

Integrar o AD para GUI do ISE e CLI Fazer login

Contents

[Introduction](#)

[Prerequisites](#)

[Componentes Utilizados](#)

[Configurar](#)

[Junte-se ao ISE para o AD](#)

[Selecionar grupos de diretórios](#)

[Habilitar Acesso Administrativo para AD](#)

[Configurar o grupo de administração para o mapeamento do grupo do AD](#)

[Definir permissões RBAC para o grupo de administradores](#)

[Acesso à GUI do ISE com credenciais do AD](#)

[Acesso à CLI do ISE com credenciais do AD](#)

[CLI ISE](#)

[Verificar](#)

[Troubleshoot](#)

[Problemas de junção](#)

[Problemas de login](#)

Introduction

Este documento descreve a configuração do Microsoft AD como um armazenamento de identidade externo para acesso administrativo à GUI e CLI de gerenciamento do Cisco ISE.

Prerequisites

A Cisco recomenda o conhecimento destes tópicos:

- Configuração do Cisco ISE versão 3.0
- AD da Microsoft

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco ISE versão 3.0
- Windows Server 2016

Este documento descreve a configuração do Microsoft **Active Directory (AD)** como um armazenamento de identidade externo para acesso administrativo ao Cisco **Identity Services Engine (ISE)** GUI e CLI de gerenciamento.

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. Se a rede estiver

ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Use esta seção para configurar o uso do Microsoft AD como um armazenamento de identidade externo para acesso administrativo à GUI de gerenciamento do Cisco ISE.

Essas portas são usadas entre o nó do ISE e o AD para esta comunicação:

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

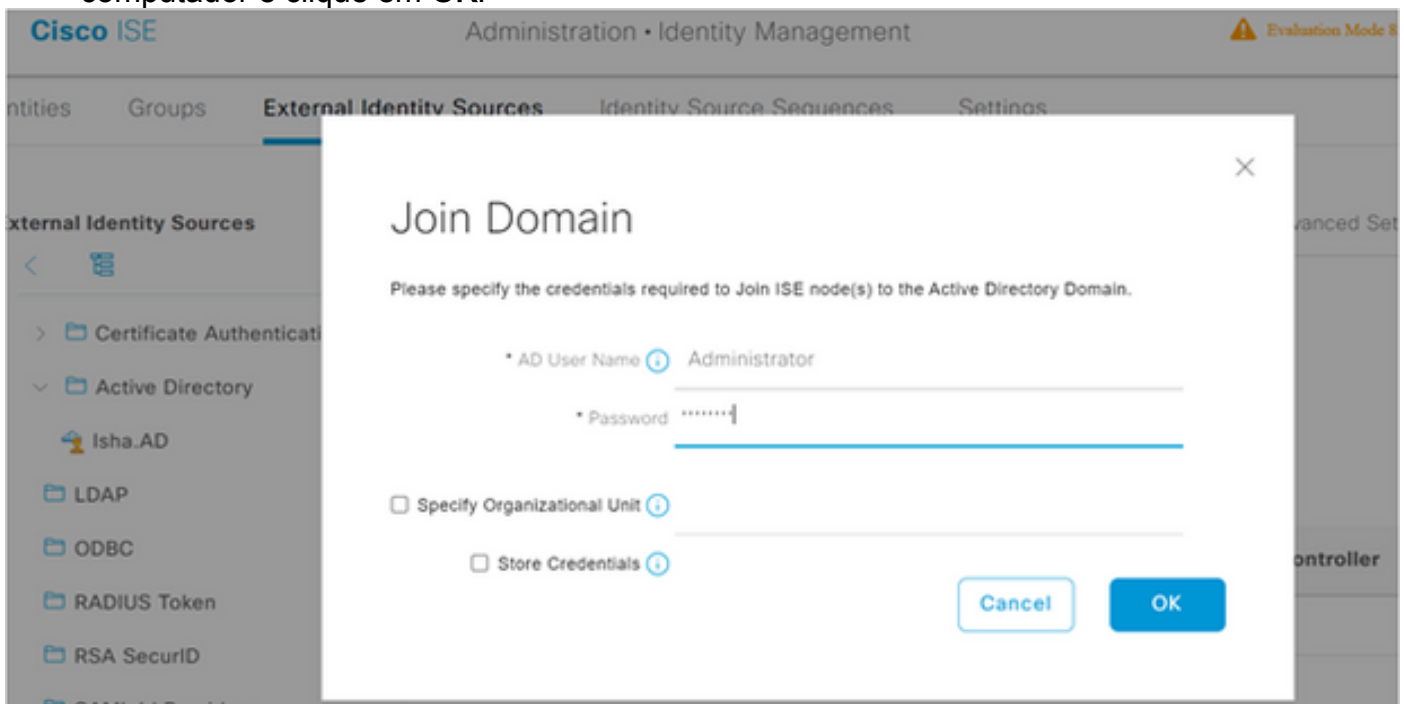
Observação: verifique se a conta do AD tem todos os privilégios necessários.

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"> • 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) <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"> • Search Active Directory (to see if a Cisco ISE machine account already exists) • Remove Cisco ISE machine account from domain <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"> • 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 <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>


Junte-se ao ISE para o AD

1. Navegue até **Administration > Identity Management > External Identity Sources > Active Directory**.
2. Insira o novo nome do ponto de ingresso e o domínio do AD.
3. Insira as credenciais da conta do AD que pode adicionar e fazer alterações em objetos de computador e clique em **OK**.



Join Operation Status

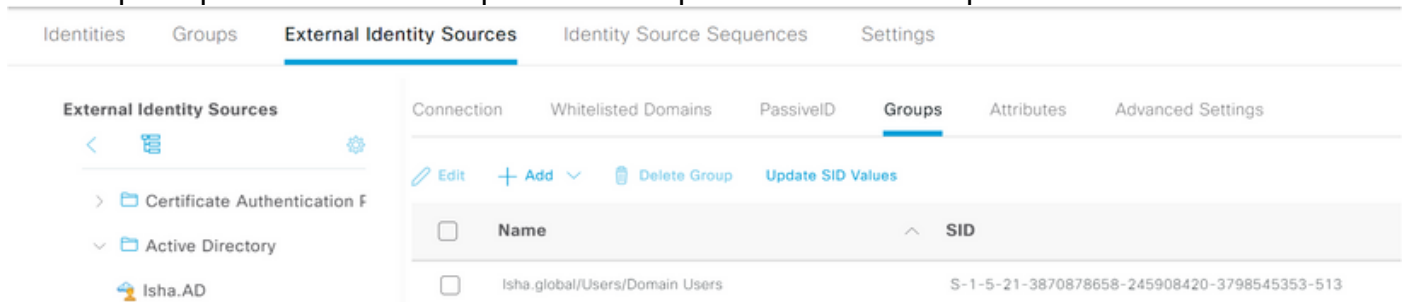
Status Summary: Successful

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

Close

Selecionar grupos de diretórios

1. Navegue até **Administration > Identity Management > External Identity Sources > Active Directory > Groups > Add > Select groups form Directory** .
2. Importe pelo menos um Grupo do AD ao qual o administrador pertence.



External Identity Sources	
Identities	Groups
External Identity Sources	
Identity Source Sequences	
Settings	
Connection	
Whitelisted Domains	
PassiveID	
Groups	
Attributes	
Advanced Settings	
Edit	
+ Add	
Delete Group	
Update SID Values	
Name	SID
Isha.global/Users/Domain Users	S-1-5-21-3870878658-245908420-3798545353-513

Habilitar Acesso Administrativo para AD

Conclua estas etapas para habilitar a autenticação baseada em senha para o AD:

1. Navegue até **Administration > System > Admin Access > Authentication** .
2. Nos **Authentication Method** , escolha o **Password Based** opção.
3. Escolha **AD** no menu **Identity Source** lista suspensa.
4. Clique em **Save Changes** .

Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks
<div> <div> Authentication </div> <div> Authorization </div> <div> Administrators </div> <div> Settings </div> </div> <div> <div>Authentication Method</div> <div> Password Policy Account Disable Policy Lock/Susp </div> </div>						
<div>Authentication Type</div> <div> <input checked="" type="radio"/> Password Based </div> <div> * Identity Source <div>AD:Isha.AD</div> </div> <div> <input type="radio"/> Client Certificate Based </div>						

Configurar o grupo de administração para o mapeamento do grupo do AD

Definir um Cisco ISE **Admin Group** e mapeá-lo para um grupo do AD. Isso permite que a autorização determine o **Role Based Access Control (RBAC)** permissões para o administrador com base na associação de grupo no AD.

1. Navegue até **Administration > System > Admin Access > Administrators > Admin Groups**.
2. Clique em **Add** no cabeçalho da tabela para exibir a nova **Admin Group** painel de configuração.
3. Digite o nome do novo grupo Admin.
4. No **Type**, marque a caixa **External** caixa de seleção.
5. Nos **External Groups** escolha o grupo do AD para o qual você deseja mapear esse Grupo de administradores, conforme definido na **Select Directory Groups** seção.
6. Clique em **Save Changes**.

Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access
<div> <div> Authentication </div> <div> Authorization </div> <div> Administrators <div>Admin Users</div> <div>Admin Groups</div> </div> <div> Settings </div> </div> <div> <div>Admin Groups > New Admin Group</div> <div>Admin Group</div> <div> * Name <div>ISE_Admin</div> </div> <div> Description <div></div> </div> <div> Type <input checked="" type="checkbox"/> External </div> <div> External Identity Source <div>Name : Isha.AD</div> </div> <div> External Groups <div> <div> Isha.global/Users/Domain User </div> </div> </div> </div>								

Definir permissões RBAC para o grupo de administradores

Conclua estas etapas para atribuir permissões RBAC aos grupos de administradores criados na seção anterior:

1. Navegue até **Administration > System > Admin Access > Authorization > Policy**.

2. Nos **Actions** à direita, escolha **Insert New Policy** para adicionar uma nova política.
3. Crie uma nova regra chamada **AD_Administrator**, mapeie-o com o grupo de administradores definido no **Enable Administrative Access** para a seção AD e atribua permissões a ela.
Observação: neste exemplo, o grupo Admin chamado **Super Admin** é atribuído, o que equivale à conta admin padrão.
4. Clique em **Save Changes**. A confirmação das alterações salvas é exibida no canto inferior direito da GUI.

Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Checks	Backup & Restore	Admin Access	Se
Authentication									
Authorization									
Permissions									
Menu Access									
Data Access									
RBAC Policy									
Administrators									

<input checked="" type="checkbox"/>	ERS Trustsec Policy	If	ERS Trustsec	+	then	Super Admin Data Access	+	Actions
<input checked="" type="checkbox"/>	Helpdesk Admin Policy	If	Helpdesk Admin	+	then	Helpdesk Admin Menu Access	+	Actions
<input checked="" type="checkbox"/>	Identity Admin Policy	If	Identity Admin	+	then	Identity Admin Menu Access...	+	Actions
<input checked="" type="checkbox"/>	MnT Admin Policy	If	MnT Admin	+	then	MnT Admin Menu Access	+	Actions
<input checked="" type="checkbox"/>	AD_Administrator	If	ISE_Admin	+	then	Helpdesk Admin Menu Ace...	×	Actions
<input checked="" type="checkbox"/>	Network Device Policy	If	Network Device Admin	+	then			
<input checked="" type="checkbox"/>	Policy Admin Policy	If	Policy Admin	+	then			
<input checked="" type="checkbox"/>	RBAC Admin Policy	If	RBAC Admin	+	then			

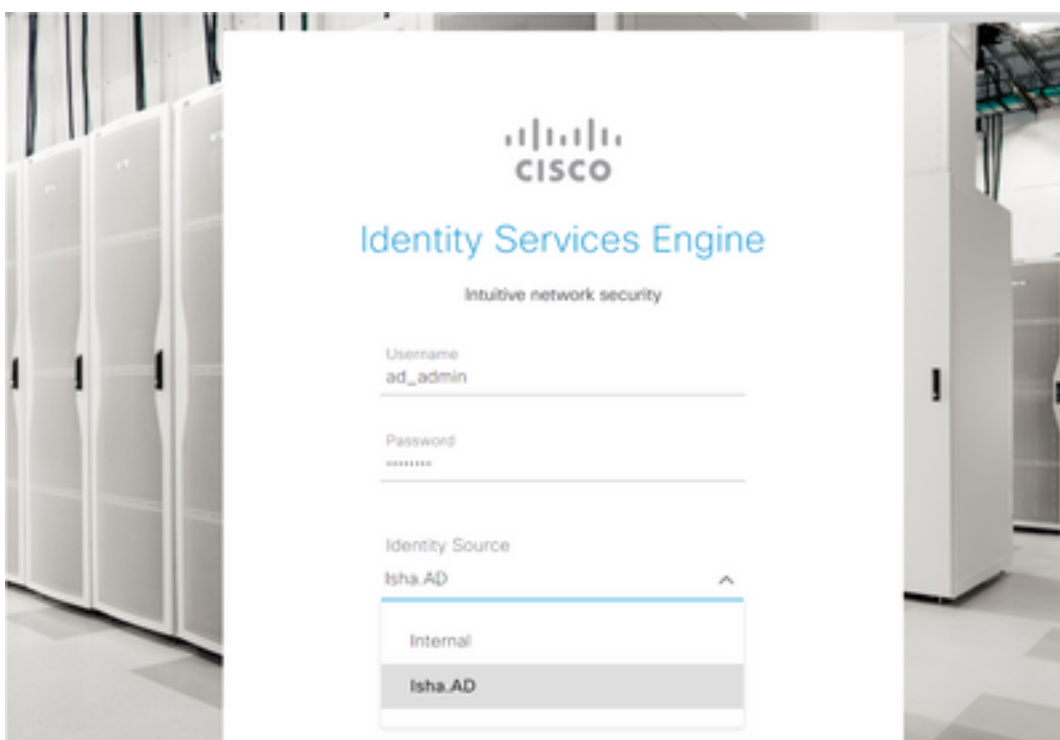
Super Admin Menu Access	+
Super Admin Data Access	

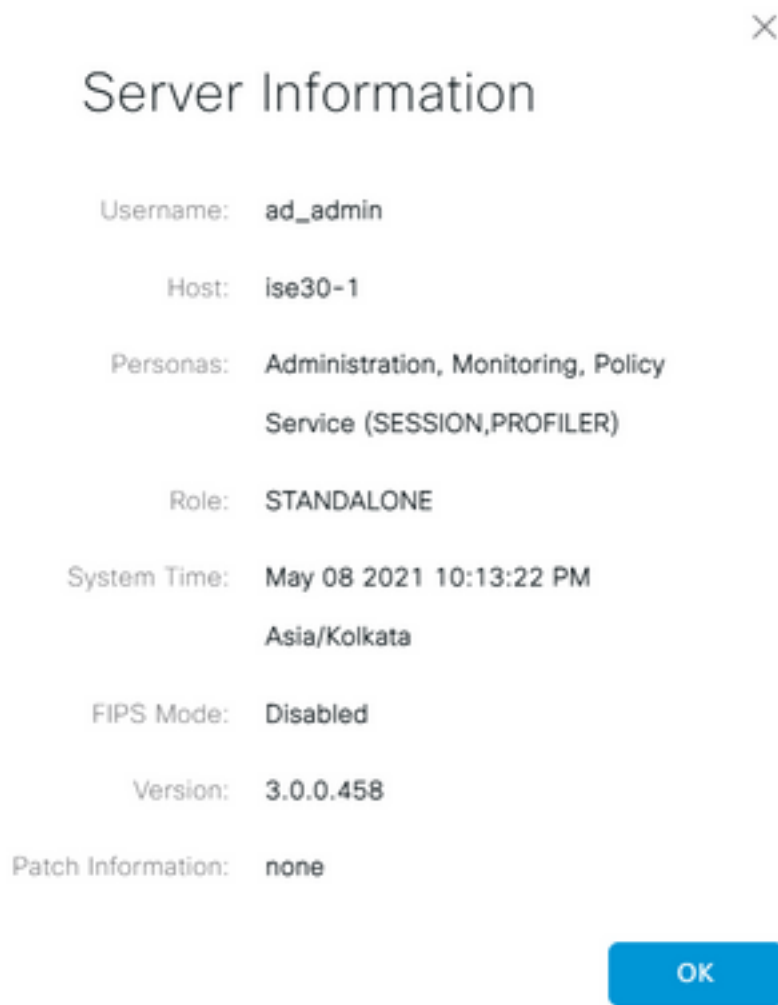
Acesso à GUI do ISE com credenciais do AD

Conclua estas etapas para acessar a GUI do ISE com credenciais do AD:

1. Encerre a sessão da GUI administrativa.
2. Escolha **AD** no menu **Identity Source** lista suspensa.
3. Insira o nome de usuário e a senha do banco de dados do AD e faça login.

Observação: o ISE assume como padrão o armazenamento de usuário interno caso o AD esteja inacessível ou as credenciais de conta usadas não existam no AD. Isso facilita o logon rápido se você usar o armazenamento interno enquanto o AD estiver configurado para acesso administrativo.





Acesso à CLI do ISE com credenciais do AD

A autenticação com uma fonte de identidade externa é mais segura do que com o banco de dados interno. RBAC para CLI Administrators oferece suporte a um repositório de identidade externo.

Observação: o ISE versão 2.6 e posterior oferece suporte à autenticação de administradores CLI por fontes de identidade externas, como o AD.

Gerenciar uma única fonte de senhas sem a necessidade de gerenciar várias políticas de senha e administrar usuários internos no ISE, o que resulta em tempo e esforço reduzidos.

Prerequisites

Você deve ter definido o usuário Administrador e adicionado-o a um grupo Administrador. O administrador deve ser um Super Admin .

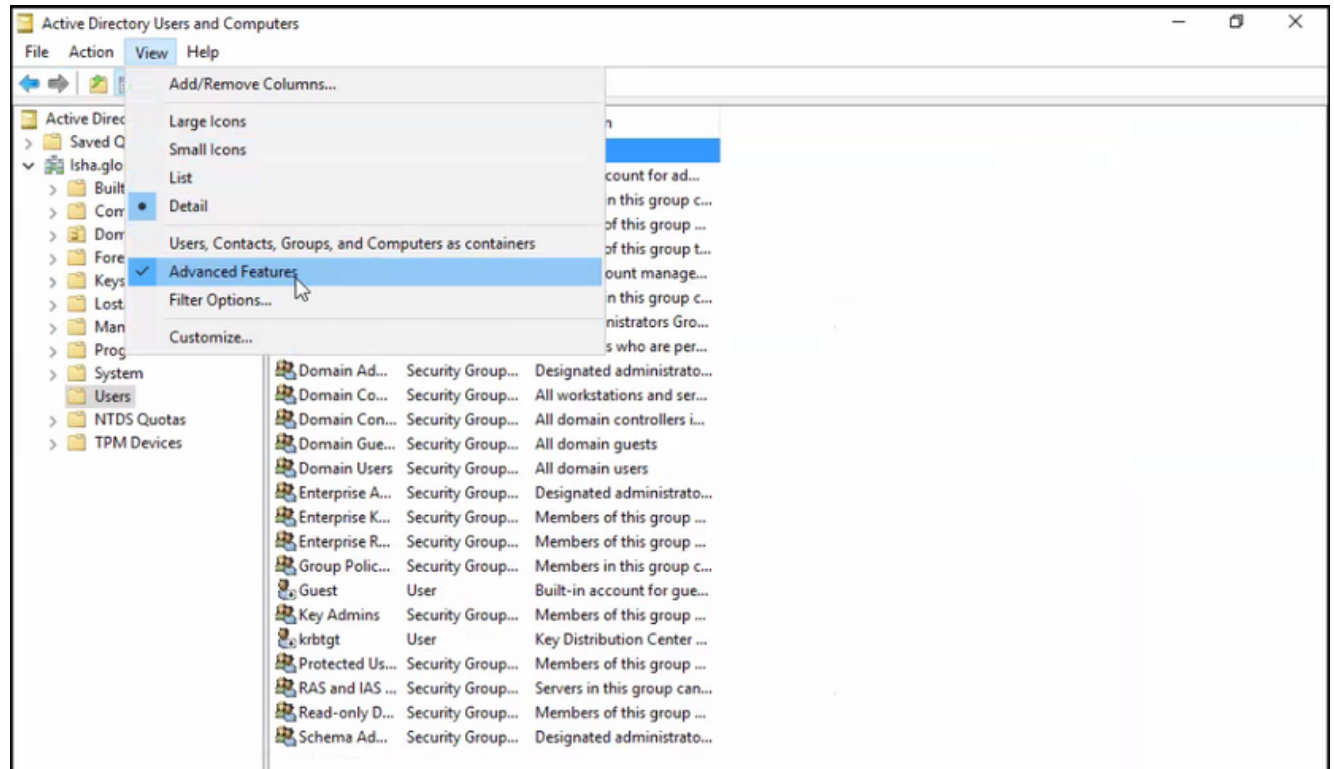
Define the User's Attributes in the AD User Directory

No servidor Windows que executa o Active Directory , modifique os atributos para cada usuário que você planeja configurar como um Administrador CLI.

1. Abra o Server Manager Window e navegue até Server Manager > Roles > Active Directory Domain Services >

Active Directory Users and Computers > [ad.adserver]

2. Enable **Advanced Features** no menu Exibir para que você possa editar os atributos de um usuário.



3. Navegue até o grupo do AD que contém o usuário Admin e localize esse usuário.
4. Clique duas vezes no usuário para abrir a **Properties** e escolha o botão **Attribute Editor**.
5. Clique em qualquer atributo e insira **gid** para localizar o atributo **gidNumber**. Se você não encontrar o **gidNumber** atributo, clique no botão **Filter** e desmarque. Mostrar somente atributos que tenham valores.
6. Clique duas vezes no nome do atributo para editar cada atributo. Para cada usuário: Atribuir **uidNumber** maior que 60000 e certifique-se de que o número seja exclusivo. Atribuir **gidNumber** como 110 ou 111. **GidNumber** 110 indica um usuário administrador, enquanto 111 indica um usuário somente leitura. Não altere o **uidNumber** após a atribuição. Se você modificar o comando **gidNumber**, aguarde pelo menos cinco minutos antes de fazer uma conexão SSH.

ad_admin Properties



Published Certificates	Member Of	Password Replication	Dial-In	Object
Security	Environment	Sessions	Remote control	
General	Address	Account	Profile	Telephones
Remote Desktop Services Profile	COM+	Attribute Editor		

Attributes:

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>

Edit

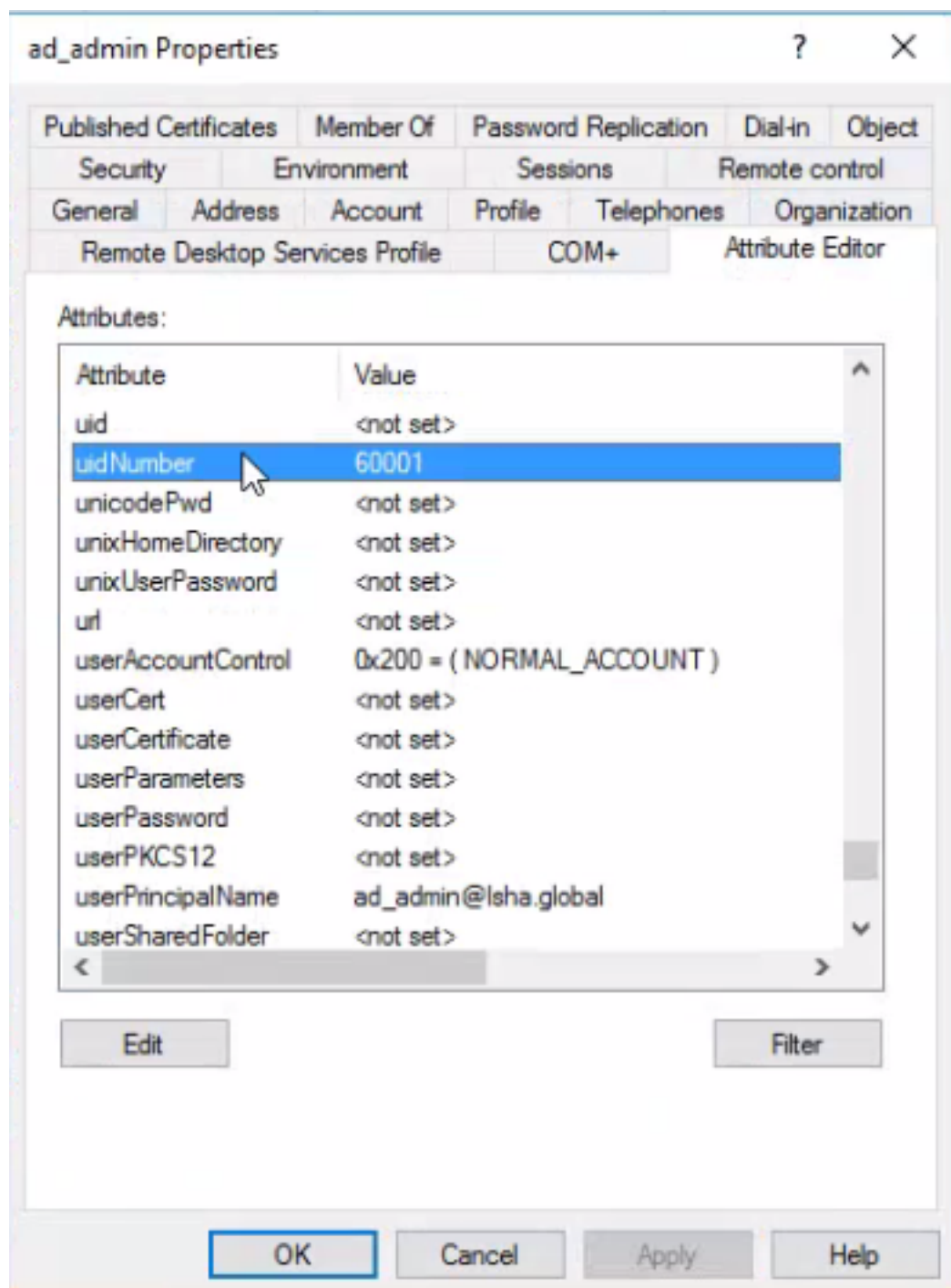
Filter

OK

Cancel

Apply

Help



Ingressar o usuário CLI do administrador no domínio do AD

Conecte-se à CLI do Cisco ISE, execute o comando `identity-store` e atribua o usuário Admin ao armazenamento de ID.

Por exemplo, para mapear o usuário admin da CLI para o Active Directory definido no ISE como isha.global, execute este comando:

```
identity-store active-directory domain-name
```

Quando a junção estiver concluída, conecte-se à CLI do Cisco ISE e faça login como o usuário da CLI Admin para verificar sua configuração.

Se o domínio usado nesse comando tiver ingressado anteriormente no nó do ISE, reingresse no domínio no console Administradores.

1. Na GUI do Cisco ISE, clique no botão **Menu** e navegue até **Administration > Identity Management > External Identity Sources**.
2. No painel à esquerda, escolha **Active Directory** e escolha seu nome do AD.
3. No painel direito, o status da conexão do AD possivelmente será **Operational**. Há erros se você testar a conexão com Usuário de Teste com MS-RPC ou Kerberos.
4. Verifique se você ainda pode fazer login na CLI do Cisco ISE como o usuário da CLI do administrador.

CLI ISE

1. Faça login na CLI do ISE:

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

2. Associe o nó ao domínio: **ise30-1/admin(config)# identity-store active-directory domain-name isha.global user Administrator**

Se o domínio **isha.global** já ingressou via interface do usuário, então você deve ingressar novamente no domínio **isha.global** da interface do usuário após esta configuração. Até que o novo ingresso ocorra, as autenticações para **isha.global** falha.

Do you want to proceed? Y/N :Y
Password for Administrator:

Ingressou no domínio **isha.global** com êxito **Notas:**

- Se o domínio já tiver ingressado via GUI, reingresse o nó a partir da GUI; caso contrário, as autenticações no AD continuarão a falhar.

- Todos os nós devem ser unidos individualmente via CLI. **Verificar** No momento, não há procedimento de verificação disponível para esta

configuração. **Troubleshoot** **Problemas de junção** Problemas durante a operação de junção e os logs relacionados a isso podem ser vistos em **"/var/log/messages file"**. Comando:

show logging system messages **Cenário de trabalho**

```
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/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[lisha.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 --enablesss --
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 **Cenário não**

funcionalFalha ao ingressar devido a senha incorreta: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/sss, /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 **Problemas de**

loginProblemas durante o login e os logs relacionados a isso podem ser vistos em

/var/log/secure .Comando: show logging system secure **Autenticação bem-sucedida:**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

Falha de autenticação devido a senha incorreta: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

ssh2Falha de autenticação devido a usuário inválido: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

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.