

# Configurar a autenticação externa e a autorização via LDAPS para acesso seguro ao Network Analytics Manager

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Etapa A. Efetue login no controlador de domínio do AD e exporte o certificado SSL usado para LDAP.](#)

[Etapa B. Faça login no SNA Manager para adicionar o certificado do servidor LDAP e da cadeia raiz.](#)

[Etapa C. Adicione a configuração do serviço externo LDAP.](#)

[SNA versão 7.2 ou posterior](#)

[SNA versão 7.1](#)

[Etapa D. Defina as configurações de autorização.](#)

[Autorização local](#)

[Autorização remota via LDAP](#)

[Verificar](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

## Introduction

Este documento descreve a configuração básica de um Secure Network Analytics Manager (antigo Stealthwatch Management Center) versão 7.1 ou posterior para usar a autenticação externa e, com a versão 7.2.1 ou posterior, para usar a autorização externa com LDAPS.

## Prerequisites

## Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Secure Network Analytics (antigo Stealthwatch)
- Operação geral LDAP e SSL
- Gerenciamento geral do Microsoft Active Directory

## Componentes Utilizados

As informações neste documento são baseadas nestes componentes:

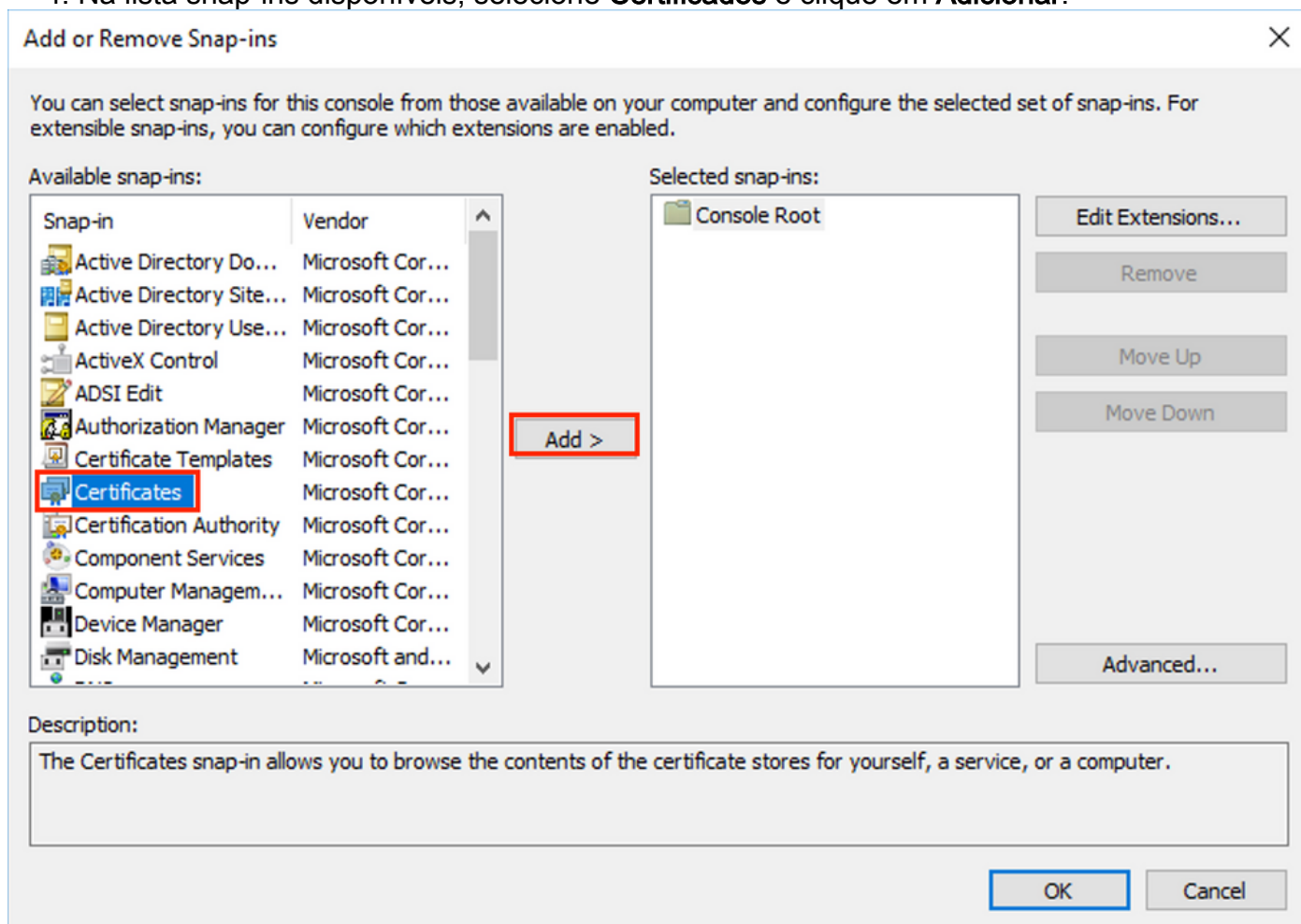
- Cisco Secure Network Analytics Manager (anteriormente SMC) versão 7.3.2
- Windows Server 2016 configurado como Controlador de Domínio do Ative Directory

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Configurar

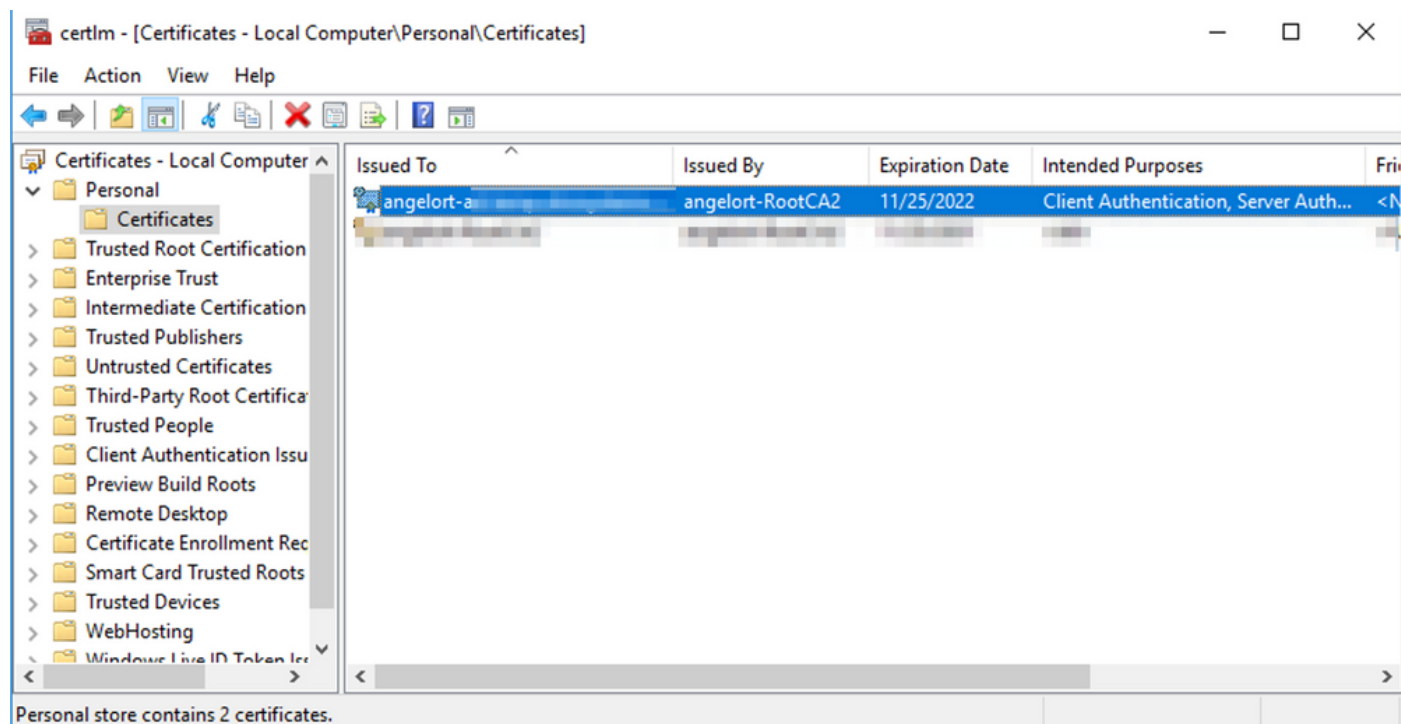
### Etapa A. Efetue login no controlador de domínio do AD e exporte o certificado SSL usado para LDAP.

1. No Windows Server 2012 ou posterior, selecione **Executar** no menu Iniciar, digite **certlm.msc** e continue com a etapa 8.
2. Para versões mais antigas do Windows Server, selecione **Executar** no menu Iniciar e digite **mmc**.
3. No menu Arquivo, selecione **Adicionar/remover snap-in**.
4. Na lista snap-ins disponíveis, selecione **Certificados** e clique em **Adicionar**.



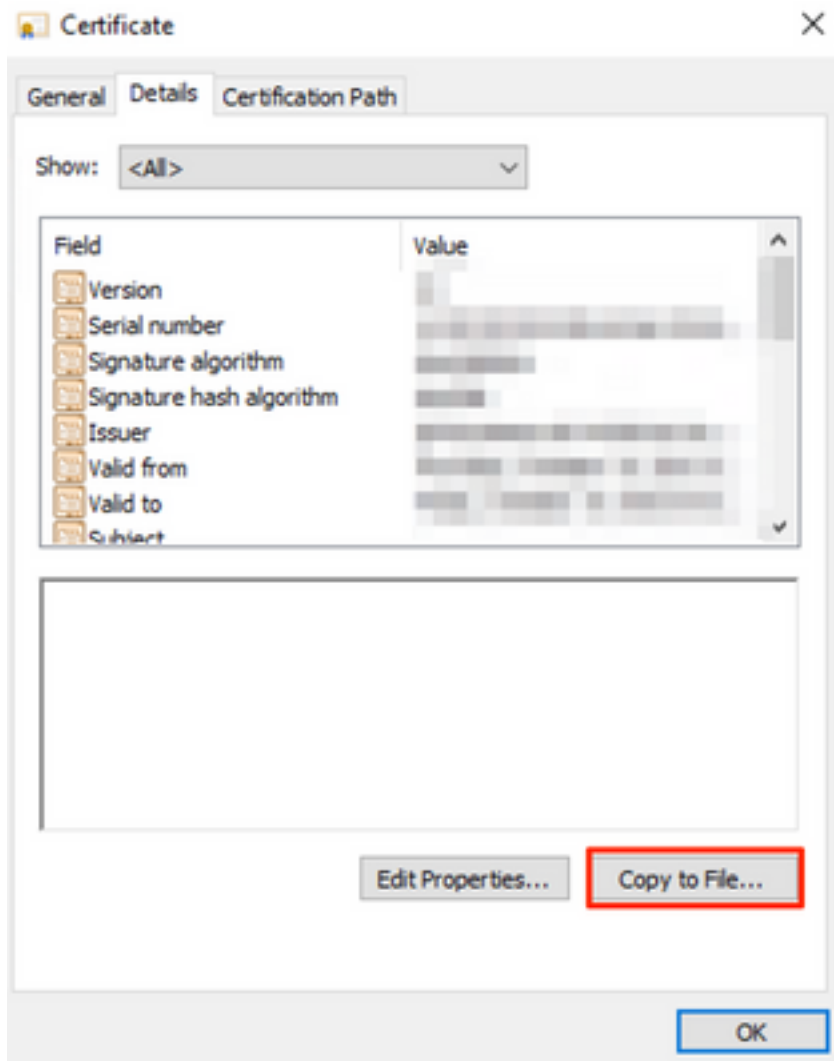
5. Na janela snap-in **Certificados**, selecione **Conta do computador** e selecione **Avançar**.
6. Deixe o **computador local** selecionado e selecione **Concluir**.
7. Na janela **Add or Remove Snap-in**, selecione **OK**.

8. Navegue até **Certificados (Computador Local) > Pessoal > Certificados**



9. Selecione e clique com o botão direito do mouse no certificado SSL usado para autenticação LDAPS em seu controlador de domínio e clique em **Abrir**.

10. Navegue até a guia **Detalhes** > clique em **Copiar para arquivo** > **Avançar**



11. Certifique-se de que **Não, não exporte a chave privada** está selecionada e clique em **Avançar**

12. Selecione o formato **X.509 codificado em Base-64** e clique em **Avançar**.



**Export File Format**

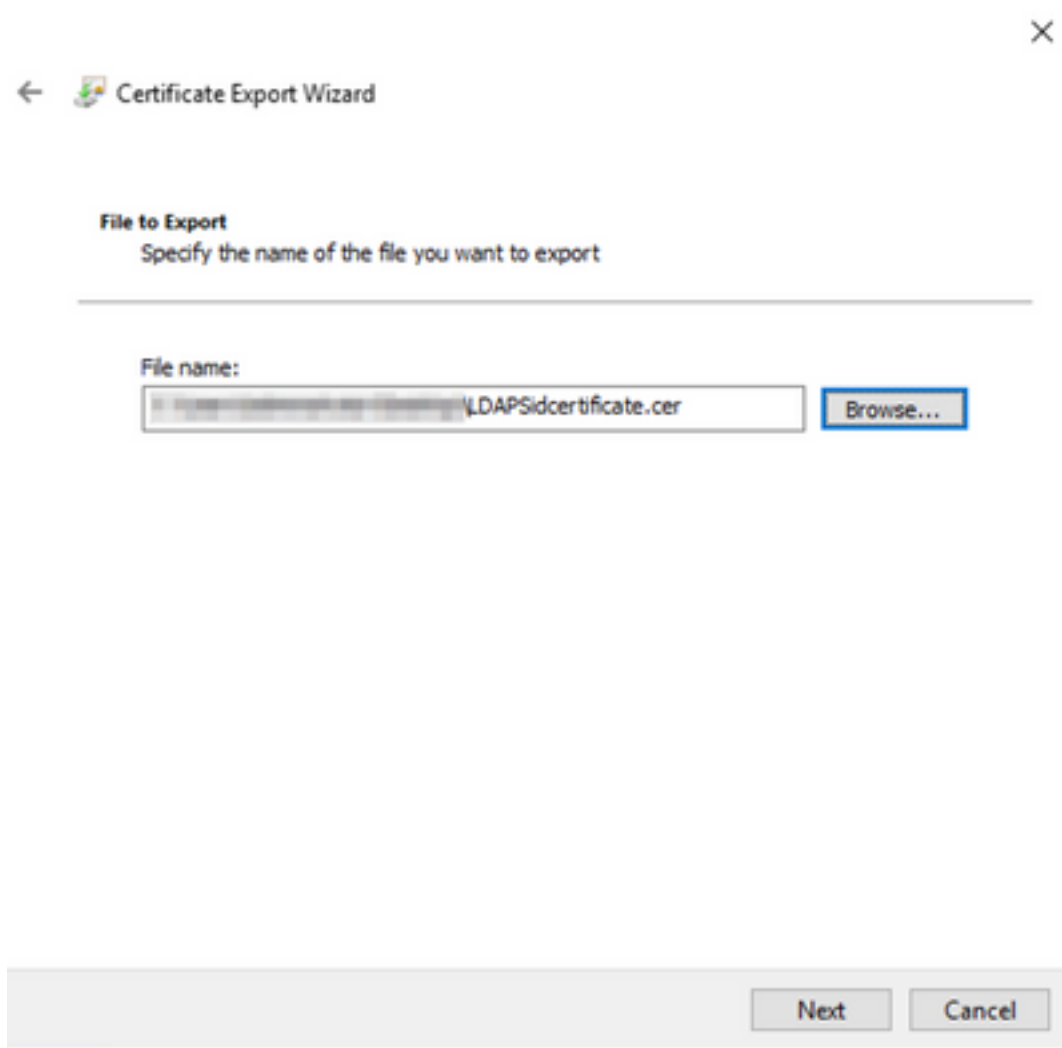
Certificates can be exported in a variety of file formats.

Select the format you want to use:

- DER encoded binary X.509 (.CER)
- Base-64 encoded X.509 (.CER)
- Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
  - Include all certificates in the certification path if possible
- Personal Information Exchange - PKCS #12 (.PFX)
  - Include all certificates in the certification path if possible
  - Delete the private key if the export is successful
  - Export all extended properties
  - Enable certificate privacy
- Microsoft Serialized Certificate Store (.SST)

Next Cancel

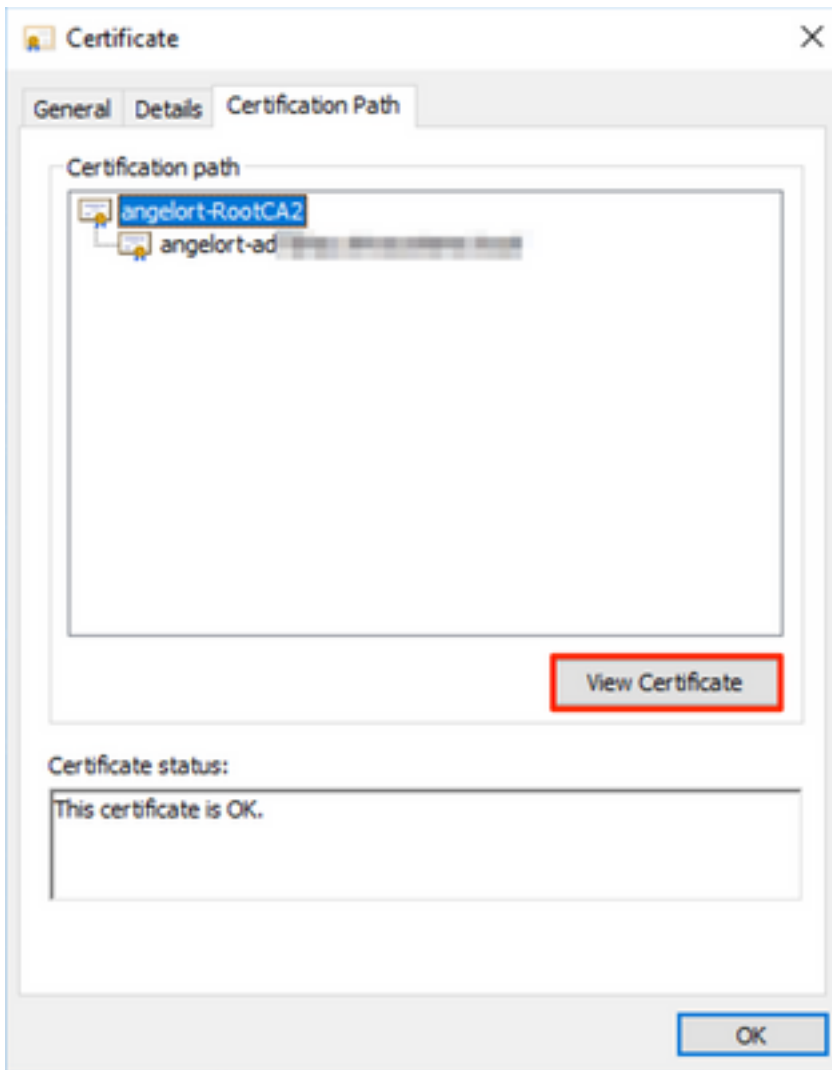
13. Selecione um local para armazenar o certificado, nomeie o arquivo e clique em **Avançar**.



14. Clique em **Concluir**, você deve obter um "A exportação foi bem-sucedida". mensagem.

15. Volte para o certificado usado para LDAPS e selecione a guia **Caminho de certificação**.

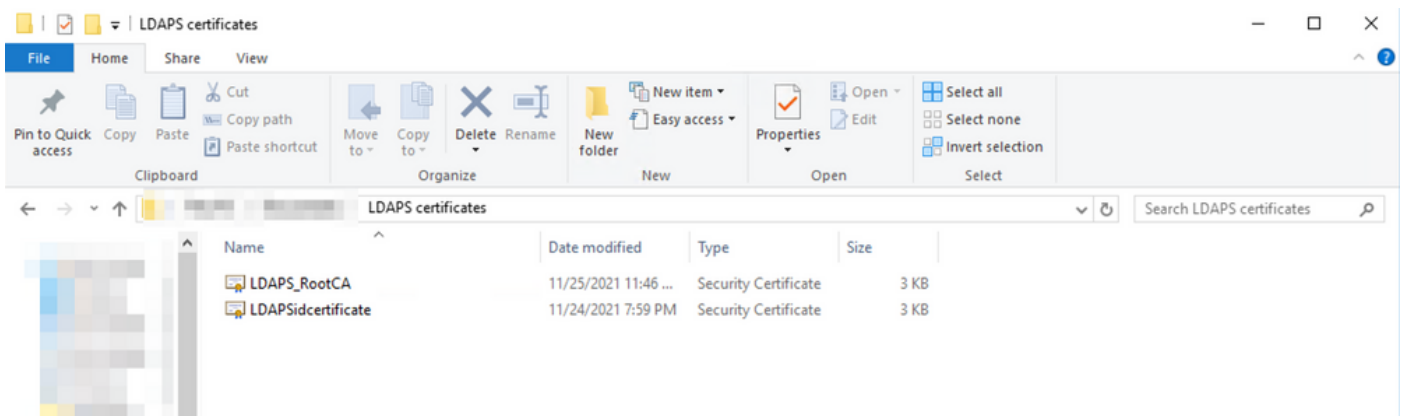
16. Selecione o emissor da CA raiz sobre o caminho de certificação e clique em **Exibir certificado**.



17. Repita as etapas 10-14 para exportar o certificado da CA raiz que assinou o certificado usado para autenticação LDAPS.

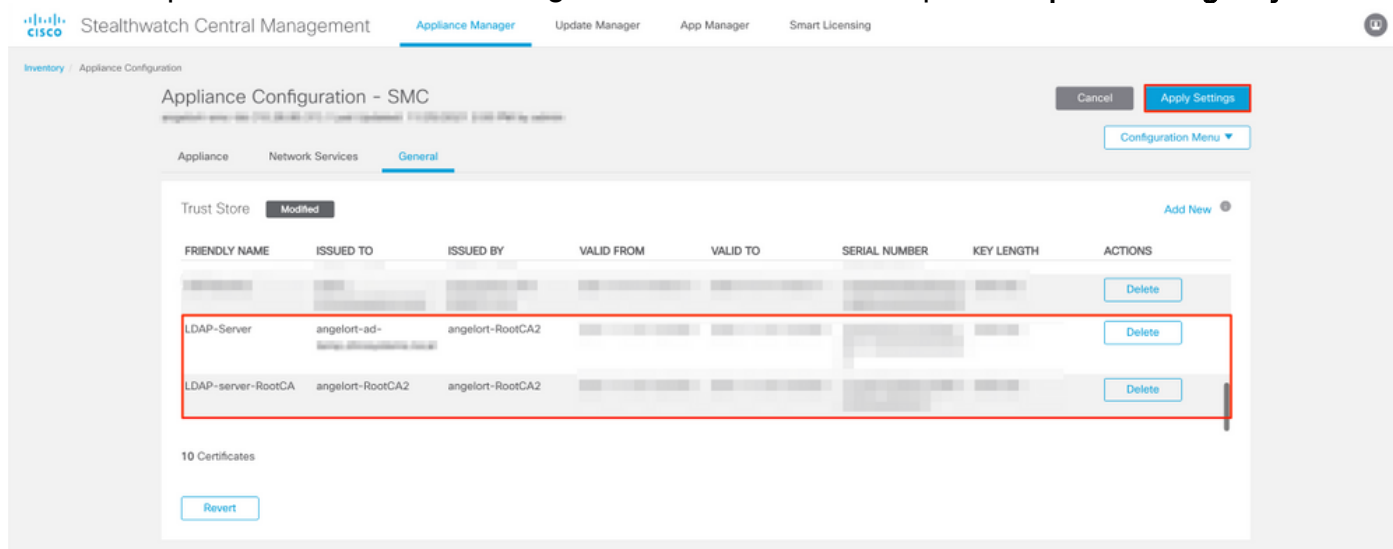
**Note:** Sua implantação pode ter uma hierarquia de CA multicamada, caso em que você precisa seguir o mesmo procedimento para exportar todos os certificados intermediários na cadeia de confiança.

18. Antes de continuar, certifique-se de que tem um ficheiro de certificado para o servidor LDAPS e para cada autoridade emitente no caminho de certificação: Certificado raiz e certificados intermediários (se aplicável).



## Etapa B. Faça login no SNA Manager para adicionar o certificado do servidor LDAP e da cadeia raiz.

1. Navegue até **Central Management > Inventory**.
2. Localize o dispositivo SNA Manager e clique em **Actions > Edit Appliance Configuration**.
3. Na janela Appliance Configuration, navegue até **Configuration Menu > Trust Store > Add New**.
4. Digite o nome amigável, clique em **Escolher arquivo**, selecione o certificado do servidor LDAP e clique em **Adicionar certificado**.
5. Repita a etapa anterior para adicionar o certificado CA raiz e os certificados intermediários (se aplicável).
6. Verifique se os certificados carregados estão corretos e clique em **Aplicar configurações**.

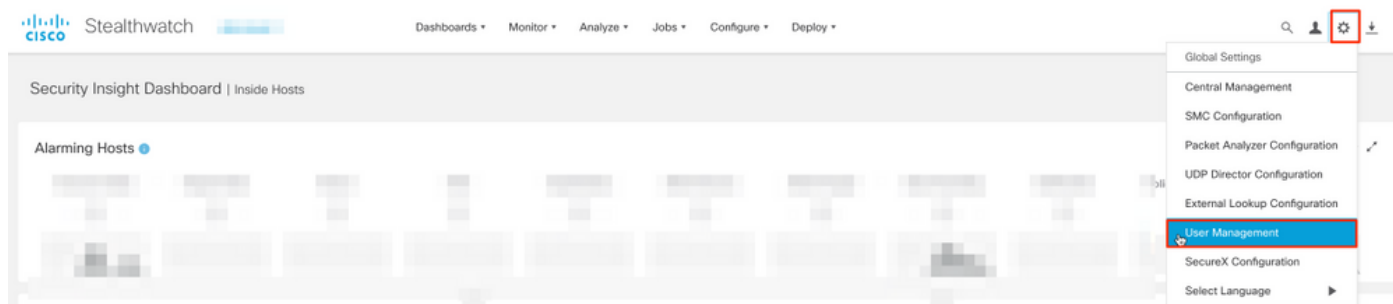


7. Aguarde até que as alterações sejam aplicadas e o status do gerente seja **ativado**.

## Etapa C. Adicione a configuração do serviço externo LDAP.

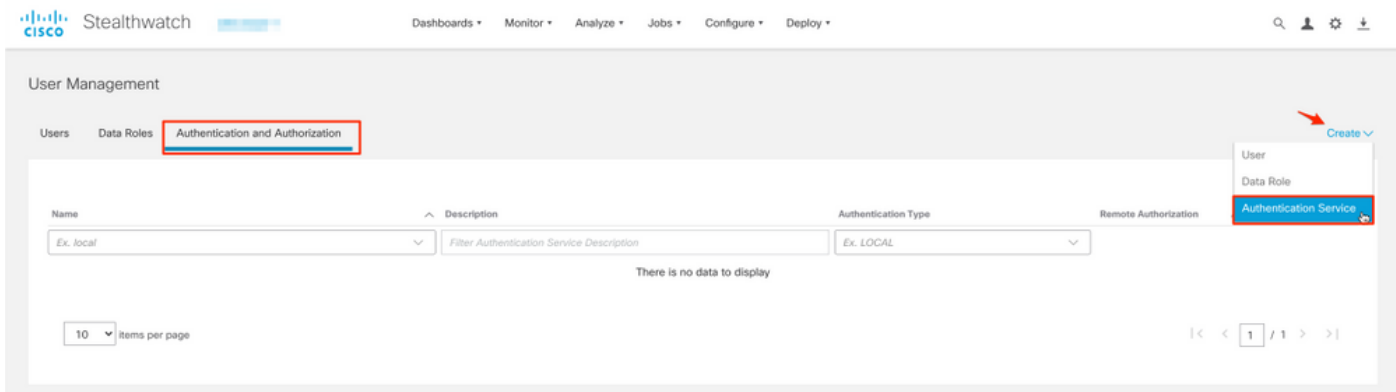
### SNA versão 7.2 ou posterior

1. Abra o painel principal do Gerente e navegue para **Configurações globais > Gerenciamento do usuário**.



2. Na janela Gerenciamento do usuário, selecione a guia **Autenticação e autorização**.
3. Clique em **Create > Authentication Service**.





4. No menu suspenso **Authentication Service**, selecione **LDAP**.

5. Preencha os campos obrigatórios.

### Campo

Nome amigável

Descrição

Endereço do servidor

Porta

Vincular usuário

### Notas

Digite um nome para o LDAP server.

Digite uma descrição para o servidor LDAP.

**Insira o nome de domínio totalmente qualificado conforme especificado no campo Subject Alternative Name (SAN) (Nome alternativo do assunto) do certificado do servidor LDAP.**

- Se o campo SAN contiver apenas o endereço IPv4, insira o endereço IPv4 no campo Server Address (Endereço do servidor).
- Se o campo SAN contiver o nome DNS, insira o nome DNS no campo Server Address (Endereço do servidor).
- Se o campo SAN contiver valores de DNS e IP, use o primeiro valor listado.

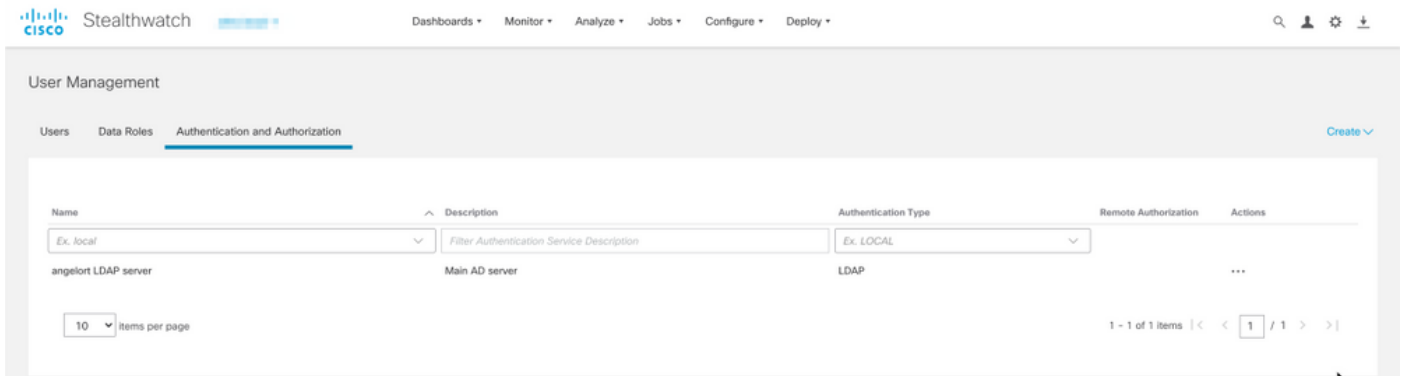
Digite a porta designada para comunicação LDAP segura (LDAP sobre TLS). A porta TCP conhecida para LDAPS é 636.

Digite a ID de usuário usada para se conectar ao servidor LDAP. Por exemplo: CN=admin,OU=Usuários,DC=exemplo,DC=com

**Note:** Se você adicionou seus usuários a um contêiner AD integrado (por exemplo, "Usuários"), o DN de vinculação do usuário deve ter o nome canônico (CN) definido para a partilha interna (por exemplo, CN=nome de usuário, CN=Usuários, DC=domínio, DC=com). No entanto, se você adicionou seus usuários a um novo contêiner, o DN de vinculação deve ter a unidade organizacional (OU) definida com o novo nome do contêiner (por exemplo, CN=username, OU=Corporate Users, DC=domain, DC=com).

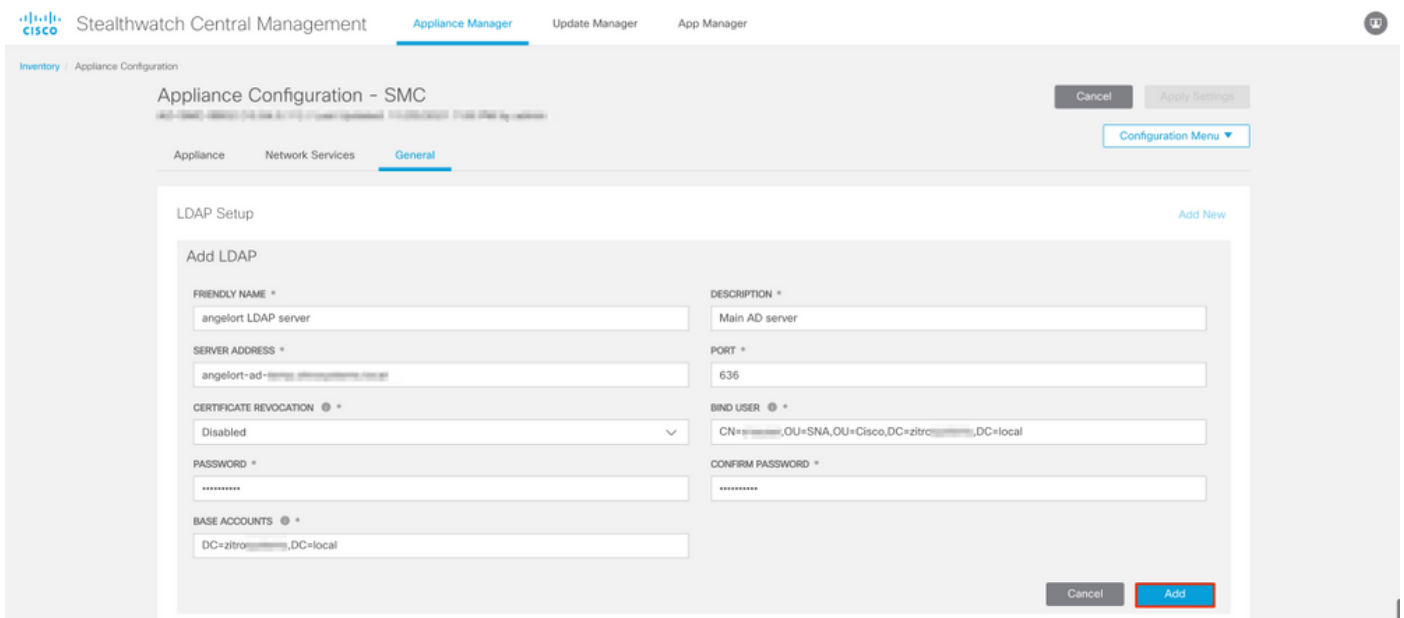
**Note:** Uma maneira útil de localizar o DN de





## SNA versão 7.1

1. Navegue até **Central Management** > Inventory.
2. Localize o dispositivo SMC e clique em **Actions** > **Edit Appliance Configuration**.
3. Na janela Appliance Configuration , navegue até **Configuration Menu** > **LDAP Setup** > **Add New**.
4. Preencha os campos obrigatórios conforme descrito na **SNA Versão 7.2** ou posterior etapa 5.



5. Clique em Add.
6. Clique em **Aplicar configurações**.
7. Quando as configurações inseridas e os certificados adicionados ao repositório de confiança estiverem corretos, as alterações no Gerenciador serão aplicadas e o estado do aplicativo deverá estar **Ativo**.

## Etapa D. Defina as configurações de autorização.

O SNA suporta autorização local e remota via LDAP. Com essa configuração, os grupos LDAP do Servidor AD são mapeados para funções SNA internas ou personalizadas.

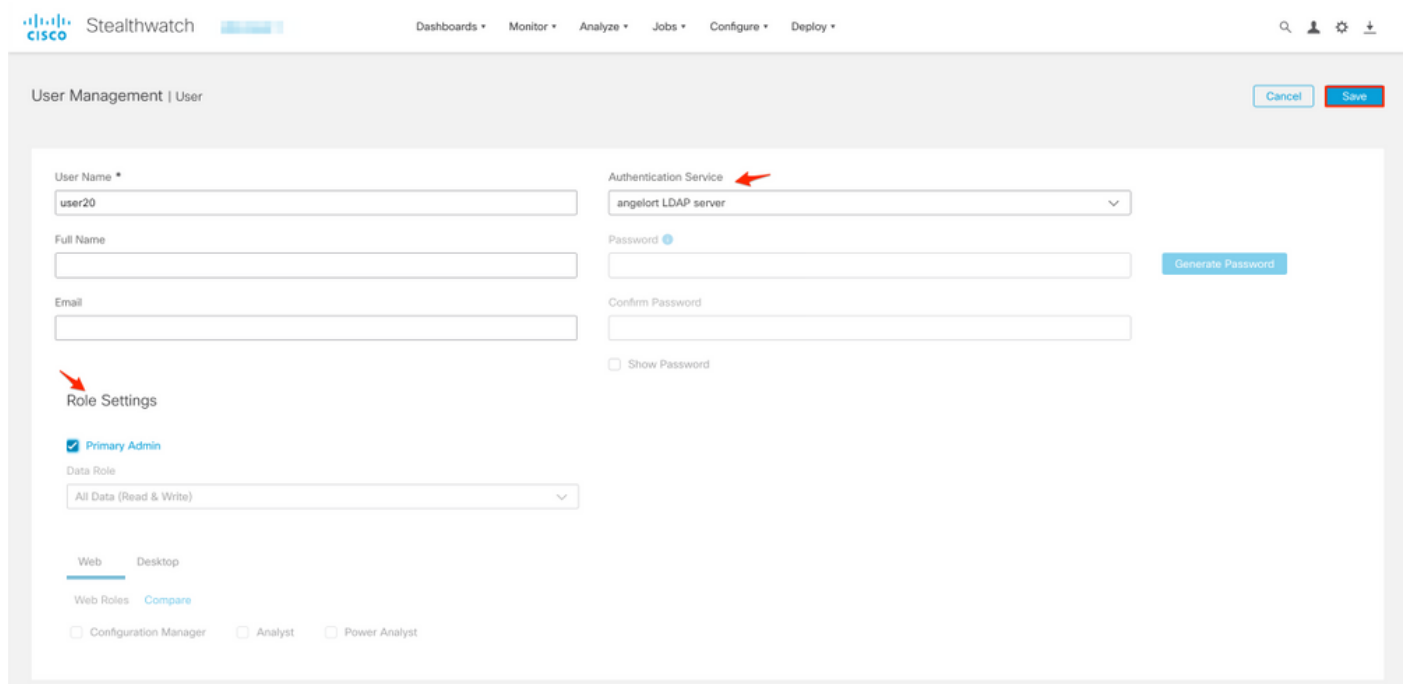
Os métodos de autenticação e autorização suportados para SNA via LDAP são:

- Autenticação remota e autorização local
- Autenticação remota e autorização remota (somente compatível com SNA versão 7.2.1 ou posterior)

## Autorização local

Nesse caso, os usuários e suas funções precisam ser definidos localmente. Para isso, faça o seguinte:

1. Navegue para **Gerenciamento de usuários** novamente, clique na guia **Usuários > Criar > Usuário**.
2. Defina o nome de usuário para autenticar com o servidor LDAP e selecione o servidor configurado no menu suspenso **Authentication Service**.
3. Defina as permissões que o usuário deve ter sobre o Gerenciador depois que ele for autenticado pelo servidor LDAP e clique em **Salvar**.



The screenshot shows the 'User Management | User' configuration page in the Cisco Stealthwatch interface. The page includes a navigation bar with 'Stealthwatch' and various menu items like 'Dashboards', 'Monitor', 'Analyze', 'Jobs', 'Configure', and 'Deploy'. The main form is titled 'User Management | User' and has 'Cancel' and 'Save' buttons. The form fields include: 'User Name' (filled with 'user20'), 'Full Name', 'Email', 'Authentication Service' (a dropdown menu with 'angelort LDAP server' selected, indicated by a red arrow), 'Password', 'Confirm Password', and a 'Generate Password' button. Below the form, there is a 'Role Settings' section with a red arrow pointing to it. It includes a checked 'Primary Admin' checkbox, a 'Data Role' dropdown menu (set to 'All Data (Read & Write)'), and a 'Web' tab. Under the 'Web' tab, there are 'Web Roles' and a 'Compare' button. At the bottom, there are three unchecked checkboxes: 'Configuration Manager', 'Analyst', and 'Power Analyst'.

## Autorização remota via LDAP

A Autenticação e Autorização Remotas via LDAP foi suportada pela primeira vez no Secure Network Analytics versão 7.2.1.

**Note:** A autorização remota com LDAP não é suportada na versão 7.1.

É importante mencionar que, se um usuário for definido e ativado localmente (no Gerenciador), o usuário será autenticado remotamente, mas autorizado localmente. O processo de seleção do usuário é o seguinte:

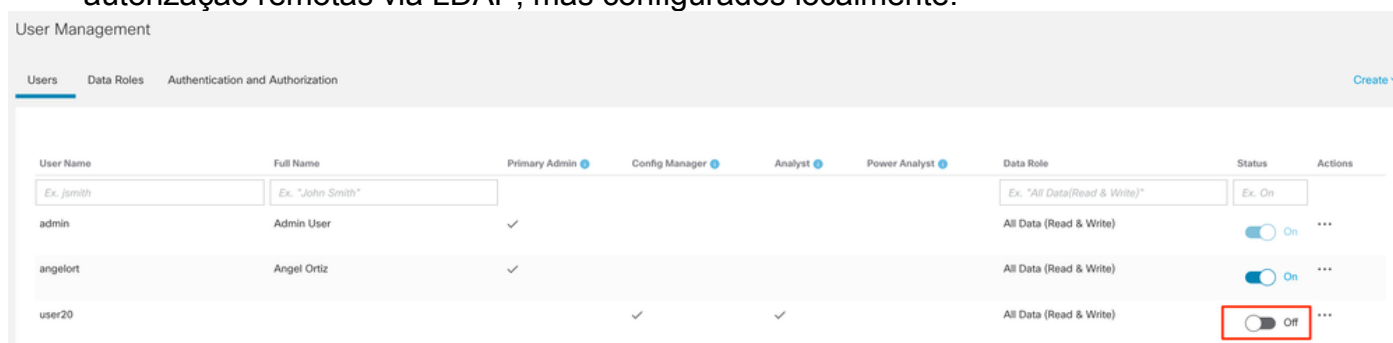
1. Quando as credenciais são inseridas na página de boas-vindas do gerente, o gerente procura um usuário local com o nome especificado.

2. Se um usuário local for encontrado e ativado, ele será autenticado remotamente (se a autenticação remota via LDAP com autorização local tiver sido configurada anteriormente), mas autorizado com as configurações locais.
3. Se a autorização remota estiver configurada e ativada e o usuário não for encontrado localmente (não configurado ou desativado), tanto a autenticação quanto a autorização serão executadas remotamente.

Por esse motivo, as etapas para configurar com êxito a autenticação remota são..

### Etapa D-1. Desabilite ou exclua os usuários destinados a usar autorização remota, mas que são definidos localmente.

1. Abra o painel principal do Gerente e navegue até Configurações globais > Gerenciamento do usuário.
2. Desabilite ou exclua os usuários (se eles existirem) destinados a usar autenticação e autorização remotas via LDAP, mas configurados localmente.



### Etapa D-2. Defina o cisco-stealthwatch Groups no servidor Microsoft AD.

Para Autenticação externa e autorização via usuários LDAP, as senhas e grupos *cisco-stealthwatch* são definidos remotamente no Microsoft Active Directory. Os grupos *cisco-stealthwatch* a serem definidos no servidor AD estão relacionados às diferentes funções que a SNA tem, eles devem ser definidos da seguinte forma.

#### Função SNA

Administrador principal

#### Nome do(s) grupo(s)

- cisco-stealthwatch-master-admin
- cisco-stealthwatch-all-data-read-and-write
- cisco-stealthwatch-all-data-read-only
- cisco-stealthwatch-<custom> (opcional)

Função de dados

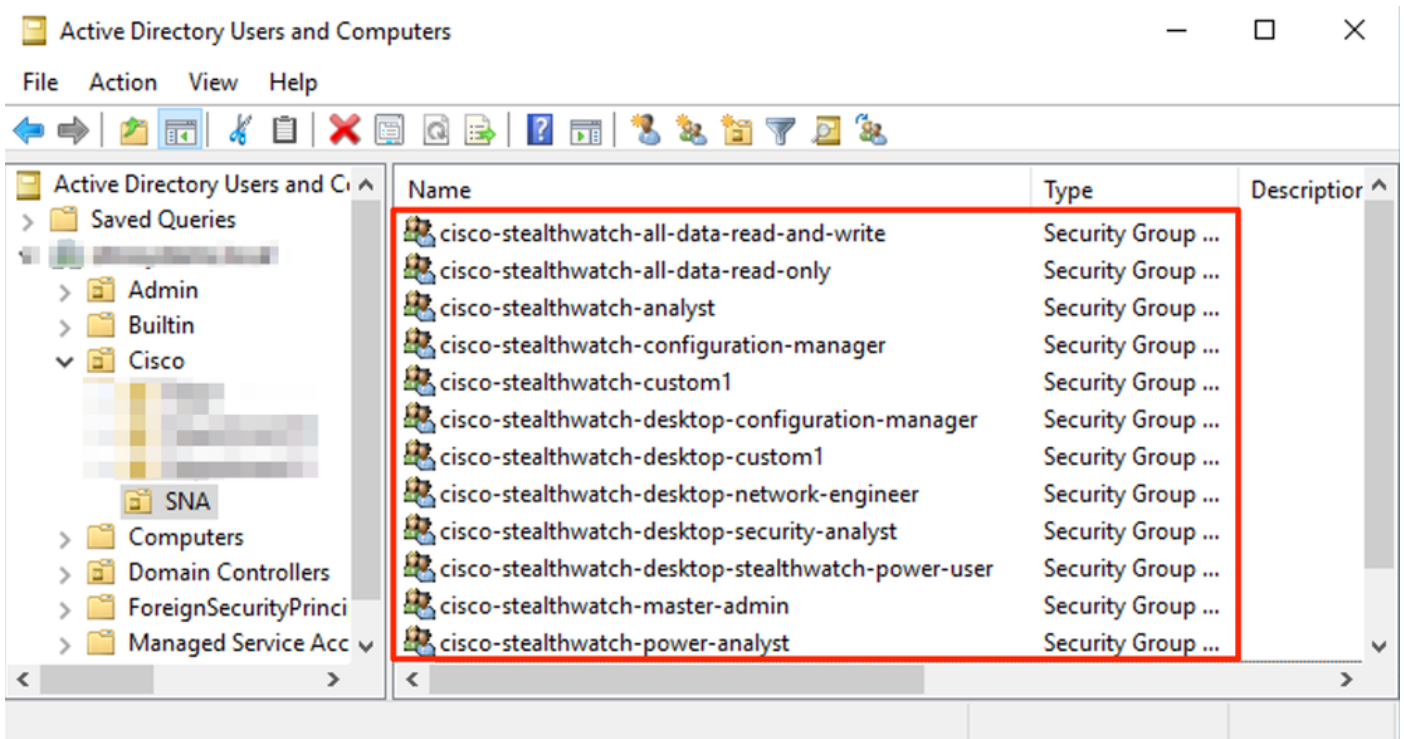
**Note:** Certifique-se de que os grupos de função de dados personalizados comecem com o "cisco-stealthwatch-".

Função funcional da Web

- cisco-stealthwatch-configuration-manager
- cisco-stealthwatch-power-analyst
- cisco-stealthwatch-analyst
- cisco-stealthwatch-desktop-stealthwatch-power-analyst
- cisco-stealthwatch-desktop-configuration-manager
- cisco-stealthwatch-desktop-network-engineer
- cisco-stealthwatch-desktop-security-analyst
- cisco-stealthwatch-desktop-<custom> (opcional)

Função funcional da área de trabalho

**Note:** Certifique-se de que os grupos de função de desktop personalizados comecem com o "cisco-stealthwatch-desktop-".

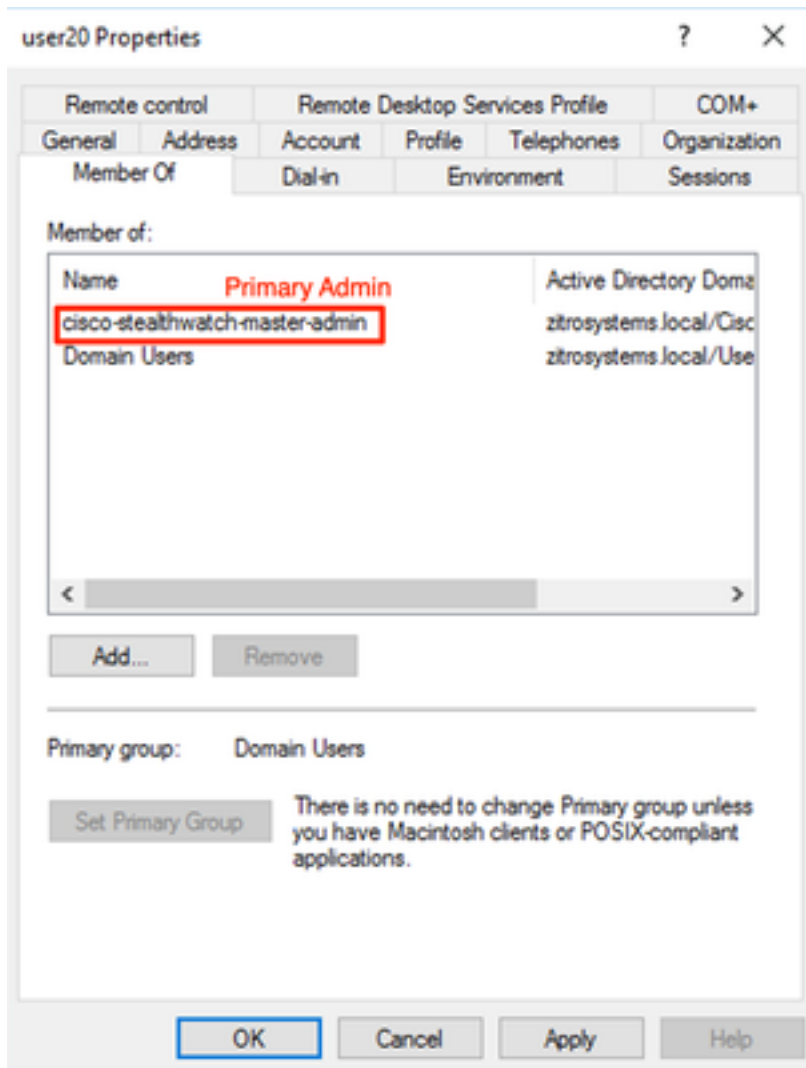


**Note:** Conforme descrito anteriormente, grupos personalizados são suportados para "Função de dados" e "Função funcional da área de trabalho", desde que o nome do grupo seja anexado à sequência correta. Essas funções e grupos personalizados devem ser definidos no SNA Manager e no servidor do Ative Directory. Por exemplo, se você definir uma função personalizada "custom1" no SNA Manager para uma função de cliente de desktop, ela deverá ser mapeada para cisco-stealthwatch-desktop-custom1 no Ative Directory.

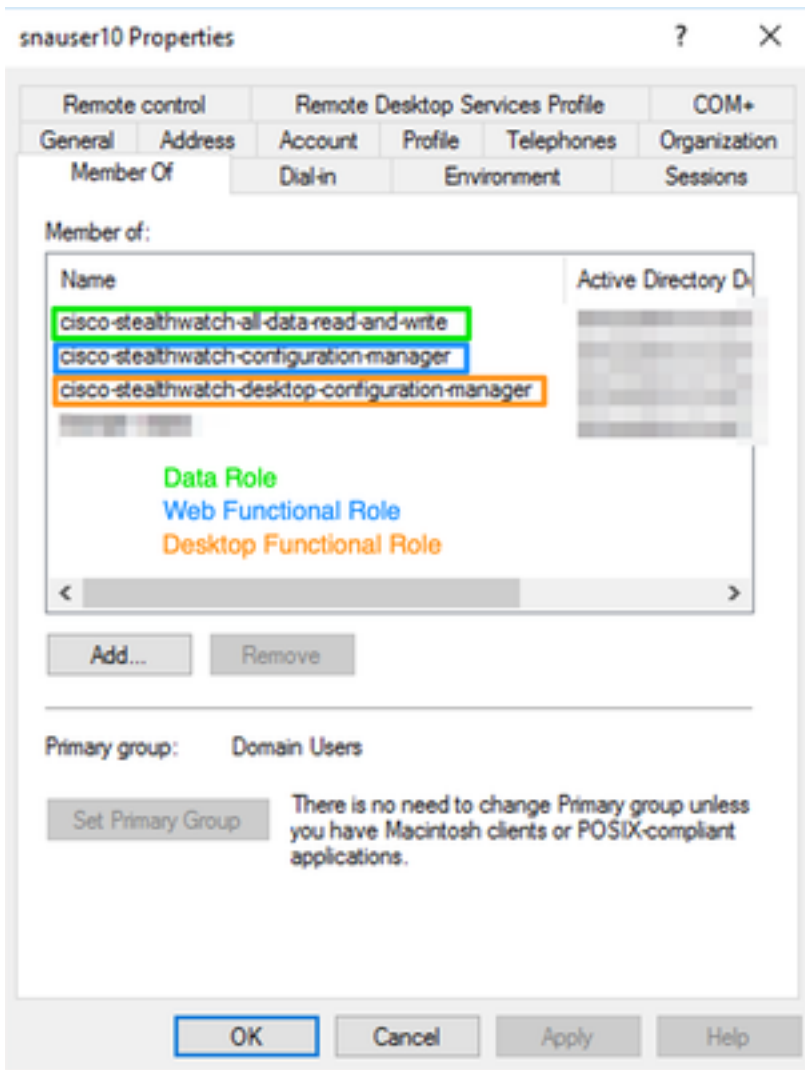
### Etapa D-3. Defina Mapeamentos de grupos de autorização LDAP para os usuários.

Depois que os grupos *cisco-stealthwatch* forem definidos no servidor AD, poderemos mapear os usuários destinados a ter acesso ao SNA Manager para os grupos necessários. Isso deve ser feito da seguinte forma.

- Um usuário **administrador principal** deve ser atribuído ao grupo *cisco-stealthwatch-master-admin* e **não deve ser membro de nenhum outro grupo do *cisco-stealthwatch*.**



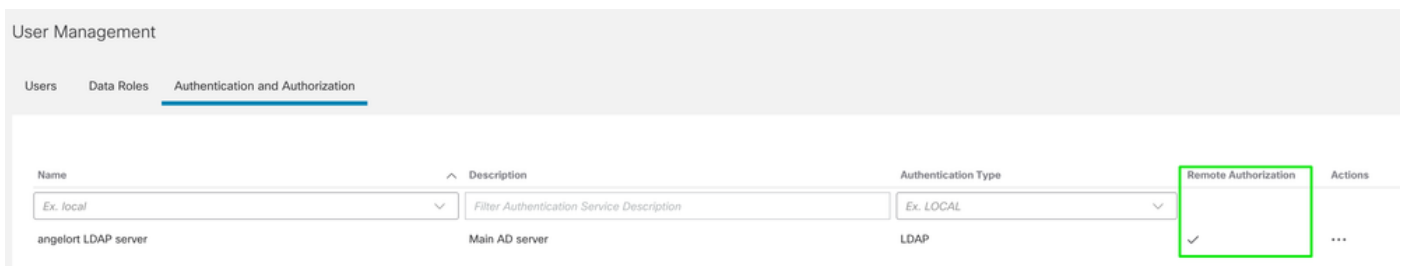
- Cada usuário, além dos usuários do Administrador principal, deve ser atribuído a um grupo de cada função com as próximas condições.
  1. **Função de dados:** O usuário deve ser atribuído a **apenas um grupo**.
  2. **Função funcional da Web:** O usuário deve ser atribuído a **pelo menos um grupo**.
  3. **Função funcional da área de trabalho:** O usuário deve ser atribuído a **pelo menos um grupo**.



#### Etapa D-4. Ative a autorização remota via LDAP no SNA Manager.

1. Abra o painel principal do Gerente e navegue para **Configurações globais > Gerenciamento do usuário**.
2. Na janela **User Management**, selecione a guia **Authentication and Authorization (Autenticação e autorização)**.
3. Localize o serviço de autenticação LDAP configurado na **Etapa C**.
4. Clique em **Ações > Ativar autorização remota**.

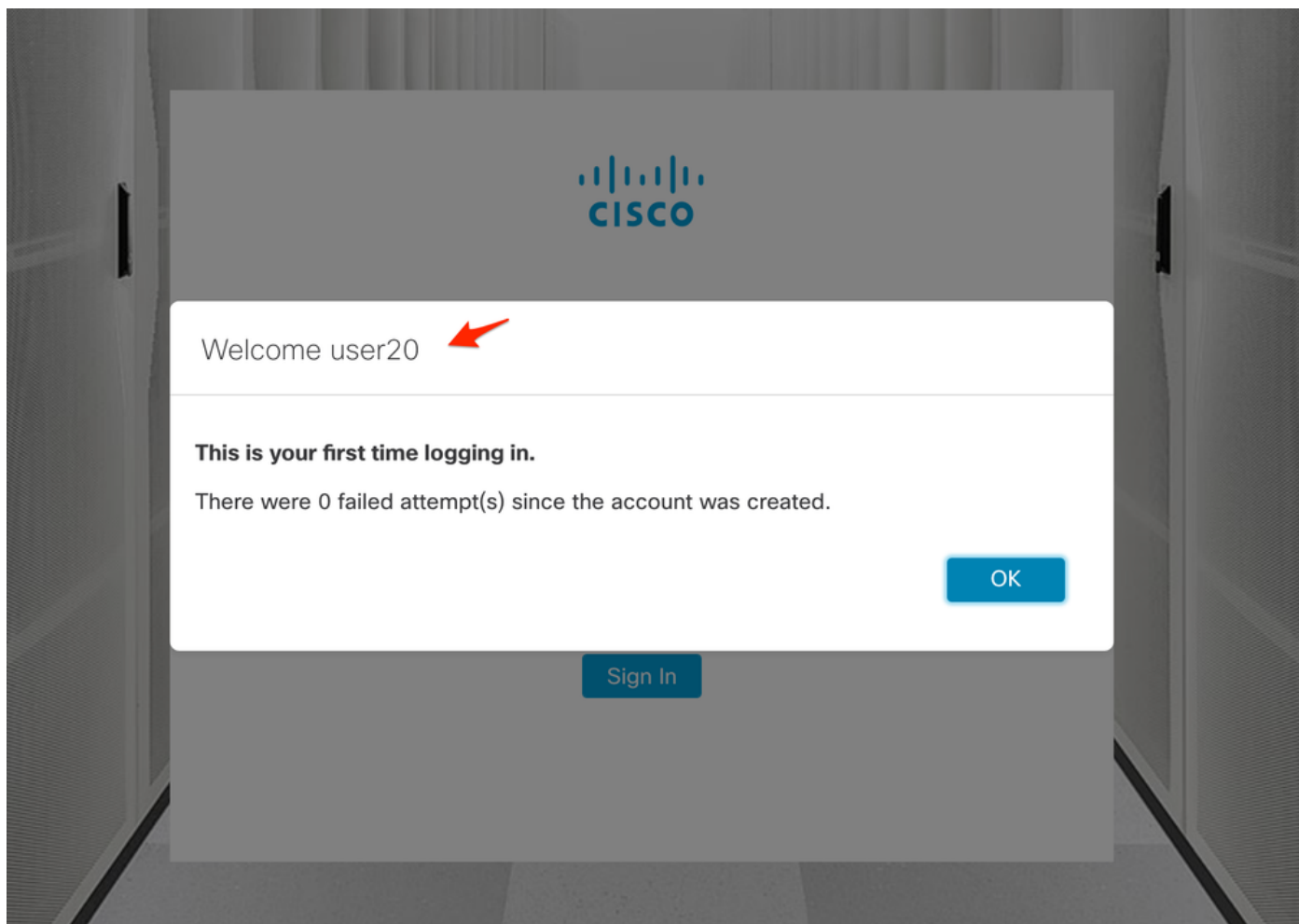
**Note:** Apenas um serviço de Autorização externa pode estar em uso de cada vez. Se outro serviço de autorização já estiver em uso, ele será automaticamente desabilitado e o novo será habilitado, no entanto, todos os usuários autorizados com o serviço externo anterior serão desconectados. Uma mensagem de confirmação é exibida antes que qualquer ação ocorra.



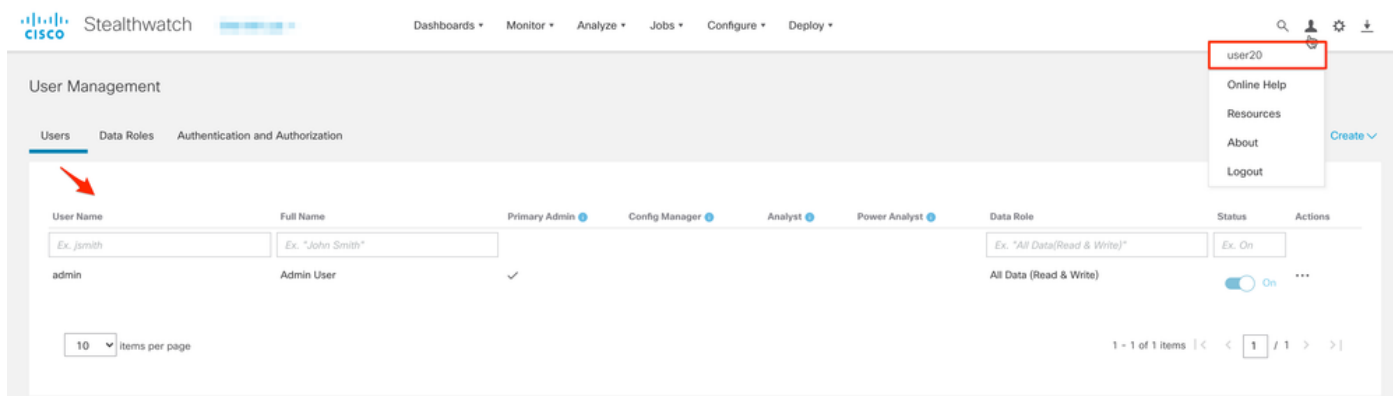


# Verificar

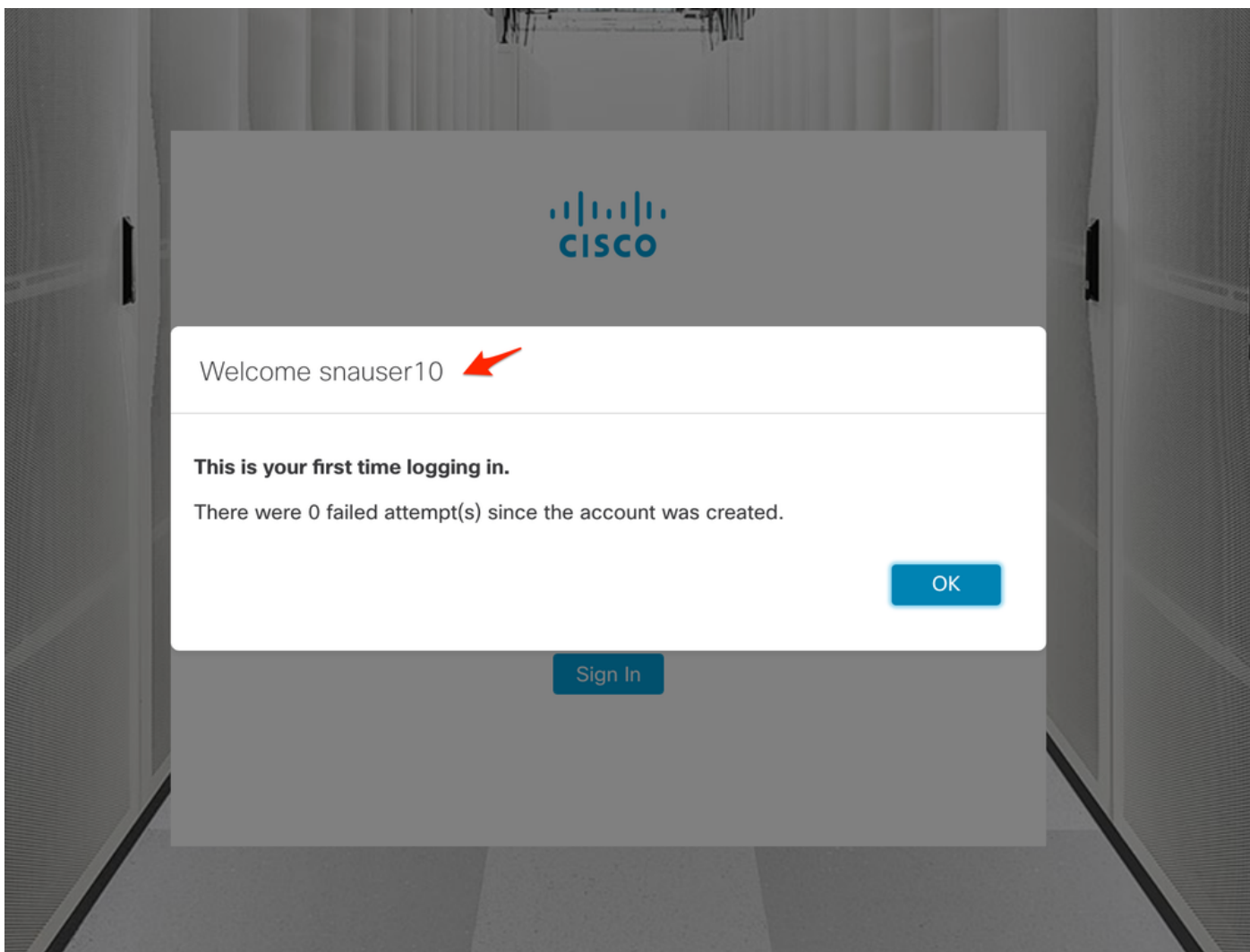
Os usuários podem fazer logon com as credenciais definidas no servidor do AD.



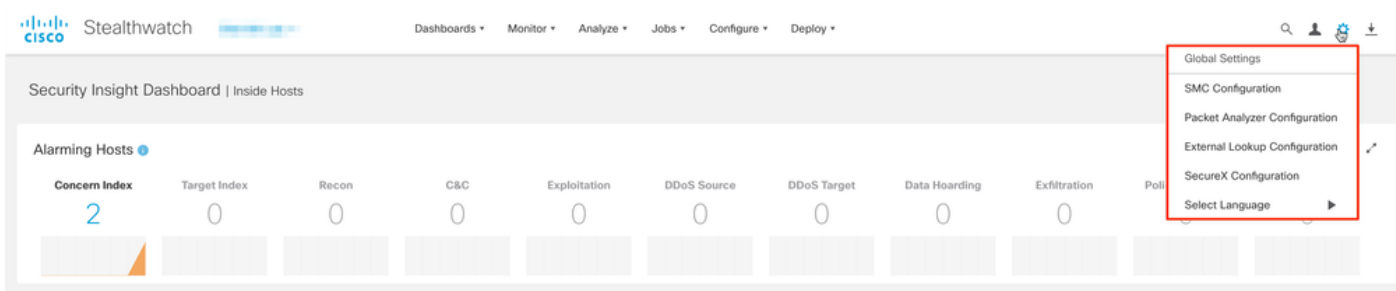
A segunda etapa de verificação diz respeito à autorização. Neste exemplo, o usuário "user20" se tornou um membro do grupo *cisco-stealthwatch-master-admin* no servidor AD e podemos confirmar se o usuário tem permissões de Administrador Primário. O usuário não está definido nos usuários locais, portanto podemos confirmar se os atributos de autorização foram enviados pelo servidor do AD.



A mesma verificação é feita para o outro usuário neste exemplo "snauser10". Podemos confirmar a autenticação com êxito com as credenciais configuradas no servidor AD.



Para a verificação de autorização, como este usuário não pertence ao grupo Administrador primário, alguns recursos não estão disponíveis.



## Troubleshoot

Se a configuração do Serviço de Autenticação não puder ser salva, verifique se:

1. Você adicionou os certificados apropriados do servidor LDAP ao armazenamento confiável do gerente.
2. O **Endereço do Servidor** configurado é conforme especificado no campo Nome Alternativo do Assunto (SAN) do certificado do servidor LDAP. Se o campo SAN contiver apenas o endereço IPv4, insira o endereço IPv4 no campo Server Address (Endereço do servidor). Se o campo SAN contiver o nome DNS, insira o nome DNS no campo Server Address (Endereço do servidor). Se o campo SAN contiver valores de DNS e IPv4, use o primeiro

valor listado.

3. Os campos **Vincular usuário** e **Conta base** configurados estão corretos, conforme especificado pelo Controlador de domínio do AD.

## Informações Relacionadas

Para obter assistência adicional, entre em contato com o Cisco Technical Assistance Center (TAC). É necessário um contrato de suporte válido: [Contatos de suporte da Cisco no mundo inteiro](#).