

Chapter 8



Users and Departments

8.1 Security Model Overview

NetVigil's security model was designed to fit the needs of large scale enterprises. The multi-tiered administrative hierarchy allows enterprises and service providers to provide each group within the organization or service model the access it needs, and no more.

NOTE The security model is necessarily complex. We recommend that you read the overview in this chapter and review the case study before designing your own security model.

The following are examples of some roles that can be configured with different privileges:

- IT Admin - global access and privileges to all systems
- Regional IT Support - access to all regional systems with full admin privileges to those systems
- CEO - access to reports on overall system performance and system usage by cost center
- CFO/Accounting - access to reports on system usage by cost center
- Marketing VP - access to reports on marketing system performance and marketing system usage
- Marketing webmaster - administrative privileges on web and e-commerce servers

In the diagrams in this chapter, icons represent the entities in the NetVigil security model:

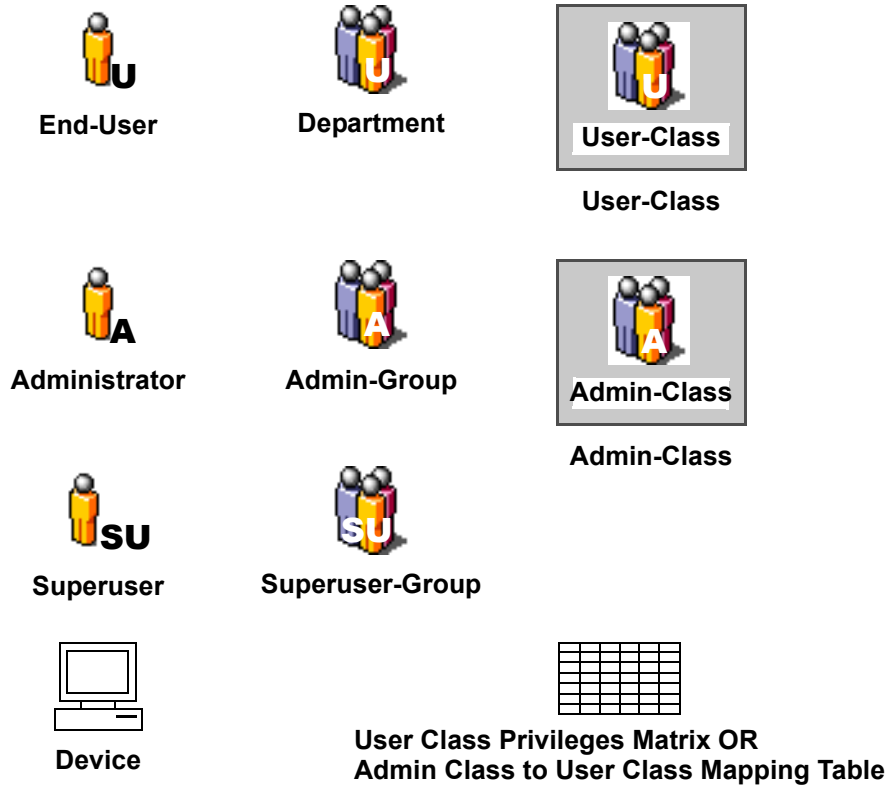


Figure 8.1 Key to Security Model Diagrams

This diagram illustrates the NetVigil security model. The components of the security model are described in detail in the sections that follow.

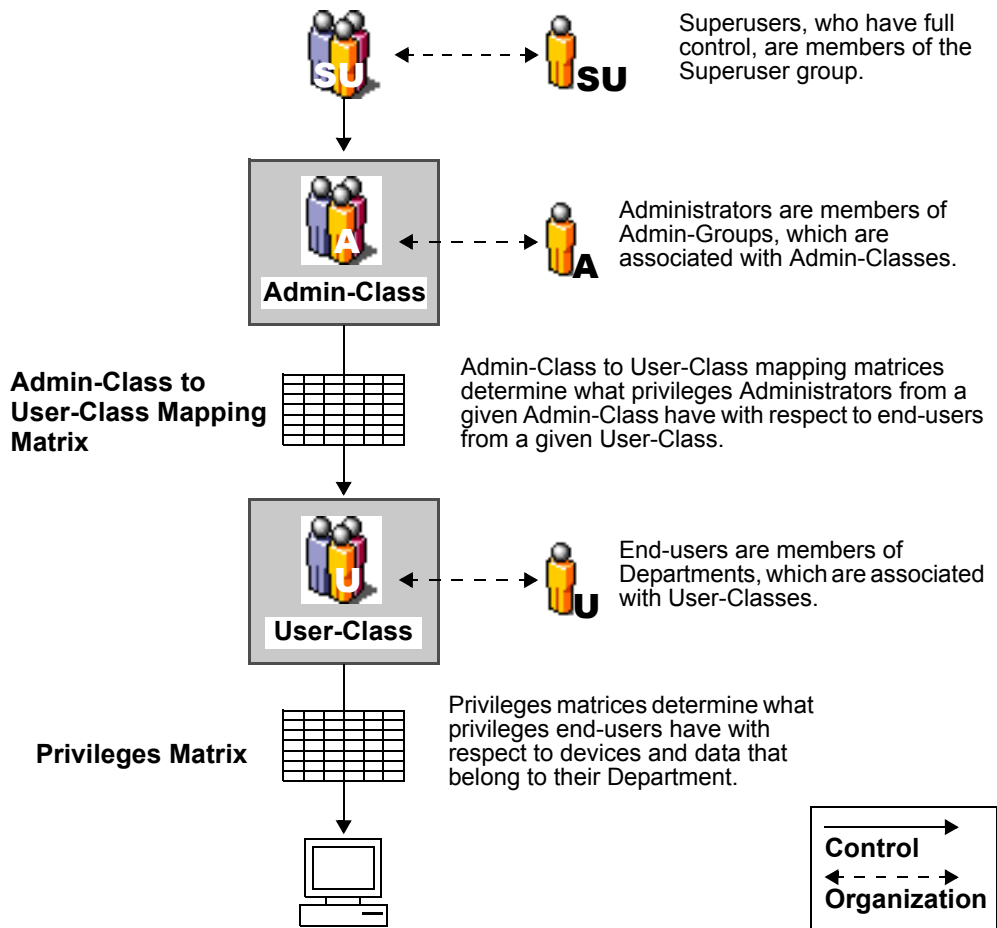


Figure 8.2 NetVigil Security Model

8.1.1 End-users and Departments

At the bottom of the NetVigil administrative hierarchy is the **end-user**. Each end-user is a member of a single **Department**. Departments can reflect divisions within the company (e.g., PAYROLL), locations (e.g., DENVER), or other meaningful categories.

End-users with full permissions can create/delete, read, update, and suspend/resume the following: devices, tests, actions, and SNMP Traps. In addition to the tasks listed in the privileges matrix (described in Section 8.1.2, “User-Classes and Privileges” on page 108), end-users can also

- view messages/alarms
- update device dependencies
- manage test baselines, containers, reports (scheduled and queried), schedules, message regular expressions, and web transaction test scripts
- update their user preferences
- access help

End-users from one Department cannot view data belonging to another Department. (An exception to this is an exported device and the tests associated with it. For information on exporting devices, see “Move a device to another department” on page 122).

8.1.2 User-Classes and Privileges

Each Department is associated with a single **User-Class**, which determines what **privileges** members of the Department have. Privileges control which tasks an end-user can perform with respect to various NetVigil entities.

In the User-Class privileges matrix that follows, each cell represents a single task/entity combination, with column headers specifying the task and row headers specifying the entity. For example, the X in the first cell of the first row means that end-users in this group can **Create and Delete Devices**. The X in the third cell of the second row means that end-users can **Update Tests**.

Table 8.1 User-Class Privileges Matrix

Access Privileges	Create/Delete	Read	Update	Suspend/Resume
Devices	X			
Tests			X	

Table 8.1 User-Class Privileges Matrix

Access Privileges	Create/Delete	Read	Update	Suspend/Resume
Actions				
SNMP Trap Actions				

NOTE When an end-user is created, it is assigned a role: either **Read-Only**, or **Read-Write**. Read-Write end-users have the privileges that are assigned to their Department’s User-Class. However, the Read-Only role supersedes the User-Class privilege matrix. In other words, if an end-user is Read-Only, they cannot create, modify, etc. even if their User-Class has the privileges to do so.

NOTE When you create User-Classes, consider two factors: The privileges of each set of end-users, and how the end-users will be administered. To give some users limited NetVigil privileges while others have full privileges, you must create separate User-Classes for each privilege level. Likewise, if two sets of users have the same NetVigil privileges, but you want each set to be administered by a separate Admin-Group, you must create separate User-Classes that can be mapped to the Admin-Classes. (For information on Administrators see Section 8.1.3, “Administrators and Admin-Groups” on page 109 and Section 8.1.4, “Admin-Classes and User-Class Mapping” on page 110.)

8.1.3 Administrators and Admin-Groups

Some administrative tasks can’t be done by end-users. These tasks are done by **Administrators**, who are members of **Admin-Groups**. Unlike end-users, Administrators can have visibility across Departments.

Each Administrator is a member of a single Admin-Group. Admin-Groups can reflect divisions within the company (e.g., NOC), locations (e.g., DENVER-ADMIN), or other meaningful categories.

Members of an Admin-Class that has full permissions with respect to a User-Class can do everything specified in the mappings matrix for entities belonging to the User-Class. (Mapping matrices are described

in Section 8.1.4, “Admin-Classes and User-Class Mapping” on page 110.) In addition to the tasks listed in the mapping matrix, Administrators can also

- view messages/alarms
- manage containers, reports (scheduled and queried), and actions for their Admin-Group
- search users
- export or move devices (if the administrator has control over both the source and the target department)
- represent users (the administrator still has write privileges, even if the represented user does not)
- update their own preferences
- access help

Administrators can NOT do the following, unless they represent an end-user:

- manage test baselines, devices, tests, schedules, message regular expressions, and web transaction test scripts
- update device dependencies

Unlike End-User Departments, Admin-Groups do not own devices and tests.

8.1.4 Admin-Classes and User-Class Mapping

Each Admin-Group is associated with one **Admin-Class**, which determines what privileges members of the Admin-Group have *with respect to specific User-Classes*. More precisely, privileges control which tasks members of an Admin-Group can perform with respect to entities belonging to the *Departments* associated with specific User-Classes.

An **Admin-Class to User-Class Mapping Matrix** determines which tasks one Admin-Class can perform with respect to one User-Class. In order to control three separate User-Classes, an Admin-Class requires three separate mapping matrices.

The relationship between Admin-Classes and User-Classes is a many-to-many relationship. That is, a single Admin-Class can control multiple User-Classes, and a single User-Class can be controlled by multiple Admin-Classes.

In the Admin-Class to User-Class Mapping matrix that follows, each cell represents a single task/entity combination. Assuming that the Admin-Class represented is called ADMIN, and the User-Class is USER, the X in the first cell of the first row means that members of Admin-Groups associated with ADMIN can **Create** and **Delete Devices** for Departments associated with USER. The X in the third cell of the fifth row means that ADMIN can **Update Departments** for USER.

Table 8.2 User-Class Mapping Matrix

Access Privileges	Create/Delete	Read	Update	Suspend/Resume
Devices	X			
Tests				
Actions				
SNMP Trap Actions				
Departments			X	
End-users				
Service Classes				

NOTE When an Administrator is created, it is assigned a role: either **Read-Only**, or **Read-Write**. Read-Write Administrators have the privileges that are assigned to their Admin-Group’s Admin-Class. However, the Read-Only role supersedes the Admin-Class to User-Class Mapping matrix. In other words, if an Administrator is Read-Only, they cannot create, modify, etc. even if their Admin-Class has the privileges to do so.

NOTE When you create Admin-Classes, consider two factors: The privileges of each set of Administrators, and how the end-users will be administered. To give some Administrators limited NetVigil privileges while others have full privileges, you must create a separate Admin-

Class for each privilege level. Likewise, if two sets of Administrators have the same NetVigil privileges, but each set will administer different end-users, you must create discrete Admin-Classes that can be mapped to separate User-Classes. (For information on User-Classes, see Section 8.1.2, “User-Classes and Privileges” on page 108.)

8.1.5 Superusers

At the top of the NetVigil security hierarchy is the **Superuser**. Superusers, who are members of the **Superuser-Group**, have complete access to all entities in the system and perform tasks that cannot be done by end-users or Administrators. For security reasons, the number of Superusers should be as small as possible.

A Superuser can do the following:

- view messages/alarms
- view all containers, departments, devices, and tests
- export/move devices between any Departments
- manage reports (scheduled and queried), containers and actions for the Superuser group
- search users
- represent Administrators or end-users
- manage DGE locations, DGEs, Admin-Classes, Admin-Groups, User-Classes, and Departments
- manage containers, actions
- update their own preferences
- access help

A superusers can NOT do the following, unless they represent an end-user:

- manage test baselines, devices, tests, schedules, message regular expressions, and web transaction test scripts
- update device dependencies

Unlike end-user Departments, The Superuser-Group does not own devices and tests.

8.2 Putting it all Together: A Case Study

The sections that follow show how a complex administrative hierarchy can be implemented in NetVigil.

Case Study: End-users and Departments

Acme Corporation has two corporate divisions:

- Finance, which consists of two subdivisions:
 - ▶ Payroll, which includes Paul and Parag
 - ▶ Human Resources, which includes Helen and Henry
- Engineering, which consists of two subdivisions:
 - ▶ Development, which includes Dave and Denise
 - ▶ Manufacturing, which includes Manoj and Maria

Paul, Parag, Helen, Henry, and the other employees of Acme are all **end-users**.

Within the NetVigil administrative hierarchy, one **Department** is set up for each corporate subdivision:

- PAYROLL, which includes Paul and Parag
- HR, which includes Helen and Henry
- DEVL, which includes Dave and Denise
- MANUF, which includes Manoj and Maria

Case Study: User-Classes and Privileges

To allow the Finance and Engineering divisions within the company to be administered separately, two User-Classes are created:

- FINANCE-RW, which is associated with the PAYROLL and HR Departments.
- ENGINEERING-RW, which is associated with the DEVL and MANUF Departments.

Privileges are configured so that end-users associated with these User-Classes have full read and write privileges over all NetVigil entities. That is, they can create their own devices, run and suspend tests, etc., and they can view data created by others within their Departments.

End-users cannot view data belonging to other Departments, so members of PAYROLL cannot check the status of tests for a server that belongs to DEVL.

Case Study: Administrators and Admin-Groups

Acme Corporation has two IT divisions, one for each of the main corporate divisions:

- Finance IT, which includes Frank
- Engineering IT, which includes Elizabeth

Each IT division is responsible for daily maintenance of the networks and equipment of two corporate subdivisions, represented in NetVigil by two distinct Departments. To give Frank and Elizabeth access to data across Departments, two Admin-Groups are set up, one for each IT division:

- IT-FINANCE, which controls the PAYROLL and HR Departments
- IT-ENGINEERING, which controls the DEVL and MANUF Departments

Acme also has a NOC group, which handles network troubleshooting, security, etc. for the entire company. Members of the NOC need access to all networks within the company.

- A third Admin-Group, NOC, controls all Departments.

Lastly, Acme's CTO and CIO want to run custom reports to check network usage by cost center, make predictions about future hardware costs, etc. While they need access to data from all Departments, they don't need to manage Departments or entities belonging to Departments.

- An Admin-Group called MGMT is created. This Admin-Group has read-only access to all Departments.

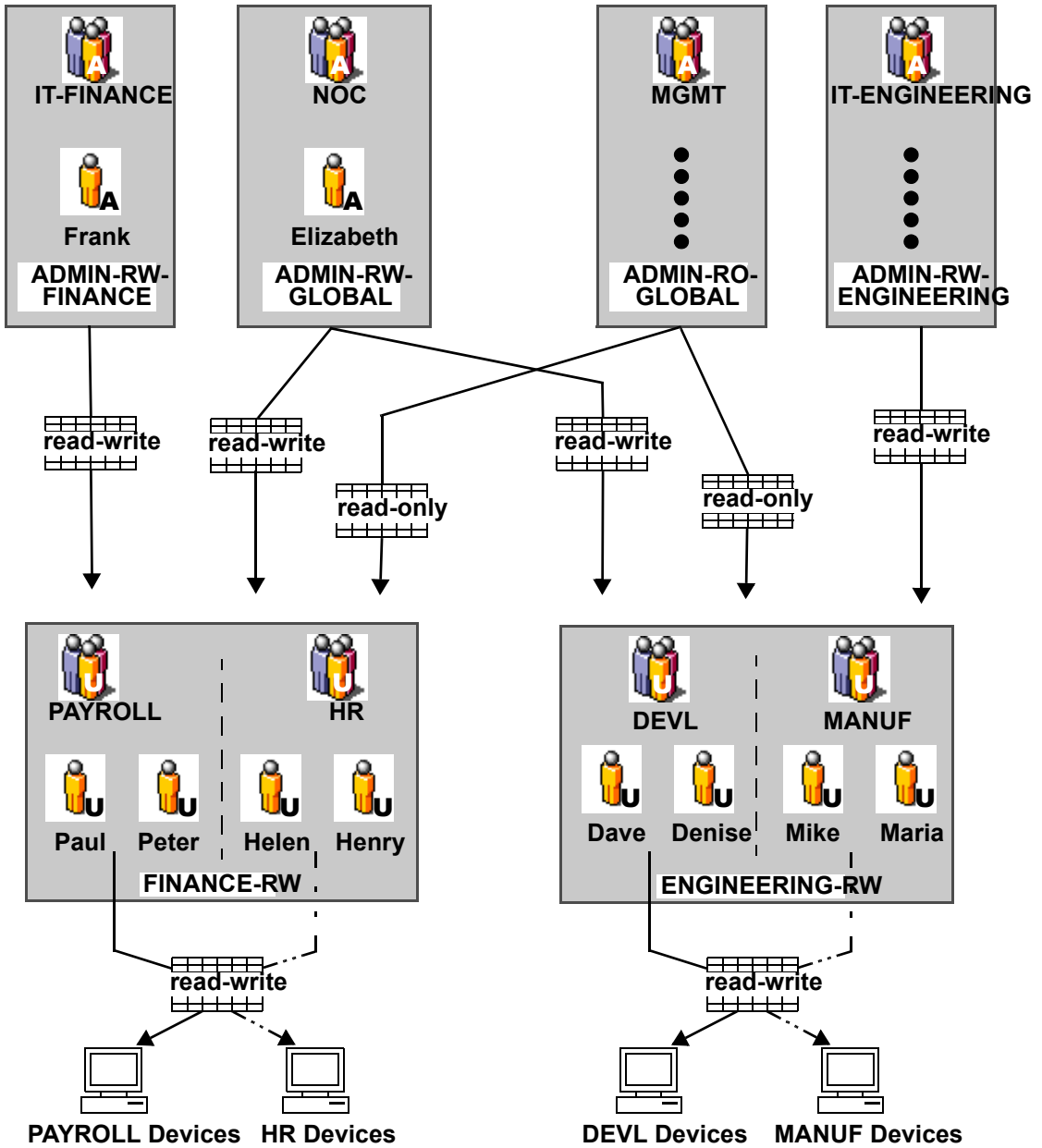
Case Study: Admin-Class to User-Class Mapping

All Admin-Groups associated with the same Admin-Class have the same level of control over the same User-Classes. In Acme Corporation, each Admin-Group has separate access requirements, so it is necessary to create a separate Admin-Class for each one:

- ADMIN-RW-FINANCE is the Admin-Class associated with IT-FINANCE. It is mapped to the FINANCE-RW User-Class, giving Frank, who belongs to IT-FINANCE, full read-write control over the PAYROLL and HR Departments.
- ADMIN-RW-ENGINEERING is the Admin-Class associated with ENGINEERING. It is mapped to the ENGINEERING-RW User-Class, giving Elizabeth, who belongs to IT-ENGINEERING, full read-write control over the DEVL and MANUF Departments.
- ADMIN-RW-GLOBAL is the Admin-Class associated with NOC. It is mapped to both the FINANCE-RW and ENGINEERING-RW User-Classes, giving members of the NOC Admin-Group full read-write control over all Departments.
- ADMIN-RO-GLOBAL is the Admin-Class associated with MGMT. It is mapped to both the FINANCE-RW and ENGINEERING-RW User-Classes, but the mapping matrices only allow limited privileges. Members of the MGMT Admin-Group have read-only control over all Departments.

Case Study Diagram

For the key to icons used in this diagram, see Section 8.1, “Security Model Overview” on page 105.



8.3 Managing the Security Model

8.3.1 Managing User-Classes

Only a superuser can create, update, and delete User-Classes.

Configuring a new User-Class involves the following tasks:

1. Create and name the User-Class
2. Define privileges and limits for end-users in the group. (For an explanation of the privileges matrix, see Section 8.1.2, “User-Classes and Privileges” on page 108.)

The instructions that follow describe these tasks in detail.

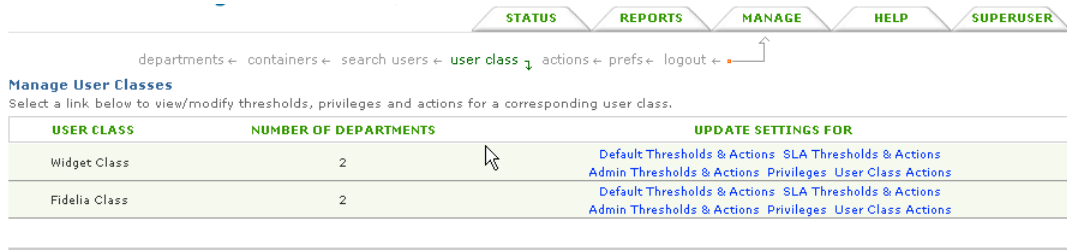


Figure 8.3 Managing User Classes

SUPERUSER

□ Step 1: Create a New User-Class

NOTE *User-Classes can also be created by importing a configuration file via the socket server (see Chapter 23, “BVE FlexAPI Protocol Reference” for details).*

1. Login to NetVigil as a superuser.
2. Click `SUPERUSER | user class`.
3. On the User Classes page, click **Create a New User Class**.
4. Fill in the **Name** field with a unique User-Class name. Optionally, enter a comment in the area provided.
5. Click **Create User Class**.

□ **Step 2: Define User-Class Privileges and Limits**

1. Login to NetVigil as a superuser.
2. Click `MANAGE | user class`.
3. On the Manage User Classes page, find the User-Class for which you want to define privileges and click the **Privileges** link in the **Update Settings For** column.
4. Select the access privileges that you want to enable for this User-Class. (For an explanation of the privileges matrix, see Section 8.1.2, “User-Classes and Privileges” on page 108.)
5. Select the limit for **Minimum Test Interval**.
6. Set the maximum limits for adding devices, reports, action profiles, and tests (use integers greater than or equal to 1, or type in unlimited).
7. Click **Update Privileges** to save your changes.

5/11/05 9:43:25 AM EDT
logged in as superuser (superuser/rw)

STATUS REPORTS MANAGE HELP SUPERUSER

dge mgmt ← admin class ↓ user class ← discover ← logout ←

User Class Privileges
Admin Class: Widget Admin Class
User Class: Widget Class

ACCESS PRIVILEGES	CREATE/DELETE	READ	UPDATE	SUSPEND/RESUME
Devices	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Tests	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Actions	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
SNMP Trap Actions	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Departments	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Users	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
User Classes	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Limits	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Containers	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Update Privileges

Figure 8.4 *Setting limits and privileges for a User Class*

8.3.2 Managing Departments

NetVigil's security/administration model is done using a combination of Department and user entities. Departments can have a single end-user, or multiple end-users. To add a new end-user to the system, you need to first create a Department and then create an end-user. For convenience, NetVigil auto-generates a default end-user for each Department created. The name of the auto-generated end-user defaults to the Department name, and the password is e-mailed to the contact e-mail address on the Department.

Service Providers can integrate the system with their customer provisioning systems, and set up new Departments automatically. In addition, lists of Departments and end-users can be imported into the system via the BVE Socket Protocol to facilitate this process (see Chapter 23, "BVE FlexAPI Protocol Reference" for details).

Create a new Department:


1. Click the **MANAGE** tab.
2. On the Manage Departments page, click **Create New Department**.
3. On the Create Department page, select the new Department's **Class** from the drop down menu.
4. Fill in all required fields, which are marked with an asterisk (*).
5. Optionally, enter additional information in the fields not marked with an asterisk.

□ Delete a Department

WARNING Deleting a Department permanently removes the Department and all the end-users associated with that Department from the database. In addition, any devices and tests created by that Department's end-users are permanently deleted. **DEPARTMENT DELETIONS ARE NOT REVERSIBLE.** We recommend that you suspend Departments instead of deleting them.


1. Click the **MANAGE** tab.
2. On the Manage Departments page, find the row for the Department you want to Delete and click the **Delete** link in the **Modify** column.
3. If you are certain that you want to delete this Department, click **Delete Department** in the confirmation dialogue that appears.

Move a device to another department

1. Click `STATUS | devices`.
2. On the Device Status Summary page, find the row for the device that you want to shift and click **Modify** .
3. On the Manage End User Device page, select **Move This Device To Another Department**.
4. Select the **Destination Department** for the device, enter the **Device Name in New Department**, and then click **Next**. (The Destination Department must be associated with the same User-Class as the original Department.)
5. If you are certain that you want to move the device, click **Move** in the Move Device page.

All of the data and provisioning information for the device are moved to the Destination Department.

Export a device to multiple Departments

1. Click `STATUS | devices`.
2. On the Device Status Summary page, find the row for the device that you want to shift and click **Modify** .
3. On the Manage End User Device page, select **Export This Device (All Or Some Tests) To Another Department**.

4. Select the **Destination Department** for the device, enter the **Device Name in New Department**, and then click **Next**. (The Destination Department must be associated with the same User-Class as the original Department.)
5. Select those tests that you want to export with the device, and then click **Export Device**.

Also note that when a device and all tests are exported to another department, the new tests created are not made visible to the target department.

← containers ← departments → devices

Manage End User Device
Device: ecos

Select an operation from the list below, provide other requested parameters and click on "Next" to continue
* - indicates a required field

Export This Device (All Or Some Tests) To Another Department

Move This Device To Another Department

Select Destination Department for "ecos"

* Device Name in New Department:

Provisioning information for the device and exported tests are available to the Destination Department. The Destination Department can configure new tests for the device.

8.3.3 Managing End-Users

Create a new user

1. Click the **MANAGE** tab.
2. On the Manage Departments page, find the Department to which you want to add a user and click **Create User**.
3. In the **Role** field, select the new user's role (Read-Only or Read-Write).
4. Fill in all required fields, which are marked with an asterisk (*).
5. Optionally, enter additional information in the fields not marked with an asterisk.
6. Click **Create User**.

Update a user

1. Click `MANAGE | search users`.
2. On the Search Users page, select the field(s) on which you want to search and enter the keyword(s) in the **Enter keyword(s) here** field. Note that keyword searches are case sensitive. For example, to find all users whose first name is John, select **First Name**, and enter “John” as the keyword.
3. Click **Search Users** to begin the user search.
4. On the User Search Results page, find the user you want to update and click **Update** in the **Modify** column.
5. On the Update User page, make the desired changes to the user’s information, and then click **Update User**.

❑ Delete a user

WARNING Deleting a user permanently removes the user and all information associated with that user from the database. **USER DELETIONS ARE NOT REVERSIBLE.** We recommend that you suspend users instead of deleting them.

1. Click `MANAGE | search users`.
2. On the Search Users page, select the field(s) on which you want to search and enter the keyword(s) in the **Enter keyword(s) here** field. Note that keyword searches are case sensitive. For example, to find all users whose first name is John, select **First Name**, and enter “John” as the keyword.
3. Click **Search Users** to begin the user search.
4. On the User Search Results page, find the user you want to delete and click **Delete** in the **Modify** column.
5. If you are sure that you want to delete the user, click **Delete** in the confirmation screen that appears.

8.3.4 Managing Admin-Classes

Only a superuser can create, update, and delete Admin-Classes.

Configuring a new Admin-Class involves the following tasks:

1. Create and name the Admin-Class

2. Map the Admin-Class to those User-Classes that it will control, defining separate privileges for each User-Class. (For an explanation of mapping matrices, see Section 8.1.4, “Admin-Classes and User-Class Mapping” on page 110.)

The instructions that follow describe these tasks in detail.

SUPERUSER

❑ Step 1: Create a New Admin-Class

NOTE Admin-Classes can also be created by importing a configuration file via the socket server (see Chapter 23, “BVE FlexAPI Protocol Reference” for details).

1. Login to NetVigil as a superuser.
2. Click SUPERUSER | admin class.
3. On the Admin Classes page, click **Create a New Admin Class**.
4. Fill in the **Name** field with a unique Admin-Class name. Optionally, enter a comment in the area provided.
5. Click **Create Admin Class**.

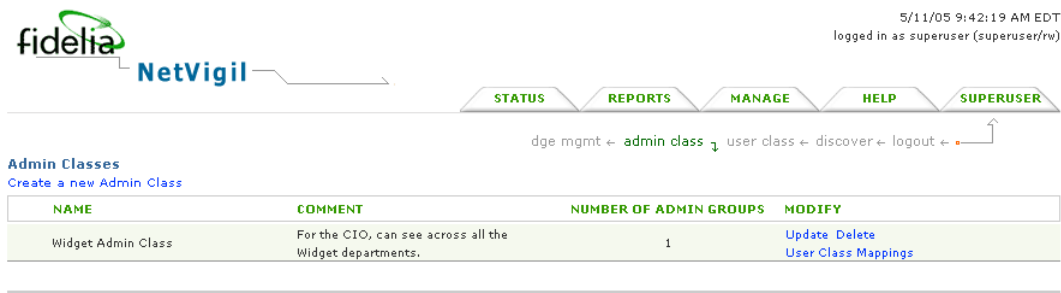


Figure 8.6 Creating an Admin Class

SUPERUSER

□ Step 2: Create User-Class Mappings and Define Admin-Class to User-Class Privileges

NOTE: *Creation of User-Class/Admin-Class relationships and privileges is complex and requires a thorough understanding of the NetVigil Security Model. For a detailed description of the security model, see Section 8.1, “Security Model Overview” on page 105.*

1. Click `SUPERUSER | admin class`.
2. On the Admin Classes page, find the Admin-Class for which you want to create a User-Class Mapping and click **User-Class Mappings**.
3. On the User Class Mappings page, click **Assign User Class to Admin Class**.
4. On the Create User Class Mapping page, select a User-Class from the **Name** list, and then click **Create User-Class Mapping**.
5. On the User-Class Privileges page, select access privileges using the check boxes provided. (For information about the Admin-Class to User-Class mapping matrix, see Section 8.1.4, “Admin-Classes and User-Class Mapping” on page 110.)

- Click **Update Privileges**. Note that once a User-Class is assigned to an Admin-Class, that User-Class is no longer available for assignment to a different Admin-Class.

5/11/05 9:43:25 AM EDT
logged in as superuser (superuser/rw)

STATUS REPORTS **MANAGE** HELP SUPERUSER

dge mgmt ← admin class ↓ user class ← discover ← logout ← →

User Class Privileges
Admin Class: Widget Admin Class
User Class: Widget Class

ACCESS PRIVILEGES	CREATE/DELETE	READ	UPDATE	SUSPEND/RESUME
Devices	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Tests	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Actions	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
SNMP Trap Actions	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Departments	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Users	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
User Classes	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Limits	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Containers	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Update Privileges

Figure 8.7 Assigning Admin-Class privileges over User-Class

8.3.5 Managing Admin-Groups

For each Admin-Group, a default Administrator is created. The username for the default Administrator is the same as the name of the Admin-Group. This information and the Administrator’s password are E-mailed to the Contact E-mail Address defined when the Admin-Group is created. You can also create additional Administrators, as described in “To create a new Administrator:” on page 129.

SUPERUSER

To create a New Admin-Group:

- Click the **MANAGE** tab.

2. On the Manage Admin Groups/Departments page, click **Create New Admin Group**.
3. On the Create Admin Group page, select the new Admin-Group's **Class** from the drop down menu.
4. Fill in all required fields, which are marked with an asterisk (*).
5. Optionally, enter additional information in the fields not marked with an asterisk.
6. Click **Create Admin Group**.

SUPERUSER

To suspend or activate an Admin-Group:

1. Click the **MANAGE** tab.
2. On the Manage Admin Groups/Departments page, find the row for the Admin-Group you want to suspend or activate and click the link in the **State** column. (If the Admin-Group is currently active, the link says **Suspend**. If the Admin-Group is currently suspended, the link says **Activate**.)
3. To suspend an Admin-Group, enter a reason for the suspension in the confirmation screen that appears, then click **Suspend Admin Group**. To activate an Admin-Group, click **Activate Admin Group** in the screen that appears.

To delete an Admin-Group:

WARNING Deleting an Admin-Group permanently removes the Admin-Group and all the Administrators associated with that Admin-Group from the database. **ADMIN-GROUP DELETIONS ARE NOT REVERSIBLE.** We recommend that you suspend Admin-Groups instead of deleting them.

1. Click the **MANAGE** tab.
2. On the Manage Admin Groups/Departments page, find the row for the Admin-Group you want to delete and click the **Delete** link in the **Modify** column.
3. If you are certain that you want to delete this Admin-Group, click **Delete Admin Group** in the confirmation screen that appears.

8.3.6 Managing Administrators

SUPERUSER

To create a new Administrator:

1. Click the **MANAGE** tab.
2. On the Manage Admin Groups/Departments page, find the Admin-Group to which you want to add an Administrator and click **Create User**.
3. In the **Role** field, select the new user's role (Read-Only or Read-Write).
4. Fill in all required fields, which are marked with an asterisk (*).
5. Optionally, enter additional information in the fields not marked with an asterisk.
6. Click **Create User**.

To update an Administrator:

See "Update a user" on page 124.

To delete an Administrator:

See "Delete a user" on page 124.

8.3.7 Representing Users

NetVigil enables Administrators to log in as if they were the end-user they are supporting. This is called **representing** an end-user. An Administrator who is representing an end-user is logged into the end-user's Department, with access to the Department's devices, tests, etc., while still retaining Administrator privileges.

This is especially helpful when an end-user has read-only capabilities and requests some type of Department modification. The Administrator can log in as Administrator, represent the end-user, and make any needed additions or modifications to devices, tests, actions, user profile or password.

□ **To represent a user:**

1. Click **MANAGE** | search users.
2. On the Search Users page, select the field(s) on which you want to search and enter the keyword(s) in the **Enter keyword(s) here** field. Note that keyword searches are case sensitive. For example, to find all users whose first name is John, select **First Name**, and enter “John” as the keyword.
3. Click **Search Users** to begin the user search.
4. On the User Search Results page, find the user you want to update and click **Represent** in the **Modify** column. You are automatically logged into that user’s Department. While you are representing the end-user, you see the Web interface as the end-user sees it.
5. Make additions or changes to the user Department as needed. Click **Logout** on the secondary navigation bar when you are finished.

NOTE *Do not use your browser's **Back** button to return to the administrator interface. You must log out and log in again to re-initiate your administrator session.*