

HPE Network Node Manager i Software 10.20

Step-by-Step Guide to Using Security Groups

White Paper

Contents

Security Groups	3
Introduction	3
Security Concepts	4
Security Groups Model	5
Security Groups Example	6
Remove Default User Group Mappings	6
Create Users	7
Create User Groups	8
Map Users to User Groups	9
Create Security Groups	11
Map User Groups to Security Groups	13
Assign Nodes to Security Groups	15
Verify Example	17
Tenants	19
Tenant Example	19
Tenants and Security Groups in Global Network Management (GNM)	24
Conclusion	
We appreciate your feedback!	

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

Network Node Manager i	<u>F</u> ile <u>V</u> iew <u>T</u> ools	Actions <u>H</u> elp			
Dashboards	Security Group Mapping				
ncident Management گ		· · ·			
🚠 Topology Maps	User Group	Security Group	Object Access Privilege		
🖵 Monitoring	NNMi Level 1 Operators	Default Security Group	Object Operator Level 1		
	NNMi Level 2 Operators	Default Security Group	Object Operator Level 2		
	NNMi Guest Users	Default Security Group	Object Guest		
	NNMi Level 1 Operators	Unresolved Incidents	Object Operator Level 1		
🧟 Management Mode	NNMI Level 2 Operators	Unresolved incidents	Object Operator Level 2		
R Incident Browsing	NNMI Guest Osers	Unresolved incidents	Object Guest		
🖉 MPLS					
🖌 IP Multicast					
Cisco IP Telephony					
🖉 Acme IP Telephony					
🖉 Nortel IP Telephony					
🖉 Avaya IP Telephony					
🖌 Microsoft IP Telephony					
🗞 Integration Module Configuration					
🗲 Configuration					
	1				
 Security 					
🎢 Security Wizard	Updated: 7/18/16 04:22:3	5 AM		Total: 6	Selected: 0
User Accounts					
🖽 User Groups	 Analysis 				
I User Account Mappings	Summary		C		
Security Groups		No Objects Selected			
E Security Group Mappings					

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.

Security Vikad Wotcome Wotcome Notaber/Souting Notaber/Souting A Topulace/Souting A Topulace/Souting A Topulace/Souting A Topulace/Souting Notaber/Souting Notaber/Souting <th>Network Node Manager I</th> <th>Elle Iools Help</th> <th></th> <th></th> <th></th> <th>Up</th> <th>r Name system NNMi Role Adn</th>	Network Node Manager I	Elle Iools Help				Up	r Name system NNMi Role Adn
<th>at Dashboards</th> <th>Security Wizard *</th> <th></th> <th></th> <th></th> <th></th> <th></th>	at Dashboards	Security Wizard *					
 ▲ Topology Maps: ▲ Monitoring ▲ Tomalicationaling ▲ Tomalicationaling ▲ Tomalicationaling ▲ Tomalicationaling ▲ Tomalicationaling A Tomalicationaling	a Incident Management	y Welcome	Use this page to do any of the	following:			
 Maladardarda Mada User Groups and Security Groups A sing Node to Security Groups A sing Node to Security Groups Management Mode Management Mode Molest Browsing MRLs Multicust Chose to Telephony A says IP Telephony Management Mode California Telephony Management Mode Californi	A Topology Maps	> Map User Accounts and User Groups	Create and Delete User Account	ts, Create and Delete User Groups	Assign User Accounts to User Groups, Assign	User Groups to User Accounts	Remove User Accounts Mappings.
 A troubleshooting Assign Noose to Security Groups Assign Noose to Security Groups View Summary of Changes Wew Summary of Changes Wew Summary of Changes Name User Account Mane User Account Mene User Account Mene User Account Mene User Account Mene <li< td=""><td>P Monitoring</td><td>>> Map User Groups and Security Groups</td><td>User Accounts</td><td>User Account M</td><td>tappings</td><td>User Group</td><td>•</td></li<>	P Monitoring	>> Map User Groups and Security Groups	User Accounts	User Account M	tappings	User Group	•
 Nventory View Summary of Changes Name User Account Mangement Mode Indiant Indiant MBLS MBLS Modical PT Rephony Across IP Telephony Across IP Telephony Model SP Telephony <l< td=""><td>A Troubleshooting</td><td>Assign Nodes to Security Groups</td><td>* 🗰 %</td><td>1</td><td></td><td>(A)#</td><td>8</td></l<>	A Troubleshooting	Assign Nodes to Security Groups	* 🗰 %	1		(A)#	8
Attangement Mode mpl3 mpl3 NNMI Web Service Clients client NNMI Web Service Clients guest NNMI Global Operators W MPLS Gasol Gasol NNMI Web Service Clients global guest NNMI Administrators W Clicos IP Telephony mmc_oper1 NNMI Web Service Clients service 1 Operators servic	E Inventory	View Summary of Changes	Name	User Account	User Group	Naine	Display Name
incodent Browsing mcas1 mcas1 NNMI Web Service Clients gues1 NNMI Gues1 Users W MPLS lpt lpt NNMI Web Service Clients globalpo NNMI Gues1 Users W Phulicas1 oppo oppo oppo oppo oppo oppo oppo nnmi oppo oppo oppo nnmi nnmi oppo nnmi oppo nnmi oppo nnmi nnmi oppo oppo nnmi oppo oppo nnmi oppo oppo oppo nnmi oppo oppo nnmi oppo oppo </td <td>n Management Mode</td> <td></td> <td>mpls</td> <td>mpis</td> <td>NNMi Web Service Clients</td> <td>client</td> <td>NNMI Web Service Clients</td>	n Management Mode		mpls	mpis	NNMi Web Service Clients	client	NNMI Web Service Clients
ip for			mcast	mcast	NNMi Web Service Clients	guest	NNMi Guest Users
# PRIS asspi asspi vasspi NMM WebService Clients admin NMM diministrators # IPRIS nmc_sbmin nmc_oper1 nmc_oper2 NMM Level 2 Operators Kev2 NMM Level 2 Operators # Acme B Talephony nmc_oper1 nmc_sdmin nmc_sdmin NMM administrators Kev2 NMM Level 2 Operators # Acme B Talephony nmc_oper2 nmc_ndmin nmc_sdmin NMM administrators # Acme B Talephony nmc_oper2 nmc_ndmin NMM Administrators # Acme B Talephony nmc_oper2 nmc_ndmin NMM Administrators # Arme JP Telephony nmc_oper3 NMM Administrators Kev3 # Microsoft IP Telephony Integration Module Contiguration Kev3 Kev3 # Contiguration voic integrade Kev3 Kev3	as indicate browsing		lpt	ipt	NNMI Web Service Clients	globalops	NNMI Global Operators
Image: Minimage: Mi	MPLS		qaspi	qaspi	NNMi Web Service Clients	admin	NNMi Administrators
Closs (P Talephony mmc_oper1 mmc_o	💉 IP Multicast		nmc_admin	nmc_oper2	NNMI Level 2 Operators	level2	NNMi Level 2 Operators
 Anne (IP Telephony Note (IP Telephony Avery (IP Telephony Microsoft (P Telephony Microsoft (P Telephony Integration Module Configuration Configuration Some microsoft Some micr	Cisco IP Telephony		nmc_oper1	nmc_oper1	NNMi Level 1 Operators	level1	NNMi Level 1 Operators
	🖌 Arma 10 Talanhony		nmc_oper2	nmc_admin	NNMi Administrators		
Avarya (B) Telephony Avarya (B) Telephony Microsoft (B) Telephony Microsoft (B) Telephony Configuration Configuration Over Immerve Security			John				
	Nortel IP Telephony						
Microsoft IP Telephony Integration Module Configuration A Configuration units interve work interve Configuration Configuration Configuration Configuration	💉 Avaya IP Telephony						
 Integration Module Configuration ✓ Over integration ✓ = ver integration ✓ = ver integration 	🖉 Microsoft IP Telephony						
Configuration use missive be Security	% Integration Module Configuration						
🔸 📾 Security 🧄	Configuration						
	🔻 😂 Security						

Figure 5: Security Wizard: Create User Group

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

Create User Grou	ip ×
Name	KentuckyOper1 ×
Display Name	Kentucky Level 1 Operato
Directory Service Name	P
Description	Kentucky Level 1 Operator
Add	Close

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.

🕼 Network Node Manager					User Name: system	NNMi Role: Admir	istrator Sign O
<u>F</u> ile <u>T</u> ools <u>H</u> elp							
2 Dashboards ¥	Security Wizard *						
👌 Incident Management 🛛 🕹 🕹	🔊 Welcome	Use this page to do any of the following: Create and Delete User Accounts, Create a	nd Delete User Gro	oups. Assign User Accounts to User Grou	ps. Assian User Gro	ups to User Account	s. Remove User Accounts
🗛 Topology Maps 🛛 😵	🔉 Map User Accounts and User Groups	Mappings. User Accounts	User Account M	anninas	User Gr	ouns	<
Monitoring ¥	🔊 Map User Groups and Security Groups	* 🗙 🚍	×		* >	۲.	•
Troubleshooting ¥	🔉 Assign Nodes to Security Groups	Name	User Account	User Group		Name	Display Name
Inventory ¥	🔊 View Summary of Changes	George	John	NNMi Level 1 Operators		a desta	
Management Mode 🛛 🕹		John	John	Detroit Level 1 Operators		admin	NNMi Administrators
5 Incident Browsing 🛛 🕹		Paul				level1	NNMi Level 1 Operators
$ m {}^{\it J}$ Integration Module Configuration $\qquad lpha$		Ringo					
Configuration		administrator				level2	NNMi Level 2 Operators
🔁 Communication Configuration.					\bigcirc	client	NNMi Web Service Clients
Discovery						quest	NNMi Guest Lisers
Monitoring						guou	
Status Configuration						globalops	NNMi Global Operators
Global Network Management.						KentuckyOper1	Kentucky Level 1 Operators
📧 🧰 User Interface							4
- 🗁 Security						KentuckyOper2	Kentucky Level 2 Operators
Recurity Wizard					6	DetroitOper1	Detroit Level 1 Operatore
User Accounts						Denotopern	Benoit Level 1 Operations
📰 User Groups					\bigcirc	DetroitOper2	Detroit Level 2 Operators
User Account Mappings							
m Security Groups							
📖 Security Group Mappings 🗸						~	
Secon Ro	Commences and and	and and a		and the stand	-	<previous next=""></previous>	Cancel Save & Clo

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.

Network Node Manager i	Eile Iools Help						User Name system NNMI Role Admini
🕍 Dashboards	Security Wizard *						
Incident Management مل	> Welcome	Use this p	age to do any of the following:				
Topology Maps	Map User Accounts and User Groups	Create and	d Delete User Groups. Create and Delete Se	urity Groups, Assign User G	roups to Secu	rity Groups, Assign Security Groups	s to User Groups, Remove Security Group Mapping
C Menitoring	Map User Groups and Security Groups	User Group		Security Grou	p Mappings		Security Groups
Troubleshooting	Assign Nodes to Security Groups	* 8	*	B Object 0	operator Level	2 2	(A) = %
a inventory	View Summary of Changes	Name	Display Name	User Group	Security Gro	u Object Access Privilege	Name
Management Mode		client	NNMi Web Service Clients	NNMI Level 1	Default		Default Security Group
Incident Browsing		guest	NNMI Guest Users	Operators	Group	Object Operator Level 1	Unresolved Incidents
MOIN S		globalops	NNMi Global Operators	NNMI Level 2	Default	Object Occupation Lawel 2	
		admin	NNMi Administrators	Operators	Group	Cojeci Operator Level 2	
e le Humast		level2	NNMi Level 2 Operators	NNMi Guest	Default	Object Guest	
Cisco IP Telephony		ievera.		Users	Group	colect ages.	
Acme IP Telephony				NNMi Level 1	Unresolved	Object Operator Level 1	
Nortel IP Telephony				NNMI Level 2	Unresolved	Object Onerster Level 2	
Avaya IP Telephony				Operators	Incidents	object operator several	
Microsoft IP Telephony				Users	Incidents	Object Guest	
Integration Module Configuration							
Configuration							
E Searth							
Z Security Wirnert							
I User Accounts							
Iller Groups							

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.

		Opera
Create S	ecurity Group	,
Name	Kentucky Security Group	
Description	Kentucky Security Group	
	Add Close	

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 \triangleleft 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.

File Tools Help								
	County Mittand \$							
Deshloards S Josenboards S	Welcome Map User Accounts and User Groups Map User Accounts and User Groups	Use this page to o Create and Delete Remove Security o User Groups	do any of the following: User Groups, Create and Delete Group Mappings.	Security Groups, Ar Security Group I	ssign User Groups I Mappings	to Security Groups, Assign	Security Gr Security	roups to User Groups Groups
Traubleshooting	Assiste Made to Security Groups	eal 🗛 🔹		A Object Ope	rator Level 2	·	* *	• tee
	Assign Nodes to Security Groups	Name	Display Name	User Group	Security Group	Object Access Privileg		Name
inventory 😵	View Summary of Changes	admin	NNMi Administrators	Detroit Level 2	Detroit Security			Default Security Gr
Management Mode 🛛 🕹 😵		level1	NNMi Level 1 Operators	Operators	Group	Object Operator Level 2		
🏠 Incident Browsing 🛛 🕹		level2	NNMi Level 2 Operators					Unresolved Incident
🛷 Integration Module Configuration 🛛 💝		client	NNMi Web Service Clients					
		guest	NNMi Guest Users				\triangleleft	Kentucky Security Group
		globalops	NNMi Global Operators					
Communication Configuration		KentuckyOper1	Kentucky Level 1 Operators					Detroit Security Gro
🗀 Discovery	1	KentuckyOper2	Kentucky Level 2 Operators					
📧 🧰 Monitoring		DetroitOper1	Detroit Level 1 Operators					
🛅 Incidents		DetroitOper2	Detroit Level 2 Operators	4				
📑 Status Configuration								
📑 Global Network Management								
📧 🧰 User Interface								
🖃 🗁 Security								
🜱 Security Wizard								
Iser Accounts								
🛲 User Groups								
IIII User Account Mappings								
📰 Security Groups 🗸 🗸								
andreas 2 million					-	<previous (<="" td=""><td>Next></td><td>Cancel Save & Clo</td></previous>	Next>	Cancel Save & Clo

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.

Metwork Node Manager							Name: system NNMi Role: Admini	strator Si
<u>file T</u> ools <u>H</u> elp								
Dashboards	×	Security Wizard *						
Incident Management	×	🔉 Welcome	The Assign Nodes to Security G For instructions, click here.	oups option ena	bles you to assign	one or more nodes to a Security G	Group. Use the Available Nodes tab	le view to select the nor
Topology Maps	*	🔊 Map User Accounts and User Groups	Security Groups	Nodes	Currently Assigne	d to Selected Group:	Nodes to be Assigned to S	elected Group:
Monitoring	*	Map User Groups and Security Groups	· •	Name	 Hostna 	me		
Troubleshooting	×	Assign Nodes to Security Groups	Name					
Inventory	×		Default Security Group					
Management Mode	*		Unresolved Incidents					
Incident Browsing	*		Detroit Security Group					
Integration Module Configuration	×		,					
Configuration	*							
Communication Configuration	^							
Discovery			Available Nodes:					
			a se			<empty g<="" td=""><td>roun filters</td><td>1.6 of 11 🖎 🕅</td></empty>	roun filters	1.6 of 11 🖎 🕅
Incidents Status Configuration						- Chipty O	Noop micro	
Glabal Natural Management			Devic Name Assign	elected Nodes	to Selected Securi	ty Group		
Global Network Management			**f*** mcrouter171 192.168	.2.245	192.168.2.245	Default Security Group		
Oser Interrace			****** mcrouter181 192.168	.2.246	192.168.2.246	Default Security Group		
Security Witterd			**** mcrouter183 192.168	.2.247	192.168.2.247	Default Security Group		
			***** mcrouter184 192.168	.2.248	192.168.2.248	Default Security Group		
Liser Groups			***** mcrouter185 192.168	2.249	192.168.2.249	Default Security Group		
user Groups			***** mcrouter186 192 16/	2 250	192 168 2 250	Default Security Group		
user Account Mappings						contraction of the second s		
Security Groups	~		Updated: 11/27/14 09:20:34 PM		т	otal: 11 Selected: 4	Filter: OFF	Auto refresh
Security Group Mappings								

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.

Metwork Node Manager		User Name: system NNMi Role: Administrator Sign Out
<u>File Tools H</u> elp		
② Dashboards >>	Security Wizard *	
👌 Incident Management 🛛 🕹	🔉 Welcome	The View Summary of Changes option enables you to view your recent configuration changes. For more information, click here.
🙏 Topology Maps 🛛 😵	🔉 Map User Accounts and User Groups	The following User Accounts will be created:
Monitoring ¥	Map User Groups and Security Groups	administrator, George, John, Paul, Ringo
Troubleshooting ¥	Assign Nodes to Security Groups	The following User Groups will be created:
Inventory ¥	Niew Summary of Changes	Kentucky Level 1 Operators, Kentucky Level 2 Operators, Detroit Level 1 Operators, Detroit Level 2 Operators
S Management Mode 🛛 🕹	-	The following User Account Mappings will be created:
🇞 Incident Browsing 🛛 🗧 🕹		John->NNMi Level 1 Operators, John->Detroit Level 1 Operators, Paul->NNMi Level 2 Operators, Paul->Detroit Level 2 Operators, George->NNMi Level 1 Operators, George->Kentucky Level 1 Operators, Paul->Kentucky Level 2 Operators, Ringo->NNMi Administrators, administrator->NNMi Administrators
A Integration Module Configuration		The following Security Groups will be created:
Communication Configuration		The following Security Group Mappings will be created:
📧 🧰 Discovery		Kentucky Level 1 Operators, SKentucky Security Group Object Operator Level 1 Detroit Level 1 Operators, SDetroit Security Group Object Operator Level 1
🛞 🧰 Monitoring	1	Detroit Level 2 Operators->Detroit Security Group:Object Operator Level 2, Kentucky Level 2 Operators->Kentucky Security Group:Object Operator Level 2
🔹 🧰 Incidents		The following User Groups are not mapped to Security Groups and may not have access to any
E Status Configuration		Nodes:
📑 Global Network Management		level1, level2, guest, globalops
📧 🧰 User Interface		The following Security Groups have Node assignment changes:
🖃 🗁 Security		Detroit Security Group, Kentucky Security Group
🜱 Security Wizard		
III User Accounts		
🕅 User Groups		
User Account Mappings		
🕅 Security Groups 🗸 🗸		
< >	X	<previous next=""> Cancel Save & Close</previous>

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.

Metwork Node Manager								User Name: Georg	e NNM	li Role: Operator Level 1	Sign
<u>F</u> ile ⊻iew <u>T</u> ools A <u>c</u> tions <u>H</u> elp											
② Dashboards	Nodes										~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
👌 Incident Management 🛛 🕹	🗵 📑	6 🖣	3 5 🖗	E				<empty filter<="" group="" th=""><th>•</th><th>💌 🔯 🔇 1 - 4 of 4</th><th></th></empty>	•	💌 🔯 🔇 1 - 4 of 4	
\Lambda Topology Maps 🛛 🗧 🗧	Status	Devic	Name 🔺	Hostname	Management Ad	Security Group	System Location	Device Profile	Agen	Status Last Modified	Notes
Monitoring ¥	Δ.	- <u>†</u>	mcrouter171	192.168.2.245	192.168.2.245	Kentucky Security Group	STSD Bangalore	cisco2621	~	Nov 27, 2014 9:16:35 PM	1
Troubleshooting ¥	0	- <u>†</u>	mcrouter181	192.168.2.246	192.168.2.246	Kentucky Security Group	STSD Bangalore	cisco2621	~	Nov 27, 2014 9:16:07 PM	
inventory *	<u>^</u>	- -	mcrouter183	192.168.2.247	192.168.2.247	Kentucky Security Group	STSD Bangalore	cisco2621	~	Nov 27, 2014 9:19:59 PM	
Modes	0		mcrouter184	192 168 2 248	192 168 2 248	Kentucky Security Group	STSD Bangalore	cisco2621	~	Nov 27, 2014 9:21:12 PM	
Interfaces	-	•		102.100.2.2.10	102.100.2.2.10		ereb bangalore	010002021			
IP Addresses											
SNMP Agents							-				
		\sim				And the second s			~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~		

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.

Page 1	8
--------	---

🕼 Network Node Manager							(User Name: John	NNMi	i Role: Operator Level 1	Sign Out
<u>File View Tools Actions Help</u>											
② Dashboards	Nodes										
♦ Incident Management ¥	🗵 🖻	S	🖪 🤭 🦃				4	Empty Group filter>		▼ 🐼 🔇 1-4 of 4	> 🛛 📑
🙏 Topology Maps 🛛 🕹	Status	Devic	Name 🔺	Hostname	Management Ad	Security Group	System Location	Device Profile	Agen	Status Last Modified	Notes
Monitoring ¥	0	瓕	mplspe511	192.168.124.126	192.168.124.126	Detroit Security Group	MIMIC	ciscoME6524-GT-	~	Nov 27, 2014 9:21:12 PM	
Troubleshooting ¥	0	111 111	mplspe512	192.168.124.127	192.168.124.127	Detroit Security Group	MIMIC	ciscoME6524-GT-	~	Nov 27, 2014 9:20:05 PM	
Inventory *	0	题	mplspe513	192.168.124.128	192.168.124.128	Detroit Security Group	MIMIC	ciscoME6524-GT-	~	Nov 27, 2014 9:19:42 PM	5
Modes	0	aa Ma	mplspe514	192,168,124,129	192,168,124,129	Detroit Security Group	міміс	ciscoME6524-GT-	~	Nov 27, 2014 9:12:06 PM	
m Interfaces	<u> </u>	**									
IP Addresses											
III SNMP Agents											
					and the second second					and the second s	Multimet

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.

⊻iew <u>T</u> ools A <u>c</u> tions <u>H</u> elp									-		
Dashboards	* Node	s									
ncident Management	* 🖉	🖻 🖉	n 🔁 🖓 🖓				<e< th=""><th>mpty Group filter></th><th></th><th>👻 🕼 🔇 1-8 of 8 🕻</th><th>> 🕅</th></e<>	mpty Group filter>		👻 🕼 🔇 1-8 of 8 🕻	> 🕅
Fopology Maps		is Devi	c Name 🔺	Hostname	Management Ad	Security Group	System Location	Device Profile	Agen	Status Last Modified	Notes
Monitoring	× 🛕		mcrouter171	192.168.2.245	192.168.2.245	Kentucky Security Group	STSD Bangalore	cisco2621	~	Nov 27, 2014 9:16:35 PM	
Froubleshooting	× 📀		mcrouter181	192.168.2.246	192.168.2.246	Kentucky Security Group	STSD Bangalore	cisco2621	~	Nov 27, 2014 9:16:07 PM	
nventory	Â		mcrouter183	192.168.2.247	192.168.2.247	Kentucky Security Group	STSD Bangalore	cisco2621	~	Nov 27, 2014 9:19:59 PM	
Modes A	0		mcrouter184	192.168.2.248	192.168.2.248	Kentucky Security Group	STSD Bangalore	cisco2621	~	Nov 27, 2014 9:21:12 PM	
m Interfaces	0	M	mplspe511	192,168,124,126	192.168.124.126	Detroit Security Group	MIMIC	ciscoME6524-GT-	~	Nov 27, 2014 9:21:12 PM	
IP Addresses	0	-	mplspe512	192,168,124,127	192,168,124,127	Detroit Security Group	MIMIC	ciscoME6524-GT-	~	Nov 27, 2014 9:20:05 PM	
ID Subarts		222	mplene513	192 168 124 128	192 168 124 128	Detroit Security Group	MIMIC	circoME6524.GT	~	Nov 27, 2014 9:19:42 PM	
			mplanoE14	100 169 104 100	102.100.124.120	Detroit Security Group	MINIC	sisseME6524 CT		Nov 27, 2014 0:12:05 DM	
Chassis		**	Inpiapeo 14	132.100.124.125	102.100.124.128	Denon Security Group		030010120324-01-	÷	1404 27, 2014 8.12.00 PM	

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.

Eile ⊻iew Tools Agtions Help												
2 Dashboards	×N	lodes										
Incident Management	* 2	9 📑	8	2 🔊 🖗	× 🖴				<empty filters<="" group="" th=""><th>• • • •</th><th>🕽 🦪 1 - 11 of 11 🗇 🛛</th><th>3 </th></empty>	• • • •	🕽 🦪 1 - 11 of 11 🗇 🛛	3
Topology Maps	* 5	Status	Device	Name	Hostname	Management Ad	Security Group	System Location	Device Profile	Agent Enabled	Status Last Modified	Note
Monitoring	*	£		mcrouter171	192.168.2.245	192.168.2.245	Kentucky Security Group	STSD Bangalore	cisco2621	~	Nov 27, 2014 9:16:35 PM	
³⁶ Troubleshooting	* 6	2		mcrouter181	192 168 2 246	192 168 2 246	Kentucky Security Group	STSD Bangalore	cisco2621	~	Nov 27, 2014 9:16:07 PM	
Inventory	*	•	•	merouter183	102 168 2 247	192 168 2 247	Kentucky Security Group	STSD Bangalore	cieco2621	- -	Nov 27, 2014 9:19:59 PM	
T Nodes		-	:	Incrouter 105	132.100.2.247	132.100.2.247	Kentucky Security Group	STSD Daligatore	015002021	•	NOV 27, 2014 5.15.35 PM	
Interfaces		2		mcrouter184	192.168.2.248	192.168.2.248	Kentucky Security Group	STSD Bangalore	cisco2621	~	Nov 27, 2014 9:21:12 PM	
IP Addresses	4	1	- †	mcrouter185	192.168.2.249	192.168.2.249	Default Security Group	STSD Bangalore	cisco2621	~	Nov 27, 2014 9:18:07 PM	
III SNMP Agents		9	- !	mcrouter186	192.168.2.250	192.168.2.250	Default Security Group	STSD Bangalore	cisco2621	~	Nov 27, 2014 9:21:57 PM	
IP Subnets		9	顨	mplspe510	192.168.124.125	192.168.124.125	Default Security Group	MIMIC	ciscoME6524-GT-8S	~	Nov 27, 2014 9:15:41 PM	,
III VLANs		9	₩.	mplspe511	192.168.124.126	192.168.124.126	Detroit Security Group	MIMIC	ciscoME6524-GT-8S	~	Nov 27, 2014 9:21:12 PM	
Chassis		2	頭	mplspe512	192.168.124.127	192.168.124.127	Detroit Security Group	MIMIC	ciscoME6524-GT-8S	~	Nov 27, 2014 9:20:05 PM	
Cards		2	Ш.	mplspe513	192.168.124.128	192.168.124.128	Detroit Security Group	міміс	ciscoME6524-GT-8S	~	Nov 27, 2014 9:19:42 PM	1
m Ports		- 9	333	mplaneE14	102 169 124 120	102 169 124 120	Datrait Security Crown	MIMIC	sinceMERE24 OT 25	4	Nev 27, 2014 0:12:05 DM	
m Node Sensors			**	Inpispes 14	132.100.124.125	132.100.124.123	Denon Security Group	MINIC	CISCOMI20324-01-03	•	140V 27, 2014 9.12.00 PM	

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, nnmsecur i ty. 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 nnmsecur i ty. ovpl script. Consider using the nnmsecur i ty. 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.

🚺 Network Node Manager			User Name: system NNMi F	Role: Administrator Sign O
<u>File View Tools Actions H</u> elp				
② Dashboards	Security Groups			
A Incident Management	🗴 🖉 🌔 🖻 🛛 🖉 😓 🖉 🔊 🦻 🔰	🕻 🔛 🛛 🗸	Iser Group filter 🔹 🗐 🐼	🔷 1-4 of 4 🗇 🕅
🛧 Topology Maps	× Name UUID		Description	
Monitoring	Default Security Group 5ea18ccc-f4ee-40	db-b640-446bc413892b	Default Security Group generated b	y NNMi
Troubleshooting	Unresolved Incidents 2d7c16a9-ccf8-42	06-be80-0005e6c9dcf1	Controls access to incidents without	t a resolved source node
1 Inventory	Kentucky Security Group cf97203a-f3cd-48t	e-83ed-1f16c2d64941	Kentucky Security Group	
📀 Management Mode	Detroit Security Group 9e33734b-0447-4	50c-844f-bf7539dd17ed	Detroit Security Group	
🏀 Incident Browsing	*			2
4 Integration Module Configuration	*			
≁ Configuration	*			
Communication Configuration Communication Configuration Monitoring Communication Configuration Communication Conf	Updated: 11/27/14 11:47:35 PM Analysis Summary C No Objects Selected	Total: 4	Selected: 0 Filter: OFF	Auto refresh: 5 m

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.

🍈 Network Node Manager				User Name: system	NNMi Role: Administrator	Sign C
<u>File View Tools Actions Help</u>						
② Dashboards ¥	Tenants					
♦ Incident Management ¥	. €	😂 🗟 🤊 🖓 🗙 🔛			🔯 🌒 1-1 of 1 🖗	ା 🔁
\Lambda Topology Maps 🛛 🕹	Name	Initial Discovery Security Group	UUID		Description	- 1
Monitoring ¥	Default Tenant	Default Security Group	1b96011e-8829-4e5d-	8ab7-f93b7b10ac79	Default Tenant generated	i by NNMi 💊
Troubleshooting ¥						5
Inventory ¥						5
O Management Mode	Updated: 11/27/14	11:57:58 PM	Total: 1 Select	ed: 0 Filter: C	OFF Auto re	fresh: 5 mil
ncident Browsing 😵	Analysis					
Integration Module Configuration *	Summary 🚭					
♪ Configuration						
📑 Communication Configuration	No	Objects Selected				1
🖃 🗁 Discovery						
Discovery Configuration						
m Seeds						
Tenants						
Overlapping Address Mappi						
🗄 🦳 Monitoring 🗸 🗸						3
🗄 🧰 Incidents		.				
have been and the second		mathematical and				

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.

🕢 Network Node Manager	User Name: system NNMi Role: Administrator Sign 7
ile ⊻iew <u>T</u> ools A <u>c</u> tions <u>H</u> elp	
Dashboards 🛛 🕹	Tenant*
Incident Management 🛛 🕹	💯 📴 🎽 🖉 Save and Close 🥭 🗶 Delete Tenant 🔛
Topology Maps 🛛 🕹	Nodes of Tenant Overlapping Address Mappings
Monitoring ¥	NNMi associates Tenant objects with Nodes to identify which This table shows the list Nodes currently assigned to this Tenant.
Troubleshooting ¥	network resources are assigned to each customer. Each Node has one Tenant. For more information. click here.
Inventory ¥	·
Management Mode 🛛 🕹	* Name
Incident Browsing ¥	UUID 7b8b2337-9f70-4d41-8527-2
$\stackrel{\scriptstyle \circ}{_{\sim}}$ Integration Module Configuration \qquad $\stackrel{\scriptstyle \circ}{_{\sim}}$	Description Status Devic Name A Hostname
Configuration *	Acme Company
📑 Communication Configuration	Group
E Discovery	
Discovery Configuration	
m Seeds	
Tenants	
📰 Overlapping Address Mappi	
🗄 🧰 Monitoring	Updated: 11/28/14 12:05:53 AM Total: 0 Selected: 0 Filter: 0
• 🗀 Incidents	Analysis Summary No Objects Selected
and the second s	the second

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.

🕼 Network Node Manager								User Name: syste	em NN	IMi Role: Ad	dministrator	Sign CL
<u>File ⊻iew Tools Actions H</u> elp												
2 Dashboards >	Nodes											
♠ Incident Management ¥	2 🖻		2 5 🖓	× 🖴			<empt< th=""><th>y Group filter></th><th></th><th></th><th>🗘 1 - 3 of 3 🕼</th><th>ା 🍺</th></empt<>	y Group filter>			🗘 1 - 3 of 3 🕼	ା 🍺
🔥 Topology Maps 🛛 💝	Status	Device	Name 🔺	Hostname	Management Ad	Tenant⊽	Security Group	Device Profile	Agent	Status La	st Modified	Notes
Monitoring ×	<u> </u>	1 ⁸ t	Bang-gw	192.168.113.3	192.168.113.3	Acme	Acme SG	cisco3640	~	Nov 28, 20	014 12:27:35 AM	<
Troubleshooting ×	0		11-11-05	100 100 110 1	100 100 110 1	A	-					- (
inventory 🛠	<u> </u>	866	NORTHPE	192.168.113.1	192.168.113.1	Acme	Acme_SG	cisco3640	*	NOV 28, 20	J14 12:26:31 AM	
	0	1 11	SouthPE	192.168.113.2	192.168.113.2	Acme	Acme_SG	cisco3640	~	Nov 28, 20	014 12:24:51 AM	
m Nodes												
Interfaces												5
IP Addresses				_								- 1
and the second sec				Annual States		March 199	-	- mark		~~~~		proven a

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.

Tenants				
🗵 * 📑	😂 🗟 🤊 🦻 🗙 🔛			
Name	Initial Discovery Security Group	UUID		Description
Default Tenant	Default Security Group	1b960	011e-8829-4e5d-8ab7-f93b7b10ac79	Default Tenant generated by NNMi
Customer2	Customer2	a8ecb	097c-2fa1-4d07-b1a3-81e7cc16c72d	
Engurity Croups	ß			
	ን 🗟 🔊 💎 🗙 🔛		User Grou	p filter 🔹 🔯 🔍 1 -
Name	UUID		Description	
Default Security Grou	up 5ea18ccc-f4ee-40db-b640-446bc413	892b	Default Security Group generated by NNI	Mi
Unresolved Incidents	2d7c16a9-ccf8-4206-be80-0005e6c9	dcf1	Controls access to incidents without a re-	solved source node
Customer2	840eb5cb-23db-448b-95dc-8e948b34	f4f8		

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 nnmsecur ity. 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 :

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**.

Node	is >								
R	📑	🖉 🖪		<set filter="" group="" node=""></set>	- 🄝				
Sta	Dev	Name 🔺	Tenant	Security Group	Device Profile	Agent (Status Last Modified	Management Server	Notes
0	€₽	bigip	Customer2	Customer2	F5 BIG-IP 6800	~	Jun 6, 2011 5:03:21 PM	nmcvm24	
8	2	c2900sw	Customer2	Customer2	<no snmp=""></no>		Jun 6, 2011 5:04:45 PM	nmcvm24	
0	ŢŢ	c2900xl-1	Customer2	Customer2	ciscoCat2912XL	~	Jun 6, 2011 5:03:21 PM	nmcvm24	
0	‡	cisco2k1	Customer2	Customer2	cisco2621	~	Jun 6, 2011 5:03:50 PM	nmcvm24	
0	‡	cisco4k1	Customer2	Customer2	cisco4500	~	Jun 6, 2011 5:01:52 PM	nmcvm24	á
0	1	dc6509-2	Customer2	Customer2	ciscocat6509	~	Jun 6, 2011 5:02:58 PM	nmcvm24	
									1
									4
			I			_			
	\sim	and the second se							

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:



[©] Copyright 2016 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise 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. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.