

# Configurazione dell'autenticazione e dell'autorizzazione esterne tramite LDAPS per l'accesso sicuro a Network Analytics Manager

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Passaggio A. Accedere al controller di dominio Active Directory ed esportare il certificato SSL utilizzato per LDAP.](#)

[Passaggio B. Accedere a SNA Manager per aggiungere il certificato del server LDAP e la catena principale.](#)

[Passaggio C. Aggiungere la configurazione del servizio esterno LDAP.](#)

[SNA versione 7.2 o successive](#)

[SNA versione 7.1](#)

[Passaggio D. Configurare le impostazioni di autorizzazione.](#)

[Autorizzazione locale](#)

[Autorizzazione remota tramite LDAP](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

## Introduzione

Questo documento descrive la configurazione di base di Secure Network Analytics Manager (in precedenza Stealthwatch Management Center) versione 7.1 o successive per utilizzare l'autenticazione esterna e, con la versione 7.2.1 o successive, per utilizzare l'autorizzazione esterna con LDAPS.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Secure Network Analytics (in precedenza Stealthwatch)
- Operazione generale LDAP e SSL
- Gestione generale di Microsoft Active Directory

### Componenti usati

Le informazioni di questo documento si basano sui seguenti componenti:

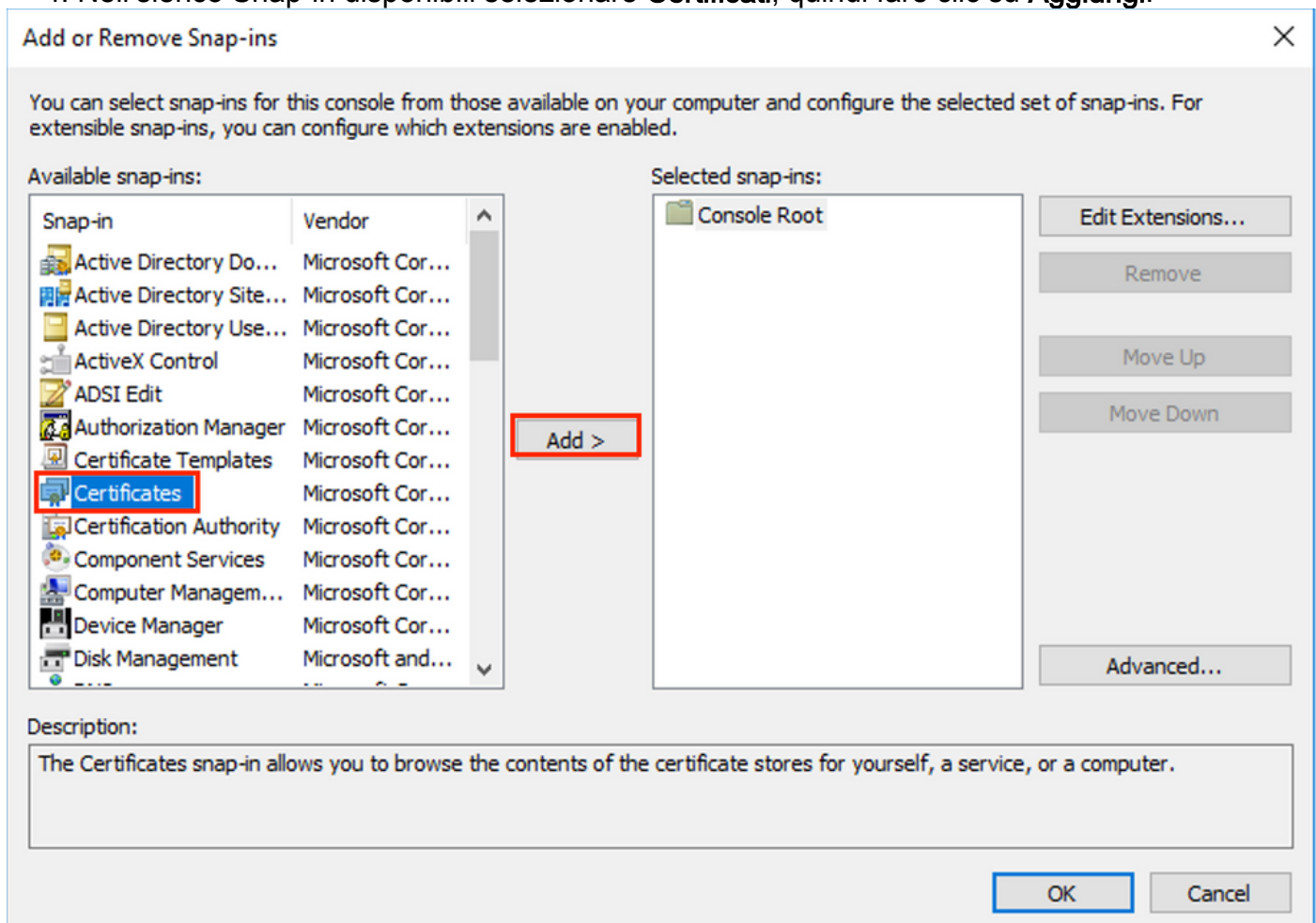
- Cisco Secure Network Analytics Manager (in precedenza SMC) versione 7.3.2
- Windows Server 2016 configurato come controller di dominio Active Directory

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Configurazione

### Passaggio A. Accedere al controller di dominio Active Directory ed esportare il certificato SSL utilizzato per LDAP.

1. Per Windows Server 2012 o versioni successive selezionare **Esegui** dal menu Start, quindi immettere **certlm.msc** e continuare con il passaggio 8.
2. Per le versioni precedenti di Windows Server, selezionare **Esegui** dal menu Start, quindi immettere **mmc**.
3. Dal menu File, selezionare **Aggiungi/Rimuovi snap-in**.
4. Nell'elenco Snap-in disponibili selezionare **Certificati**, quindi fare clic su **Aggiungi**.

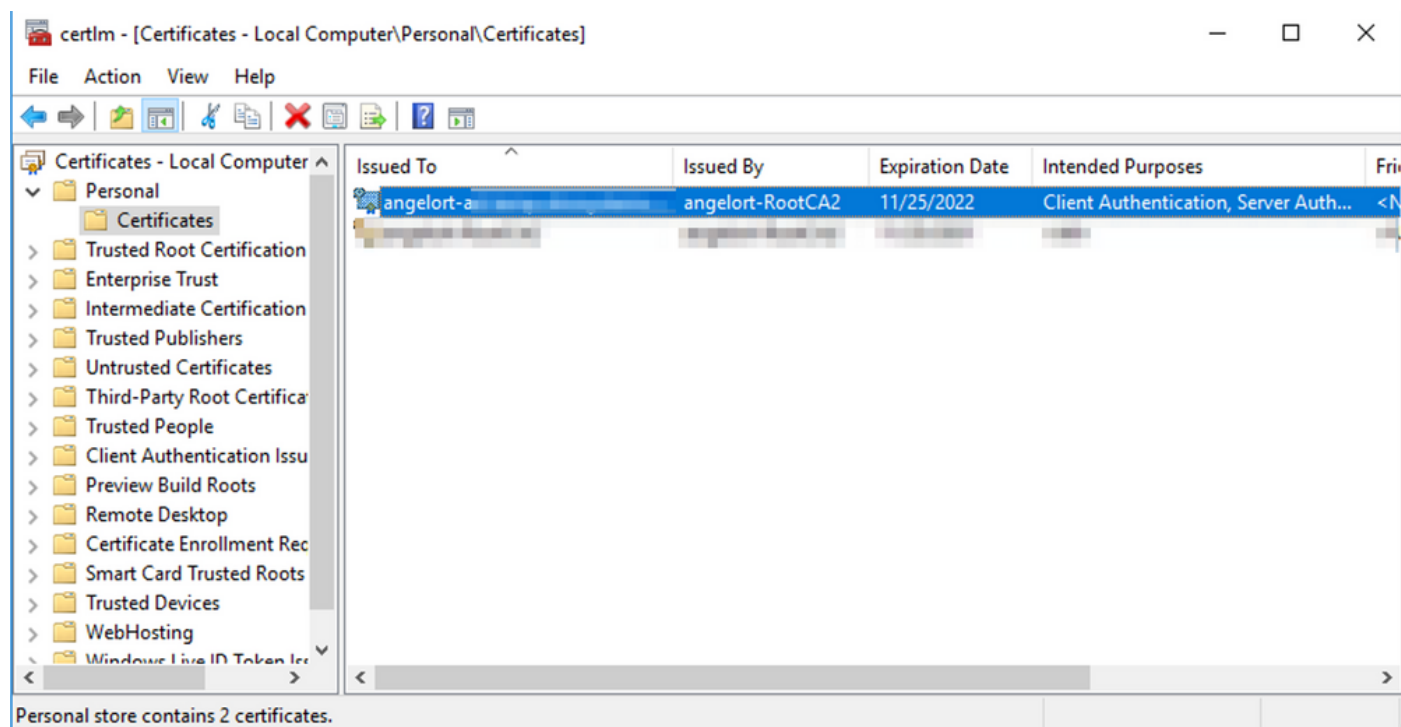


5. Nella finestra **snap-in Certificati**, selezionare **Account computer**, quindi selezionare **Avanti**.

6. Lasciare selezionato **Computer locale**, quindi selezionare **Fine**.

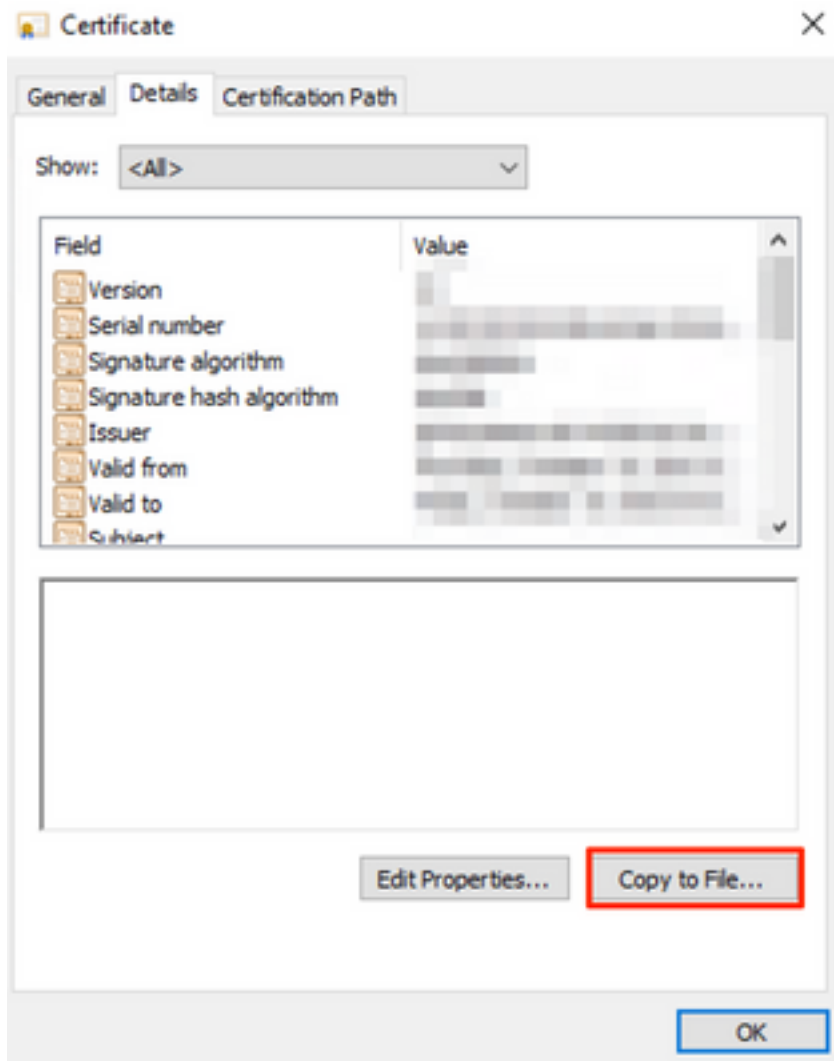
7. Nella finestra **Aggiungi o rimuovi snap-in**, selezionare **OK**.

8. Passare a **Certificati (computer locale) > Personale > Certificati**



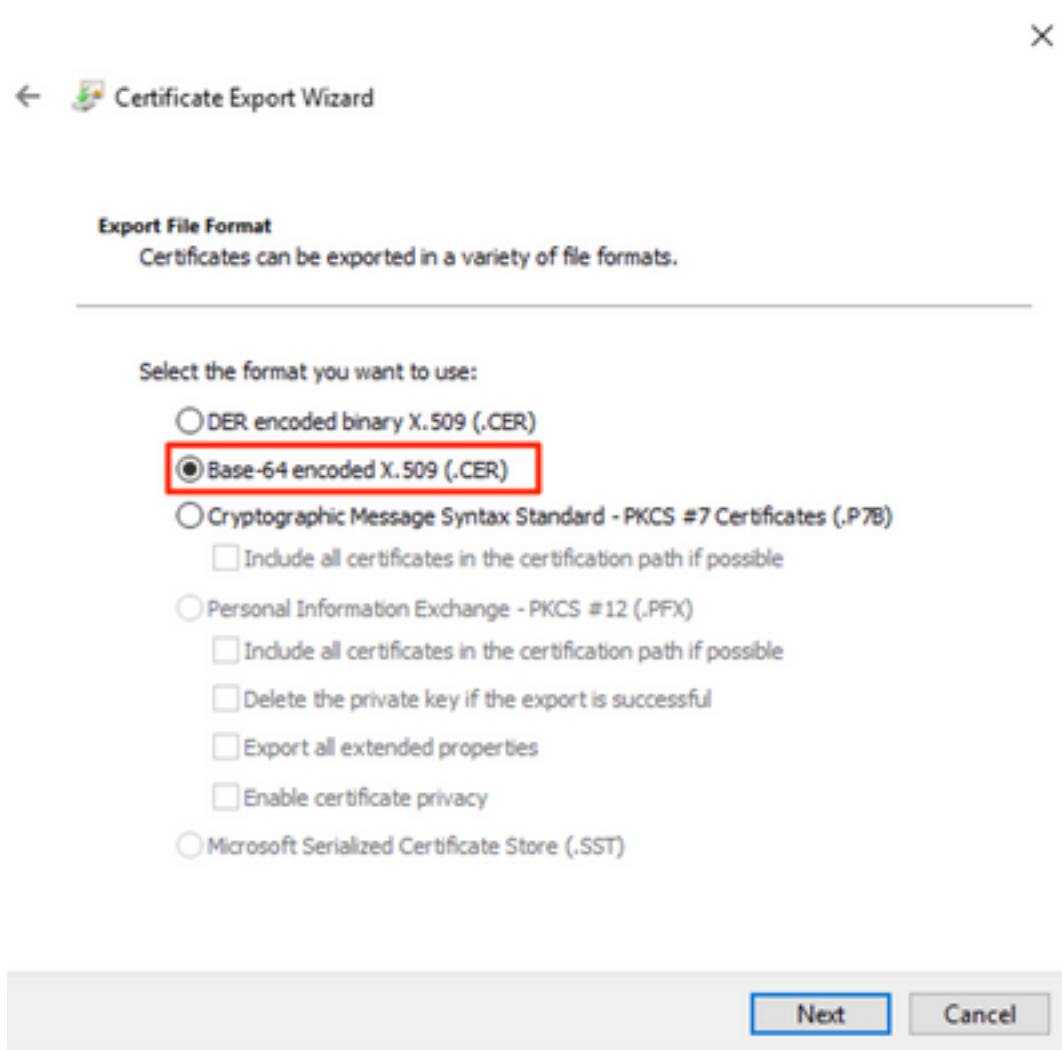
9. Selezionare e fare clic con il pulsante destro del mouse sul certificato SSL utilizzato per l'autenticazione LDAPS sul controller di dominio e fare clic su **Apri**.

10. Passare alla scheda **Dettagli** > fare clic su **Copia su file** > **Avanti**

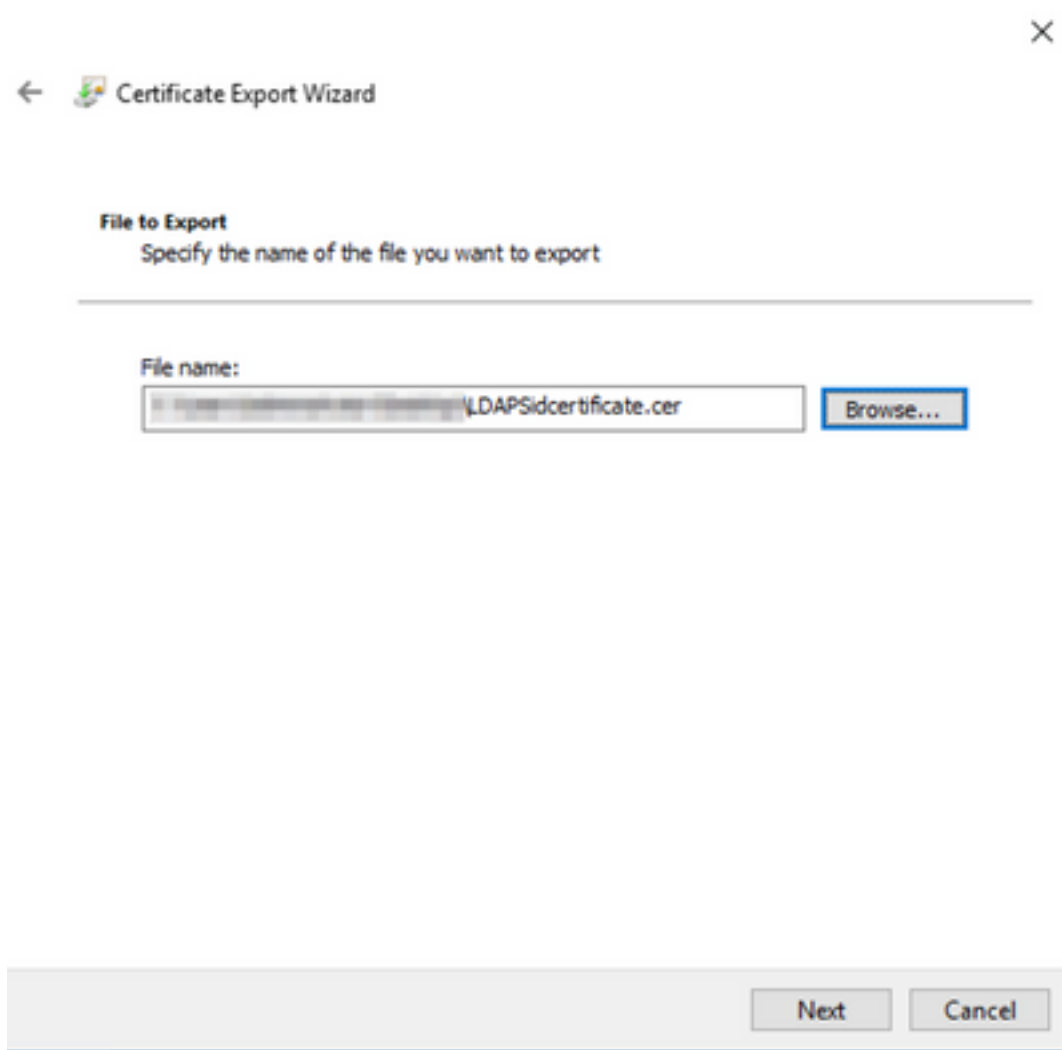


11. Verificare che l'opzione **No, non esportare la chiave privata** sia selezionata e fare clic su **Avanti**

12. Selezionare il formato **X.509 con codifica Base 64** e fare clic su **Avanti**.



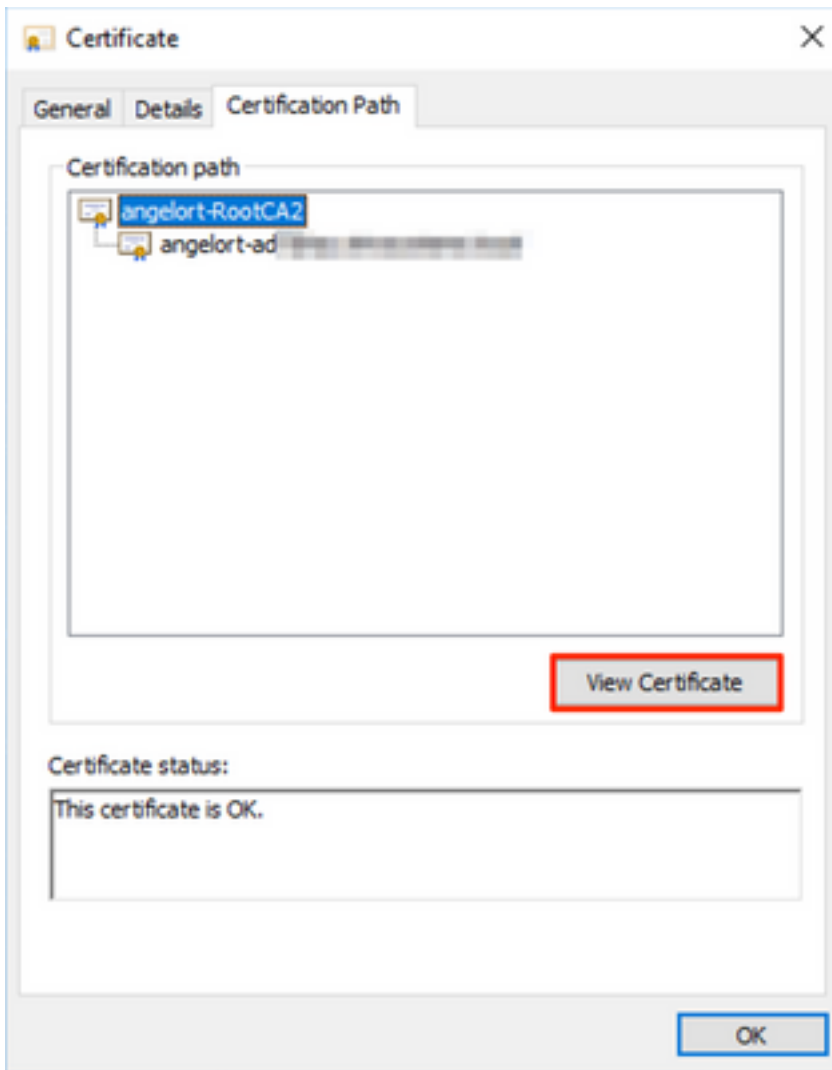
13. Selezionare il percorso in cui memorizzare il certificato, assegnare un nome al file e fare clic su **Avanti**.



14. Fare clic su **Finish** (Fine) per visualizzare il messaggio "Esportazione completata". messaggio.

15. Tornare al certificato utilizzato per LDAPS, quindi selezionare la scheda **Percorso certificazione**.

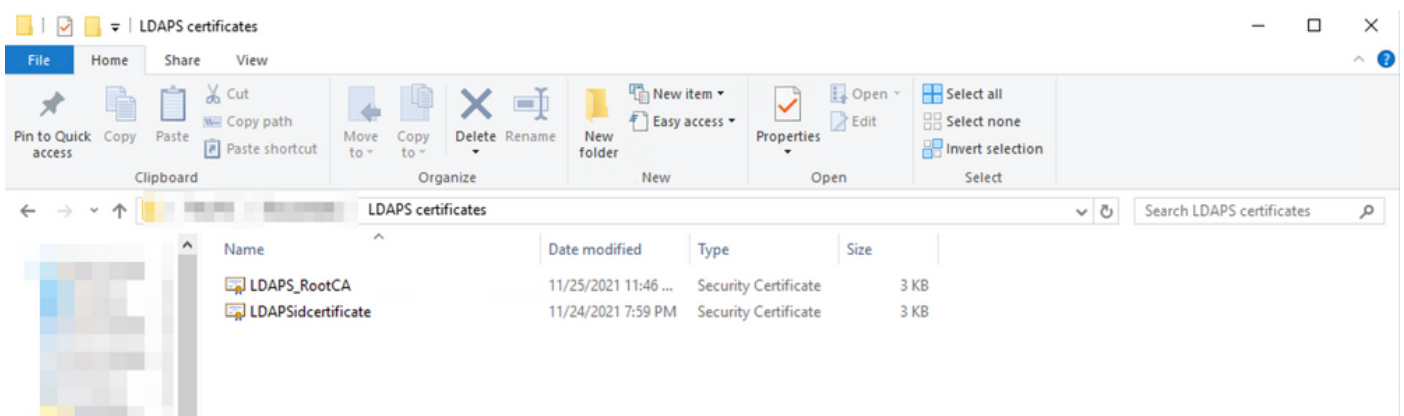
16. Selezionare l'autorità di certificazione radice sul percorso della certificazione e fare clic su **Visualizza certificato**.



17. Ripetere i passaggi da 10 a 14 per esportare il certificato della CA radice che ha firmato il certificato utilizzato per l'autenticazione LDAPS.

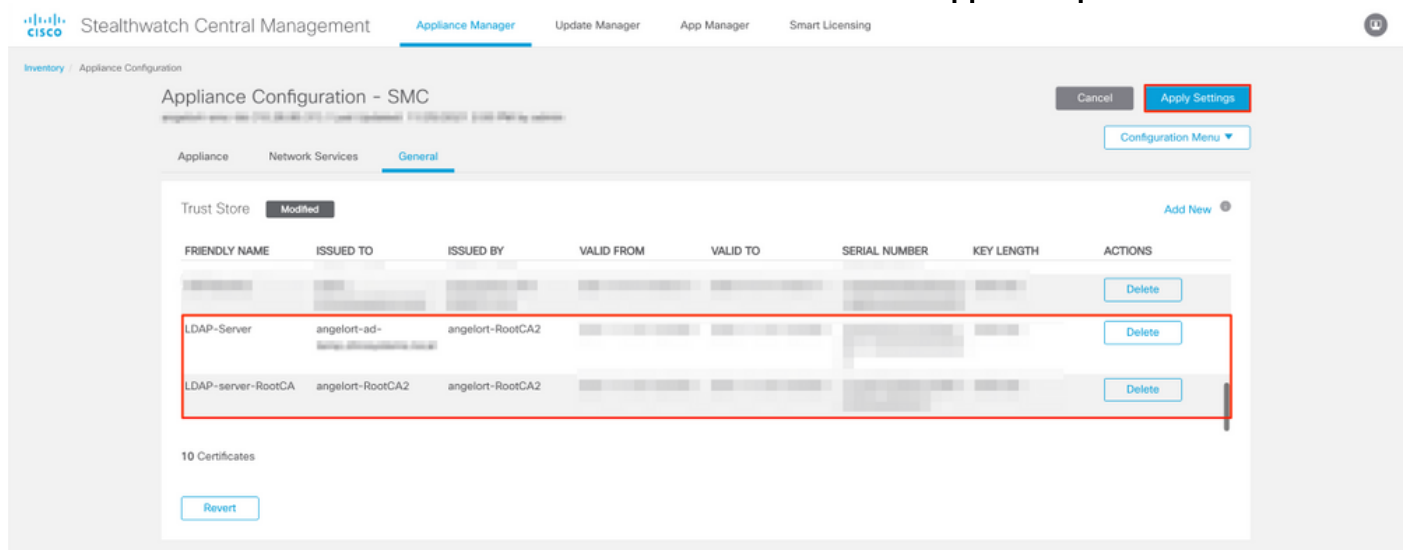
**Nota:** La distribuzione può avere una gerarchia di CA a più livelli. In questo caso, è necessario seguire la stessa procedura per esportare tutti i certificati intermedi nella catena di attendibilità.

18. Prima di continuare, assicurarsi di disporre di un file di certificato per il server LDAPS e per ogni autorità emittente nel percorso di certificazione: Certificato radice e certificati intermedi (se applicabile).



## Passaggio B. Accedere a SNA Manager per aggiungere il certificato del server LDAP e la catena principale.

1. Passare a **Gestione centrale** > Magazzino.
2. Individuare l'accessorio SNA Manager e fare clic su **Azioni** > **Modifica configurazione accessorio**.
3. Nella finestra Configurazione accessorio passare a **Menu Configurazione** > **Archivio protezione** > **Aggiungi nuovo**.
4. Digitare il Nome descrittivo, fare clic su **Scegli file** e selezionare il certificato del server LDAP, quindi fare clic su **Aggiungi certificato**.
5. Ripetere il passaggio precedente per aggiungere il certificato CA radice e i certificati intermedi (se applicabile).
6. Verificare che i certificati caricati siano corretti e fare clic su **Applica impostazioni**.

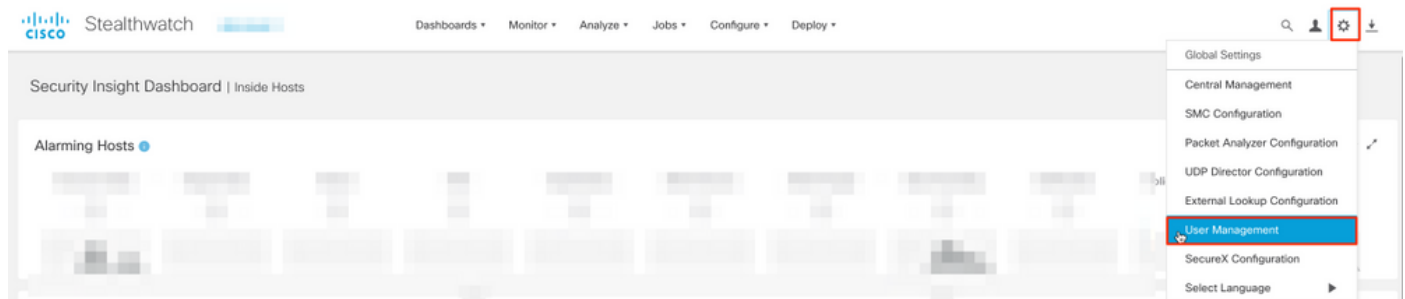


7. Attendere che le modifiche vengano applicate e che lo stato del responsabile sia **Attivo**.

## Passaggio C. Aggiungere la configurazione del servizio esterno LDAP.

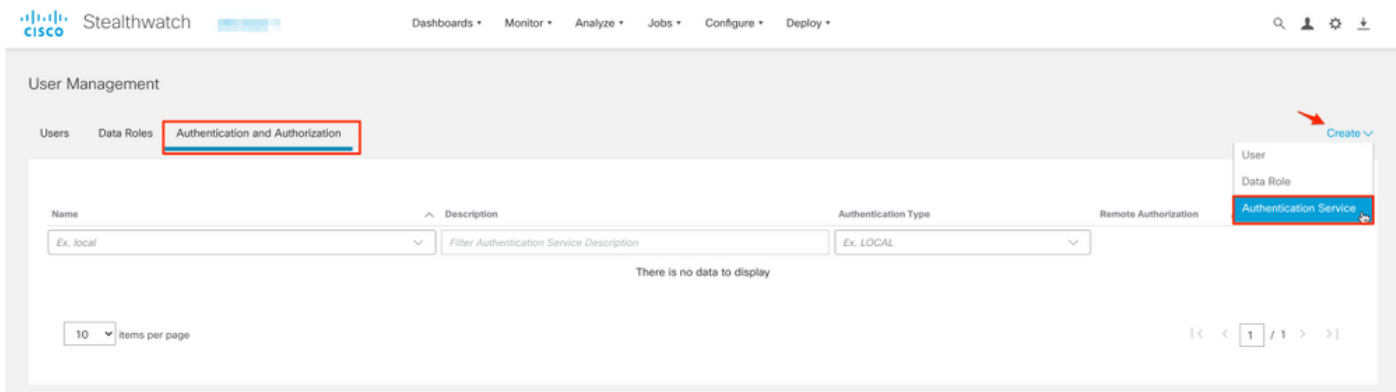
### SNA versione 7.2 o successive

1. Aprire il pannello di controllo principale Responsabile e passare a **Impostazioni globali** > **Gestione utente**.



2. Nella finestra Gestione utenti, selezionare la scheda **Autenticazione e autorizzazione**.
3. Fare clic su **Crea** > **Servizio di autenticazione**.





4. Dal menu a discesa **Servizio di autenticazione** selezionare **LDAP**.

5. Completare i campi obbligatori.

### Campo

Nome

Descrizione

Indirizzo server

Port

Associa utente

### Note

Immettere un nome per il server LDAP.

Immettere una descrizione per il server LDAP.

**Immettere il nome di dominio completo specificato nel campo Nome alternativo soggetto (SAN) del certificato del server LDAP.**

- Se il campo SAN contiene solo l'indirizzo IPv4, immettere l'indirizzo IPv4 nel campo Indirizzo server.
- Se il campo SAN contiene il nome DNS, immettere il nome DNS nel campo Indirizzo server.
- Se il campo SAN contiene sia valori DNS che IPv4, utilizzare il primo valore elencato.

Immettere la porta designata per la comunicazione LDAP protetta (LDAP su TLS). La porta TCP nota per LDAPS è la 636.

Immettere l'ID utente utilizzato per la connessione al server LDAP. Ad esempio: CN=admin,OU=utenti aziendali,DC=esempio,DC=com

**Nota:** Se gli utenti sono stati aggiunti a un contenitore AD incorporato (ad esempio, "Utenti"), il DN di associazione dell'utente di associazione deve avere il nome canonico (ad esempio, impostato sulla cartella predefinita (ad esempio, CN=nomeutente, CN=Utenti, DC=dominio, DC=com). Se tuttavia sono stati aggiunti gli utenti a un nuovo contenitore, l'unità organizzativa del DN di associazione deve essere impostata sul nuovo nome del contenitore, ad esempio, CN=nomeutente, OU=Utenti aziendali, DC=dominio, DC=com.

**Nota:** Un modo utile per trovare il DN di binding dell'utente di binding consiste nell'eseguire un query su Active Directory in un server Windows.

connesso al server Active Directory. Per ottenere queste informazioni, è possibile aprire un prompt dei comandi di Windows e digitare il comando `dsquery user dc=<distinguished>,dc=<name>,dc=<name>,dc=<name> -name <user>`. Ad esempio: `dsquery user dc=example,dc=com -name user1`. Il risultato sarà "CN=user1,OU=Corporate Users,DC=example,DC=com"

Password

Immettere la password utente di binding utilizzata per la connessione al server LDAP.

Immettere il nome distinto (DN).

Il DN si applica alla sezione della directory in cui devono iniziare le ricerche degli utenti. Spesso si trova nella parte superiore della struttura di directory (dominio), ma è possibile specificare anche una sottostruttura all'interno della directory. L'utente di binding e gli utenti da autenticare devono essere accessibili dagli account di base.

Ad esempio: DC=esempio,DC=com

Conti base

## 6. Fare clic su **Salva**.

Stealthwatch

Dashboards \* Monitor \* Analyze \* Jobs \* Configure \* Deploy \*

⚠ Add your SSL/TLS certificate to this appliance's Trust Store before you configure the LDAP Authentication service.

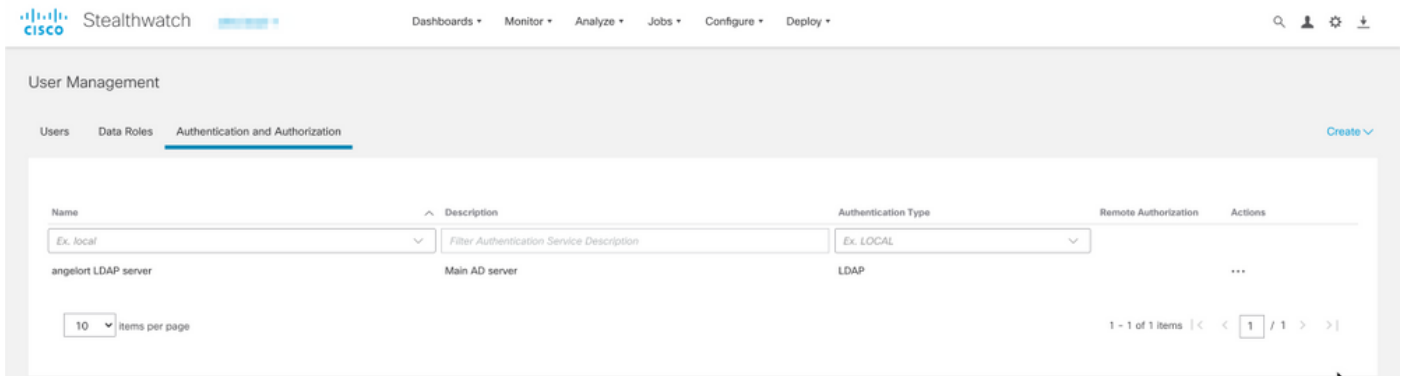
User Management | Authentication Service Cancel Save

\* = Required

Friendly Name *	angelort LDAP server	Authentication Service	LDAP
Description *	Main AD server	Port *	636
Server Address *	angelort-ad-10.10.10.10	Bind User *	CN=angelort,OU=SNA,OU=Cisco,DC=zitros,DC=local
Certificate Revocation *	Disabled	Base Accounts *	DC=zitros,DC=local
Password *	*****	Confirm Password *	*****

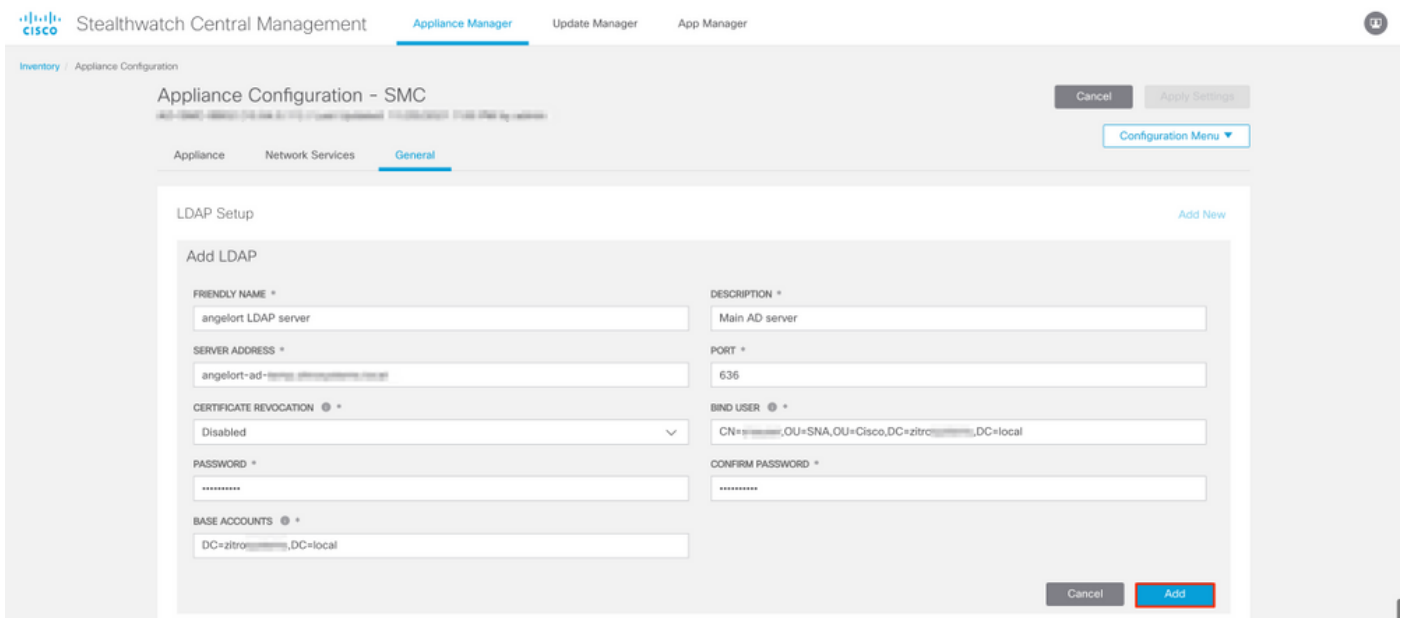
7. Se le impostazioni immesse e i certificati aggiunti all'archivio di attendibilità sono corretti, è necessario visualizzare il banner "Salvataggio delle modifiche completato".

8. Il server configurato deve essere visualizzato in **Gestione utenti > Autenticazione e autorizzazione**.



## SNA versione 7.1

1. Passare a **Gestione centrale** > Magazzino.
2. Individuare l'accessorio SMC e fare clic su **Azioni** > **Modifica configurazione accessorio**.
3. Nella finestra Configurazione accessorio passare a **Menu Configurazione** > **Impostazione LDAP** > **Aggiungi nuovo**.
4. Completare i campi obbligatori come descritto nel passaggio 5 della **SNA versione 7.2 o successive**.



5. Fare clic su **Aggiungi**.
6. Fare clic su **Applica impostazioni**.
7. Quando le impostazioni immesse e i certificati aggiunti all'archivio di attendibilità sono corretti, le modifiche apportate al Manager vengono applicate e lo stato dell'accessorio deve essere **Attivo**.

## Passaggio D. Configurare le impostazioni di autorizzazione.

La SNA supporta l'autorizzazione locale e remota tramite LDAP. Con questa configurazione, i gruppi LDAP del server AD vengono mappati a ruoli SNA predefiniti o personalizzati.

I metodi di autenticazione e autorizzazione supportati per SNA tramite LDAP sono:

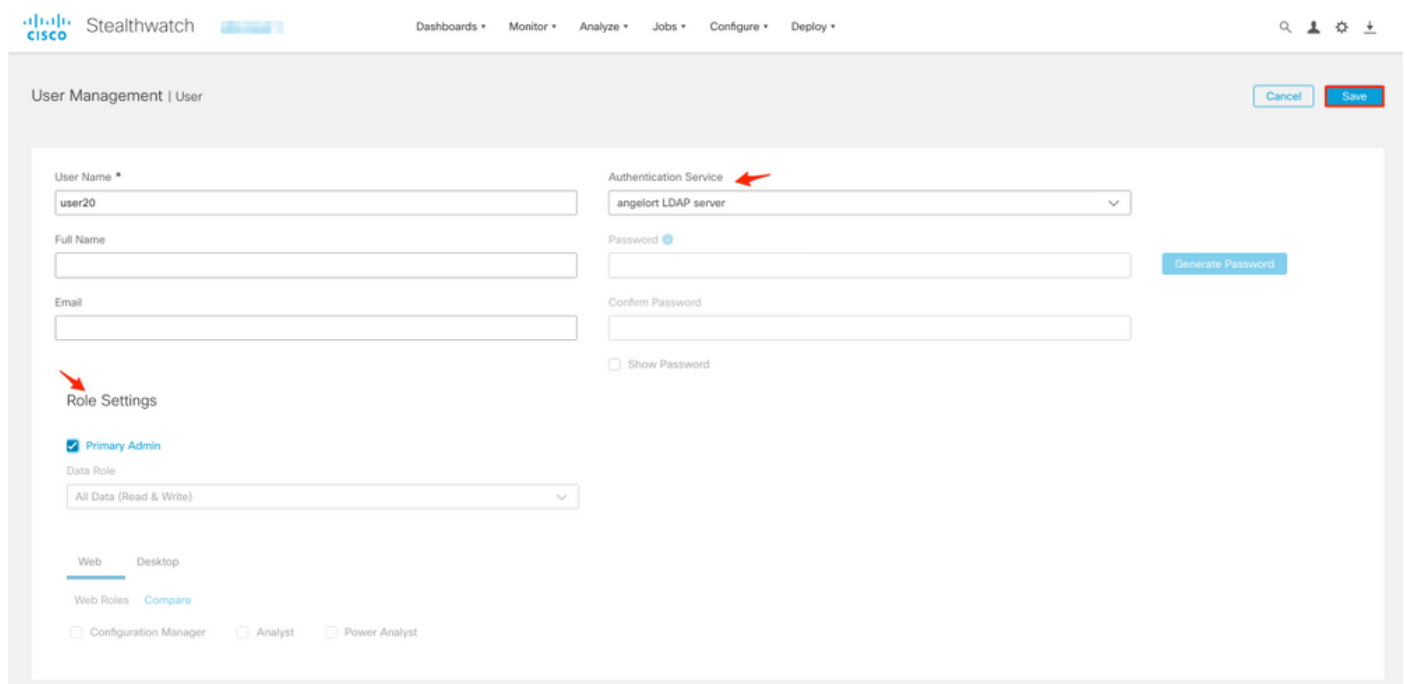
- Autenticazione remota e autorizzazione locale

- Autenticazione e autorizzazione remote (supportate solo per SNA versione 7.2.1 o successive)

## Autorizzazione locale

In questo caso, gli utenti e i relativi ruoli devono essere definiti localmente. A tale scopo, procedere come segue.

1. Passare di nuovo a **Gestione utente**, fare clic sulla scheda **Utenti > Crea > Utente**.
2. Definire il nome utente da autenticare con il server LDAP e selezionare il server configurato dal menu a discesa **Servizio di autenticazione**.
3. Definire le autorizzazioni che l'utente deve avere sul Manager una volta autenticato dal server LDAP e fare clic su **Salva**.



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 are:

- User Name \***: user20
- Authentication Service**: angelort LDAP server (indicated by a red arrow)
- Full Name**: (empty)
- Password**: (empty) with a 'Generate Password' button
- Confirm Password**: (empty)
- Show Password**:
- Role Settings**: (indicated by a red arrow)
- Primary Admin**:
- Data Role**: All Data (Read & Write)
- Web** / **Desktop** tabs
- Web Roles**: **Compare** (selected)
- Configuration Manager**:
- Analyst**:
- Power Analyst**:

## Autorizzazione remota tramite LDAP

L'autenticazione e l'autorizzazione in remoto tramite LDAP sono state inizialmente supportate in Secure Network Analytics versione 7.2.1.

**Nota:** L'autorizzazione remota con LDAP non è supportata nella versione 7.1.

È importante ricordare che se un utente è definito e abilitato localmente (in Manager), viene autenticato in remoto, ma autorizzato localmente. Il processo di selezione degli utenti è il seguente:

1. Una volta immesse le credenziali nella pagina di benvenuto del Manager, quest'ultimo cerca un utente locale con il nome specificato.
2. Se un utente locale viene individuato e abilitato, viene autenticato in remoto (se l'autenticazione remota tramite LDAP con autorizzazione locale è stata configurata in

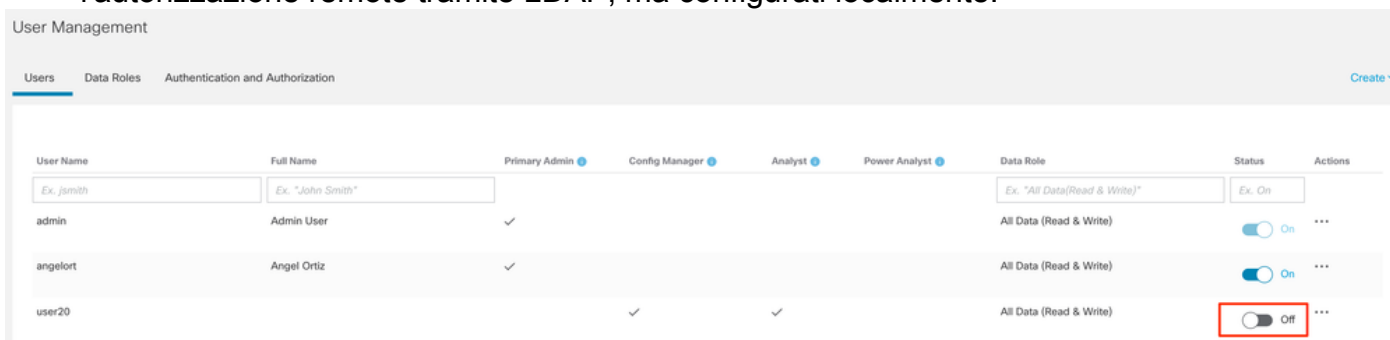
precedenza) ma autorizzato con le impostazioni locali.

3. Se l'autorizzazione remota è configurata e abilitata e l'utente non viene trovato localmente (non configurato o disabilitato), sia l'autenticazione che l'autorizzazione vengono eseguite in remoto.

Per questo motivo, per configurare correttamente l'autenticazione remota, è necessario eseguire la procedura seguente.

### Passaggio D-1. Disabilitare o eliminare gli utenti che intendono utilizzare l'autorizzazione remota ma che sono definiti localmente.

1. Aprire il dashboard principale di Manager e selezionare Impostazioni globali > Gestione utente.
2. Disabilitare o eliminare gli utenti (se esistenti) destinati a utilizzare l'autenticazione e l'autorizzazione remote tramite LDAP, ma configurati localmente.



### Passaggio D-2. Definire i gruppi cisco-stealthwatch nel server AD Microsoft.

Per l'autenticazione e l'autorizzazione esterne tramite utenti LDAP, le password e i gruppi *cisco-stealthwatch* vengono definiti in remoto in Microsoft Active Directory. I gruppi *cisco-stealthwatch* da definire nel server AD sono correlati ai diversi ruoli svolti dalla SNA e devono essere definiti come segue.

#### Ruolo SNA

Amministratore primario

#### Ruolo dati

#### Ruolo funzionale Web

#### Ruolo funzionale del desktop

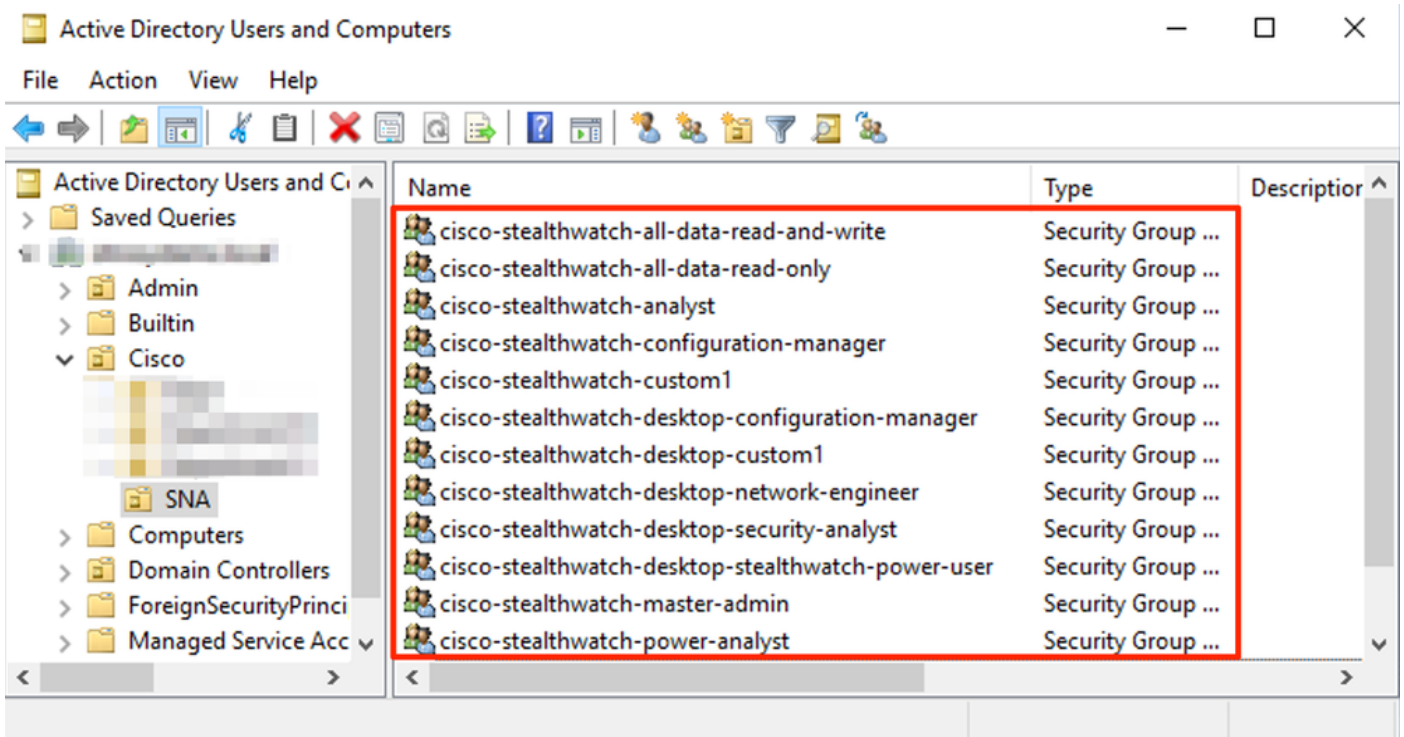
#### Nome gruppo/i

- cisco-stealthwatch-master-admin
- cisco-stealthwatch-all-data-read-and-write
- cisco-stealthwatch-all-data-read-only
- cisco-stealthwatch-<personalizzato> (opzionale)

**Nota:** Verificare che i gruppi di ruoli dati personalizzati inizino con "cisco-stealthwatch"

- 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-<personalizzato> (opzionale)

**Nota:** Verificare che i gruppi di ruoli funzionali desktop personalizzati inizino con "cisco-stealthwatch-desktop-".

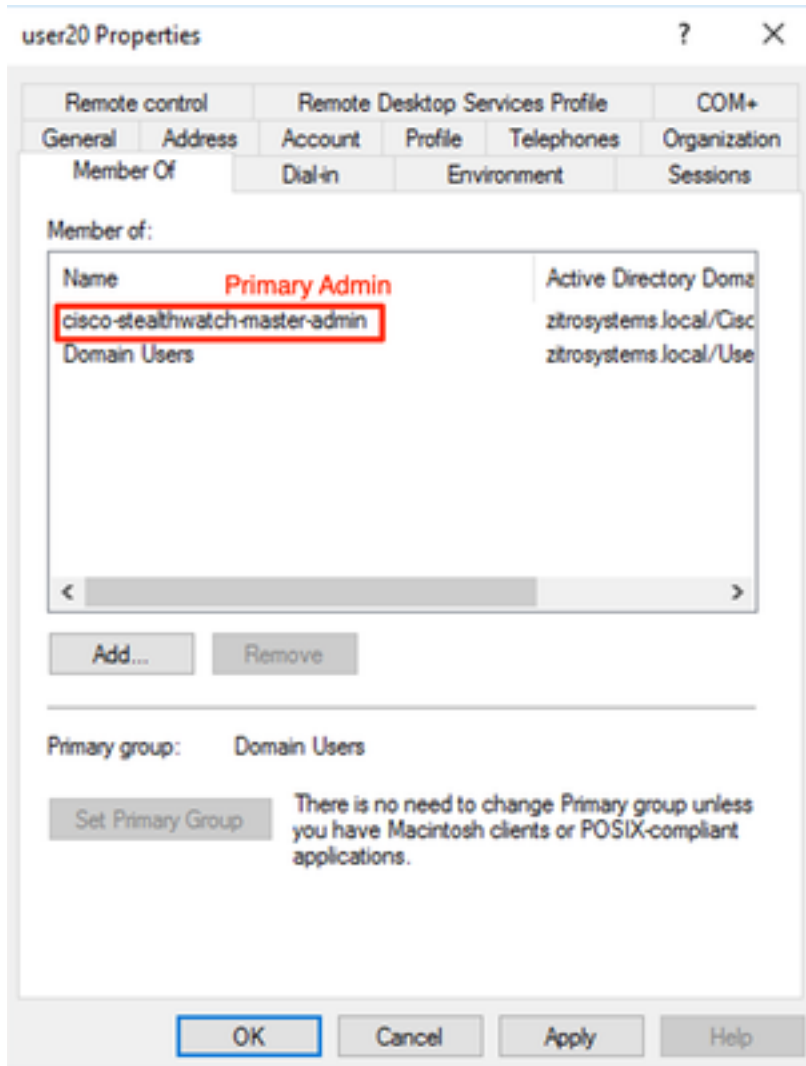


**Nota:** Come descritto in precedenza, i gruppi personalizzati sono supportati per "Ruolo dati" e "Ruolo funzionale desktop" a condizione che al nome del gruppo sia anteposta la stringa corretta. I ruoli e i gruppi personalizzati devono essere definiti sia in Gestione SNA che nel server Active Directory. Ad esempio, se si definisce un ruolo personalizzato "custom1" in Gestione SNA per un ruolo client desktop, è necessario mapparli a cisco-stealthwatch-desktop-custom1 in Active Directory.

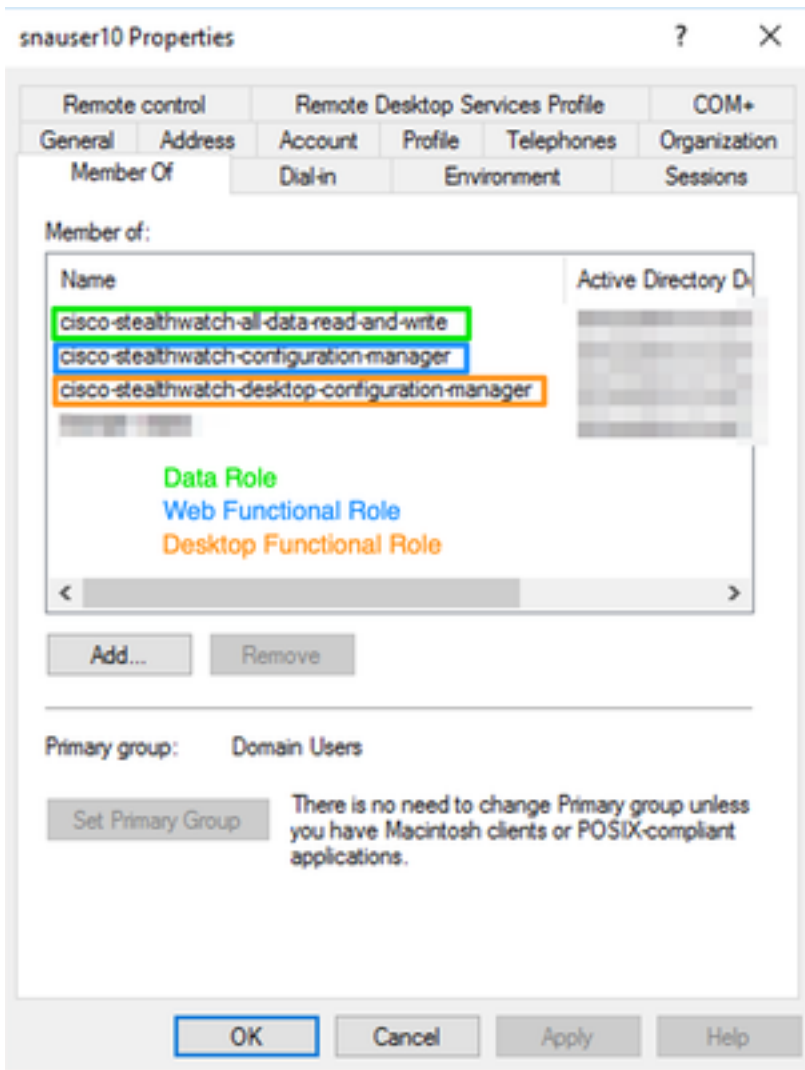
### Passaggio D-3. Definire i mapping dei gruppi di autorizzazione LDAP per gli utenti.

Una volta definiti i gruppi *cisco-stealthwatch* nel server AD, è possibile mappare gli utenti che devono accedere a SNA Manager sui gruppi necessari. Ciò deve avvenire nel modo seguente.

- Un utente **Admin primario** deve essere assegnato al gruppo *cisco-stealthwatch-master-admin* e non deve essere membro di alcun altro gruppo *cisco-stealthwatch*.



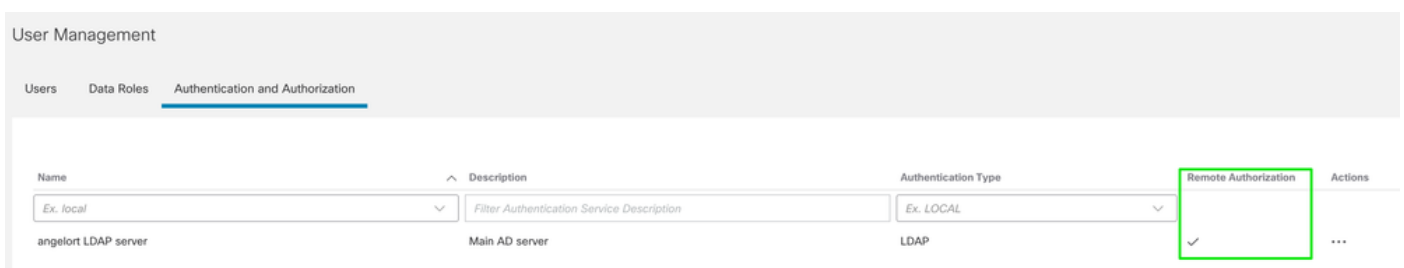
- Ogni utente, diverso dagli utenti Amministratore primario, deve essere assegnato a un gruppo di ogni ruolo con le condizioni successive.
  1. **Ruolo dati:** L'utente deve essere assegnato a **un solo gruppo**.
  2. **Ruolo funzionale Web:** L'utente deve essere assegnato ad **almeno un gruppo**.
  3. **Ruolo funzionale del desktop:** L'utente deve essere assegnato ad **almeno un gruppo**.



#### Passaggio D-4. Abilitare l'autorizzazione remota tramite LDAP su SNA Manager.

1. Aprire il dashboard principale di Manager e passare a **Impostazioni globali > Gestione utente**.
2. Nella finestra **Gestione utenti** selezionare la scheda **Autenticazione e autorizzazione**.
3. Individuare il servizio di autenticazione LDAP configurato nel **passo C**.
4. Fare clic su **Azioni > Abilita autorizzazione remota**.

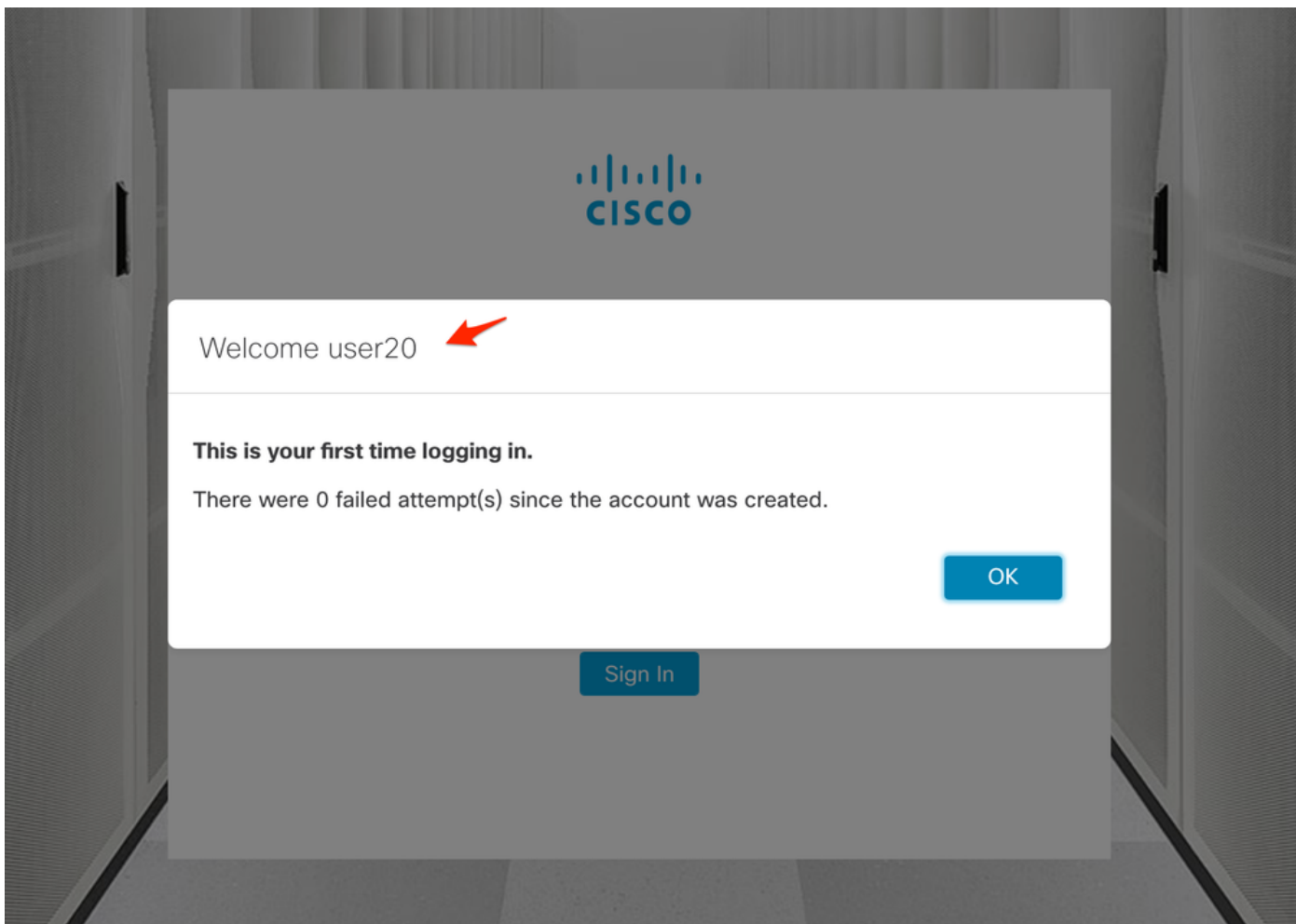
**Nota:** È possibile utilizzare un solo servizio di autorizzazione esterno alla volta. Se un altro servizio di autorizzazione è già in uso, viene automaticamente disabilitato e il nuovo servizio viene abilitato, tuttavia tutti gli utenti autorizzati con il servizio esterno precedente verranno disconnessi. Prima di eseguire qualsiasi azione viene visualizzato un messaggio di conferma.



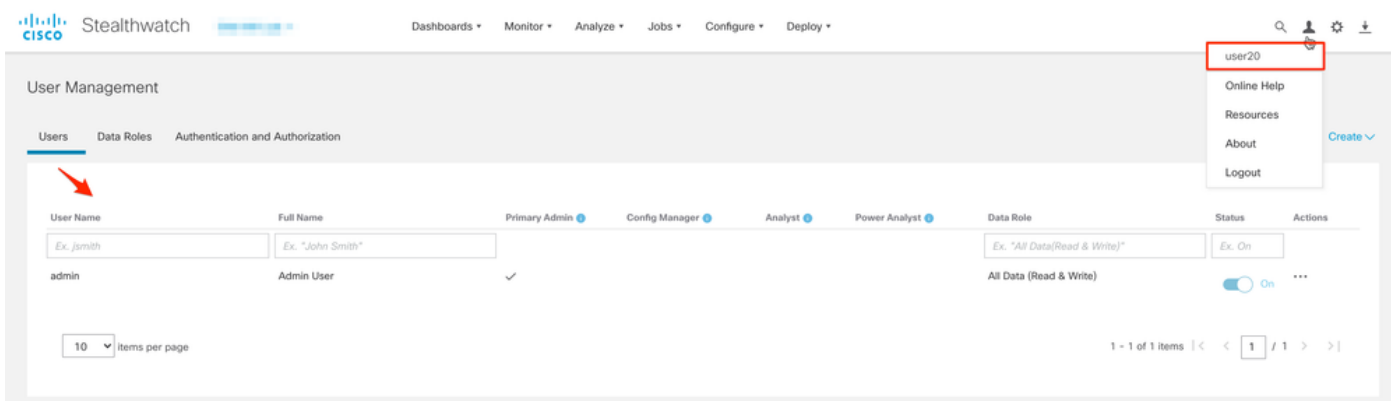
## Verifica



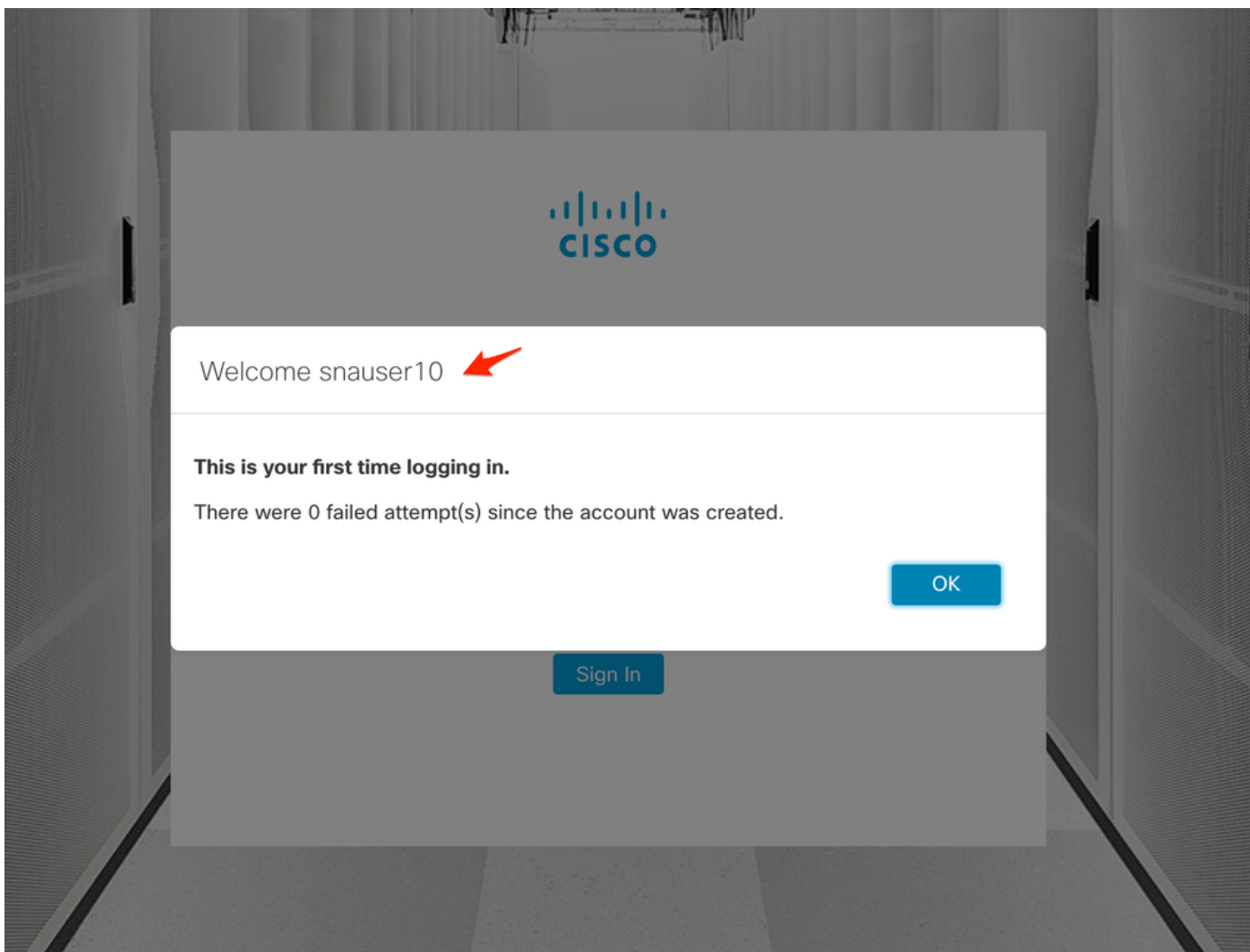
Gli utenti possono accedere con le credenziali definite nel server AD.



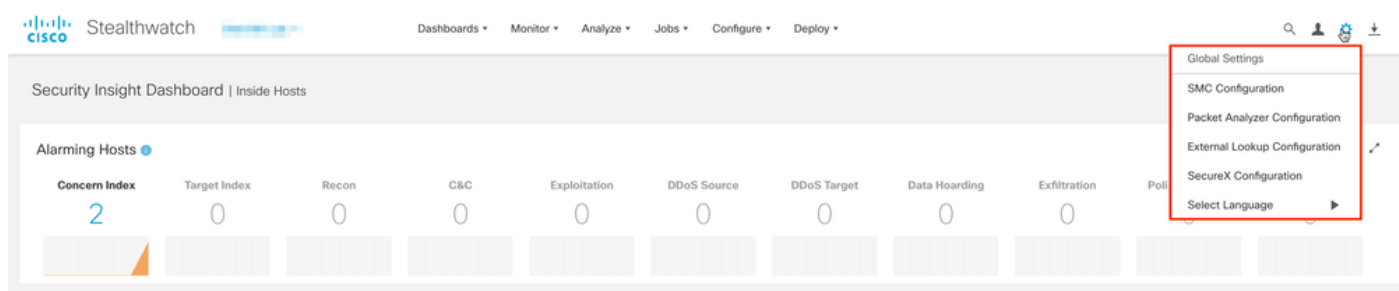
La seconda fase di verifica riguarda l'autorizzazione. Nell'esempio, l'utente "user20" è stato aggiunto al gruppo *cisco-stealthwatch-master-admin* nel server AD e possiamo confermare che l'utente ha le autorizzazioni di amministratore primario. L'utente non è definito negli utenti locali, pertanto è possibile verificare che gli attributi di autorizzazione siano stati inviati dal server AD.



La stessa verifica viene effettuata per l'altro utente in questo esempio "serpente10". È possibile confermare la riuscita dell'autenticazione con le credenziali configurate nel server AD.



Per la verifica dell'autorizzazione, alcune funzionalità non sono disponibili perché l'utente non appartiene al gruppo Amministratore primario.



## Risoluzione dei problemi

Se non è possibile salvare la configurazione del servizio di autenticazione, verificare che:

1. I certificati appropriati del server LDAP sono stati aggiunti all'archivio di attendibilità di Manager.
2. L'**indirizzo del server** configurato è quello specificato nel campo Nome alternativo soggetto (SAN) del certificato del server LDAP. Se il campo SAN contiene solo l'indirizzo IPv4, immettere l'indirizzo IPv4 nel campo Indirizzo server. Se il campo SAN contiene il nome DNS, immettere il nome DNS nel campo Indirizzo server. Se il campo SAN contiene sia valori DNS che IPv4, utilizzare il primo valore elencato.

3. I campi **Associa utente** e **Account di base** configurati sono corretti, come specificato dal controller di dominio Active Directory.

## Informazioni correlate

Per ulteriore assistenza, contattare il Cisco Technical Assistance Center (TAC). È necessario un contratto di supporto valido: [Contatti del supporto Cisco internazionali](#).