

## ISE Active Directory Admin Login:

If you're working in an Active Directory environment you should consider using AD credentials for authenticating against ISE instead of locally stored credentials. Not only are AD credentials more convenient to use, it's also easier to track the activity of user's within ISE when they are using their own credentials versus shared locally stored credentials. It will fall back to the local credentials should AD be unavailable. Another nice thing about AD integration is you can use AD security groups for Role Based Access Control (RBAC) to ISE. Once you've set up the roles in ISE and created the AD groups it's as simple as adding AD users to a security group when they're hired and removing them from the AD group when they retire or change positions.

## Setting NTP Server:

Navigate to **Administration -> System -> Settings -> System Time** and expand the **NTP Server Configuration** field. Enter your NTP server information in the NTP Server fields and click **Save**. We already have NTP setting in the time of Installation we provide.

The screenshot displays the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Administration' menu is expanded, showing 'System', 'Identity Management', 'Network Resources', 'Device Portal Management', 'pxGrid Services', 'Feed Service', and 'Threat Center'. The 'System' menu is further expanded, showing 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance', 'Upgrade', 'Backup & Restore', 'Admin Access', and 'Settings'. The 'Settings' menu is expanded, showing 'System Time Configuration' and 'NTP Authentication Keys'. The 'System Time Configuration' page is displayed, showing the 'Time Zone' set to 'UTC'. The 'NTP Server Configuration' section is expanded, showing three NTP Server entries. The first entry, 'NTP Server 1', has the IP address '192.168.100.230' entered in the 'NTP Server' field and 'None' selected in the 'Key' dropdown. The second and third entries, 'NTP Server 2' and 'NTP Server 3', have empty 'NTP Server' fields and 'None' selected in the 'Key' dropdown. The 'Save' and 'Reset' buttons are visible at the bottom of the configuration section.

## Verifying DNS Settings:

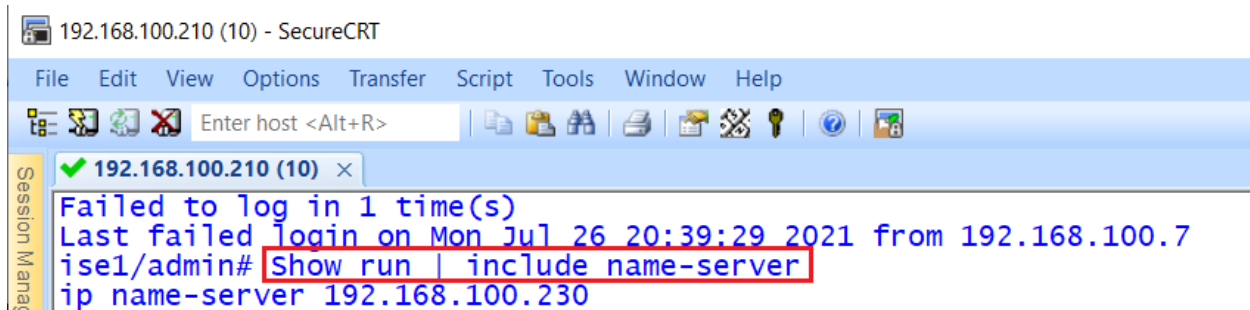
If you do not have DNS servers listed or the incorrect servers are listed, then you need to fix it. Within the console or SSH session into your ISE appliance run the command:

**config**

**ip name-server 192.168.100.230**

**write memory**

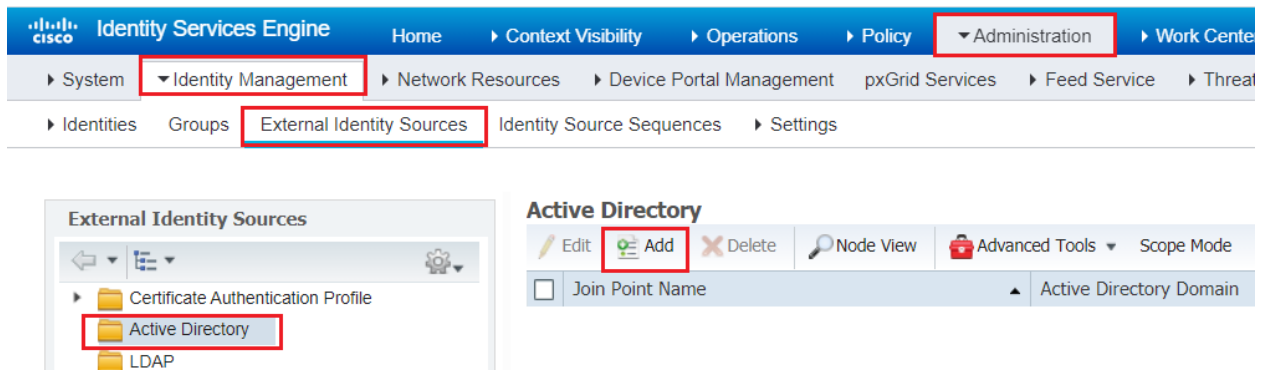
We also need to verify that DNS is set correctly. If ISE cannot resolve DNS with your domain name servers then joining your domain will fail. Open the console or an SSH session into your ISE appliance and run the command. **show run | include name-server**



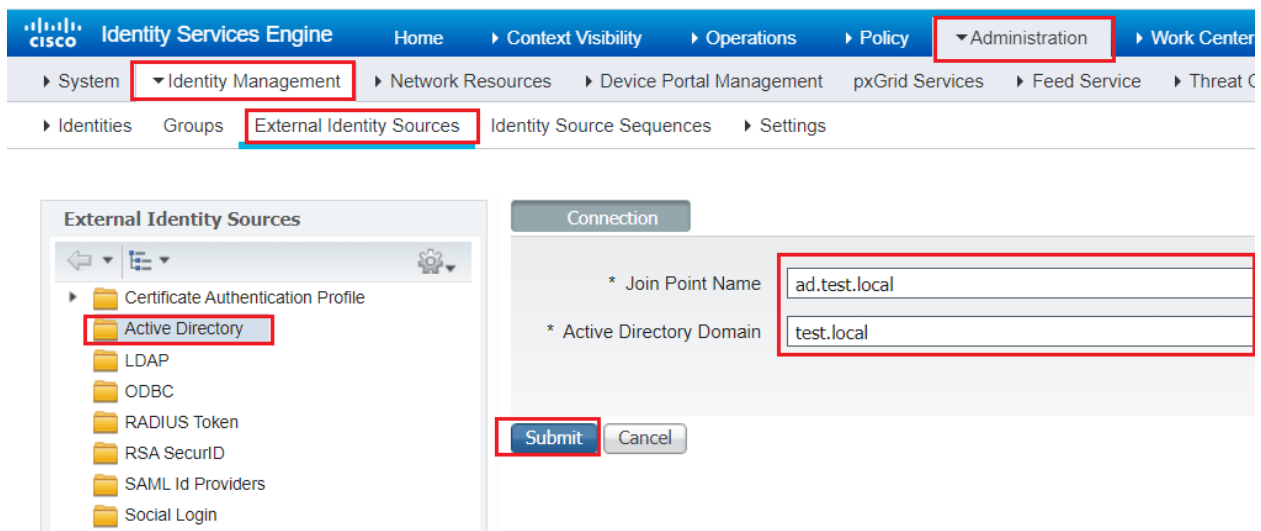
```
192.168.100.210 (10) - SecureCRT
File Edit View Options Transfer Script Tools Window Help
Enter host <Alt+R>
192.168.100.210 (10) x
Failed to log in 1 time(s)
Last failed login on Mon Jul 26 20:39:29 2021 from 192.168.100.7
ise1/admin# Show run | include name-server
ip name-server 192.168.100.230
```

### Joining Active Directory Domain:

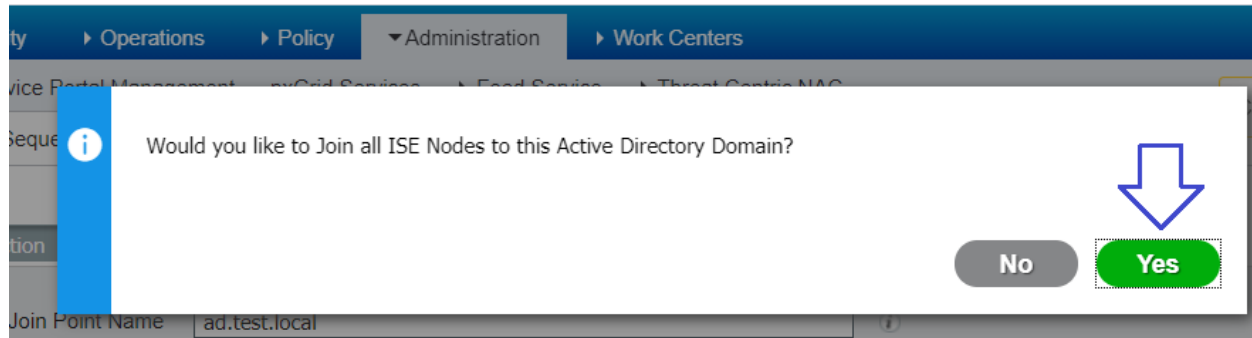
Before we can use Active Directory to control authentication to ISE for admins we need to join ISE to the domain. Navigate to **Administration > Identity Management > External Identity Sources > Active Directory** and click on **Add**



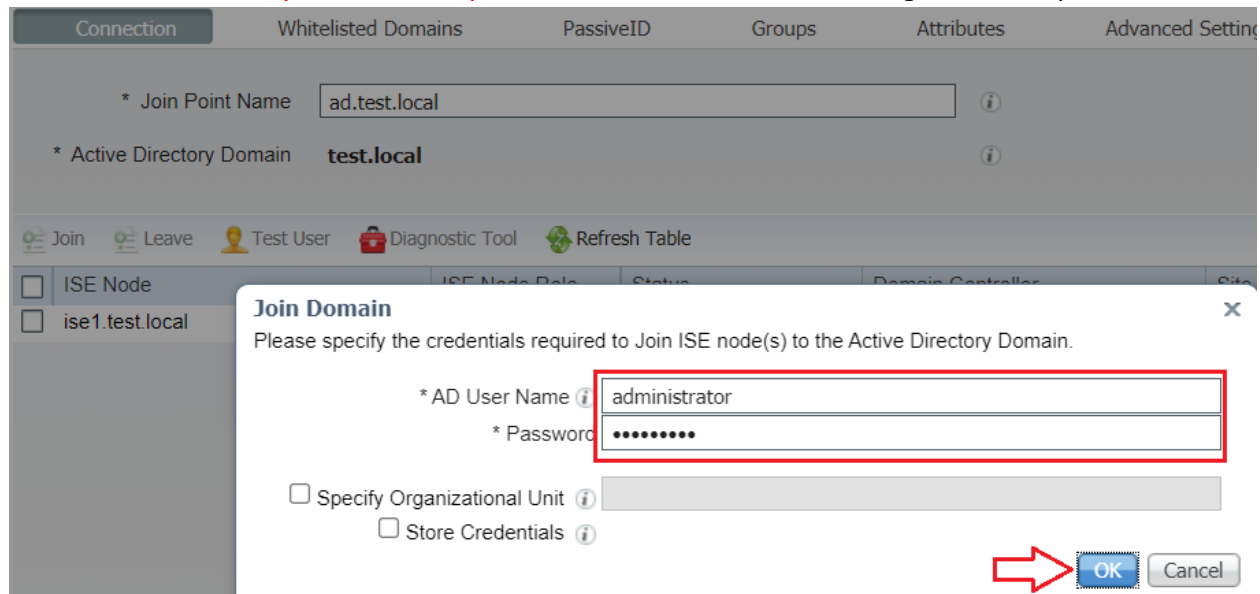
Enter domain name in **Active Directory Domain** boxes and **Join Point Name** anything you like click the **Submit** button.



A pop-up appears asking if you want to join the newly created join point to the domain. Click **Yes**. If you want to join immediately. If you clicked **No**, then saving the configuration saves the Active Directory domain configuration globally, but none of the Cisco ISE nodes are joined to the domain yet.



Enter **Active Directory username & password** from Join Domain dialog box that opens. Click **OK**.

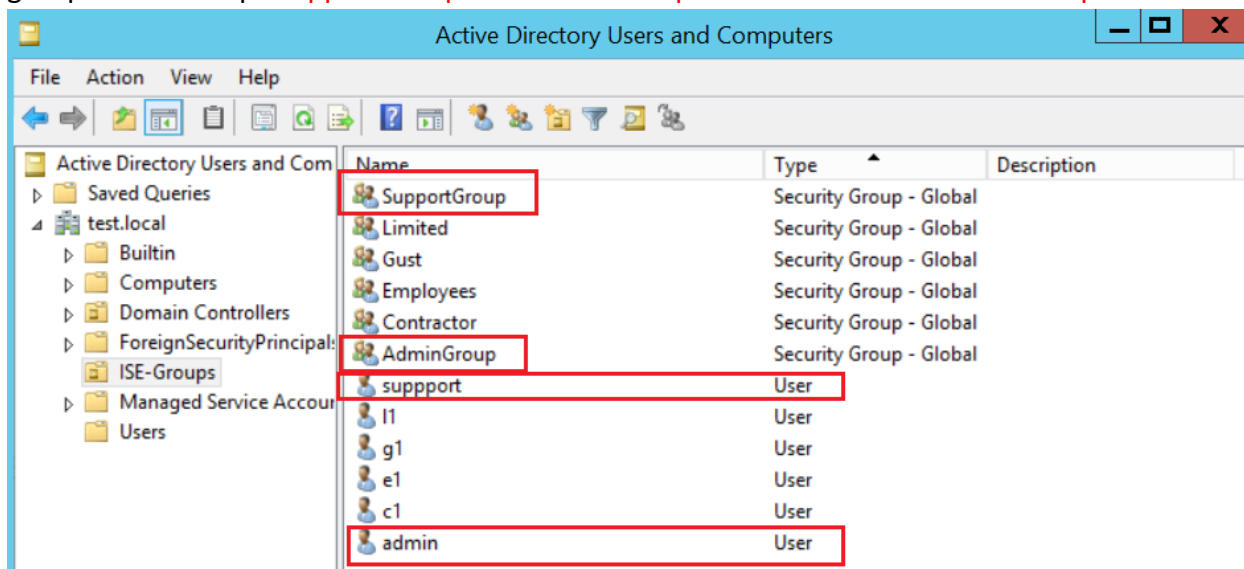


Now the status of Join Point change to **Operational** and list of Domain Controller.

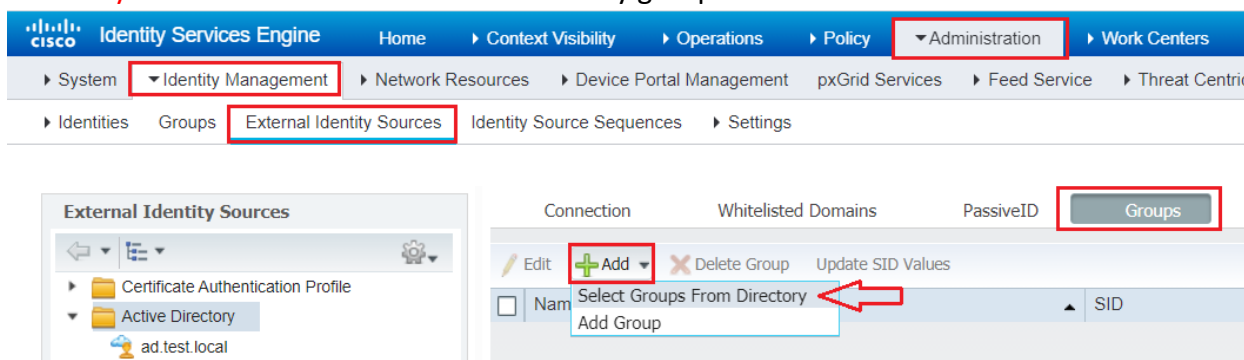
Connection					
Whitelisted Domains					
PassiveID					
Groups					
Attributes					
Advanced Settings					
* Join Point Name <input type="text" value="ad.test.local"/>					
* Active Directory Domain <b>test.local</b>					
<input type="button" value="Join"/> <input type="button" value="Leave"/> <input type="button" value="Test User"/> <input type="button" value="Diagnostic Tool"/> <input type="button" value="Refresh Table"/>					
<input type="checkbox"/> ISE Node	ISE Node Role	Status	Domain Controller	Site	
<input checked="" type="checkbox"/> ise1.test.local	STANDALONE	<input checked="" type="checkbox"/> Operational	srv.test.local	Default-First-Site-Name	

## Create Groups and Users:

Create two groups in Active Directory and for test purpose create two users and add them to groups. Two Groups **SupportGroup** and **AdminGroup** and two users **admin1** and **sup1**



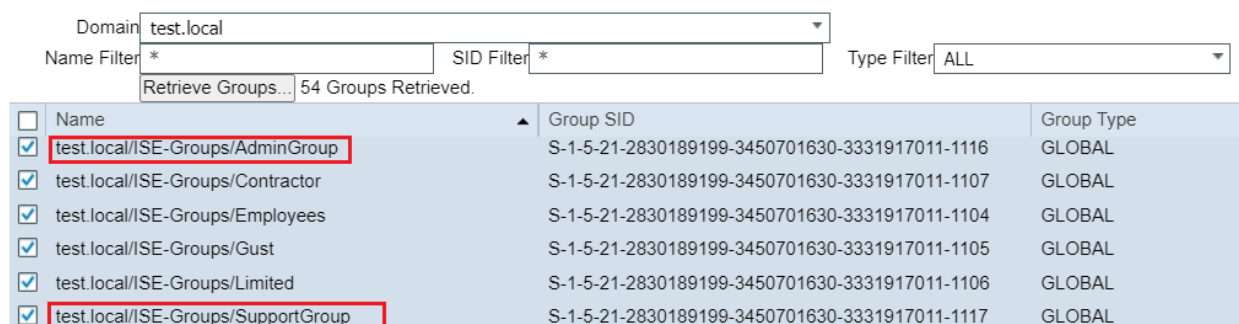
After ISE is joined to domain, Choose **Administration > Identity Management > External Identity Sources > Active Directory**. Click the **Groups** Tab. Click on **Add** and then **Select Groups from Directory**. This is where we add Active Directory groups to ISE for future use.



Used an asterisk to pull up all my AD groups: Check the check boxes next to the groups that you want to be available for use in authorization policies and click **OK**.

### Select Directory Groups

This dialog is used to select groups from the Directory.



## Set ISE to Use AD for Admin Login Authentication:

Now that we've prepared our environment we can begin configuring ISE to use AD for authenticating admins to the ISE admin page. Navigate to **Administration -> System -> Admin Access -> Authentication Method** and change Identity Source to **AD:ad.test.local**

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation path is **Administration > System > Admin Access > Authentication Method**. The **Authentication Method** page is displayed, showing the **Authentication Type** section. The **Password Based** radio button is selected. The **\* Identity Source** dropdown menu is open, showing the selected source **AD:ad.test.local** and other options like **Internal** and **AD:ad.test.local**. The **Save** button is highlighted.

Navigate to **Administration -> System -> Admin Access -> Administrators -> Admin Groups** and click **Add**

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation path is **Administration > System > Admin Access > Administrators > Admin Groups**. The **Admin Groups** page is displayed, showing a table of existing groups. The **Add** button is highlighted.

Name	External Groups Mapped
AdminGroup	1
Customization Admin	0
ERS Admin	0

In the screen that opens enter a group name, check the **External** box, and then select the AD security group you added to ISE earlier **AdminGroup**. Click **Submit**.

**Cisco Identity Services Engine** Home Context Visibility Operations Policy **Administration**

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service

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

Authentication

Authorization

**Administrators**

Admin Users

**Admin Groups**

Settings

Admin Groups > **New Admin Group**

### Admin Group

\* Name



Description

Type ☒ External

#### External Identity Source

Name : ad.test.local

#### External Groups

\*   

Repeat the same for Support Group, enter a group name, check the **External** box, and then select the AD security group you added to ISE earlier **SupportGroup**. Click **Submit**.

**Cisco Identity Services Engine** Home Context Visibility Operations Policy **Administration**

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service

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

Authentication

Authorization

**Administrators**

Admin Users

**Admin Groups**

Settings

Admin Groups > **New Admin Group**

### Admin Group

\* Name



Description

Type ☒ External

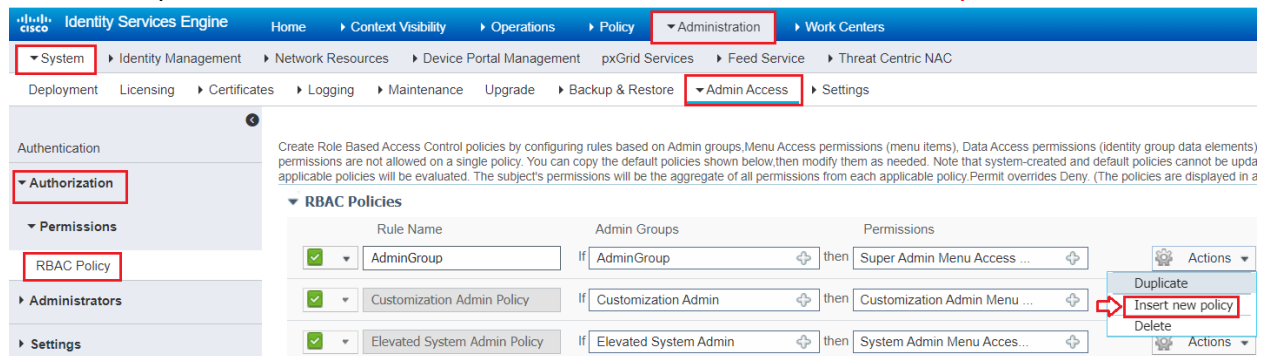
#### External Identity Source

Name : ad.test.local

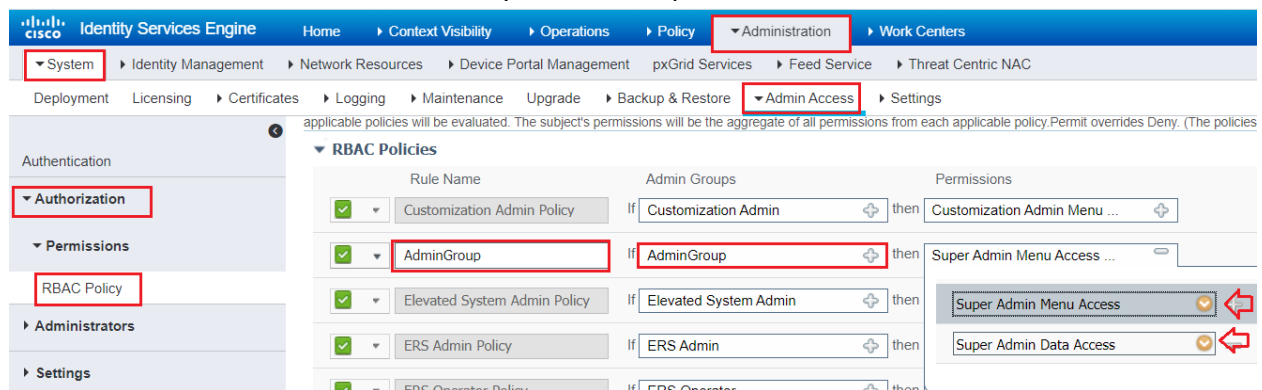
#### External Groups

\*   

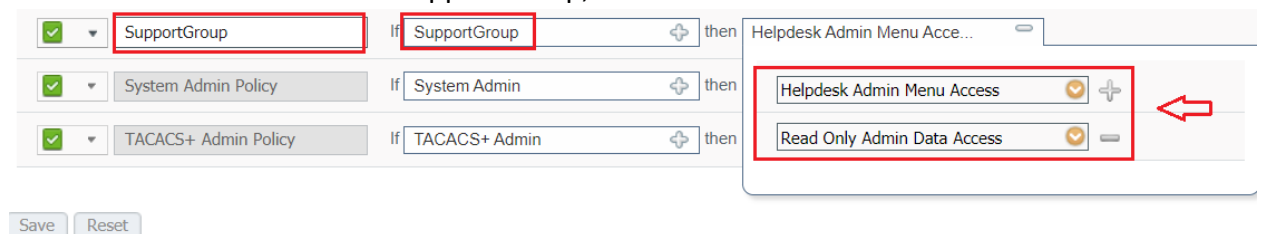
Navigate to **Administration -> System -> Admin Access -> Authorization -> Policy** and click the **Actions** drop down on one of the RBAC Policies and click **Insert New Policy**.



Enter a Rule Name, add the group you created above to the Admin Groups filed, then add both the Menu Access and Data Access for your desired permission level.

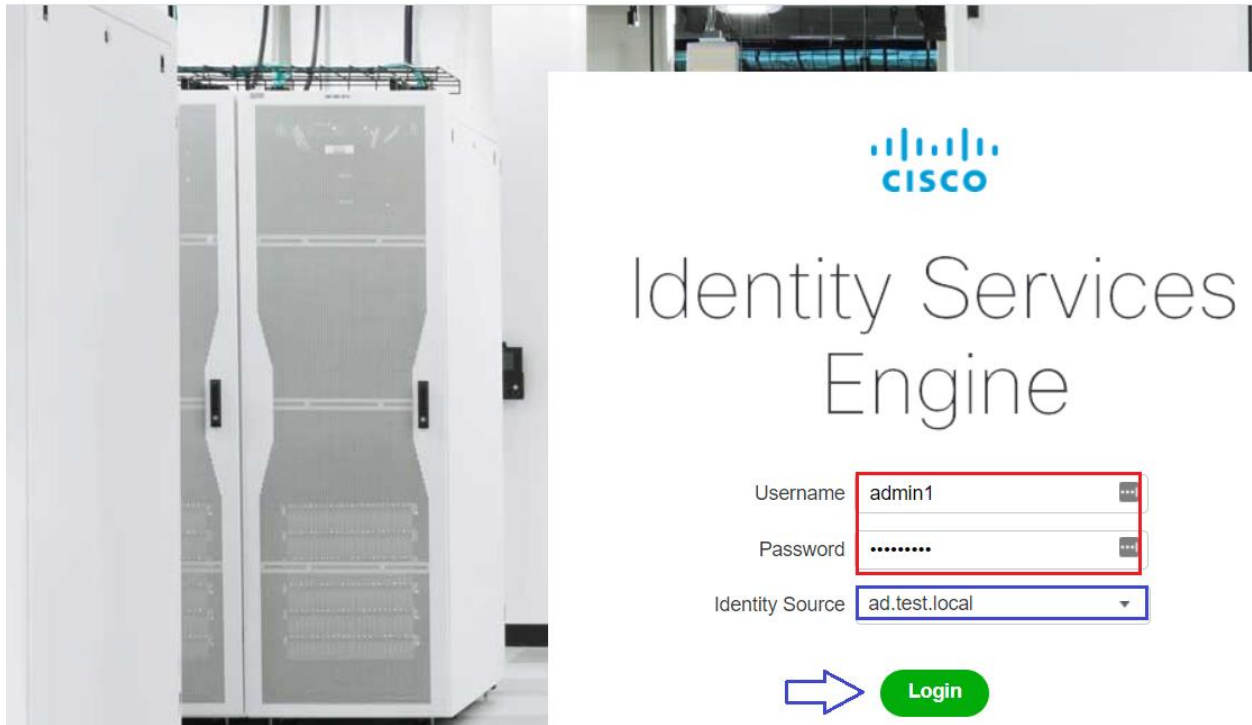


Create new Rule this time for SupportGroup, then add both Menu and Data Access. Click **Save**.



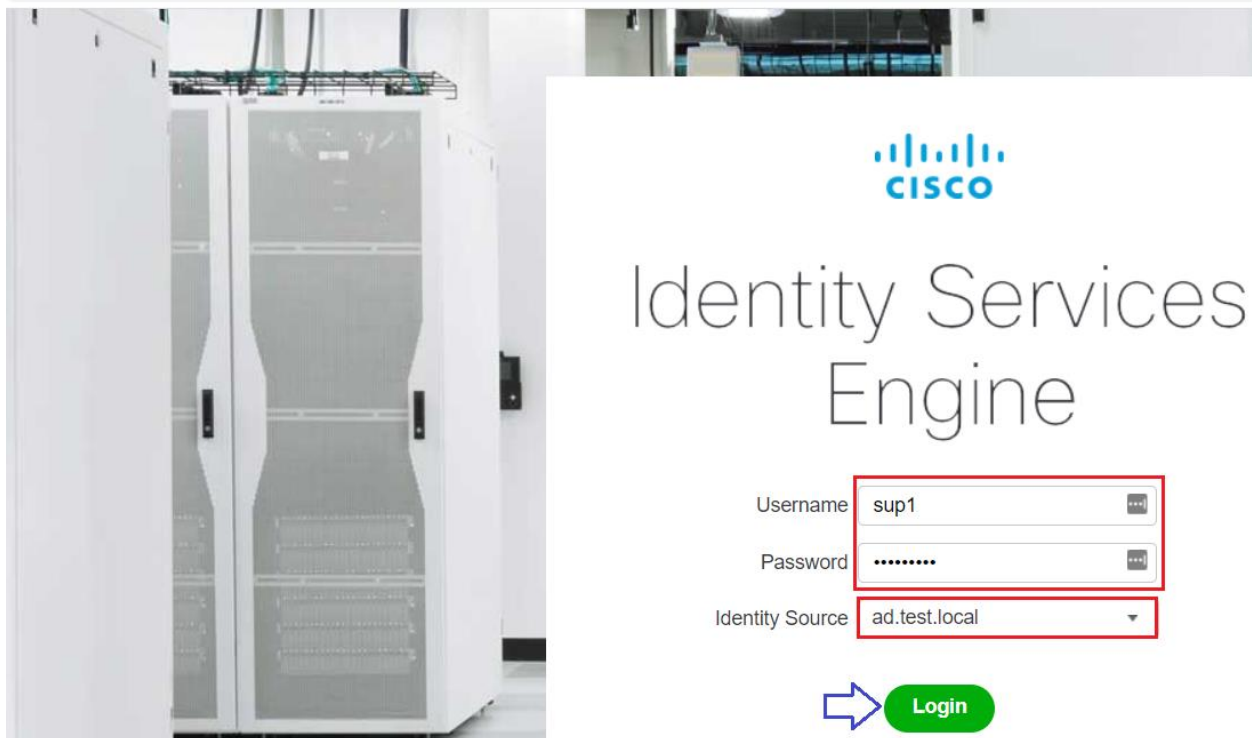
Now, you should be able to log into your ISE server using your domain credentials. Login **AdminGroup** user in this case **admin1** when login he will get full read and write access.





The image shows the Cisco Identity Services Engine (ISE) login page. On the left is a photograph of a server rack. On the right is the login interface. At the top is the Cisco logo. Below it is the title "Identity Services Engine". The login form includes three fields: "Username" with the value "admin1", "Password" with masked characters "\*\*\*\*\*", and "Identity Source" with a dropdown menu showing "ad.test.local". A green "Login" button is at the bottom right, preceded by a blue arrow icon.

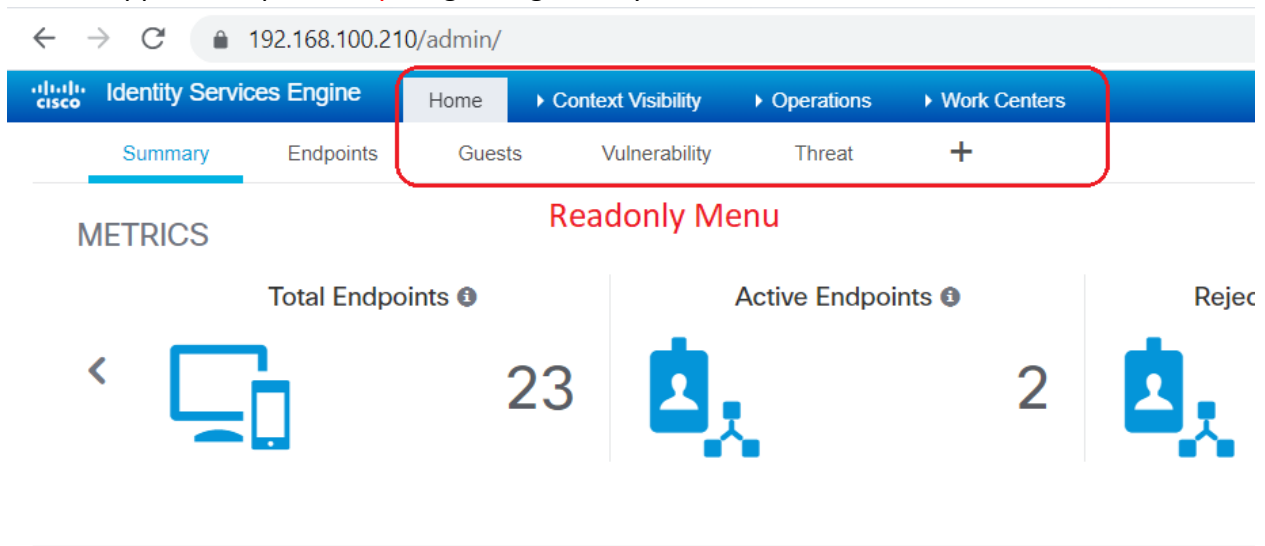
Now, you should be able to log into your ISE server using your domain credentials. Login SupportGroup user in this case **sup1** when login he will get read access.



This image is similar to the one above, showing the Cisco Identity Services Engine login page. The "Username" field now contains "sup1". The "Password" field is masked with "\*\*\*\*\*". The "Identity Source" dropdown still shows "ad.test.local". The "Login" button and blue arrow icon remain at the bottom right.



When SupportGroup user **sup1** login he gets only limited access and Manu.



Should you ever have troubling logging in using domain credentials you can click the drop down after your domain in the Identity Source screen and choose Internal. You can then sign in using the local admin account you created at install.

