Integrate AD for ISE GUI and CLI Log in

Contents

Introduction

This document describes configuration of Microsoft AD as external identity store for administrative access to the Cisco ISE management GUI and CLI.

Prerequisites

Requirements

Cisco recommends knowledge of these topics:

- Configuration of Cisco ISE Version 3.0
- Microsoft AD

Components Used

The information in this document is based on these software and hardware versions:

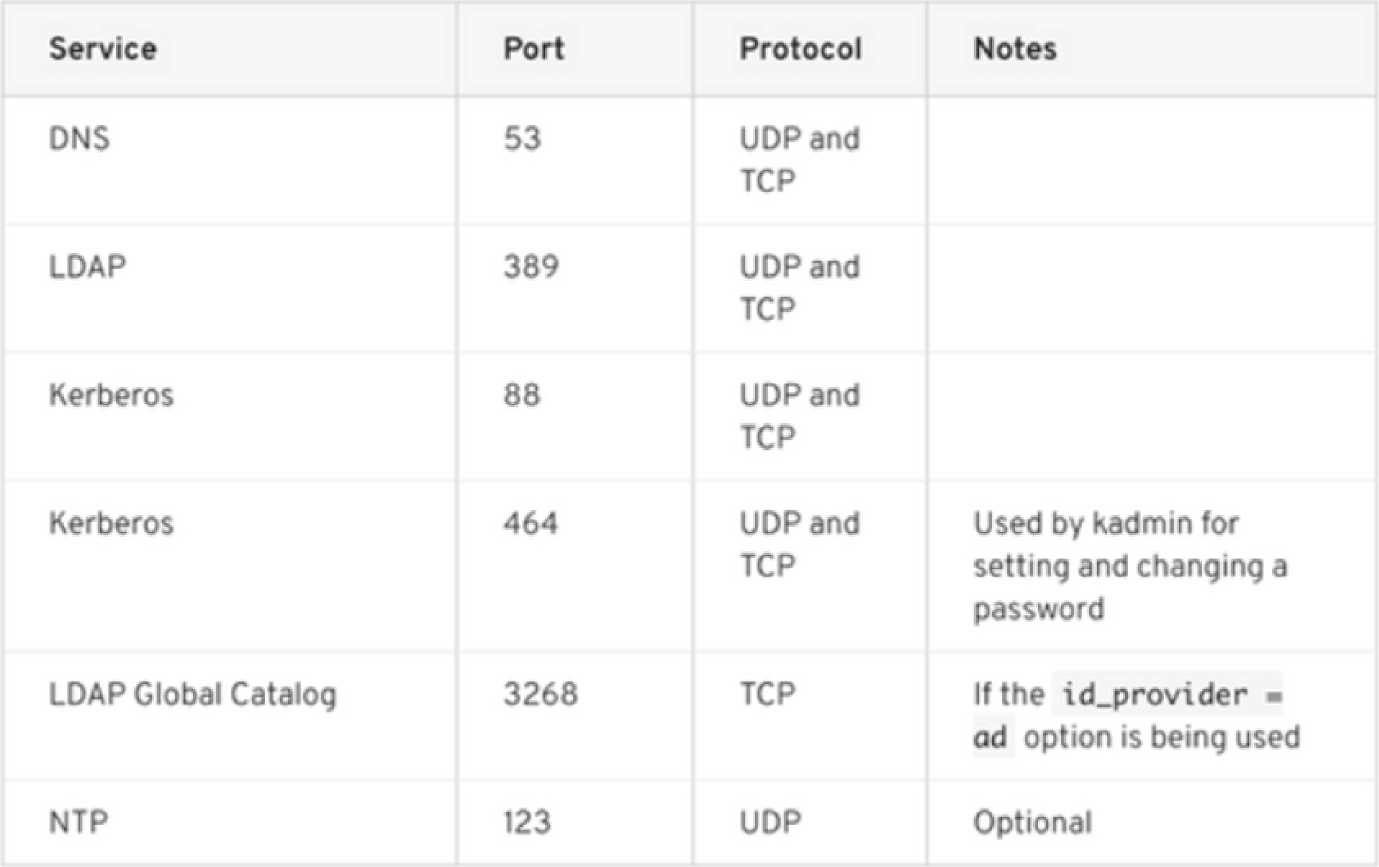
- Cisco ISE Version 3.0
- Windows Server 2016

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. If your network is live, ensure that you understand the potential impact of any command.

Configure

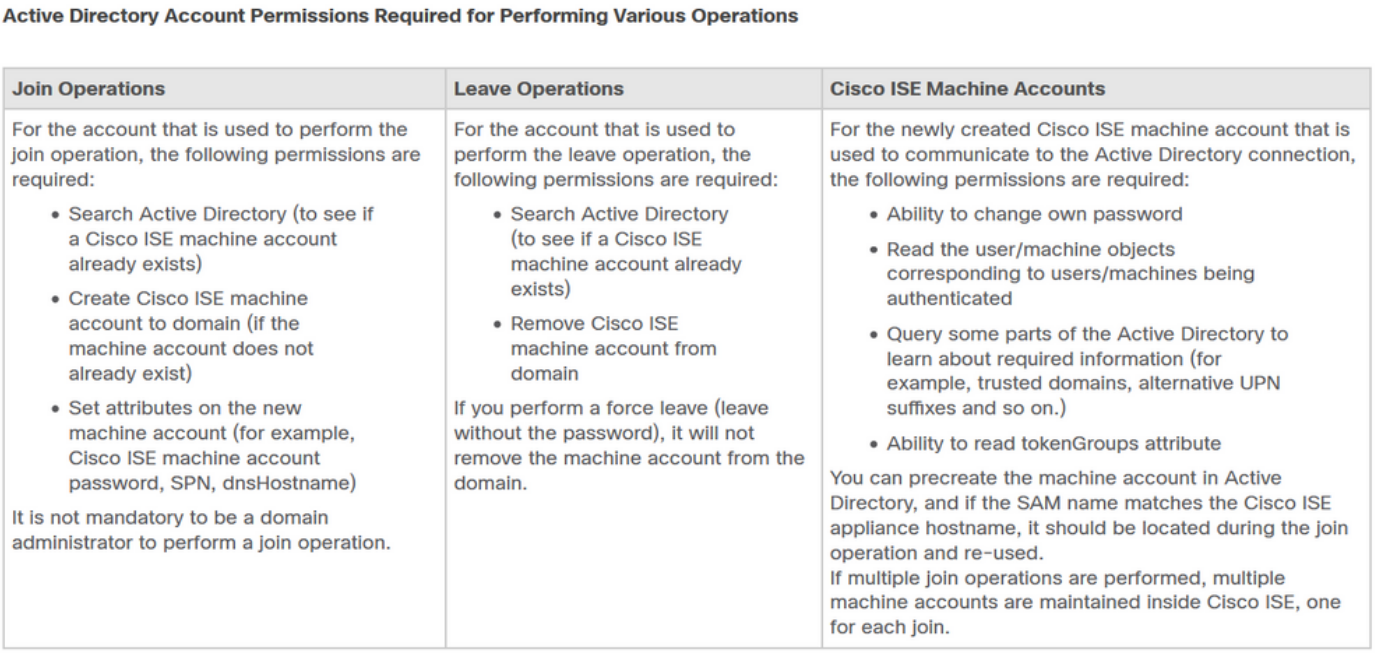
Use this section in order to configure the use of Microsoft AD as an external identity store for administrative access to the Cisco ISE management GUI.

These ports are used between ISE node and AD for this communication:



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 `id_provider = ad` option is being used
NTP	123	UDP	Optional

Note: Ensure the AD account has all the required privileges.

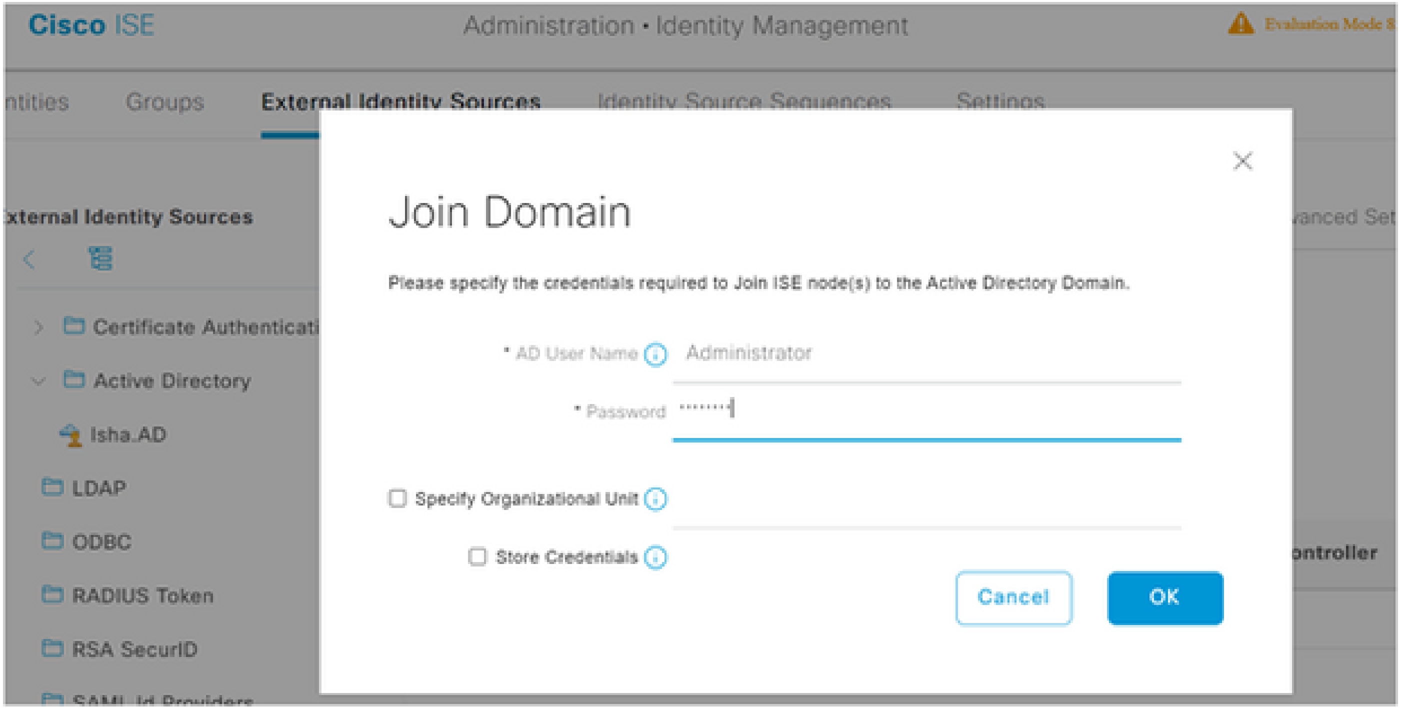


Active Directory Account Permissions Required for Performing Various Operations

Join Operations	Leave Operations	Cisco ISE Machine Accounts
For the account that is used to perform the join operation, the following permissions are required: • Search Active Directory (to see if a Cisco ISE machine account already exists) • Create Cisco ISE machine account to domain (if the machine account does not already exist) • Set attributes on the new machine account (for example, Cisco ISE machine account password, SPN, dnsHostname) It is not mandatory to be a domain administrator to perform a join operation.	For the account that is used to perform the leave operation, the following permissions are required: • Search Active Directory (to see if a Cisco ISE machine account already exists) • Remove Cisco ISE machine account from domain If you perform a force leave (leave without the password), it will not remove the machine account from the domain.	For the newly created Cisco ISE machine account that is used to communicate to the Active Directory connection, the following permissions are required: • Ability to change own password • Read the user/machine objects corresponding to users/machines being authenticated • Query some parts of the Active Directory to learn about required information (for example, trusted domains, alternative UPN suffixes and so on.) • Ability to read tokenGroups attribute 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. If multiple join operations are performed, multiple machine accounts are maintained inside Cisco ISE, one for each join.

Join ISE to AD

1. Navigate to **Administration** > **Identity Management** > **External Identity Sources** > **Active Directory**.
2. Enter the new join point name and the AD domain.
3. Enter the credentials of the AD account that can add and make changes to computer objects and click **OK**.



Join Domain

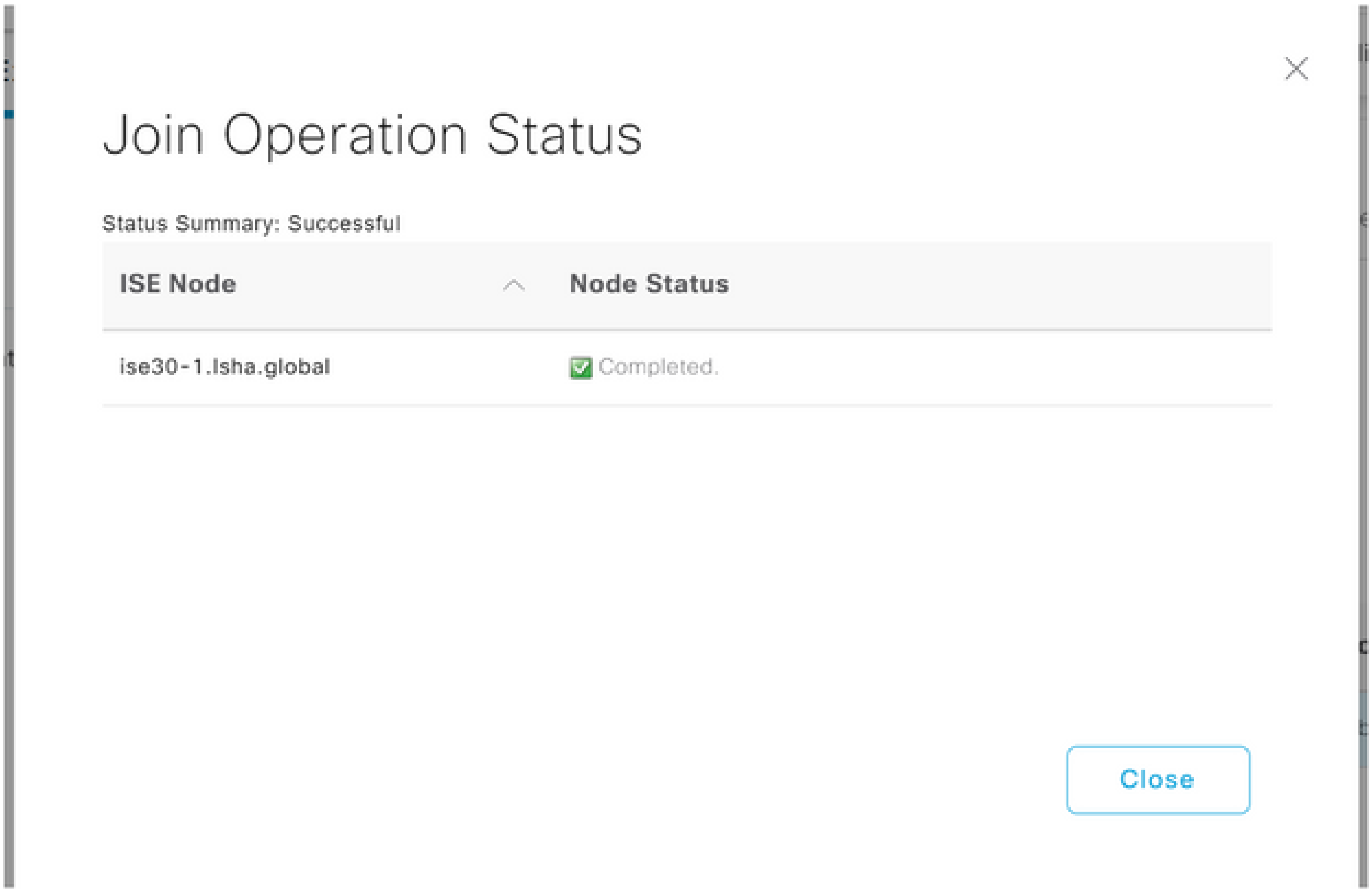
Please specify the credentials required to Join ISE node(s) to the Active Directory Domain.

* AD User Name: Administrator

* Password: ••••••••

□ Specify Organizational Unit

□ Store Credentials



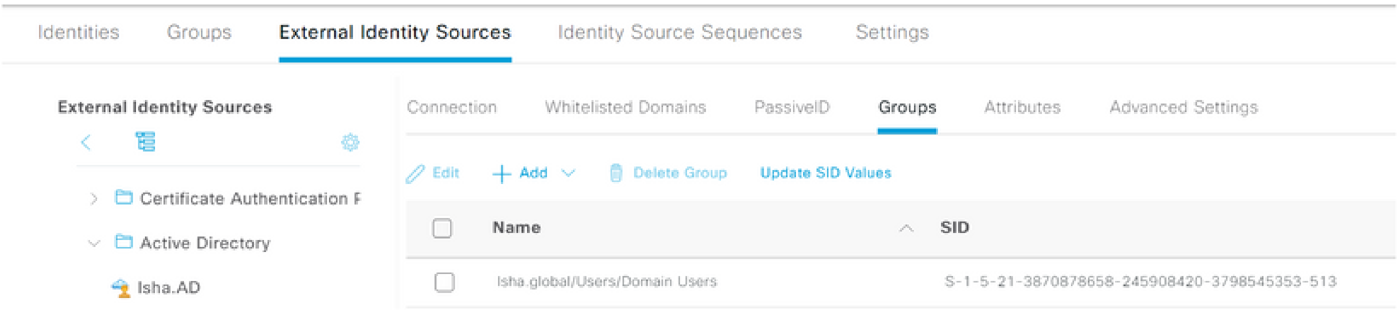
Join Operation Status

Status Summary: Successful

ISE Node	Node Status
ise30-1.Isha.global	✓ Completed.

Select Directory Groups

1. Navigate to **Administration** > **Identity Management** > **External Identity Sources** > **Active Directory** > **Groups** > **Add** > **Select groups form Directory**.
2. Import at least one AD Group to which your administrator belongs.

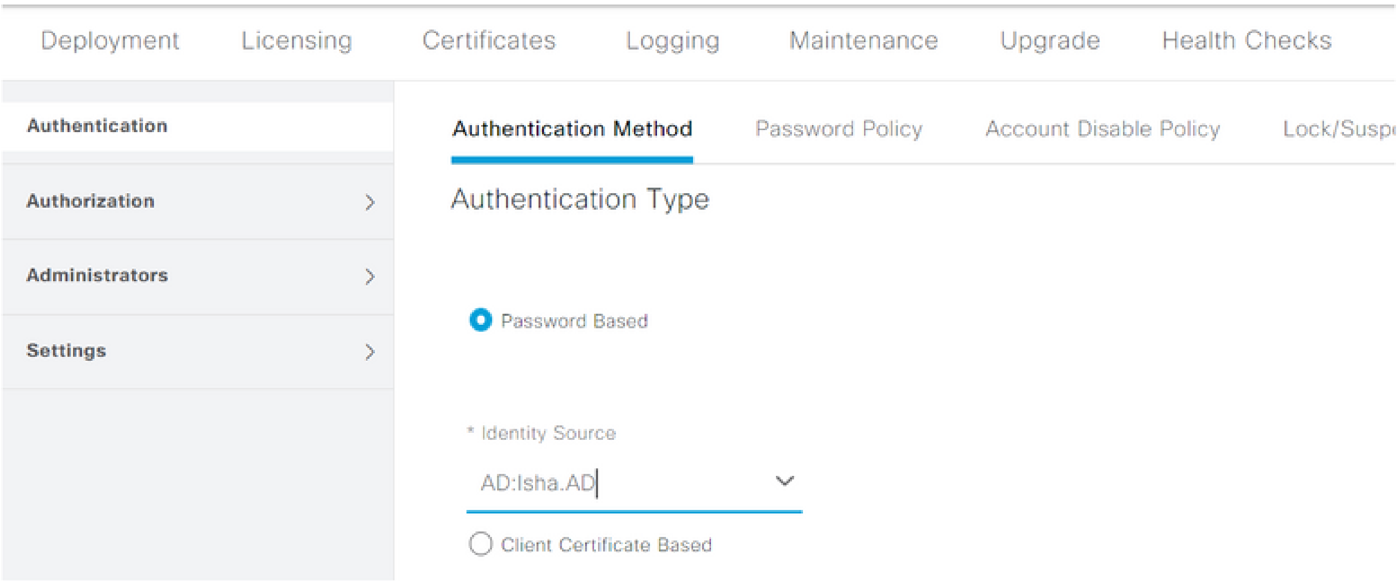


□	Name	SID
□	Isha.global/Users/Domain Users	S-1-5-21-3870878658-245908420-3798545353-513

Enable Administrative Access for AD

Complete these steps in order to enable password-based authentication for AD:

1. Navigate to **Administration** > **System** > **Admin Access** > **Authentication**.
2. From the **Authentication Method** tab, choose the **Password Based** option.
3. Choose **AD** from the **Identity Source** drop-down list.
4. Click **Save Changes**.



Authentication Type

● Password Based

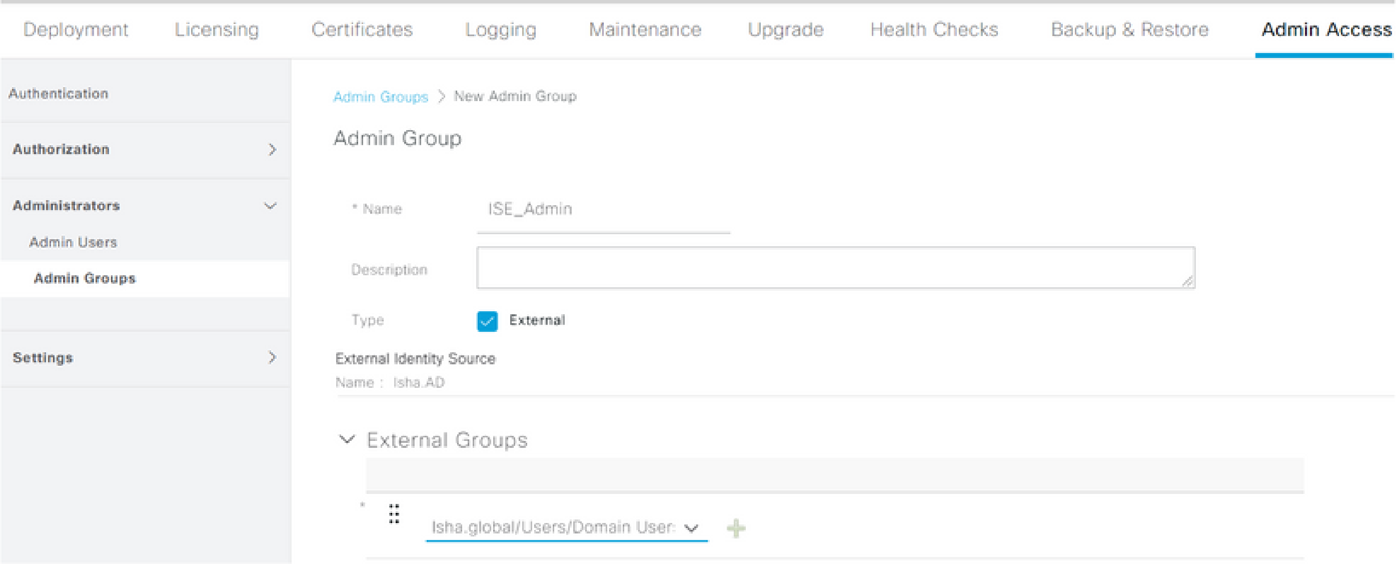
* Identity Source: AD:Isha.AD

○ Client Certificate Based

Configure the Admin Group to AD Group Mapping

Define a Cisco ISE Admin Group and map it to an AD group. This allows authorization to determine the Role Based Access Control (RBAC) permissions for the administrator based on group membership in AD.

1. Navigate to **Administration** > **System** > **Admin Access** > **Administrators** > **Admin Groups**.
2. Click **Add** in the table header in order to view the new Admin Group configuration pane.
3. Enter the **name** for the new Admin group.
4. In the Type field, check the **External** check box.
5. From the **External Groups** drop-down list, choose the AD group to which you want this Admin Group to map, as defined in the Select Directory Groups section.
6. Click **Save Changes**.



Admin Group

* Name: ISE_Admin

Description:

Type: ☑ External

External Identity Source
Name : Isha.AD

External Groups

* Isha.global/Users/Domain User:

Set RBAC Permissions for the Admin Group

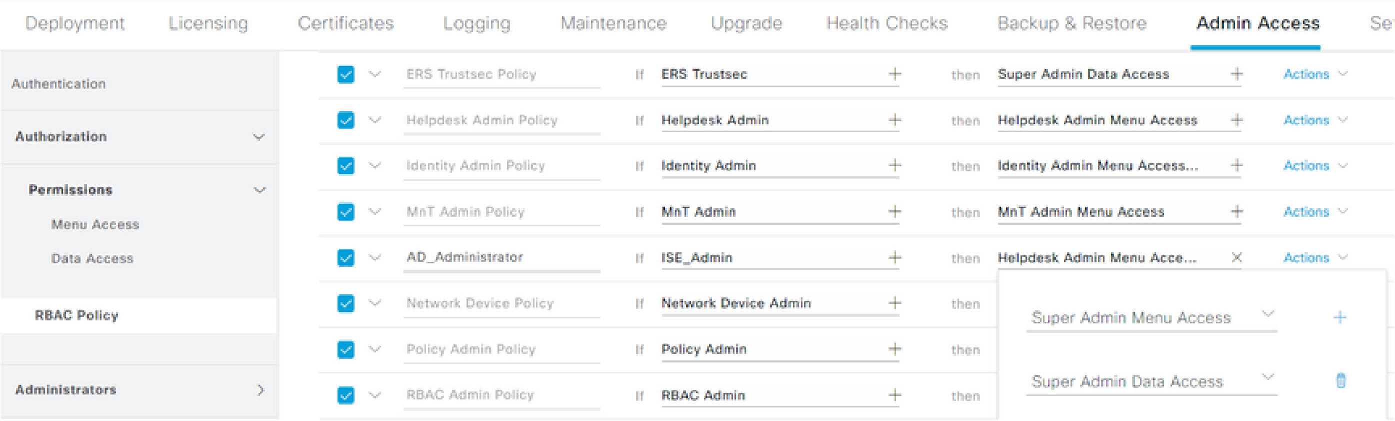
Complete these steps in order to assign RBAC permissions to the Admin Groups created in the previous section:

1. Navigate to **Administration** > **System** > **Admin Access** > **Authorization** > **Policy**.
2. From the Actions drop-down list on the right, choose **Insert New Policy** to add a new policy.

3. Create a new rule called AD_Administrator. Map it with the Admin Group defined in the Enable Administrative Access for AD section, and assign it permissions.

> **Note**: In this example, the Admin Group called Super Admin is assigned, which is equivalent to the standard admin account.

4. Click **Save Changes**. Confirmation of the changes saved are displayed in the lower-right corner of the GUI.



☑	ERS Trustsec Policy	If	ERS Trustsec	+	then	Super Admin Data Access	+	Actions
☑	Helpdesk Admin Policy	If	Helpdesk Admin	+	then	Helpdesk Admin Menu Access	+	Actions
☑	Identity Admin Policy	If	Identity Admin	+	then	Identity Admin Menu Access...	+	Actions
☑	MnT Admin Policy	If	MnT Admin	+	then	MnT Admin Menu Access	+	Actions
☑	AD_Administrator	If	ISE_Admin	+	then	Helpdesk Admin Menu Acce...	×	Actions
☑	Network Device Policy	If	Network Device Admin	+	then			
☑	Policy Admin Policy	If	Policy Admin	+	then			
☑	RBAC Admin Policy	If	RBAC Admin	+	then			

Super Admin Menu Access

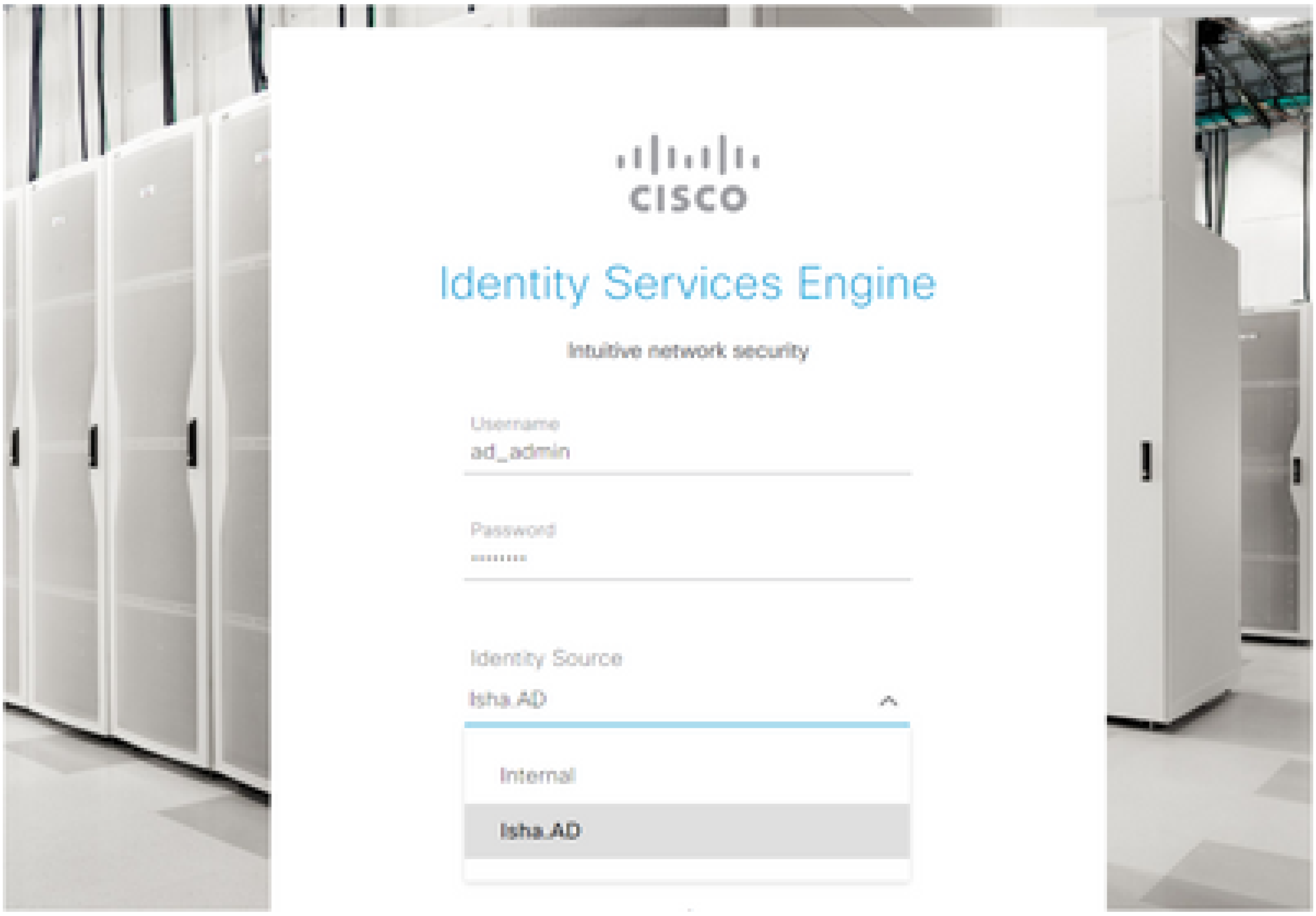
Super Admin Data Access

ISE GUI Access with AD Credentials

Complete these steps in order to access the ISE GUI with AD credentials:

1. Log out of the administrative GUI.
2. Choose **AD** from the Identity Source drop-down list.
3. Enter the **username** and **password** from the AD database and log in.

> **Note**: ISE defaults to the internal user store in the event that AD is unreachable, or the account credentials used do not exist in AD. This facilitates quick log in if you use the internal store while AD is configured for administrative access.



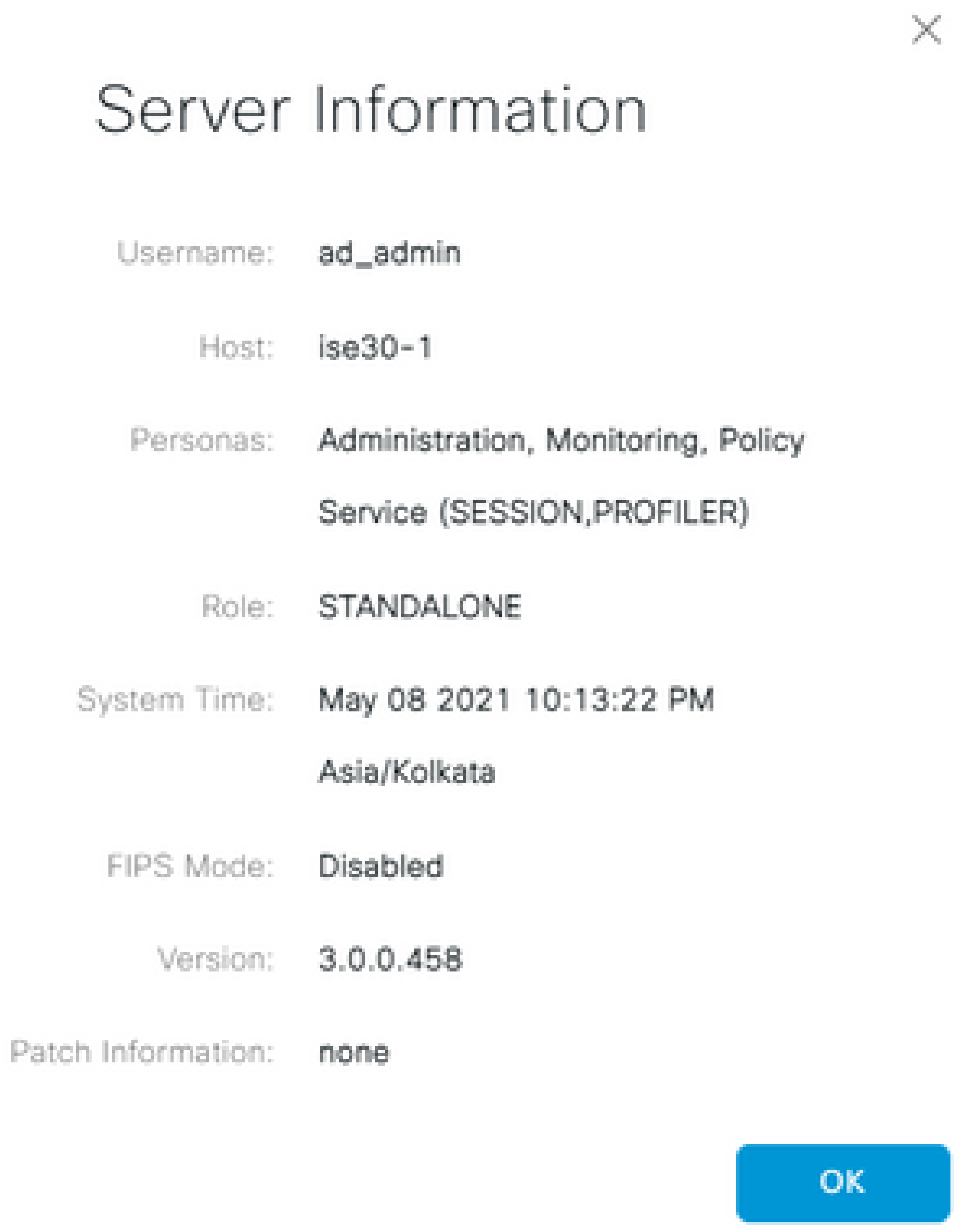
Identity Services Engine

Intuitive network security

Username
ad_admin

Password
••••••••

Identity Source
Isha.AD



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

ISE CLI Access with AD Credentials

Authentication with an external identity source is more secure than with the internal database. RBAC for CLI Administrators supports an external identity store.

Note: ISE Version 2.6 and later releases only support AD as the external identity source for CLI login.

Manage a single source for passwords without the need to manage multiple password policies and administer internal users within ISE, which results in reduced time and effort.

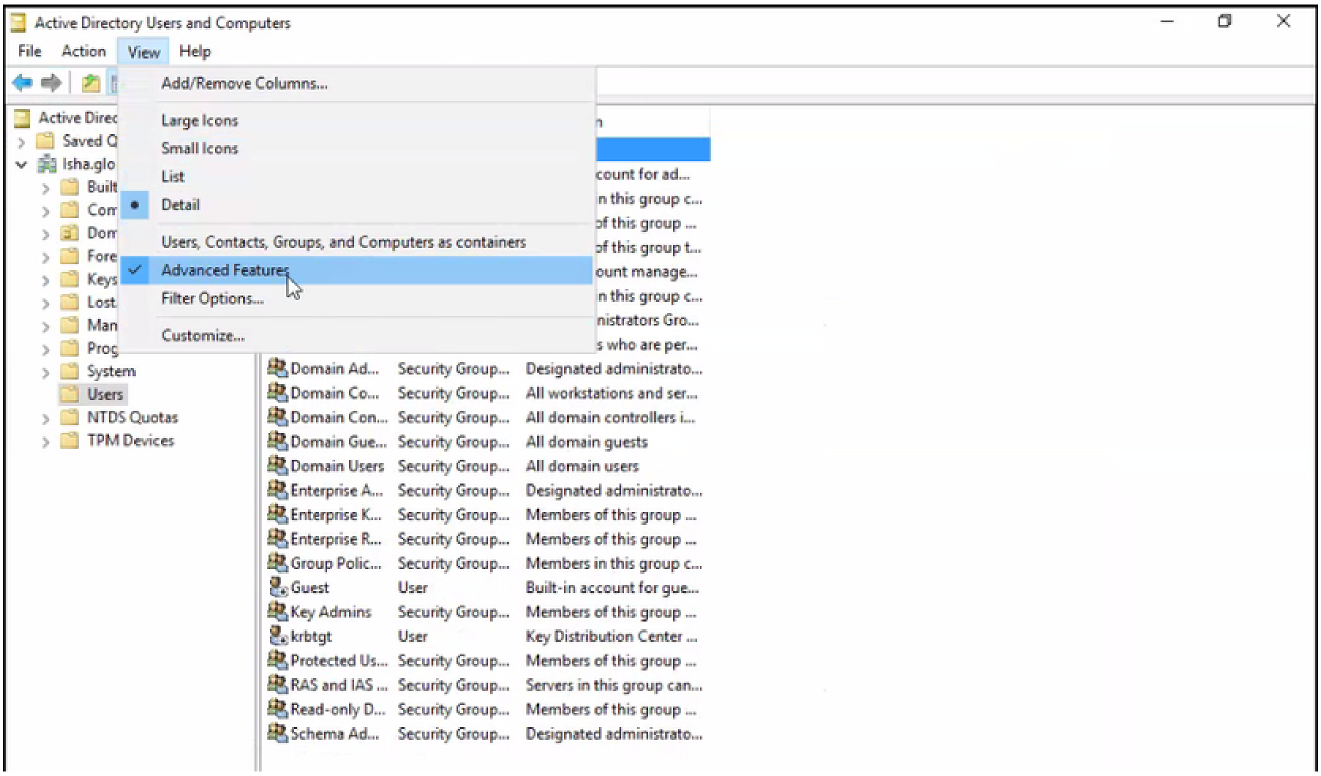
Prerequisites

You must have defined the Admin user, and added them to an Administrator group. The Admin must be a Super Admin**.**

Definethe User’s Attributes in the AD User Directory.

On the Windows server that runs Active Directory, modify the attributes for each user that you plan to configure as a CLI Administrator.

1. Open the **Server Manager Window**, and navigate to **Server Manager > Roles > Active Directory Domain Services > Active Directory Users and Computers > [ad.adserver] <ad_server>.local**.
2. Enable **Advanced Features** under the View menu so you can edit a user’s attributes.

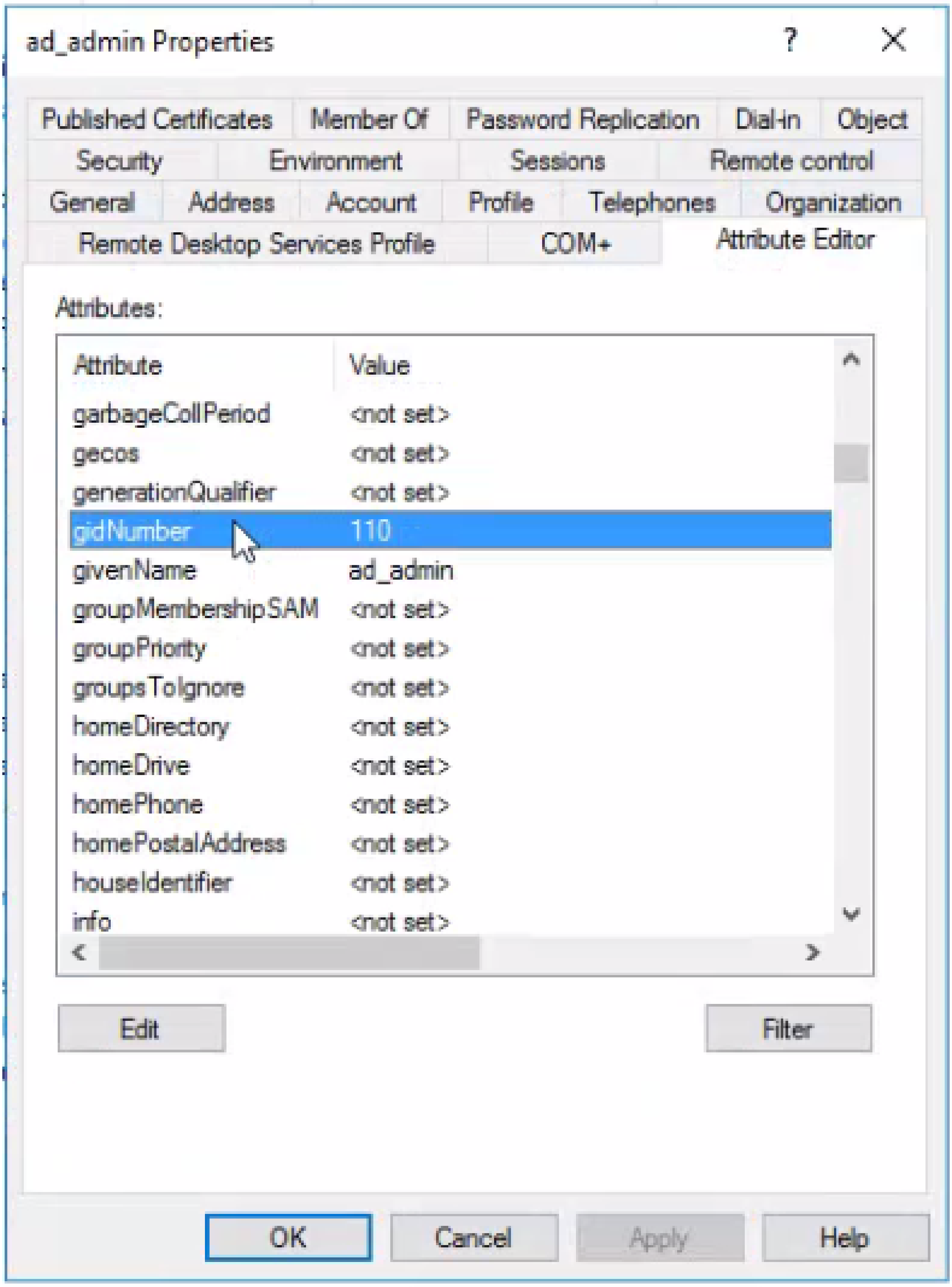


Domain Ad...	Security Group...	Designated administrato...
Domain Co...	Security Group...	All workstations and ser...
Domain Con...	Security Group...	All domain controllers i...
Domain Gue...	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise A...	Security Group...	Designated administrato...
Enterprise K...	Security Group...	Members of this group ...
Enterprise R...	Security Group...	Members of this group ...
Group Polic...	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...
Key Admins	Security Group...	Members of this group ...
krbtgt	User	Key Distribution Center ...
Protected Us...	Security Group...	Members of this group ...
RAS and IAS ...	Security Group...	Servers in this group can...
Read-only D...	Security Group...	Members of this group ...
Schema Ad...	Security Group...	Designated administrato...

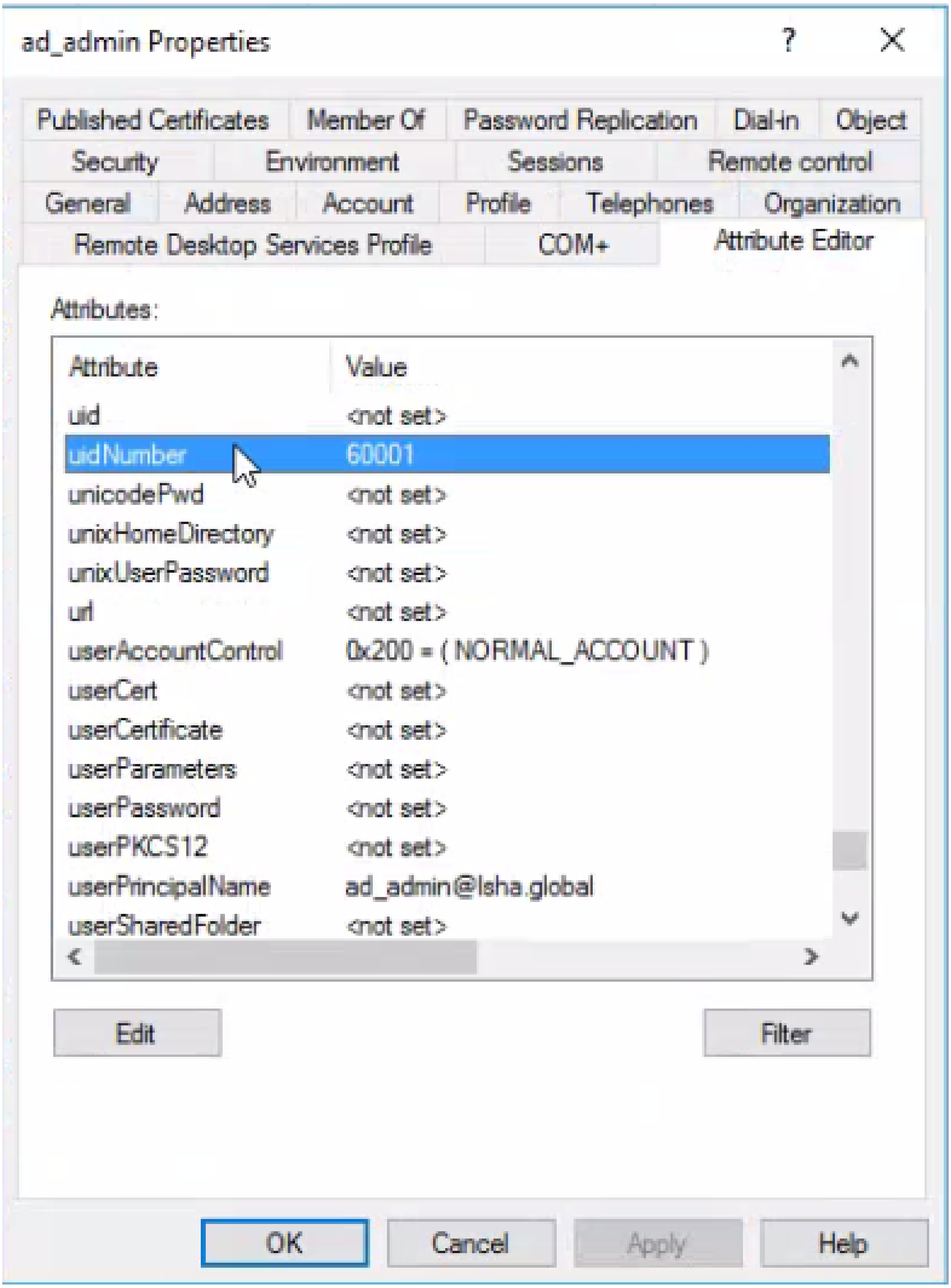
3. Navigate to the AD group that contains the Admin user and find that user.
4. Double-click the **user** to open the Properties window and choose the **Attribute Editor** .
5. Click any attribute and enter **gid** to locate the attribute **gidNumber** . If you do not find the gidNumber attribute, click the **Filter** button and uncheck.

   Show only attributes that have values.

6. Double-click the attribute name to edit each attribute. For each user:
   - Assign **uidNumber** greater than 60000, and make sure that the number is unique.
   - Assign **gidNumber** as 110 or 111.
   - GidNumber 110 denotes an admin user whereas 111 denotes a read-only user.
   - Do not change the **uidNumber** after assignment.
   - If you modify the **gidNumber** , wait at least five minutes before you make an SSH connection.



Attribute	Value
garbageCollPeriod	<not set>
gecos	<not set>
generationQualifier	<not set>
gidNumber	110
givenName	ad_admin
groupMembershipSAM	<not set>
groupPriority	<not set>
groupsToIgnore	<not set>
homeDirectory	<not set>
homeDrive	<not set>
homePhone	<not set>
homePostalAddress	<not set>
houseIdentifier	<not set>
info	<not set>



Attribute	Value
uid	<not set>
uidNumber	60001
unicodePwd	<not set>
unixHomeDirectory	<not set>
unixUserPassword	<not set>
url	<not set>
userAccountControl	0x200 = (NORMAL_ACCOUNT)
userCert	<not set>
userCertificate	<not set>
userParameters	<not set>
userPassword	<not set>
userPKCS12	<not set>
userPrincipalName	ad_admin@Isha.global
userSharedFolder	<not set>

Join the Admin CLI User to the AD Domain

Connect to the Cisco ISE CLI, run the **identity-store** command, and assign the Admin user to the ID store.

For example, to map the CLI admin user to the Active Directory defined in ISE as isha.global, run this command:

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

When the join is complete, connect to the **Cisco ISE CLI** and log in as the Admin CLI user to verify your configuration.

If the domain you use in this command was previously joined to the ISE node, then rejoin the domain in the Administrators console.

1. In the Cisco ISE GUI, click the **Menu** icon and navigate to **Administration > Identity Management > External Identity Sources**.
2. In the left-hand pane, choose **Active Directory** and choose your **AD name**.
3. In the right-hand pane, the status for your AD connection possibly reads Operational. There are errors if you test the connection with Test User with either MS-RPC or Kerberos.
4. Verify that you can still log in to the Cisco ISE CLI as the Admin CLI user.

ISE CLI

1. Log in to the ISE CLI:
   <#root>

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

   ```
   configure terminal
   ```

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

2. Join the node to the domain:

   ```
   ise30-1/admin(config)# identity-store active-directory domain-name isha.global user Administrator
   ```
   If the domain isha.global is already joined via UI, then you must rejoin the domain **isha.global** from UI after this configuration. Until the rejoin happens, authentications to isha.global fails.
   Do you want to proceed? Y/N: **Y**
   Password for Administrator:
   Joined to domain isha.global successfully.

Notes:
- If the domain is already joined via GUI, then rejoin the node from GUI, otherwise, the authentications against AD continues to fail.
- All nodes must be joined individually via CLI.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

Join Issues

Issues during the join operation and the logs related to this can be seen under /var/log/messages file.

Command: **show logging system messages**

Working Scenario

```
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/oddjobd, /usr/libexec/oddjob/mkhomedir, /usr/sbin/sssd, /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/sssd.service to /usr/lib/systemd/system/sssd.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 realmd: * /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 realmd: * Successfully enrolled machine in realm
```

Non-Working Scenario

Join failure due to incorrect password:

```
2021-07-19T21:12:45.487538+05:30 ise30-1 dbus[9675]: [system] Activating via systemd: service name='org.freedesktop.realmd' unit='realmd.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.realmd'
 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 realmd: * Resolving: _ldap._tcp.isha.global
 2021-07-19T21:12:45.571092+05:30 ise30-1 realmd: * Performing LDAP DSE lookup on: 10.127.197.115
 2021-07-19T21:12:45.572854+05:30 ise30-1 realmd: * Performing LDAP DSE lookup on: 10.127.197.236
 2021-07-19T21:12:45.573376+05:30 ise30-1 realmd: * Successfully discovered: Isha.global
 2021-07-19T21:12:52.273667+05:30 ise30-1 realmd: * Required files: /usr/sbin/oddjobd, /usr/libexec/oddjob/mkhomedir, /usr/sbin/sssd, /usr/bin/net
 2021-07-19T21:12:52.274730+05:30 ise30-1 realmd: * LANG=C LOGNAME=root /usr/bin/net -s /var/cache/realmd/realmd-smb-
```

```
conf.R0SM60 -U Administrator ads join Isha.global
 2021-07-19T21:12:52.369726+05:30 ise30-1 realmd: Enter Administrator's password:
 2021-07-19T21:12:52.370190+05:30 ise30-1 realmd: 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 realmd: ! Joining the domain Isha.global failed
```

Log in Issues

Issues during log in and the logs related to this can be seen under /var/log/secure.

Command: show logging system secure

Successful authentication:

```
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
```

Authentication failure due to incorrect password:

```
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
```

Authentication failure due to invalid user:

```
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
```