

# ISE GUI 및 CLI용 AD 통합 로그인

## 목차

---

### [소개](#)

### [사전 요구 사항](#)

#### [요구 사항](#)

#### [사용되는 구성 요소](#)

### [구성](#)

#### [ISE를 AD에 가입](#)

#### [디렉터리 그룹 선택](#)

#### [AD에 대한 관리 액세스 사용](#)

#### [AD 그룹에 대한 관리 그룹 매핑 구성](#)

#### [관리자 그룹에 대한 RBAC 권한 설정](#)

#### [AD 자격 증명을 사용한 ISE GUI 액세스](#)

#### [AD 자격 증명을 사용한 ISE CLI 액세스](#)

#### [ISE CLI](#)

### [다음을 확인합니다.](#)

### [문제 해결](#)

#### [참가 문제](#)

##### [작업 시나리오](#)

##### [비작업 시나리오](#)

#### [로그인 문제](#)

---

## 소개

이 문서에서는 Microsoft AD를 Cisco ISE 관리 GUI 및 CLI에 대한 관리 액세스를 위한 외부 ID 저장소로 구성하는 방법을 설명합니다.

## 사전 요구 사항

### 요구 사항

Cisco에서는 다음 항목에 대한 지식을 권장합니다.

- Cisco ISE 버전 3.0 컨피그레이션
- Microsoft AD

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ISE 버전 3.0

- Windows Server 2016

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


## 구성

Microsoft AD를 Cisco ISE 관리 GUI에 대한 관리 액세스를 위한 외부 ID 저장소로 사용하도록 구성하려면 이 섹션을 사용합니다.

이러한 포트는 ISE 노드와 AD 간에 이 통신에 사용됩니다.

Service	Port	Protocol	Notes
DNS	53	UDP and TCP	
LDAP	389	UDP and TCP	
Kerberos	88	UDP and TCP	
Kerberos	464	UDP and TCP	Used by kadmin for setting and changing a password
LDAP Global Catalog	3268	TCP	If the <code>id_provider = ad</code> option is being used
NTP	123	UDP	Optional

---

 주: AD 계정에 모든 필수 권한이 있는지 확인합니다.

---

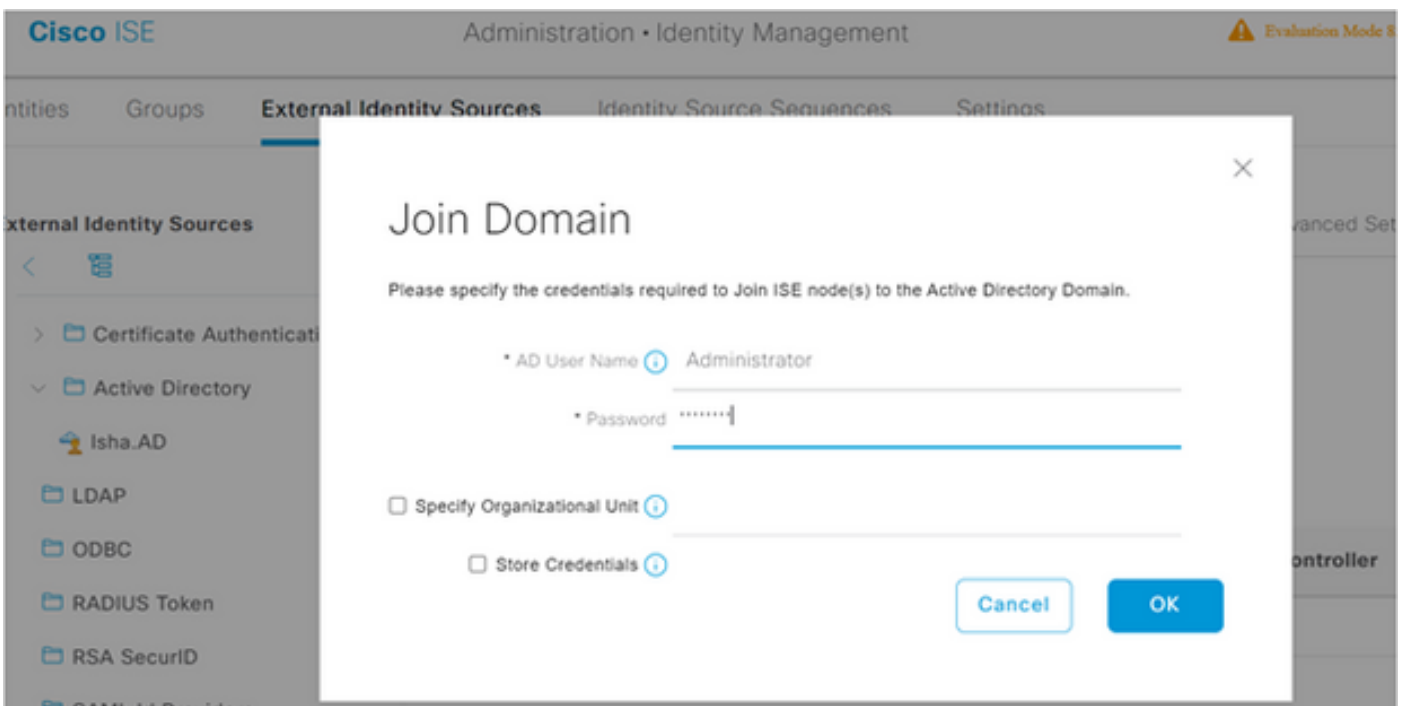
## Active Directory Account Permissions Required for Performing Various Operations

Join Operations	Leave Operations	Cisco ISE Machine Accounts
<p>For the account that is used to perform the join operation, the following permissions are required:</p> <ul style="list-style-type: none"> <li>• Search Active Directory (to see if a Cisco ISE machine account already exists)</li> <li>• Create Cisco ISE machine account to domain (if the machine account does not already exist)</li> <li>• Set attributes on the new machine account (for example, Cisco ISE machine account password, SPN, dnsHostname)</li> </ul> <p>It is not mandatory to be a domain administrator to perform a join operation.</p>	<p>For the account that is used to perform the leave operation, the following permissions are required:</p> <ul style="list-style-type: none"> <li>• Search Active Directory (to see if a Cisco ISE machine account already exists)</li> <li>• Remove Cisco ISE machine account from domain</li> </ul> <p>If you perform a force leave (leave without the password), it will not remove the machine account from the domain.</p>	<p>For the newly created Cisco ISE machine account that is used to communicate to the Active Directory connection, the following permissions are required:</p> <ul style="list-style-type: none"> <li>• Ability to change own password</li> <li>• Read the user/machine objects corresponding to users/machines being authenticated</li> <li>• Query some parts of the Active Directory to learn about required information (for example, trusted domains, alternative UPN suffixes and so on.)</li> <li>• Ability to read tokenGroups attribute</li> </ul> <p>You can precreate the machine account in Active Directory, and if the SAM name matches the Cisco ISE appliance hostname, it should be located during the join operation and re-used.</p> <p>If multiple join operations are performed, multiple machine accounts are maintained inside Cisco ISE, one for each join.</p>

## ISE를 AD에 가입

### 1. 탐색 Administration > Identity Management > External Identity Sources > Active Directory.

- 새 조인 지점 이름 및 AD 도메인을 입력합니다.
- 컴퓨터 개체를 추가하고 변경할 수 있는 AD 계정의 자격 증명을 입력하고 [확인]을 클릭합니다.



# Join Operation Status

Status Summary: Successful

ISE Node	Node Status
ise30-1.lsha.global	✔ Completed.

Close

## 디렉터리 그룹 선택

- 탐색 **Administration > Identity Management > External Identity Sources > Active Directory > Groups > Add > Select groups form Directory.**
- 관리자가 속한 하나 이상의 AD 그룹을 가져옵니다.

The screenshot shows the 'External Identity Sources' configuration page. The 'Groups' tab is selected, displaying a table of groups. The table has columns for 'Name' and 'SID'. One group is listed: 'Isha.global/Users/Domain Users' with the SID 'S-1-5-21-3870878658-245908420-3798545353-513'. The page includes navigation tabs for 'Identities', 'Groups', 'External Identity Sources', 'Identity Source Sequences', and 'Settings'. On the left, there is a sidebar with 'External Identity Sources' and a tree view showing 'Certificate Authentication F' and 'Active Directory' with 'Isha.AD' selected.

## AD에 대한 관리 액세스 사용

AD에 대해 비밀번호 기반 인증을 활성화하려면 다음 단계를 완료하십시오.

- 탐색 **Administration > System > Admin Access > Authentication.**
- 탭에서 **Authentication Method** 옵션을 **Password Based** 선택합니다.

### Identity Source

- 드롭다운 목록에서 AD를 선택합니다.
- 클릭 **Save Changes**.

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks

**Authentication**

Authentication Method Password Policy Account Disable Policy Lock/Susp

Authentication Type

Password Based

\* Identity Source

AD:Isha.AD

Client Certificate Based

### AD 그룹에 대한 관리 그룹 매핑 구성

Cisco ISE를 정의 Admin Group 하고 AD 그룹에 매핑 합니다. 이렇게 하면 권한 부여가 AD의 그룹 Role Based Access Control (RBAC) 멤버십을 기반으로 관리자에 대한 권한을 결정할 수 있습니다.

- 탐색 **Administration > System > Admin Access > Administrators > Admin Groups**.
- 새 구성 창 **Add** 을 보려면 표 헤더를 Admin Group 클릭합니다.
- 새 관리자 그룹의 이름을 입력합니다.
- 필드에서 Type 확인란을 **External** 선택합니다.
- 섹션에 정의된 대로 **External Groups** 드롭다운 목록에서 이 관리 그룹을 매핑할 AD 그룹을 Select Directory Groups 선택 합니다.
- 클릭 **Save Changes**.

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore **Admin Access**

Authentication

Authorization >

Administrators >

Admin Users

**Admin Groups**

Settings >

Admin Groups > New Admin Group

### Admin Group

\* Name ISE\_Admin

Description

Type  External

External Identity Source  
Name : Isha.AD


External Groups

Isha.global/Users/Domain User +

### 관리자 그룹에 대한 RBAC 권한 설정

이전 섹션에서 생성된 관리 그룹에 RBAC 권한을 할당하려면 다음 단계를 완료하십시오.

- 탐색 **Administration > System > Admin Access > Authorization > Policy**.
- 오른쪽의 Actions 드롭다운 목록에서 새 정책 **Insert New Policy** 을 추가하도록 선택합니다.
- Map it with the Admin Group defined in AD\_Administrator. the Enable Administrative Access for AD(AD용) 섹션에 정의된 Admin Group(관리자 그룹으로 매핑)이라는 새 규칙을 생성하고 권한을 할당합니다.

 **참고:** 이 예에서는 Super Admin이라는 관리자 그룹이 할당됩니다. 이는 표준 관리자 계정과 동일합니다.

- Confirmation **Save Changes**. 을 클릭하면 저장된 변경 사항이 GUI의 오른쪽 아래 모서리에 표시됩니다.

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore **Admin Access** Se

Policy Name	Condition	Action
ERS Trustsec Policy	If ERS Trustsec	Super Admin Data Access
Helpdesk Admin Policy	If Helpdesk Admin	Helpdesk Admin Menu Access
Identity Admin Policy	If Identity Admin	Identity Admin Menu Access...
MnT Admin Policy	If MnT Admin	MnT Admin Menu Access
AD_Administrator	If ISE_Admin	Helpdesk Admin Menu Ace...
Network Device Policy	If Network Device Admin	Super Admin Menu Access
Policy Admin Policy	If Policy Admin	Super Admin Data Access
RBAC Admin Policy	If RBAC Admin	

### AD 자격 증명을 사용한 ISE GUI 액세스


AD 자격 증명으로 ISE GUI에 액세스하려면 다음 단계를 완료하십시오.

- 관리 GUI에서 로그아웃합니다.

Identity Source

- 드롭다운 목록에서 AD를 선택합니다.

- AD 데이터베이스에서 사용자 이름과 비밀번호를 입력하고 로그인합니다.

 **참고:** AD에 연결할 수 없거나 사용된 계정 자격 증명이 AD에 없는 경우 ISE는 기본적으로 내부 사용자 저장소로 설정됩니다. 이렇게 하면 AD가 관리 액세스에 대해 구성된 상태에서 내부 저장소를 사용하는 경우 빠른 로그인이 용이합니다.





# Server Information

Username: **ad\_admin**

Host: **ise30-1**

Personas: **Administration, Monitoring, Policy  
Service (SESSION,PROFILER)**

Role: **STANDALONE**

System Time: **May 08 2021 10:13:22 PM  
Asia/Kolkata**

FIPS Mode: **Disabled**

Version: **3.0.0.458**

Patch Information: **none**

OK

AD 자격 증명을 사용한 ISE CLI 액세스

외부 ID 소스와의 인증은 내부 데이터베이스보다 안전합니다. 의 RBAC는 외부 ID 저장소를 CLI Administrators 지원합니다.



**참고:** ISE 버전 2.6 이상 릴리스는 CLI 로그인을 위한 외부 ID 소스로 AD만 지원합니다.

여러 비밀번호 정책을 관리하고 ISE 내에서 내부 사용자를 관리할 필요 없이 비밀번호에 대한 단일 소스를 관리하여 시간과 노력을 줄일 수 있습니다.

사전 요구 사항

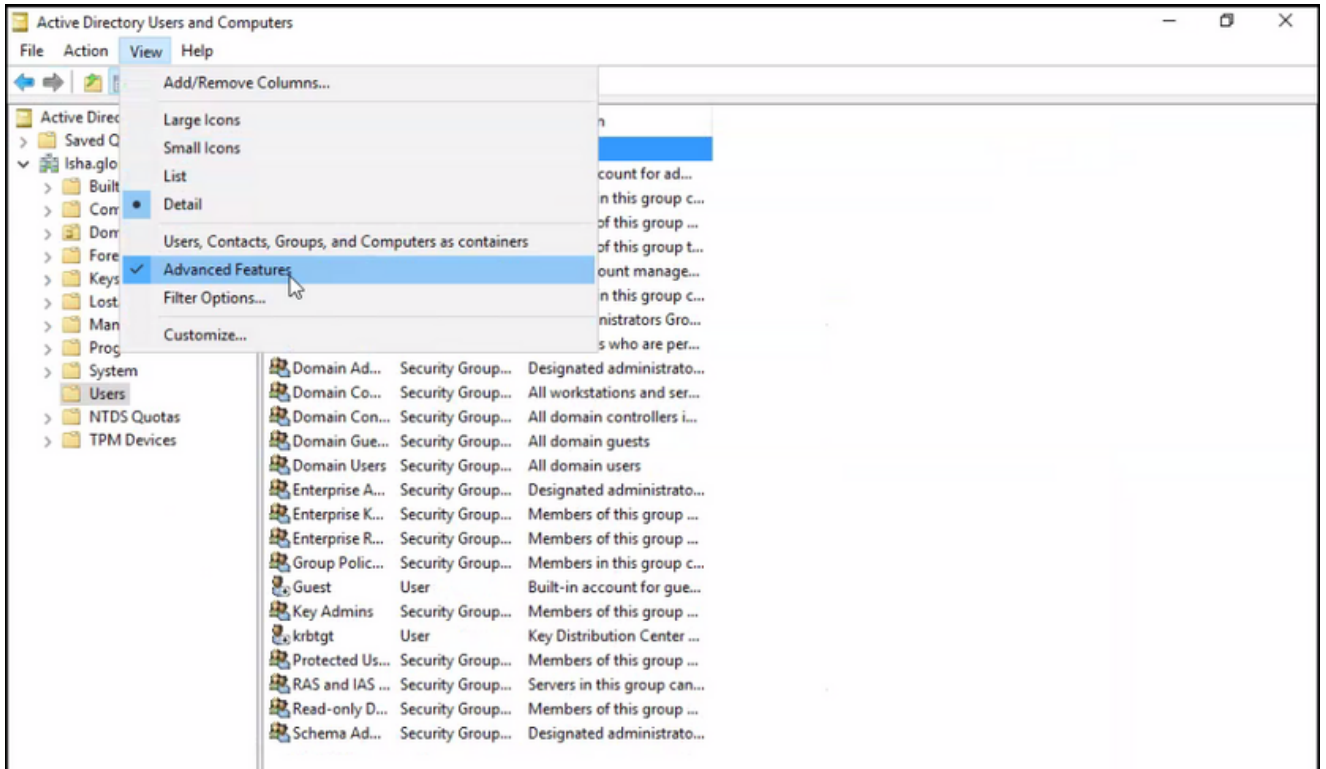


Admin 사용자를 정의하여 Administrator 그룹에 추가해야 합니다. 관리자는 Super Admin.

정의the User's Attributes in the AD User Directory.

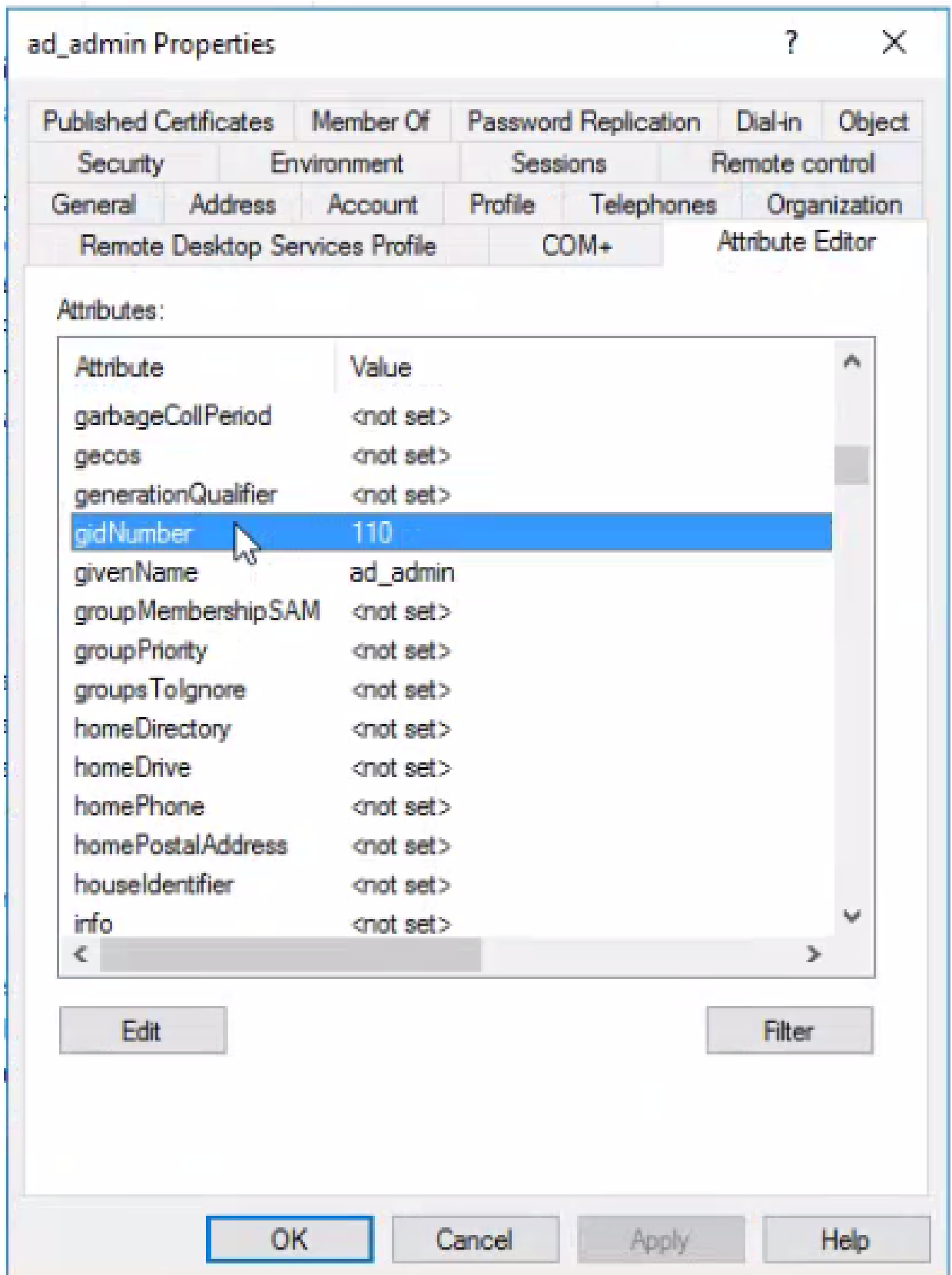
를 실행하는 Windows 서버에서 Active Directory, CLI 관리자로 구성하려는 각 사용자의 특성을 수정합니다.

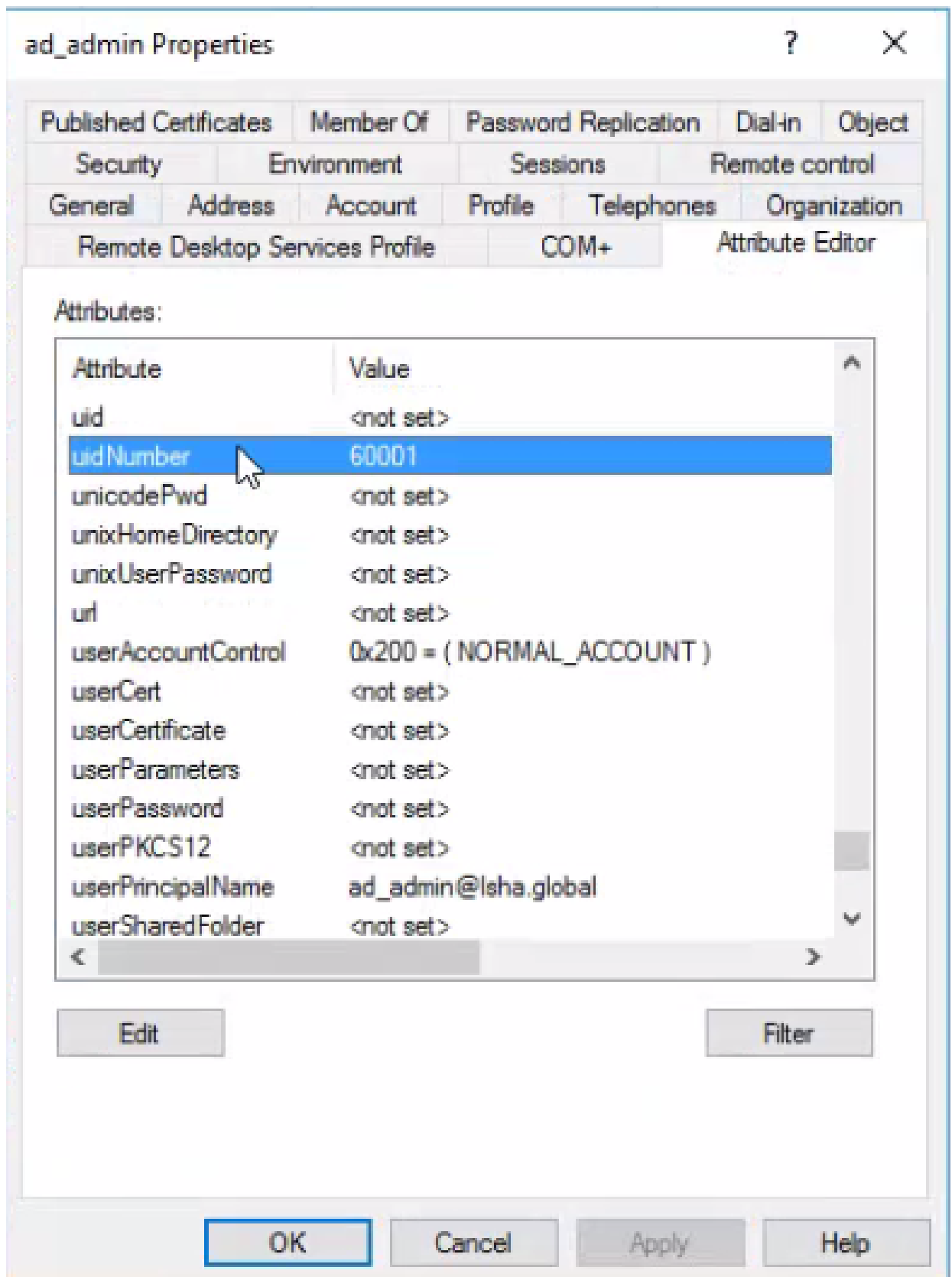
- 를 열고 다음 **Server Manager Window**, 으로 이동합니다. **Server Manager > Roles > Active Directory Domain Services > Active Directory Users and Computers > [ ad.adserver ] <ad\_server>.local**.
- 사용자 **Advanced Features** 의 속성을 편집할 수 있도록 보기 메뉴에서 을 활성화합니다.



- Admin 사용자가 포함된 AD 그룹으로 이동하여 해당 사용자를 찾습니다.
- 사용자를 두 번 클릭하여 창을 Properties 열고 를 **Attribute Editor** 선택합니다.
- 특성을 클릭하고 **gid** 을 입력하여 특성을 찾습니다 **gidNumber** . 특성을 찾을 수 없으면 gidNumber 단추를 클릭하고 **Filter** 선택을 취소합니다.  
값이 있는 특성만 표시합니다.
- 각 특성을 편집하려면 특성 이름을 두 번 클릭합니다. 각 사용자의 경우:
  - 60000 **uidNumber** 보다 큰 값을 할당하고 번호가 고유한지 확인합니다.
  - 110 또 **gidNumber** 는 111로 할당합니다.

- GidNumber 110은 관리자 사용자를 나타내고, 111은 읽기 전용 사용자를 나타냅니다.
- 할당 후에는 **uidNumber** 변경하지 마십시오.
- 를 수정하는 **gidNumber** 경우 SSH 연결을 설정하기 전에 최소 5분 정도 기다립니다.





Admin CLI 사용자를 AD 도메인에 가입

Cisco ISE CLI에 연결하고 명령을 **identity-store** 실행한 다음 Admin 사용자를 ID 저장소에 할당합니다.

예를 들어 CLI 관리자 사용자를 ISE에 isha.global로 정의된 Active Directory에 매핑하려면 다음 명령을 실행합니다.

```
identity-store active-directory domain-name <Domain name> user <AD join username>
```

가입이 완료되면 Cisco ISE CLI에 연결하고 관리자 CLI 사용자로 로그인하여 컨피그레이션을 확인합니다.

이 명령에서 사용하는 도메인이 이전에 ISE 노드에 조인된 경우 Administrators 콘솔에서 도메인에 다시 조인합니다.

- Cisco ISE GUI에서 아이콘을 **Menu** 클릭하고 다음으로 이동합니다. **Administration > Identity Management > External Identity Sources**.
- 왼쪽 창에서 AD 이름 **Active Directory** 을 선택하고 선택합니다.
- MS-RPC 또는 Kerberos를 사용하여 테스트 사용자와의 연결을 테스트할 경우 오른쪽 창에서 AD 연결의 상태가 There Operational. is errors(오류가 있음)로 표시될 수 있습니다.
- Cisco ISE CLI에 관리자 CLI 사용자로 계속 로그인할 수 있는지 확인합니다.

#### ISE CLI

- ISE CLI에 로그인합니다.

```
<#root>
```

```
ise30-1/admin#
```

```
configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.  
ise30-1/admin(config)#
```

- 노드를 도메인에 조인합니다.

```
ise30-1/admin(config)# identity-store active-directory domain-name isha.global user Administrator
```

도메인이 UI를 통해 이미 isha.global 조인된 경우 이 컨피그레이션 후 UI **isha.global** 에서 도메인을 다시 조인해야 합니다. 재 가입이 발생할 때까지 인증에 isha.global 실패합니다.

```
Do you want to proceed? Y/N: Y
```

```
Password for Administrator:
```

도메인 isha.global에 가입했습니다.



#### 참고:

- 도메인이 GUI를 통해 이미 조인된 경우 GUI에서 노드를 다시 조인합니다. 그렇지 않으면 AD에 대한 인증이 계속 실패합니다.
- 모든 노드는 CLI를 통해 개별적으로 연결해야 합니다.

## 다음을 확인합니다.

현재 이 설정에 사용 가능한 확인 절차는 없습니다.

## 문제 해결

### 참가 문제

조인 작업 중 발생한 문제와 이와 관련된 로그는 `/var/log/messages` 파일에서 확인할 수 있습니다.

명령을 사용합니다: **show logging system messages**

### 작업 시나리오

```
2021-07-19T21:15:01.457723+05:30 ise30-1 dbus[9675]: [system] Activating via systemd: service name='org.freedesktop.realmd'
unit='realmd.service'
2021-07-19T21:15:01.462981+05:30 ise30-1 systemd: Starting Realm and Domain Configuration...
2021-07-19T21:15:01.500846+05:30 ise30-1 dbus[9675]: [system] Successfully activated service 'org.freedesktop.realmd'
2021-07-19T21:15:01.501045+05:30 ise30-1 systemd: Started Realm and Domain Configuration.
2021-07-19T21:15:01.541478+05:30 ise30-1 realmd: * Resolving: _ldap._tcp.isha.global
2021-07-19T21:15:01.544480+05:30 ise30-1 realmd: * Performing LDAP DSE lookup on: 10.127.197.115
2021-07-19T21:15:01.546254+05:30 ise30-1 realmd: * Performing LDAP DSE lookup on: 10.127.197.236
2021-07-19T21:15:01.546777+05:30 ise30-1 realmd: * Successfully discovered: Isha.global
2021-07-19T21:15:09.282364+05:30 ise30-1 realmd: * Required files: /usr/sbin/odjjobd, /usr/libexec/odjjob/mkhomedir,
/usr/sbin/sss, /usr/bin/
2021-07-19T21:15:09.282708+05:30 ise30-1 realmd: * LANG=C LOGNAME=root /usr/bin/net -s /var/cache/realmd/realmd-smb-
conf.MU0M60 -U Administrator ads join Isha.global
2021-07-19T21:15:12.701071+05:30 ise30-1 realmd: Enter Administrator's password:DNS update failed:
NT_STATUS_INVALID_PARAMETER
2021-07-19T21:15:12.705753+05:30 ise30-1 realmd:
2021-07-19T21:15:12.706142+05:30 ise30-1 realmd: Use short domain name -- ISHA
2021-07-19T21:15:12.706580+05:30 ise30-1 realmd: Joined 'ISE30-1' to dns domain 'Isha.global'
2021-07-19T21:15:12.708781+05:30 ise30-1 realmd: * LANG=C LOGNAME=root /usr/bin/net -s /var/cache/realmd/realmd-smb-
conf.MU0M60 -U Administrator ads keytab create
2021-07-19T21:15:13.786749+05:30 ise30-1 realmd: Enter Administrator's password:
2021-07-19T21:15:13.859916+05:30 ise30-1 realmd: * /usr/bin/systemctl enable sssd.service
2021-07-19T21:15:13.870511+05:30 ise30-1 systemd: Reloading.
2021-07-19T21:15:13.870724+05:30 ise30-1 realmd: Created symlink from /etc/systemd/system/multi-user.target.wants/sss.service to
/usr/lib/systemd/system/sss.service.
2021-07-19T21:15:13.943407+05:30 ise30-1 realmd: * /usr/bin/systemctl restart sssd.service
2021-07-19T21:15:13.956987+05:30 ise30-1 systemd: Starting System Security Services Daemon...
```

```
2021-07-19T21:15:14.240764+05:30 ise30-1 sssd: Starting up
2021-07-19T21:15:14.458345+05:30 ise30-1 sssd[be[Isha.global]]: Starting up
2021-07-19T21:15:15.180211+05:30 ise30-1 sssd[nss]: Starting up
2021-07-19T21:15:15.208949+05:30 ise30-1 sssd[pam]: Starting up
2021-07-19T21:15:15.316360+05:30 ise30-1 systemd: Started System Security Services Daemon.
2021-07-19T21:15:15.317846+05:30 ise30-1 realm: * /usr/bin/sh -c /usr/sbin/authconfig --update --enablesssd --enablesssdauth --enablemkhomedir --nostart && /usr/bin/systemctl enable oddjobd.service && /usr/bin/systemctl start oddjobd.service
2021-07-19T21:15:15.596220+05:30 ise30-1 systemd: Reloading.
2021-07-19T21:15:15.691786+05:30 ise30-1 systemd: Reloading.
2021-07-19T21:15:15.750889+05:30 ise30-1 realm: * Successfully enrolled machine in realm
```

## 비작업 시나리오

잘못된 암호로 인해 참가 실패:

```
2021-07-19T21:12:45.487538+05:30 ise30-1 dbus[9675]: [system] Activating via systemd: service name='org.freedesktop.realm' unit='realm.service'
2021-07-19T21:12:45.496066+05:30 ise30-1 systemd: Starting Realm and Domain Configuration...
2021-07-19T21:12:45.531667+05:30 ise30-1 dbus[9675]: [system] Successfully activated service 'org.freedesktop.realm'
2021-07-19T21:12:45.531950+05:30 ise30-1 systemd: Started Realm and Domain Configuration.
2021-07-19T21:12:45.567816+05:30 ise30-1 realm: * Resolving: _ldap._tcp.isha.global
2021-07-19T21:12:45.571092+05:30 ise30-1 realm: * Performing LDAP DSE lookup on: 10.127.197.115
2021-07-19T21:12:45.572854+05:30 ise30-1 realm: * Performing LDAP DSE lookup on: 10.127.197.236
2021-07-19T21:12:45.573376+05:30 ise30-1 realm: * Successfully discovered: Isha.global
2021-07-19T21:12:52.273667+05:30 ise30-1 realm: * Required files: /usr/sbin/oddjobd, /usr/libexec/oddjob/mkhomedir, /usr/sbin/sss, /usr/bin/net
2021-07-19T21:12:52.274730+05:30 ise30-1 realm: * LANG=C LOGNAME=root /usr/bin/net -s /var/cache/realm/realm-smb-conf.R0SM60 -U Administrator ads join Isha.global
2021-07-19T21:12:52.369726+05:30 ise30-1 realm: Enter Administrator's password:
2021-07-19T21:12:52.370190+05:30 ise30-1 realm: Failed to join domain: failed to lookup DC info for domain 'Isha.global' over rpc: The attempted logon is invalid. This is either due to a bad username or authentication information.
2021-07-19T21:12:52.372180+05:30 ise30-1 realm: ! Joining the domain Isha.global failed
```

## 로그인 문제

로그인 시 발생하는 문제 및 이와 관련된 로그는에서 확인할 수 있습니다. /var/log/secure.

명령을 사용합니다: show logging system secure

인증 성공:

```
2021-07-19T21:25:10.435849+05:30 ise30-1 sshd[119435]: pam_tally2(sshd:auth): unknown option: no_magic_root
2021-07-19T21:25:10.438694+05:30 ise30-1 sshd[119435]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.227.243.67 user=ad_admin
2021-07-19T21:25:11.365110+05:30 ise30-1 sshd[119435]: pam_sss(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.227.243.67 user=ad_admin
2021-07-19T21:25:11.365156+05:30 ise30-1 sshd[119435]: pam_sss(sshd:auth): received for user ad_admin: 12 (Authentication token is no longer valid; new one required)
2021-07-19T21:25:11.368231+05:30 ise30-1 sshd[119435]: pam_tally2(sshd:account): unknown option: reset
```

2021-07-19T21:25:11.370223+05:30 ise30-1 sshd[119435]: pam\_succeed\_if(sshd:account): 'uid' resolves to '60001'  
2021-07-19T21:25:11.370337+05:30 ise30-1 sshd[119435]: Accepted password for ad\_admin from 10.227.243.67 port 61613 ssh2  
2021-07-19T21:25:11.371478+05:30 ise30-1 sshd[119435]: pam\_tally2(sshd:setcred): unknown option: no\_magic\_root  
2021-07-19T21:25:11.781374+05:30 ise30-1 sshd[119435]: pam\_limits(sshd:session): reading settings from '/etc/security/limits.conf'  
2021-07-19T21:25:11.781445+05:30 ise30-1 sshd[119435]: pam\_limits(sshd:session): reading settings from '/etc/security/limits.d/20-nproc.conf'  
2021-07-19T21:25:11.781462+05:30 ise30-1 sshd[119435]: pam\_limits(sshd:session): process\_limit: processing soft nproc 4096 for DEFAULT  
2021-07-19T21:25:11.781592+05:30 ise30-1 sshd[119435]: pam\_unix(sshd:session): session opened for user ad\_admin by (uid=0)  
2021-07-19T21:25:11.784725+05:30 ise30-1 sshd[121474]: pam\_tally2(sshd:setcred): unknown option: no\_magic\_root

#### 잘못된 암호로 인한 인증 실패:

2021-07-19T21:25:10.435849+05:30 ise30-1 sshd[119435]: pam\_tally2(sshd:auth): unknown option: no\_magic\_root  
2021-07-19T21:25:10.438694+05:30 ise30-1 sshd[119435]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.227.243.67 user=ad\_admin  
2021-07-19T21:25:11.365110+05:30 ise30-1 sshd[119435]: pam\_sss(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.227.243.67 user=ad\_admin  
2021-07-19T21:25:11.365156+05:30 ise30-1 sshd[119435]: pam\_sss(sshd:auth): received for user ad\_admin: 12 (Authentication token is no longer valid; new one required)  
2021-07-19T21:25:11.368231+05:30 ise30-1 sshd[119435]: pam\_tally2(sshd:account): unknown option: reset  
2021-07-19T21:25:11.370223+05:30 ise30-1 sshd[119435]: pam\_succeed\_if(sshd:account): 'uid' resolves to '60001'  
2021-07-19T21:25:11.370337+05:30 ise30-1 sshd[119435]: Accepted password for ad\_admin from 10.227.243.67 port 61613 ssh2  
2021-07-19T21:25:11.371478+05:30 ise30-1 sshd[119435]: pam\_tally2(sshd:setcred): unknown option: no\_magic\_root  
2021-07-19T21:25:11.781374+05:30 ise30-1 sshd[119435]: pam\_limits(sshd:session): reading settings from '/etc/security/limits.conf'  
2021-07-19T21:25:11.781445+05:30 ise30-1 sshd[119435]: pam\_limits(sshd:session): reading settings from '/etc/security/limits.d/20-nproc.conf'  
2021-07-19T21:25:11.781462+05:30 ise30-1 sshd[119435]: pam\_limits(sshd:session): process\_limit: processing soft nproc 4096 for DEFAULT  
2021-07-19T21:25:11.781592+05:30 ise30-1 sshd[119435]: pam\_unix(sshd:session): session opened for user ad\_admin by (uid=0)  
2021-07-19T21:25:11.784725+05:30 ise30-1 sshd[121474]: pam\_tally2(sshd:setcred): unknown option: no\_magic\_root  
2021-07-19T21:25:56.737559+05:30 ise30-1 sshd[119435]: pam\_unix(sshd:session): session closed for user ad\_admin  
2021-07-19T21:25:56.738341+05:30 ise30-1 sshd[119435]: pam\_tally2(sshd:setcred): unknown option: no\_magic\_root  
2021-07-19T21:26:21.375211+05:30 ise30-1 sshd[122957]: pam\_tally2(sshd:auth): unknown option: no\_magic\_root  
2021-07-19T21:26:21.376387+05:30 ise30-1 sshd[122957]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.227.243.67 user=ad\_admin  
2021-07-19T21:26:21.434442+05:30 ise30-1 sshd[122957]: pam\_sss(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.227.243.67 user=ad\_admin  
2021-07-19T21:26:21.434461+05:30 ise30-1 sshd[122957]: pam\_sss(sshd:auth): received for user ad\_admin: 17 (Failure setting user credentials)  
2021-07-19T21:26:21.434480+05:30 ise30-1 sshd[122957]: pam\_nologin(sshd:auth): unknown option: debug  
2021-07-19T21:26:22.742663+05:30 ise30-1 sshd[122957]: Failed password for ad\_admin from 10.227.243.67 port 61675 ssh2

#### 유효하지 않은 사용자로 인한 인증 실패:

2021-07-19T21:28:08.756228+05:30 ise30-1 sshd[125725]: Invalid user Masked(xxxxx) from 10.227.243.67 port 61691  
2021-07-19T21:28:08.757646+05:30 ise30-1 sshd[125725]: input\_userauth\_request: invalid user Masked(xxxxx) [preauth]  
2021-07-19T21:28:15.628387+05:30 ise30-1 sshd[125725]: pam\_tally2(sshd:auth): unknown option: no\_magic\_root  
2021-07-19T21:28:15.628658+05:30 ise30-1 sshd[125725]: pam\_tally2(sshd:auth): pam\_get\_uid; no such user  
2021-07-19T21:28:15.628899+05:30 ise30-1 sshd[125725]: pam\_unix(sshd:auth): check pass; user unknown  
2021-07-19T21:28:15.629142+05:30 ise30-1 sshd[125725]: pam\_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.227.243.67  
2021-07-19T21:28:15.631975+05:30 ise30-1 sshd[125725]: pam\_sss(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.227.243.67 user=isha  
2021-07-19T21:28:15.631987+05:30 ise30-1 sshd[125725]: pam\_sss(sshd:auth): received for user isha: 10 (User not known to the

underlying authentication module)

2021-07-19T21:28:15.631993+05:30 ise30-1 sshd[125725]: pam\_nologin(sshd:auth): unknown option: debug

2021-07-19T21:28:17.256541+05:30 ise30-1 sshd[125725]: Failed password for invalid user Masked(xxxxx) from 10.227.243.67 port 61691 ssh2



이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.