Konfigurieren der externen Authentifizierung und Autorisierung über LDAPS für den Zugriff auf Secure Network Analytics Manager

Inhalt

Einleitung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Konfigurieren
Schritt A: Melden Sie sich beim AD-Domänencontroller an, und exportieren Sie das für LDAP verwendete SSL-Zertifikat.
Schritt B: Melden Sie sich beim SNA Manager an, um das Zertifikat des LDAP-Servers und der Stammkette hinzuzufügen.
Schritt C: Hinzufügen der Konfiguration des externen LDAP-Diensts.
SNA Version 7.2 oder höher
SNA Version 7.1
Schritt D. Konfigurieren der Autorisierungseinstellungen
Lokale Autorisierung
Remote-Autorisierung über LDAP
Überprüfung
Fehlerbehebung
Zugehörige Informationen

Einleitung

Dieses Dokument beschreibt die Basiskonfiguration eines Secure Network Analytics Manager (ehemals Stealthwatch Management Center) Version 7.1 oder höher, um eine externe Authentifizierung zu verwenden und, mit Version 7.2.1 oder höher, eine externe Autorisierung mit LDAPS zu verwenden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Secure Network Analytics (ehemals Stealthwatch)
- Allgemeiner LDAP- und SSL-Betrieb
- Allgemeines Microsoft Active Directory-Management

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Komponenten:

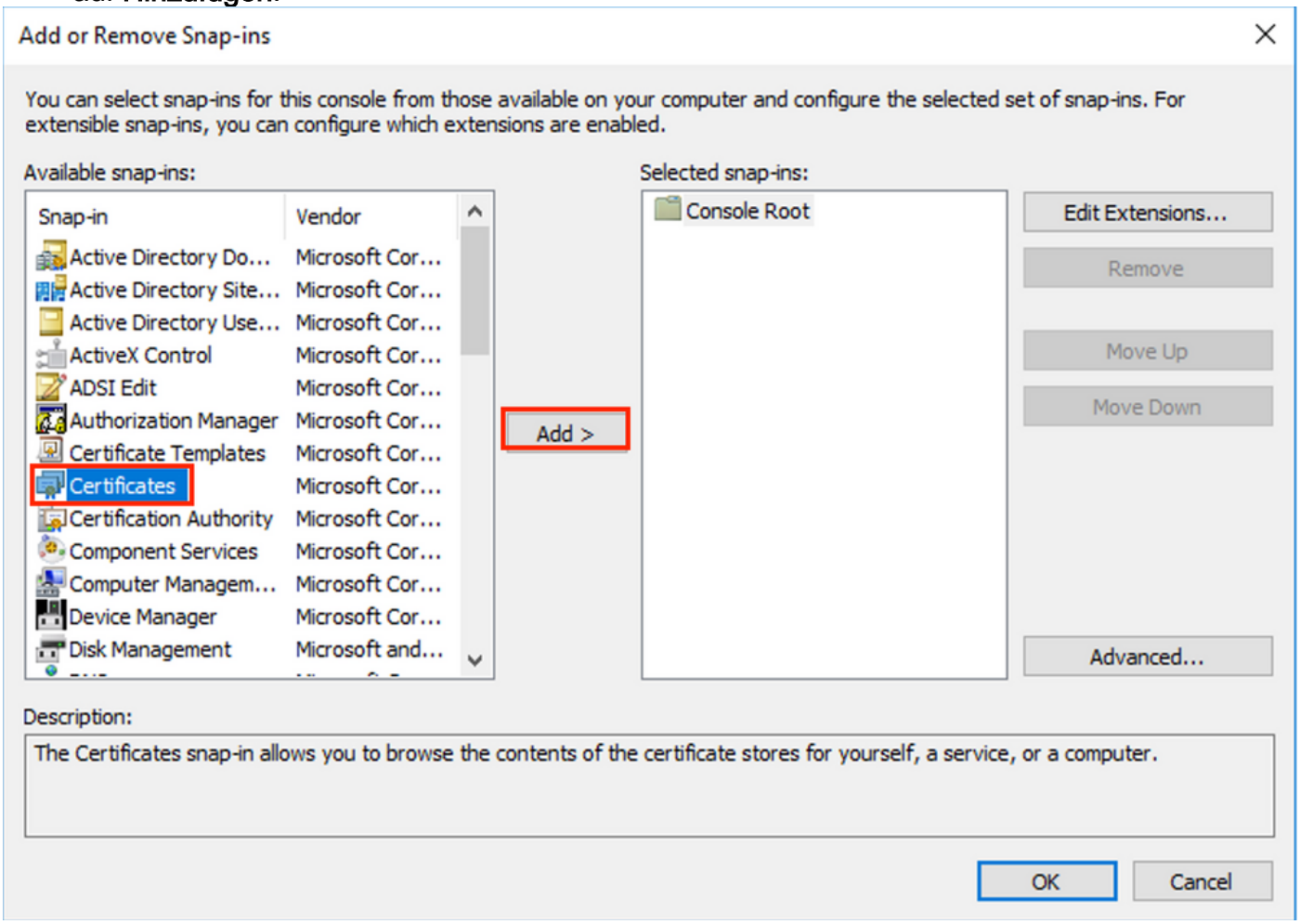
- Cisco Secure Network Analytics Manager (ehemals SMC) Version 7.3.2
- Windows Server 2016 wird als Active Directory-Domänencontroller konfiguriert

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Schritt A: Melden Sie sich beim AD-Domänencontroller an, und exportieren Sie das für LDAP verwendete SSL-Zertifikat.

1. Wählen Sie für Windows Server 2012 oder höher im Startmenü die **Option Ausführen** aus, geben Sie dann **certlm.msc ein** und fahren Sie mit Schritt **8** fort.
2. Bei älteren Windows-Serverversionen wählen Sie **Ausführen** im Startmenü aus, und geben Sie dann **mmc** ein.
3. Wählen Sie im Menü Datei die Option **Einscannen hinzufügen/entfernen**.
4. Wählen Sie in der Liste Verfügbare Snap-Ins die Option **Zertifikate aus**, und klicken Sie dann auf **Hinzufügen**.

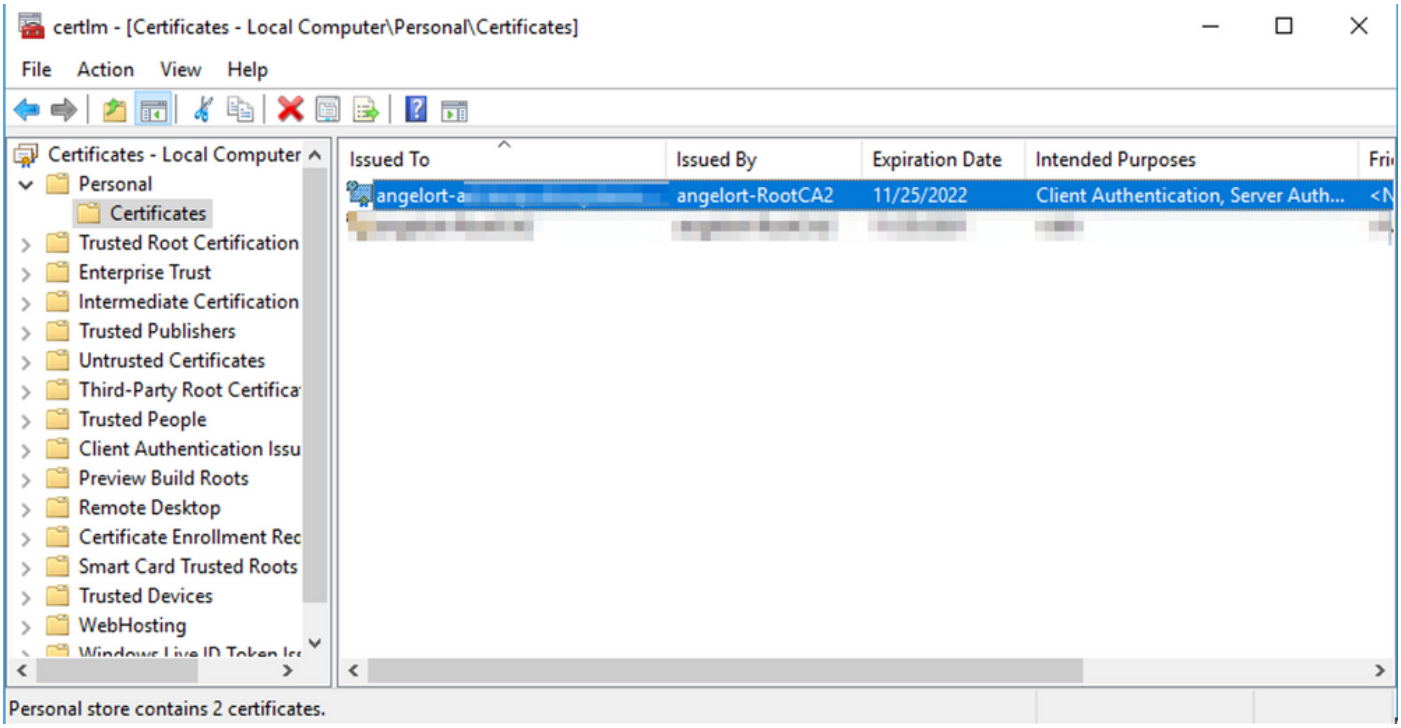


5. Wählen Sie im **Snap-In für Zertifikate** die Option **Computerkonto** und anschließend **Weiter aus**.

6. Lassen Sie **Lokaler Computer** ausgewählt, und wählen Sie **Fertig stellen** aus.

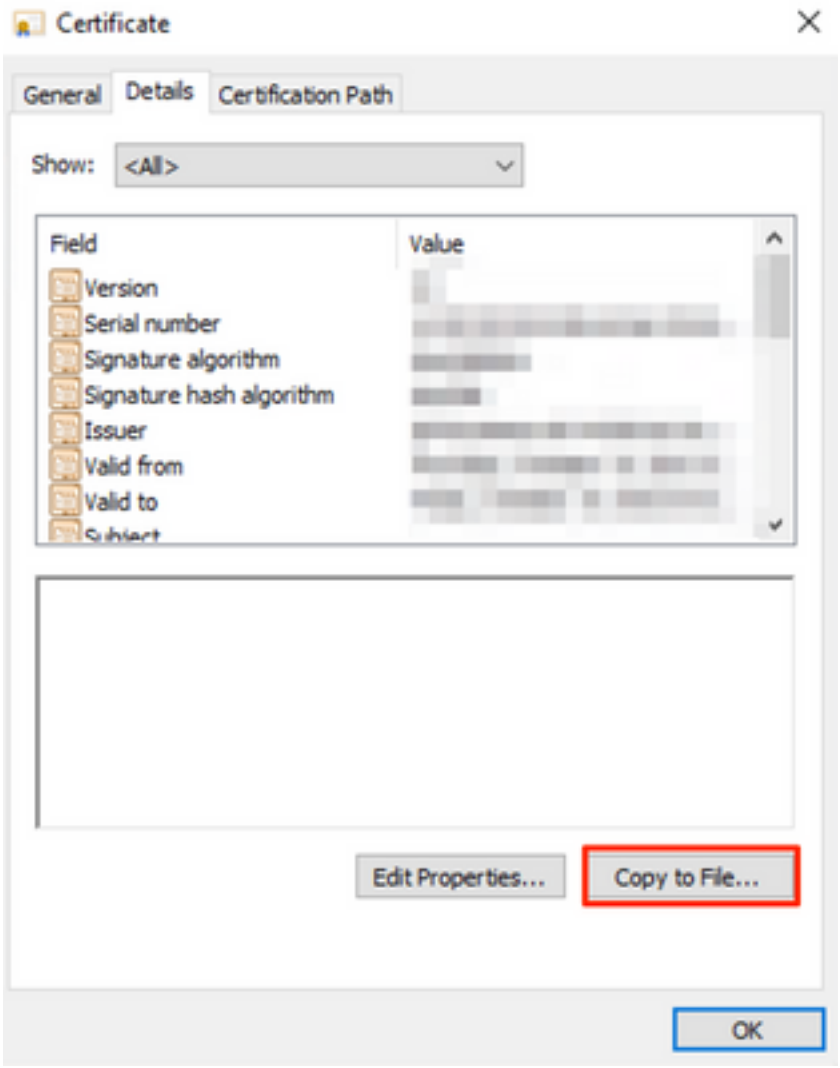
7. Wählen Sie im Fenster **Snap-In hinzufügen oder entfernen die** Option **OK**.

8. Navigieren Sie zu **Zertifikate (Lokaler Computer) > Personal > Certificates (Personal > Zertifikate).**



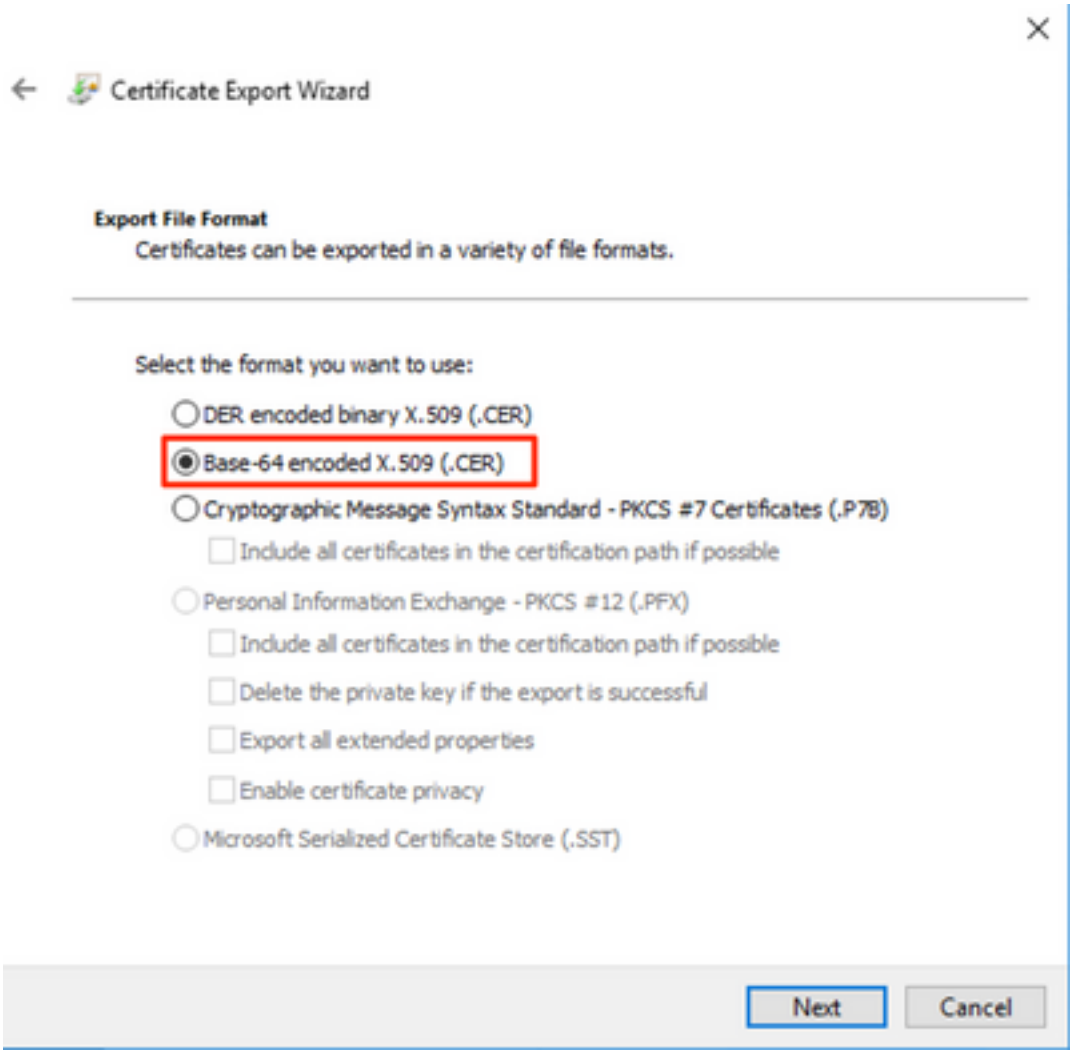
9. Wählen Sie das SSL-Zertifikat aus, das für die LDAPS-Authentifizierung auf Ihrem Domänen-Controller verwendet wird, und klicken Sie mit der rechten Maustaste, und klicken Sie dann auf **Öffnen**.

10. Navigieren Sie zur Registerkarte **Details** > klicken Sie auf **In Datei kopieren > Weiter**

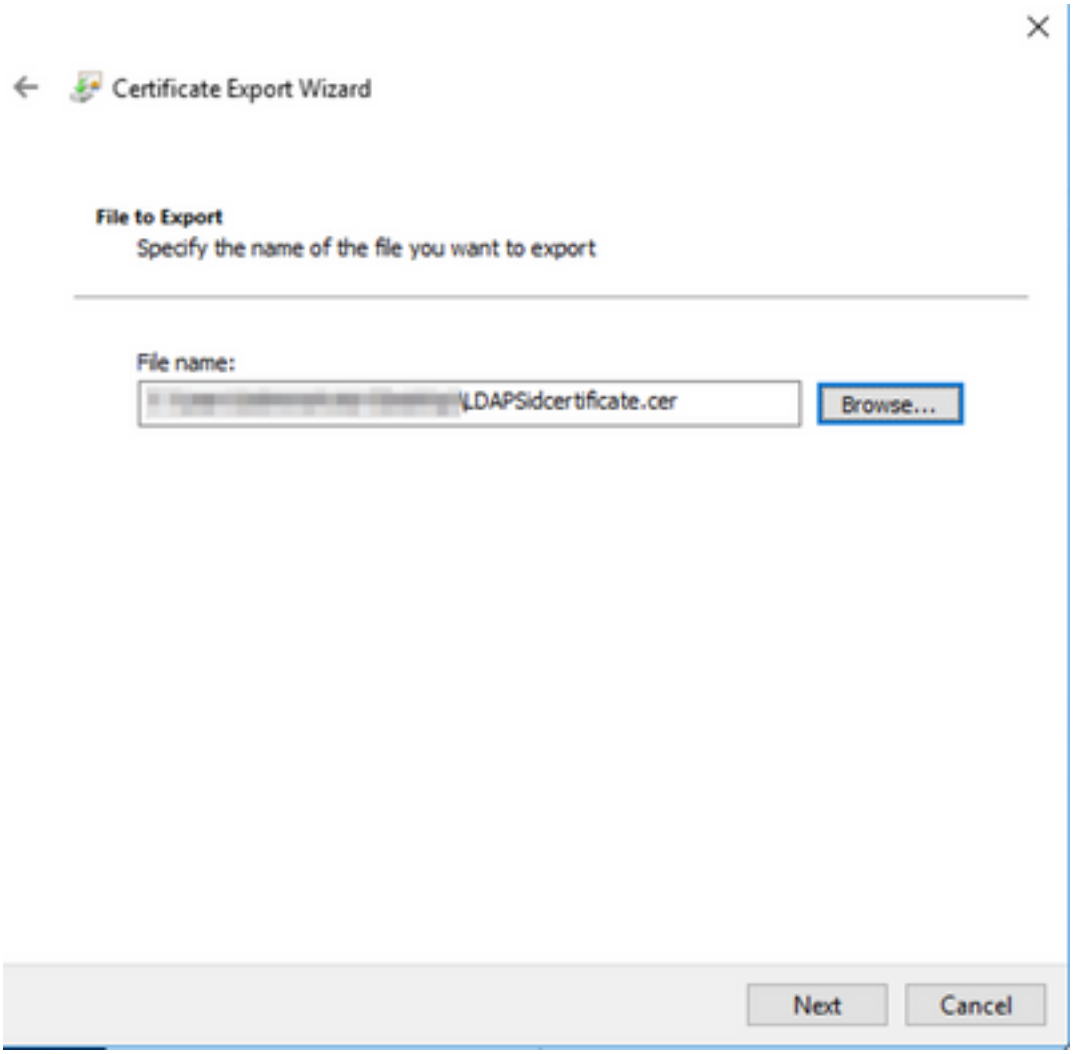


11. Vergewissern Sie sich, dass **Nein, privaten Schlüssel nicht exportieren** ausgewählt ist, und klicken Sie auf **Weiter.**

12. Wählen Sie **Base-64-kodiertes X.509-**Format aus, und klicken Sie auf **Weiter**.



13. Wählen Sie einen Speicherort für das Zertifikat aus, nennen Sie die Datei, und klicken Sie auf **Weiter**.



14. Klicken Sie auf **Fertig stellen**, um die Meldung "Der Export war erfolgreich." zu erhalten. Nachricht.

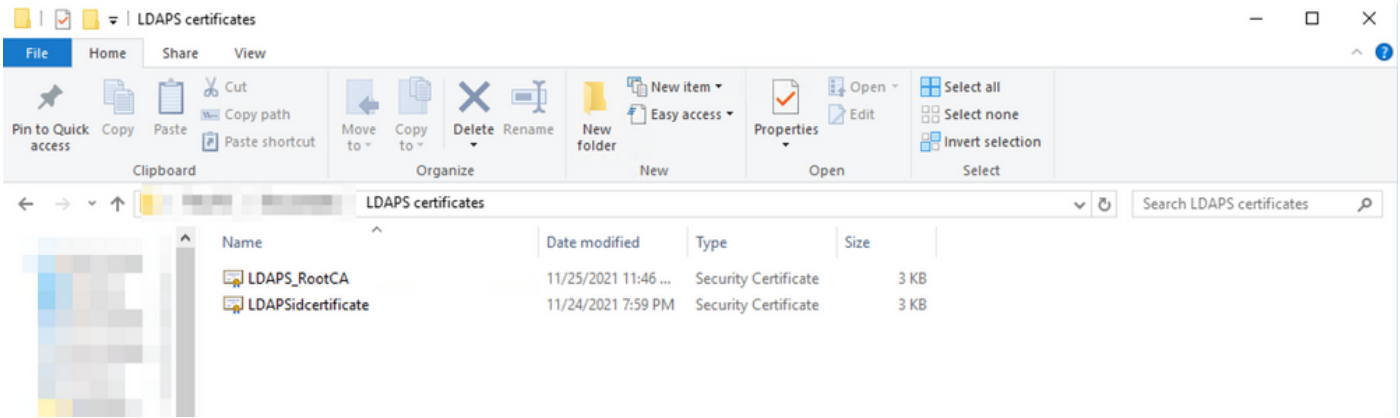
15. Kehren Sie zum für LDAPS verwendeten Zertifikat zurück, und wählen Sie die Registerkarte **Zertifizierungspfad** aus.

16. Wählen Sie oben im Zertifizierungspfad den Root CA-Emittenten aus, und klicken Sie auf **Zertifikat anzeigen**.

17. Wiederholen Sie die Schritte 10-14, um das Zertifikat der Root-Zertifizierungsstelle zu exportieren, die das für die LDAPS-Authentifizierung verwendete Zertifikat signiert hat.

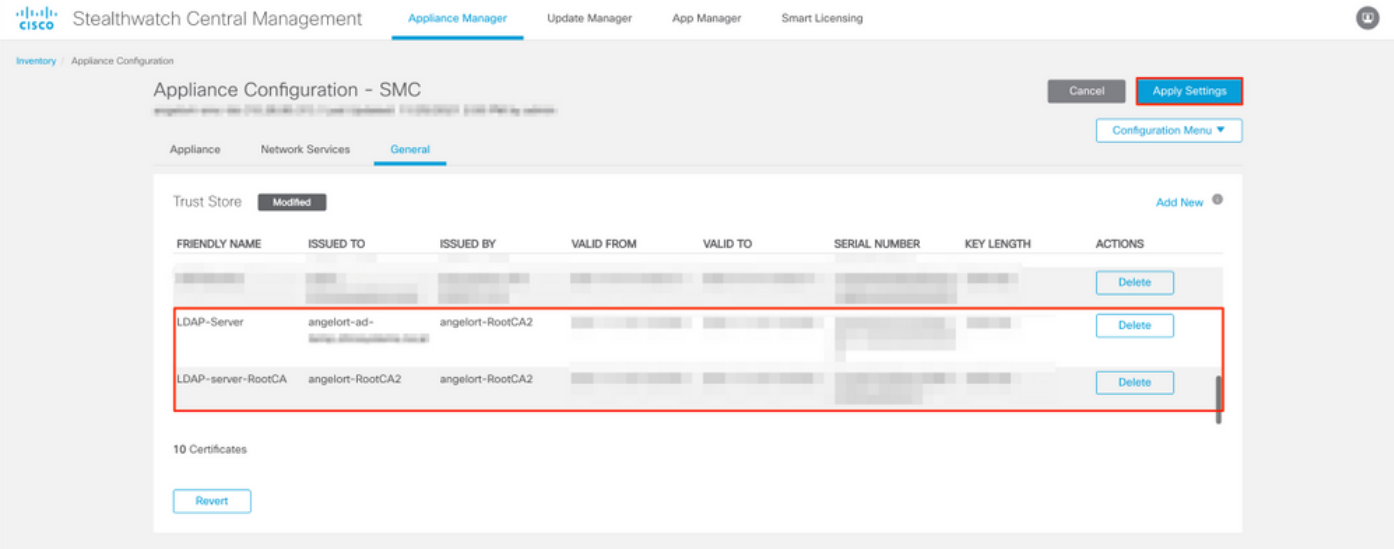
> **Anmerkung:** Ihre Bereitstellung kann über eine mehrschichtige CA-Hierarchie verfügen. In diesem Fall müssen Sie die gleiche Prozedur befolgen, um alle Zwischenzertifikate in der Vertrauenskette zu exportieren.

18. Bevor Sie fortfahren, stellen Sie sicher, dass Sie über eine Zertifikatsdatei für den LDAPS-Server und für jede Emittenten-Behörde im Zertifizierungspfad verfügen: Stammzertifikat und Zwischenzertifikate (falls zutreffend).



Schritt B: Melden Sie sich beim SNA Manager an, um das Zertifikat des LDAP-Servers und der Stammkette hinzuzufügen.

1. Navigieren Sie zu **Zentrale Verwaltung** > Bestand.
2. Suchen Sie die SNA Manager-Appliance, und klicken Sie auf **Aktionen** > **Appliance Configuration (Einheitenkonfiguration bearbeiten)**.
3. Navigieren Sie im Fenster Appliance Configuration (Appliance-Konfiguration) zu **Configuration Menu (Konfigurationsmenü)** > **Trust Store** > **Add New (Neu hinzufügen)**.
4. Geben Sie den Namen des Empfängers ein, klicken Sie auf **Datei auswählen**, und wählen Sie das Zertifikat des LDAP-Servers aus, und klicken Sie dann auf **Zertifikat hinzufügen**.
5. Wiederholen Sie den vorherigen Schritt, um das Zertifikat der Stammzertifizierungsstelle und ggf. Zwischenzertifikate hinzuzufügen.
6. Überprüfen Sie, ob die hochgeladenen Zertifikate die richtigen sind, und klicken Sie auf **Apply Settings**.

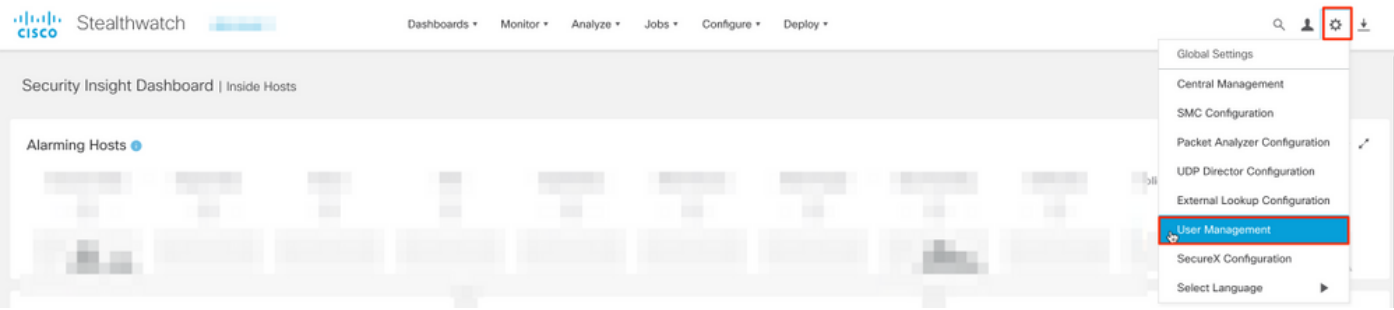


7. Warten Sie, bis die Änderungen übernommen wurden und der Manager-Status **aktiv** ist.

Schritt C: Hinzufügen der Konfiguration des externen LDAP-Diensts.

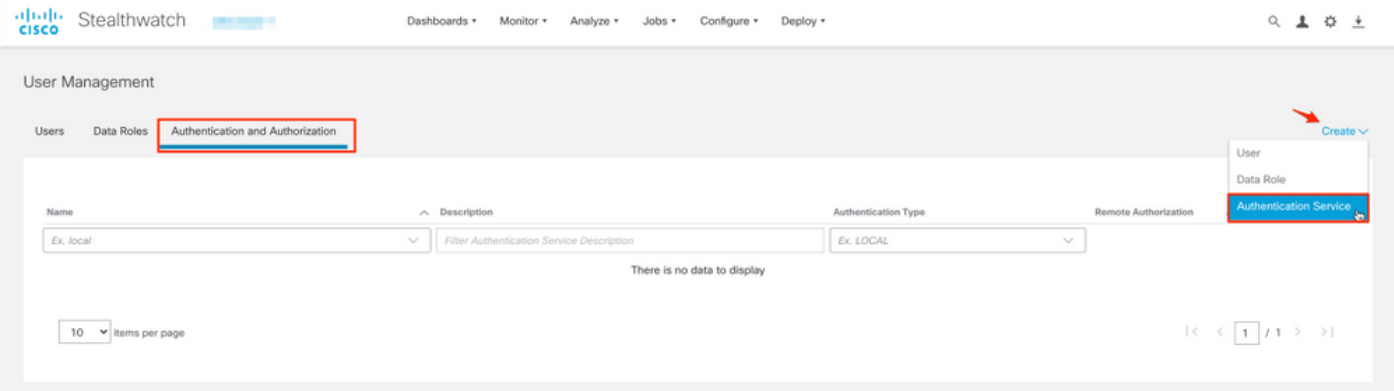
SNA Version 7.2 oder höher

1. Öffnen Sie das Haupt-Dashboard Manager, und navigieren Sie zu **Globale Einstellungen** > **Benutzerverwaltung**.



2. Wählen Sie im Fenster Benutzerverwaltung die Registerkarte **Authentifizierung und Autorisierung aus**.

3. Klicken Sie auf **Erstellen > Authentifizierungsdienst**.



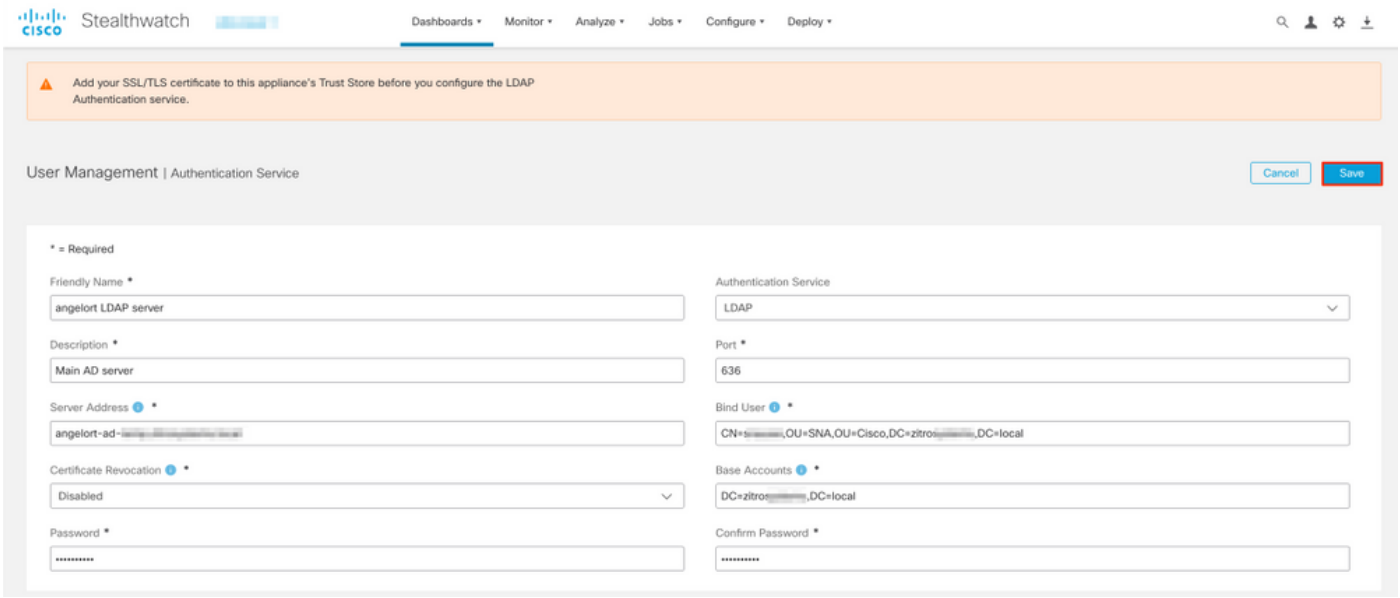
4. Wählen Sie im Dropdown-Menü **Authentication Service** die Option **LDAP aus**.

5. Füllen Sie die erforderlichen Felder aus.

Feld	Hinweise
Name des Freundes	Geben Sie einen Namen für den LDAP-Server ei
Beschreibung	Geben Sie eine Beschreibung für den LDAP-Serv ein.
Serveradresse	**Geben Sie den vollqualifizierten Domänennamen wie im Feld Subject Alternative Name (SAN) des LDAP-Serverzertifikats angegeben.** • Wenn das SAN-Feld nur die IPv4-Adresse er geben Sie die IPv4-Adresse im Feld Server Address (Serveradresse) ein. • Wenn das Feld SAN den DNS-Namen enthäl geben Sie den DNS-Namen in das Feld Serv Address (Serveradresse) ein. • Wenn das SAN-Feld sowohl DNS- als auch I Werte enthält, verwenden Sie den ersten aufgeführten Wert.
Anschluss	Geben Sie den Port ein, der für die sichere LDAP Kommunikation (LDAP über TLS) festgelegt wurd Der bekannte TCP-Port für LDAPS ist 636.
Bind-Benutzer	Geben Sie die Benutzer-ID ein, die für die Verbin zum LDAP-Server verwendet wird. Beispiele: CN=admin,OU=Unternehmensbenutzer,DC=exar DC=com **Anmerkung:** Wenn Sie Ihre Benutzer zu eine integrierten AD-Container hinzugefügt haben B. "Users"), muss der kanonische Name (CN die Bind-DN des Bind-Benutzers auf den integrierten Ordner (z. B. CN=username, CN=Users, DC=domain, DC=com) festgeleg sein. Wenn Sie Ihre Benutzer jedoch einem neuen Container hinzugefügt haben, muss d Organisationseinheit (OU) für die Bind-DN a den neuen Containernamen festgelegt sein (CN=username, OU=Corporate Users,

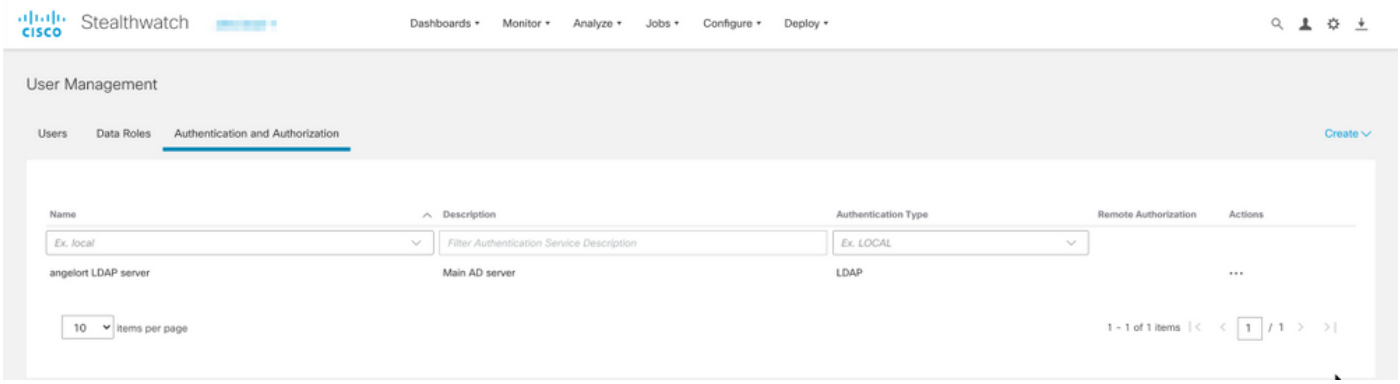
	DC=domain, DC=com). **Anmerkung:** Eine nützliche Möglichkeit, die E DN des Bind-Benutzers zu finden, besteht da das Active Directory auf einem Windows-Ser abzufragen, der über eine Verbindung zum Active Directory-Server verfügt. Um diese Informationen abzurufen, können Sie eine Windows-Eingabeaufforderung öffnen und d Befehl **dsquery user dc=<Distinguished>,dc=<name> -name <use** eingeben. Beispiel: **dsquery user dc=example,dc=com -name user1**. Das Erge sieht aus wie "CN=user1,OU=Corporate Users,DC=example,DC=com"
Kennwort	Geben Sie das Bind-Benutzerkennwort ein, das fü Verbindung zum LDAP-Server verwendet wird.
Basiskonten	Geben Sie den Distinguished Name (DN) ein. Die DN gilt für die Verzweigung des Verzeichniss dem die Suche nach Benutzern beginnen muss. G es der Anfang der Verzeichnisstruktur (Ihre Domä aber Sie können auch eine Unterstruktur innerhal Verzeichnisses angeben. Der Bind-Benutzer und zur Authentifizierung vorgesehenen Benutzer müs über Basiskonten erreichbar sein. Beispiele: DC=Beispiel, DC=com

6. Klicken Sie auf **Speichern**.



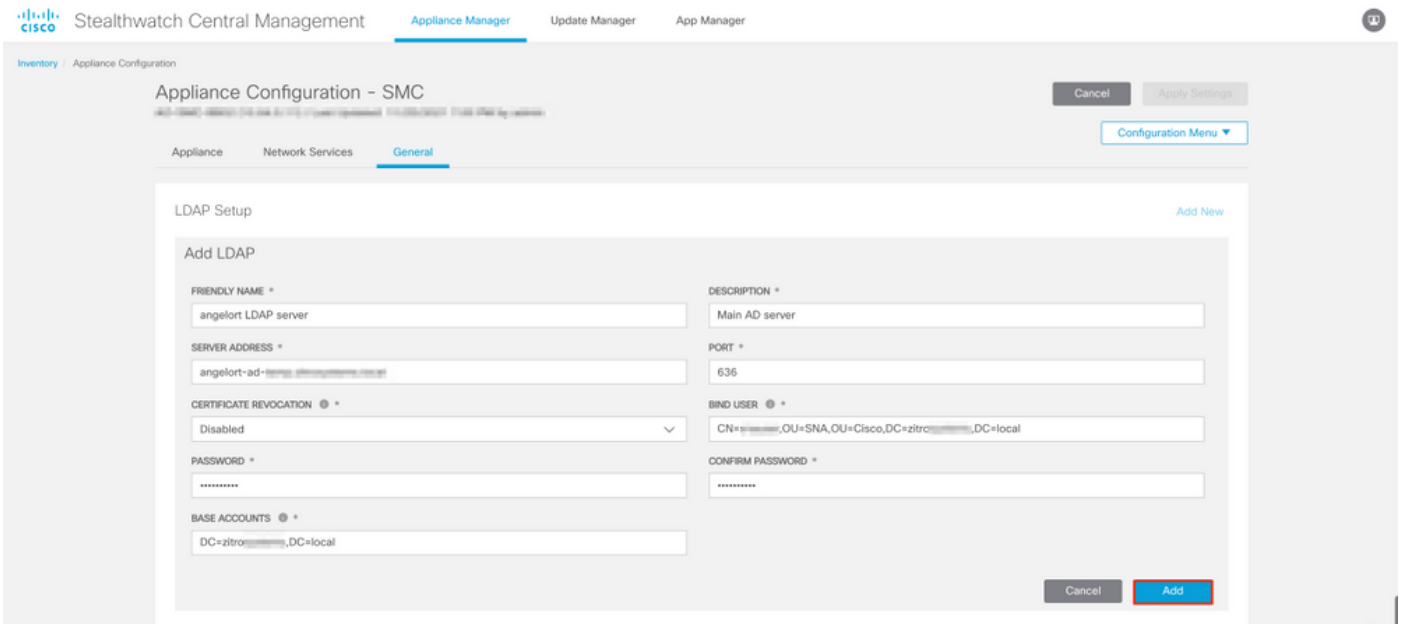
7. Wenn die eingegebenen Einstellungen und die Zertifikate, die dem Vertrauensspeicher hinzugefügt wurden, korrekt sind, müssen Sie das Banner "Sie haben Ihre Änderungen erfolgreich gespeichert" öffnen.

8. Der konfigurierte Server muss unter **User Management > Authentication and Authorization** (Benutzerverwaltung > **Authentifizierung und Autorisierung)** angezeigt werden.



SNA Version 7.1

1. Navigieren Sie zu **Zentrale Verwaltung** > Bestand.
2. Suchen Sie die SMC-Appliance, und klicken Sie auf **Aktionen** > **Appliance Configuration (Einheitenkonfiguration bearbeiten)**.
3. Navigieren Sie im Fenster "Appliance Configuration" zu **Configuration Menu** > **LDAP Setup** > **Add New**.
4. Füllen Sie die erforderlichen Felder wie in **SNA Version 7.2 oder höher** Schritt 5 beschrieben aus.



5. Klicken Sie auf **Hinzufügen**.

6. Klicken Sie auf **Einstellungen übernehmen**.

7. Wenn die eingegebenen Einstellungen und die Zertifikate, die dem Vertrauensspeicher hinzugefügt wurden, korrekt sind, werden die Änderungen am Manager angewendet, und der Anwendungszustand muss **aktiv** sein.

Schritt D. Konfigurieren der Autorisierungseinstellungen

SNA unterstützt die lokale und Remote-Autorisierung über LDAP. Bei dieser Konfiguration werden die LDAP-Gruppen des AD-Servers integrierten oder benutzerdefinierten SNA-Rollen zugeordnet.

Folgende Authentifizierungs- und Autorisierungsmethoden werden für SNA über LDAP unterstützt:

- Remote-Authentifizierung und lokale Autorisierung
- Remote-Authentifizierung und Remote-Autorisierung (wird nur für SNA Version 7.2.1 oder höher unterstützt)

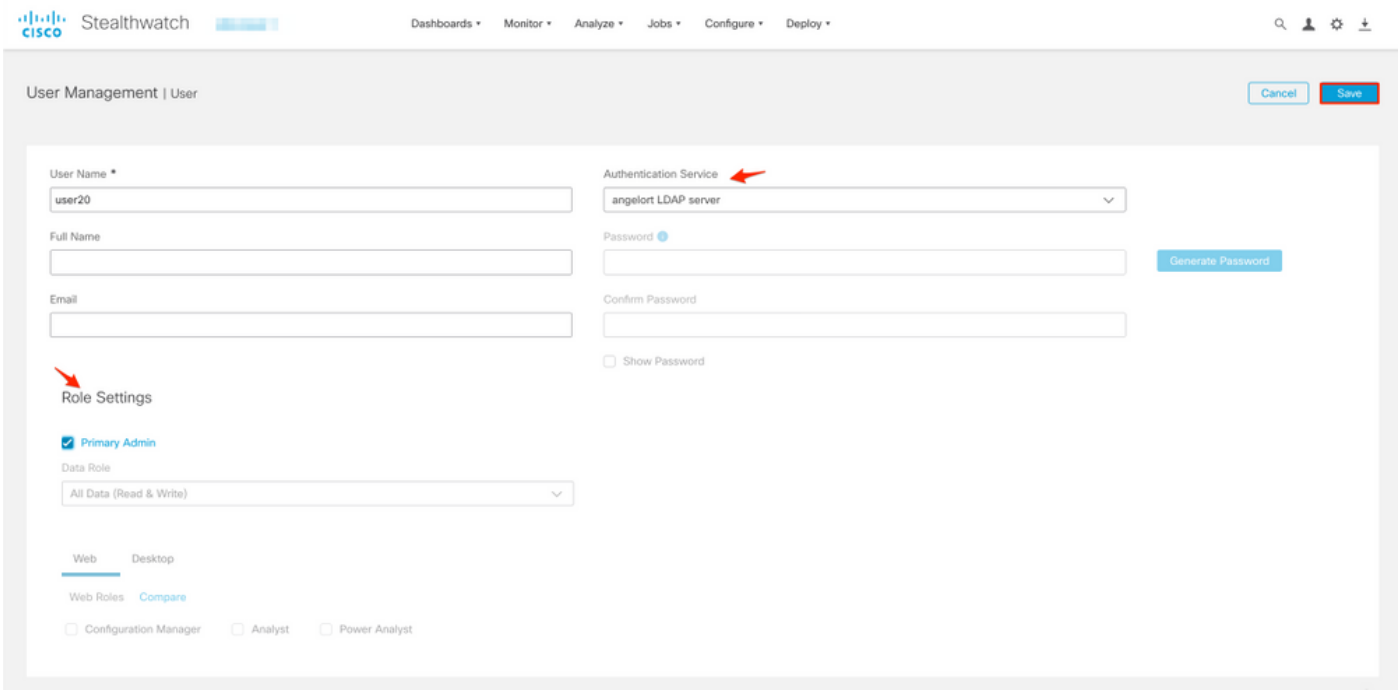
Lokale Autorisierung

In diesem Fall müssen die Benutzer und ihre Rollen lokal definiert werden. Gehen Sie wie folgt vor, um dies zu erreichen.

1. Navigieren Sie erneut zur **Benutzerverwaltung**, und klicken Sie auf die Registerkarte **Benutzer > Erstellen > Benutzer**.

2. Legen Sie den Benutzernamen für die Authentifizierung mit dem LDAP-Server fest, und wählen Sie den konfigurierten Server aus dem Dropdown-Menü **Authentifizierungsdienst aus**.

3. Legen Sie fest, welche Berechtigungen der Benutzer über den Manager verfügen muss, nachdem er vom LDAP-Server authentifiziert wurde, und klicken Sie auf **Speichern**.



Remote-Autorisierung über LDAP

Die Remote-Authentifizierung und -Autorisierung über LDAP wurde erstmals von Secure Network Analytics Version 7.2.1 unterstützt.

> **Anmerkung:** Remote Authorization mit LDAP wird in Version 7.1 nicht unterstützt.

Wenn ein Benutzer lokal (im Manager) definiert und aktiviert ist, muss erwähnt werden, dass der Benutzer remote authentifiziert, aber lokal autorisiert wird. Die Benutzerauswahl wird wie folgt durchgeführt:

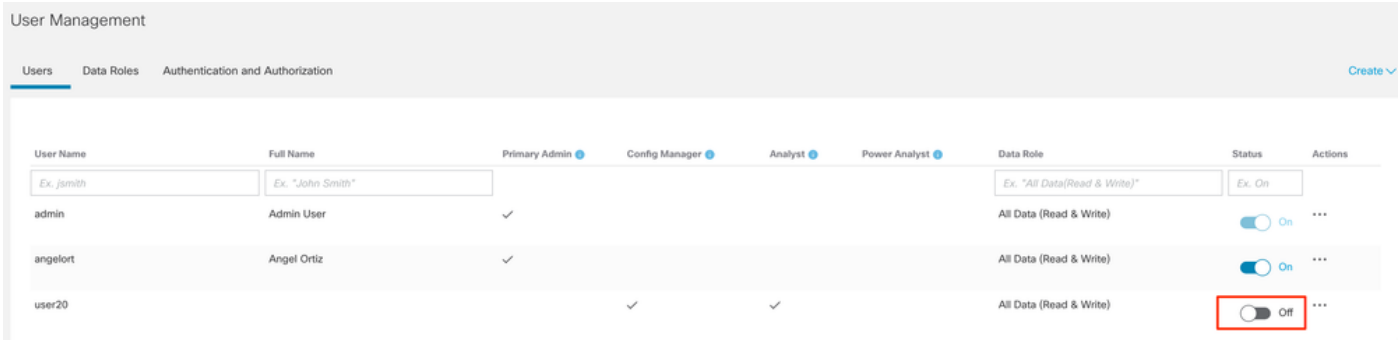
1. Sobald die Anmeldeinformationen auf der Begrüßungsseite des Managers eingegeben wurden, sucht der Manager nach einem lokalen Benutzer mit dem angegebenen Namen.

2. Wenn ein lokaler Benutzer gefunden wird und aktiviert ist, wird er remote authentifiziert (wenn die Remote-Authentifizierung über LDAP mit lokaler Autorisierung zuvor konfiguriert wurde), aber mit den lokalen Einstellungen autorisiert.
3. Wenn die Remote-Autorisierung konfiguriert und aktiviert ist und der Benutzer nicht lokal (nicht konfiguriert oder deaktiviert) gefunden wird, werden Authentifizierung und Autorisierung per Remote-Zugriff durchgeführt.

Aus diesem Grund sind die Schritte zur erfolgreichen Konfiguration der Remote-Authentifizierung nicht.

Schritt D-1: Deaktivieren oder löschen Sie die Benutzer, die Remote-Autorisierung verwenden sollen, aber lokal definiert sind.

1. Öffnen Sie das Haupt-Dashboard des Managers, und navigieren Sie zu Global Settings > User Management (Globale Einstellungen > Benutzerverwaltung).
2. Deaktivieren oder löschen Sie die Benutzer (sofern vorhanden), die Remote-Authentifizierung und -Autorisierung über LDAP verwenden möchten, aber lokal konfiguriert werden.



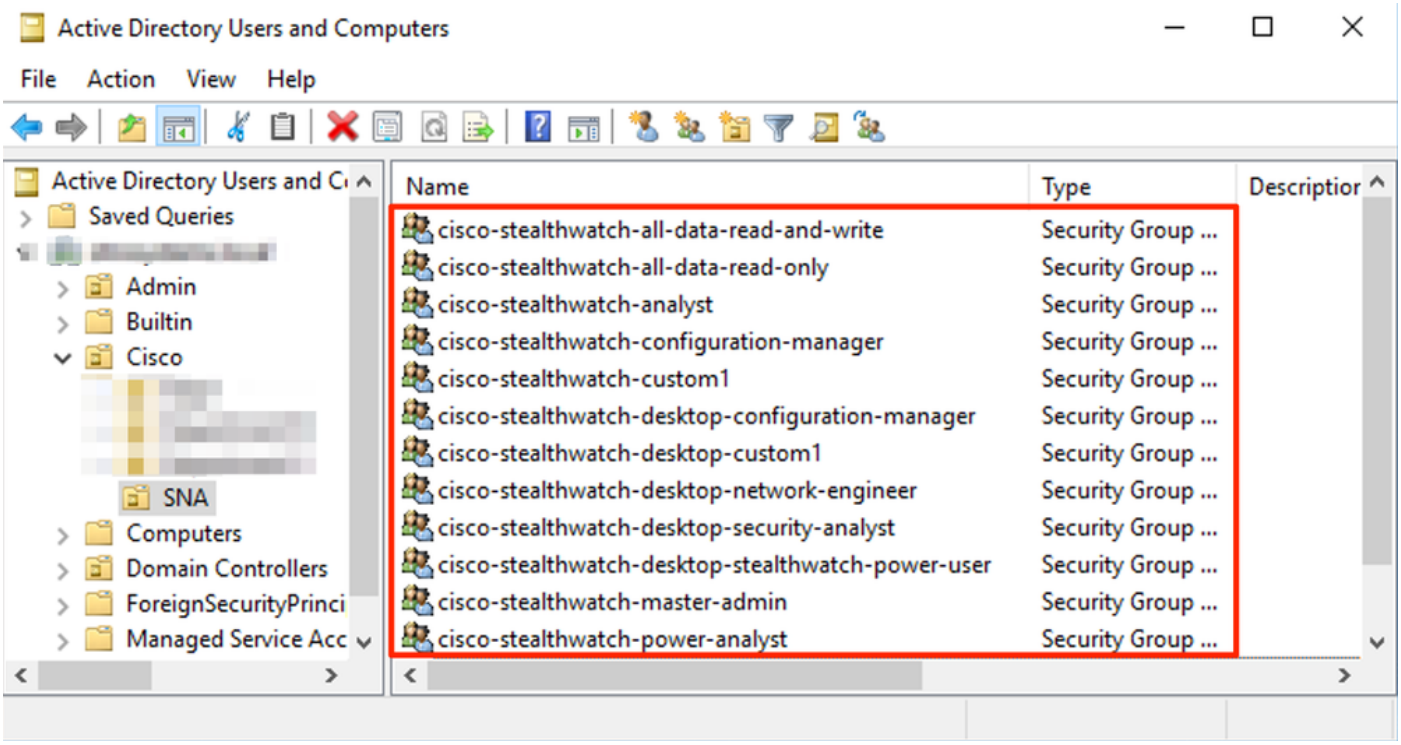
Schritt D-2: Definieren Sie cisco-stealthWatch-Gruppen im Microsoft AD-Server.

Für die externe Authentifizierung und Autorisierung über LDAP-Benutzer werden Kennwörter und *cisco-stealthwatch*-Gruppen in Microsoft Active Directory remote definiert. Die im AD-Server definierten *Cisco Stealthwatch*-Gruppen beziehen sich auf die verschiedenen Rollen, die die SNA innehat. Sie müssen wie folgt definiert werden.

SNA-Rolle	Gruppe(n) Name
Hauptadministrator	• cisco-stealthwatch-master-admin • cisco-stealthWatch-all-Lese- und Schreibzug • cisco-stealthwatch-all-data-read-only • cisco-stealthwatch-<custom> (optional)
Datenrolle	**Anmerkung:** Stellen Sie sicher, dass benutzerdefinierte Data-Rollengruppen mit "cisco-stealthwatch-" beginnen.
Webfunktionale Rolle	• cisco-stealthWatch-configuration-manager • cisco-stealthwatch-power-analyst • cisco-stealthwatch-analyst
Desktop-Funktionsrolle	• cisco-stealthwatch-desktop-stealthwatch-pow user • cisco-stealthwatch-desktop-configuration-ma • cisco-stealthwatch-desktop-network-enginee

- cisco-stealthwatch-desktop-security-analyst
- cisco-stealthwatch-desktop-<custom> (optior

Anmerkung: Stellen Sie sicher, dass benutzerdefinierte Desktop-Funktionsgruppe "cisco-stealthwatch-desktop-" beginnen.

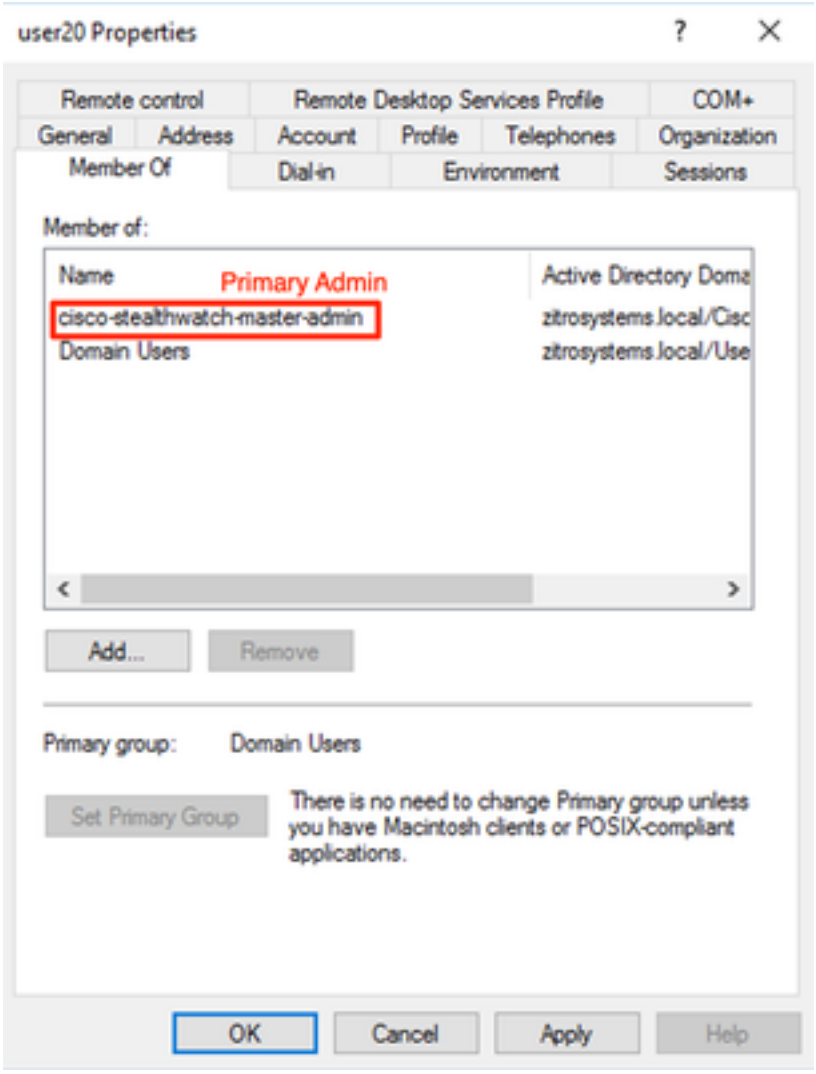


Anmerkung: Wie bereits beschrieben, werden benutzerdefinierte Gruppen für "Datenrolle" und "Desktop-Funktionsrolle" unterstützt, solange dem Gruppennamen die entsprechende Zeichenfolge vorangestellt wird. Diese benutzerdefinierten Rollen und Gruppen müssen sowohl im SNA Manager als auch im Active Directory-Server definiert werden. Wenn Sie z. B. im SNA Manager eine benutzerdefinierte Rolle "custom1" für eine Desktop-Client-Rolle definieren, muss sie cisco-stealthwatch-desktop-custom1 in Active Directory zugeordnet werden.

Schritt D-3: Definieren Sie LDAP-Autorisierungsgruppenzuordnungen für die Benutzer.

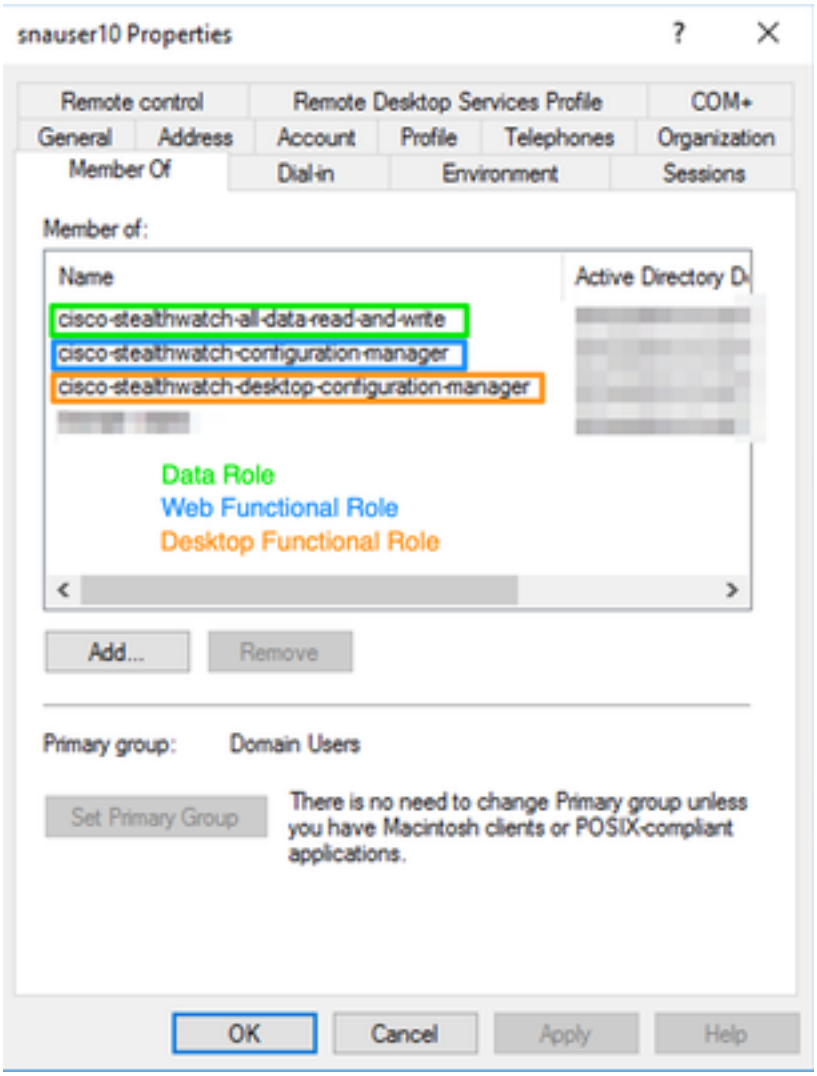
Nachdem die *cisco-stealthwatch*-Gruppen im AD-Server definiert wurden, können wir die Benutzer, die Zugriff auf den SNA Manager haben sollen, den erforderlichen Gruppen zuordnen. Dies muss wie folgt geschehen.

- Ein **primärer Admin-**Benutzer **muss** der *Cisco-stealthwatch-master-admin*-Gruppe zugewiesen und **darf keiner anderen** *cisco-stealthwatch*-Gruppe **angehören**.



- Jeder Benutzer, der keine primären Admin-Benutzer ist, muss einer Gruppe jeder Rolle mit den folgenden Bedingungen zugewiesen werden.

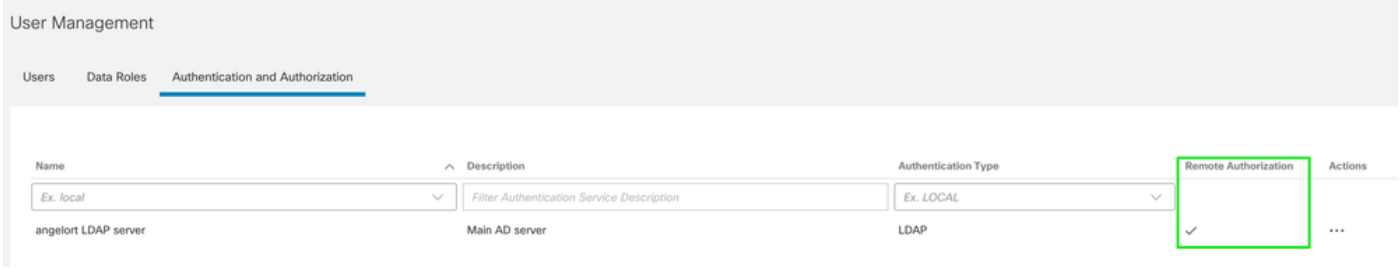
1. **Datenrolle**: Der Benutzer muss **nur einer Gruppe** zugewiesen sein.
2. **Webfunktionale Rolle**: Der Benutzer muss **mindestens einer Gruppe** zugewiesen sein.
3. **Funktion des Desktops**: Der Benutzer muss **mindestens einer Gruppe** zugewiesen sein.



Schritt D-4: Aktivieren Sie die Remote-Autorisierung über LDAP im SNA Manager.

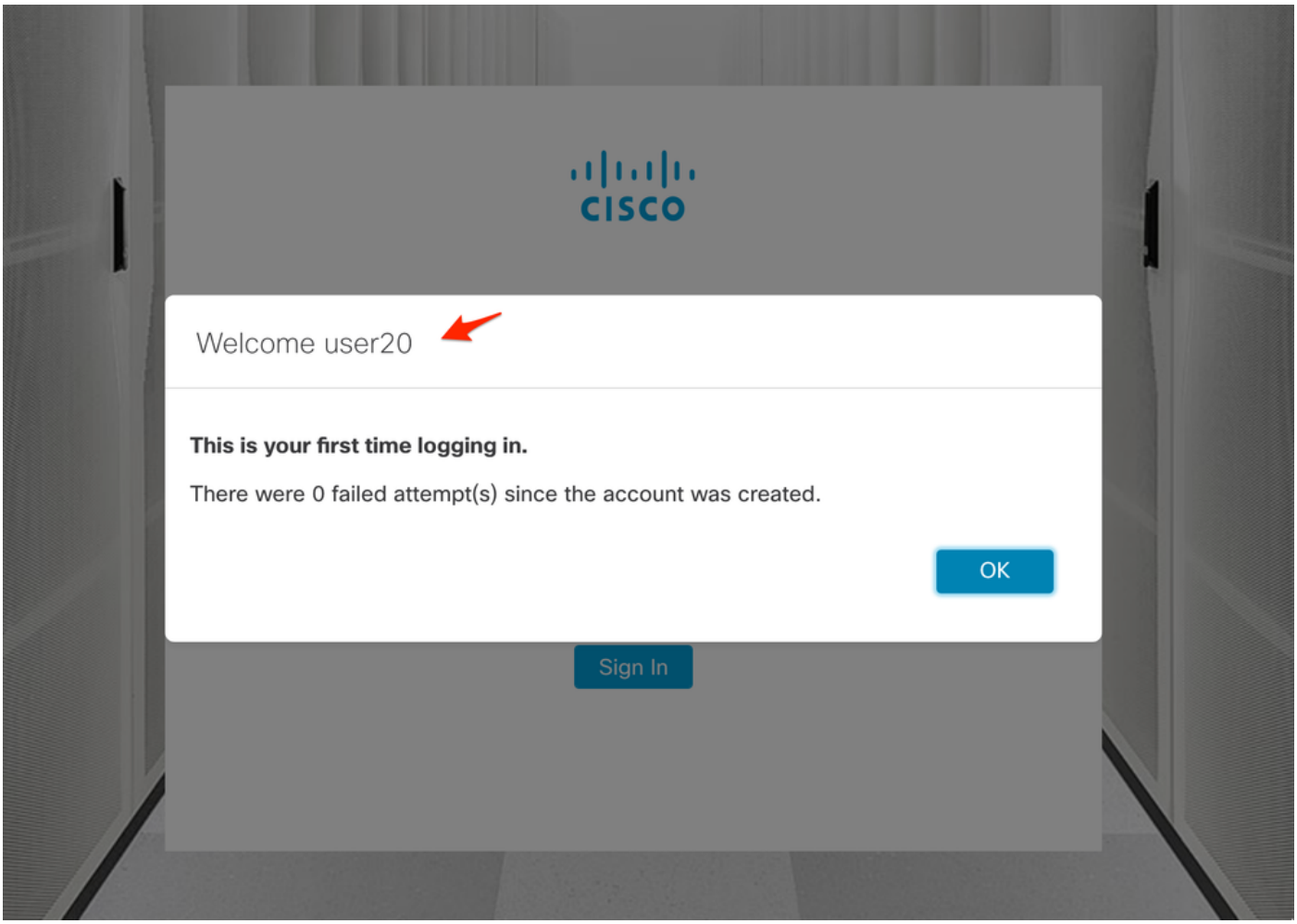
1. Öffnen Sie das Haupt-Dashboard Manager, und navigieren Sie zu **Globale Einstellungen > Benutzerverwaltung**.
2. Wählen Sie im Fenster **Benutzerverwaltung** die Registerkarte **Authentifizierung und Autorisierung aus**.
3. Suchen Sie den LDAP-Authentifizierungsdienst, der in **Schritt C** konfiguriert wurde.
4. Klicken Sie auf **Aktionen > Remote Authorization aktivieren**.

Anmerkung: Es kann jeweils nur ein externer Autorisierungsdienst verwendet werden. Wenn bereits ein anderer Autorisierungsdienst verwendet wird, wird dieser automatisch deaktiviert und der neue Dienst aktiviert. Alle Benutzer, die mit dem vorherigen externen Dienst autorisiert wurden, werden jedoch abgemeldet. Eine Bestätigungsmeldung wird angezeigt, bevor eine Aktion ausgeführt wird.

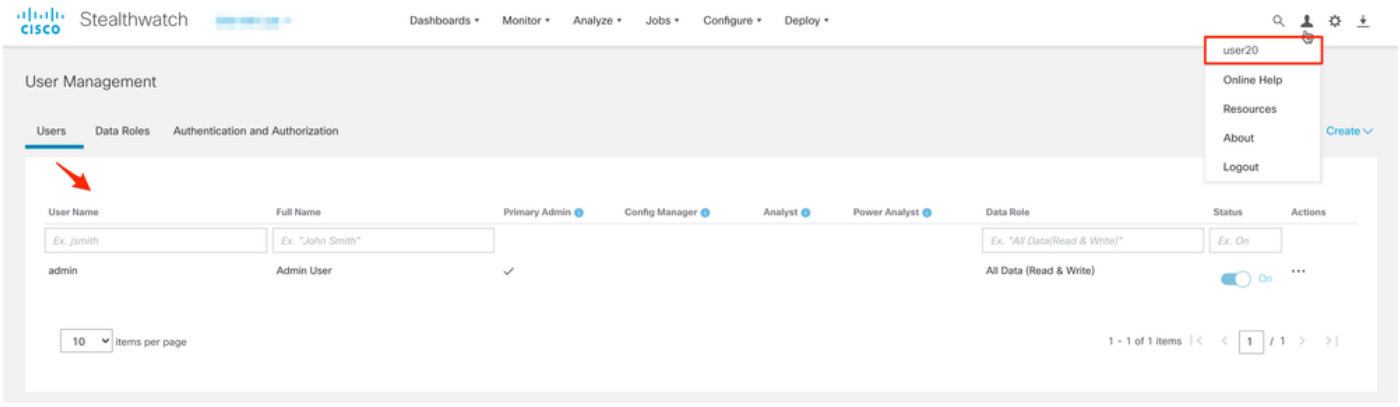


Überprüfung

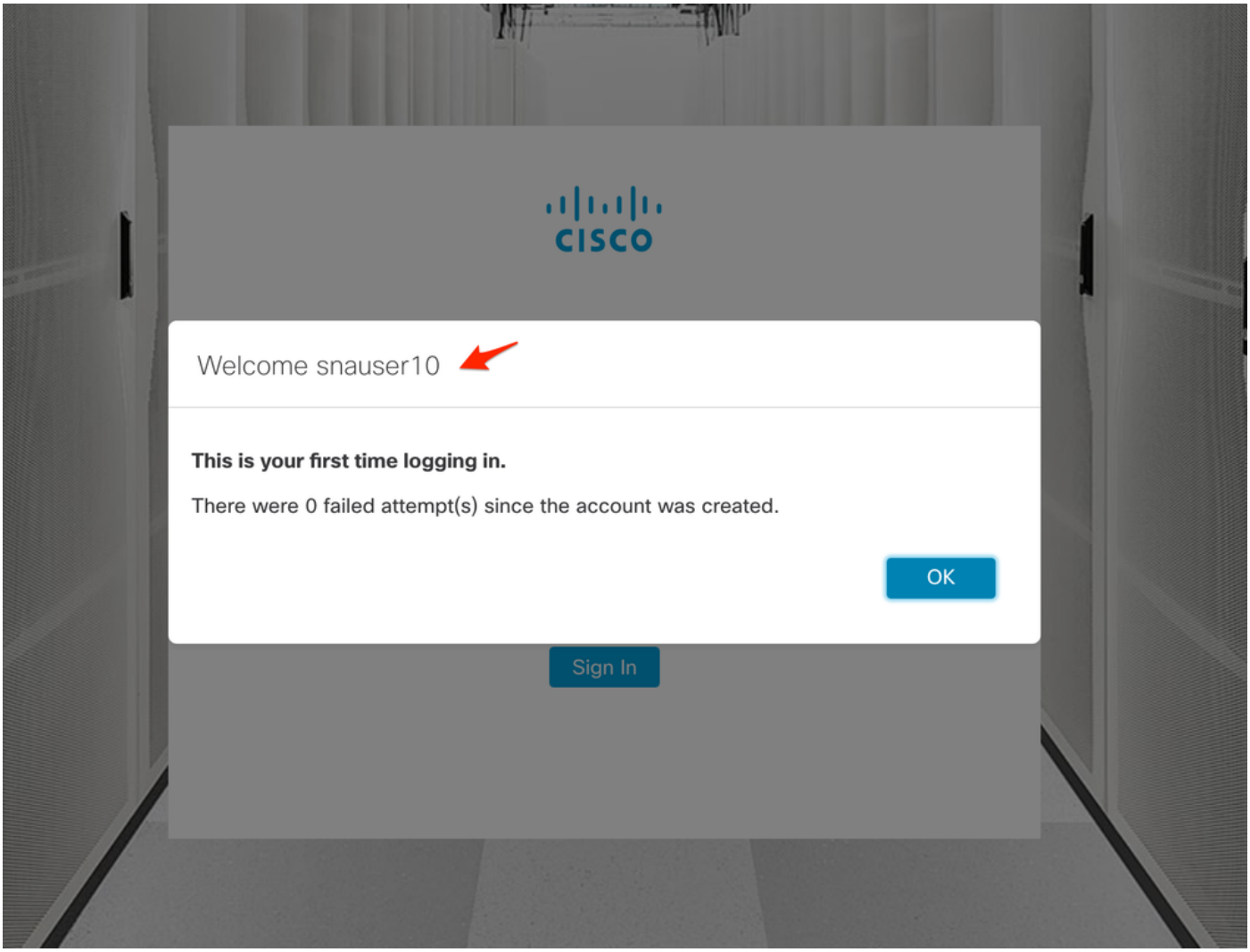
Die Benutzer können sich mit den auf dem AD-Server definierten Anmeldeinformationen anmelden.



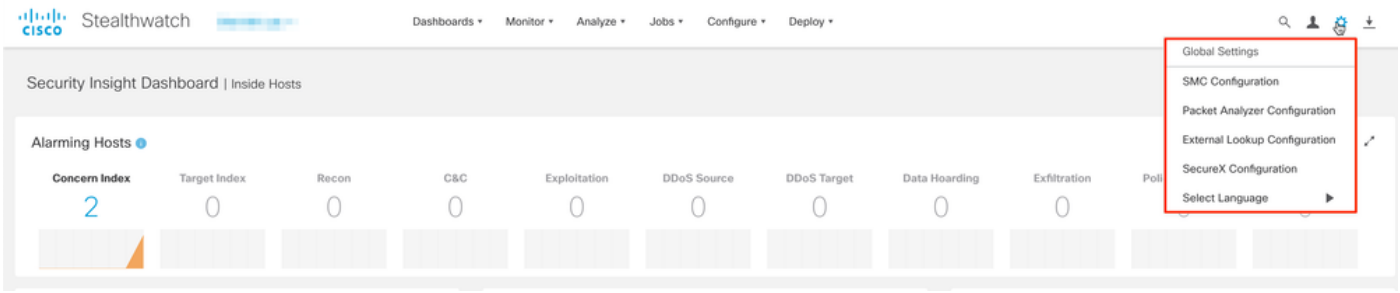
Der zweite Überprüfungsschritt betrifft die Autorisierung. In diesem Beispiel wurde der Benutzer "user20" zum Mitglied der Gruppe *cisco-stealthwatch-master-admin* im AD-Server gemacht, und wir können bestätigen, dass der Benutzer über primäre Administratorberechtigungen verfügt. Der Benutzer ist in den lokalen Benutzern nicht definiert, daher können wir bestätigen, dass die Autorisierungsattribute vom AD-Server gesendet wurden.



Dieselbe Überprüfung wird für den anderen Benutzer in diesem Beispiel "snauser10" durchgeführt. Die erfolgreiche Authentifizierung kann mit den Anmeldeinformationen bestätigt werden, die auf dem AD-Server konfiguriert wurden.



Da dieser Benutzer nicht zur primären Administratorgruppe gehört, sind zur Autorisierungsüberprüfung einige Funktionen nicht verfügbar.



Fehlerbehebung

Wenn die Konfiguration des Authentifizierungsdienstes nicht erfolgreich gespeichert werden kann, überprüfen Sie Folgendes:

1. Sie haben dem Vertrauensspeicher des Managers die entsprechenden Zertifikate des LDAP-Servers hinzugefügt.
2. Die konfigurierte **Serveradresse** entspricht den Angaben im Feld Subject Alternative Name (SAN) des LDAP-Serverzertifikats. Wenn das SAN-Feld nur die IPv4-Adresse enthält, geben Sie die IPv4-Adresse im Feld Server Address (Serveradresse) ein.Wenn das Feld SAN den DNS-Namen enthält, geben Sie den DNS-Namen in das Feld Server Address

(Serveradresse) ein.Wenn das SAN-Feld sowohl DNS- als auch IPv4-Werte enthält, verwenden Sie den ersten aufgeführten Wert.

3. Die konfigurierten Felder **Bind User** und **Base Account** sind korrekt, wie vom AD Domain Controller angegeben.

Zugehörige Informationen

Weitere Unterstützung erhalten Sie vom Cisco Technical Assistance Center (TAC). Ein gültiger Support-Vertrag ist erforderlich: Weltweiter Kontakt zum Cisco Support.