# Secure Network Analytics Manager 액세스를 위해 LDAPS를 통해 외부 인증 및 권한 부여 구성

## 목차



## 소개

이 문서에서는 외부 인증을 사용하기 위해 Secure Network Analytics Manager(이전의 Stealthwatch Management Center) 버전 7.1 이상의 기본 컨피그레이션을 설명하고 버전 7.2.1 이상의 LDAPS에서 외부 권한 부여를 사용하는 방법에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Secure Network Analytics(이전의 Stealthwatch)
- 일반 LDAP 및 SSL 작업
- 일반 Microsoft Active Directory 관리

### 사용되는 구성 요소

이 문서의 정보는 다음 구성 요소를 기반으로 합니다.

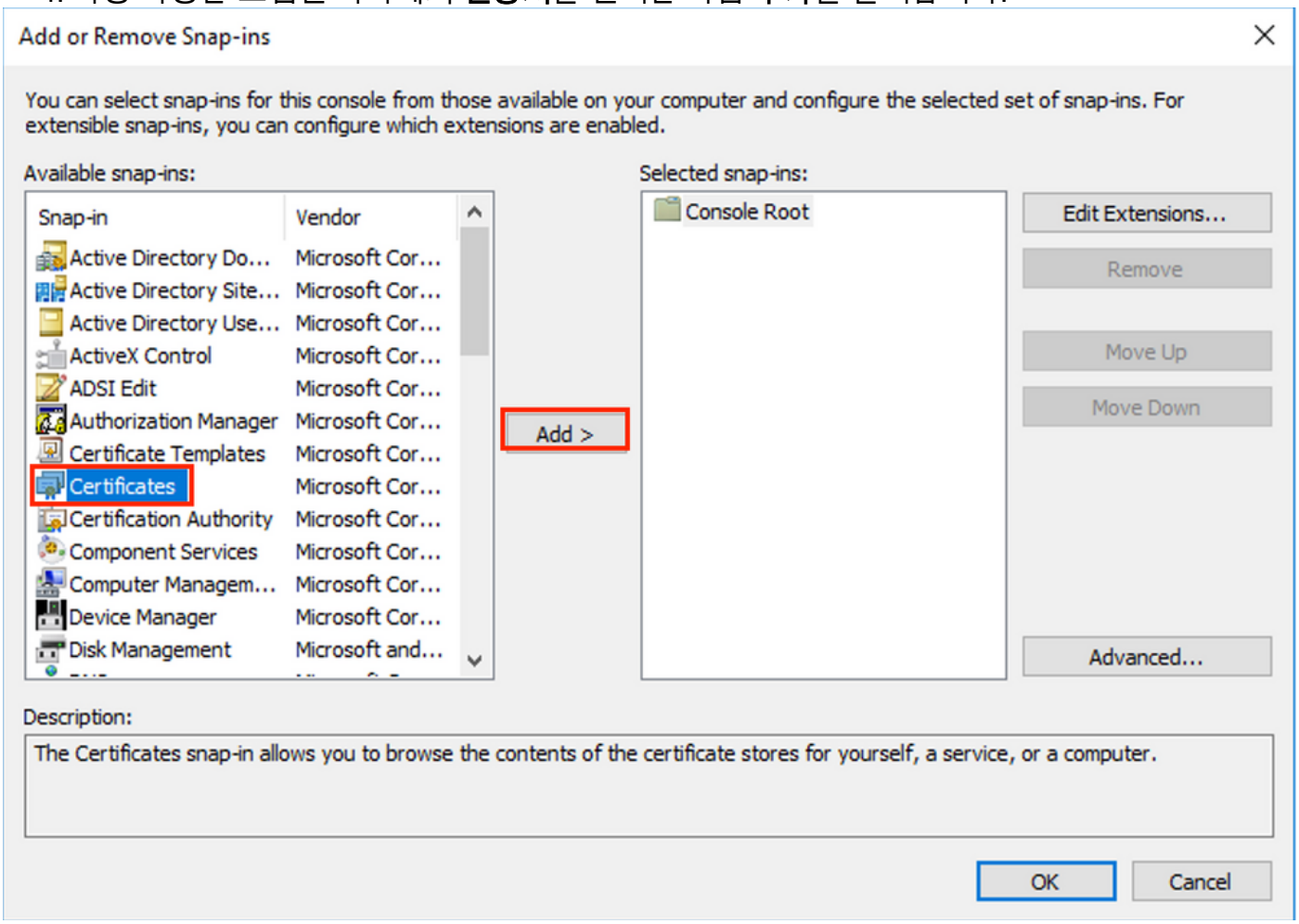
- Cisco Secure Network Analytics Manager(이전의 SMC) 버전 7.3.2
- Active Directory 도메인 컨트롤러로 구성된 Windows Server 2016

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

# 구성

## A단계. AD 도메인 컨트롤러에 로그인하고 LDAP에 사용되는 SSL 인증서를 내보냅니다.

1. Windows Server 2012 이상의 경우 시작 메뉴에서 **실행**을 선택한 다음 certlm.**msc를** 입력하고 **8**단계를 계속 **진행합니다**.
2. 이전 Windows Server 버전의 경우 시작 메뉴에서 **실행**을 선택한 다음 mmc를 **입력합니다**.
3. [파일] 메뉴에서 [스냅인 추가/**제거]를 선택합니다**.
4. 사용 가능한 스냅인 목록에서 **인증서**를 선택한 다음 **추가**를 클릭합니다.

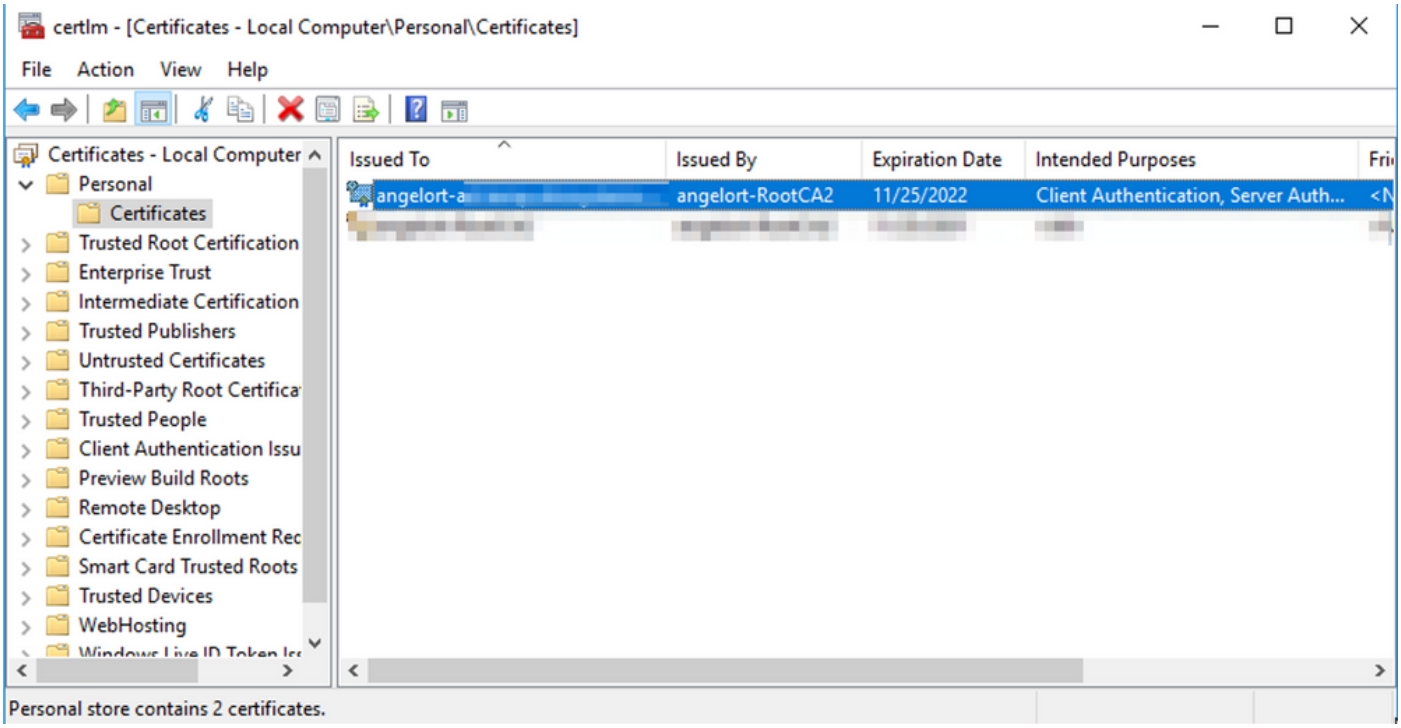



5. **인증서 스냅인** 창에서 **컴퓨터 계정**을 선택한 다음 **다음을 선택합니다**.

6. **로컬 컴퓨터**를 선택한 다음 **마침**을 선택합니다.

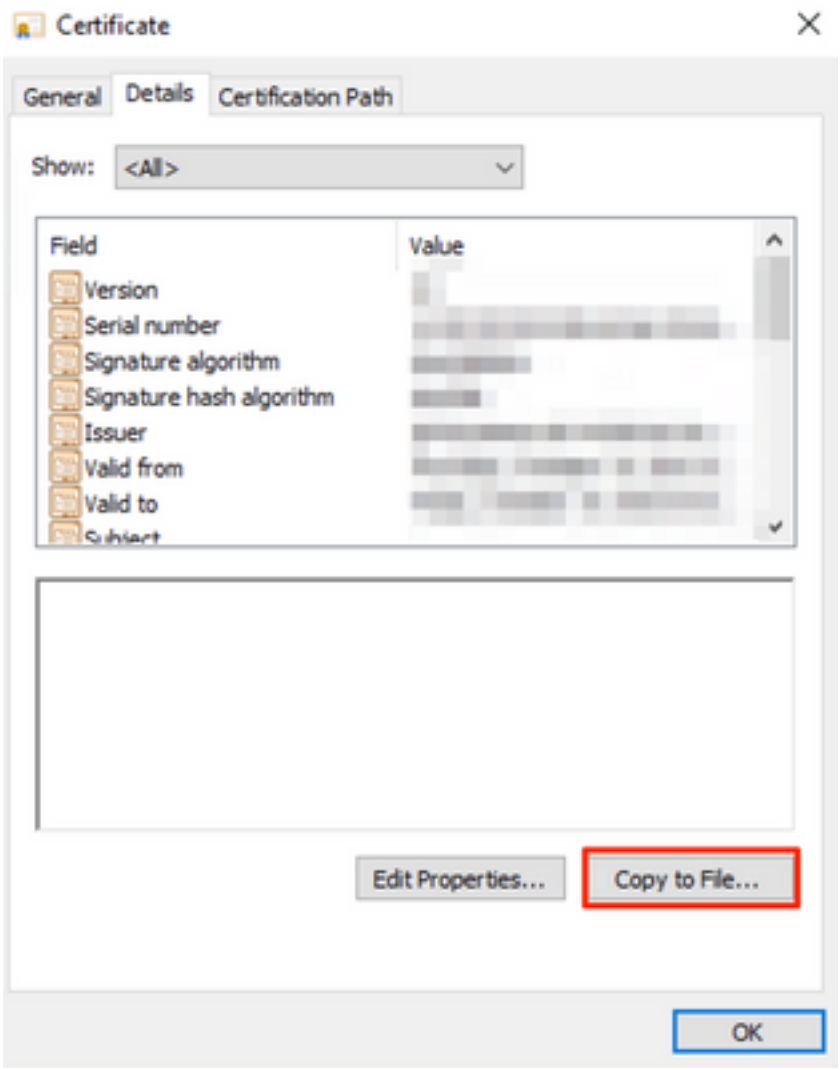
7. 스냅인 **추가 또는 제거** 창**에서 확인**을 선택합니다.

8. **인증서(로컬 컴퓨터) > 개인 > 인증서로 이동합니다.**



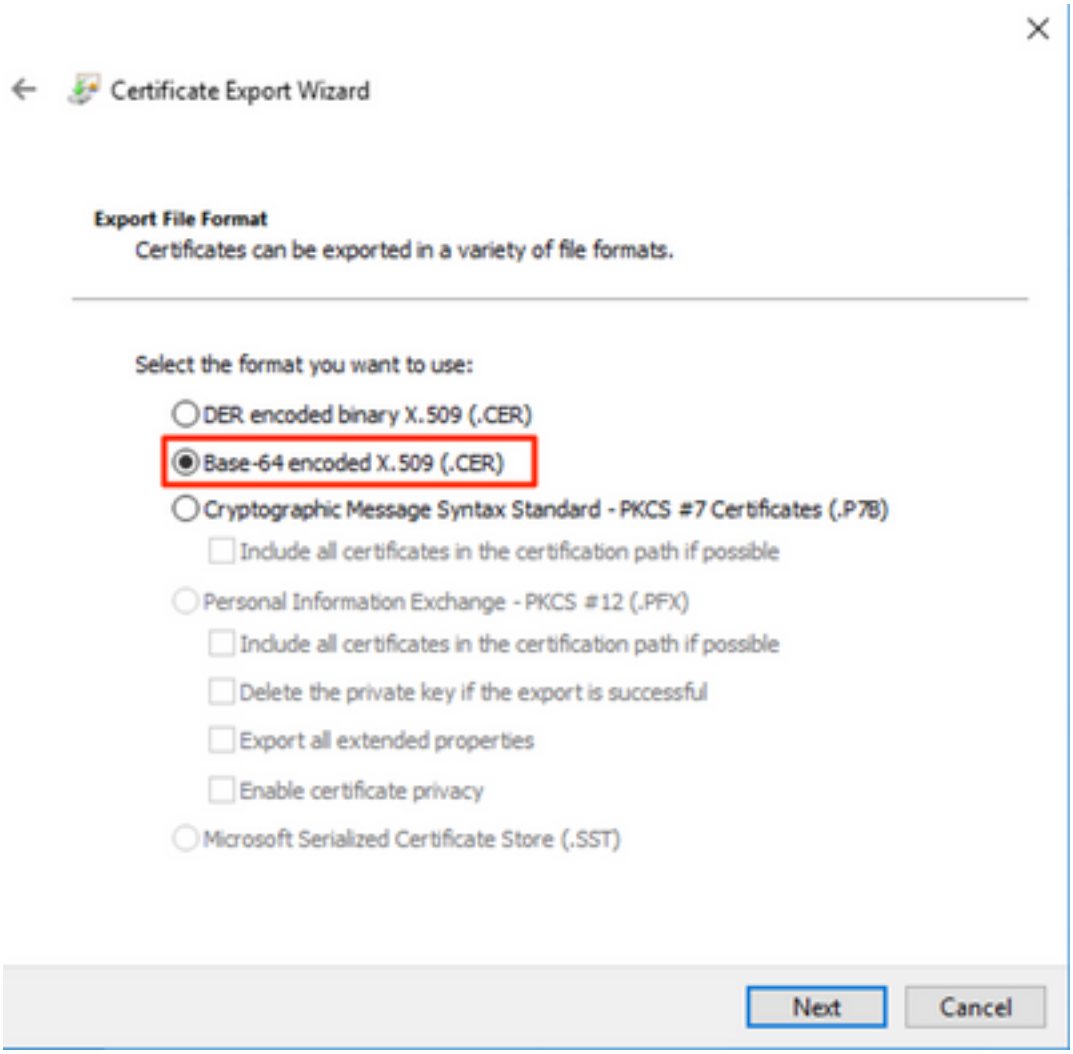

9. 도메인 컨트롤러에서 LDAPS 인증에 사용되는 SSL 인증서를 선택하고 마우스 오른쪽 버튼으로 클릭하고 **열기**를 클릭합니다.

10. 상세내역 탭으로 이동 > **파일로 복사** > **다음을** 누릅니다.

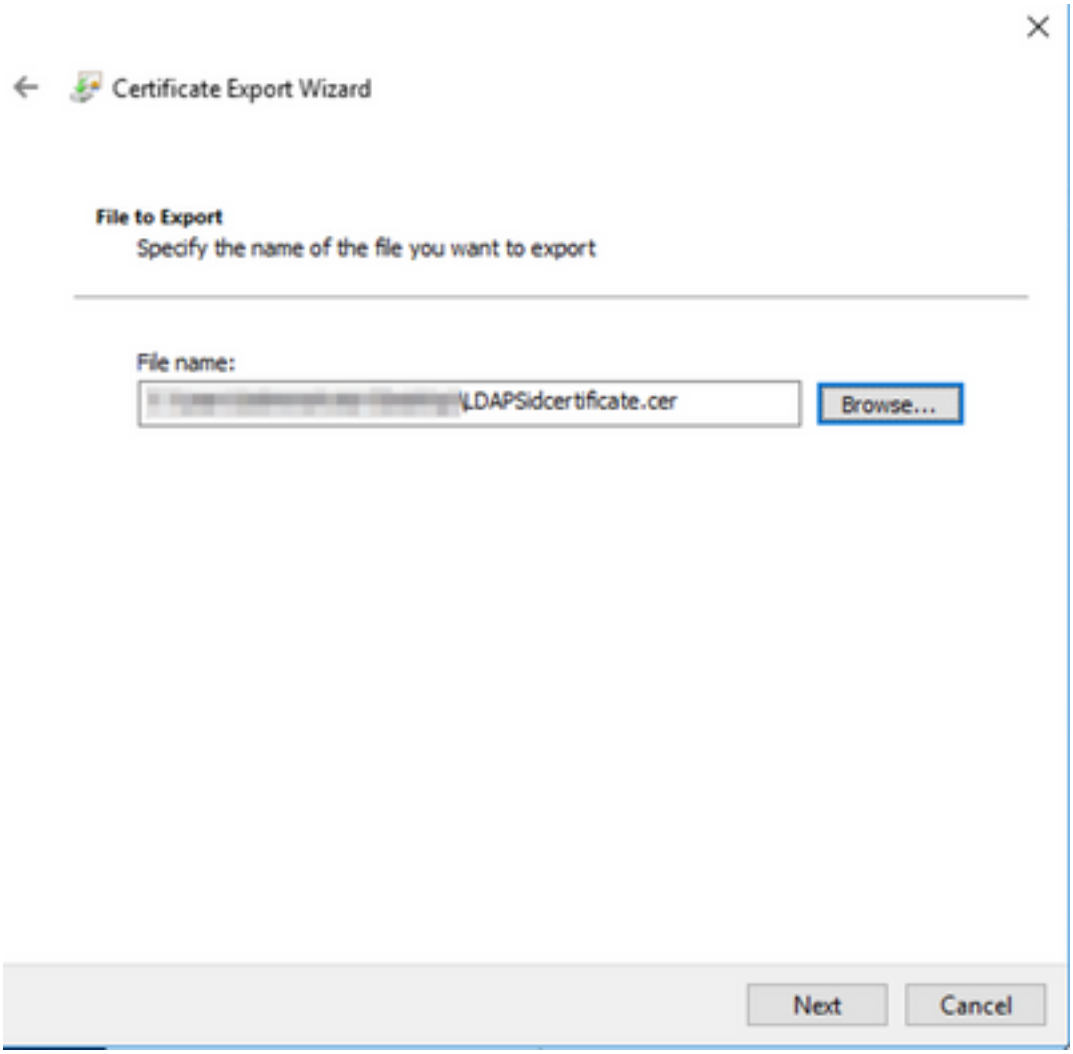


11. **아니요, 개인 키를 내보내지 않음**을 선택했는지 확인하고 **다음**을 클릭합니다.

12. **Base-64 인코딩 X.509** 형식을 선택하고 **다음**을 클릭합니다.




13. 인증서를 저장할 위치를 선택하고 파일 이름을 지정한 다음 **다음**을 클릭합니다.




14. **[마침]**을 클릭하면 "The export was successful"이 표시됩니다. 메시지.

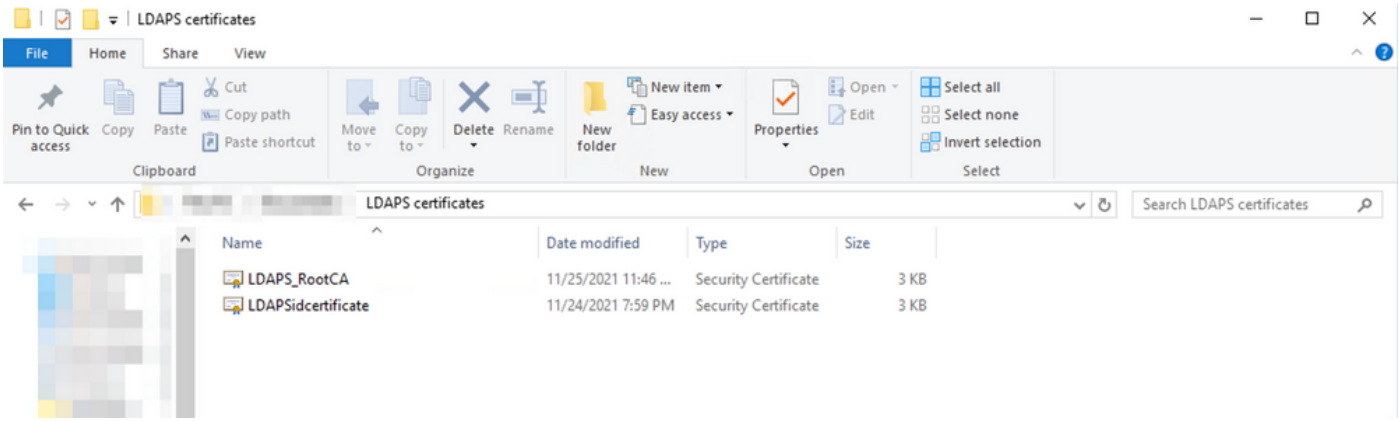
15. LDAPS에 사용된 인증서로 돌아가서 **Certification Path** 탭을 선택합니다.

16. 인증 경로 위에 있는 루트 CA 발급자를 선택하고 **인증서 보기**를 클릭합니다.


17. 10-14단계를 반복하여 LDAPS 인증에 사용되는 인증서를 서명한 루트 CA의 인증서를 내보냅니다.

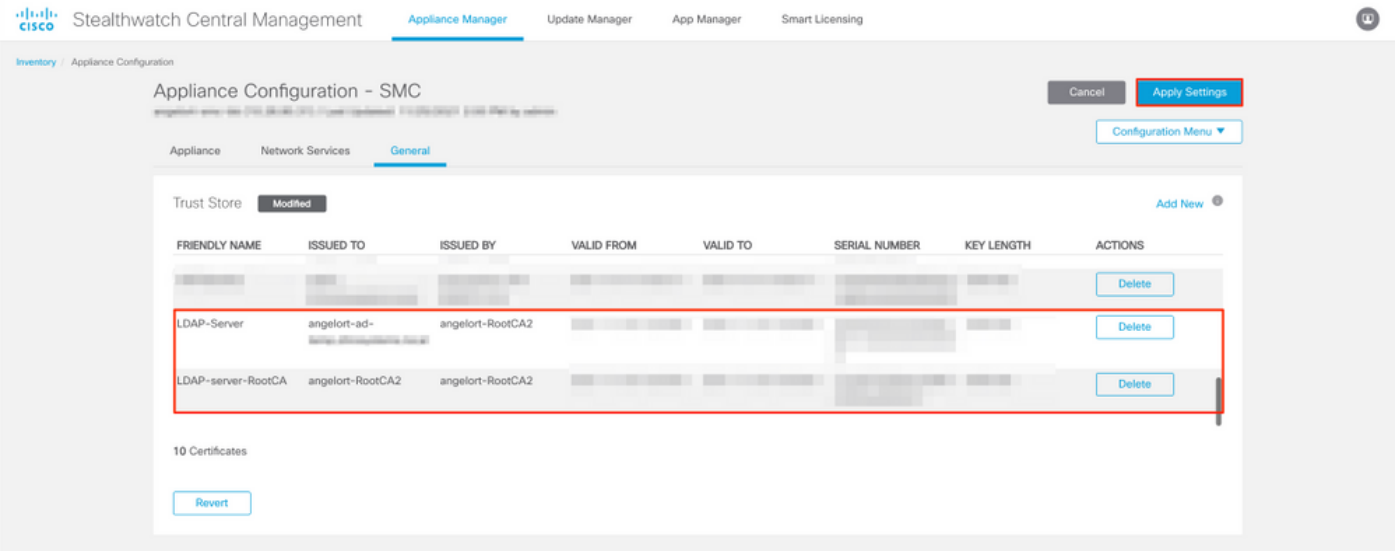
> **참고:** 구축에는 다중 계층 CA 계층이 있을 수 있습니다. 이 경우 신뢰 체인의 모든 중간 인증서를 내보내려면 동일한 절차를 따라야 합니다.

18. 계속하기 전에 인증 경로에 LDAPS 서버 및 발급자 기관별 인증서 파일이 하나씩 있는지 확인하십시오. 루트 인증서 및 중간 인증서(해당되는 경우).




## B단계. SNA Manager에 로그인하여 LDAP 서버 및 루트 체인의 인증서를 추가합니다.

1. **Central Management** > Inventory로 이동합니다.
2. SNA Manager 어플라이언스를 찾아 Actions(작업) > **Edit Appliance Configuration(어플라이언스 컨피그레이션 수정)을** 클릭합니다.
3. Appliance Configuration(어플라이언스 컨피그레이션) 창에서 **Configuration Menu(컨피그레이션 메뉴) > Trust Store(트러스트 저장소)** > Add New(**새로 추가)로 이동합니다**.
4. Friendly Name(식별 이름)을 입력하고 Choose **File(파일 선택)**을 클릭하고 LDAP 서버의 인증서를 선택한 다음 Add Certificate(인증서 추가)를 **클릭합니다**.
5. 이전 단계를 반복하여 루트 CA 인증서 및 중간 인증서(해당하는 경우)를 추가합니다.
6. 업로드된 인증서가 올바른지 확인하고 Apply Settings(설정 **적용)**를 클릭합니다.

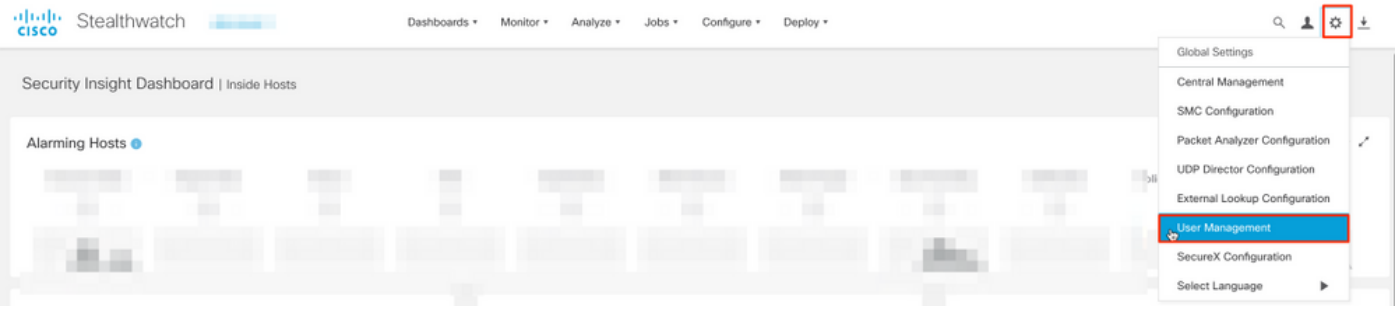



7. 변경 사항이 적용되고 관리자 상태가 작동 상태가 될 때까지 **기다립니다**.

## C단계 LDAP 외부 서비스 컨피그레이션을 추가합니다.

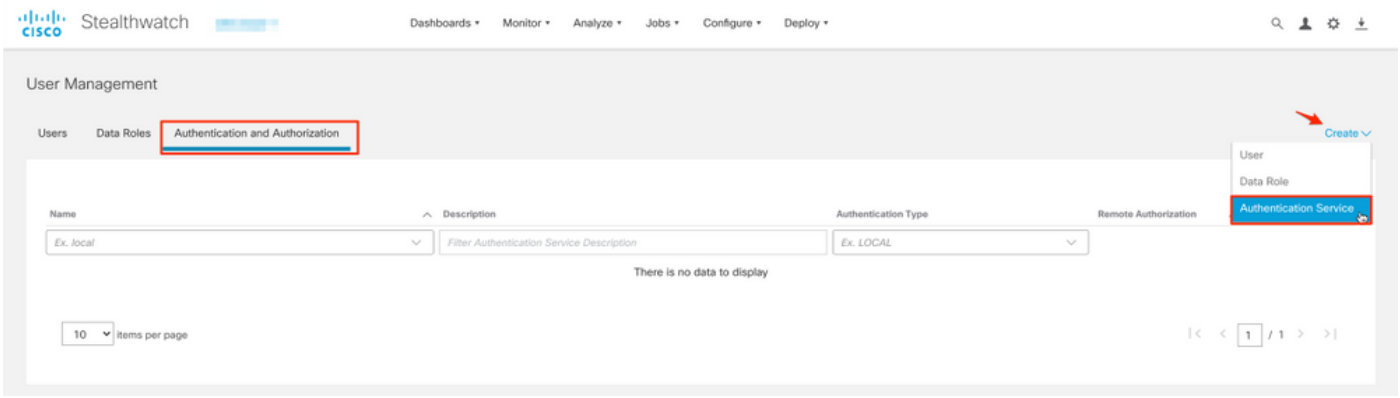
### SNA 버전 7.2 이상

1. 관리자 기본 대시보드를 열고 **전역 설정 > 사용자 관리로 이동합니다**.




2. 사용자 관리 창에서 **인증 및 권한 부여** 탭을 선택합니다.

3. **생성 > 인증 서비스를** 클릭합니다.



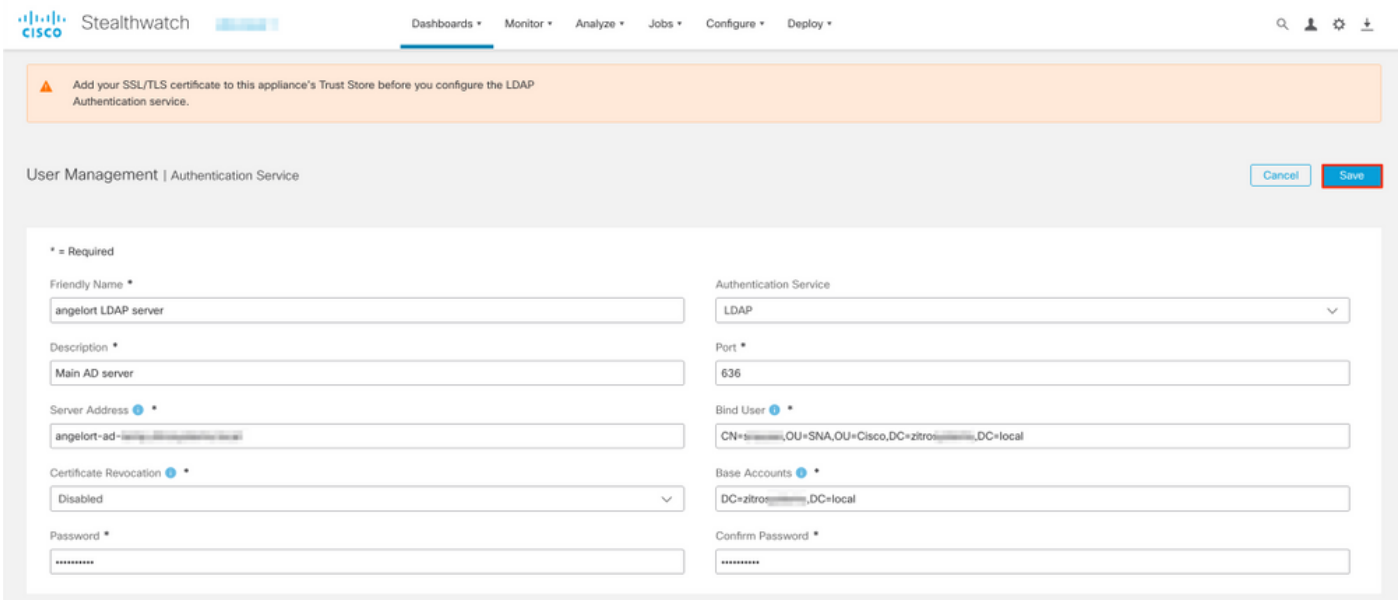

4. **Authentication Service** 드롭다운 메뉴에서 **LDAP를** 선택합니다.

5. 필수 필드를 완료합니다.

| **필드** | **참고** |
| --- | --- |
| 이름 | LDAP서버의 이름을 입력합니다. |
| 설명 | LDAP 서버에 대한 설명을 입력합니다. |
| **서버 주소** | **LDAP 서버 인증서의 SAN(Subject Alternative Na 필드에 지정된 대로 정규화된 도메인 이름을 입력 다.**<br>• SAN 필드에 IPv4 주소만 포함된 경우 Server Address 필드에 IPv4 주소를 입력합니다.<br>• SAN 필드에 DNS 이름이 포함된 경우 Server Address 필드에 DNS 이름을 입력합니다.<br>• SAN 필드에 DNS 값과 IPv4 값이 모두 포함도 으면 나열된 첫 번째 값을 사용합니다. |
| 포트 | 보안 LDAP 통신(LDAP over TLS)을 위해 지정된 를 입력합니다. LDAPS에 대해 잘 알려진 TCP 포 636입니다. |
| 사용자 바인딩 | LDAP 서버에 연결하는 데 사용되는 사용자 ID를 합니다. 예를 들면 다음과 같습니다. CN=admin,O 업 사용자,DC=example,DC=com<br><br>**참고:** 사용자를 기본 제공 AD 컨테이너(예: "Users")에 추가한 경우 바인드 사용자의 바인 DN에는 기본 제공 폴더(예: CN=username, CN=Users, DC=domain, DC=com)에 정식 이 (CN)이 설정되어 있어야 합니다. 그러나 사용 새 컨테이너에 추가한 경우 바인드 DN에는 테이너 이름(예: CN=username, OU=Corpora Users, DC=domain, DC=com)으로 설정된 O 직 단위)가 있어야 합니다.<br><br>**참고:** 바인드 사용자의 바인드 DN을 찾는 유 방법은 Active Directory 서버에 연결된 Windo Server에서 Active Directory를 쿼리하는 것입 . 이 정보를 가져오려면 Windows 명령 프롬프 를 열고 명령 dsquery **user dc=<distinguished>,dc=<name> -name <use 입력합니다**. 예: dsquery **user** |

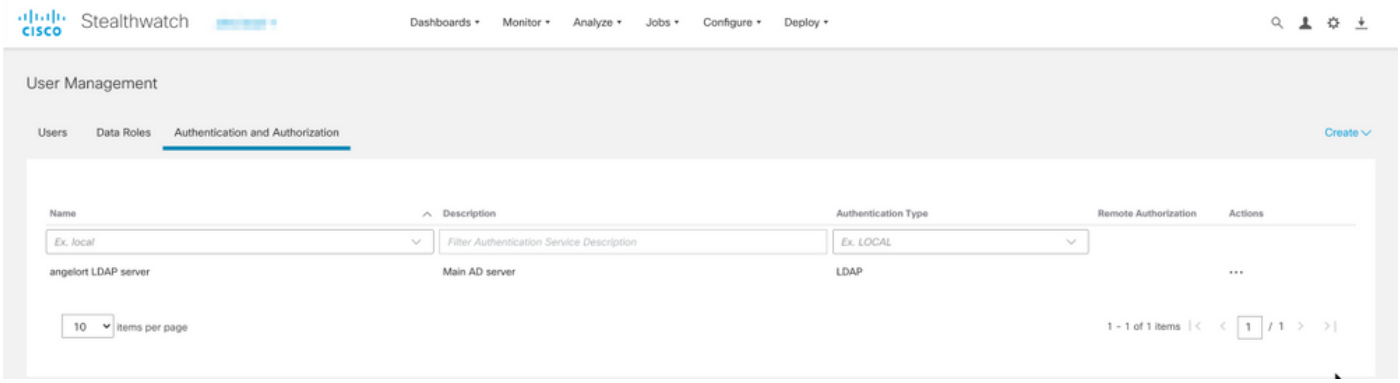
| | |
|---|---|
| | **dc=example,dc=com -name user1**. 결과는 "CN=user1,OU=Corporate Users,DC=example,DC=com"과 같습니다. |
| 비밀번호 | LDAP 서버에 연결하는 데 사용되는 바인드 사용자 밀번호를 입력합니다. |
| 기본 계정 | DN(Distinguished Name)을 입력합니다. DN은 사용자 검색을 시작해야 하는 디렉토리의 분 적용됩니다. 디렉터리 트리의 맨 위(도메인)인 경우 많으나 디렉터리 내에서 하위 트리를 지정할 수도 니다. 바인드 사용자와 인증하려는 사용자는 기본 에서 액세스할 수 있어야 합니다. 예를 들면 다음과 같습니다. DC=예,DC=com |

6. 저장을 **클릭합니다**.




7. 입력한 설정과 신뢰 저장소에 추가된 인증서가 올바르면 "변경 내용을 저장했습니다." 배너가 있어야 합니다.

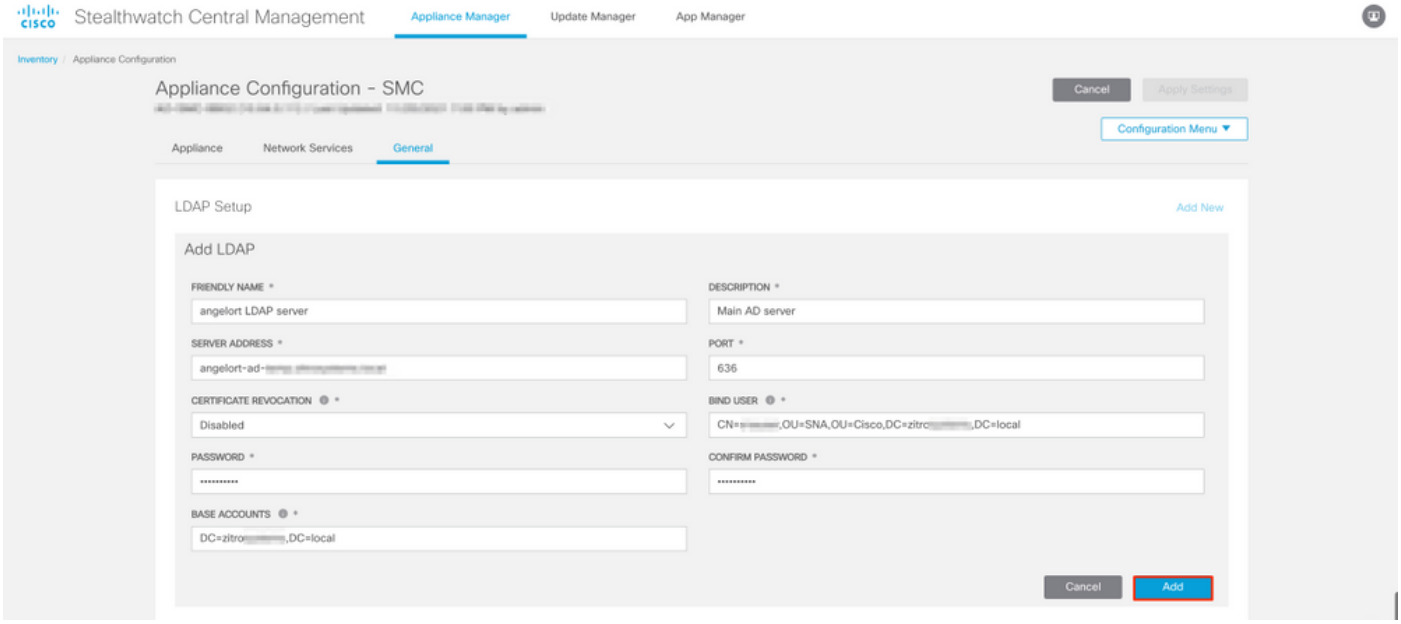
8. 구성된 서버는 **User Management**(사용자 **관리**) > **Authentication and Authorization(인증 및 권한 부여)에** 표시되어야 합니다.




## SNA 버전 7.1

1. **Central Management** > Inventory로 이동합니다.

2. SMC 어플라이언스를 찾아 Actions(작업) > **Edit Appliance Configuration(어플라이언스 컨피그레이션 편집)을 클릭합니다**.
3. Appliance Configuration(어플라이언스 컨피그레이션) 창에서 **Configuration Menu(컨피그레이션 메뉴) > LDAP Setup(LDAP 설정)** > Add New(**새로 추가)로 이동합니다**.
4. SNA **버전 7.2 이상** 5단계에 설명된 대로 필수 필드**를** 완료합니다.




5. 추가를 **클릭합니다**.

6. 설정 **적용을 클릭합니다**.

7. 입력한 설정과 신뢰 저장소에 추가된 인증서가 올바르면 관리자의 변경 사항이 적용되며 어플라이언스 상태가 **Up**이어야 합니다.

## D단계. 권한 부여 설정을 구성합니다.

SNA는 LDAP를 통한 로컬 및 원격 권한 부여를 모두 지원합니다. 이 컨피그레이션에서는 AD 서버의 LDAP 그룹이 기본 제공 또는 사용자 지정 SNA 역할에 매핑됩니다.

LDAP를 통해 SNA에 대해 지원되는 인증 및 권한 부여 방법은 다음과 같습니다.

- 원격 인증 및 로컬 권한 부여
- 원격 인증 및 원격 권한 부여(SNA 버전 7.2.1 이상에서만 지원됨)

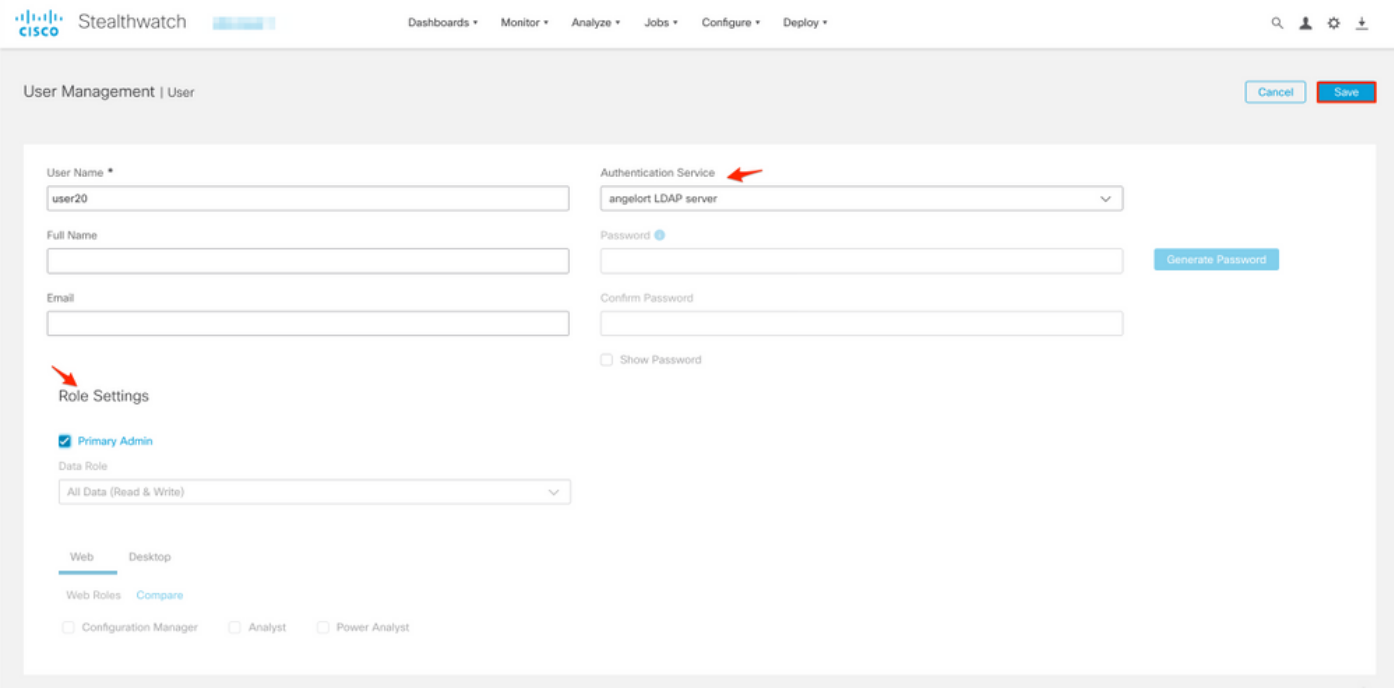
### 로컬 권한 부여

이 경우 사용자와 해당 역할을 로컬로 정의해야 합니다. 이를 위해서는 다음과 같이 진행합니다.

1. **사용자 관리**로 다시 이동하여 **사용자** 탭 > 생성 > **사용자**를 클릭합니다.

2. LDAP 서버로 인증할 사용자 이름을 정의하고 **Authentication Service** 드롭다운 메뉴에서 구성된 서버를 선택합니다.

3. LDAP 서버가 인증한 후 관리자를 통해 사용자가 가져야 하는 권한을 정의하고 **Save**를 클릭합니다.




## LDAP를 통한 원격 권한 부여

LDAP를 통한 원격 인증 및 권한 부여는 Secure Network Analytics 버전 7.2.1에서 먼저 지원됩니다.

> **참고:** LDAP를 사용한 원격 권한 부여는 버전 7.1에서 지원되지 않습니다.

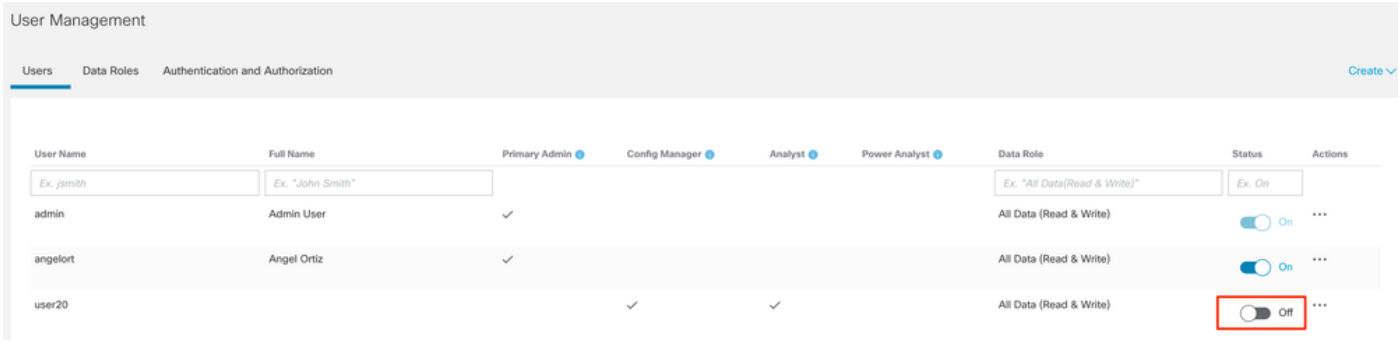
사용자가 로컬로 정의되고 활성화된 경우(Manager에서) 사용자는 원격으로 인증되지만 로컬로 인증됩니다. 사용자 선택 프로세스는 다음과 같습니다.

1. 관리자의 시작 페이지에 자격 증명이 입력되면 관리자는 지정된 이름의 로컬 사용자를 찾습니다.
2. 로컬 사용자가 발견되어 활성화되면 로컬 권한 부여를 통해 LDAP를 통한 원격 인증이 이전에 구성된 경우 원격으로 인증되지만 로컬 설정으로 인증됩니다.
3. 원격 권한 부여가 구성 및 활성화되고 사용자가 로컬에서(구성 또는 사용 안 함) 발견되지 않으면 인증 및 권한 부여가 모두 원격으로 수행됩니다.

따라서 원격 인증을 성공적으로 구성하는 단계는 다음과 같습니다.

### D-1단계. 원격 권한 부여를 사용하지만 로컬에서 정의된 사용자를 비활성화하거나 삭제합니다.

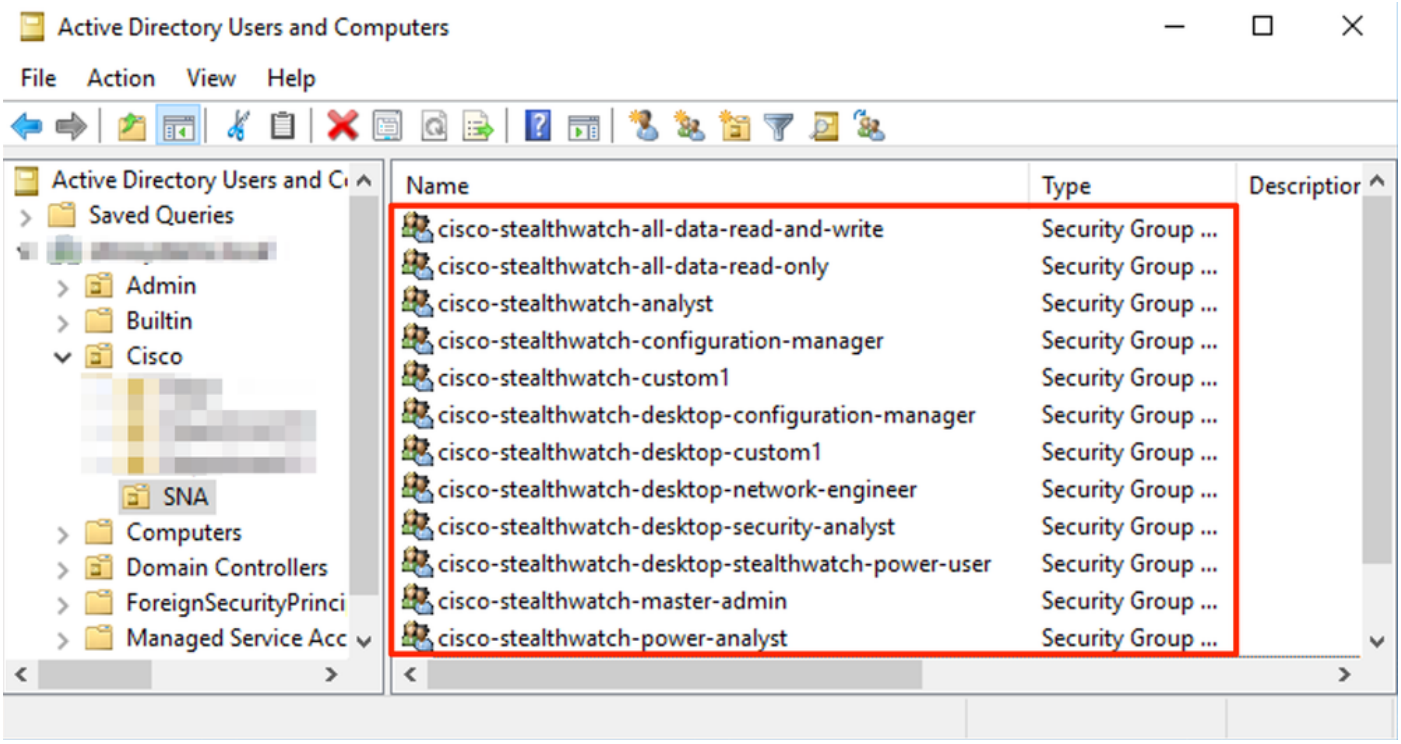
1. Manager 기본 대시보드를 열고 Global Settings(전역 설정) > User Management(사용자 관리)로 이동합니다.
2. LDAP를 통해 원격 인증 및 권한 부여를 사용하지만 로컬에서 구성하려는 사용자(있는 경우)를 비활성화 또는 삭제합니다.




**D-2단계. Microsoft AD 서버에서 cisco-stealthwatch 그룹을 정의합니다.**

LDAP 사용자를 통한 외부 인증 및 권한 부여의 경우 비밀번호 및 *cisco-stealthwatch* 그룹은 Microsoft Active Directory에서 원격으로 정의됩니다. AD 서버에 *정의할 cisco-stealthwatch* 그룹은 SNA가 가진 다양한 역할과 관련이 있으며 다음과 같이 정의해야 합니다.

| SNA 역할 | 그룹 이름 |
| --- | --- |
| 기본 관리자 | • cisco-stealthwatch-master-admin<br>• cisco stealthwatch-all-data-read-and-write<br>• cisco-stealthwatch-all-data-read-only<br>• cisco-stealthwatch-<custom>(선택 사항) |
| 데이터 역할 | **참고:** 사용자 지정 데이터 역할 그룹이 "cisco stealthwatch-"로 시작되는지 확인합니다. |
| 웹 기능 역할 | • cisco-stealthwatch-configuration manager<br>• cisco-stealthwatch-power-analyst<br>• cisco-stealthwatch 분석가<br>• cisco-stealthwatch-desktop-stealthwatch-pow user<br>• cisco-stealthwatch-desktop-configuration ma<br>• cisco-stealthwatch-desktop-network-enginee<br>• cisco-stealthwatch-desktop-security-analyst |
| 데스크톱 기능 역할 | • cisco-stealthwatch-desktop-<custom>(선택 사<br>**참고:** 맞춤형 데스크톱 기능 역할 그룹이 "cis stealthwatch-desktop-"으로 시작되는지 확인다. |

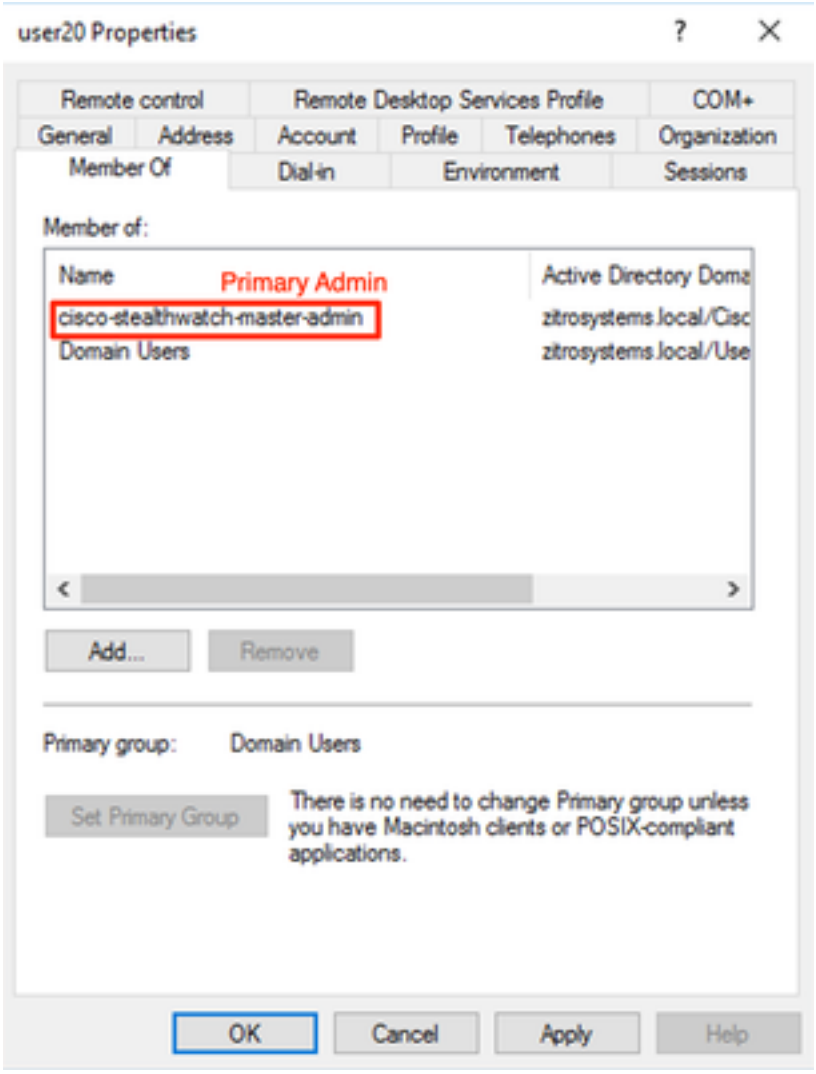



**참고:** 앞서 설명한 대로 그룹 이름 앞에 적절한 문자열이 붙은 경우 "데이터 역할" 및 "데스크톱 기능 역할"에 대해 사용자 지정 그룹이 지원됩니다. 이러한 사용자 지정 역할 및 그룹은 SNA Manager 및 Active Directory 서버 모두에서 정의되어야 합니다. 예를 들어 데스크톱 클라이언트 역할에 대해 SNA Manager에서 사용자 지정 역할 "custom1"을 정의하는 경우 Active Directory의 cisco-stealthwatch-desktop-custom1에 매핑되어야 합니다.

### D-3단계. 사용자에 대한 LDAP 권한 부여 그룹 매핑을 정의합니다.

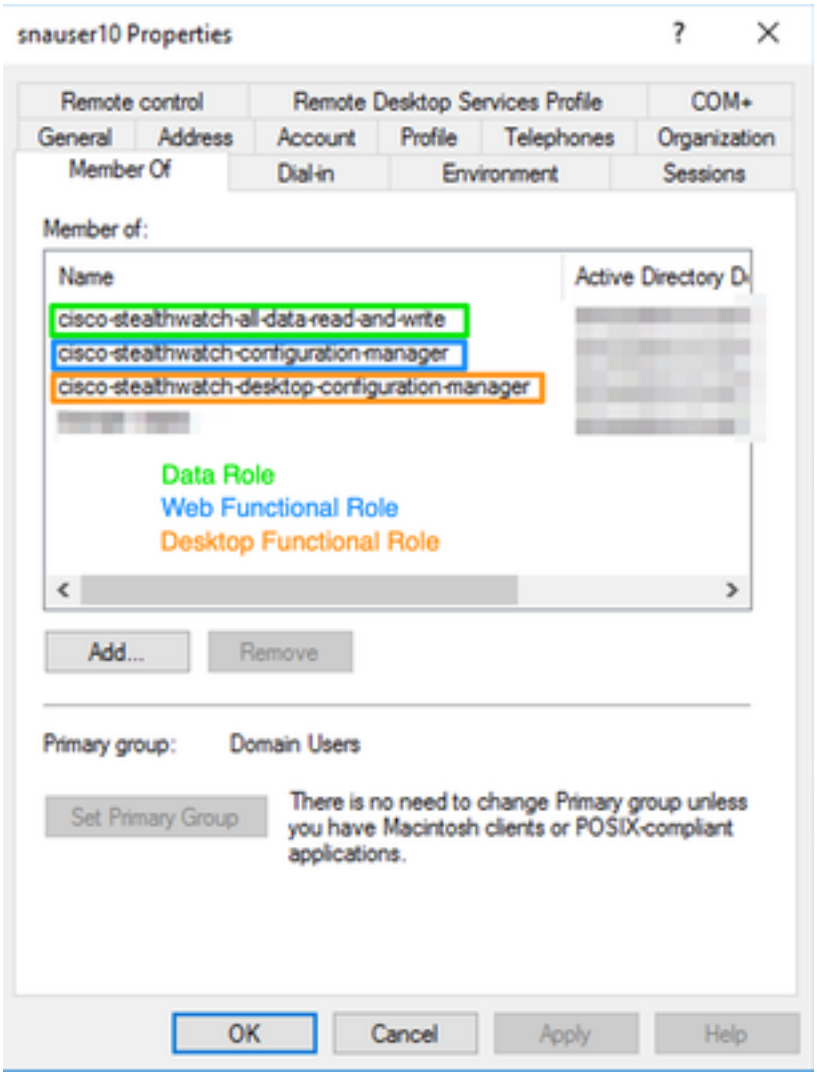
*cisco*-stealthwatch 그룹이 AD 서버에 정의되면 SNA Manager에 액세스하려는 사용자를 필요한 그룹에 매핑할 수 있습니다. 이 작업은 다음과 같이 수행해야 합니다.

- 기본 **관리자** 사용자**는** *cisco-stealthwatch-master-admin* 그룹에 할당되어야 하며 **다른** *cisco-stealthwatch* 그룹**의 구성원이 아니어야 합니다**.




- 기본 관리자 사용자를 제외한 각 사용자는 다음 조건을 가진 각 역할의 그룹에 할당되어야 합니다.

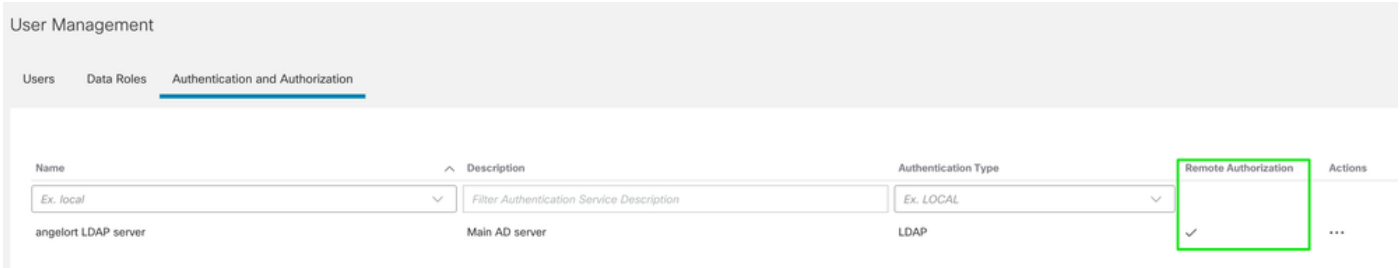
1. **데이터 역할**: 사용자는 **하나의 그룹에만 할당되어야** 합니다.
2. **웹 기능 역할**: 사용자를 **하나 이상의 그룹**에 할당해야 합니다.
3. **데스크톱 기능 역할**: 사용자를 **하나 이상의 그룹**에 할당해야 합니다.




**D-4단계. SNA Manager에서 LDAP를 통한 원격 권한 부여를 활성화합니다.**

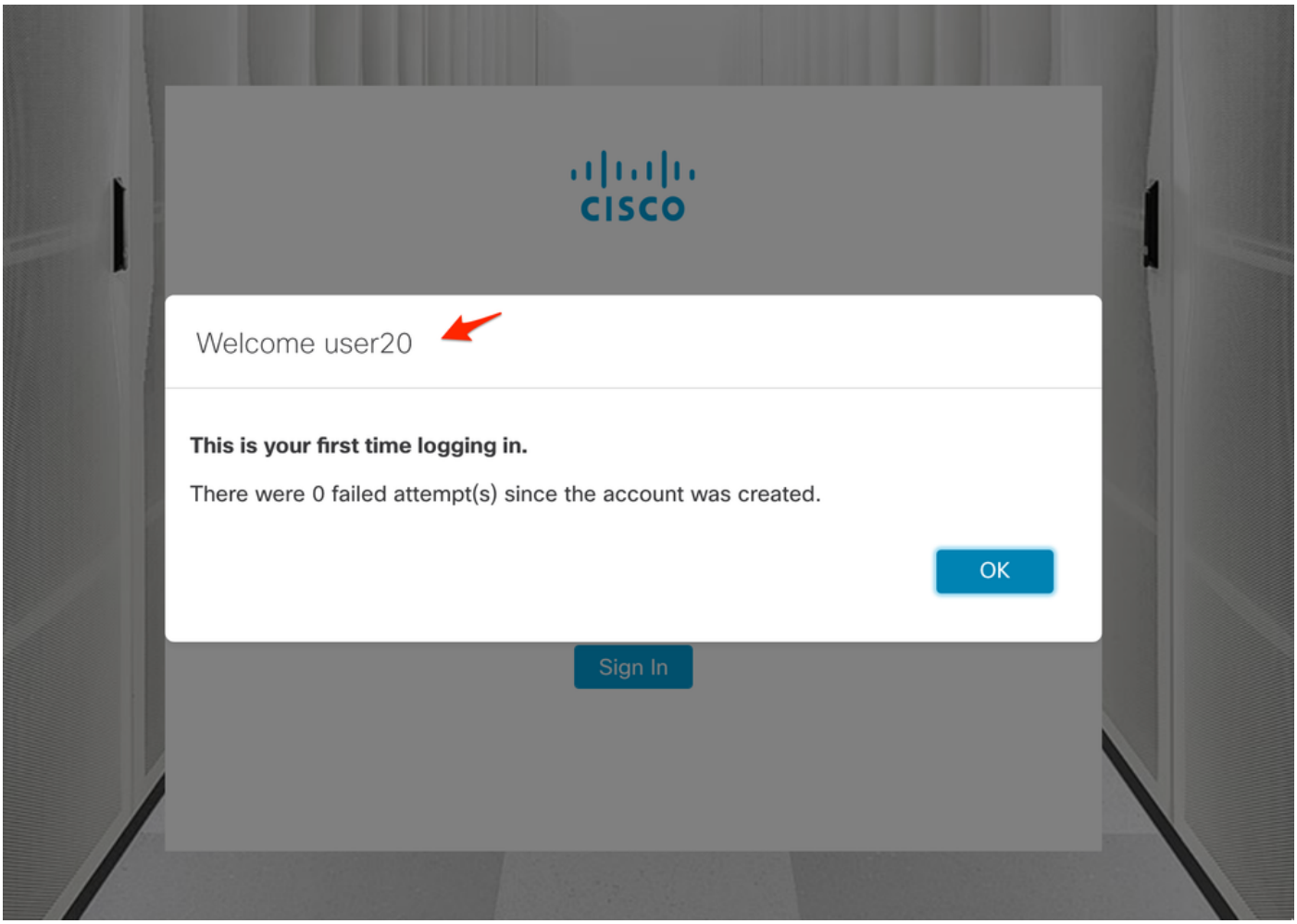
1. Manager 기본 대시보드를 열고 Global Settings(전역 설정) > **User Management(사용자 관리)로 이동합니다**.
2. User **Management** 창에서 **Authentication and Authorization** 탭을 선택합니다.
3. **C단계**에서 구성된 LDAP 인증 서비스를 **찾습니다**.
4. Actions(작업) > Enable **Remote Authorization(원격 권한 부여 활성화)을 클릭합니다**.

**참고: 한 번에 하나의 외부 권한 부여 서비스만 사용할 수 있습니다.** 다른 권한 부여 서비스가 이미 사용 중인 경우 자동으로 비활성화되고 새 서비스가 활성화되지만 이전 외부 서비스로 권한을 부여받은 모든 사용자가 로그아웃됩니다. 작업이 수행되기 전에 확인 메시지가 표시됩니다.

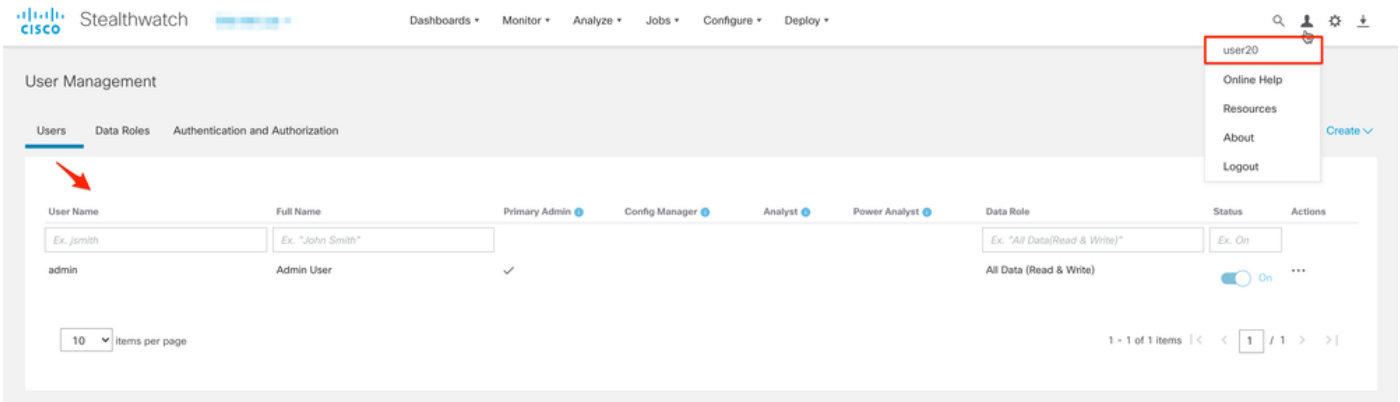



# 다음을 확인합니다.

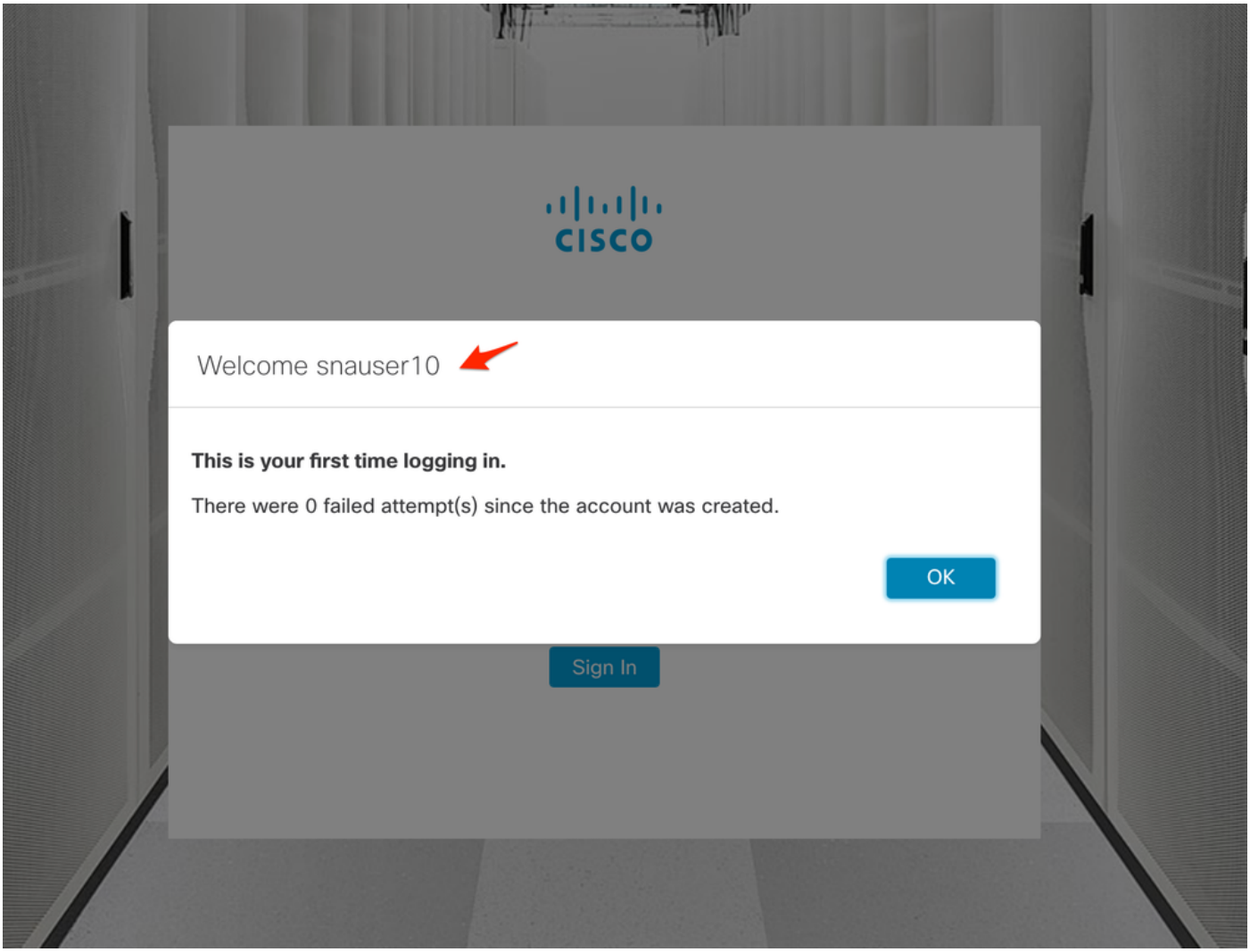
사용자는 AD 서버에 정의된 자격 증명으로 로그인할 수 있습니다.



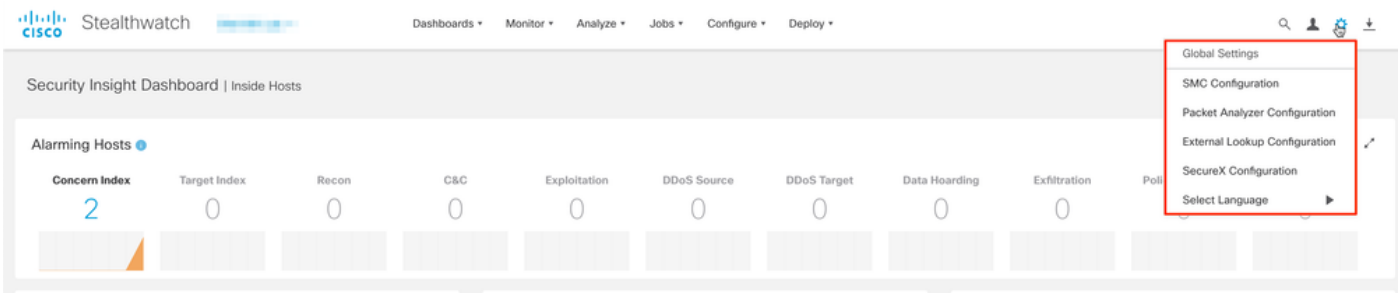

두 번째 확인 단계는 권한 부여와 관련된 것입니다. 이 예에서 사용자 "user20"은 AD 서버에서 *cisco-stealthwatch-master-admin* 그룹의 멤버가 되었으며 사용자에게 기본 관리자 권한이 있는지 확인할 수 있습니다. 사용자가 로컬 사용자에 정의되어 있지 않으므로 AD 서버에서 권한 부여 특성을 전송했는지 확인할 수 있습니다.




이 예에서 다른 사용자도 동일한 확인을 수행합니다. AD 서버에 구성된 자격 증명으로 성공적인 인증을 확인할 수 있습니다.




권한 부여 확인을 위해 이 사용자는 기본 관리 그룹에 속하지 않으므로 일부 기능을 사용할 수 없습니다.




# 문제 해결

인증 서비스의 컨피그레이션을 저장할 수 없는 경우 다음을 확인합니다.

1. LDAP 서버의 올바른 인증서를 관리자의 트러스트 저장소에 추가했습니다.
2. 구성된 **서버 주소**는 LDAP 서버 인증서의 SAN(Subject Alternative Name) 필드에 지정됩니다. SAN 필드에 IPv4 주소만 포함된 경우 Server Address 필드에 IPv4 주소를 입력합니다.SAN 필드에 DNS 이름이 포함된 경우 Server Address 필드에 DNS 이름을 입력합니다.SAN 필드에 DNS 값과 IPv4 값이 모두 포함되어 있으면 나열된 첫 번째 값을 사용합니다.
3. 구성된 **Bind User** 및 **Base Account** 필드가 AD 도메인 컨트롤러에서 지정한 대로 올바릅니다.

# 관련 정보

추가 지원이 필요한 경우 Cisco Technical Assistance Center(TAC)에 문의하십시오. 유효한 지원 계약이 필요합니다. Cisco 전 세계 지원 문의처.