Chapter 10

Setting Up AIM Users

This chapter describes how to add users to Advanced Insight Manager (AIM). Users are able to view only incidents and intelligence messages to which they have appropriate permissions. Permissions are based on the user group(s) to which users are assigned and the association of those user groups to specified device groups. For more information about configuring user groups, see “Setting Up AIM Users” on page 89. For more information about configuring device groups, see “Creating Device Groups” on page 72.

Additionally, users can be assigned permissions that allow them access only to a subset of AIM operations. If the Multi-Site license is present, allowing for multiple organizations, users have access to organizations and the devices contained in them based on their user group and device group associations.

Incidents and Intelligence Updates assigned to users are filtered based on the user’s user group and device group associations.

An AIM user must have the following:

- Unique user name
- Unique Password
- Privileges that determine the operations that can be performed

The password for the administrator should not match the username, and should not be a word that can be easily guessed.

In general, AIM passwords should be:

- Easy to remember so that users are not tempted to write them down.
- Contain up to 32 characters, using at least two of the four defined character sets (uppercase, lowercase, numeric, other). The characters in the set "other" are those that can be entered using a single keystroke, or a keyboard character accessed using the Shift key, that does not fall into any of the other three groups.

This chapter includes the following sections:

Default AIM User Account

The default AIM user account is:

- Username: admin
- Password: aimadmin

The default AIM user account is granted all privileges and is the primary administrator account for the application. You cannot delete the default AIM user account, and privileges cannot be modified.

It is recommended that you change the default password after the AIM administrator logs in. The password can be up to 32 character.

Understanding AIM Ownership

AIM provides ownership for incidents and intelligence messages. Once an AIM user becomes owner, that user is responsible for keeping track of the progress of a case or updates from JSS to ensure that case is resolved or for what actions are needed for an intelligence message. The incident or intelligence message owner can also update the case status to reflect progress made.

When an AIM user has ownership and appropriate privileges, that user can do the following:

- Incidents
  - Edit priority and email list if incident is not submitted to JSS
  - Submit incident to JSS
  - Update owner status to reflect progress
- Intelligence Messages
  - Update owner status to reflect progress

There are three levels of user ownership that an AIM administrator can assign when adding or modifying user privileges (see Table 45).

Table 45: AIM Ownership Levels

Ownership Level	Description
None	User is not allowed to own or assign ownership to any AIM user.
Level I	User can voluntarily take ownership of any unassigned incidents or intelligence messages.
Level II	User can voluntarily take ownership of any incidents or intelligence messages regardless if assigned or unassigned.
Level III	User can either give or take away ownership of incidents or intelligence messages to any user.

AIM User Privileges

The AIM application enforces user privileges so that users can only have access the information to which they have privileges. Table 46 defines the AIM user privileges.

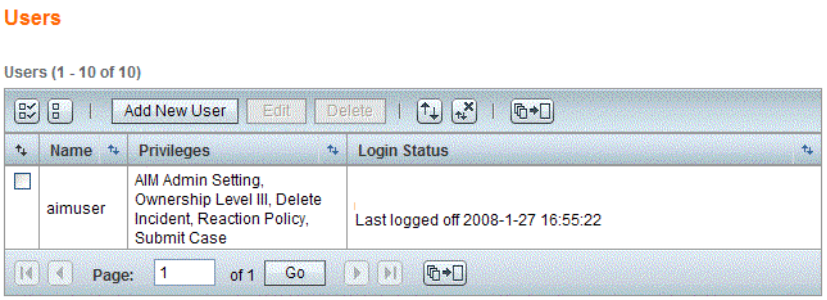
Table 46: AIM User Privileges

Privilege	Description
AIM Admin Setting	AIM administrators can perform the following tasks: If the logged in user does not have Admin privileges, these settings can only be viewed: ■ Connect AIM to JSS ■ Perform alert registration ■ Set archive locations incident detection interval ■ Set up and manage organizations ■ Set up and manage licensing ■ Create, edit, and delete trap destinations ■ Create, edit, and delete users ■ Create, edit, and delete user groups ■ Create, edit, and delete device groups ■ Associate device groups ■ Associate user groups
Ownership	Three levels of AIM user ownership are provided that the administrator can use when assigning new user privileges. See Table 45.
Delete Incident	AIM user can delete incidents in Incident Manager.
Reaction Policy	AIM user can manage all the policies he/she owns. It includes creation, deletion, disable, and enable policies. The policy will automatically be owned by the user who created it. If a user is deleted from AIM, all policies belonging to that user will be automatically deleted as well.
Submit Case	AIM user can submit any unassigned incidents to JSS.

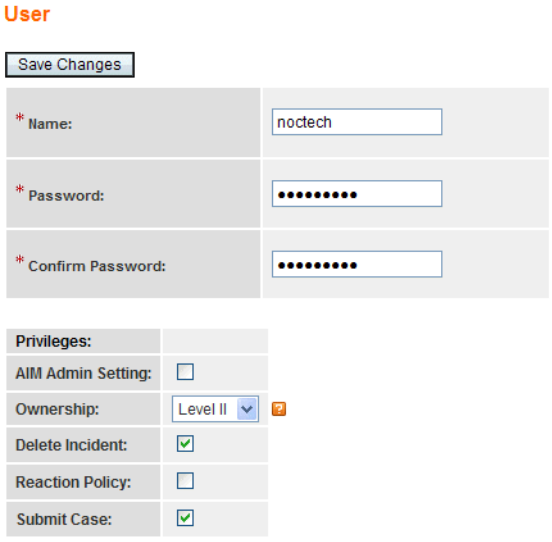
Adding a AIM User

To create an AIM user, follow these steps:

1. Click Settings > Users. The Users page appears with the default AIM admin user if you have added no other users. See “Default AIM User Account” on page 90.



2. Click Add New User. The User page appears.



3. Type the user name.

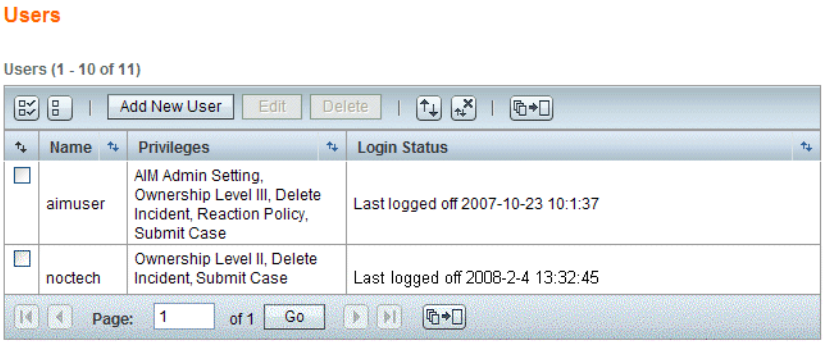
4. Type the user password.

5. Retype the password to confirm it.

6. Select the user privileges that you want. For more information about AIM user ownership, see Table 45. For more information about AIM user privileges, see Table 46.

7. Repeat Steps 2 through 6 for each new AIM user you add. For more information about the Add New User page, see

8. Click Save Changes. The AIM user settings are saved in the database and the new user appears in the Users table.



Add New User Page/Edit User Page Description

Table 47: Add New User Page/Edit User Page Command Button

Button Name	Description	Privileges	Enabled/ Disabled	Results
Save Changes	Saves the changes made to AIM user name, password, and privileges.	AIM Admin Settings	Enabled if admin privileges	Error message is displayed if settings were not saved

Table 50 describes the New User Field descriptions.

Table 48: Add New User Page/Edit User Page Field Descriptions

Name	Description	Privileges	Range/ Length	Default
Name	AIM user name	AIM Admin Settings	32 characters	Blank on the Add User page. Display username only on the Edit User page
Password	AIM user password	AIM Admin Settings	32 characters	Blank
Confirm Password	Retyped AIM user password for confirmation	AIM Admin Settings	32 characters	Blank
AIM Admin Setting Privilege	See Table 46	AIM Admin Settings	N/A	Unchecked
Ownership Privilege	Three levels of AIM user ownership are provided that the administrator can use when assigning new user privileges: ■ Level I ■ Level II ■ Level III See Table 45.	AIM Admin Settings	N/A	None

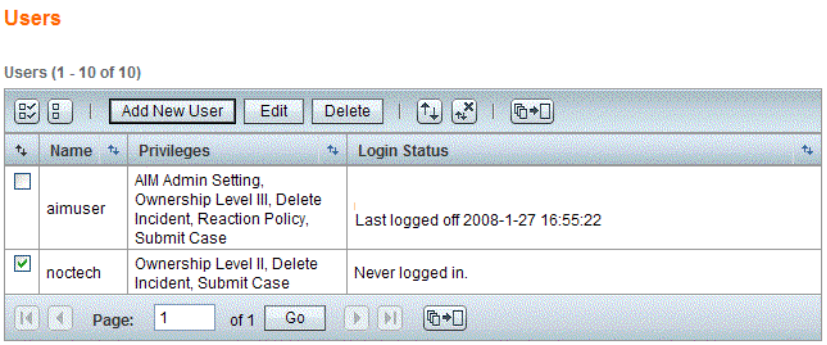
Name	Description	Privileges	Range/ Length	Default
Delete Incident Privilege	AIM user can delete incidents in Incident Manager.	AIM Admin Settings	N/A	Unchecked
Reaction Policy Privilege	AIM user can manage all the policies he/she owns. It includes creation, deletion, disable, and enable policies. The policy will automatically be owned by the user who created it. If a user is deleted from AIM, all policies belonging to that user will be automatically deleted as well.	AIM Admin Settings	N/A	Unchecked
Submit Case Privilege	AIM user can submit any unassigned incidents to JSS.	AIM Admin Settings	N/A	Unchecked

Editing a User

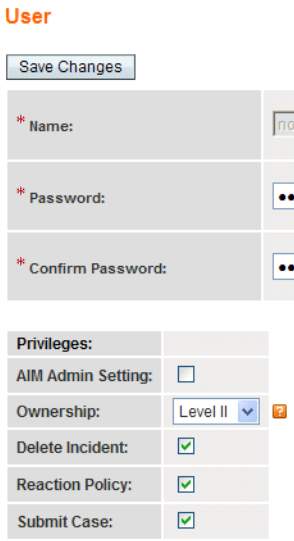
You can edit an AIM user password and privileges.

To edit an AIM user, follow these steps:

1. Click Settings > Users. The Users page appears.
2. Select the AIM user you want to edit. The Edit button is enabled.

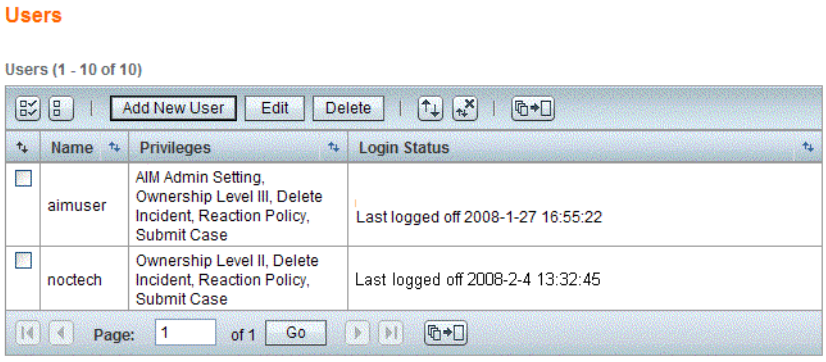


3. Click Edit. The Edit User page appears.



4. Edit the user password or the privileges. To change a username, you must delete that user, then create a new one. For more information about the Edit User page, see “Add New User Page/Edit User Page Description” on page 93.

5. Click Save Changes. The user information is saved in the AIM database. The User table appears with the edited user information (except password information) added.

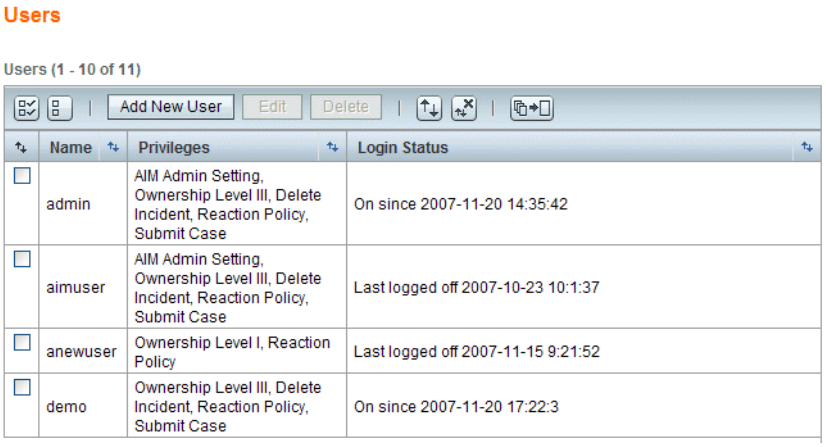


Using the User Table

The User page provides a single point to view and manage AIM user names, privileges, and login status of AIM users.

To view the User table, follow these steps:

1. Click Settings > Users. The Users page appears.



For more information about using the Users table, see

Users Table Description

Table 49 describes the User table command buttons.

Table 49: User Table Command Buttons

Button Name	Description	Privileges	Enabled/ Disabled	Results
Add New User	Displays User page used to add a new AIM user	AIM Admin Settings	Enabled if admin privileges	Displays User page
Edit	Displays User page used to edit user password and privileges. You must select one user to edit the parameters. **Note:** You cannot edit default admin user privileges. You cannot edit a user name.	AIM Admin Settings	Enabled if admin privileges and if user is selected	Displays User page
Delete	Removes the selected user from the User table and the AIM database.	AIM Admin Settings	Enabled if admin privileges and if user is selected	Deletes selected user

Table 50 describes the Users table columns.

Table 50: Users Table Columns

Name	Description	Privileges	Range/ Length	Default
Name	Name of AIM user.	Not allowed to modify	N/A	N/A

Name	Description	Privileges	Range/ Length	Default
Privileges	AIM privileges assigned to user, see Table 46 for description of AIM user privileges.	Not allowed to modify	N/A	N/A
Login Status	Date and time AIM user has been logged in to the application. Also, date and time when AIM user last logged out of the application.	Not allowed to modify	N/A	N/A

Deleting a User

To delete an AIM user, follow these steps:

1. Click Settings > Users. The Users page appears.
2. Select the AIM user you want to delete. The Delete button is enabled.
3. Click Delete.
4. Click Save Changes. The user is removed from the AIM database.