Hewlett Packard Enterprise

HPE Network Node Manager i Software 10.20

Step-by-Step Guide to Using Security Groups

White Paper

Contents

Security Groups

This document discusses some Security Group concepts and provides an example of how to use Security Groups. This paper also provides an example of how to use Tenants and Security Groups in Global Network Management.

Introduction

NNMi includes a security model that provides restrictions to object access based on group membership (similar to Access Control Lists (ACLs), though different in implementation). This document discusses some Security Group concepts and gives a specific example of using Security Groups. This paper also discusses another feature of NNMi, Multi-Tenancy, which is closely related to Security Groups.

Using Security Groups and Multi-Tenancy you can configure NNMi to enable different operators to view items specific to their assignments and privileges. This restriction applies to nodes (and indirectly, to all subcomponents like interfaces, addresses, cards controlled at the node level) as well as incidents, maps, lists, and other views.

Security Concepts

Consider two types of groups: User Groups and Security Groups. User Groups combine users (user accounts) into groups. Users can belong to multiple User Groups. For example, a user could be a member of two different regional Level1 Operator groups.

Security Groups control which User Groups can access nodes. Each node (for instance, a switch, router, load balancer, or server) is a member of only one Security Group. An example of a Security Group would be nodes in a specific region, such as a data center.

A User Group mapping maps users to User Groups.

Security Group mapping establishes a relationship between User Groups and Security Groups, effectively granting permission for User Group members to access nodes in the Security Group. Security Group mapping also controls the level of action User Group members can perform on the nodes.

NNMi Administrator accounts can always access all nodes because Security Groups do not apply to NNMi Administrator accounts.

User interface access determines what actions and menu items are visible to User Group members while viewing the graphical user interface. This is achieved using predefined User Groups shipped along with the product. In most cases, you make the Security Group access level match the user interface access level; although this is not required.

Figure 1 provides a graphical representation of the groups and their relationships. The asterisks indicate that one or more mappings are permitted. The only restriction is that nodes must be in only one Security Group.

Figure 1: Groups and their Relationships

Security Groups Model

Consider the following scenario. Suppose you want to divide responsibility of your network monitoring based on geography. You have one set of operators that are in charge of monitoring nodes in the Kentucky region (a state with multiple cities). In addition, you have another set of operators in charge of monitoring nodes in the Detroit region (a large city). You also have one operator that needs to access nodes from both regions. You also have two NNMi administrators that maintain the NNMi system.

Figure 2 depicts the NNMi model of the scenario just described.

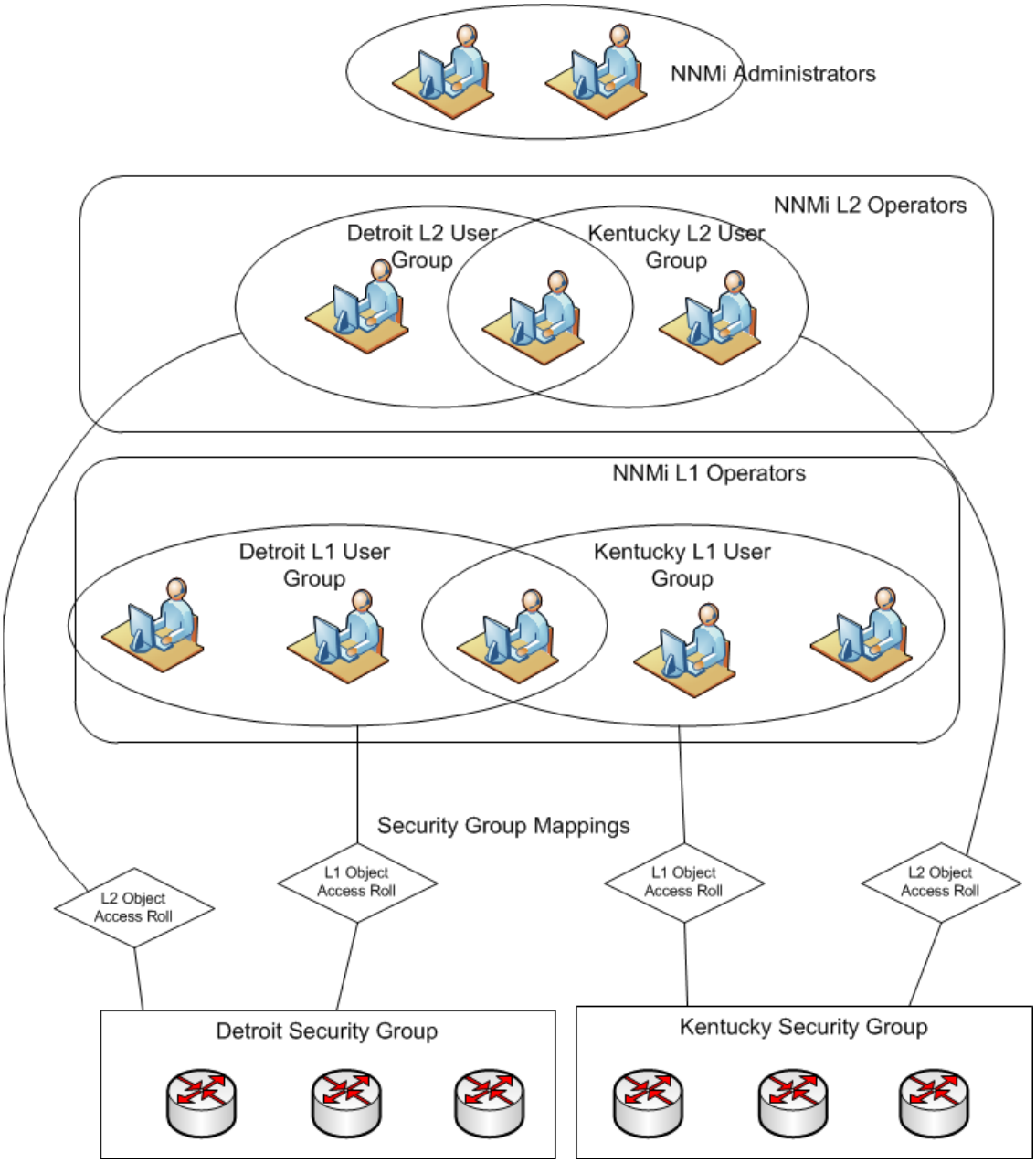

Figure 2: Security Groups Model

Security Groups Example

Consider the following example of the model previously discussed. In this implementation, there are the following users:

- A single NNMi administrator (Ringo)
- Level 1 and Level 2 operators (John, Paul, and George). One of the users, Paul, has access to both regions.

Table 1 shows the responsibilities of each user.

Tip: While it is possible for a user to be a Level 1 Operator for one set of nodes and a Level 2 Operator on another set of nodes within the security model, the NNMi console does not have the same level of separation. Therefore, do not mix levels for individual operators (unless you want to give some users additional capabilities).

TABLE 2. Users and Roles

Geography	User	User Group	Security Role
All	Ringo	N/A	NNMi Administrator
Detroit	John	Detroit Oper1	Level 1 Operator
	Paul	Detroit Oper2	Level 2 Operator
Kentucky	George	Kentucky Oper1	Level 1 Operator
	Paul	Kentucky Oper2	Level 2 Operator

The following list is the summary of the steps in this example. This example uses the Security Wizard but you could also use the Cli option of `nnmsecurity.ovpl` comprising arguments for below actions & also workspaces in the console.

1. Remove default User Group mappings
2. Create users
3. Create User Groups
   a. Kentucky Oper1
   b. Kentucky Oper2
   c. Detroit Oper1
   d. Detroit Oper2
4. Map Users to User Groups
5. Create Security Groups
   e. Kentucky Security Group
   f. Detroit Security Group
6. Map User Groups to Security Groups
7. Assign nodes to Security Groups

Note:
In this example, two User Groups, NNMi L1 Operators and NNMi L2 Operators, have been predefined to access the user interface.

Remove Default User Group Mappings

Remove the default User Group mappings (provided for backwards compatibility) so that no operator sees any nodes initially:

1. From the workspace navigation panel, select the Configuration workspace.
2. Expand the Security folder.

3. Click Security Group Mappings.
4. Select all the current mappings and delete them as shown in Figure 3

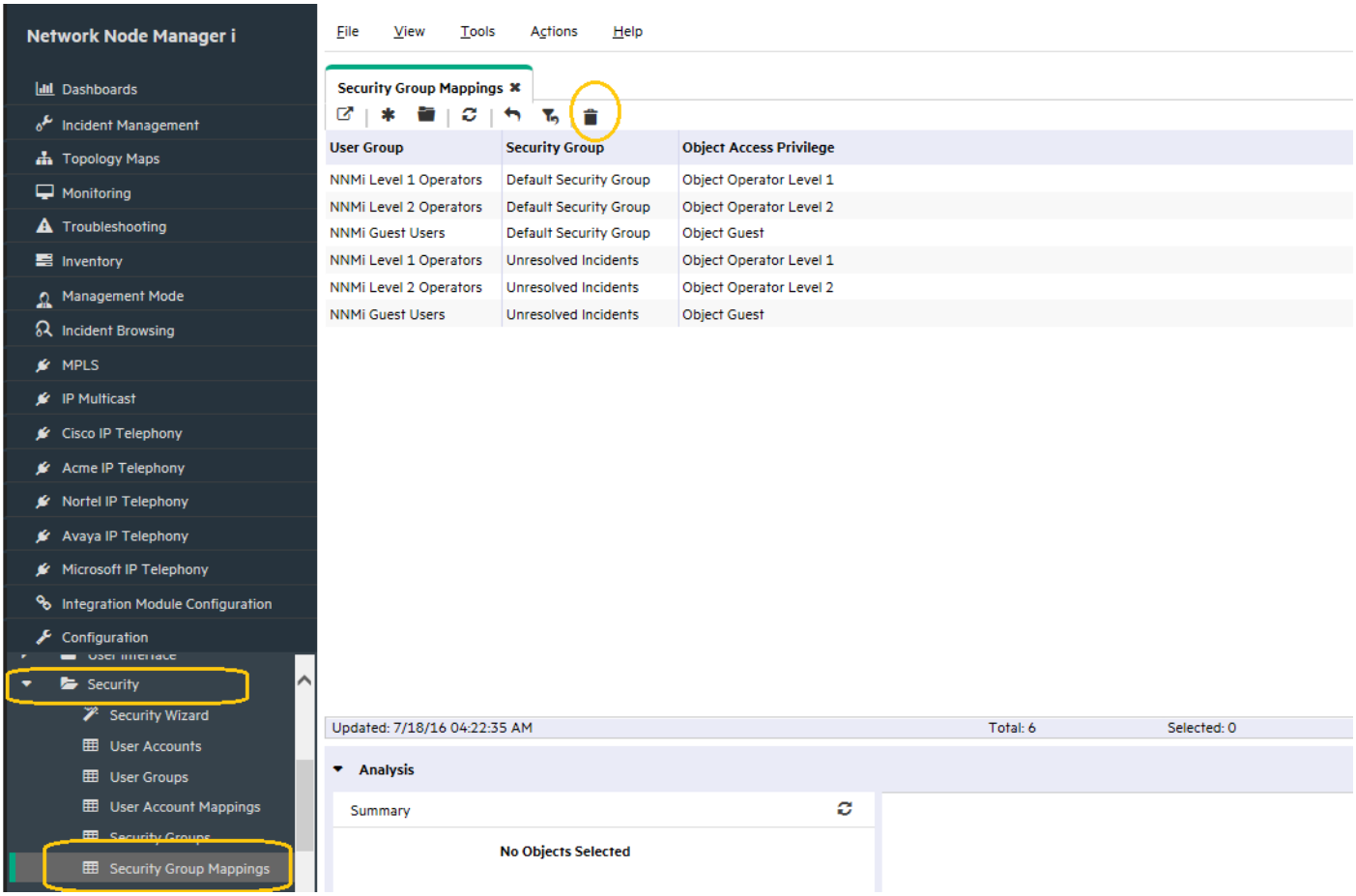

Figure 2: Security Group Mappings: Delete Default Mapping

Create Users

1. From the workspace navigation panel, select the **Configuration** workspace.
2. Expand the **Security** folder.
3. Click **Security Wizard**.
4. Click **Map User Accounts and User Groups**.
5. Click the **Create User Account** icon as shown in **Figure 4.**

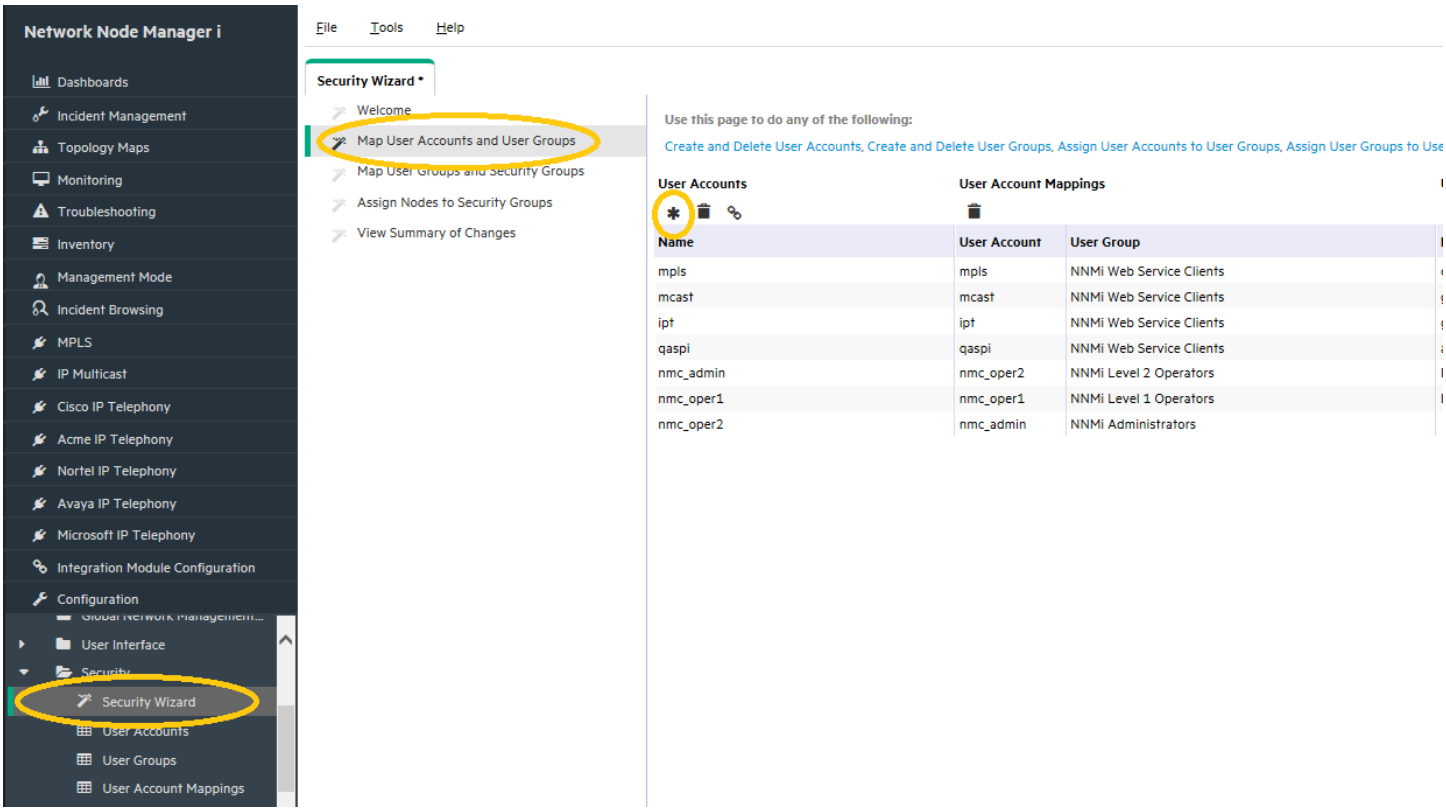

Figure 3: Security Wizard: Create User Account

6. Enter the **Name** and **Password** for each user

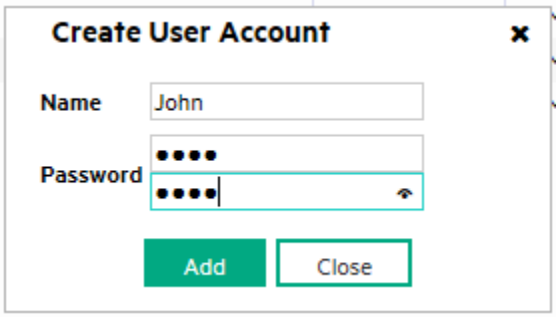

Figure 4: Create User Account Dialog Box

Create User Groups

1. Click the **Create User Group** icon as shown in **Figure 6**.

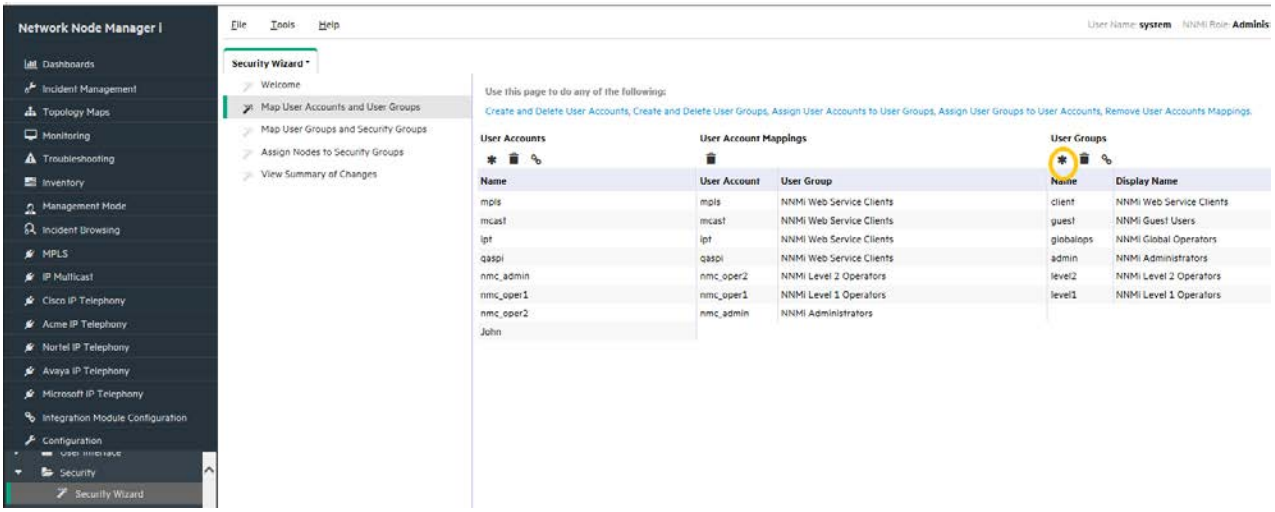

Figure 5: Security Wizard: Create User Group

2. Complete the **Create User Group** dialog box for each User Group.

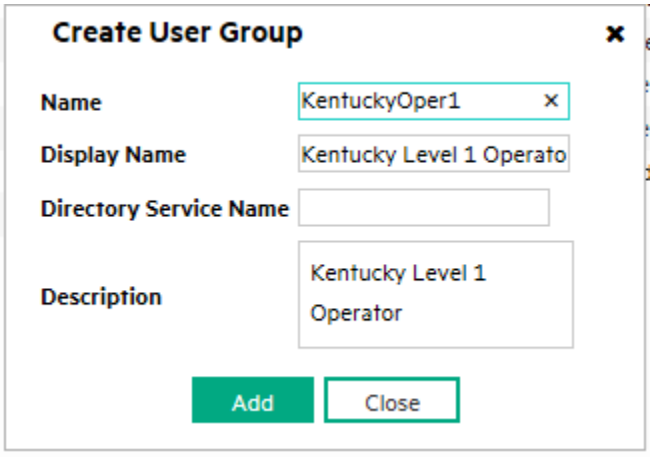

Figure 6: Create User Group Dialog Box

Map Users to User Groups

For each user, create a User Account Mapping as follows:

1. In the Security Wizard, click the user Name, then click the icon beside the desired level to define the mapping assignment as shown in **Figure 8**. Be sure to include both the special NNMi User Group for the user interface (Level 1, Level 2) and the custom User Group (for example, Detroit Level 1 Operators).
2. After creating all the User Account Mappings, click the Next button.

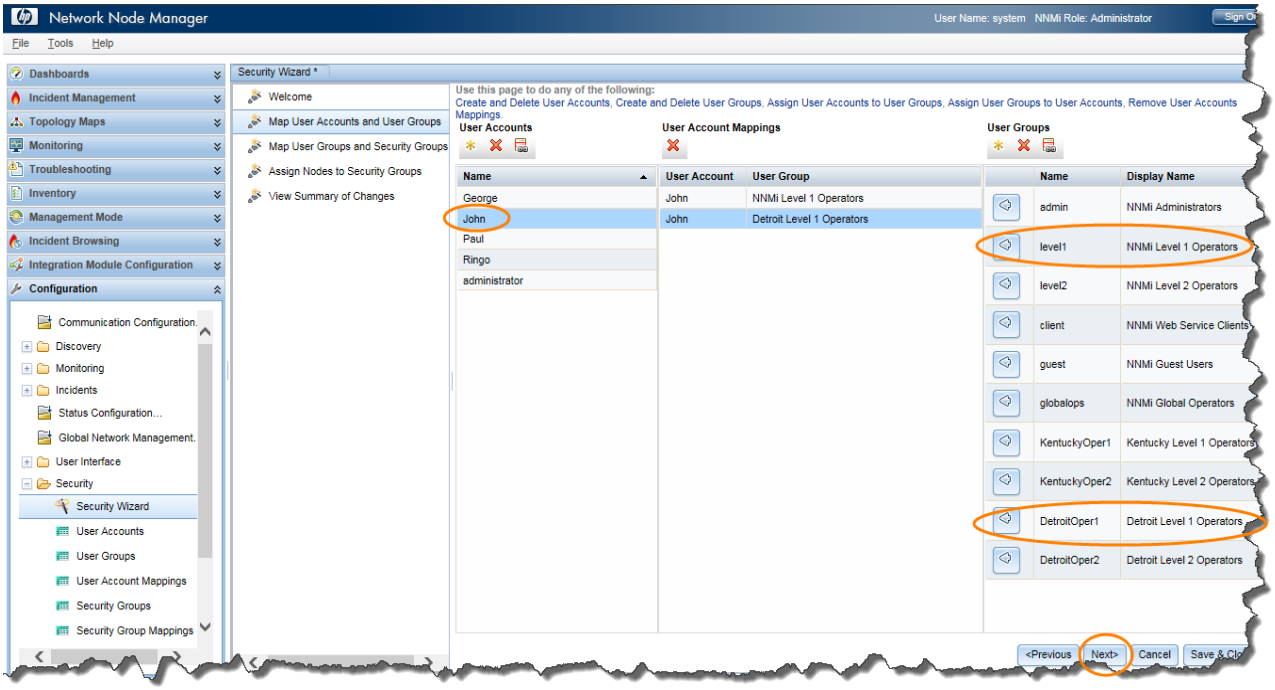

Figure 7: Security Wizard: User Account Mappings

Figure 9 indicates the items completed to this point (shown in yellow):

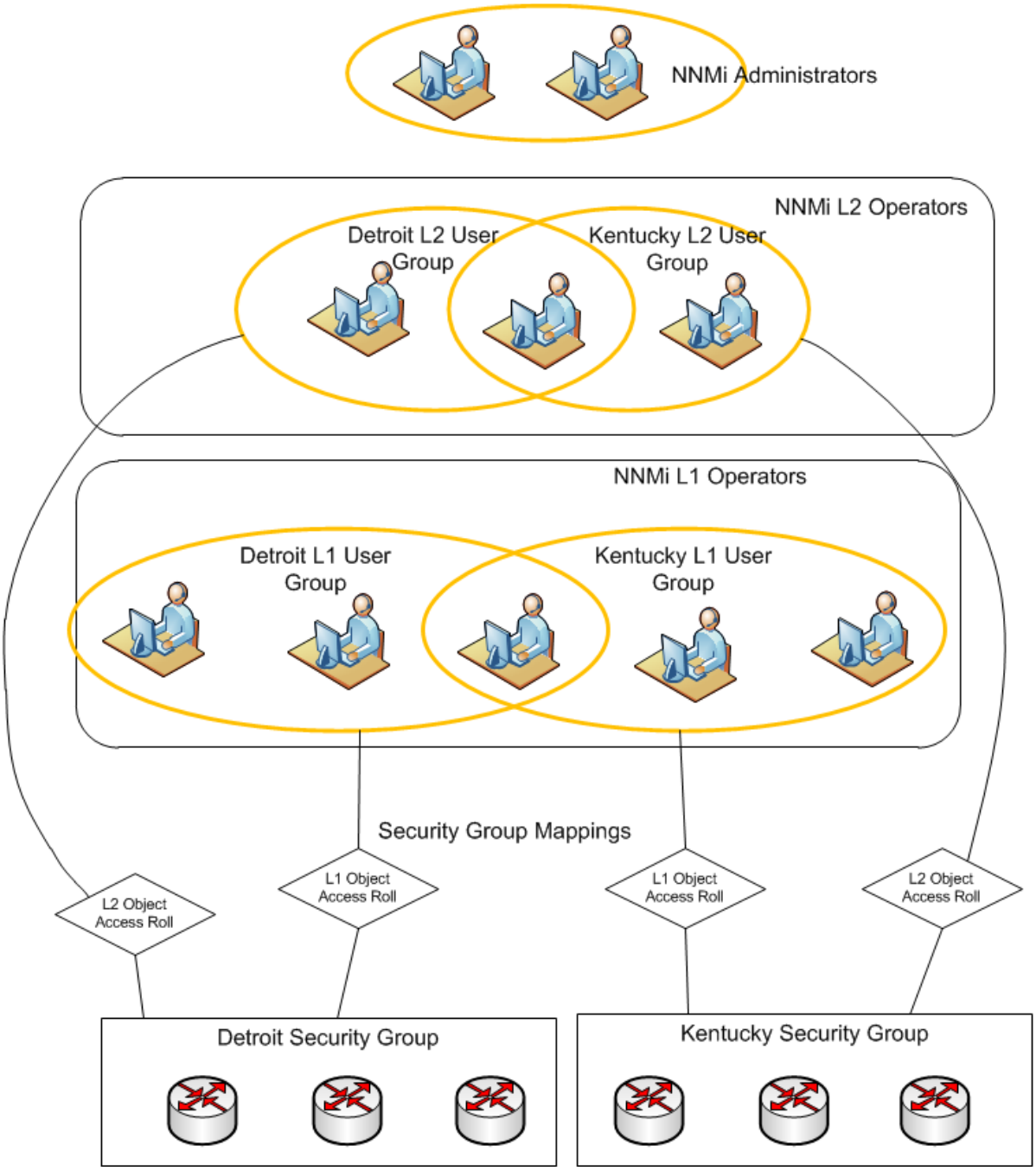

Figure 8: Completed Items

Create Security Groups

Create two Security Groups, one for Kentucky and one for Detroit:

1. In the Security Wizard, click the Create Security Group icon as shown in **Figure 10**.

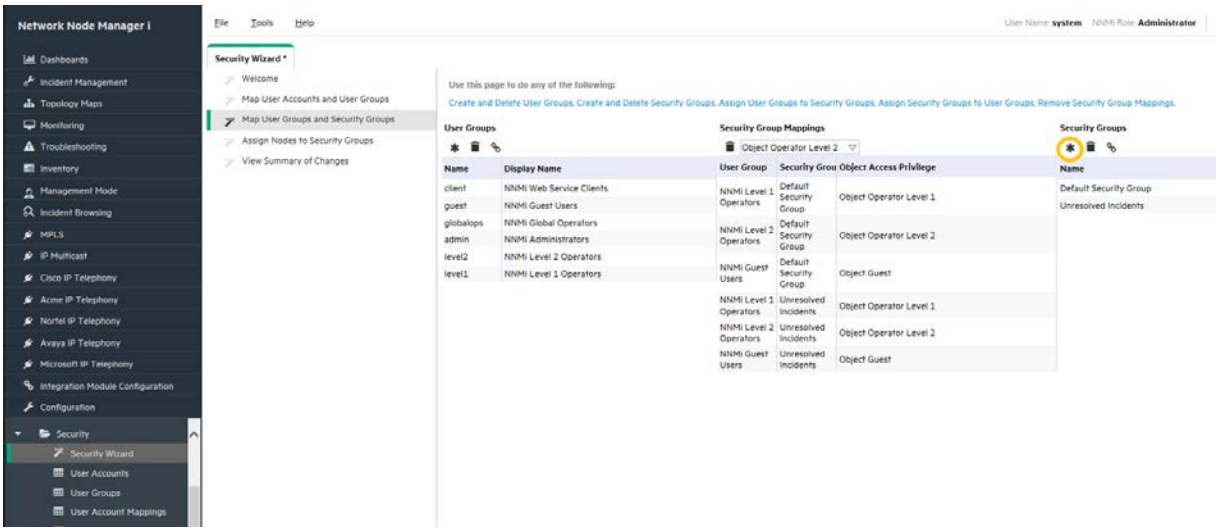

Figure 9: Security Wizard: Create Security Group

2. Enter the information for each Security Group in the **Create Security Group** dialog box as shown in **Figure 11.**

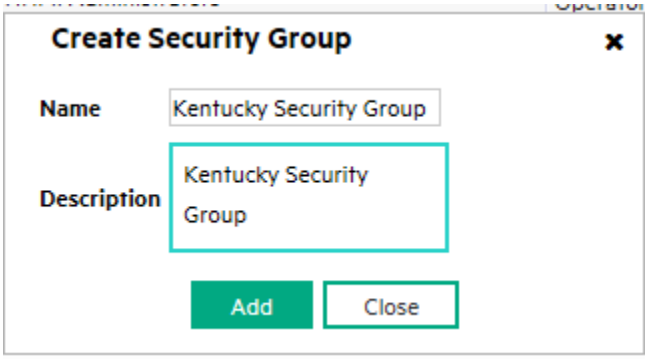

Figure 10: Create Security Group Dialog Box

Figure 12 indicates the items now completed (shown in yellow):

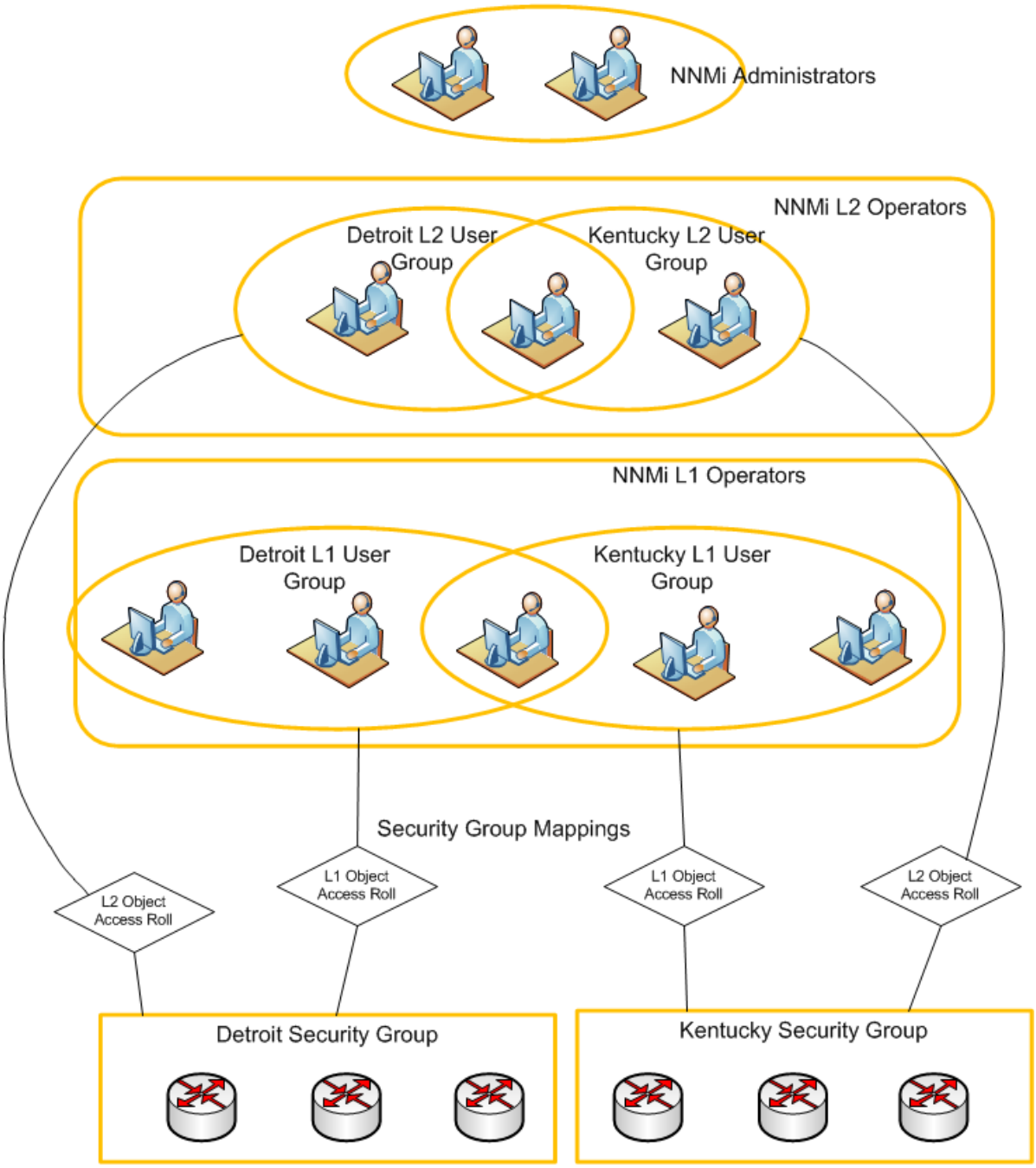

Figure 11: Completed Items

Map User Groups to Security Groups

For each User Group, do the following as shown in **Figure 13**:

1. Click the **User Group**.
2. Click the appropriate object level in the **Security Group Mappings** pull-down list.
3. Click the icon beside the desired **Security Group**.

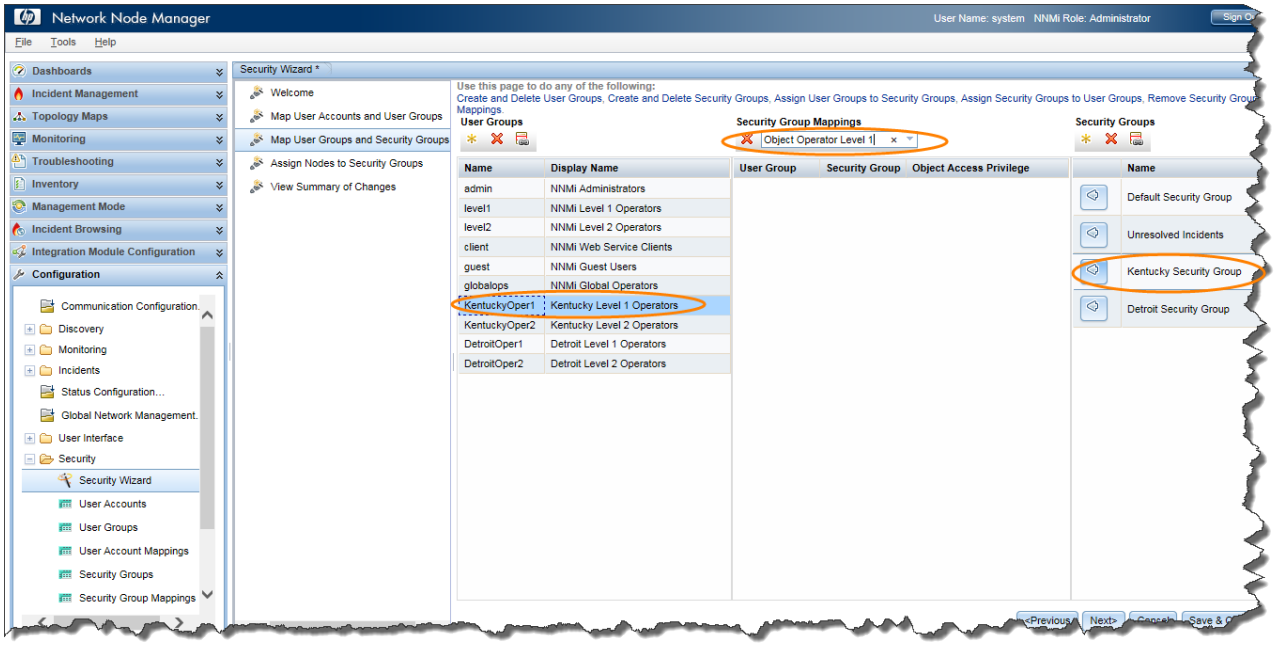

Figure 12: Security Wizard: Mapping Security Group

4. After you have defined all of the Security Group Mappings, click the Next button as shown in **Figure 14.**

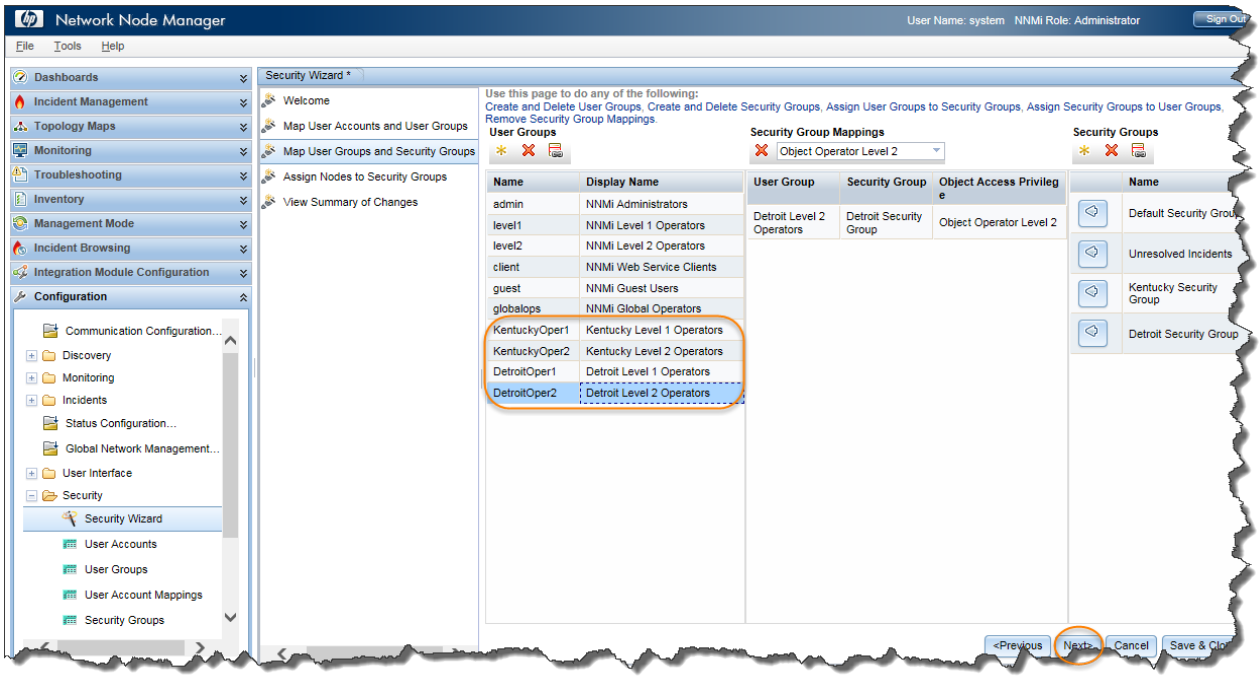

Figure 13: Security Wizard: Define Security Group Mappings

Figure 15 indicates the items now completed (shown in yellow).

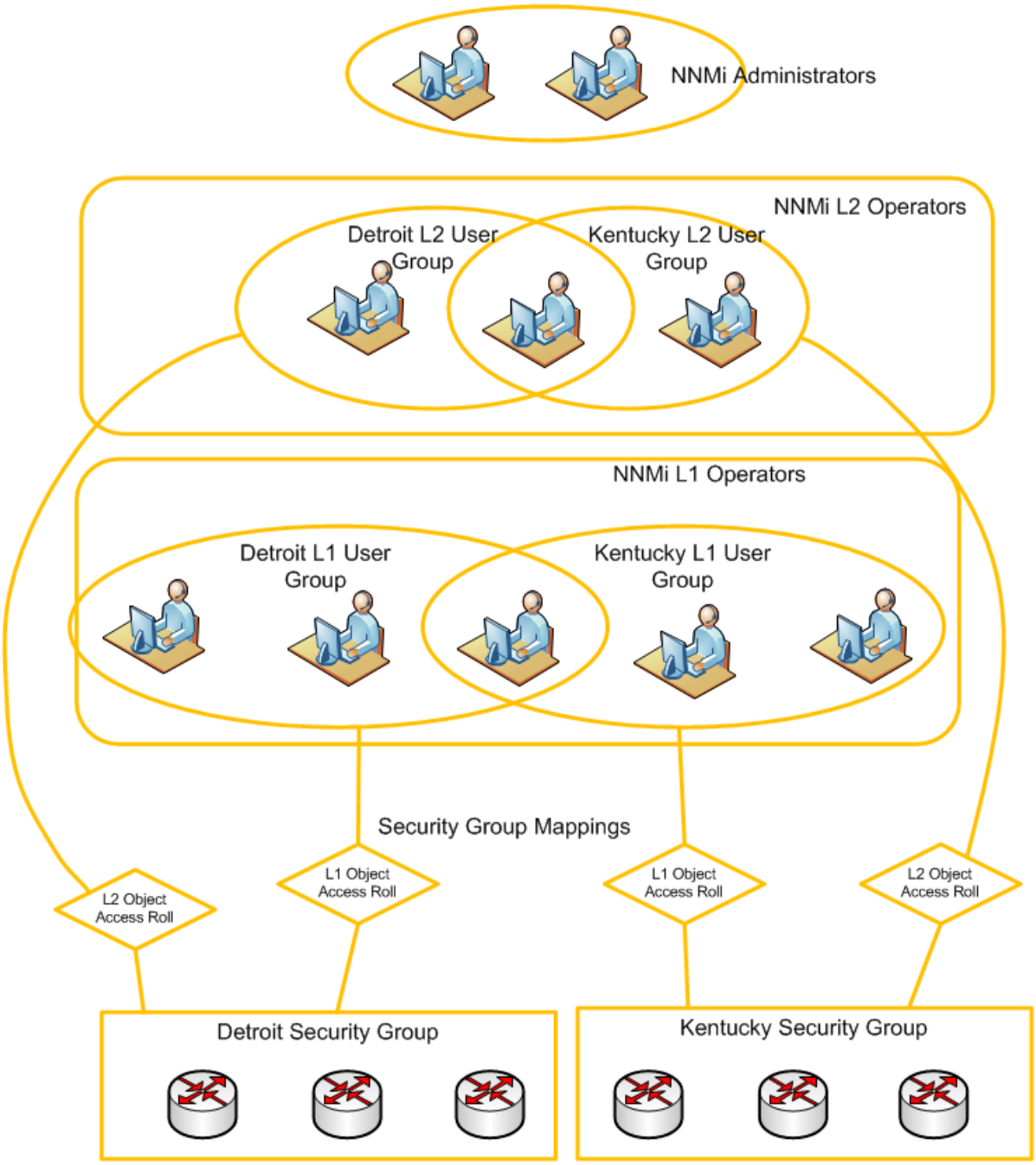

Figure 14: Completed Items

Assign Nodes to Security Groups

You can assign previously discovered nodes to Security Groups either in the **Security Wizard**, the **Node** form, or with the `nnmsecurity.ovpl` script. If you want to automatically assign nodes to a Security Group as they are discovered, use a "seeded discovery" along with the Tenant feature (discussed later in the Tenants section of this document).

This example includes the following assumptions:

1. The nodes have already been discovered.
2. You have created a Node Group that corresponds to each Security Group (Kentucky Nodes and Detroit Nodes).

Assign nodes to Security Groups as follows:

1. Click the Security Group to which you want to assign nodes (Kentucky Security Group in this example) as shown in **Figure 16**.
2. Click the nodes that needs to be assigned to the Security Group in the bottom portion of the wizard.

Tip: To facilitate the process of assigning nodes, you can use the Node Group Filter pull-down if a node group comprising Kentucky nodes is already created.

Tip: If there are many nodes in the Node Group, use the **CTRL+A** shortcut to select all of the nodes in the group.

3. Click the  Assign Selected Nodes to Selected Security Group icon.

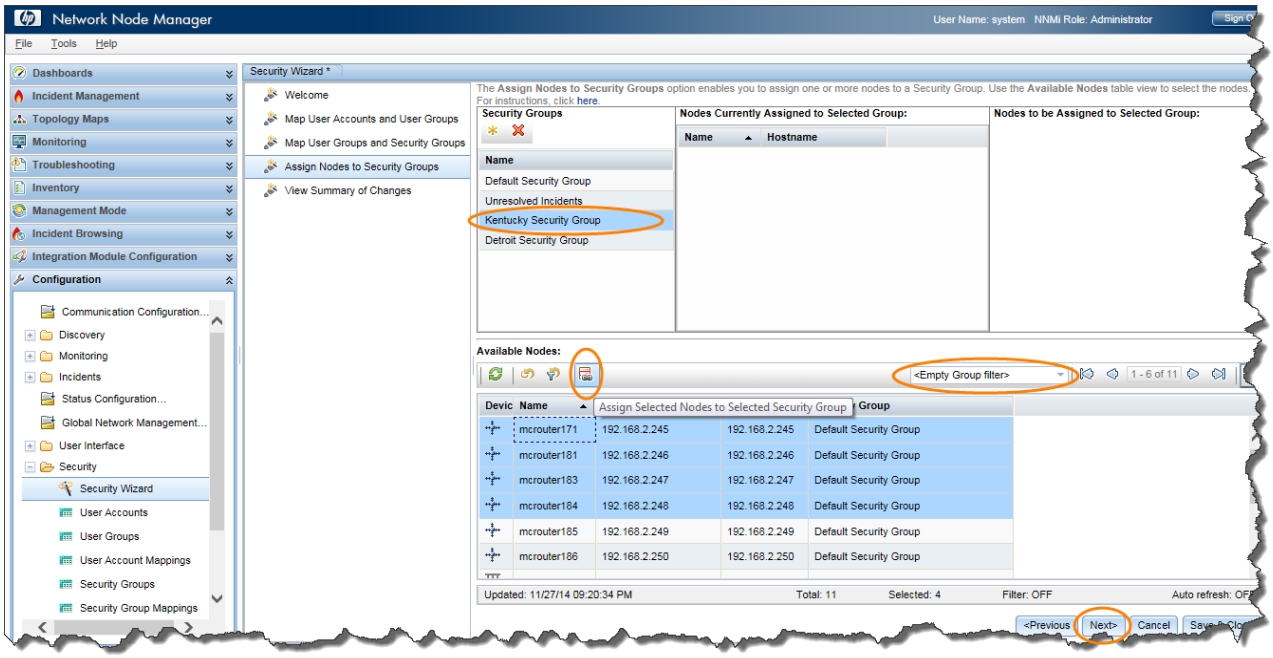

Figure 15: Security Wizard: Assign Nodes to Security Group

4. After you have assigned all the nodes, check to see that they are marked to be assigned; then click **Next**.
5. Finally, review the summary of changes as shown in **Figure 17**. After verifying the changes, click **Save and Close**.

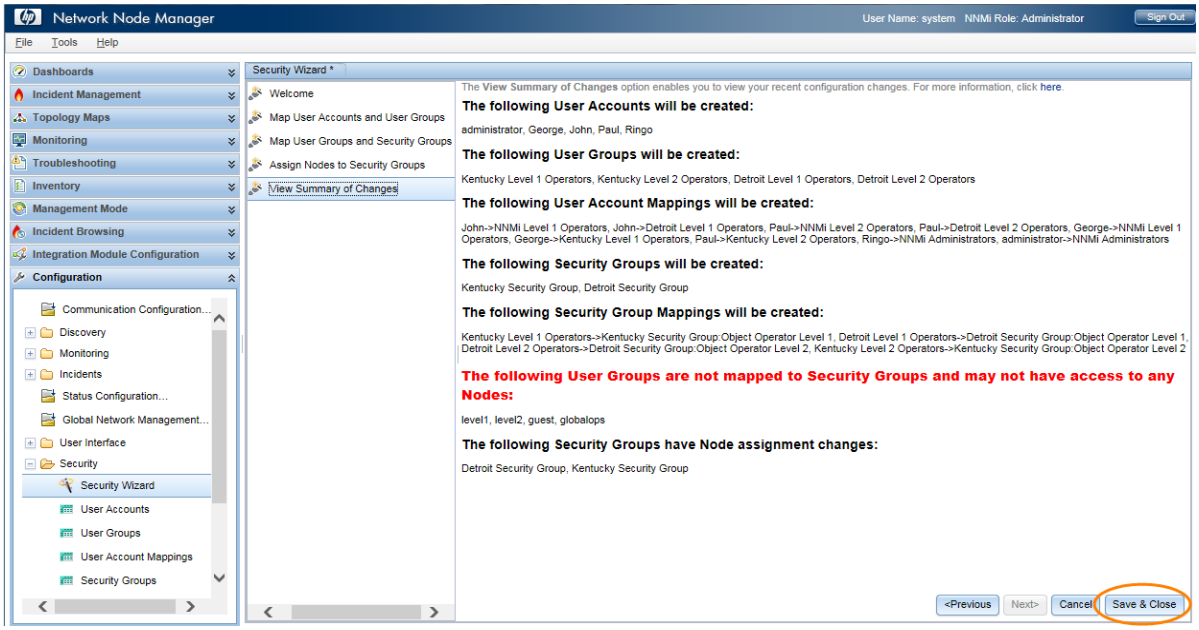

Figure 16: Security Wizard: Final Summary

Watch out for the red sentence before you click on **Save & Close**. This alerts the administrators configuring security model to re-visit if any configuration is missing. In the example above there have been no users who have been directly assigned only to User groups of level1, level 2, guest & globalops and hence the alert can be ignored and clicked on Save & Close.

Verify Example

Verify the previous example as follows:

1. Sign in to NNMi as George. You should see only Kentucky nodes as well as incidents on Kentucky nodes as shown in **Figure 18**.

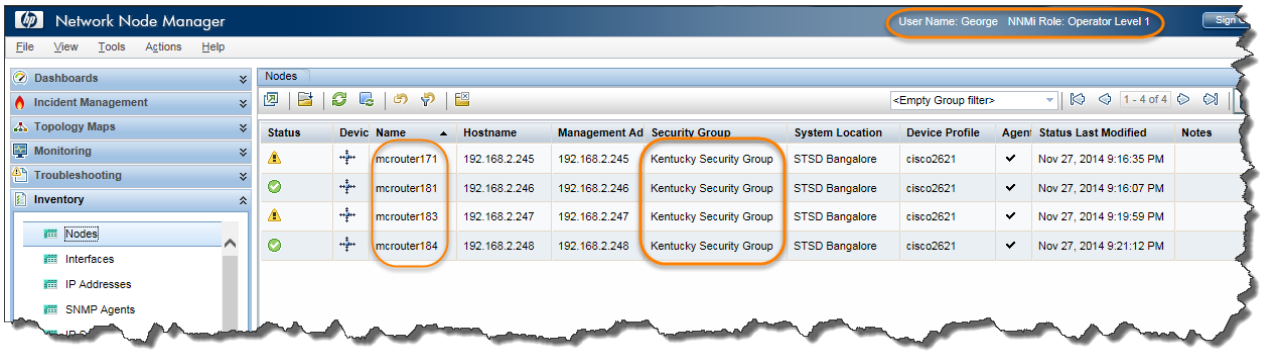

Figure 17: Nodes: Sign in as George

2. Sign in to NNMi as John. You should see only Detroit nodes as shown in **Figure 19**. You will also only see incidents related to nodes from **Detroit Security** group.

Figure 18: Nodes: Sign in as John

3. Sign in to NNMi as Paul. You should see the nodes and incidents from both Detroit and Kentucky as shown in **Figure 20**.

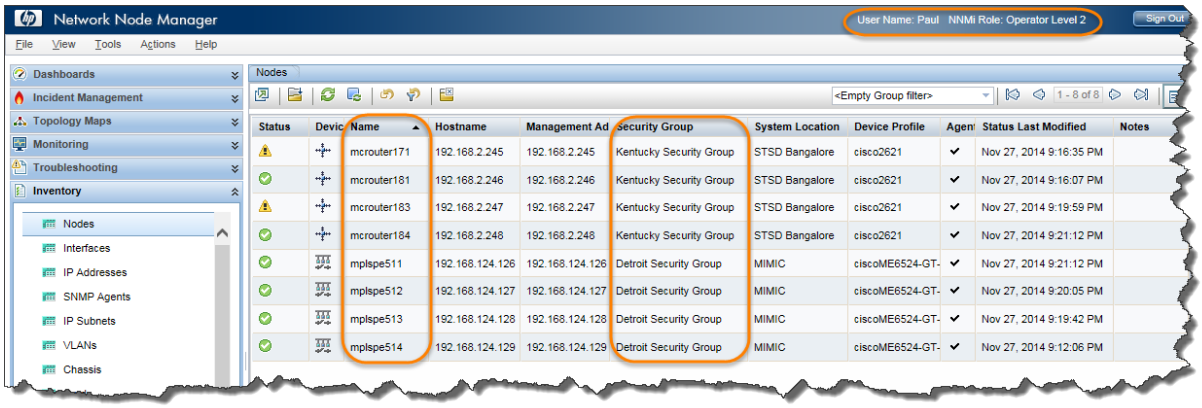

Figure 19: Nodes: Sign in as Paul

4. Sign in to NNMi as Ringo. You should see all nodes (including nodes that are in the Default Security Group) as shown in **Figure 21** because you are an administrator.

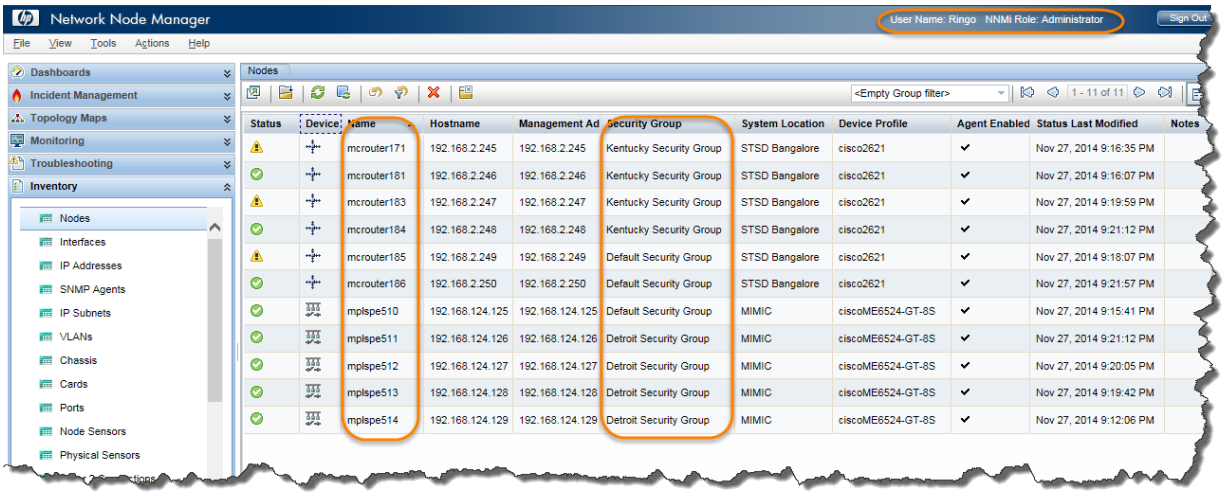

Figure 20: Nodes: Sign in as Ringo

Tenants

NNMi includes a feature called a Tenant (which may also be referred to as a customer or an organization). Each node is permitted one and only one Tenant assignment. Tenants are not Security Groups but they can be used in conjunction with Security Groups. The Tenant model provides a logical separation of nodes and is designed to be used with a “seeded discovery”. A Tenant can have an Initial Discovery Security Group assigned to it. When discovering a node into NNMi using a seed, you can specify the Tenant assignment. This means that if a node is discovered with a Tenant assigned, it can automatically be assigned into a Security Group. Thus, there is never a risk of accidentally having nodes visible to operators that are not supposed to see those nodes.

This model is appropriate for use by large enterprises and service providers, especially managed service providers that have multiple customers (tenants) managed from the same NNMi management server.

NNMi provides a cli script, `nnmsecurity.ovpl`. (See the *nnmsecurity.ovpl* reference page, or the UNIX manpage for more information.) The following example uses the NNMi console for most actions but be aware that all of these same actions are available using the `nnmsecurity.ovpl` script. Consider using the `nnmsecurity.ovpl` script for large deployments with many Tenants.

Tenant Example

Consider the following example. Begin by creating a Security Group for the Tenant.

Note:
This example does not build on any of the previous examples.

---

1. From the workspace navigation panel, select the **Configuration** workspace as shown in **Figure 22**.
2. Expand the **Security** folder.
3. Click **Security Groups**.
4. Click the **New** icon.

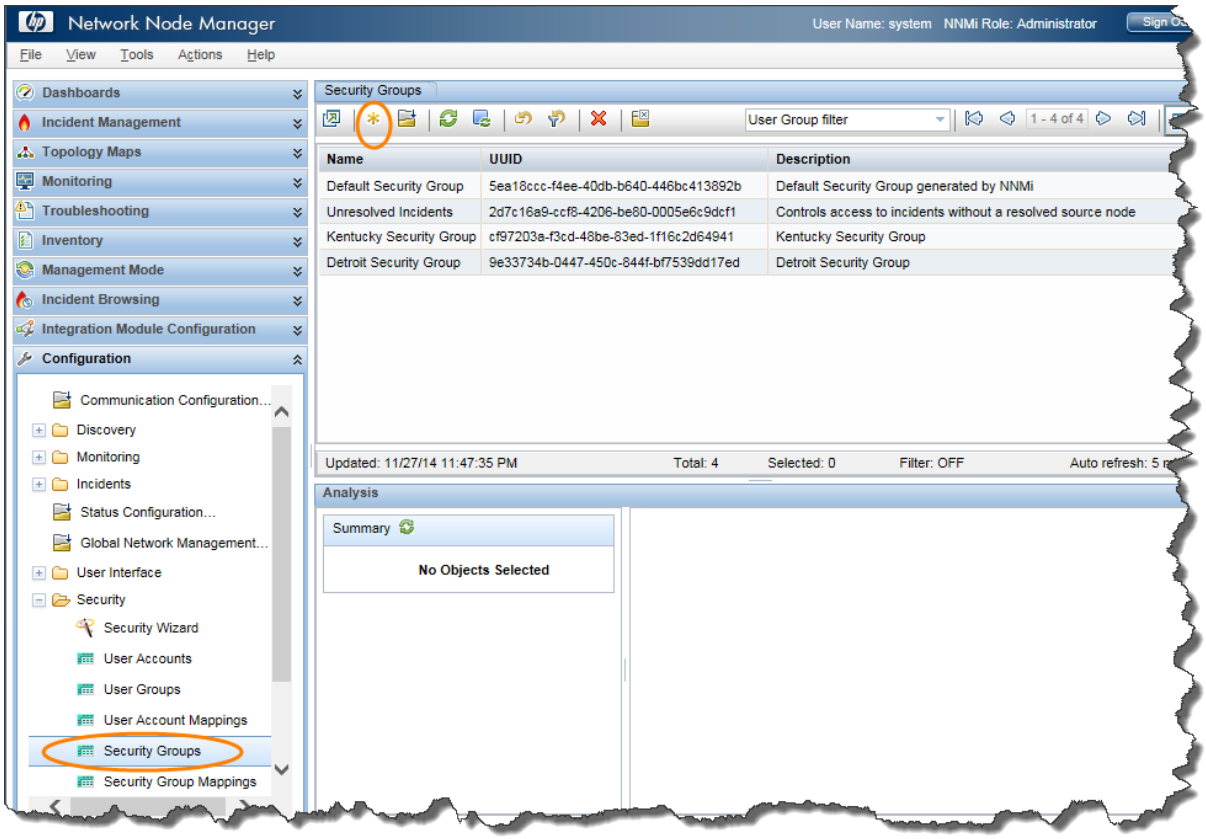

Figure 21: Security Groups: Create a Security Group for the Tenant

5. Complete the form and save the Security Group as shown in **Figure 23.**

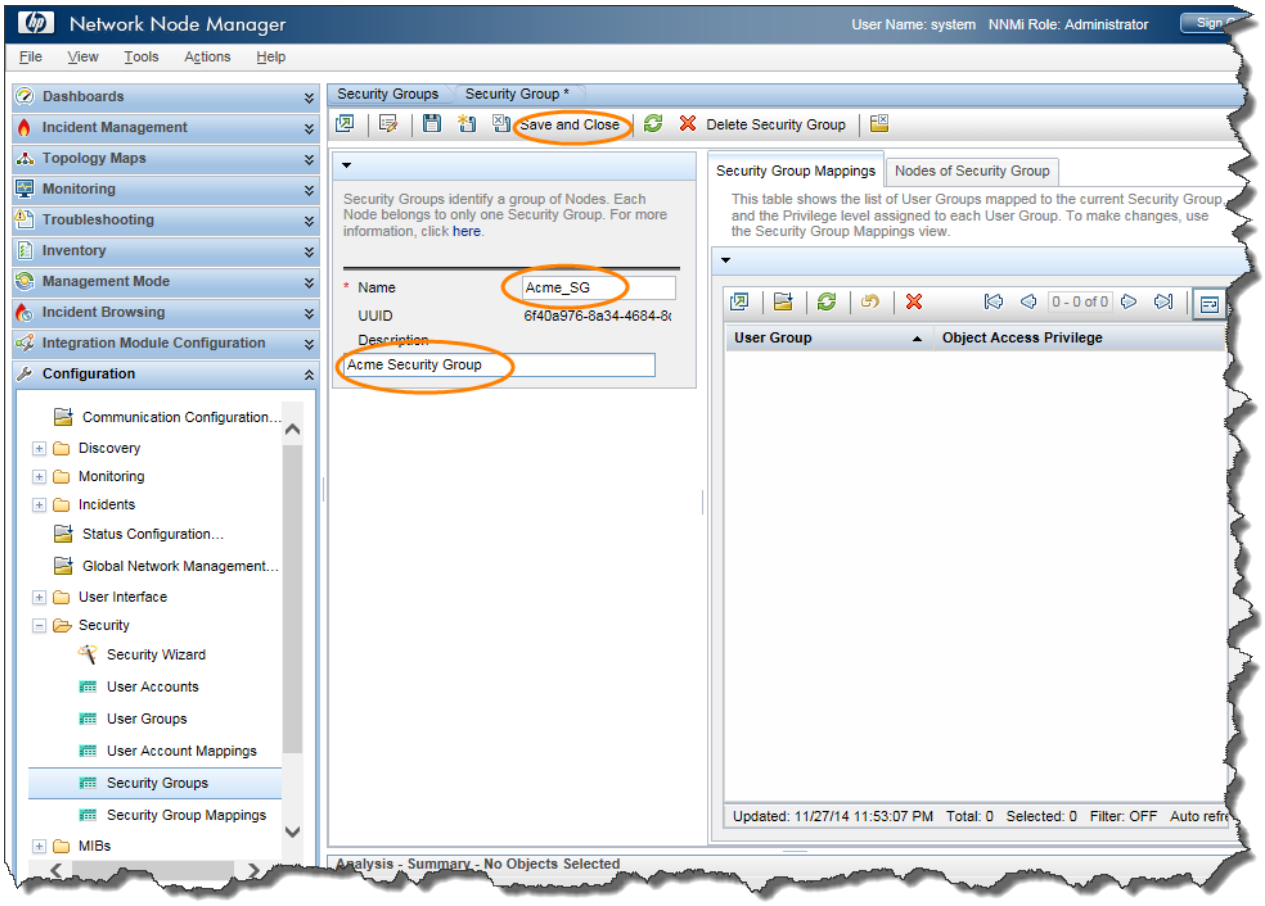

Figure 22: Security Group: Save and Close

Next, create a Tenant as follows:

1. From the workspace navigation panel, select the **Configuration** workspace as shown in **Figure 24.**
2. Expand the **Discovery** folder.
3. Click **Tenants**.
4. Click the **New** icon.

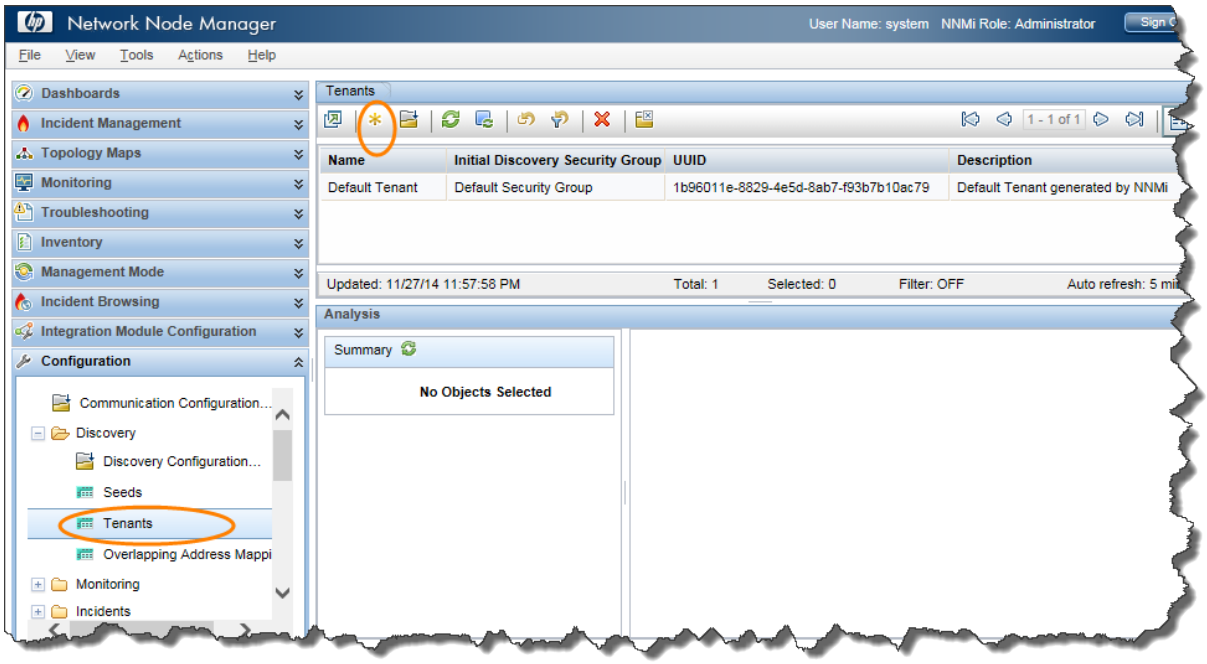

Figure 23: Tenants: Create New Tenant

5. Complete the **Tenant** form as shown in **Figure 25** (Remember to assign an Initial Discovery Security Group).
6. Click the **Save and Close** button.

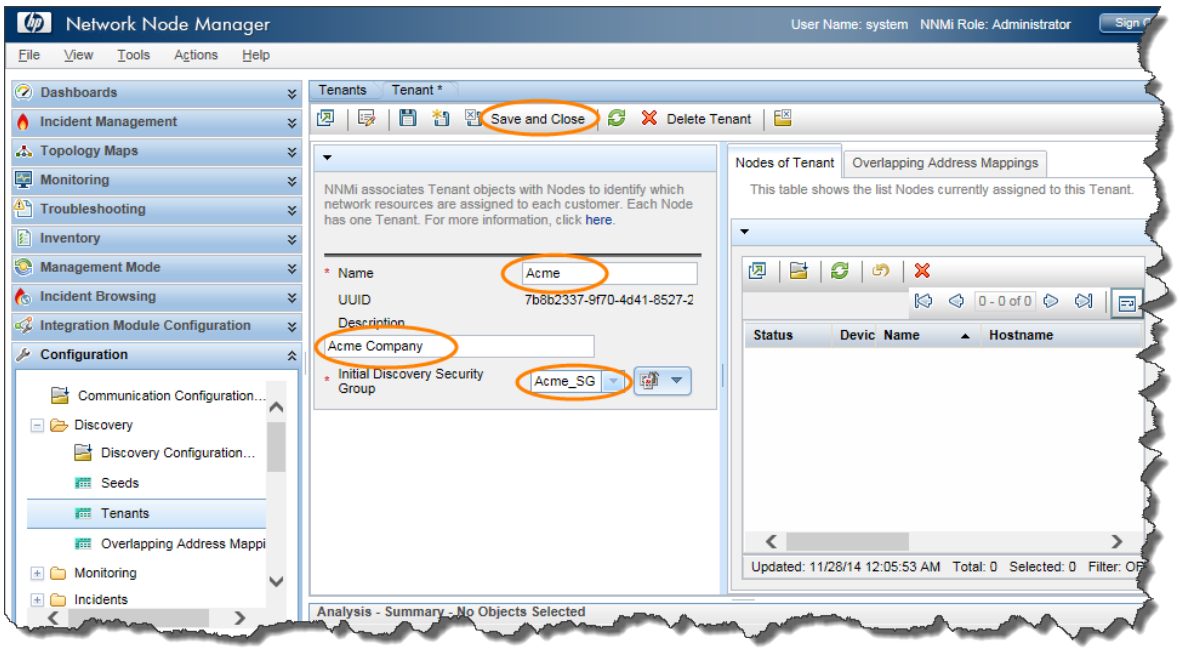

Figure 24: Tenant Form: Save and Close

7. Finally, use the `nnmloadseeds.ovpl` script to load seeds into NNMi. (For this example, there is a seed file, `acme_nodes.txt`, already created for the nodes to be loaded.) Use the `-t` option to assign the Tenant for the nodes, as shown in the following example:

   ```
   nnmloadseeds.ovpl -t Acme -f acme_nodes.txt
   ```

The nodes are assigned a Tenant and a Security Group as they are discovered as shown in **Figure 26.** Now the normal Security Group restrictions apply as previously discussed in this document.

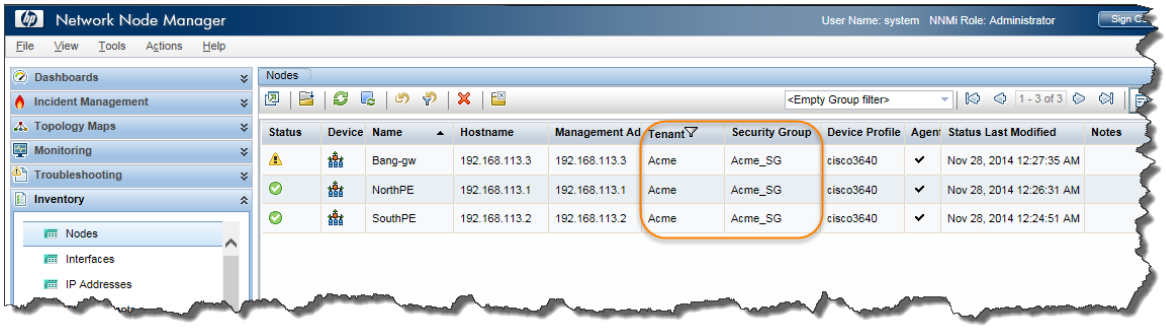

Figure 25: Nodes Form: Tenant and Security Group

Tip: You can use Tenants as filter criteria for Node Groups.

Tenants and Security Groups in Global Network Management (GNM)

Tenants and Security Groups are uniquely identified by their Universally Unique Identifier (UUID). When using Tenants (Multi-Tenancy) and Security Groups in a GNM environment, you must keep the Tenant UUIDs identical between the Global NNMi management server and the Regional NNMi management server; the same is true for Security Groups if you want to share the security restrictions between the servers.

Consider the following example.

Note:
This example does not build on any of the previous examples.

---

1. Use the command line to create a Security Group and Tenant at the Global NNMi station for Customer2.

Tip: When you create a Tenant from the command line using the nnmsecurity.ovpl script as a convenience, if you do not specify a default Security Group, the tool creates a matching Security Group of the same name.

The first UUID in the output is the Tenant UUID and the second UUID is the Security Group UUID. The return values in the following example are highlighted in different colors to show how the values are used at the Regional NNMi station.

```
nnmsecurity.ovpl -createTenant Customer2
```

```
a8ecb97c-2fa1-4d07-b1a3-81e7cc16c72d : 840eb5cb-23db-448b-95dc-8e948b34f4f8 : Customer2 :
```

In **Figure 27**, notice that the Global NNMi management server has created a Tenant and a Security Group with corresponding UUIDs.

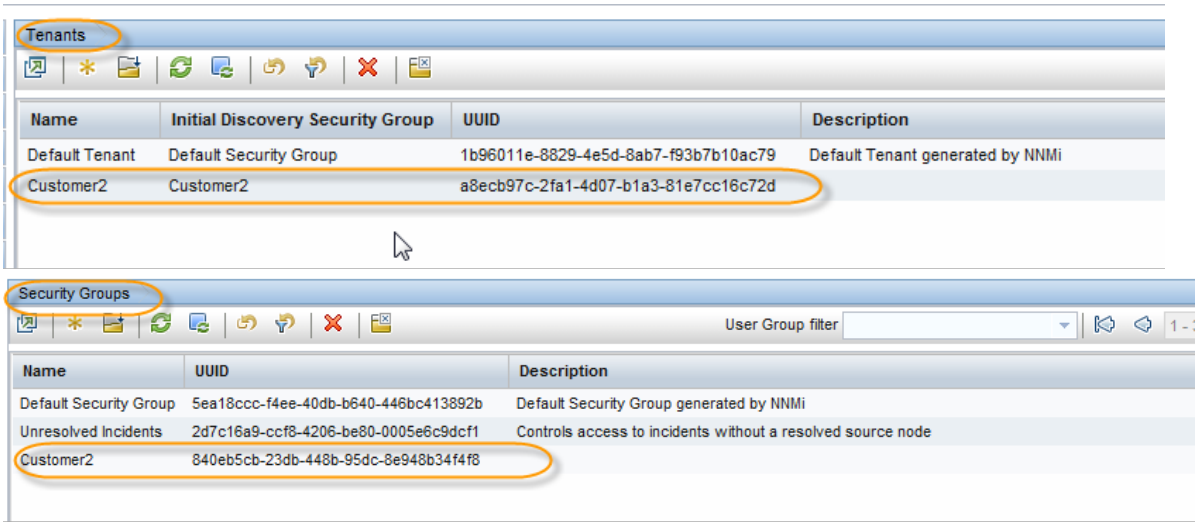

Figure 26: Tenants Form: Tenant and Security Group for Customer2 at the Global NNMi Management Server

2. Now, at the Regional NNMi management server, use the `nnmsecurity.ovpl` script to create a Tenant and Security Group (include the return values from the command output when the script was previously run at the Global NNMi management server). Specifying the UUIDs causes NNMi to create a Tenant and a Security Group with these same UUIDs, allowing for proper synchronization.

   See the following sample command line:

   ```
   nnmsecurity.ovpl -createTenant Customer2 -tenantUuid a8ecb97c-2fa1-4d07-b1a3-81e7cc16c72d -securityGroupUuid
   840eb5cb-23db-448b-95dc-8e948b34f4f8
   a8ecb97c-2fa1-4d07-b1a3-81e7cc16c72d : 840eb5cb-23db-448b-95dc-8e948b34f4f8 : Customer2 :
   ```
3. Now you can load seeds at the Regional NNMi management server with the Tenant specified using the following command line syntax:

```
nnmloadseeds.ovpl -t Customer2 -f <seedfile>
```

All of these seeds are created on the Regional NNMi management server with the Tenant as Customer2 and the associated Security Group as Customer2. These nodes are synchronized to the Global NNMi management server using the same Tenant and Security Group UUID, as shown in **Figure 28**.

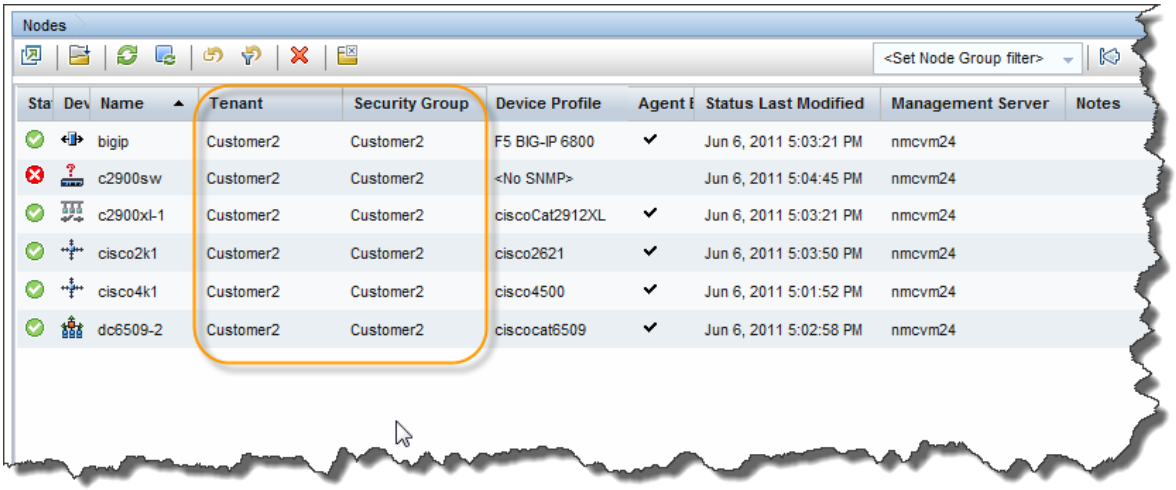

Figure 27: Nodes Form: Customer2 Tenant and Security Group at the Global NNMi Management Server

4. At the Global NNMi management server (and at the Regional NNMi management server, as necessary), create users and User Groups, and then map the User Groups to the Security Groups. You do not need to do this at the Regional NNMi management server if your users are signing into the Global NNMi management server only. Users and User Groups are private to each NNMi management server and are not synchronized.

Conclusion

This paper has shown a sample implementation of the security model by providing examples of Users Accounts, User Groups, Security Groups, mappings and Tenants. An example using the Global Network Management feature was also shown.

We appreciate your feedback!

If an email client is configured on this system, by default an email window opens when you click here.

If no email client is available, copy the information below to a new message in a web mail client, and then send this message to **network-management-doc-feedback@hpe.com**.

Product name and version: NNMi 10.20

Document title: Step-by-Step Guide to Using Security Groups

Feedback:

Hewlett Packard
Enterprise