

# HP Network Node Manager i Software Step-by-Step Guide to Using Security Groups

NNMi 9.1x Patch 1

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.

## CONTENTS

Introduction	3
Security Concepts	3
Security Groups Model	4
Security Groups Example Remove Default User Group Mappings Create Users	5
Create User Groups Map Users to User Groups	8 9
Create Security Groups Map User Groups to Security Groups Assign Nodes to Security Groups Verify Example	12 16
Tenants	20
Tenant Example	21
Tenants and Security Groups in Global Network Management (GNM)	24
Tenants and Security Groups in GNM Example	24
Conclusion	25

# 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 Level 1 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.

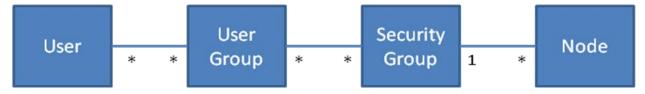
Security Group mapping establishes a relationship between User Groups and Security Groups, effectively granting permission for User Group members to access nodes in the Security Group. Security Group mapping also controls the level of action User Group members can perform on the nodes.

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. In most cases, you make the Security Group access level match the user interface access level; although this is not required.

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



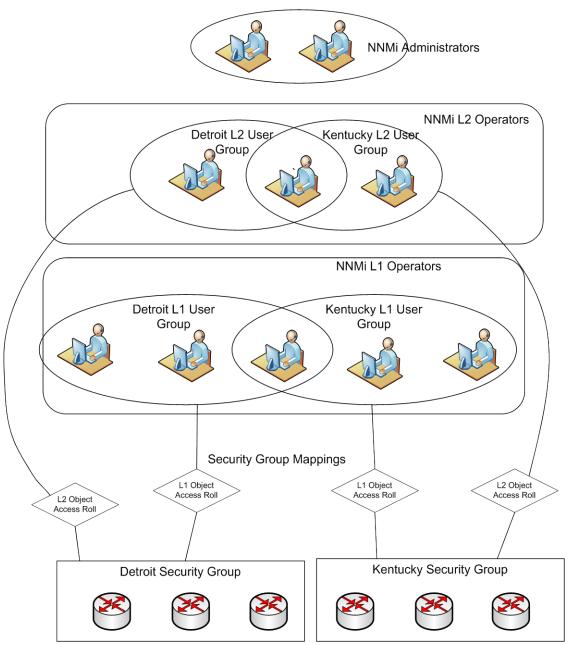


# Security Groups Model

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.

The following figure depicts the NNMi model of the scenario just described.





# 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.

The following table 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 graphical user interface 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).

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

#### Table 1 Users and Roles

The following list is the summary of the steps in this example. This example uses the Security Wizard but you could also use the 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
  - a. Kentucky Security Group
  - b. 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.

#### Figure 3: Security Group Mappings: Delete Default Mappings

🍈 Network Node Manage	r					
File View Tools Actions Help						
👌 Incident Management	*	Security Group Mappings				
🛧 Topology Maps	×	🗵   * 🖻   🖉   🖉	> 🔊 📉 🖴 👘			
Monitoring	×	User Group	Security	Object Acc	cess Privilege	
Troubleshooting	×	NNMi Level 1 Operators	Default Security Group	Object Ope	rator Level 1	
Inventory	×	NNMi Level 2 Operators	Default Security Group	Object Ope	rator Level 2	
🚱 Management Mode	×	NNMi Guest Users	Default Security Group	Object Gue		
🇞 Incident Browsing	×	NNMi Level 1 Operators NNMi Level 2 Operators	Unresolved Incidents Unresolved Incidents		rator Level 1 rator Level 2	
4 Integration Module Configuration	×	NNMi Guest Users	Unresolved Incidents	Object Ope Object Gue		
Configuration	*					
<ul> <li>Custom Poller Configuration</li> <li>Incidents</li> <li>Trap Forwarding Configuration</li> <li>Custom Correlation Configuratio</li> <li>Status Configuration</li> <li>Global Network Management</li> </ul>	•					
E Contentace		Updated: 5/31/11 01:53:12 P	M MDT		Total: 6	Sele
E 🔁 Security		Analysis				
Security Wizard		Summary 😰				
Iser Accounts		Multi	ple Objects Selected			
🗰 User Groups	E					
User Account Mappings						
🛲 Security Groups						
🧰 Security Group Mappings						
🛨 🧰 MIBs						
Device Profiles						
m Node Groups						
interface Groups						
RAMS Servers						
Management Stations (6 x/7 x)     ✓	*					

## **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.

Figure 4: Security Wizard: Create User Account

🕼 Network Node Manager				
File Tools Help				- E
♠ Incident Management ¥	Security Wizard *			
🛧 Topology Maps 🛛 😵	Je Welcome	Use this page to do any of the fol Create and Delete User Accounts, Cr		ps. Assign
🖾 Monitoring 🛛 😵	Map User Accounts and User Groups	Mappings User Accounts	User Account Map	
Troubleshooting ¥	Dap User Groups and Security Groups	× × E		
linventory ¥	ኞ Assign Nodes to Security Groups		User Account	
🗞 Management Mode 🛛 🕹 🕹	View Summary of Changes	Create User Account	Administrator	User Gr
🏠 Incident Browsing 🛛 🕹		Administrator	Administrator	NNMI Adı
🗳 Integration Module Configuration 🛛 🗧 🕹				- 🧹
Configuration \$				
Communication Configuration  Control Discovery  Monitoring Configuration  Custom Poller Configuration  Custom Poller Configuration  Custom Correlation Configuration  Custom Correlation Configuration  Status Configuration  Global Network Management  Custom User Interface  Security  Custom Vizard  User Accounts  User Groups  Additional Mateution				

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

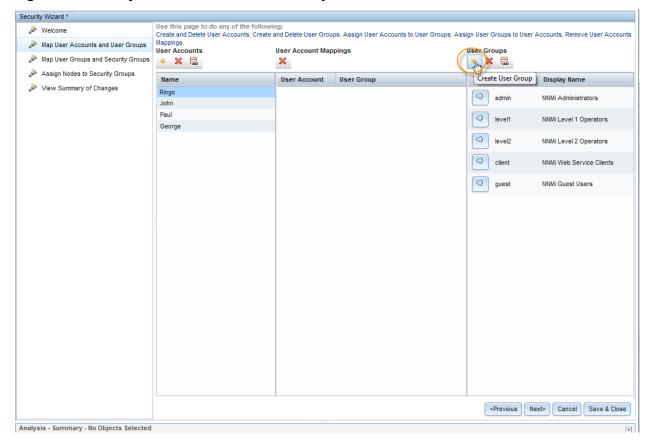
#### Figure 5: Create User Account Dialog Box

Create Use	r Account	х
Name	John	
Password	••••	
Passworu	••••	
	Add Close	e
		_

## Create User Groups

1. Click the **\* Create User Group** icon.

Figure 6: Security Wizard: Create User Group



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

Figure 7: Create User Group Dialog Box

Create User Group	х
Name	KentuckyOper1
Display Name	Kentucky Level 1 Operators
Directory Service Name	
	Kentucky Level 1 Operators
Description	
	Add Close

## Map Users to User Groups

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

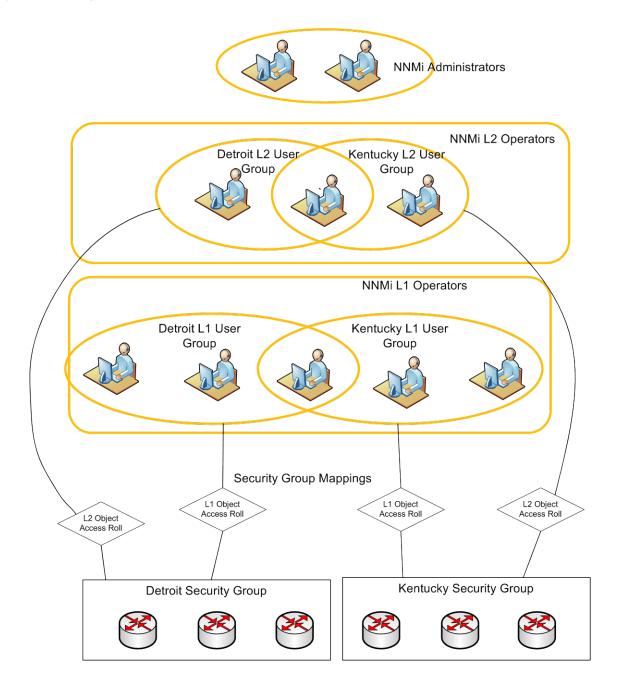
- In the Security Wizard, click the user Name, the User Group, and then click the icon beside the desired level to define the mapping assignment. Be sure to include both the special NNMi User Group for the user interface (Level 1, Level 2) and the custom User Group (for example, Detroit Level 1 Operators).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

#### Figure 8: Security Wizard: User Account Mappings

curity Wizard *						
le Welcome	Use this page to do any of the followin Create and Delete User Accounts, Create a		ps, Assign User Accounts to User Groups, Ass	sion User	Groups to User A	ccounts. Remove User Account
Map User Accounts and User Groups	Mappings.	User Account Map		User Gr		
🔉 Map User Groups and Security Groups	* 🗙 🚍	×	pinga	* 🗙		
🔉 Assign Nodes to Security Groups	Name	User Account	User Group		Name	Display Name
ኞ View Summary of Changes	Ringo	John	Detroit Level 1 Operators	4		
(	John	John	NNMi Level 1 Operators		admin	NNMi Administrators
	Paul				level1	NNMi Level 1 Operators
	George				) level2	NNMi Level 2 Operators
					client	NNMi Web Service Clients
				$\bigcirc$	guest	NNMi Guest Users
					KentuckyOper1	Kentucky Level 1 Operators
				$\bigcirc$	KentuckyOper2	Kentucky Level 2 Operators
				0	DetroitOper1	Detroit Level 1 Operators
				$\bigcirc$	DetroitOper2	Detroit Level 2 Operators
					<pre>Previous Nex</pre>	t> Cancel Save & Close

The following figure indicates the items completed to this point (shown in yellow):

#### Figure 9: Completed Items



## Create Security Groups

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

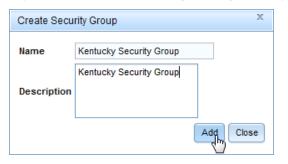
1. In the Security Wizard, click the \* Create Security Group icon.



urity Wizard *	Use this page to	o do any of the following:				
Welcome	Create and Delete		urity Groups, Assigr	User Groups to S	ecurity Groups, Assign Se	curity Groups to User Groups, Remove Securit
Map User Accounts and User Groups	Group Mappings. User Groups		Security Group	Mappinge		Security Groups
Map User Groups and Security Groups	* 🗙 🗟		X Object Op		-	
Assign Nodes to Security Groups			•• Object op			
	Name	Display Name	User Group	Security Grou	Object Access Privileg	e N Create Security Group
View Summary of Changes	admin	NNMi Administrators				Default Security Group
	level1	NNMi Level 1 Operators				Unresolved Incidents
	level2	NNMi Level 2 Operators				
	client	NNMi Web Service Clients				
	guest	NNMi Guest Users				
	KentuckyOper1	Kentucky Level 1 Operators				
	KentuckyOper2	Kentucky Level 2 Operators				
	DetroitOper1	Detroit Level 1 Operators				
	DetroitOper2	Detroit Level 2 Operators				
	L					
						<previous next=""> Cancel Save &amp; Clo</previous>

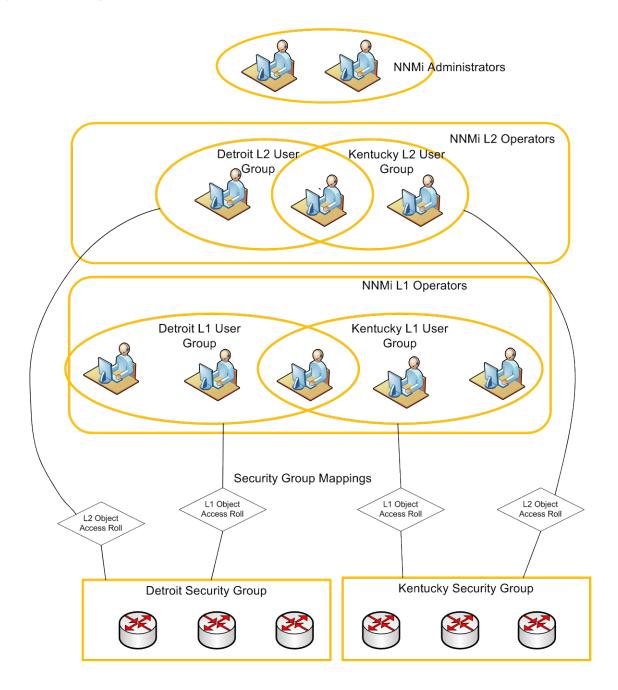
2. Enter the information for each Security Group in the **Create Security Group** dialog box.

Figure 11: Create Security Group Dialog Box



The following figure indicates the items now completed (shown in yellow).

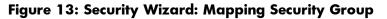
#### Figure 12: Completed Items

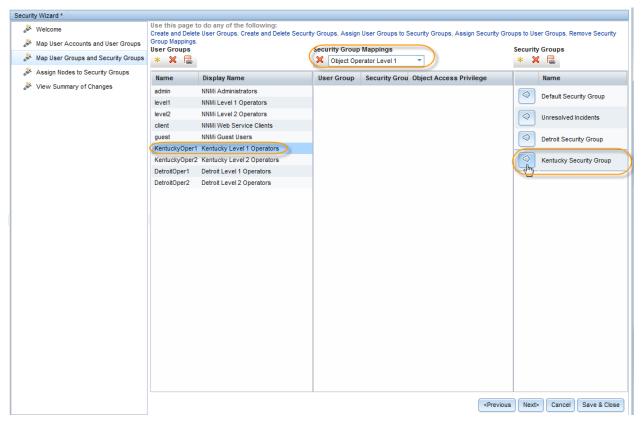


## Map User Groups to Security Groups

For each User Group, do the following:

- 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.





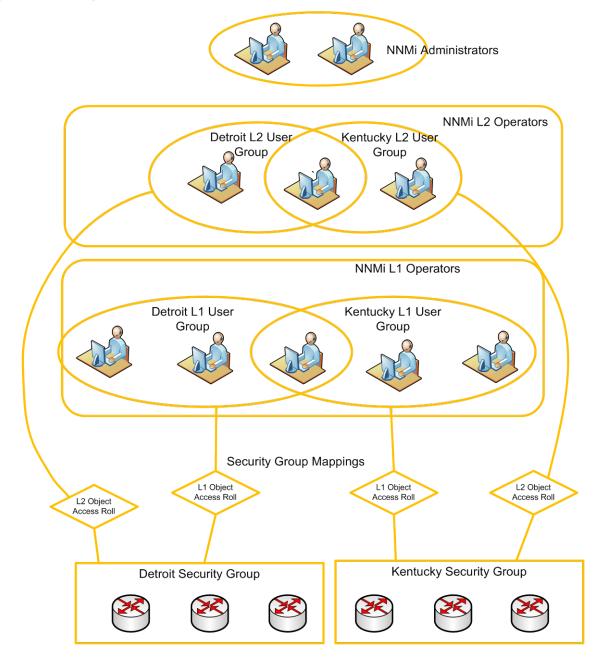
4. After you have defined all of the Security Group Mappings, click the **Next** button.

Figure 14: Security Wizard: Define Security Group Mappings

curity Wizard *						
Welcome	Create and Delet	to do any of the following: e User Groups, Create and Delete Security			rity Groups, Assign Security Group	ps to User Groups, Remove Security Group Map
Map User Accounts and User Groups	User Groups 🙁 🗮		Security Group		<b>v</b>	Security Groups 😽 🔀
Map User Groups and Security Groups	·· 🔶 📾	1	<ul> <li>Object Op</li> </ul>	erator Level 2		
Assign Nodes to Security Groups	Name	Display Name	User Group	Security Grou	Object Access Privilege	Name
View Summary of Changes	admin	NNMi Administrators	Kentucky	Kentucky	01110	Default Security Group
	level1	NNMi Level 1 Operators	Level 2 Operators	Security Group	Object Operator Level 2	
	level2	NNMi Level 2 Operators				Unresolved Incidents
	client	NNMi Web Service Clients				
	guest	NNMi Guest Users				Detroit Security Group
	DetroitOper2	Detroit Level 2 Operators				
	DetroitOper1	Detroit Level 1 Operators				Kentucky Security Group
		Kentucky Level 1 Operators				
	KentuckyOper2	Kentucky Level 2 Operators				
	L					
						<pre><previous next=""> Cancel Save &amp; Clo </previous></pre>
lysis - Summary - No Objects Selected						

The following figure indicates the items now completed (shown in yellow).

#### Figure 15: 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 tool. 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).
- 2. Click the nodes you want 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 list (**Kentucky Nodes** in the example below).

**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 16: Security Wizard: Assign Nodes to Security Group

curity Wizard *					
å Welcome	The Assign Nodes to Security Group instructions, click here.	os option enables you to assign one or	nore nodes to a Security Group. Use ti	he Available Nodes table view	v to select the nodes. For
🔉 Map User Accounts and User Groups	Security Groups	Nodes Currently Assigned to	Selected Group:	Nodes to be Assigned to	Selected Group:
🔉 Map User Groups and Security Groups	* ×	Name 🔺 Host	name	Hostname	
🖇 Assign Nodes to Security Groups	Name				
View Summary of Changes	Default Security Group				
	Unresolved Incidents Detroit Security Group				
	Kentucky Security Group				
		•	11	•	
	Available Nodes:				
					A 44
	S   S V 💽		Kentucky Nodes	) 🛇 🗘 1 - 3 of 3	0 0
	Dev Name 🔺 Ho Assign Sele	cted Nodes to Selected Security Grou	ip ss Security Group	1	
	ST ENDNODE4 10.2.1.59	10.2.1.59	Default Security	Group	
	schaumburgpr 10.2.1.9	10.2.1.9	Default Security	Group	
	westcoast-sw 10.2.1.26	10.2.1.26	Default Security	Group	
	Updated: 6/1/11 01:08:30 PM MDT	Tota	: 3 Selected: 3	Filter: ON	Auto refresh:
				<previous 1<="" td=""><td>lext&gt; Cancel Save &amp; Clo</td></previous>	lext> Cancel Save & Clo
				SPIEVIOUS	Save a cit

4. After you have assigned all the nodes, check to see that they are marked to be assigned, and then click **Next**.

Security Wizard *				
å Welcome	The Assign Nodes to Security Groups of instructions, click here.	option enables you to assign one or more nodes	to a Security Group. Use the <i>I</i>	Available Nodes table view to select the nodes. For
🖉 Map User Accounts and User Groups	Security Groups	Nodes Currently Assigned to Selected	Group:	lodes to be Assigned to Selected Group:
🔉 Map User Groups and Security Groups	* 🗙	Name 🔺 Hostname		Hostname
🔉 Assign Nodes to Security Groups	Name			10.2.1.9
ኞ View Summary of Changes	Default Security Group Unresolved Incidents			10.2.1.59
	Detroit Security Group			
	Kentucky Security Group			
		۰ III	•	
	Available Nodes:			
			Kentucky Nodes 👻	🔯 🔄 1 - 3 of 3 🔅 🖓 📃
	Dev Name 🔺 Hostname	Management Address	Security Group	
	ENDNODE4 10.2.1.59	10.2.1.59	Default Security Gro	hup
	schaumburgpr 10.2.1.9	10.2.1.9	Default Security Gro	hup
	westcoast-sw 10.2.1.26	10.2.1.26	Default Security Gro	up
	Updated: 6/1/11 01:08:30 PM MDT	Total: 3	Selected: 0	Filter: ON Auto refresh: OFF
				<previous next=""> Cancel Save &amp; Close</previous>

Figure 17: Security Wizard: Verify Nodes are Assigned to Security Group

5. Finally, review the summary of changes. After verifying changes, click **Save and Close**.

Figure 18: Security Wizard: Final Summary

Security Wizard *	
🔊 Welcome	The View Summary of Changes option enables you to view your recent configuration changes. For more information, click here.
🚴 Map User Accounts and User Gro	The following Security Groups have Node assignment changes:
🔊 Map User Groups and Security Gr	
🔉 Assign Nodes to Security Groups	Romony Secondy Shoup, Series Secondy
View Summary of Changes	
۰ III ا	<previous next=""> Cancel Save &amp; Close</previous>
Analysis - Summary - Multiple Objects	

## 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.

Figure 19: Nodes: Sign in as George

File View Tools Actions Help												
👌 Incident Management	× N	odes 📎										
🛧 Topology Maps	*	1   🖻	i   😂 🖪   🔊	🌮   🔛			<set i<="" th=""><th>Node Group filter&gt; 👻</th><th>🔯 🍳 1-3 (</th><th>of 3</th><th><math>\diamond</math></th><th>Ø   E</th></set>	Node Group filter> 👻	🔯 🍳 1-3 (	of 3	$\diamond$	Ø   E
Monitoring	× s	ta Dey	Name 🔺	Hostname	Managemen	t Security Group		System Location	Device Profile	Age	Status Last Modified	Notes
Troubleshooting	* (	) 💣	ENDNODE4	10.2.1.59	10.2.1.59	Kentucky Security Group		NTC	microsoftNTServer	~	May 23, 2011 10:42:28 AM	
inventory	* (	1	schaumburgpr	10.2.1.9	10.2.1.9	Kentucky Security Group		1204 E. Algonquin R	cisco7206VXR	~	Jun 1, 2011 5:21:30 PM	
Nodes				10.2.1.26	10.2.1.26	Kentucky Security Group		5 upper east compu	ciscoCat2950t24	~	Jun 1, 2011 5:31:51 PM	
m Interfaces												
IP Addresses						G						
III SNMP Agents												
IP Subnets												

2. Sign in to NNMi as John. You should see only Detroit nodes and incidents.

#### Figure 20: Nodes: Sign in as John

🕼 Network Node Manager								Usi	er Name: John 🛛 NNM	i Role	: Operator Level 1	Sign Out
File View Tools Actions Help												
👌 Incident Management 🛛 😵	Note	des 👌										
🛧 Topology Maps 🛛 😵	<u>ب</u>		i   😂 尾   🤊	🔊   🖴			<set n<="" td=""><td>ode Group filter&gt; 🚽</td><td>🔯 🌖 1-3 (</td><td>of 3</td><td>٥</td><td></td></set>	ode Group filter> 🚽	🔯 🌖 1-3 (	of 3	٥	
Monitoring *	St	a Dey	Name	Hostname	Management	Security Group		System Location	Device Profile	Age	Status Last Modified	Notes
Troubleshooting *	6	2	10.161.4.3	10.161.4.3		Detroit Security Group			<no snmp=""></no>		May 26, 2011 4:05:39 PM	
Inventory A	۵	*	dc6509-1	dc6509-1.	10.715.56.8	Detroit Security Group		5 upper east compu	ciscocat6509	~	May 13, 2011 9:10:20 AM	
Te Nodes	0	*	dc6509-2	dc6509-2.	10.75.56.9	Detroit Security Group		5 upper east compu	ciscocat6509	~	May 13, 2011 9:18:18 AM	
m Interfaces							/					
IP Addresses												
III SNMP Agents	11					45						
IP Subnets												
III VLANS	11											
and and some from the	-blace		and the second s		and the second s	and a strength	~~	Canal Contract,		~~	and the second	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

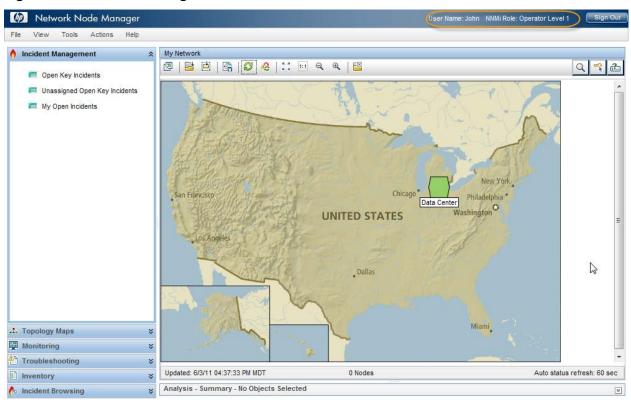


Figure 21: Incident Management: John's Network

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

ile View Tools Actions Help												
Incident Management	× No	des 📎										
A Topology Maps	* 🖄	🖻	🖉 🖪   🔊	💎   🖴			<set< th=""><th>Node Group filter&gt;</th><th>🔝 🌖 1-6 o</th><th>of 6</th><th>٥</th><th>Ø   E</th></set<>	Node Group filter>	🔝 🌖 1-6 o	of 6	٥	Ø   E
Monitoring	× st	a Dev	ilame 🔺	Hostname	Management	Security Group		System Location	Device Profile	Age	Status Last Modified	Notes
Troubleshooting	* 😣	2	10.161.4.3	10.161.4.3		Detroit Security Group			<no snmp=""></no>		May 26, 2011 4:05:39 PM	
Inventory	^	1	dc6509-1	dc6509-1 1	148,778,588.8	Detroit Security Group		5 upper east compu	ciscocat6509	~	May 13, 2011 9:10:20 AM	
Nodes	0	å	dc6509-2	dc6509-2 1	18.75.58.9	Detroit Security Group		5 upper east compu	ciscocat6509	~	May 13, 2011 9:18:18 AM	
Interfaces	0	ď	ENDNODE4	10.2.1.59	10.2.1.59	Kentucky Security Group		NTC	microsoftNTServer	~	May 23, 2011 10:42:28 AN	
IP Addresses	0	å	schaumburgpr	10.2.1.9	10.2.1.9	Kentucky Security Group		1204 E. Algonquin R	cisco7206VXR	~	Jun 1, 2011 5:21:30 PM	
SNMP Agents		111 ***	westcoast-sw1	10.2.1.26	10.2.1.26	Kentucky Security Group		5 upper east compu	ciscoCat2950t24	~	Jun 1, 2011 5:31:51 PM	
IP Subnets					(		Γ					
III VLANs												
Cards												
Ports												

Figure 22: Nodes: Sign in as Paul

Metwork Node Manager	User Name: Paul NNA	/i Role: Operator Level 2 Sign Out
File View Tools Actions Help		
👌 Incident Management 🛛 🛠	My Network	
<ul> <li>Open Key Incidents</li> <li>Unassigned Open Key Incidents</li> <li>My Open Incidents</li> </ul>	San Francisco Los Angeles	E.
🔥 Topology Maps 🛛 🕹		5
🖓 Monitoring 🛛 🗧 🗧	Miami	
Troubleshooting ¥		
Inventory ¥		• • •
Management Mode *	Updated: 6/3/11 04:39:14 PM MDT 0 Nodes	Auto status refresh: 60 sec
🏠 Incident Browsing 🛛 😵	Analysis - Summary - No Objects Selected	

Figure 23: Incident Management: Paul's Network

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

ile View Tools Actions Help	p									
Incident Management	*	Nodes	$\geq$							
Topology Maps	*	2	3   🖉 🖪   🕫	) 💎   🗙   🔛		<	Get Node Group filter> 👻	🖾 🔇 24	- 33 of 142	
Monitoring Troubleshooting	× ×		ev Name 🔺	Security Group Kentucky Security Group	Device Profile cisco2828sysID		Status Last Modified May 27, 2011 3:25:28 PM	Notes		
Inventory	*	<u> </u>		Default Security Group	ciscocat6509	~	Apr 19, 2011 11:58:40 PM			
m Nodes	<b>A</b>	83	cisco7	Default Security Group	ciscocatalyst2924X	~	May 27, 2011 3:28:42 PM			
m Interfaces		<u> </u>	colby	Default Security Group	microsoftNTServer	~	May 10, 2011 12:53:37 PM			
IP Addresses		<u> </u>	core6509-1	Default Security Group	ciscocat6509	~	May 18, 2011 4:08:18 PM			
SNMP Agents		<u> </u>	core6509-2	Default Security Group	ciscocat6509	¥	May 26, 2011 4:01:41 PM			
IP Subnets		O 🕯	dc6509-1	Detroit Security Group	ciscocat6509	~	May 13, 2011 9:10:20 AM			
WLANs		📀 🖸	dc6509-2	Detroit Security Group	ciscocat6509	~	May 13, 2011 9:18:18 AM			
Cards		o 3	em1	Default Security Group	juniperEX4200	~	May 23, 2011 1:27:43 AM			
Ports		0	ENDNODE4	Kentucky Security Group	microsoftNTServer	~	May 23, 2011 10:42:28 AN			
Node Components	E									
Layer 2 Connections		Update	d: 6/3/11 04:41:42 PM	IMDT	Total: 142		Selected: 0	Filter: OFF	A	Auto refresh: 3 mi

Figure 24: 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 allowed one and only one Tenant assignment. Tenants are not Security Groups but they can be used in conjunction with Security Groups. The Tenant model 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.

NNMi provides a helpful command line tool, nnmsecurity.ovpl. (See the *nnmsecurity.ovpl* reference page, or the UNIX manpage for more information.) The following example uses the graphical user interface for most actions but be aware that all of these same actions are available using the command line. Consider using the command line tool 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.
- 2. Expand the **Security** folder.
- 3. Click Security Groups.
- 4. Click the **\*New** icon.

#### Figure 25: Security Groups: Create a Security Group for the Tenant

Network Node Manager ie View Tools Actions Help			Userl
	Security Groups		
-	<ul> <li>Becanity Groups</li> <li>Bec</li></ul>	User Group filter	- 14
		Description	
-	Marine New Oor	Description Default Security Group generated by NNMi	4
-	Benauk Secarky Group Sea roccontect to bottor the	Controls access to incidents without a resolved so	ource node
	Detroit Security Group 2da8204a-1698-40fb-8bc0-9946 [		
-	Kentucky Security Grou f4228324-e0f7-46e1-885e-d5e6	Kentucky Security Group	
-	*		
	*		
Custom Poller Configuration  Incidents  Trap Forwarding Configuration  Custom Correlation Configuration			
📑 Status Configuration	Updated: 6/3/11 05:14:38 PM MDT	Total: 4 Selected: 0	Fi
📑 Global Network Management	Analysis		
🗄 🧰 User Interface	Summary 🔂		
🖃 🗁 Security	No Objects Selected		
🔨 Security Wizard			
User Accounts			
🗰 User Groups			
🗰 User Account Mappings			
User Account Mappings			
		1	1

5. Complete the form and save the Security Group.

Figure 26: Security Group: Save and Close

Metwork Node Manager			User Name: R
File View Tools Actions Help			
💧 Incident Management	岽	Security Groups Security Group *	
🛧 Topology Maps	¥	🗵   🗟 📋 🎦 Save and Close 💋 🗶 Delete Secur	rity Group   🖼
Monitoring	¥	-	Security Group Mappings Nodes of Security Group
Troubleshooting	¥	Security Groups identify a group of Nodes, Each Node belongs to	This table shows the list of User Groups mapped to the
Inventory	*	only one Security Group. For more information, click here.	level assigned to each User Group. To make changes,
📀 Management Mode	×		•
🇞 Incident Browsing	¥	Name Acme_SG	
🐝 Integration Module Configuration	¥	UUID 1b4a01d7-2683-49b2-a03b-0fa8b8f66a0	User Group    Object Access Prive
✤ Configuration	*	Description	User Group _ Object Access Priv
📑 Monitoring Configuration 🗸	•	Acme Security Group	
📑 Custom Poller Configuration			
\pm 🧰 Incidents			
📑 Trap Forwarding Configuration			
📑 Custom Correlation Configuration			
📑 Status Configuration			
📑 Global Network Management		Analysis	
🗄 🧰 User Interface		Summary Panel 🕵	
🖃 🗁 Security			1
🜱 Security Wizard			1
User Accounts	E		•
🛅 User Groups			
User Account Mappings			
🗰 Security Groups			
curity Group Mapping			the set of the second

Next, create a Tenant as follows:

- 1. From the workspace navigation panel, select the **Configuration** workspace.
- 2. Expand the **Discovery** folder.
- 3. Click Tenants.
- 4. Click the **\*New** icon.

Figure 27: Tenants: Create New Tenant

Network Node Manager						NNMi Role: Administrator	(	Sign Out
File View Tools Actions Help								
👌 Incident Management	*	Tenants						
🛧 Topology Maps	ຸ×	፼((*)] =   3 €   5 ♦   🗙   🖻			4 1-1	of 1	$\diamond$	
Monitoring	≈	Name New Initial Discovery Security Group UUID	Des	scription				
Troubleshooting	*	Default Tenant Default Security Group 1b96011e-	8829-4e5d-8ab7-f93t Defa	ault Tenant generated by NNMi				
Inventory	≈							
🧐 Management Mode	ຸ×							
🍖 Incident Browsing	*							
4 Integration Module Configuration	≈							
✤ Configuration	*							
📑 Communication Configuration 🔺								
E Discovery	н							
Discovery Configuration	Н							
i Seeds	н							
Tenants								
Monitoring Configuration		Updated: 6/3/11 05:06:52 PM MDT	Total: 1 Se		r: OFF	A	Auto refre	esh: 5 min

- 5. Complete the **Tenant** form. (Remember to assign an Initial Discovery Security Group.)
- 6. Click the **Save and Close** button.

Figure 28: Tenant Form: Save and Close

🍈 Network Node Manager		User Name: Ringo NNMi Role: Administrator Sign Out
File View Tools Actions Help		
Incident Management ¥	Tenants Tenant *	
🛧 Topology Maps 🛛 🕹	🗵   📴   💾 🎦 🚰 Save and Close 🖉 🗶 Delete Tenant	
Monitoring ¥	- ( <sup>11</sup> )	odes of Tenant
Troubleshooting ¥		This table shows the list Nodes currently assigned to this Tenant.
Inventory ¥	network resources are assigned to each customer. Each Node has one Tenant. For more information, click here.	
Management Mode ¥		,
ncident Browsing ¥	Name	🗵 😂 🗶 🔯 0-0of0 🖉 🔛
	UUID d62be23c-d0ac-4b0d-a6d6-8de59f500di	Sta Dev Name A Hostname Security Group Management
Configuration \$	Description	
📑 Communication Configuration 📥	Acme Company	
🖃 🗁 Discovery	Initial Discovery Security	
Discovery Configuration	Group	
m Seeds		
Tenants		
📑 Monitoring Configuration		• • • • • • • • • • • • • • • • • • •
Custom Poller Configuration	Analysis	

Finally, use the nnmloadseeds.ovpl command line tool 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. Now the normal Security Group restrictions apply as previously discussed in this document.

× No	des							
; 🗷	📑	🛃 尾   🔊	💎   🗙   🔛		<set fi<="" group="" node="" td=""><td>iter&gt;</td><td>👻 🔯 🗘 1-6 of</td><td>6</td></set>	iter>	👻 🔯 🗘 1-6 of	6
St	a Dev	Name 🔺	Tenant√	Security Group	Device Profile	Age	Status Last Modified	Notes
2	頭	internet-switch-2	Acme	Acme_SG	ciscoCat3524XL	~	Jun 3, 2011 5:29:15 PM	
		internet-switch-3	Acme	Acme_SG	ciscoCat2950t24	~	Jun 3, 2011 5:31:54 PM	
0	頭	internet-switch-4	Acme	Acme_SG	ciscoCat2950t24	~	Jun 3, 2011 5:31:29 PM	
0		internet-switch-6	Acme	Acme_SG	ciscoCat2950t24	~	Jun 3, 2011 5:32:08 PM	
0	頭	intsw-1	Acme	Acme_SG	cisco3560G-24PS	~	Jun 3, 2011 5:29:31 PM	
0	•	ipv6-vlan5-sw3	Acme	Acme_SG	hpProCurve3500yl-F	~	Jun 3, 2011 5:29:07 PM	
			3					
		Star Dev ○ 班 ○ 班 ○ 班 ○ 班 ○ 班 ○ 班 ○ 班 ○ 班	Sta Dev Name	Sta       De       Name       Tenant⊽         ○       Internet-switch-2       Acme         ○       Internet-switch-3       Acme         ○       Internet-switch-4       Acme         ○       Internet-switch-6       Acme         ○       Internet-switch-8       Acme         ○       Internet-switch-8       Acme         ○       Internet-switch-8       Acme         ○       Internet-switch-8       Acme         ○       Internet-switch-9       Acme         ○       Internet-switch-9	Sta       Dev       Name       Tenant       Security Group         Internet-switch-2       Acme       Acme_SG         Image: Internet-switch-3       Acme       Acme_SG         Image: Internet-switch-4       Acme       Acme_SG         Image: Internet-switch-4       Acme       Acme_SG         Image: Internet-switch-6       Acme       Acme_SG         Image: Internet-switch-7       Acme       Acme_SG         Image: Internet-switch-8       Acme       Acme_SG         Image: Internet-switch-9       Acme       Acme_SG         Image: Internet-switch-9       Acme       <	Sta       Dev       Name       Tenant√       Security Group       Device Profile         Internet-switch-2       Acme       Acme_SG       ciscoCat3524XL         Image: Internet-switch-3       Acme       Acme_SG       ciscoCat2950124         Image: Internet-switch-4       Acme       Acme_SG       ciscoCat2950124         Image: Internet-switch-6       Acme       Acme_SG       cisco3560G-24PS         Image: Internet-switch-7       Acme       Acme_SG       hpProCurve3500yLF	Sta       Dev       Name       Tenant√       Security Group       Device Profile       Age         ②       Image: Internet-switch-2       Acme       Acme_SG       ciscoCat3524XL       ✓         ③       Internet-switch-4       Acme       Acme_SG       ciscoCat2950124       ✓         ③       Internet-switch-4       Acme       Acme_SG       ciscoCat2950124       ✓         ④       Internet-switch-4       Acme       Acme_SG       ciscoCat2950124       ✓         ④       Internet-switch-6       Acme       Acme_SG       ciscoCat2950124       ✓         ●       Internet-switch-6       Acme_SG       ciscoS560G-24PS       ✓         ●       Internet-swit       Acme       Acme_SG       hpProCurve3500yl-J       ✓	Sta       Dev       Name       Tenant V       Security Group       Device Profile       Agr       Status Last Modified         Image: Status internet-switch-2       Image: Status internet-switch-3       Acme       Acme_SG       ciscoCat3524XL       Jun 3, 2011 5:31:54 PM         Image: Status internet-switch-4       Image: Status internet-switch-4       Acme       Acme_SG       ciscoCat2950t24       Jun 3, 2011 5:31:29 PM         Image: Status internet-switch-4       Acme       Acme_SG       ciscoCat2950t24       Jun 3, 2011 5:31:29 PM         Image: Status internet-switch-4       Acme       Acme_SG       ciscoCat2950t24       Jun 3, 2011 5:31:29 PM         Image: Status internet-switch-4       Acme       Acme_SG       ciscoCat2950t24       Jun 3, 2011 5:32:08 PM         Image: Status internet-switch-4       Acme       Acme_SG       cisco3560G-24PS       Jun 3, 2011 5:29:31 PM         Image: Status internet-switch-6       Image: Status internet-SG       cisco3560G-24PS       Jun 3, 2011 5:29:31 PM         Image: Status internet-switch-8       Acme       Acme_SG       hpProCurve3500yLF       Jun 3, 2011 5:29:07 PM         Image: Status internet-switch-8       Acme       Acme_SG       hpProCurve3500yLF       Jun 3, 2011 5:29:07 PM

Figure 29: 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 station and the Regional NNMi station; the same is true for Security Groups if you want to share the security restrictions between the servers.

## Tenants and Security Groups in GNM Example

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 nnmsecurity.ovpl, 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-2fal-4d07-bla3-8le7cc16c72d : <mark>840eb5cb-23db-448b-95dc-8e948b34f4f8</mark> : Customer2 :

In the following figure, notice that the Global NNMi has created a Tenant and a Security Group with corresponding UUIDs.

Figure 30: Tenants Form: Tenant and Security Group for Customer2 at Global NNMi

Tenants				
🛛   * 🖻	😂 🖪   🤊 🖗   🗙   🔛			
Name	Initial Discovery Security Group	UUI	D	Description
Default Tenant	Default Security Group	1b96	6011e-8829-4e5d-8ab7-f93b7b10ac79	Default Tenant generated by NNMi
Customer2	Customer2	a8ec	cb97c-2fa1-4d07-b1a3-81e7cc16c72d	
	$\searrow$			
Security Groups	; 🗟   ማ 🐬   🗙   🖺		User Group 1	riiter 🔹 🗎 😒 🔍 1 -
Name	UUID		Description	
Default Security Grou	p 5ea18ccc-f4ee-40db-b640-446bc4138	92b	Default Security Group generated by NNMi	
Unresolved Incidents	2d7c16a9-ccf8-4206-be80-0005e6c9d	cf1	Controls access to incidents without a reso	lved source node
Customer2	840eb5cb-23db-448b-95dc-8e948b34f	4f8	$\supset$	

2. Now, at the Regional NNMi station, use the nnmsecurity.ovpl command line tool 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 station). 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-2fal-4d07-bla3-
8le7cc16c72d -securityGroupUuid 840eb5cb-23db-448b-95dc-8e948b34f4f8
a8ecb97c-2fal-4d07-bla3-8le7cc16c72d : 840eb5cb-23db-448b-95dc-8e948b34f4f8 :
Customer2 :
```

3. Now you can load seeds at the Regional NNMi 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 with the Tenant as Customer2 and the associated Security Group as Customer2. These nodes are synchronized to the Global NNMi station using the same Tenant and Security Group UUID, as shown in the following figure.

Figure 31: Nodes Form: Customer2 Tenant and Security Group at Global NNMi

( <b>•</b> )					Agenti	Status Last Modified	Management Server	Notes
	bigip	Customer2	Customer2	F5 BIG-IP 6800	~	Jun 6, 2011 5:03:21 PM	nmcvm24	
2	c2900sw	Customer2	Customer2	<no snmp=""></no>		Jun 6, 2011 5:04:45 PM	nmcvm24	
	c2900xl-1	Customer2	Customer2	ciscoCat2912XL	~	Jun 6, 2011 5:03:21 PM	nmcvm24	
·‡	cisco2k1	Customer2	Customer2	cisco2621	~	Jun 6, 2011 5:03:50 PM	nmcvm24	
) <b>‡</b>	cisco4k1	Customer2	Customer2	cisco4500	<b>~</b>	Jun 6, 2011 5:01:52 PM	nmcvm24	
1	dc6509-2	Customer2	Customer2	ciscocat6509	~	Jun 6, 2011 5:02:58 PM	nmcvm24	
				/				

4. At the Global NNMi station (and at the Regional NNMi station, 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 station if your users are signing into the Global NNMi station only. Users and User Groups are private to each NNMi system 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 GNM feature was also shown.

#### Legal Notices

#### Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

#### **Restricted Rights Legend**

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

#### **Copyright Notices**

© Copyright 2011 Hewlett-Packard Development Company, L.P.

#### Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

HP-UX Release 10.20 and later and HP-UX Release 11.00 and later (in both 32 and 64-bit configurations) on all HP 9000 computers are Open Group UNIX 95 branded products.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

#### Oracle Technology - Notice of Restricted Rights

Programs delivered subject to the DOD FAR Supplement are 'commercial computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement. Otherwise, programs delivered subject to the Federal Acquisition Regulations are 'restricted computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the restrictions in FAR 52.227-19, Commercial Computer Software-Restricted Rights (June 1987). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

For the full Oracle license text, see the license-agreements directory on the NNMi product DVD.

#### Acknowledgements

This product includes software developed by the Apache Software Foundation.

(http://www.apache.org)

This product includes software developed by the Indiana University Extreme! Lab.

(http://www.extreme.indiana.edu)

#### Support

Visit the HP Software Support web site at:

#### www.hp.com/go/hpsoftwaresupport

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

#### http://h20229.www2.hp.com/passport-registration.html

To find more information about access levels, go to:

http://h20230.www2.hp.com/new\_access\_levels.jsp