



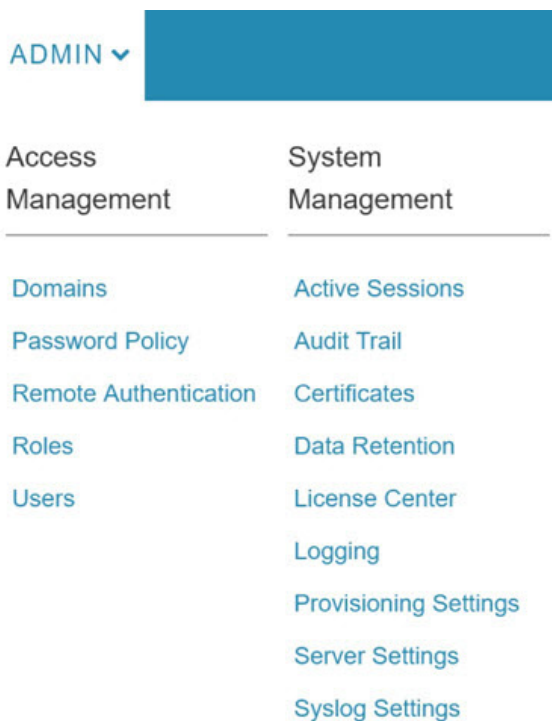
Managing User Access

This section has the following topics for managing users and roles in IoT FND:

- [Managing the Password Policy](#)
- [Configuring Remote Authentication](#)
- [Managing Roles and Permissions](#)
- [Managing Users](#)

All user management actions are accessed through the **Admin > Access Management** menu ([Figure 1](#)).

Figure 1 Admin Menu



Managing the Password Policy

IoT FND provides default password policy values that you can enforce among IoT FND users.

Note: To modify these values, you must be logged in either as root or as a user with Administrative Operations permissions.

Caution: In some cases, changing password policies immediately terminates all user sessions and resets all passwords.

Note: The “Password history size” and “Max unsuccessful login attempts” policies do not apply to IoT FND North Bound API users.

These changes *invalidate* all user sessions and expire their passwords (including the root user):

- When you increase the minimum length of passwords
- When you decrease the password expiry interval
- When you enable “**Password cannot contain username or reverse of username**”
- When you enable “**Password cannot be cisco or ocsic (cisco reversed)**”
- When you enable “**No character can be repeated more than three times consecutively in the password**”
- When you enable “**Must contain at least one character from all the character sets (upper-case, lower-case, digits and special characters)**”

To edit password policies:

1. Choose **ADMIN > Access Management > Password Policy**.

Policy	Value	Status	Terminate Session and Reset Password
Password minimum length	6	Enabled	Yes, if minimum password length is increased.
Password history size	4	Disabled	
Max unsuccessful login attempts	5	Enabled	
Password expire interval (days)	180	Disabled	Yes, if password expire interval is reduced.
Password cannot contain username or reverse of username		Disabled	Yes, if changed to Enabled state.
Password cannot be cisco or ocsic (cisco reversed)		Disabled	Yes, if changed to Enabled state.
No character can be repeated more than three times consecutively in the password		Disabled	Yes, if changed to Enabled state.
Must contain at least one character from all the character sets (upper-case, lower-case, digits and special characters)		Disabled	Yes, if changed to Enabled state.

2. To enable or disable a policy, choose the appropriate option (**Enabled** or **Disabled**) from the Status drop-down menu.
3. To modify the value of a policy, if applicable, enter the new value in the Value field.

Note: IoT FND supports a maximum password length of 32 characters.

4. Click **Save** to start enforcing the new policies.

Note: The password policy you configure in IoT FND applies only to local users and not to remote Active Directory (AD) users. The password policy for AD users is determined and enforced by the AD admin.

Configuring Remote Authentication

To configure remote authentication for IoT FND, you need to perform the configurations steps (listed below) in Active Directory (AD) and IoT FND.

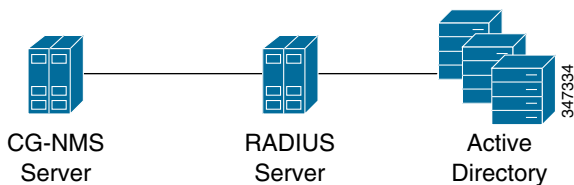
- [Support for Remote Authentication](#)
- [Configuring Remote Authentication in AD](#)
- [Configuring Security Policies on the RADIUS Server](#)

- [Configuring Remote Authentication in IoT FND](#)
- [Enabling and Disabling Remote User Accounts](#)
- [Deleting Remote User Accounts](#)
- [Logging In to IoT FND Using a Remote User Account](#)

Support for Remote Authentication

With Remote Authentication, it is easier to integrate IoT FND into an existing AD and Network Policy Server (NPS) infrastructure. This allows administrators to configure IoT FND access for users in AD.

When you configure remote authentication in IoT FND, it hands over the authentication and authorization responsibility to AD and NPS. AD performs user authentication to check the validity of user credentials. The RADIUS server performs user authorization to check whether a user belongs to a group that defines the user role. If so, the server returns the role name to IoT FND.



The following is the flow of user authentication and authorization by AD and NPS:

1. The user enters their credentials.
 - If user was created locally on the NMS server, authentication and authorization occurs locally.
 - If IoT FND determines that the user is a remote user, authentication and authorization occurs on the configured RADIUS server.
 - If remote authentication is not configured, authentication fails and user is denied access.
2. For remote users, if authentication and authorization are successful, the assigned user role returns to the NMS server from the RADIUS server.
3. If the role that returns is valid, the user is granted access.

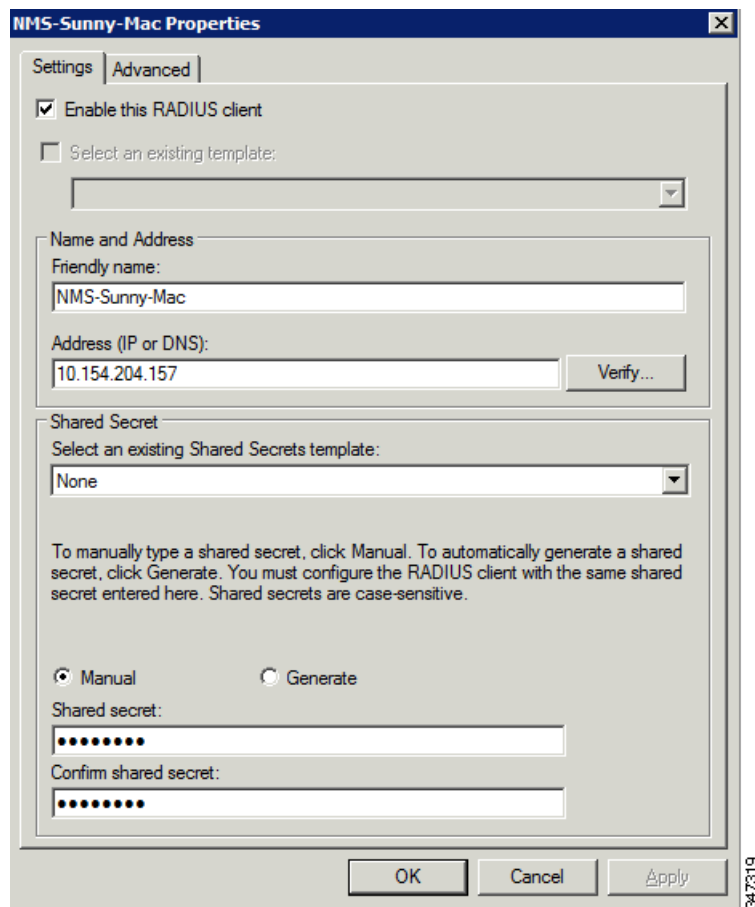
Note: When remote authentication is enabled, user management is done in AD. If an AD user logs in who was deleted from IoT FND, their profile is added back to IoT FND. To prevent access to IoT FND, their AD user profiles must first be deleted from AD.

Configuring Remote Authentication in AD

To allow IoT FND to remotely authenticate users, configure the following within Active Directory

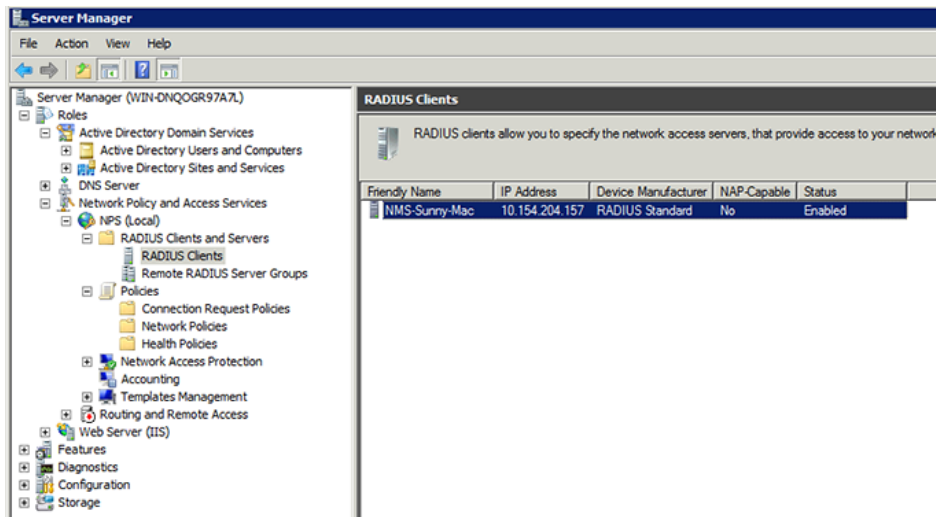
1. Log in to NPS.
2. Add IoT FND as a radius client on the RADIUS server.

Provide a friendly name, and IP address or DNS name of the IoT FND server and configure the shared secret that IoT FND uses to connect to the RADIUS server.



347319

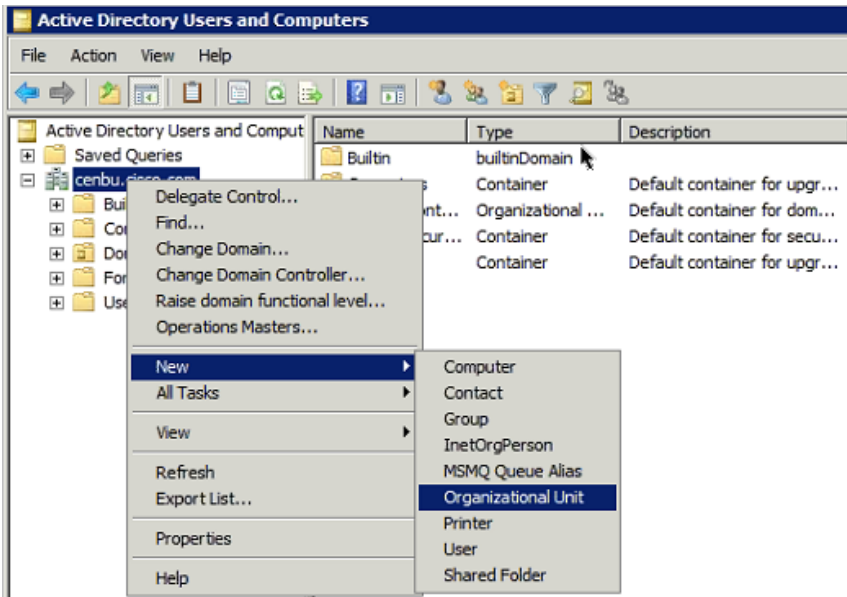
An entry for the RADIUS client appears under RADIUS Clients and Servers.



347318

3. Log in to AD and create an Organizational Unit.

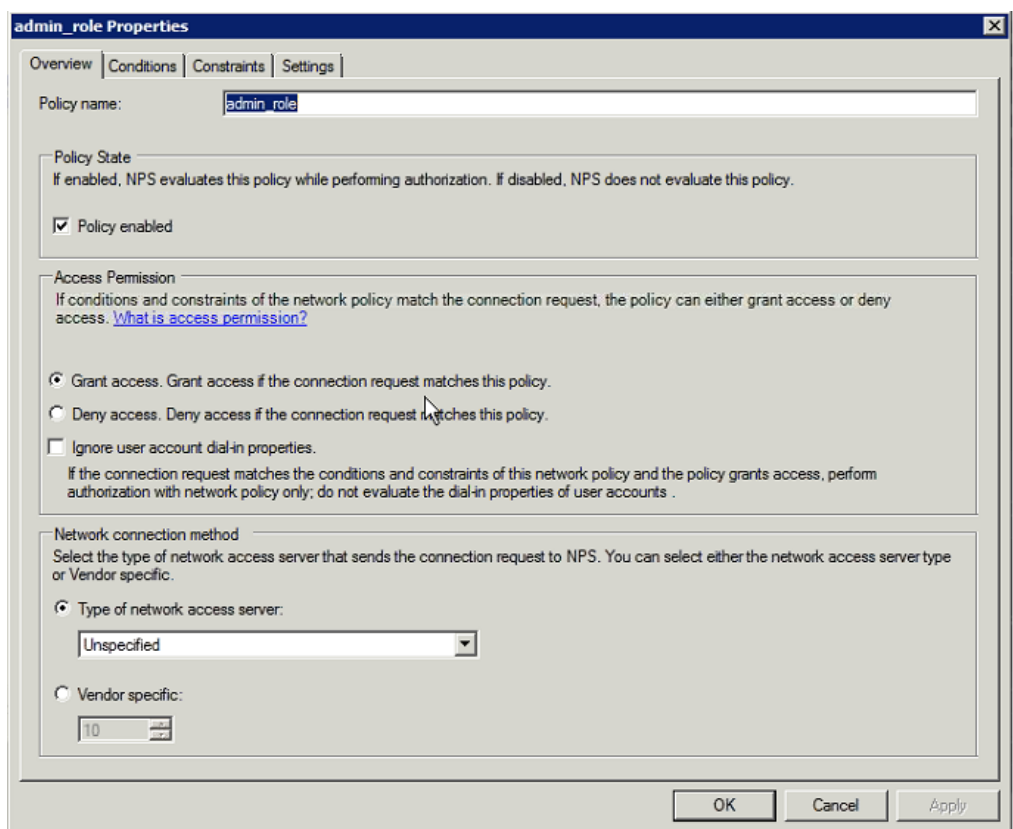
Cisco recommends that you create all security groups (IoT FND roles) within this Organizational Unit.



347328

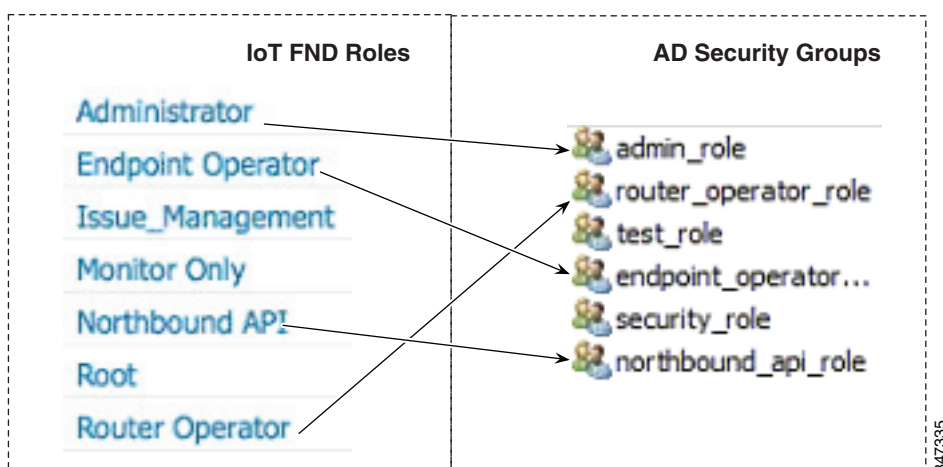
4. Add security groups corresponding to IoT FND roles to the Organizational Unit.

The following example shows the security groups defined in the NMS_ROLES Organizational Unit.



Tip: When creating the security groups, ensure that they map one-to-one to IoT FND roles (that is, every role defined in IoT FND maps to only one AD security group). The name of the security group does not have to match a role name in IoT FND, but for organizational purposes, Cisco recommends using names that correlate the security group name to a IoT FND role.

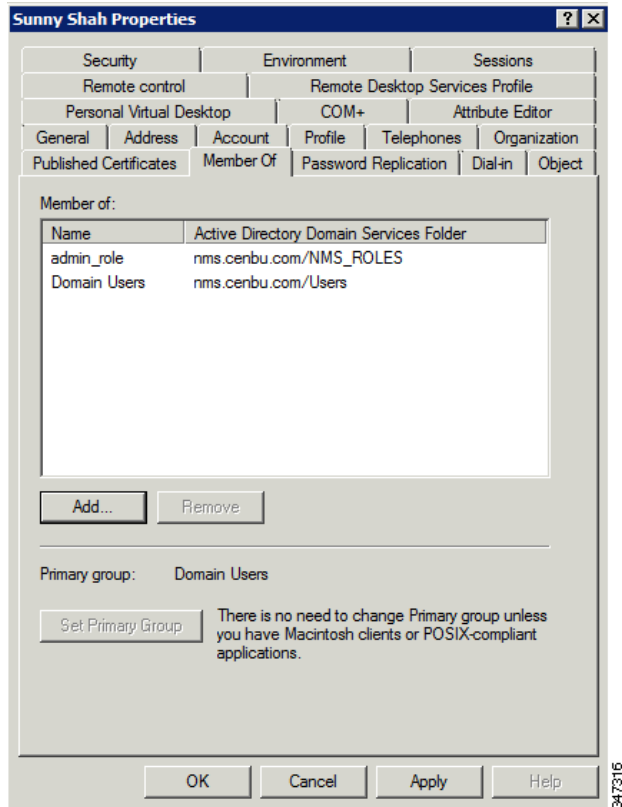
Note: You cannot create or assign the IoT FND root role in AD.



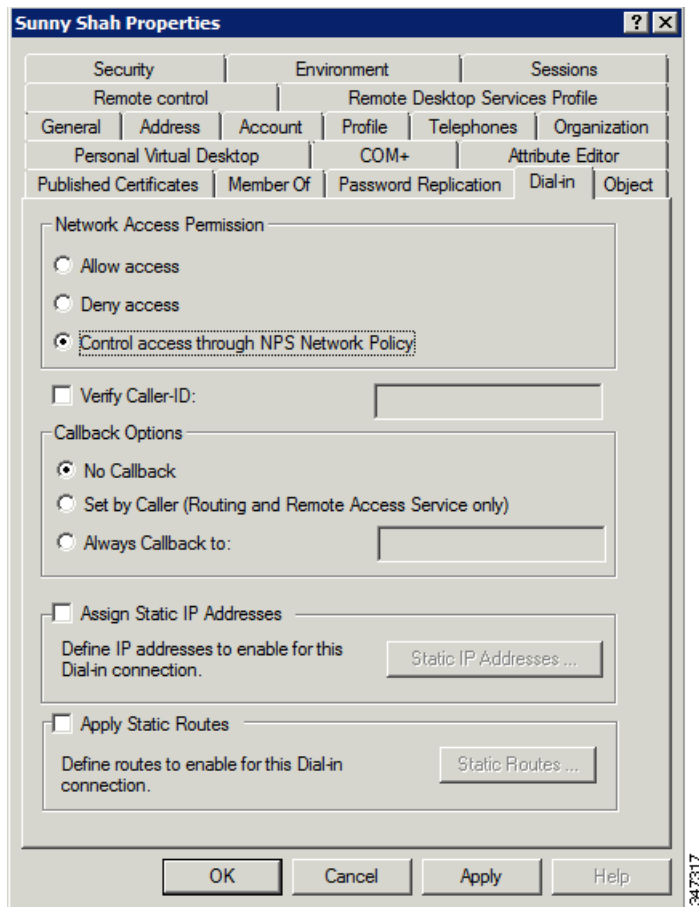
5. Assign AD users a role by adding them to the security group mapping to that role.

Since, users can only belong to one security group, the IoT FND role that the user is assigned after log in is dependent on their assigned AD security group.

Tip: In AD, users cannot be assigned multiple IoT FND roles, and cannot belong to multiple security groups. To assign permissions from more than one role to a group of users, create a new IoT FND role with the required permissions, and create the corresponding AD security group. Users in this new group can then carry out the tasks allowed by this role.



6. Configure the Dial-in Network Access Permission to use the NPS Network Policy.

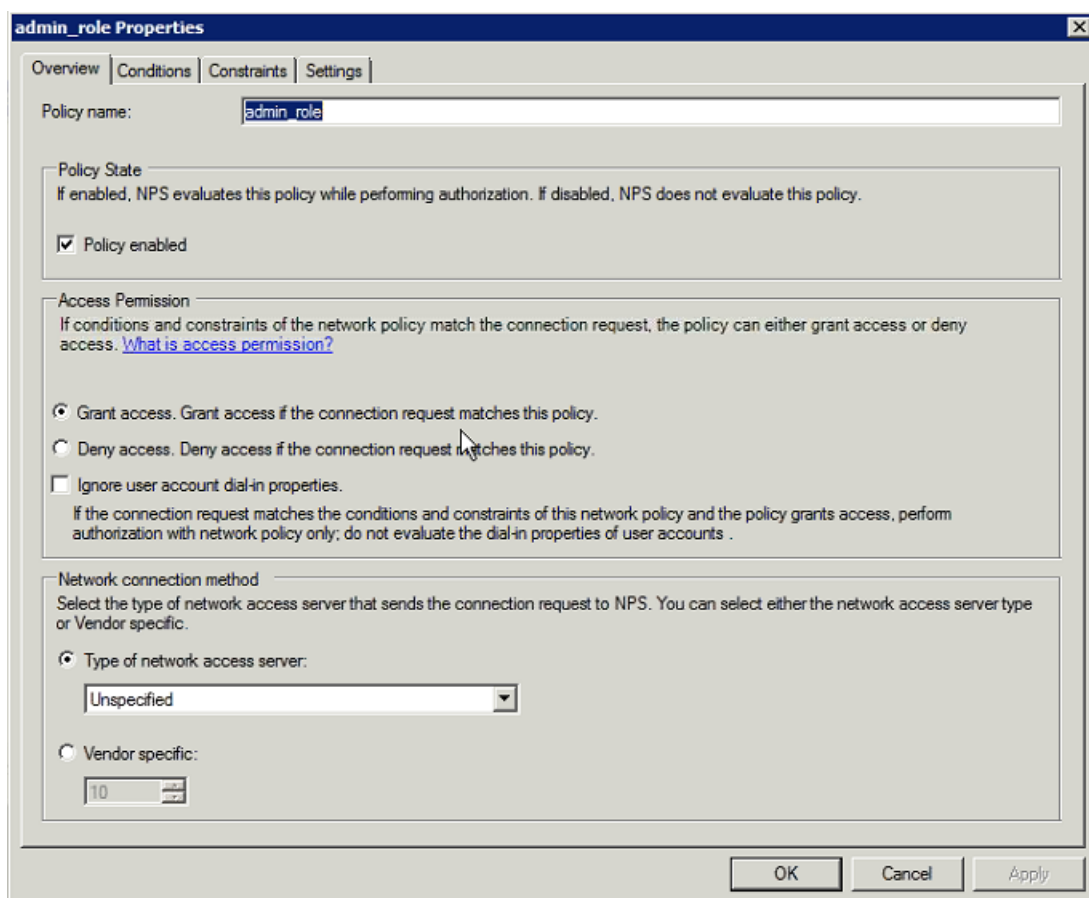


Configuring Security Policies on the RADIUS Server

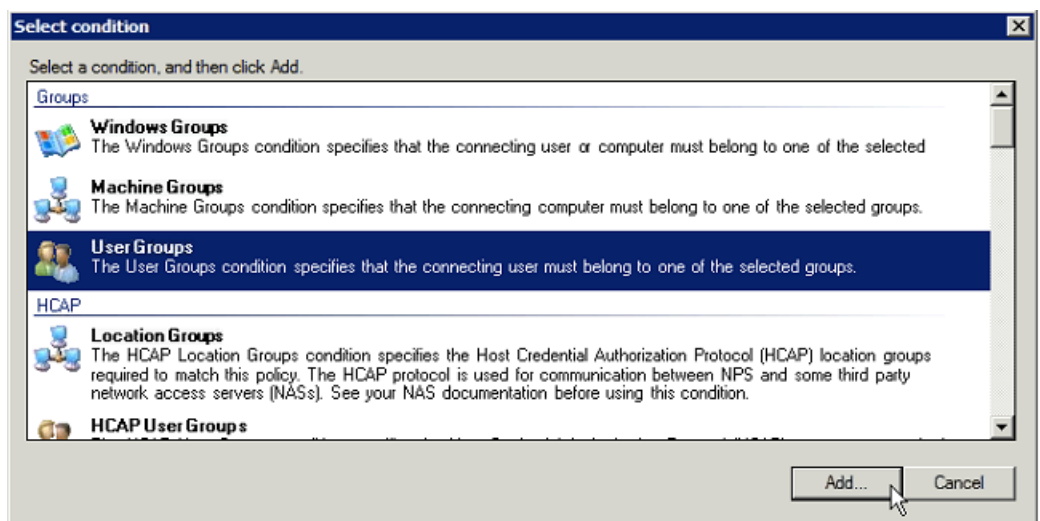
To authorize users for IoT FND access, configure security policies for the RADIUS server.

To configure security policies on the RADIUS server, follow these steps:

1. Create a network policy for each security group you created in AD.
2. Configure the policy as follows:
 - a. In the Overview pane, define the policy name, enable it, and grant access permissions.

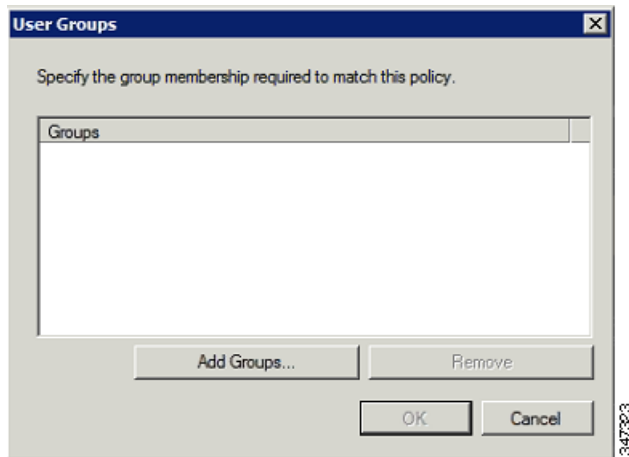


- b. Click the **Conditions** tab, select the **User Groups** condition, and click **Add**.

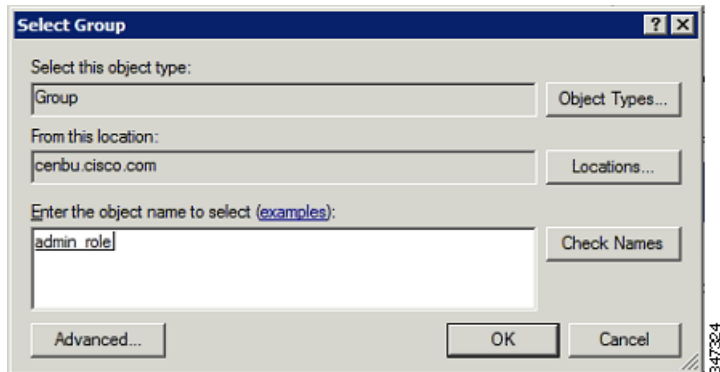


The User Groups condition specifies that the connecting user must belong to the selected group. For this policy to pass, the user being authorized must belong to the user group configured in this policy.

- c. In the User Groups window, click **Add Groups**.

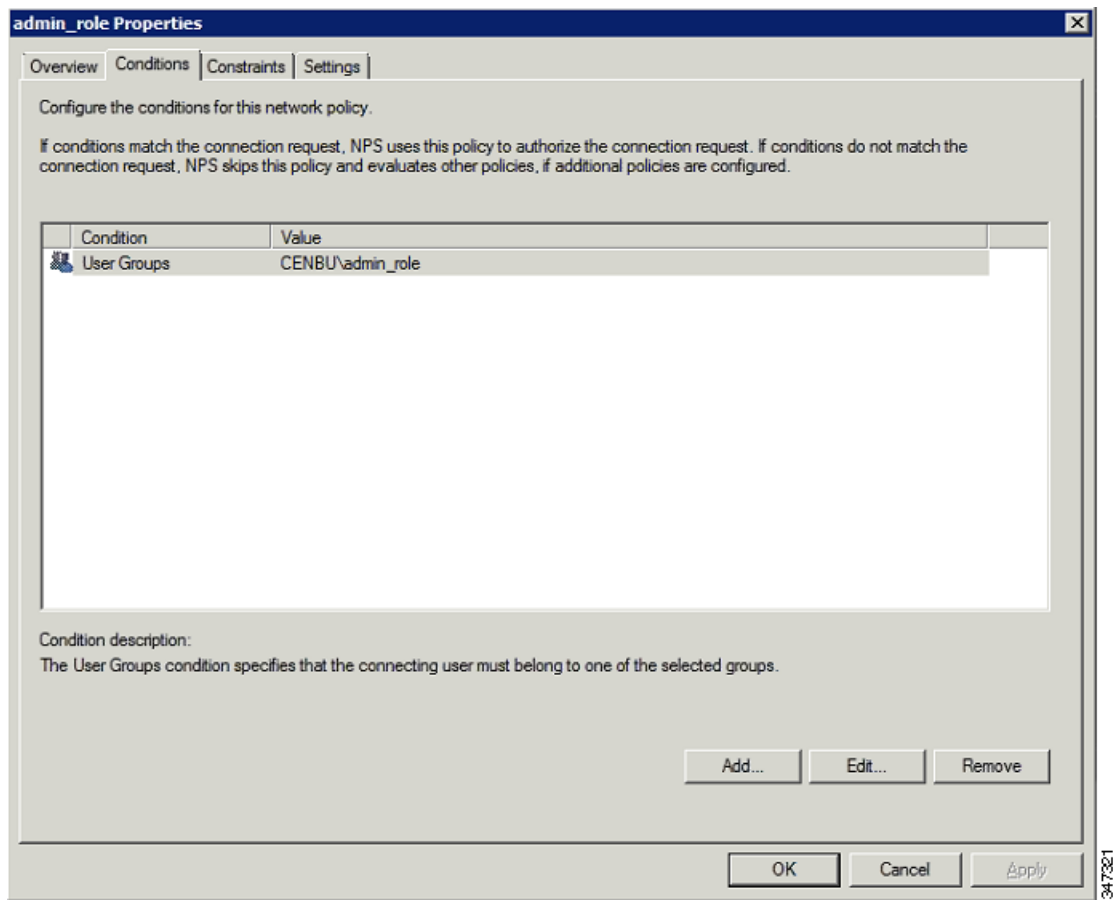


- d. In the Select Group window, enter the name of the group
- e. Click **OK** to close the Select Group dialog box, and then click **OK** to close the User dialog box.



- f. Click **Cancel** to close the Select condition window.

The condition appears in the Conditions pane.



- g. Click the **Settings** tab, and then click **Add** to display the Attribute Information window.

Add Vendor Specific Attribute

To add an attribute to the settings, select the attribute, and then click Add.

To add a Vendor Specific attribute that is not listed, select Custom, and then click Add.

Vendor:

Cisco

Attributes:

Name	Vendor
Cisco-AV-Pair	Cisco

Description:

Specifies the Cisco AV Pair VSA.

Add... Close

347331

- h. Click **Add** to define a Vendor Specific Attribute (VSA) that is sent to IoT FND (RADIUS client) after the user credentials and security group membership are verified.

The VSA to configure is:

- Attribute Name: Cisco-AV-Pair
- Attribute number: 5000
- Attribute format: String.
- Attribute value: Enter the attribute value to send to IoT FND.

Attribute Information

Attribute name:

Cisco-AV-Pair

Attribute number:

5000

Attribute format:

String

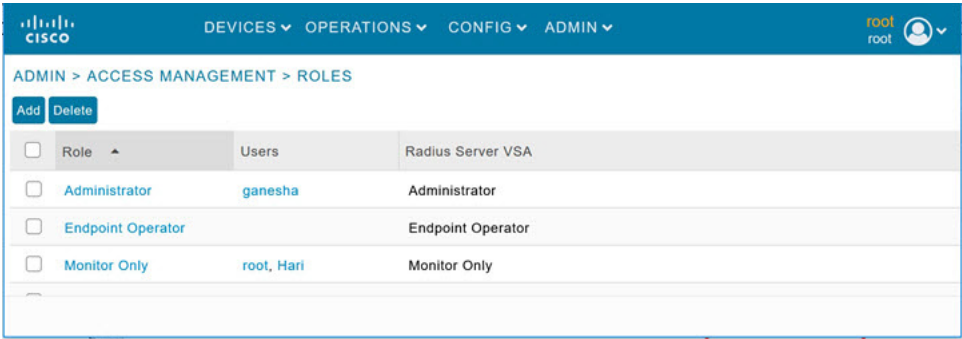
Attribute value:

Administrator

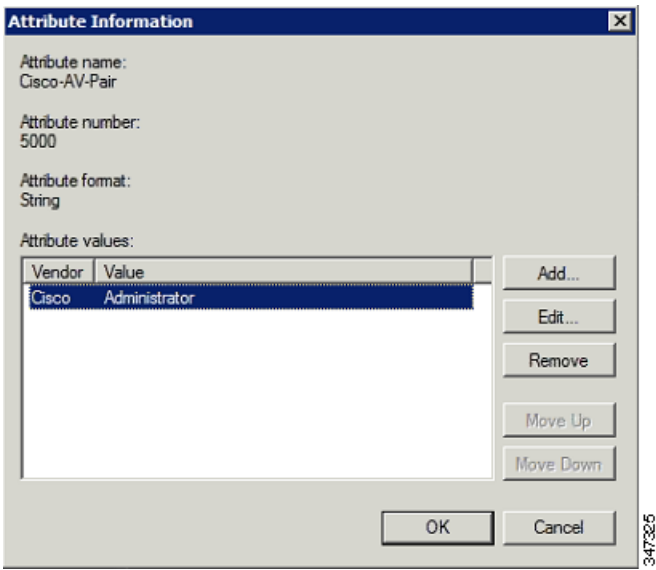
OK Cancel

347326

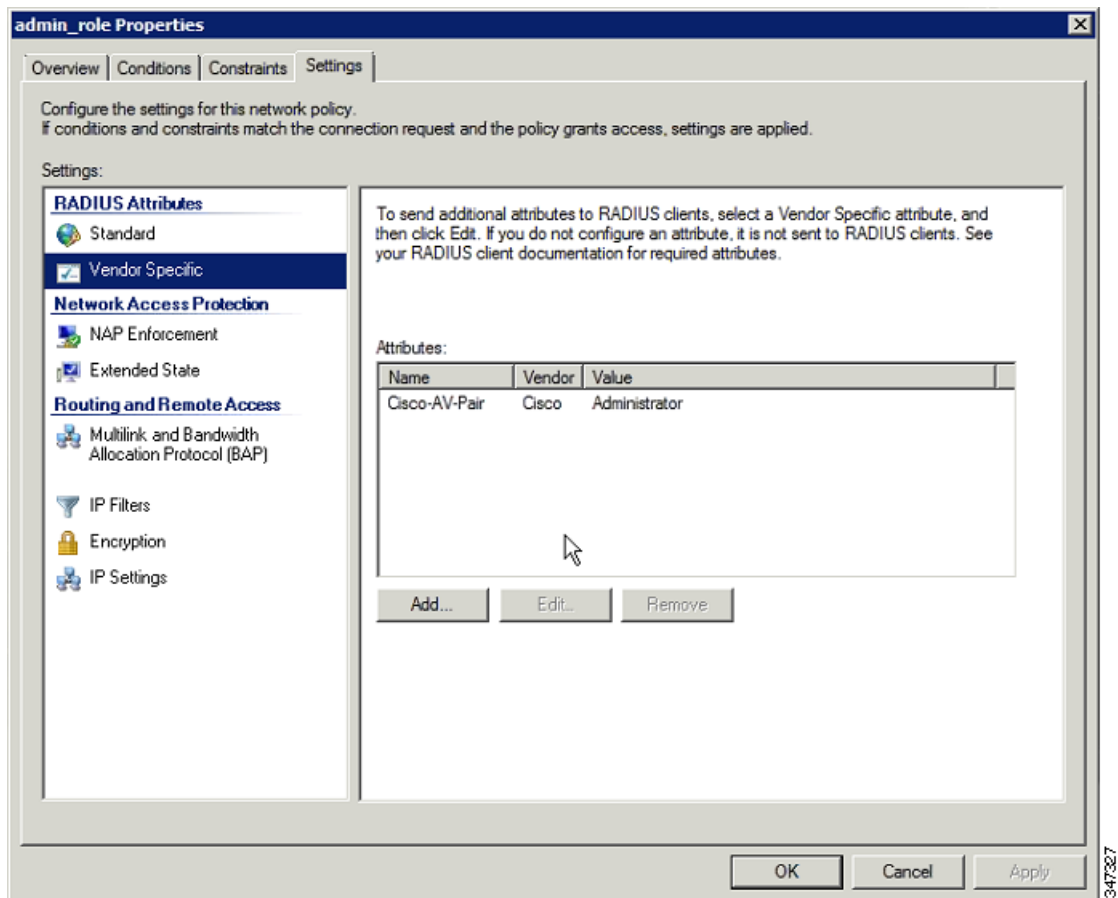
Note: The string entered in the Attribute value field must be the exact string listed in the Radius Server VSA column on the Roles page in IoT FND (**ADMIN > Access Management > Roles**).



i. Click **OK**.



The VSA attribute appears in the Settings pane.



j. Click **OK**.

Configuring Remote Authentication in IoT FND

You enable remote user authentication and configure RADIUS server settings on the Remote Authentication page (**Admin > Access Management > Remote Authentication**).

To configure remote authentication:

1. Choose **ADMIN > Access Management > Remote Authentication**.
2. Check the **Enable Remote Authentication** check box.
3. Enter this information about the RADIUS server:

Field	Description
IP	The IP address of the RADIUS server.
Radius Server Description	A descriptive name of the RADIUS server.
Shared Secret	The shared secret you configured on the RADIUS server.
Confirm Shared Secret	
Authentication Port	The RADIUS server port that IoT FND uses to send request to. The default port is 1812.

Field	Description
Accounting Port	The RADIUS server accounting port. The default port is 1813.
Retries	The number of times to send a request to the RADIUS server before IoT FND times out and remote authentication fails because no response was received from the RADIUS server.
Timeout (seconds)	The number of seconds before IoT FND times out and remote authentication fails because no response was received from the RADIUS server.

4. To ensure that IoT FND can reach the RADIUS server, click **Test Connectivity**.

a. Enter your Remote (AD) username and password.

b. Click **Submit**.

The results of the configuration test displays.

c. Click **OK**.

5. Click **Save** when done.

Enabling and Disabling Remote User Accounts

In IoT FND you cannot enable or disable remote AD user accounts. To enable or disable remote AD user accounts, use your AD server.

Deleting Remote User Accounts

In IoT FND, you can delete remote user accounts. However, this only removes the user from the IoT FND Users page (**ADMIN > Access Management > Users**); it does not delete the user account from AD. If a deleted user logs in to IoT FND and AD authentication is successful, an entry for the user is added to the IoT FND Users page.

Logging In to IoT FND Using a Remote User Account

Logging in to IoT FND using a remote AD user account is transparent to the user. In the background, IoT FND checks whether the account is local, and for remote users sends an authentication request to the RADIUS server configured on the Remote Authentication page (**ADMIN > Access Management > Remote Authentication**). If both authentication and authorization are successful, IoT FND adds an entry for the user in the Users page (**ADMIN > Access Management > Users**).

Unlike entries for local users on the Users page, the user name filed in remote user entries is not a link. You cannot click the name of a remote user to obtain more information about the user.

Note: Remote users cannot be managed through IoT FND. If a remote user wants to update their password, they must use their organization's AD password update tool. Remote users cannot update their password using IoT FND.

Managing Roles and Permissions

Roles define the type of tasks specific role IoT FND users can perform. The operations the user can perform are based on the permissions enabled for the role This section has the following topics:

- [Adding Roles](#)
- [Deleting Roles](#)
- [Editing Roles](#)

■ Viewing Roles

IoT FND lets you assign a system-defined role to a user such as admin or operator (**ADMIN >Access Management > Roles**). The operations the user can perform are based on the permissions enabled for the role. The following topics are discussed in this section:

- Basic User Permissions
- System-Defined User Roles
- Custom User Roles

Basic User Permissions

Table 1 describes basic IoT FND permissions.

Table 1 IoT FND User Permissions

Permission	Description
Add/Modify/Delete Devices	Allows users to import, remove and change router and endpoint devices.
Administrative Operations	Allows users to perform system administration operations such as user management, role management, and server configuration settings.
Asset Management	Allows users to view details on Assets (non-Cisco equipment) that are associated with an FND managed device.
BACT Operations	Special Battery powered meters managed by CAM. The interaction with these endpoints should be kept to a minimum in order to reduce draw down of battery within the endpoints.
Device Manager User	Permission for IoT-DM user (field technician) to retrieve a Work Order from FND through the Work Order NB APIs.
Endpoint Certificate Management	Permission for erasing node certificates on IR500 gateways.
Endpoint Configuration	Allows users to edit configuration templates and push configuration to mesh endpoints.
Endpoint Firmware Update	Allows users to add and delete firmware images and perform ME firmware update operations.
Endpoint Group Management	Allows users to assign, remove and change devices from ME configuration and firmware groups.
Endpoint Reboot	Allows users to reboot the ME device.
GOS Application Management	Allows uses to add and delete Guest OS applications.
Issue Management	Allows users to close issues.
Label Management	Allows users to add, change, and remove labels.
LoRA Modem Reboot	Permission for rebooting LoRaWAN gateways and modems.
Manage Device Credentials	Allows users to view router credentials such as WiFi pre-shared key, admin user password, and master key.
Manage Head-End Devices Credentials	Allows users to view the ASR admin NETCONF password.
NBAPI Audit Trail	Allows users to query and delete audit trails using IoT FND NB API.
NBAPI Device Management	Allows users to add, remove, export, and change router and endpoint devices using IoT FND NB API.
NBAPI Endpoint Group Management	Permission for accessing the Group Management NB API.
NBAPI Endpoint Operations	Allows users to manage endpoint operations using IoT FND NB API.
NBAPI Event Subscribe	Allows users to search events, subscribe and unsubscribe from events (including Outage events) using IoT FND NB API.

Table 1 IoT FND User Permissions (continued)

Permission	Description
NBAPI Issues	Allows users to search issues.
NBAPI Orchestration Services	Permission for IOK Orchestration Service to access the Orchestration NB APIs.
NBAPI Reprovision	Allows users to reprovision devices using IoT FND NB API.
NBAPI Rules	Allows users to search, create, delete, activate, and deactivate rules using IoT FND NB API.
NBAPI Search	Allows users to search devices, get device details, group information, and metric history using IoT FND NB API.
NB API Tunnels	Permission for accessing the Tunnel Status NB APIs.
Password Policy	Provides a flexible password policy system to manage user passwords. It contains configurable properties for password expiration, failed login attempts, password strength and other aspects of password maintenance.
Router Configuration	Allows users to edit router configuration templates and push configuration to routers.
Router File Management	Permission for managing router files on the Device File Management GUI page.
Router Firmware Update	Allows users to add and delete firmware images and perform firmware update operations for routers.
Router Group Management	Allows users to assign, remove, and change device assignments to router configuration and firmware groups.
Router Reboot	Allows users to reboot the router.
Rules Management	Allows users to add, edit, activate, and deactivate rules.
Security Policy	Allows users to block mesh devices, refresh mesh keys, and so on.
Tunnel Provisioning Management	Allows users to manage tunnel groups, edit/apply tunnel-related templates, and perform factory reprovisioning.
View Device Configuration	Allows users to view field device configuration.
View Head-end	Allows users to view ASR configuration, tunnel provisioning, and HER events.
View Work Orders	Allows users to view work orders.
Work Order Management	Allows users to manage work orders for IoT-Device Manager (IoT-DM).

System-Defined User Roles

Note: The system-defined Root role cannot be assigned to users.

[Table 2](#) lists system-defined roles. These roles cannot be modified.

Table 2 System-defined User Roles

Role	Description
Administrator	This role combines these basic permissions: <ul style="list-style-type: none"> ■ Administrative Operations ■ Label Management ■ Rules Management
Endpoint Operator	This role combines these basic permissions: <ul style="list-style-type: none"> ■ Label Management ■ Endpoint Configuration ■ Endpoint Firmware Update ■ Endpoint Group Management ■ Endpoint Reboot
Monitor Only	Optional role. This role is not defined for every user.
North Bound API	This role combines these basic permissions: <ul style="list-style-type: none"> ■ NB API Audit Trail ■ NB API Device Management ■ NB API Endpoint Operations ■ NB API Event Subscribe ■ NB API Orchestration Service ■ NB API Rules ■ NB API Search
Root	The system-defined root role cannot be assigned to users. This role can use the password utility to reset the password for any IoT FND user.
Router Operator	This role combines these basic permissions: <ul style="list-style-type: none"> ■ Label Management ■ Router Configuration ■ Router Firmware Update ■ Router Group Management ■ Router Reboot

Custom User Roles

In IoT FND you can define custom roles. For each role you create, you can assign it one or more basic user permissions (see [Table 1](#)). These permissions specify the type of actions users with this role can perform.

Adding Roles

To add IoT FND user roles:

1. Choose **ADMIN > Access Management > Roles**.
2. Click **Add**.
3. Enter the name of the role.
4. Check the appropriate check boxes to assign permissions.
5. Click **Save**.
6. To continue to add roles, click **Yes**; otherwise, click **No** to return to the Roles page.

Deleting Roles

Note: You cannot delete a custom role if it is in use.

To delete IoT FND user roles:

1. Choose **ADMIN > Access Management > Roles**.
2. Check the check boxes of the roles to delete.
3. Click **Delete**.
4. Click **Yes**.
5. Click **OK**.

Editing Roles

Note: You cannot edit system-defined roles, but you can edit custom roles.

To edit IoT FND custom roles:

1. Choose **ADMIN > Access Management > Roles**.
2. Click the role to edit.
3. Make changes to the permission assignments by checking or unchecking the relevant check boxes.
4. Click **Save**.

Viewing Roles

To view IoT FND user roles:

1. Choose **ADMIN > Access Management > Roles**.

For every role, IoT FND lists the Users assigned to this role and the RADIUS Server VSA.

2. To view permission assignments for the role, click the role link.

Managing Users

This section has the following topics on managing users:

- [Resetting Passwords](#)
- [Viewing Users](#)
- [Adding Users](#)
- [Deleting Users](#)
- [Enabling Users](#)
- [Disabling Users](#)
- [Editing Users](#)

Resetting Passwords

As the root user of the Linux server on which IoT FND runs, you can reset your password and use the password utility to reset the password for any other IoT FND user.

To reset a password, enter this command:

```
[root@yourname-lnx1 bin]#./password_admin.sh root
```

IoT FND manages its own user account database; therefore, you must add all new local users from the IoT FND user interface at the **Admin > Access Management > Users** page. Remote users are automatically added to the database. You can also enable, disable, edit, or delete users on this page.

A user with a disabled account cannot log in until an administrator enables their account. After a user account is active, the user must reset their password. There is no limit to the number of users that you can define on the system other than the available database storage.

Viewing Users

To view IoT FND users, open the Users page (**ADMIN > Access Management > Users**).

IoT FND displays this information about users:

Field	Description
User Name	Specifies the user name.
Default Domain	Shows the default domains for each user.
Enabled	Indicates whether the user account is enabled.
Time Zone	Specifies the user's time zone.
Roles	Specifies the roles assigned to the user.
Audit Trail	A link to the user's audit trail.
Remote User	Indicates whether the user account is stored locally. If the value is false, the user account is stored in Active Directory and is accessed via the RADIUS server configured in the Remote Authentication page (ADMIN > Access Management > Remote Authentication).

Adding Users

To add users to IoT FND:

1. Choose **ADMIN > Access Management > Users**.
2. Click **+** icon to **Add User**.
3. Enter the following user information:

Field	Description
User Name	Enter the user name.
New Password	Enter the password. The password must conform to the IoT FND password policy.
Confirm Password	Re-enter the password.
Time Zone	Choose a time zone from the drop-down menu.

4. Click **Assign Domain** to open the configuration panel:
 - Select the domain name from the drop-down menu
 - Assign Role(s) and its associated Permission for the user by selecting the role check box.

5. Click **Assign** to save the entries.

IoT FND creates a record for this user in the IoT FND database.

6. To add the new user, click the **Disk** icon; otherwise, click **X** to close the window and return to the Users page.

Note: A new user account is enabled by default. This means that the user can access IoT FND.

You can make future edits to the User entry by selecting the **Edit** or **Delete** buttons that appear under the Actions column.

Deleting Users

Deleting user accounts removes user preferences such as the default map location from the system. Disable a user account to temporarily deactivate it.

To delete users from IoT FND:

1. Choose **ADMIN > Access Management > Users**.
2. Check the box next to the User Name entry that you want to remove from the User Account list.
3. To delete the entry, click the **trash can** icon.
4. To confirm action, click **Yes**.

Enabling Users

You must enable the user account for users to access IoT FND. When users log in for the first time, IoT FND prompts them to change their password.

To enable user accounts in IoT FND:

1. Choose **Admin > Access Management > Users**.

2. Check the check boxes for the user account(s) to enable.
3. Click the **solid person** icon.
4. To confirm action, click **Yes**.

Disabling Users

To prevent users from accessing IoT FND, disable their accounts. Disabling user accounts does not delete their records from the IoT FND database.

To disable user accounts in IoT FND:

1. Choose **Admin > Access Management > Users**.
2. Check the check boxes for the user account(s) to disable.
3. Click the **outlined person** icon.
Note: If you disable a user account, IoT FND resets the user password.
4. To confirm action, click **Yes**.

Editing Users

To edit user settings in IoT FND:

1. Choose **Admin > Access Management > Users**.
2. To edit user credentials:
 - a. Click the user name link.
 - b. Edit the role assignments.
 - c. Click **Save**.