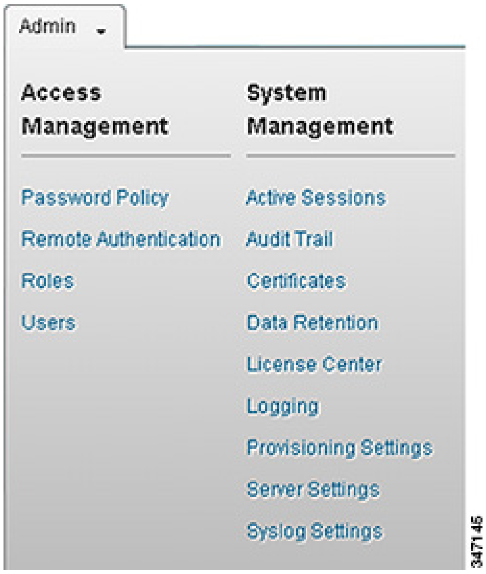
Managing User Access

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

- Managing the Password Policy
- Configuring Remote Authentication
- Managing Roles
- 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.

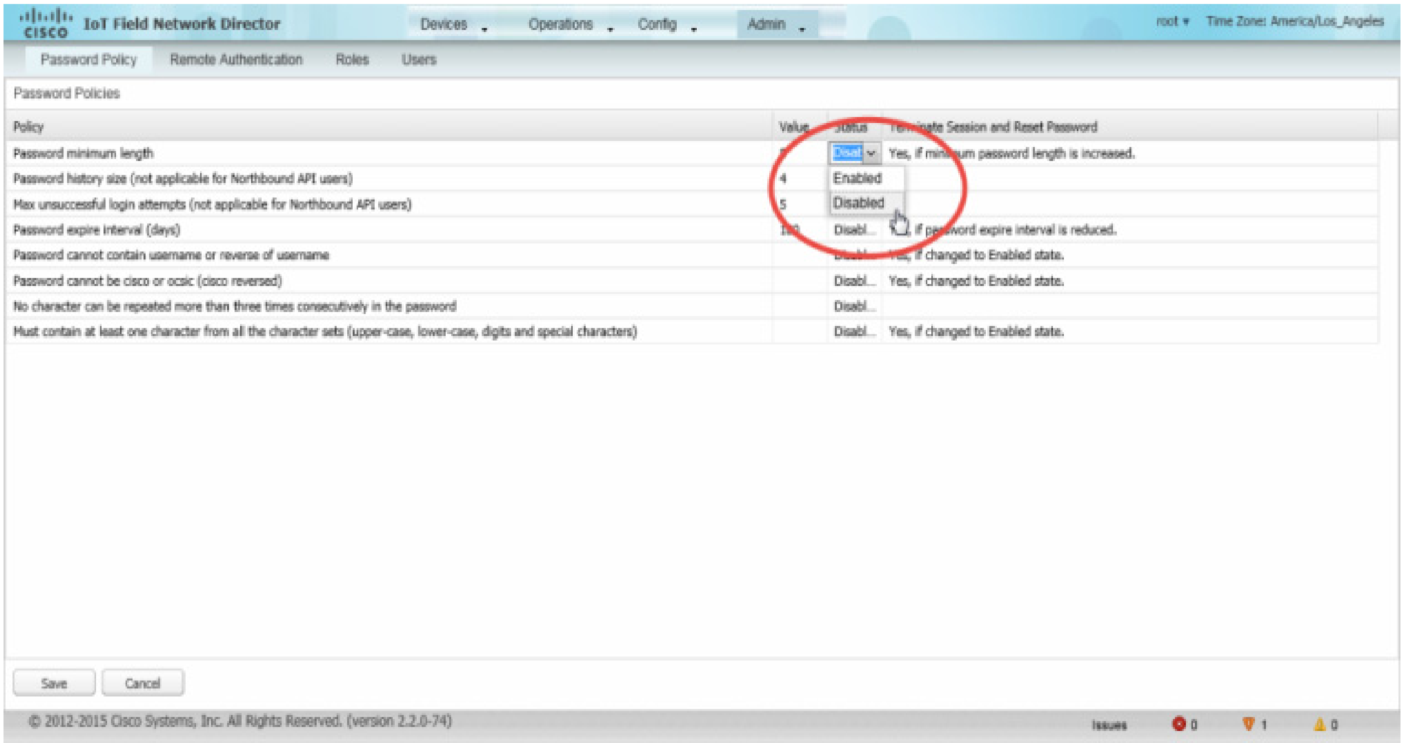
These changes *invalidate* all user sessions and expire their passwords (including the root user):

- 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	[illegible]	Disal	Yes, if minimum password length is increased.
Password history size (not applicable for Northbound API users)	4		
Max unsuccessful login attempts (not applicable for Northbound API users)	5		
Password expire interval (days)	[illegible]	Disabl...	Yes, if password expire interval is reduced.
Password cannot contain username or reverse of username		Disabl...	Yes, if changed to Enabled state.
Password cannot be cisco or ocsic (cisco reversed)		Disabl...	Yes, if changed to Enabled state.
No character can be repeated more than three times consecutively in the password		Disabl...	
Must contain at least one character from all the character sets (upper-case, lower-case, digits and special characters)		Disabl...	Yes, if changed to Enabled state.

© 2012-2015 Cisco Systems, Inc. All Rights Reserved. (version 2.2.0-74)

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 configurations steps in Active Directory (AD) and IoT FND.

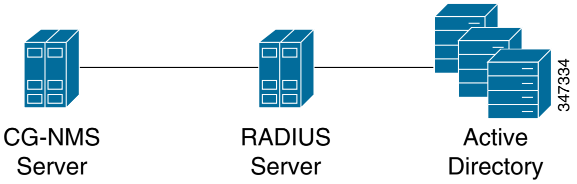
- Support for Remote Authentication
- Configuring Remote Authentication in AD
- Configuring Security Policies on the RADIUS Server

- 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.

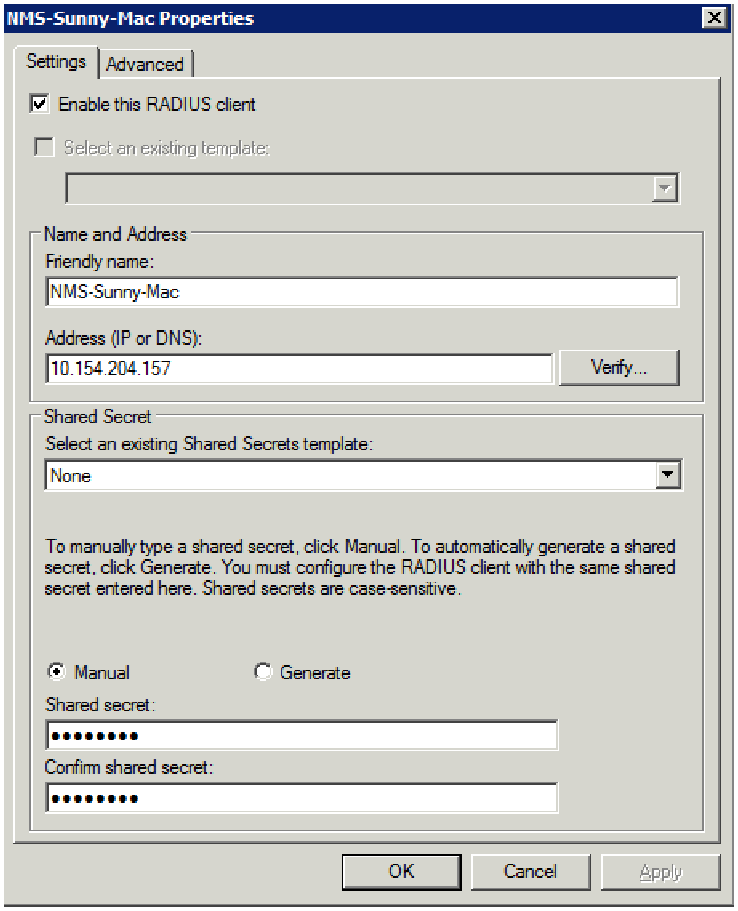
Configuring Remote Authentication in AD

To configure AD to allow IoT FND to remotely authenticate users:

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.



☑ Enable this RADIUS client

□ Select an existing template:

Name and Address

Friendly name: NMS-Sunny-Mac

Address (IP or DNS): 10.154.204.157

Shared Secret

Select an existing Shared Secrets template: None

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

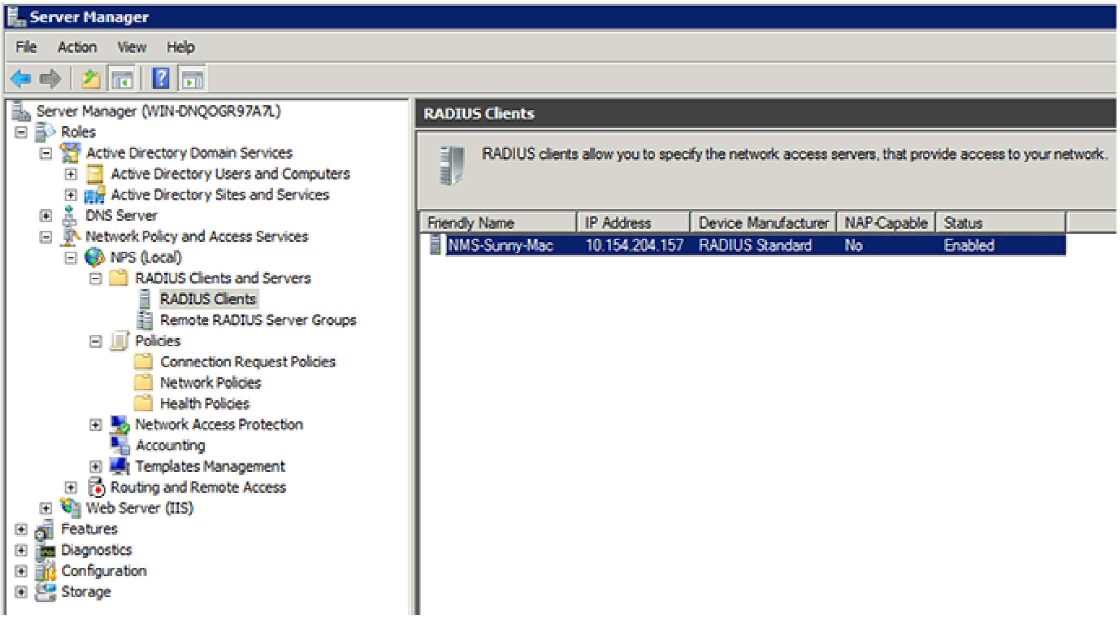
● Manual ○ Generate

Shared secret: ••••••••

Confirm shared secret: ••••••••

347319

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


Server Manager
File
Action
View
Help
Server Manager (WIN-DNQOGR97A7L)
Roles
Active Directory Domain Services
Active Directory Users and Computers
Active Directory Sites and Services
DNS Server
Network Policy and Access Services
NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server Groups
Policies
Connection Request Policies
Network Policies
Health Policies
Network Access Protection
Accounting
Templates Management
Routing and Remote Access
Web Server (IIS)
Features
Diagnostics
Configuration
Storage
RADIUS Clients

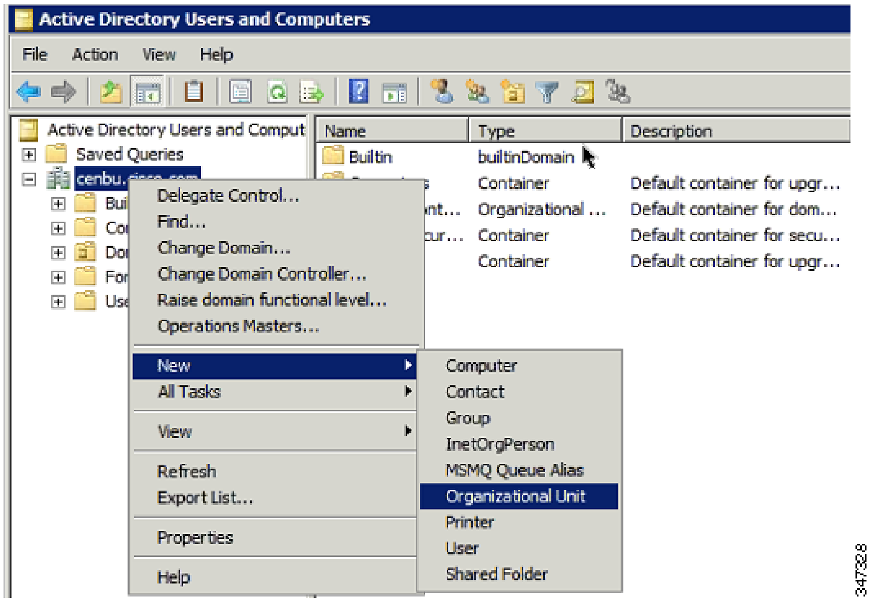
RADIUS clients allow you to specify the network access servers, that provide access to your network.

Friendly Name	IP Address	Device Manufacturer	NAP-Capable	Status
NMS-Sunny-Mac	10.154.204.157	RADIUS Standard	No	Enabled

347318

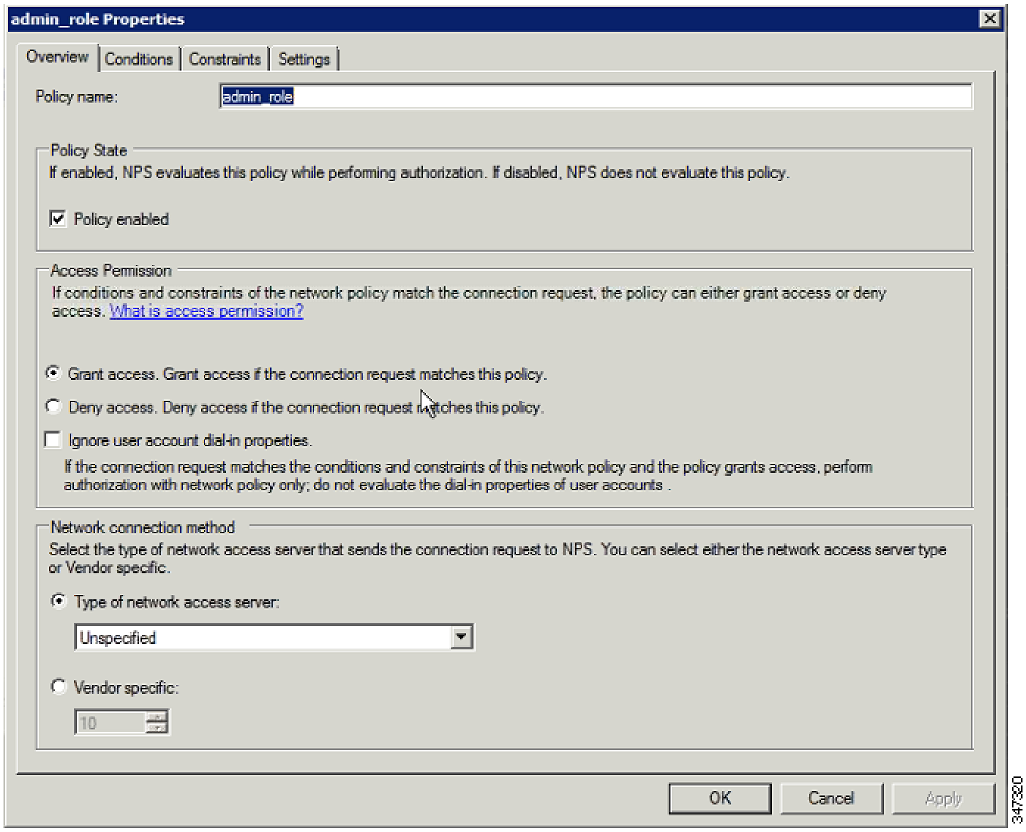
3. Log in to AD and create an organizational unit.

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



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.



Policy name: admin_role

Policy State

If enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy.

☑ Policy enabled

Access Permission

If conditions and constraints of the network policy match the connection request, the policy can either grant access or deny access. What is access permission?

● Grant access. Grant access if the connection request matches this policy.

○ Deny access. Deny access if the connection request matches this policy.

□ Ignore user account dial-in properties.

If the connection request matches the conditions and constraints of this network policy and the policy grants access, perform authorization with network policy only; do not evaluate the dial-in properties of user accounts .

Network connection method

Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific.

● Type of network access server:

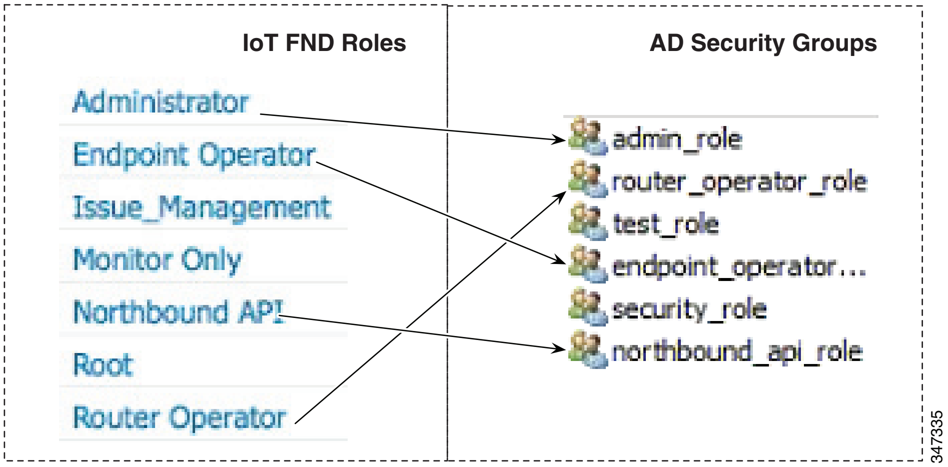
Unspecified

○ Vendor specific:

10

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.

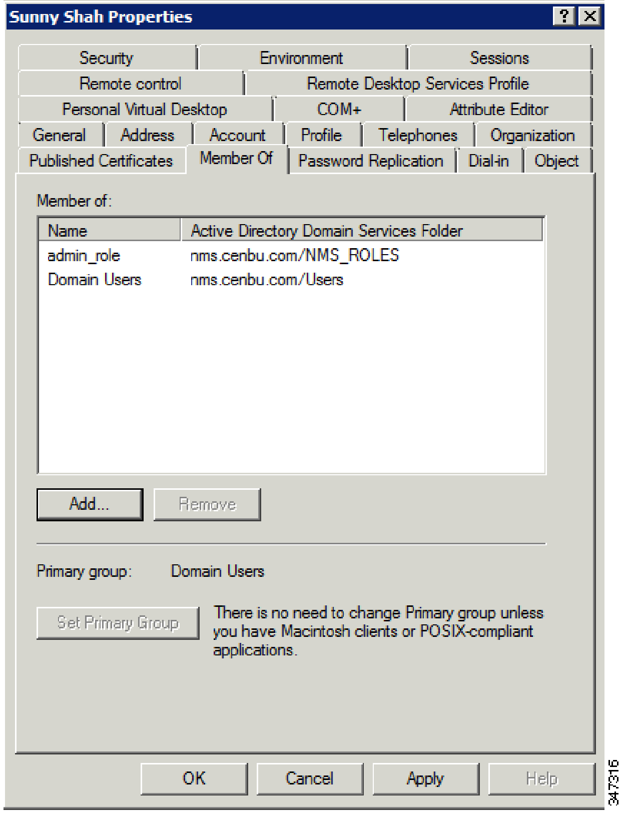
Note: You cannot create or assign the IoT FND root role in AD.



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 a create the corresponding AD security group. Users in this new group can then carry out the tasks allowed by this role.



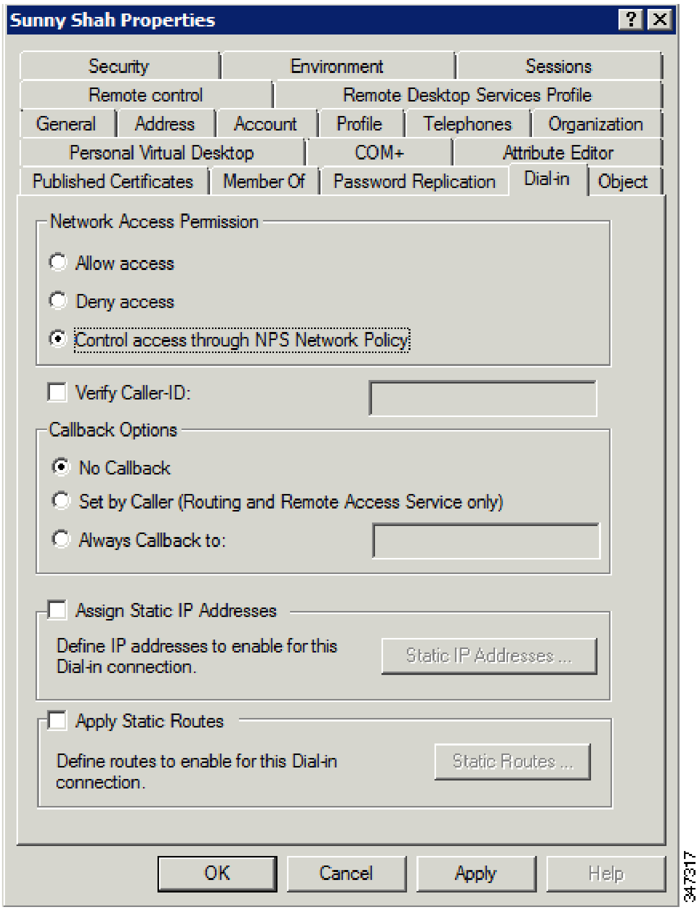
Member of:

Name	Active Directory Domain Services Folder
admin_role	nms.cenbu.com/NMS_ROLES
Domain Users	nms.cenbu.com/Users

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

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



Network Access Permission

○ Allow access

○ Deny access

● Control access through NPS Network Policy

□ Verify Caller-ID:

Callback Options

● No Callback

○ Set by Caller (Routing and Remote Access Service only)

○ Always Callback to:

□ Assign Static IP Addresses

Define IP addresses to enable for this Dial-in connection.

□ Apply Static Routes

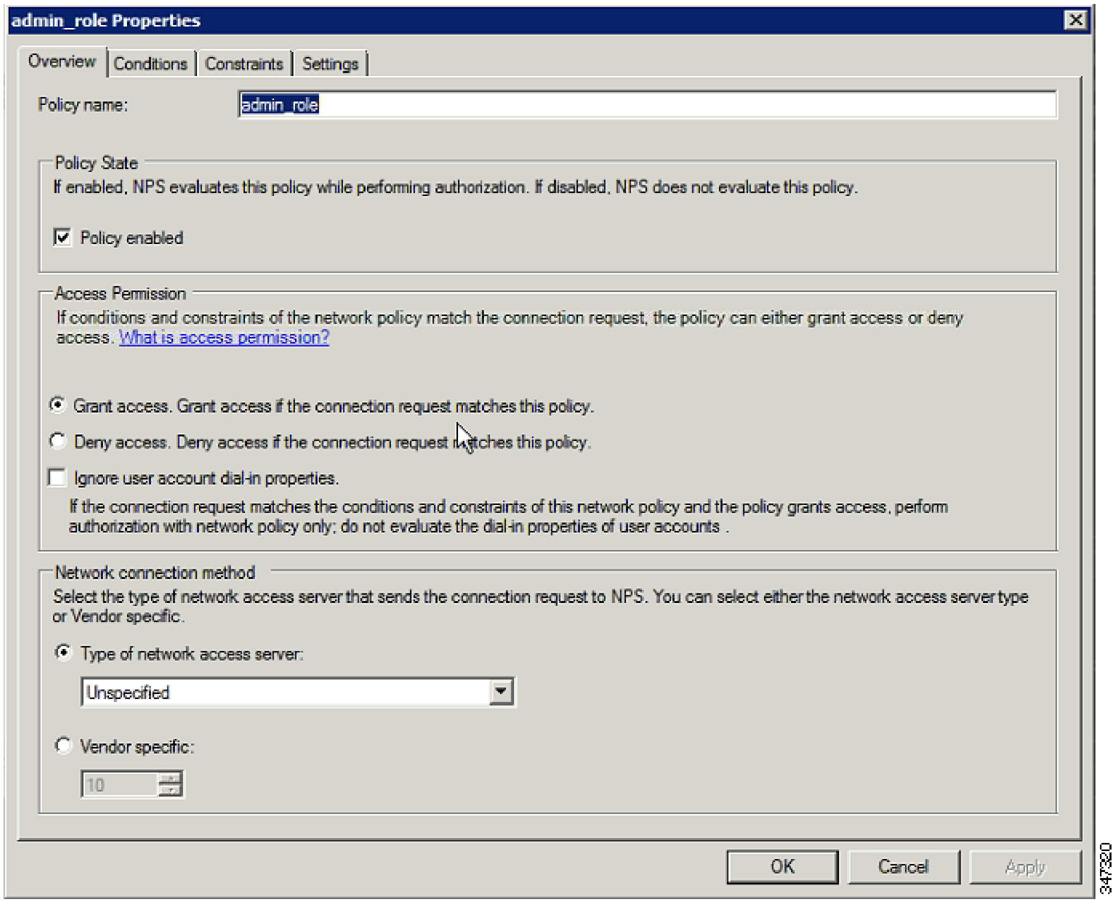
Define routes to enable for this Dial-in connection.

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.



admin_role Properties

Overview | Conditions | Constraints | Settings

Policy name: admin_role

Policy State

If enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy.

☑ Policy enabled

Access Permission

If conditions and constraints of the network policy match the connection request, the policy can either grant access or deny access. What is access permission?

● Grant access. Grant access if the connection request matches this policy.

○ Deny access. Deny access if the connection request matches this policy.

□ Ignore user account dial-in properties.

If the connection request matches the conditions and constraints of this network policy and the policy grants access, perform authorization with network policy only; do not evaluate the dial-in properties of user accounts .

Network connection method

Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific.

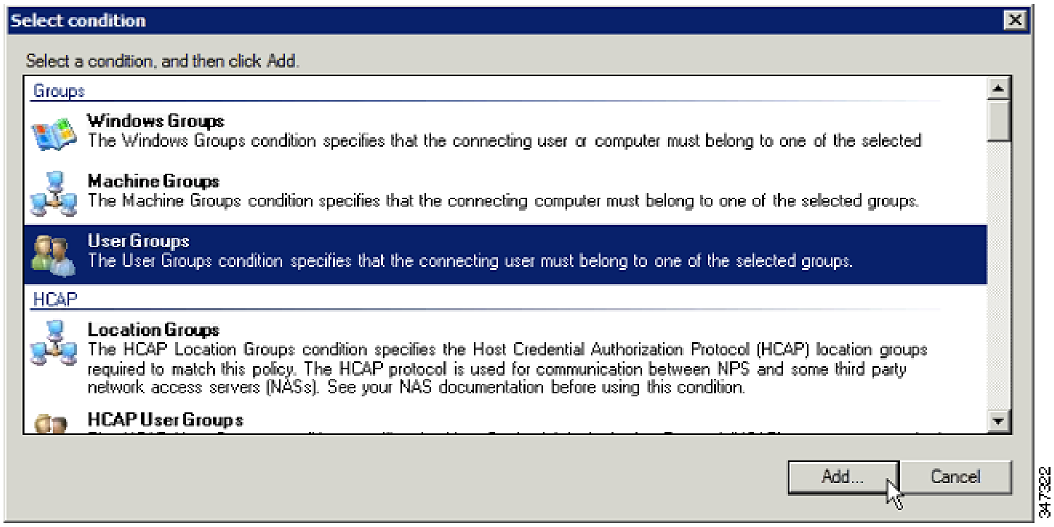
● Type of network access server:

Unspecified

○ Vendor specific:

10

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



Select condition

Select a condition, and then click Add.

Groups

Windows Groups
The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected

Machine Groups
The Machine Groups condition specifies that the connecting computer must belong to one of the selected groups.

User Groups
The User Groups condition specifies that the connecting user must belong to one of the selected groups.

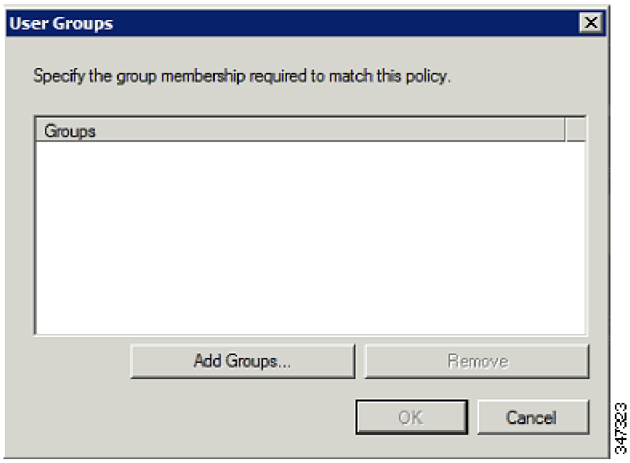
HCAP

Location Groups
The HCAP Location Groups condition specifies the Host Credential Authorization Protocol (HCAP) location groups required to match this policy. The HCAP protocol is used for communication between NPS and some third party network access servers (NASs). See your NAS documentation before using this condition.

HCAP User Groups

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**.

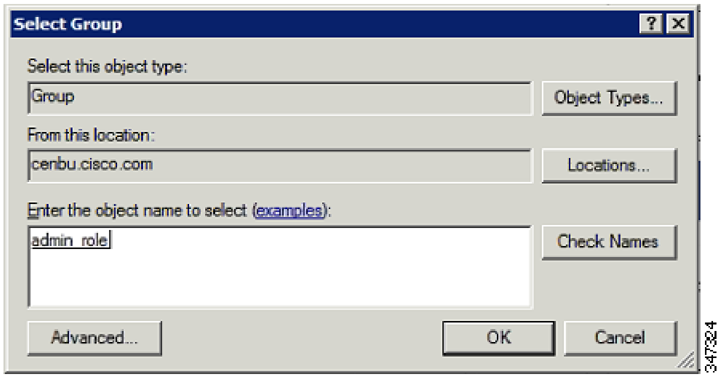


User Groups

Specify the group membership required to match this policy.

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.



Select Group

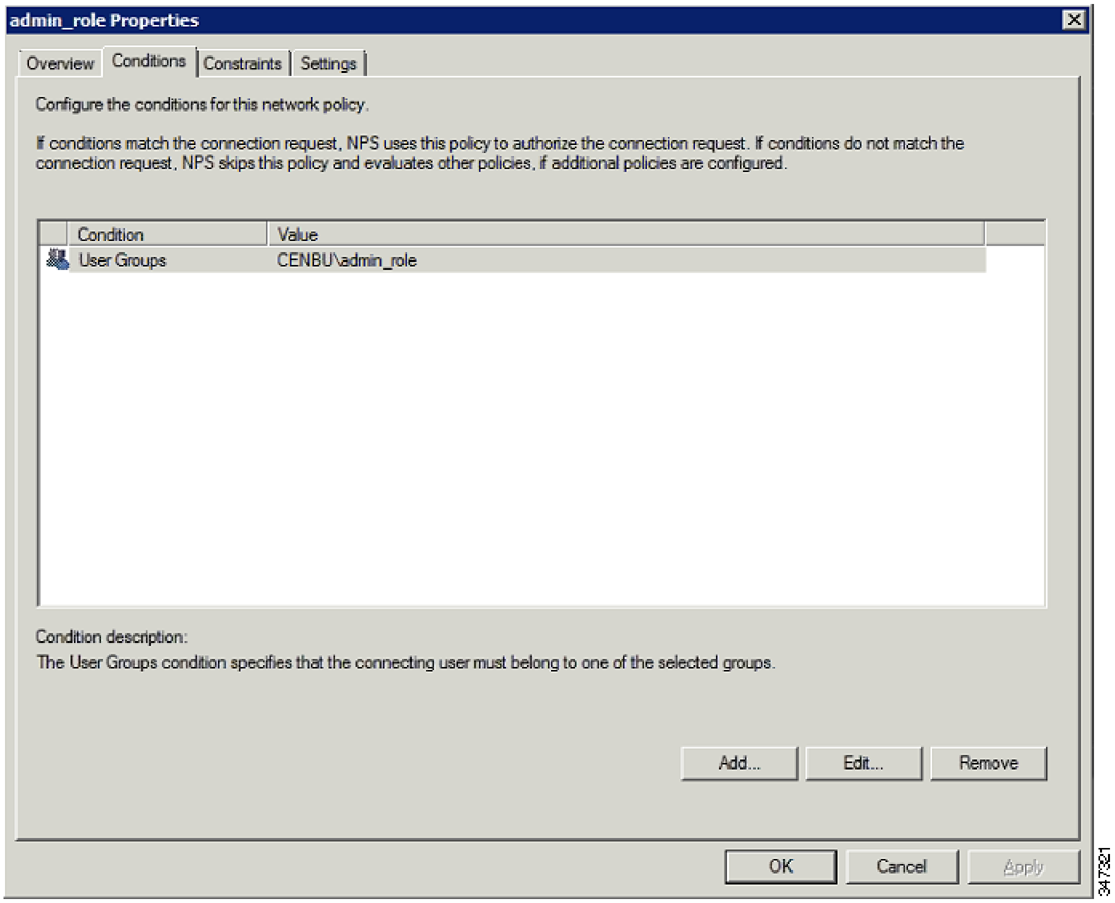
Select this object type: Group

From this location: cenbu.cisco.com

Enter the object name to select (examples): admin_role

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

The condition appears in the Conditions pane.



admin_role Properties

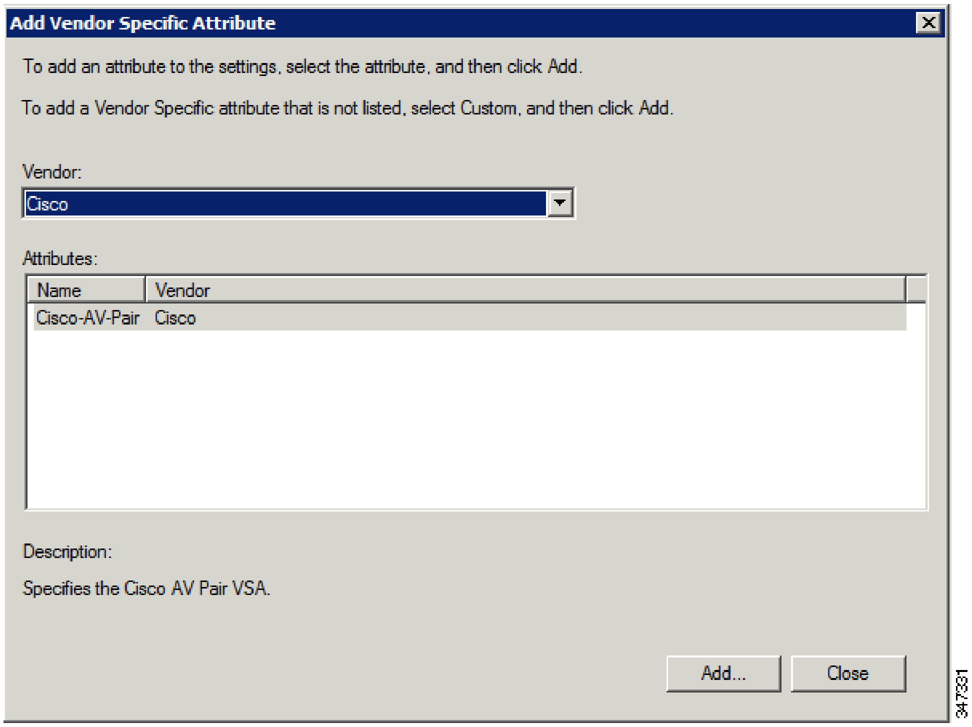
Configure the conditions for this network policy.

If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.

Condition	Value
User Groups	CENBU\admin_role

Condition description:
The User Groups condition specifies that the connecting user must belong to one of the selected groups.

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

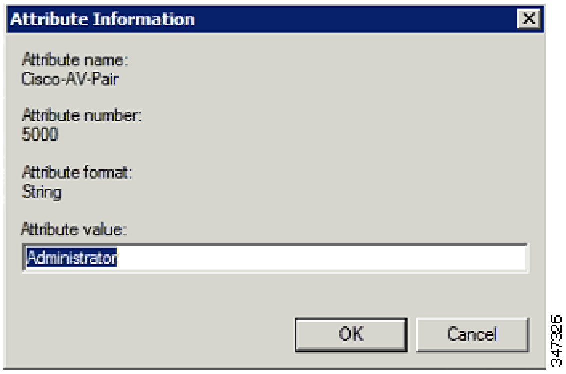
Description:

Specifies the Cisco AV Pair VSA.

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

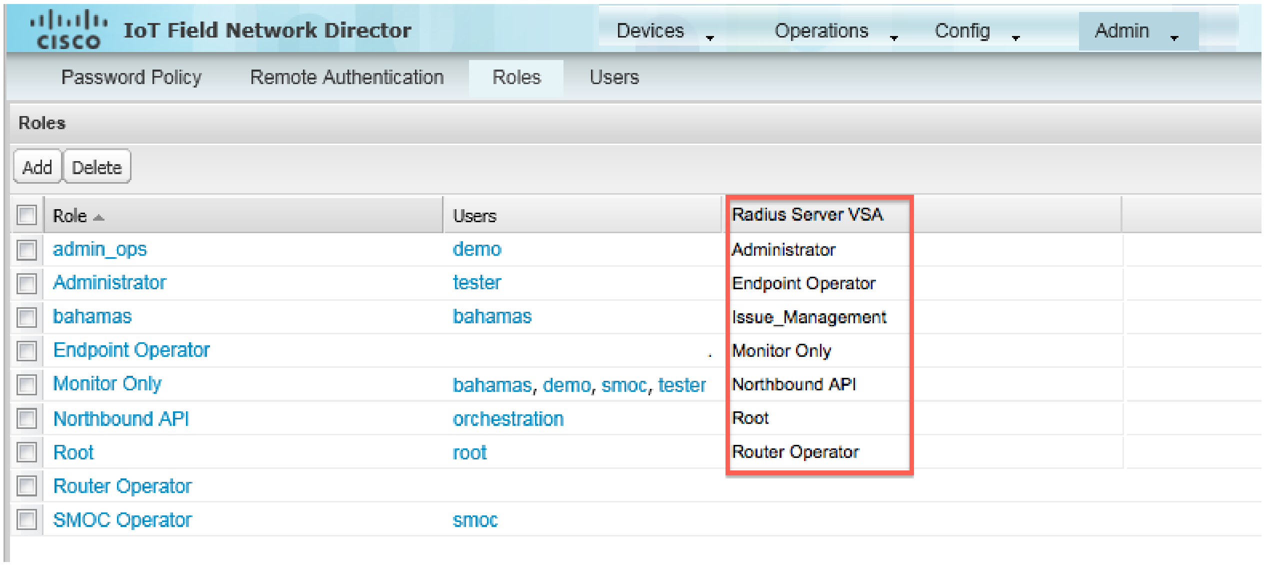
Attribute name:
Cisco-AV-Pair

Attribute number:
5000

Attribute format:
String

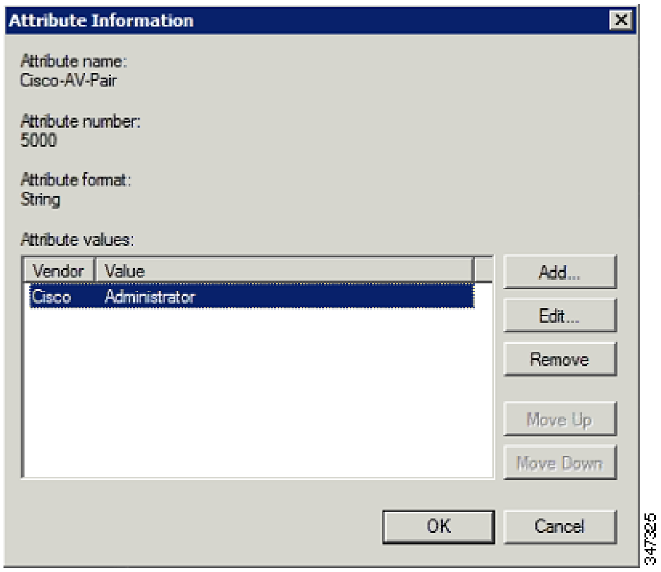
Attribute value: Administrator

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**).



Role	Users	Radius Server VSA
admin_ops	demo	Administrator
Administrator	tester	Endpoint Operator
bahamas	bahamas	Issue_Management
Endpoint Operator	.	Monitor Only
Monitor Only	bahamas, demo, smoc, tester	Northbound API
Northbound API	orchestration	Root
Root	root	Router Operator
Router Operator		
SMOC Operator	smoc	

i. Click **OK**.



Attribute name:
Cisco-AV-Pair

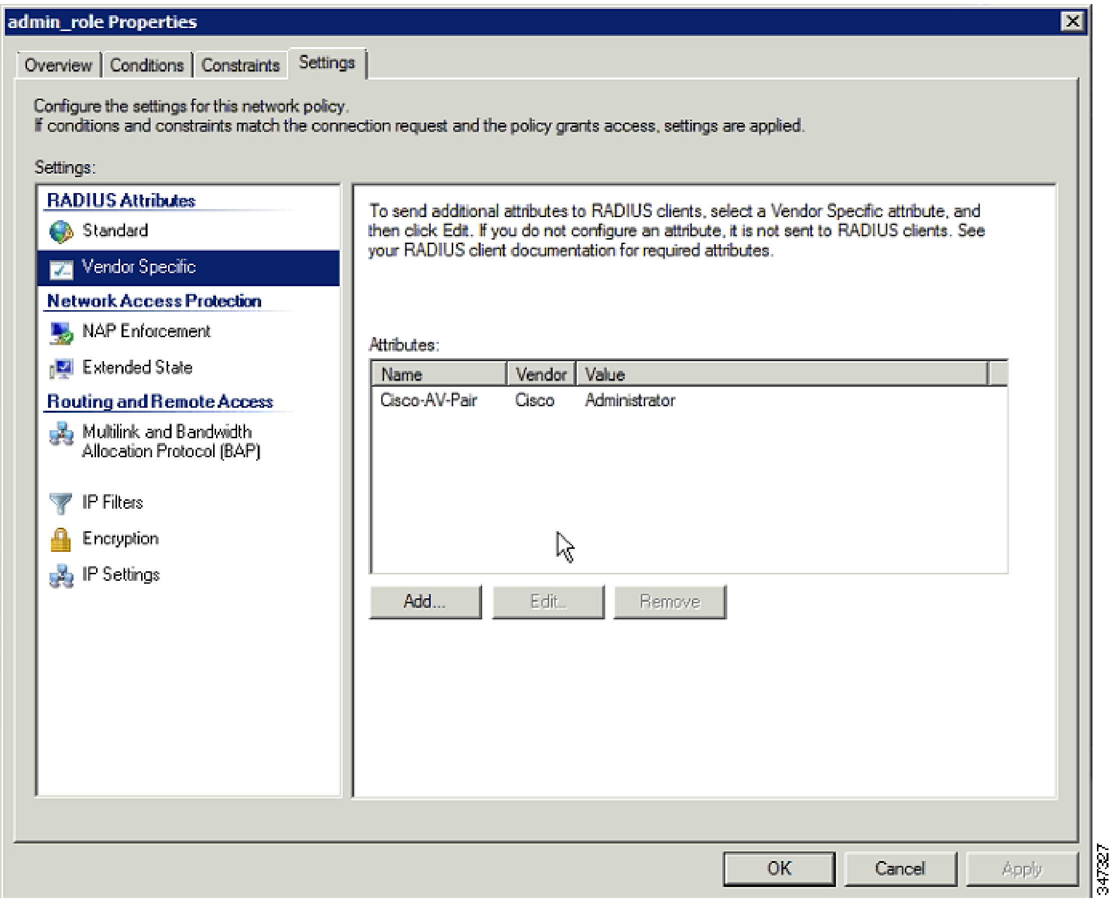
Attribute number:
5000

Attribute format:
String

Attribute values:

Vendor	Value
Cisco	Administrator

The VSA attribute appears in the Settings pane.



Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

To send additional attributes to RADIUS clients, select a Vendor Specific attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Name	Vendor	Value
Cisco-AV-Pair	Cisco	Administrator

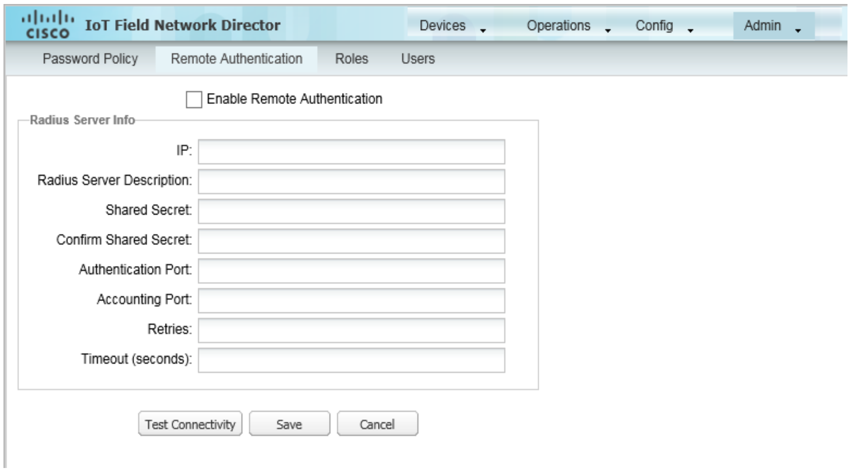
j. Click **OK**.

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**.



□ Enable Remote Authentication

Radius Server Info

IP:

Radius Server Description:

Shared Secret:

Confirm Shared Secret:

Authentication Port:

Accounting Port:

Retries:

Timeout (seconds):

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.
Name	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.
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	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 Configuration**.
   a. Enter your 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

Use roles to assign permissions based on the role or roles a user plays. Roles define the type of tasks IoT FND users can perform. This section has the following topics:

- Adding Roles
- Deleting Roles
- Editing Roles
- Viewing Roles

IoT FND lets you assign a role to any user. 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 FAR and endpoint devices.
Administrative Operations	Allows users to perform system administration operations such as user management, role management, and server configuration settings.
Endpoint Configuration	Allows users to edit configuration templates and push configuration to MEs.
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.

Table 1 IoT FND User Permissions (continued)

Permission	Description
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.
Manage Device Credentials	Allows users to view FAR 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 FAR and endpoint devices using IoT FND 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.
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.
Router Configuration	Allows users to edit FAR configuration templates and push configuration to FARs.
Router Firmware Update	Allows users to add and delete firmware images and perform firmware update operations for FARs.
Router Group Management	Allows users to assign, remove, and change device assignments to FAR configuration and firmware groups.
Router Reboot	Allows users to reboot the FAR.
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.
Work Order Management	Allows users to manage work orders for 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
Add Devices	This role can add, modify, and delete devices from IoT FND.
Administrator	This role combines these basic permissions: ■ Administrative Operations ■ Label Management ■ Rules Management
Endpoint Operator	This role combines these basic permissions: ■ Label Management ■ Endpoint Configuration ■ Endpoint Firmware Update ■ Endpoint Group Management ■ Endpoint Reboot
Monitor Only	This role provides users with read-only access to IoT FND. By default, this role is defined for every user.
North Bound API	This role combines these basic permissions: ■ 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
Router Operator	This role combines these basic permissions: ■ Label Management ■ Router Configuration ■ Router Firmware Update ■ Router Group Management ■ Router Reboot
Router Operator with Manage Device Creds	This role combines the permissions of a Router Operator with: ■ Device credential management
Security Policy	This role can manage security policies through IoT FND.
Tunnel Provisioning Management	This role can provision tunnels.

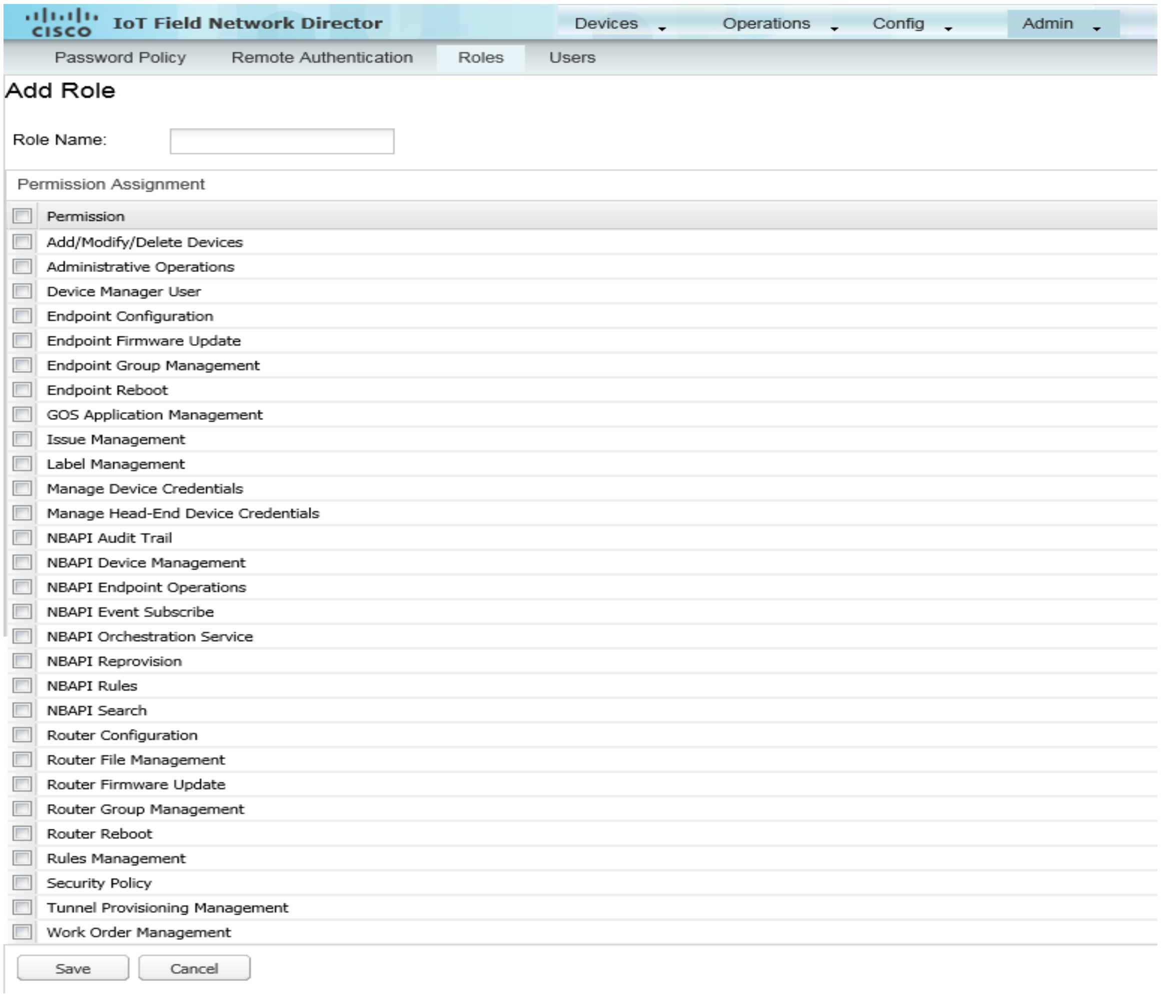
Custom User Roles

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**.



Add Role

Role Name:

Permission Assignment

□	Permission
□	Add/Modify/Delete Devices
□	Administrative Operations
□	Device Manager User
□	Endpoint Configuration
□	Endpoint Firmware Update
□	Endpoint Group Management
□	Endpoint Reboot
□	GOS Application Management
□	Issue Management
□	Label Management
□	Manage Device Credentials
□	Manage Head-End Device Credentials
□	NBAPI Audit Trail
□	NBAPI Device Management
□	NBAPI Endpoint Operations
□	NBAPI Event Subscribe
□	NBAPI Orchestration Service
□	NBAPI Reprovision
□	NBAPI Rules
□	NBAPI Search
□	Router Configuration
□	Router File Management
□	Router Firmware Update
□	Router Group Management
□	Router Reboot
□	Rules Management
□	Security Policy
□	Tunnel Provisioning Management
□	Work Order Management

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.

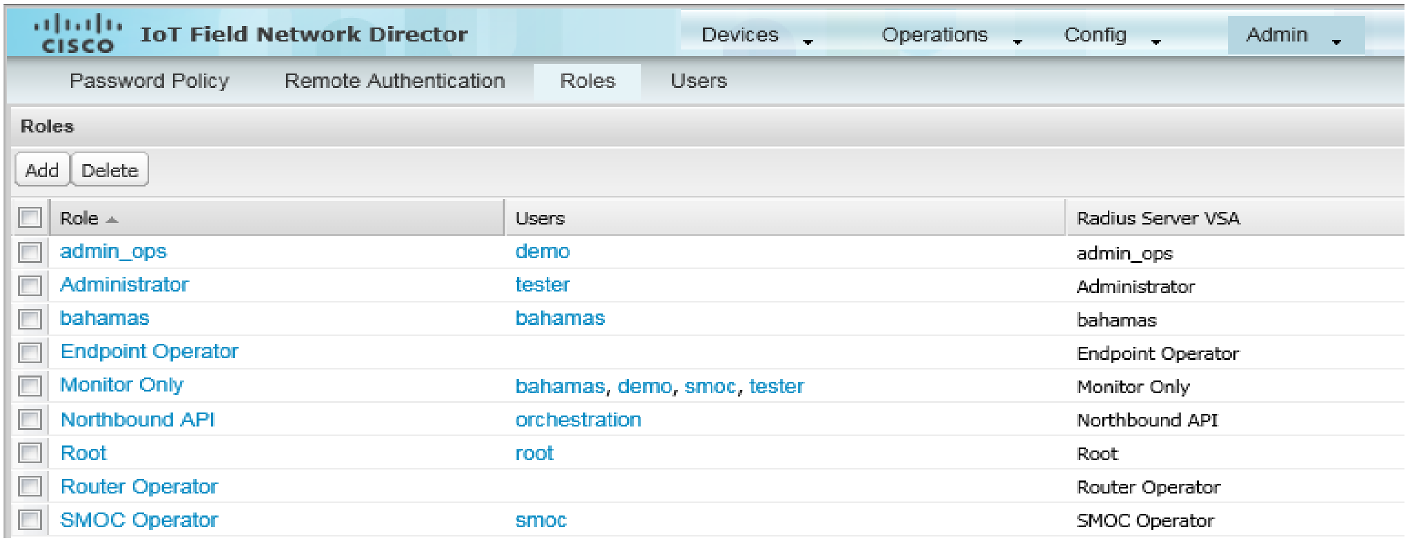
To edit IoT FND custom roles:

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**.



☐	Role ▲	Users	Radius Server VSA
☐	admin_ops	demo	admin_ops
☐	Administrator	tester	Administrator
☐	bahamas	bahamas	bahamas
☐	Endpoint Operator		Endpoint Operator
☐	Monitor Only	bahamas, demo, smoc, tester	Monitor Only
☐	Northbound API	orchestration	Northbound API
☐	Root	root	Root
☐	Router Operator		Router Operator
☐	SMOC Operator	smoc	SMOC Operator

For every role, IoT FND lists the users assigned to this role.

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:

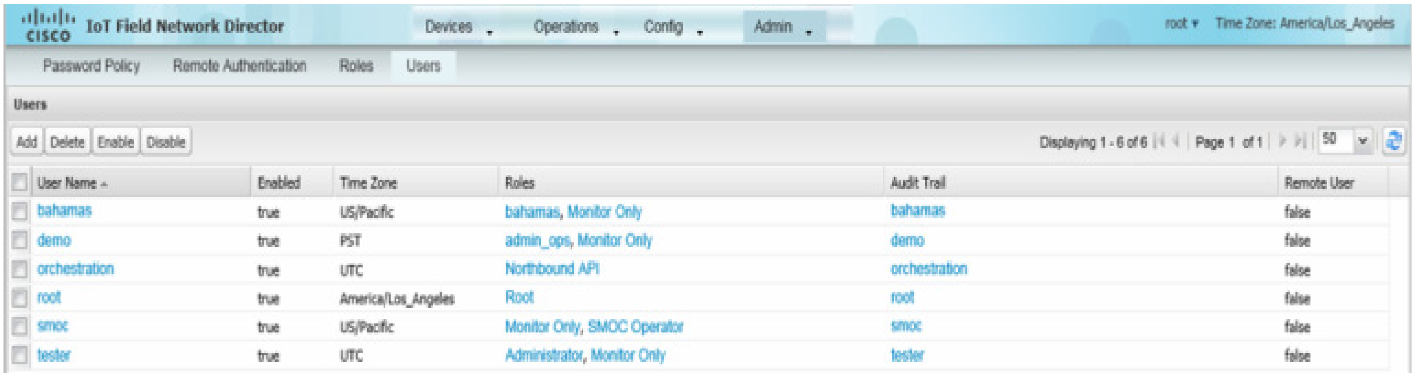
```
[root@yourname-lnx1 bin}#./password_admin.sh root
```

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**).



□	User Name	Enabled	Time Zone	Roles	Audit Trail	Remote User
□	bahamas	true	US/Pacific	bahamas, Monitor Only	bahamas	false
□	demo	true	PST	admin_ops, Monitor Only	demo	false
□	orchestration	true	UTC	Northbound API	orchestration	false
□	root	true	America/Los_Angeles	Root	root	false
□	smoc	true	US/Pacific	Monitor Only, SMOC Operator	smoc	false
□	tester	true	UTC	Administrator, Monitor Only	tester	false

IoT FND displays this information about users:

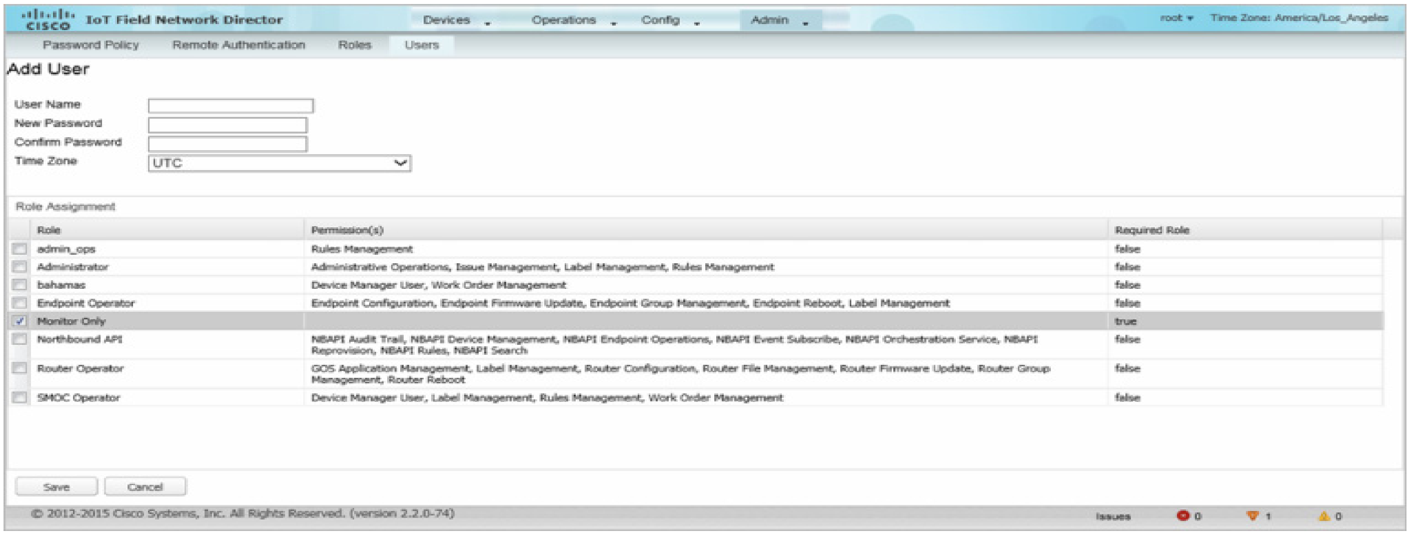
Field	Description
User Name	Specifies the user name.
Enabled	Indicates whether the user account is enabled.
Time Zone	Specifies the user’s time zone.

Field	Description
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 **Add**.



Add User

User Name	
New Password	
Confirm Password	
Time Zone	UTC

Role Assignment

	Role	Permission(s)	Required Role
□	admin_ops	Rules Management	false
□	Administrator	Administrative Operations, Issue Management, Label Management, Rules Management	false
□	bahamas	Device Manager User, Work Order Management	false
□	Endpoint Operator	Endpoint Configuration, Endpoint Firmware Update, Endpoint Group Management, Endpoint Reboot, Label Management	false
☑	Monitor Only		true
□	Northbound API	NBAPI Audit Trail, NBAPI Device Management, NBAPI Endpoint Operations, NBAPI Event Subscribe, NBAPI Orchestration Service, NBAPI Reprovision, NBAPI Rules, NBAPI Search	false
□	Router Operator	GOS Application Management, Label Management, Router Configuration, Router File Management, Router Firmware Update, Router Group Management, Router Reboot	false
□	SMOC Operator	Device Manager User, Label Management, Rules Management, Work Order Management	false

Save
Cancel
© 2012-2015 Cisco Systems, Inc. All Rights Reserved. (version 2.2.0-74)
Issues
0
1
0

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. Select the user roles to assigned to this user by checking the appropriate check box under Role Assignment.
5. Click **Save**.

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

6. To add the new user, click **Yes**; otherwise, click **No** to return to the Users page.

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

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 check boxes of the user accounts to delete.
3. Click **Delete**.
4. Click **Yes** to confirm.
5. Click **OK**.

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 accounts to enable.
3. Click **Enable**.
4. Click **Yes**.
5. Click **OK**.

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 accounts to disable.
3. Click **Disable**.

   Note: If you disable a user account, IoT FND resets the user password.
4. Click **Yes**.
5. Click **OK**.

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**.