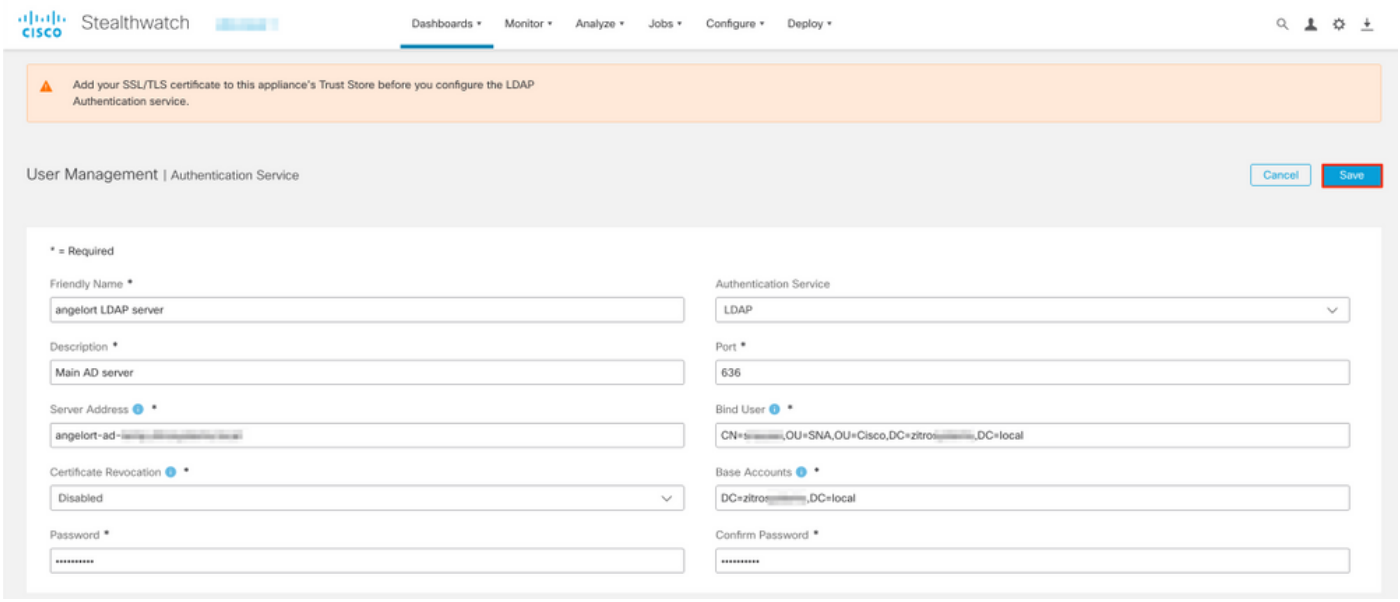
4.从“身份验**证服务**”下拉菜单中选择**LDAP**。

5.填写必填字段。

字段	**备注**
友好名称	输入LDAP服务器的名称。
描述	输入LDAP服务器的说明。
服务器地址	**输入在LDAP服务器证书的Subject Alternative Name(SAN)字段中指定的完全限定域名。** • 如果SAN字段仅包含IPv4地址，请在Server Address字段中输入IPv4地址。 • 如果SAN字段包含DNS名称，请在Server Address字段中输入DNS名称。 • 如果SAN字段同时包含DNS和IPv4值，请使用的第一个值。
端口	输入为安全LDAP通信(LDAP over TLS)指定的端口LDAPS的公认TCP端口是636。
绑定用户	输入用于连接到LDAP服务器的用户ID。例如：CN=admin，OU=企业用户，DC=example，DC=com **注意**：如果已将用户添加到内置AD容器（例，“用户”），则绑定用户的绑定DN必须将规称(CN)设置为内置文件夹（例如，CN=username、CN=Users、DC=domainDC=com）。 但是，如果已将用户添加到新容，则绑定DN必须将组织单位(OU)设置为新容称（例如，CN=用户名，OU=企业用户，DC，DC=com）。 **注意**：查找绑定用户的绑定DN的有用方法是与Active Directory服务器连接的Windows服务上的Active Directory。要获取此信息，您可以开Windows命令提示符并键入命令**dsquery us dc=<distinguished>,dc=<name> -name <use**例如： **dsquery user dc=example，dc=com name user1**。结果看起来像"CN=user1,OU=Corporate Users，DC=example，DC=com"

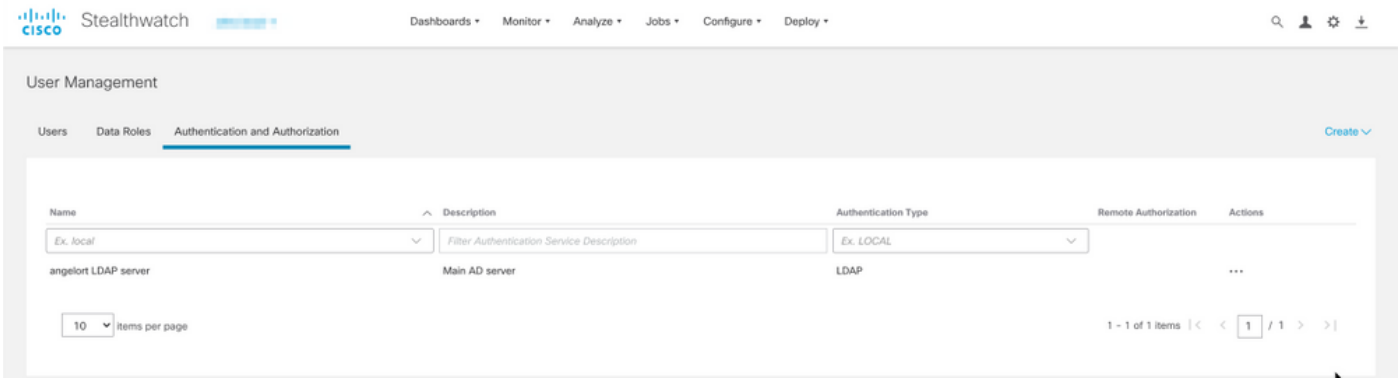
密码	输入用于连接到LDAP服务器的绑定用户密码。
基本客户	输入可分辨名称(DN)。 DN适用于必须开始搜索用户的目录的分支。它通常 目录树（域）的顶部，但您也可以在目录中指定子 绑定用户和要进行身份验证的用户必须可从基本帐 问。 例如：DC=example，DC=com

6.单击“保**存**”。



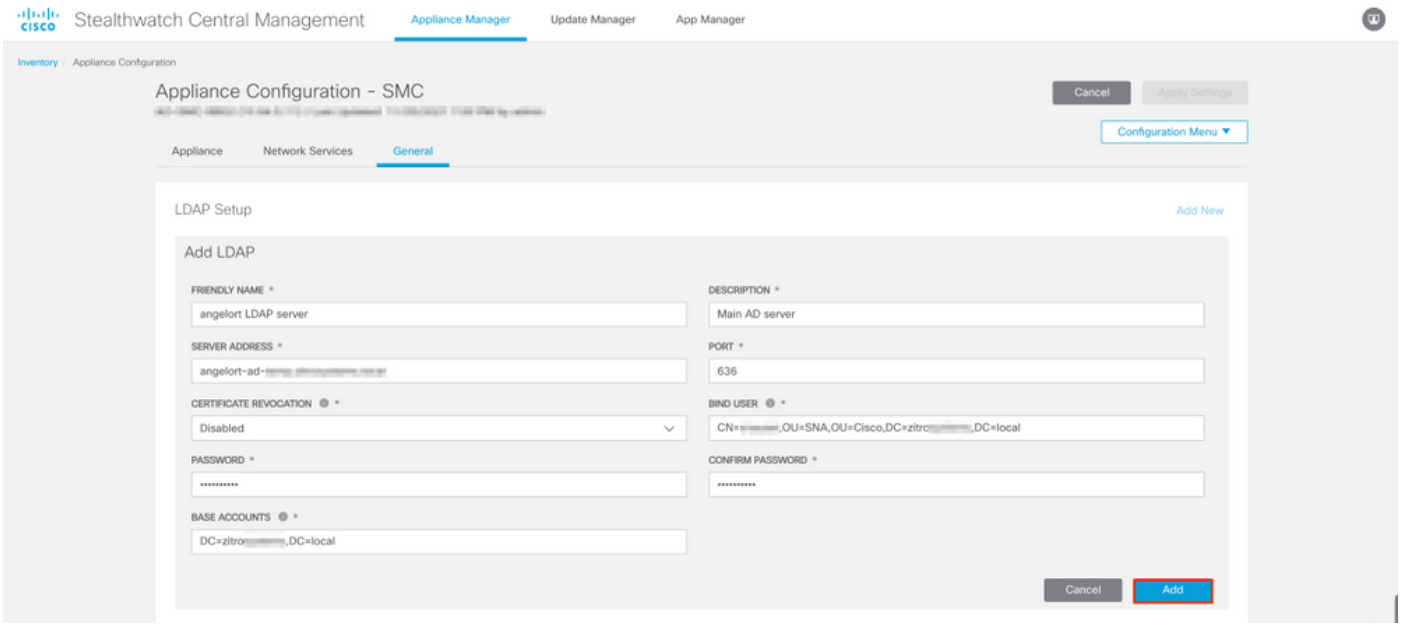
7.如果输入的设置和添加到信任库的证书正确，您必须收到“您已成功保存更改”标语。

8.配置的服务器必须显示在“用户管理”**>“身份验证**和授**权”下**。



SNA版本7.1

1. 导航至**Central Management >** Inventory。
2. 找到SMC设备，然后单击“操**作”>**“编**辑设备配置**”。
3. 在“装置配置”(Appliance Configuration)窗口中，导航**至“配置”**(Configuration)菜**单>“LDAP设**置”(LDAP Setup)**>“添加新**”。
4. 按照SNA 7.2版或更高**版本步骤5中的说明填**写必填字段。



5.单击“添**加”**。

6.单击“应用**设置”**。

7.输入的设置和添加到信任库的证书正确后，将应用Manager上的更改，设备状态必须**为Up**。

步骤D.配置授权设置。

SNA通过LDAP支持本地和远程授权。使用此配置，AD服务器中的LDAP组将映射到内置或自定义SNA角色。

通过LDAP支持的SNA身份验证和授权方法包括：

- 远程身份验证和本地授权
- 远程身份验证和远程授权（仅支持SNA版本7.2.1或更高版本）

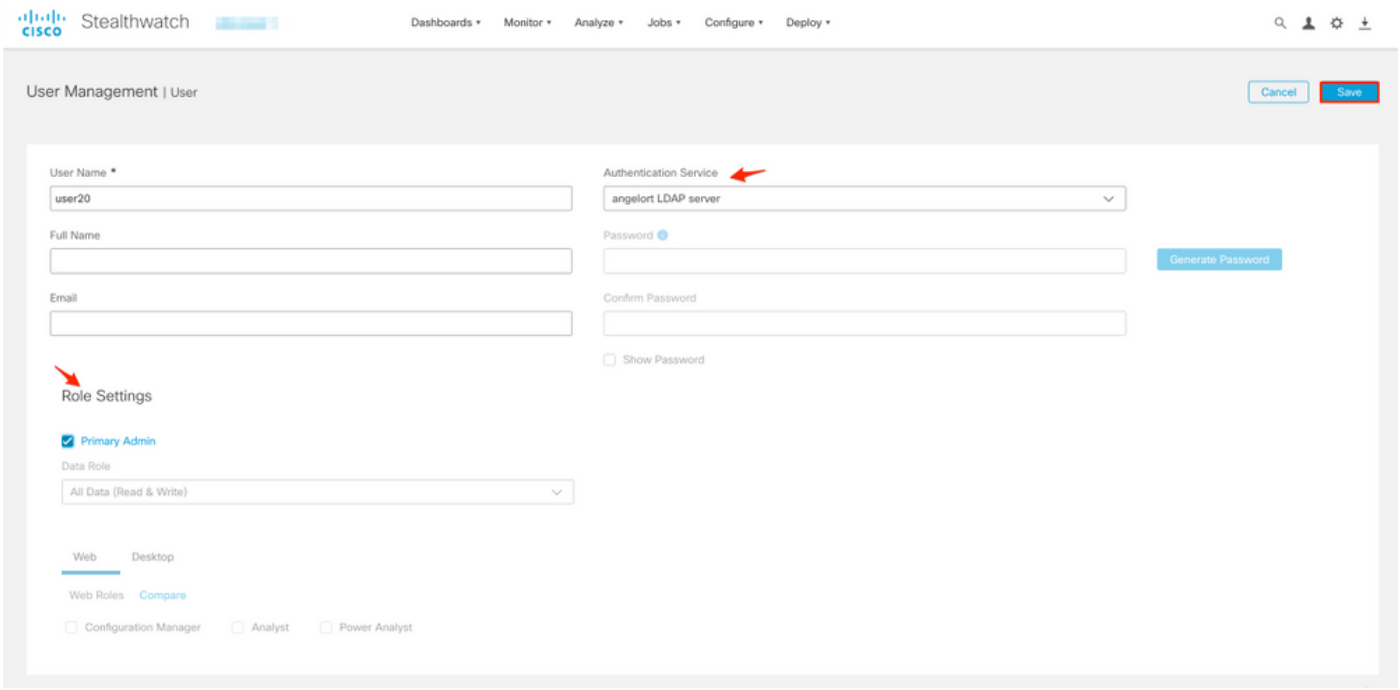
本地授权

在这种情况下，用户及其角色需要在本地定义。为此，请按如下步骤操作。

1.再次导航**至“用户**管理”，单击“**用户”**选项卡**> 创建> 用户**。

2.定义要向LDAP服务器进行身份验证的用户名，并从“身份验证服务”下**拉菜单中选择**已配置的服务器。

3.定义用户在通过LDAP服务器验证后对Manager必须拥有的权限，然后单击“保**存”**。



通过LDAP进行远程授权

安全网络分析7.2.1版首先支持通过LDAP进行远程身份验证和授权。

> **注意**：版本7.1不支持使用LDAP的远程授权。

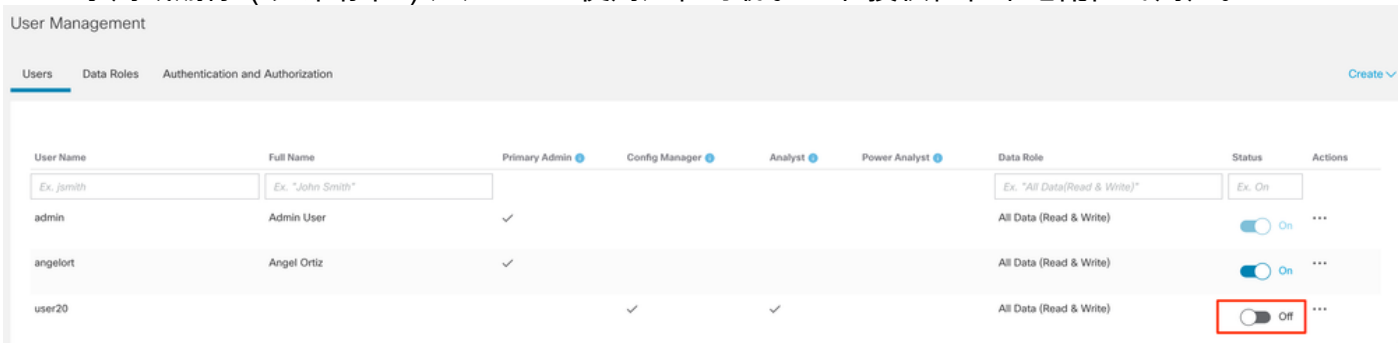
请注意，如果用户在本地（在Manager中）定义和启用，则用户将通过远程身份验证，但在本地获得授权。用户选择过程如下：

1. 在Manager的欢迎页面上输入凭证后，Manager将查找具有指定名称的本地用户。
2. 如果找到本地用户并启用了该用户，则会对其进行远程身份验证（如果之前配置了通过本地授权的LDAP进行远程身份验证），但会使用本地设置进行授权。
3. 如果配置并启用了远程授权，并且在本地找不到用户（未配置或禁用），则会远程执行身份验证和授权。

因此，成功配置远程身份验证的步骤为……

步骤D-1.禁用或删除本地定义的远程授权用户。

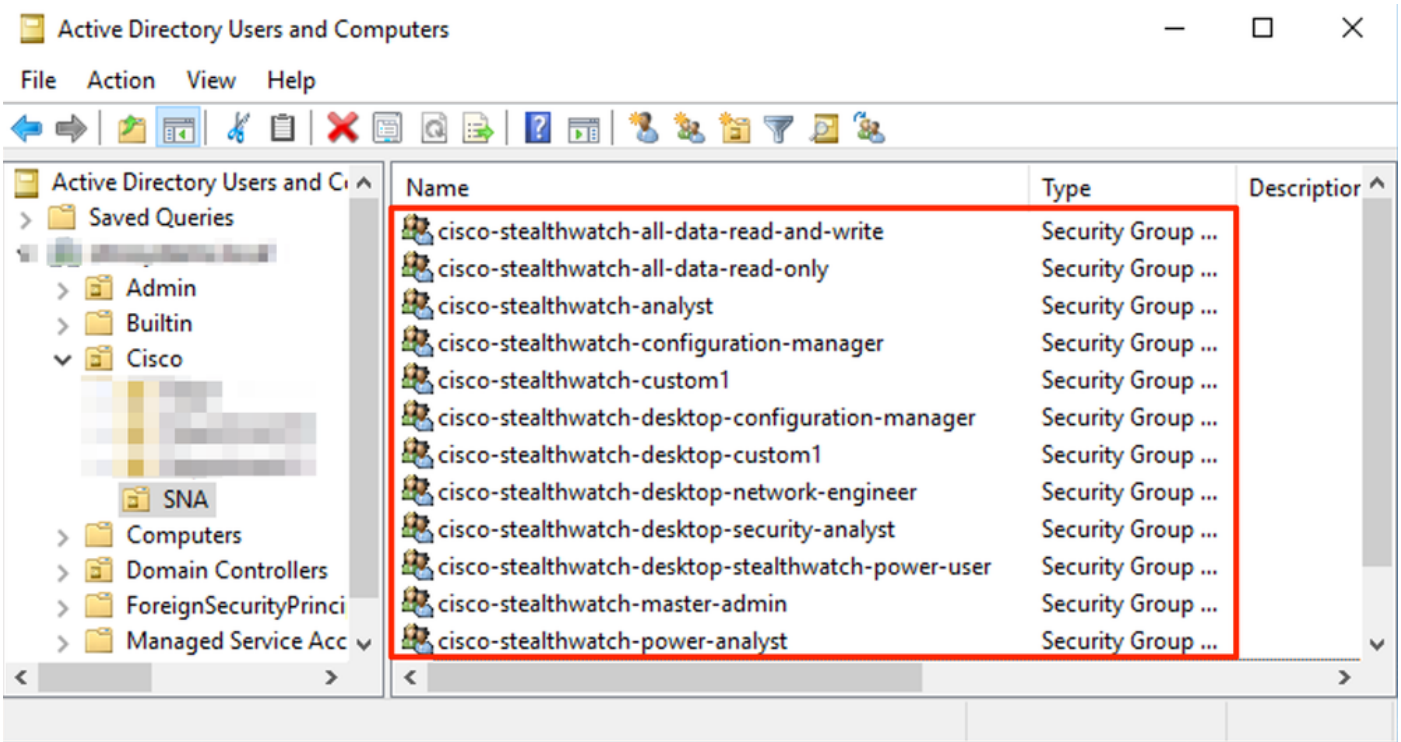
1. 打开Manager主控制面板并导航至Global Settings > User Management。
2. 禁用或删除（如果存在）通过LDAP使用远程身份验证和授权但在本地配置的用户。



步骤D-2.在Microsoft AD服务器中定义cisco-stealthwatch组。

对于通过LDAP用户进行外部身份验证和授权，密码*和cisco-stealthwatch*组在Microsoft Active Directory中远程定义。在AD服务器*中定义的cisco-stealthwatch组与SNA具有的不同角色相关，必须按照如下方式定义。*

SNA角色	组名称
主要管理员	• cisco-stealthwatch-master-admin • cisco stealthwatch-all-data-read-and-write • cisco-stealthwatch-all-data-read-only • cisco-stealthwatch-<custom>（可选） **注意**：确保自定义数据角色组以“cisco-stealthwatch — ”开头。
数据角色	
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
桌面功能角色	• cisco-stealthwatch-desktop-security-analyst • cisco-stealthwatch-desktop-<custom>（可选 **注意**：确保自定义桌面功能角色组以“cisco-stealthwatch-desktop — ”开头。

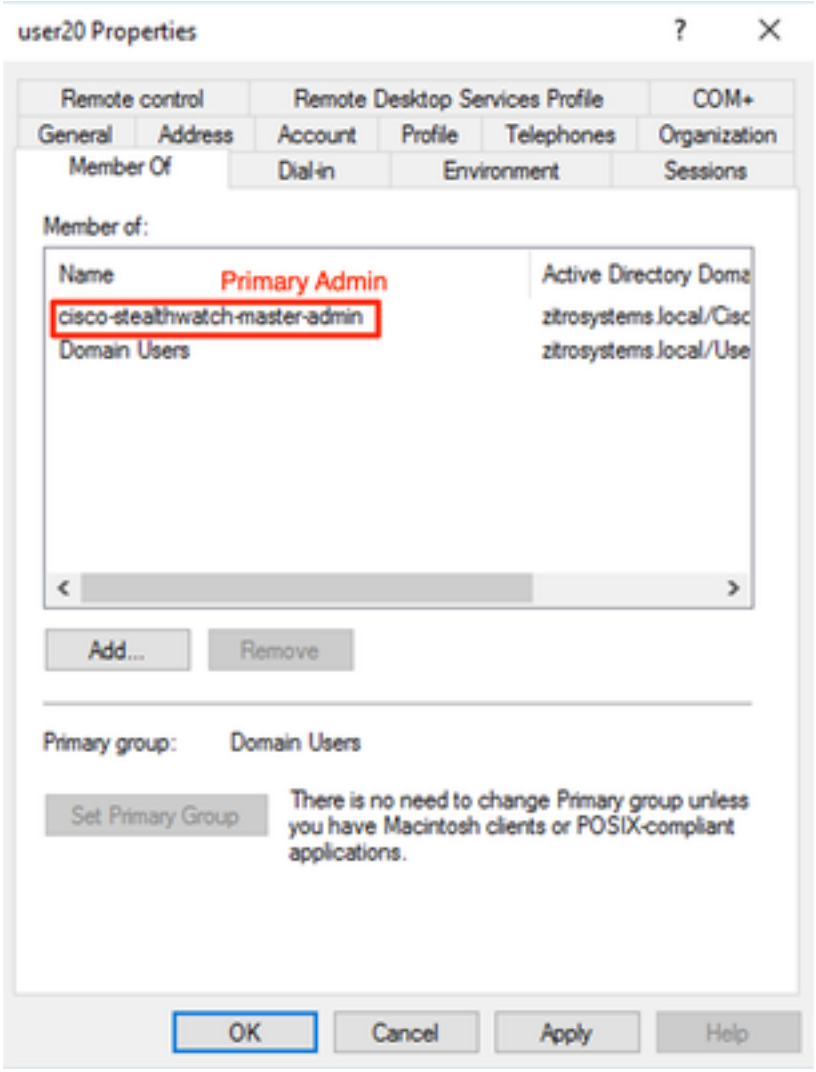


注意：如前所述，只要组名前加正确的字符串，“数据角色”和“桌面功能角色”就支持自定义组。这些自定义角色和组必须在SNA Manager和Active Directory服务器中定义。例如，如果在SNA管理器中为桌面客户端角色定义自定义角色“custom1”，则必须在Active Directory中将其映射到cisco-stealthwatch-desktop-custom1。

步骤D-3.为用户定义LDAP授权组映射。

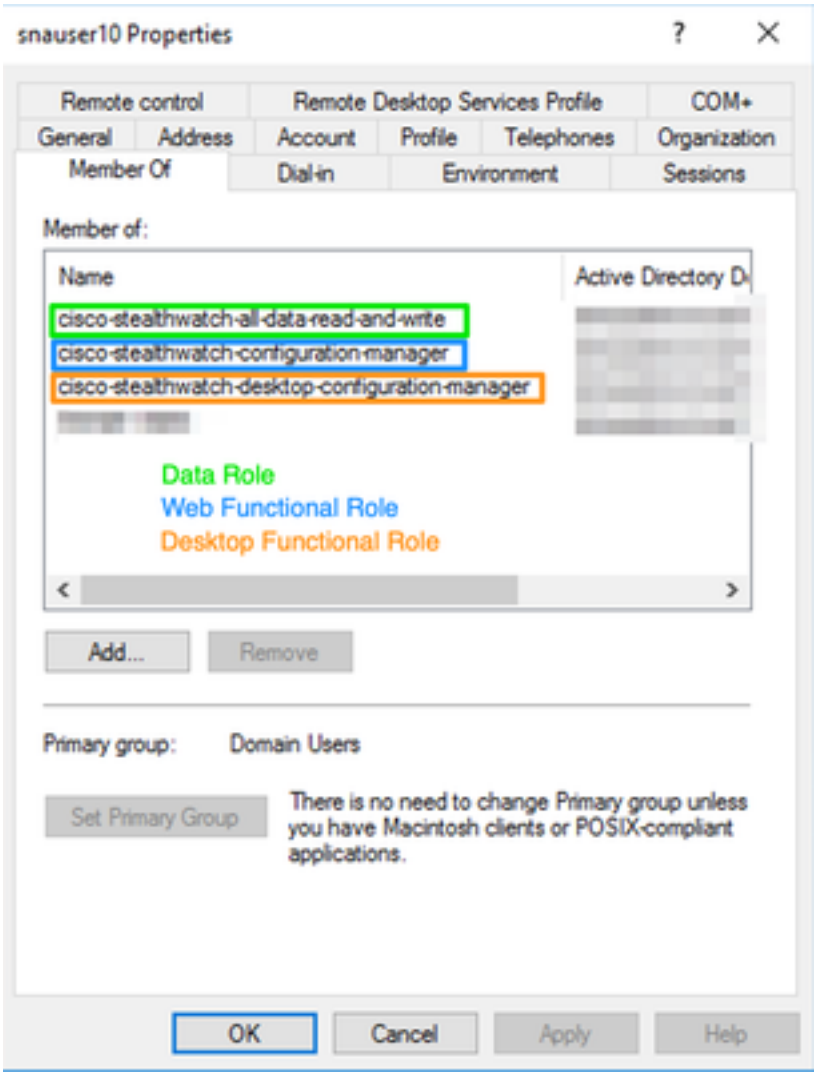
在AD服务器中定义了cisco-stealthwatch组后，我们可以将要访问SNA Manager的用户映射到必要的组。这必须按如下方式完成。

- **主管理**用户**必须**分配给*cisco-stealthwatch-master-admin*组，并且**不得是任何其他cisco-stealthwatch组**的成员。



- 除主要管理员用户外，每个用户必须分配到每个角色的组，并具有下一个条件。

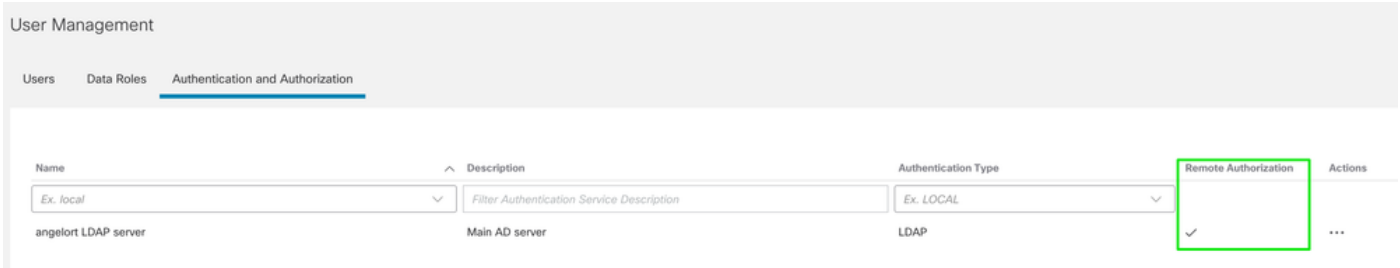
1. **数据角色**:用户只能分配给**一个组**。
2. **Web功能角色**:必须将用户分配到**至少一个组**。
3. **桌面功能角色**:必须将用户分配到**至少一个组**。



步骤D-4.在SNA管理器上通过LDAP启用远程授权。

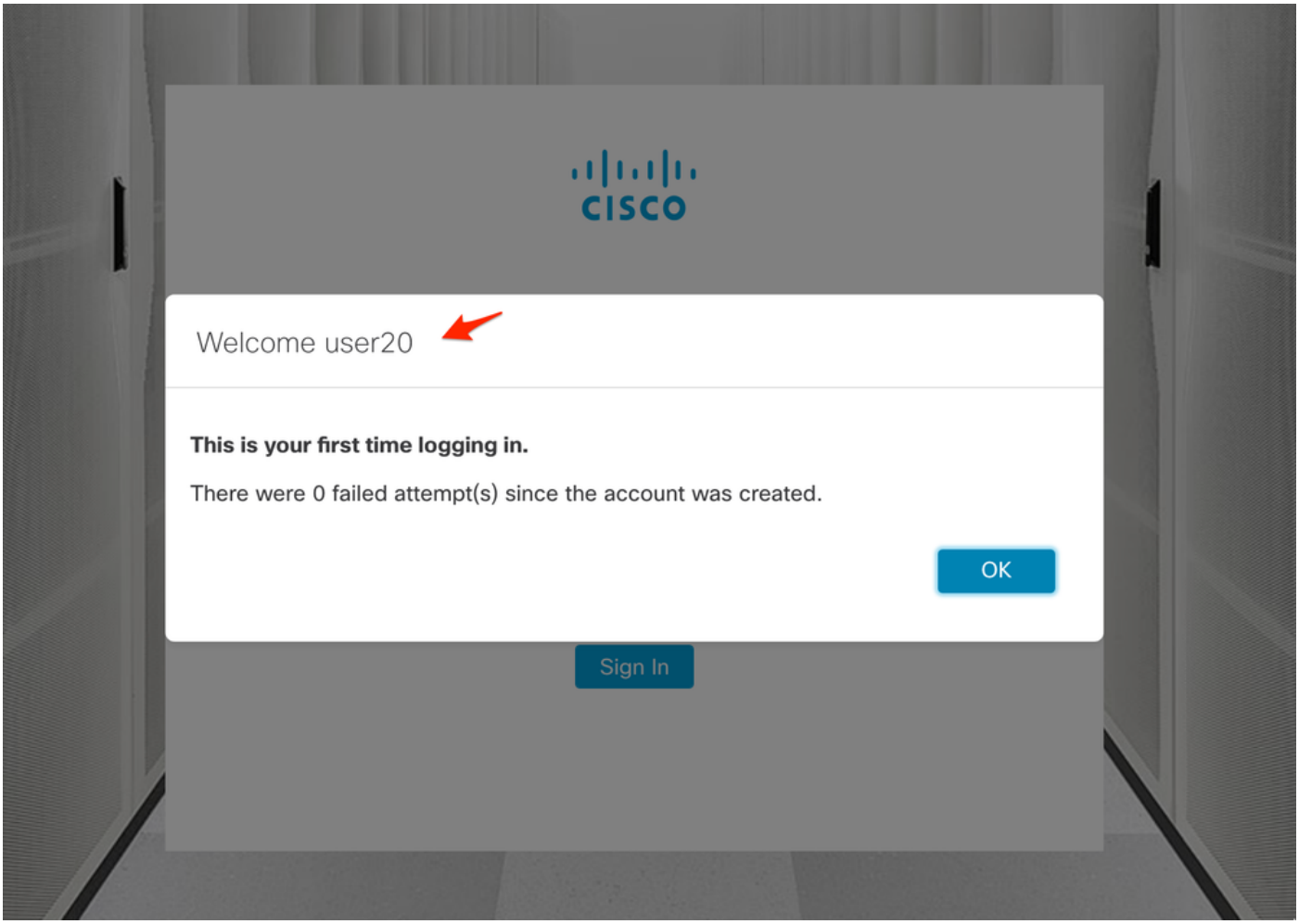
1. 打开Manager主控制面板并导航至“全局**设置”>**“用**户管理”**。
2. 在“用户**管理”**窗口中，选**择“身份验证和授**权”选项卡。
3. 找到在步骤C中配置的LDAP身**份验证服务**。
4. 单击Actions > Enable Remote Authorization。

注意：一次只能使用一个外部授权服务。如果另一个授权服务已在使用中，则会自动禁用它并启用新的授权服务，但是，已通过先前外部服务授权的所有用户都将注销。在执行任何操作之前，系统会显示确认消息。

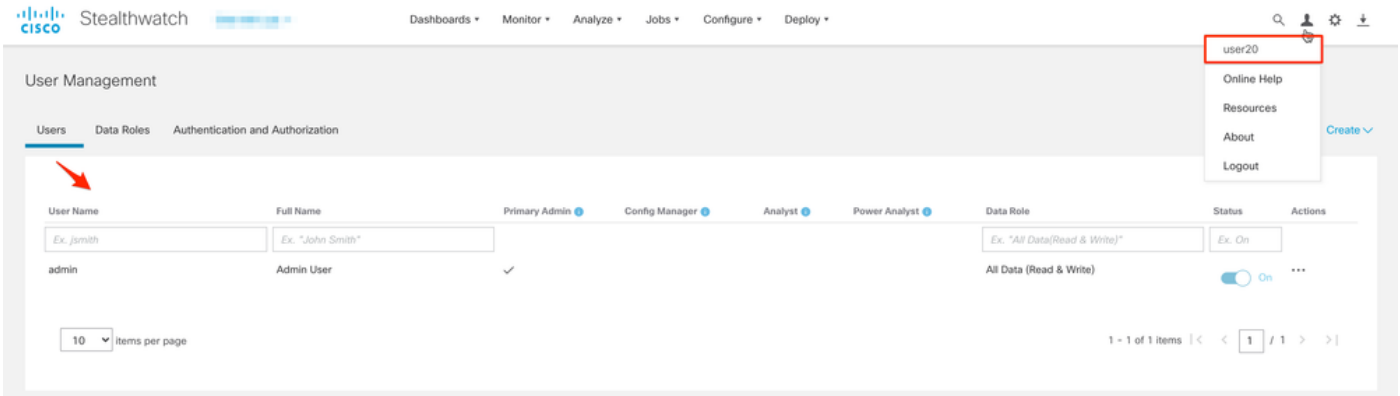


验证

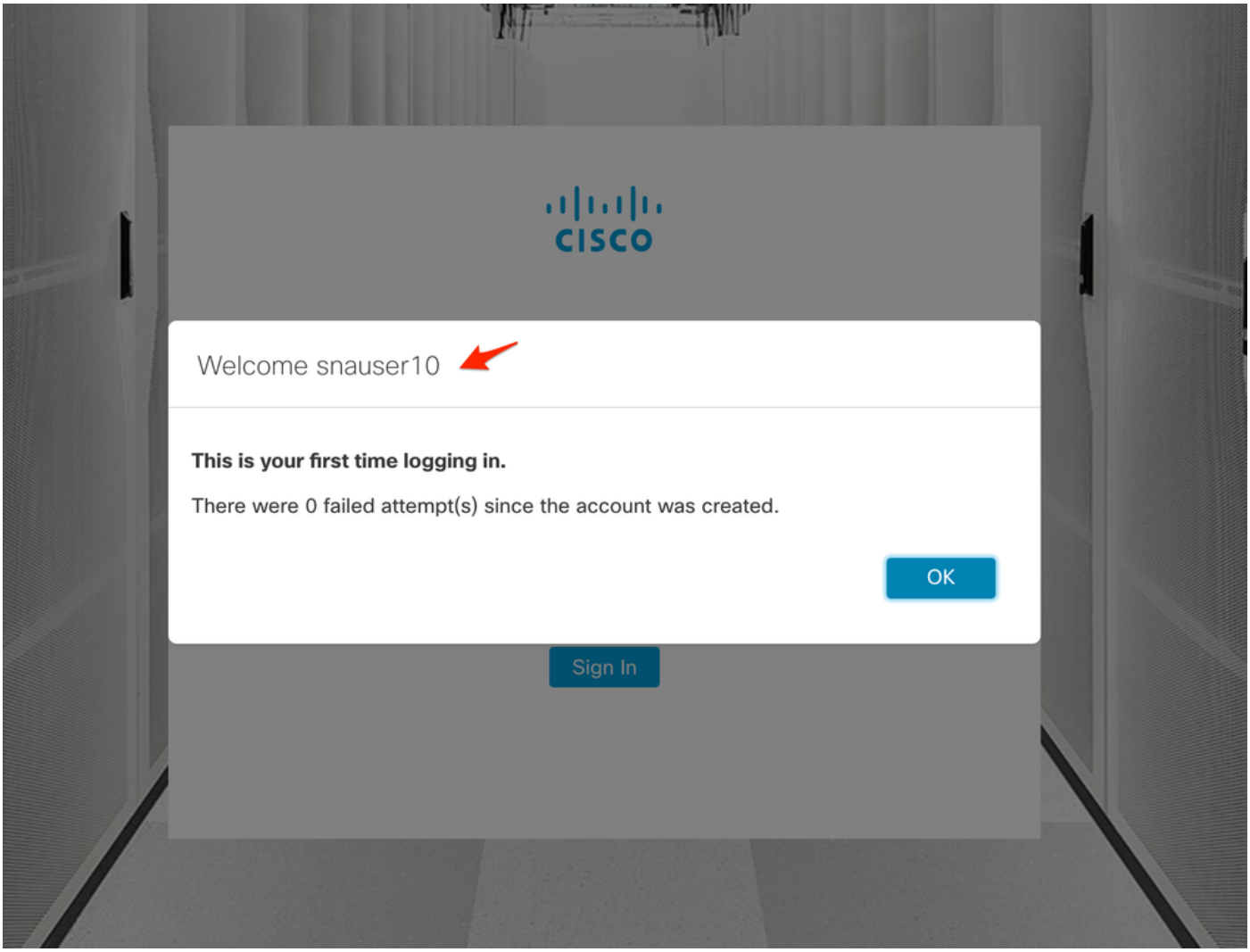
用户可以使用在AD服务器上定义的凭证登录。



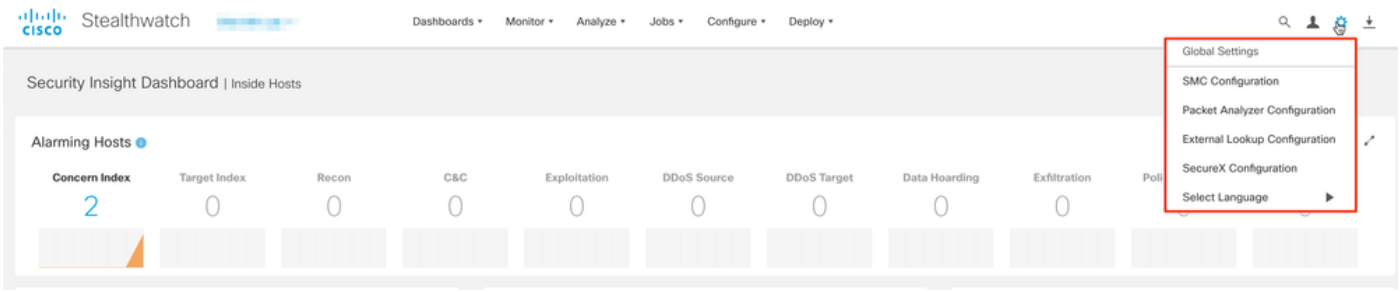
第二个验证步骤涉及授权。在本示例中，用户“user20”在AD服务器中成为*cisco-stealthwatch-master-admin*组的成员，我们可以确认该用户具有主要管理员权限。用户未在本地用户中定义，因此我们可以确认授权属性是由AD服务器发送的。



此示例“snauser10”中的其他用户也进行了相同的验证。 我们可以使用AD服务器上配置的凭证确认身份验证成功。



对于授权验证，由于此用户不属于主管理员组，因此某些功能不可用。



故障排除

如果无法成功保存身份验证服务的配置，请验证：

1. 您已将LDAP服务器的正确证书添加到Manager的信任存储。
2. 配置的**服务器地**址在LDAP服务器证书的使用者备用名称(SAN)字段中指定。 如果SAN字段仅包含IPv4地址，请在Server Address字段中输入IPv4地址。如果SAN字段包含DNS名称，请在Server Address字段中输入DNS名称。如果SAN字段同时包含DNS和IPv4值，请使用列出的第一个值。
3. 所配置**的"绑定**用户"**和"基**本帐户"字段正确，由AD域控制器指定。

相关信息

如需其他帮助，请联系思科技术支持中心(TAC)。需要有效的支持合同： 思科全球支持联系方式.