

# **Alcatel-Lucent Security Management Server (SMS)**

Release 9.4

Administration Guide

260-100-017R9.4  
Issue 2  
September 2009

Alcatel, Lucent, Alcatel-Lucent and the Alcatel-Lucent logo are trademarks of Alcatel-Lucent. All other trademarks are the property of their respective owners.

The information presented is subject to change without notice. Alcatel-Lucent assumes no responsibility for inaccuracies contained herein.

Copyright © 2009 Alcatel-Lucent. All Rights Reserved.

# Contents

## About this information product

Purpose .....	xxi
Reason for reissue .....	xxi
Who Should Read this Book? .....	xxi
What is in this Book .....	xxi
What is Not in this Book .....	xxiv
Supported Brick devices .....	xxiv
Where to Find Technical Support .....	xxv
How to comment .....	xxv

## 1 Getting Started

Overview .....	1-1
To Log On and Off the SMS Server or Compute Server .....	1-2
To Use the Navigator Window .....	1-8
To Operate the SMS .....	1-13
Organizing the SMS Interface .....	1-20
Using the Find Name Tool .....	1-23
Using the Find IP Address Tool .....	1-29
Applying Changes .....	1-33
Concurrency Control .....	1-36
To Enable Concurrency Control .....	1-39

	To Force a Logout of an Administrator .....	1-41
	Basic Configuration Requirements .....	1-43
<b>2</b>	<b>SMS Redundancy</b>	
	Overview .....	2-1
	SMS Redundancy Concepts .....	2-2
	How Redundancy Works .....	2-6
	Redundant SMS Monitoring .....	2-8
	To Configure a Secondary SMS or Compute Server .....	2-11
<b>3</b>	<b>Configuring and Activating an Alcatel-Lucent VPN Firewall Brick™ Security Appliance</b>	
	Overview .....	3-1
	Deployment Considerations for a Brick Device .....	3-2
	To Configure a Brick Device on the SMS .....	3-19
	Brick Device Failover .....	3-38
	To Set Up Brick Device Failover .....	3-42
	To Manually Initiate Failover .....	3-48
	To Migrate Model 1100 Bricks to a Model 1200 Bricks That Are in a Failover Pair .....	3-50
	To Activate a Brick Device .....	3-52
<b>4</b>	<b>Configuring Alcatel-Lucent VPN Firewall Brick™ Security Appliance Ports</b>	
	Overview .....	4-1
	To Configure a Physical Port .....	4-3
	To Assign a Security Policy to a Port .....	4-9
	To Enable or Disable the BSR Voice Gateway (BVG) And/Or BSR Packet Gateway (BPG) Feature(s) .....	4-21
	Static Routes .....	4-32
	To Add a Static Route .....	4-34
	To Modify a Static Route .....	4-38
	To Activate or Deactivate a Static Route .....	4-39

	To Delete a Static Route .....	4-40
	To Activate a Login Banner on the Brick Serial Port Console .....	4-41
<b>5</b>	<b>Maintaining an Alcatel-Lucent VPN Firewall Brick™ Security Appliance Configuration</b>	
	Overview .....	5-1
	To View a Brick Snapshot .....	5-3
	To Modify a Brick .....	5-6
	To Apply Changes to a Brick Device .....	5-7
	To Delete a Brick Device .....	5-11
	To Move a Brick Device .....	5-12
	To Reboot a Brick Device .....	5-13
	To Reboot a Brick Device via the SMS .....	5-14
	To Refresh the MAC Table .....	5-16
	ARP and MAC Handling in the Brick .....	5-18
	Static MAC and ARP Assignments .....	5-20
	To Initiate a Ping or Traceroute from a Brick Device .....	5-22
	To Download Software to a Standalone Brick .....	5-24
	To Download Software to a Failover Brick .....	5-26
	To Download Software to Multiple Bricks .....	5-27
	To Configure Intelligent Cache Management .....	5-29
<b>6</b>	<b>Configuring VLANs on Alcatel-Lucent VPN Firewall Brick™ Security Appliances</b>	
	Overview .....	6-1
	What is a VLAN? .....	6-2
	Why Build VLANs? .....	6-4
	Forwarding Packets and VLAN Boundaries .....	6-5
	To Configure and Activate the Brick .....	6-6
	To Configure the Brick Physical Ports for VLAN-Tagged Traffic .....	6-7

	To Assign a Policy to the Ports .....	6-12
	To Associate a Network with a VLAN .....	6-15
	What are VLAN Bridge Groups? .....	6-18
	To Enable a Brick to Support VLAN Bridge Groups .....	6-19
	Configuring Bridging Between Specific VLANs .....	6-20
	Save and Apply the VLAN Configuration .....	6-21
<b>7</b>	<b>Configuring Alcatel-Lucent VPN Firewall Brick™ Security Appliance Partitions</b>	
	Overview .....	7-1
	What are Brick Partitions? .....	7-3
	Configure Brick Partitions .....	7-4
	Use Static Routes with Partitions .....	7-6
	Allow Partitions to Intercommunicate with Static Routes .....	7-7
	Save and Apply the Brick Configuration .....	7-10
	Interpreting IP Addresses When Brick Partitions Are Configured .....	7-11
<b>8</b>	<b>Creating SMS Groups and Administrators</b>	
	Overview .....	8-1
	What is a Group? .....	8-2
	To Create a Group .....	8-5
	To Maintain Groups .....	8-7
	SMS and Group Administrators .....	8-9
	To Create Administrator Accounts .....	8-10
	To Assign Groups and Privileges .....	8-17
	To Maintain Administrator Accounts .....	8-21
	To Use the SMS Messenger .....	8-25
<b>9</b>	<b>Compute Servers</b>	
	Overview .....	9-1

	What is a Compute Server? .....	9-2
	To Configure a Compute Server .....	9-5
<b>10</b>	<b>Remote Administration</b>	
	Overview .....	10-1
	The SMS Remote Navigator .....	10-2
	To Install the Remote Navigator on <i>Microsoft® Windows®</i> or <i>Vista®</i> .....	10-3
	To Install the Remote Navigator on <i>Solaris®</i> .....	10-7
	Permitting Remote Administration on the SMS .....	10-10
	To Create the Host Group .....	10-11
	To Create the Security Rules .....	10-12
	To Log In from a Remote Host .....	10-15
	Remote Administrator Capabilities .....	10-18
<b>11</b>	<b>Using the Configuration Assistant</b>	
	Overview .....	11-1
	The SMS Configuration Assistant .....	11-3
	Alarms .....	11-9
	Audit Trail .....	11-11
	Direct Paging .....	11-13
	FIPS .....	11-15
	GUI and Status Monitor Parameters .....	11-17
	Log Files .....	11-19
	Log Transfer .....	11-22
	Login Banner .....	11-25
	LSMS Web Parameters .....	11-27
	Reports .....	11-29
	SNMP Agent .....	11-31

	Software Download .....	11-34
	Strong Passwords .....	11-40
	TL1 Alarms .....	11-42
	Tunable Parameters .....	11-44
	User Authentication .....	11-46
<b>12</b>	<b>Backing Up and Restoring Data</b>	
	Overview .....	12-1
	Automatic Backup .....	12-2
	Manual Backup .....	12-3
	Scheduled Backups .....	12-6
	To Restore SMS Data on a Primary SMS .....	12-7
	To Restore SMS Data on a Secondary SMS .....	12-9
	Restore Scenarios on Redundant SMSs .....	12-11
	Other Restore Scenarios .....	12-12
<b>13</b>	<b>Task Scheduler</b>	
	Overview .....	13-1
	What is the Task Scheduler? .....	13-2
	Schedule Editor .....	13-3
<b>14</b>	<b>Using the Status Monitor</b>	
	Overview .....	14-1
	To Access the Status Monitor .....	14-2
	How to Interpret the Status Monitor .....	14-3
	Status Overview Window .....	14-6
	Administrators Window .....	14-14
	SMS/CS and Bricks Status Window .....	14-16
	Brick Status Windows .....	14-19



	Console Alarms Window .....	14-35
<b>15</b>	<b>Simple Network Management Protocol (SNMP)</b>	
	Overview .....	15-1
	Basic SNMP Concepts .....	15-2
	SNMP on the SMS .....	15-6
	SNMP on the Brick .....	15-9
	To Configure the SNMP on the Brick Feature .....	15-10
<b>A</b>	<b>Administer an Alcatel-Lucent VPN Firewall Brick™ Security Appliance Over the Internet from an Unregistered SMS</b>	
	Overview .....	A-1
	Background .....	A-2
	To Configure the Brick .....	A-3
	To Assign the Administrative Zone and Enter a VBA .....	A-4
	To Add NAT Rules to the <i>administrativezone</i> Ruleset .....	A-5
	To Activate the Remote Brick .....	A-8
<b>B</b>	<b>Sizing Guidelines</b>	
	Overview .....	B-1
	Sizing Tool .....	B-2
	Determine CPU Capacity .....	B-4
	Memory Utilization .....	B-6
	Disk Capacity for Log Files .....	B-7
	Disk Configuration .....	B-8
<b>C</b>	<b>Changing the IP Address of the SMS</b>	
	Overview .....	C-1
	To Change the IP Address of an SMS (Primary SMS Only) .....	C-2
	To Change the IP Address of a Primary SMS (Primary/Secondary SMS Pair) .....	C-4

To Change the IP Address of a Secondary SMS (Primary/Secondary SMS Pair) ..... C-6  
After the Update ..... C-8

**D Support for Non-IP Protocols**

Overview ..... D-1  
Ethertype and DSAP Files ..... D-2  
Procedure for Passing Non-IP Packets ..... D-3

**E VPN Firewall Solution Ports**

Overview ..... E-1

**F New Feature Setup**

Overview ..... F-1  
Determining Current SMS Feature Setup ..... F-2  
To Use the New Feature Setup Utility ..... F-3

**Index**

# List of tables

- 1     Getting Started**
  - 1-1    [Editing Buttons](#) ..... 1-17
  
- 14    Using the Status Monitor**
  - 14-1   [Brick Graphs from Status Overview Window](#) ..... 14-12



# List of figures

## 1 Getting Started

1-1	Navigator Login Window .....	1-4
1-2	SMS Remote Navigator Login Window .....	1-5
1-3	SMS Navigator Locked Window .....	1-7
1-4	Navigator Window .....	1-8
1-5	Folders Panel .....	1-10
1-6	Contents Panel .....	1-11
1-7	Move Column Header .....	1-19
1-8	Group (Folders and Subfolders) .....	1-20
1-9	Find Name (Search Results Example) .....	1-25
1-10	Find Name Dialog Box .....	1-26
1-11	Text List of Name Search Retrieval Entries .....	1-28
1-12	Find IP Address Window (Search Results) .....	1-30
1-13	Find IP Address Dialog Box .....	1-31
1-14	SMS Parameters Editor .....	1-39
1-15	Administrators Status Window .....	1-41

## 2 SMS Redundancy

2-1	LSMS/Computer Servers Editor Window .....	2-11
2-2	Host Group Editor window (SMS Host Group) .....	2-12

### 3 Configuring and Activating an Alcatel-Lucent VPN Firewall Brick™ Security Appliance

3-1	Brick Configuration .....	3-3
3-2	Firewall Configuration .....	3-5
3-3	LAN-LAN and Client Tunnels .....	3-6
3-4	Deployment of Brick device as BVG/BPG in BSR-based mobile network .....	3-8
3-5	Deployment of Brick devices in a customer's enterprise VoIP network .....	3-12
3-6	Brick/ALG Firewall Protection of MWG-CS Communications .....	3-15
3-7	Media Gateway - Call Server Initialization and Maintenance Flows .....	3-16
3-8	Telephone service provider hosting private communication exchange (PCX) equipment with full VoIP deployment .....	3-18
3-9	SMS Parameters Editor .....	3-20
3-10	SMS Parameters Editor (Brick User Defined Fields Tab) .....	3-21
3-11	SMS Parameters Editor (sample user-defined field entries) .....	3-22
3-12	Brick Editor (Brick Tab, sample user-defined fields for configuring a Brick) .....	3-23
3-13	Brick Editor (Brick Tab) .....	3-24
3-14	LSMS/LSCS Priority Editor .....	3-29
3-15	Brick Editor (Dynamic Addresses Tab) .....	3-31
3-16	Brick Editor (Options Tab) .....	3-33
3-17	Example of Brick Device Failover Physical Topology .....	3-41
3-18	Brick Editor (Failover Tab, Brick Failover Enabled) .....	3-43
3-19	Ping Failover Editor .....	3-45
3-20	Make Brick Boot Media Window .....	3-54
3-21	Make Brick Boot Media Window (Linux SMS floppy drive creation) .....	3-55
3-22	Make Brick Boot Media Window (Linux SMS flash drive creation) .....	3-56
3-23	Make Brick Boot Media Window .....	3-58
3-24	Make Brick Boot Media Window (with Password Fields) .....	3-59
3-25	Browser Window .....	3-60

3-26	Make Brick Boot Media Window .....	3-64
3-27	Make Brick Boot Media Window (Make Serial Port Boot Image Option Selected) .....	3-65
3-28	Serial Port Boot Image Output (1 of 2) .....	3-66
3-29	Serial Port Boot Image Output (2 of 2) .....	3-67
3-30	Make a Serial Port Boot Image (FTP Option) .....	3-68
<b>4</b>	<b>Configuring Alcatel-Lucent VPN Firewall Brick™ Security Appliance Ports</b>	
4-1	Brick Editor(Physical Ports Tab) .....	4-4
4-2	Brick Ports Editor .....	4-5
4-3	Brick Editor (Policy Assignment Tab) .....	4-10
4-4	Brick Policy Assignment Editor (Basic Tab) .....	4-11
4-5	Brick Policy Assignment Editor (Bandwidth Tab) .....	4-15
4-6	Brick Policy Assignment Editor (TOS Tab) .....	4-17
4-7	Policy Assignment Tab (Two Rulesets Assigned to Ether1) .....	4-18
4-8	Brick Editor (Policy Assignment Tab) .....	4-24
4-9	Brick Policy Assignment Editor .....	4-25
4-10	Brick Policy Assignment Editor (BVG/BPG Tab) .....	4-26
4-11	BVG Sub-Tab (QoS for RTP Parameters) .....	4-28
4-12	BVG/BPG Tab, BPG Sub-Tab .....	4-30
4-13	Brick Editor (Static Routes Tab) .....	4-34
4-14	Brick Static Route Editor .....	4-35
4-15	Confirm Deletion Window .....	4-40
<b>5</b>	<b>Maintaining an Alcatel-Lucent VPN Firewall Brick™ Security Appliance Configuration</b>	
5-1	Brick Snapshot .....	5-4
5-2	Apply Brick Window .....	5-8
5-3	Confirmation Window .....	5-11
5-4	Warning Window for Rebooting Standalone Brick Device .....	5-14

5-5	Warning Window for Rebooting Brick Device in Failover Pair .....	5-15
5-6	Warning Window .....	5-16
5-7	Warning Windows (Standalone Brick) .....	5-24
5-8	Warning Window (Failover Brick) .....	5-26
5-9	Multiple Brick Operations Window .....	5-27
5-10	Brick Editor (Cache Management Tab) .....	5-31
5-11	Brick Cache Management Editor .....	5-32
5-12	Brick Cache Management Editor .....	5-33
5-13	Confirmation Window .....	5-34
<b>6</b>	<b>Configuring VLANs on Alcatel-Lucent VPN Firewall Brick™ Security Appliances</b>	
6-1	Flat Switched Network (no VLANs) .....	6-2
6-2	Switched Network (with two VLANs) .....	6-3
6-3	Switched Network (with VLANs and Brick on trunk) .....	6-3
6-4	Brick Editor (VLAN View) .....	6-7
6-5	Brick Ports Editor .....	6-8
6-6	Brick Editor (Policy Assignment Tab) .....	6-12
6-7	Brick Policy Assignment Editor .....	6-13
6-8	Brick Editor (VLAN/IP Assignment Tab) .....	6-15
6-9	Brick/VLAN IP Assignment Editor .....	6-16
<b>7</b>	<b>Configuring Alcatel-Lucent VPN Firewall Brick™ Security Appliance Partitions</b>	
7-1	Brick Editor (Partition Tab) .....	7-4
7-2	Brick VLAN Partition Editor .....	7-5
7-3	Brick Static Route Editor .....	7-8
<b>8</b>	<b>Creating SMS Groups and Administrators</b>	
8-1	Group Editor Window .....	8-5
8-2	GroupEditor Window .....	8-7



8-3	Administration Editor (Administrator Tab) .....	8-11
8-4	Administrator Editor (Authentication Tab) .....	8-13
8-5	Administration Editor (Authentication Service) .....	8-15
8-6	Group Administrator Privileges Window .....	8-18
8-7	Administrator Editor (Edit Mode) .....	8-21
8-8	Contents Panel (Administrators folder) .....	8-23
8-9	SMS Messenger .....	8-25
8-10	Records of Sent Message .....	8-27
8-11	Messenger Envelope .....	8-27
8-12	SMS Messenger (Message Sent) .....	8-28
<b>9</b>	<b>Compute Servers</b>	
9-1	SMS Cluster Arrangement of Computer Servers and Redundant SMS Pair .....	9-3
9-2	LSMS/Computer Servers Editor Window .....	9-5
9-3	Host Group Editor window (ComputeServers Host Group) .....	9-6
<b>10</b>	<b>Remote Administration</b>	
10-1	How to Install the Remote Navigator Window ( <i>Windows</i> <sup>®</sup> Version) .....	10-5
10-2	How to Install the Remote Navigator ( <i>Solaris</i> <sup>®</sup> Version) .....	10-8
10-3	LSMS Remote Navigator Login Window .....	10-16
<b>11</b>	<b>Using the Configuration Assistant</b>	
11-1	Configuration Assistant Window .....	11-4
11-2	Configuration Parameters Window .....	11-8
11-3	Edit Alarms Servers .....	11-9
11-4	Edit Audit Trail Configuration Window .....	11-12
11-5	Edit Direct Paging Configuration Window .....	11-13
11-6	Edit FIPS Configuration Window .....	11-15
11-7	Edit GUI/Status Monitor Timeouts Window .....	11-17

11-8	Edit Log File Configuration Window .....	11-19
11-9	Edit Log Transfer Configuration Window .....	11-22
11-10	Same FTP Server .....	11-24
11-11	Edit Login Banner Configuration Window (With Default Banner Text) .....	11-25
11-12	Sample Login Banner Window .....	11-26
11-13	Edit LSMS Web Parameters Window .....	11-27
11-14	Edit Reports Configuration Window .....	11-29
11-15	Edit SNMP Configuration Window .....	11-32
11-16	Edit Software Download Configuration Window .....	11-34
11-17	Edit Strong Passwords Window .....	11-41
11-18	Edit TL1 Alarms Configuration Window .....	11-42
11-19	Edit Tunable Parameters Window .....	11-44
11-20	Edit User Authentication Configuration Window .....	11-46
<b>13</b>	<b>Task Scheduler</b>	
13-1	Schedule Editor Window (Initial View) .....	13-3
13-2	Schedule Editor Window (Initial View) .....	13-4
13-3	Edit Command Schedule Window .....	13-5
13-4	New Command Schedule .....	13-6
<b>14</b>	<b>Using the Status Monitor</b>	
14-1	Status Window Toolbar .....	14-4
14-2	Status Overview Window .....	14-7
14-3	Configure Status Overview Window .....	14-9
14-4	Select Summary Time & Date window .....	14-11
14-5	Administrators Status Window .....	14-14
14-6	SMS/CS and Bricks Status Window (with Display Bricks option selected) .....	14-17
14-7	Brick Lists (All Bricks) .....	14-21

List of figures

14-8	Brick Editor (Brick Tab, showing user-defined configuration fields)	14-23
14-9	All Bricks Status Window (showing user-defined configuration fields)	14-24
14-10	Single Brick Status Window	14-25
14-11	Select Summary Time and Date Window	14-28
14-12	Single Brick Ports Window	14-29
14-13	Single Brick Ports Window (Brick Failover Pair)	14-30
14-14	Single Brick Zones Window	14-32
14-15	Select Summary Time and Date Window (Brick Bandwidth Statistics)	14-34
14-16	Console Alarms Window	14-36
<b>15</b>	<b>Simple Network Management Protocol (SNMP)</b>	
15-1	Brick Editor (Options Tab)	15-11
15-2	Brick Options Tab - SNMP Brick Agent Option Fields Activated	15-12
<b>D</b>	<b>Support for Non-IP Protocols</b>	
D-1	Apply Brick Window	D-5



# About this information product

## Purpose

The purpose of this manual is to explain how to use Release 9.4 of the Alcatel-Lucent Security Management Server (SMS) application.

## Reason for reissue

Updated for R9.4 features.

## Who Should Read this Book?

The *SMS Administration Guide* is intended to be read by Network administrators who will be using the SMS application to:

- Configure and install one or more Alcatel-Lucent *VPN Firewall Brick™* Security Appliances so that they are communicating with the SMS
- Configure Compute Servers (CSs) as an alternative means of polling and collecting log information from Brick devices.

In the terminology used by the SMS, these administrators are referred to as *SMS Administrators* and *Group Administrators*, depending on the privileges they have been given when their profiles were created.

## What is in this Book

The *SMS Administration Guide* explains how to configure and activate a Brick device and its associated interfaces. It describes the various functions of a Brick device—firewall, tunnel endpoint, VLAN switch — and explains how to configure the Brick device once its role has been identified.

This document also explains how to configure CSs as an alternative means of collecting log information from Brick devices managed by the SMS.

The *SMS Administration Guide* covers the following topics:

Chapter	Purpose
<p><a href="#">Chapter 1, “Getting Started”</a></p>	<p>This chapter explains how to log on and off the SMS. It describes the Navigator window, which appears immediately after you log in, and explains how to use this window to access the system functions.</p> <p>It also explains how to organize the groups, folders, and other objects that appear in the Navigator window.</p>
<p><a href="#">Chapter 2, “SMS Redundancy”</a></p>	<p>This chapter explains the concept of SMS Redundancy and describes how to configure Primary and Secondary SMSs in your operating environment.</p>
<p><a href="#">Chapter 3, “Configuring and Activating an Alcatel-Lucent VPN Firewall Brick™ Security Appliance”</a></p>	<p>This chapter explains how to configure and activate a Brick device. It describes the questions you should ask before beginning the configuration, and it explains how to configure a Brick device from a Primary SMS and a redundant SMS pair.</p> <p>It also explains how to activate a Brick device from the SMS host and from a remote host.</p>
<p><a href="#">Chapter 4, “Configuring Alcatel-Lucent VPN Firewall Brick™ Security Appliance Ports”</a></p>	<p>This chapter explains how to configure the ports on a Brick device and assign security policies to the ports. It also explains how to create static routes and configure the intelligent cache management feature.</p>
<p><a href="#">Chapter 5, “Maintaining an Alcatel-Lucent VPN Firewall Brick™ Security Appliance Configuration”</a></p>	<p>This chapter explains how to modify and delete a Brick device configuration. It is also explains how to move Brick devices, and how to reboot a Brick device and refresh its MAC table from the SMS.</p> <p>Finally, it describes how to download a software upgrade to the Brick device from the SMS.</p>
<p><a href="#">Chapter 6, “Configuring VLANs on Alcatel-Lucent VPN Firewall Brick™ Security Appliances”</a></p>	<p>This chapter explains how to configure a Brick device to recognize, forward and filter VLAN-tagged frames.</p> <p>The Brick device now recognizes IEEE 802.1Q VLAN tagged Ethernet frames when received from the network, and can generate VLAN tagged frames.</p>

Chapter	Purpose
Chapter 7, “Configuring Alcatel-Lucent VPN Firewall Brick™ Security Appliance Partitions”	This chapter explains the concept of a Brick device partition, how to configure a partition, and how to use static routes with Brick device partitions.
Chapter 8, “Creating SMS Groups and Administrators”	<p>This chapter discusses the concept of a group, describes the <i>system</i> group (a special group provided with the SMS), and explains how to create new groups.</p> <p>The chapter also describes the two types of Administrators (SMS Administrators and Group Administrators), and how to create new Administrator accounts. It explains how to authenticate administrators with RADIUS and SecurID.</p>
Chapter 9, “Compute Servers”	This chapter explains the concept of Compute Servers as an alternative means of collecting Brick device log information and explains how to configure a Compute Server as a logging device in the SMS.
Chapter 10, “Remote Administration”	<p>This chapter explains how to administer the SMS from a remote host. It explains how to install the SMS Remote Navigator on the host (<i>Windows</i>®, <i>Vista</i>™, and <i>Solaris</i>®), and how to log into the SMS using the Remote Navigator application.</p> <p>It also explains how to create the host group and security rules needed to allow the remote session to reach the SMS through a Brick device.</p>
Chapter 11, “Using the Configuration Assistant”	This chapter explains how to use the Configuration Assistant to set a number of parameters that affect the SMS operation and performance.
Chapter 12, “Backing Up and Restoring Data”	<p>This chapter explains how to backup the database and if necessary, restore this database.</p> <p>Configuration data that is managed by the SMS, including policy, device, and VPN tunnel data, and stored in the database should be backed up on a regular basis.</p>
Chapter 13, “Task Scheduler”	This chapter explains how to use the SMS Task Scheduler to schedule tasks such as database backups or log file transfers.

Chapter	Purpose
<a href="#">Chapter 14, “Using the Status Monitor”</a>	This chapter explains how to use the Status Monitor.  The Status Monitor is a tool for monitoring the status of all Brick devices, VPN tunnels, and SMSs. It also shows all SMS and Group Administrators currently logged into your resident SMS and all console alarm messages.

The *SMS Administration Guide* also contains five appendices that provide additional information about the system.

### What is Not in this Book

If you are looking for information on any of the following topics, you should refer to the *SMS Policy Guide*:

- How to set up and manage security policies on one or more Brick devices.
- How to create components of a security policy, such as host groups, service groups and dependency masks.
- How to set up network address translation (NAT).
- How to set up Brick zone rulesets to route incoming and outgoing HTTP, SMTP and FTP sessions to a router for content filtering
- How to set up user authentication, using either a database residing on the SMS, a RADIUS or SecurID server, or X.509 digital certificates.
- How to obtain and install X.509 digital certificates.
- How to set up LAN-LAN tunnels between Brick devices.
- How to configure a Brick device to serve as the endpoint of a client tunnel.

These and other topics are covered in the *SMS Policy Guide*. Since these topics pertain primarily to the set up and administration of the software, we recommend that you read this *SMS Administration Guide* — and perform all required hardware tasks — before referencing the *SMS Policy Guide*.

### Supported Brick devices

The following available Brick models are supported by the current SMS release:

- Alcatel-Lucent *VPN Firewall Brick*® Model 50 Security Appliance
- Alcatel-Lucent *VPN Firewall Brick*® Model 150 Security Appliance
- Alcatel-Lucent *VPN Firewall Brick*® Model 350 Security Appliance
- Alcatel-Lucent *VPN Firewall Brick*® Model 1100/1100A Security Appliance



- Alcatel-Lucent VPN Firewall Brick® Model 700 Security Appliance
- Alcatel-Lucent VPN Firewall Brick® Model 1200 Standard and HS VPN Security Appliances

**Important!** *Note: only later Model 20 Brick devices are supported with this release. Model 20 Bricks that have 6-8 MB of RAM and 8 MB of flash are not supported with this release.*

Some of the above Brick device models require a specific patch of the current SMS release in order to be fully supported. For details about the SMS patch release required for a specific Brick device model, refer to the *User's Guide* for the Brick device model or contact your Alcatel-Lucent customer support team representative for more information.

### Where to Find Technical Support

Technical assistance and additional information can be acquired by telephone or e-mail. If you require technical assistance, first collect information that technical support staff can use to diagnose the problem. This includes:

- Software version of the SMS.
- Model number and serial number of the Brick device.
- The SMS server platform operating system (*Microsoft®MicrosoftWindows®, Microsoft® Vista®, Sun Microsystems® Solaris®, or Linux*).
- Description of problem.
- Layout of your network. For example, is the Brick device connected to a device such as a hub or router? Is the Brick device operating as a bridge or is it using static routes? What is connected to the Brick device ports? What is the IP address range and VBA for each zone? What is the security policy for each port?

After gathering the information, contact Alcatel-Lucent Security Customer Care at 1-866-582-3688.

### How to comment

To comment on this information product, go to the [Online Comment Form](http://www.lucent-info.com/comments/enus/) (<http://www.lucent-info.com/comments/enus/>) or e-mail your comments to the Comments Hotline ([comments@alcatel-lucent.com](mailto:comments@alcatel-lucent.com)).



# 1 Getting Started

## Overview

---

### Purpose

This chapter explains how to log on and off the SMS server or a Compute Server using the SMS Navigator and SMS Remote Navigator applications. These are utilities that have been provided with the SMS for you to use to access the system.

This chapter also describes the Navigator window, which appears immediately after you log in. It explains how to use this window, and how to organize the groups, folders, and other objects that appear in the Navigator window. Finally, the chapter suggests where to turn to begin setting up your environment.

### Contents

To Log On and Off the SMS Server or Compute Server	1-2
To Use the Navigator Window	1-8
To Operate the SMS	1-13
Organizing the SMS Interface	1-20
Using the Find Name Tool	1-23
Using the Find IP Address Tool	1-29
Applying Changes	1-33
Concurrency Control	1-36
To Enable Concurrency Control	1-39
To Force a Logout of an Administrator	1-41
Basic Configuration Requirements	1-43



## To Log On and Off the SMS Server or Compute Server

---

### When to use

The computer running the SMS application is called the SMS *host*. You can log into the SMS directly from the SMS host, or you can log into the SMS remotely from another host (Windows-based PC or laptop, or a Sun workstation) that has a LAN or Internet connection to the SMS host.

To facilitate the collection of log data from one or more Alcatel-Lucent *VPN Firewall Brick™* Security Appliances being managed by the SMS host, a set of up to ten Compute Servers can be configured and associated with a Primary/Secondary SMS pair through the SMS GUI. For additional information about Compute Servers, refer to [Chapter 9, “Compute Servers”](#). Once it is added, you can log into a Compute Server (CS) directly or remotely from another host, using the SMS Remote Navigator, in the same way that you would log into the SMS host.

If you are logging in remotely, your login is secure because the ID and password you enter — as well as the entire remote administrative session — is protected by Triple DES encryption.

**Important!** To allow remote Administrator sessions (including your own) through the Brick, you first have to create two rules in the Administrative Zone or the NOC Gateway Zone, depending on how the Brick protecting the SMS host is configured.

Refer to the *Remote Administration* chapter for instructions on creating the two rules required for remote access.

It is possible to install the SMS Remote Navigator on the SMS host so that you are running both the SMS Navigator and the SMS Remote Navigator on the same machine. The only reason to do this is if you intend to use the SMS host to log into another SMS or Compute Server remotely.

If you are logging into the SMS application on a *Microsoft® Vista™* server, and if *Vista™* User Account Control (UAC) is enabled (which is the default), and you run the SMS application using a *Vista™* standard user account, you may be prompted via screens for consent or credentials (such as a valid local administrator password) the first time that the SMS Navigator or Remote Navigator is brought up on the screen. *Vista™* UAC is designed to prevent unauthorized access of your computer by users or malicious software programs, with changes in the *Vista™* operating system that affect standard user and administrator account permissions to perform certain activities or run applications.

If this is the case, respond to the UAC screen prompt by allowing the SMS application to be run or by entering a valid administrator password, based on what is requested.

If you encounter prompting for permission to run the SMS application each time, it may be advisable to disable *Vista*<sup>™</sup> UAC, depending on the security requirements of your local operational environment.

### To log into an SMS or Compute Server from the SMS host

The SMS Navigator is installed automatically on the SMS host when the SMS application is installed. To log into an SMS or Compute Server from the SMS host using the SMS Navigator, follow the steps below:

- 1 If the SMS is running on *Microsoft®Windows®* or *Vista®*, click the **Start** menu and select:

**Programs ► Alcatel-Lucent Security Management Server ► SMS Navigator**

If the SMS is running on *Solaris®*, bring up the desktop menu by right-clicking on the display background and then click on LSMS Navigator or go to the installation root directory (*/opt/isms/lmf* if you used the defaults during installation) and enter:

```
./StartLSMSNavigator
```

from the command line.

If the SMS is running on Linux, click the **Applications** menu at the top of the window task bar and select **Alcatel-Lucent Security Management Server ► SMS Navigator** or, at the command line, go to the installation root directory (*/opt/isms/lmf* if you used the defaults during installation) and enter:

```
./StartLSMSNavigator
```

**Result** The Navigator Login window is displayed (Figure 1-1, “Navigator Login Window” (p. 1-4)).

**Figure 1-1 Navigator Login Window**



- 
- 2 Enter your **Admin ID** and **Password**. The Admin ID and password are the ones that were created during SMS installation, or those given to you by your SMS Administrator.

If you want to access the Status Monitor of the SMS or Compute Server, you can check **Status Monitor Only Login**. However, if you later decide you want to access the complete SMS or Compute Server, you will have to exit the Status Monitor and log into the SMS or Compute Server again. (Refer to [Chapter 14, “Using the Status Monitor”](#) for a discussion of the Status Monitor.)

- 
- 3 Click **Connect** or press **[Enter]**. A progress bar will appear and track the progress of the login. When you have successfully logged in, the Navigator window is displayed.

END OF STEPS

---

### To Log into an SMS or Compute Server from a Remote Host

If you intend to log into the SMS or a Compute Server remotely from another host — for example, a desktop at home or a laptop when traveling — you have to install the SMS Remote Navigator on that host. Instructions for installing the SMS Remote Navigator are found in [Chapter 10, “Remote Administration”](#).

To log in from a remote host using the SMS Remote Navigator, follow the steps below:

- 1 If the remote host is running *Microsoft® Windows®* or *Vista®*, click the **Start** menu and select:

**Programs ► Alcatel-Lucent Security Management Server ► SMS Remote Navigator 9.4**

If the remote host is running *Solaris®*, go to the installation root directory (*/opt/isms/lmf* if you used the defaults during installation) and enter:

```
./StartLSMSNavigator [<valid URL>]
```

from the command line. The [<valid URL>] is optional. If the URL of the SMS is provided on the command line, it pre-populates the **LSMS/LSCS URL** field on the SMS Remote Navigator Login window.

If the SMS is running on a Linux host, you can only log into it remotely from another host that is running *Windows®*, *Vista®*, or *Solaris®* and has the Remote Navigator software installed.

**Result** The SMS Remote Navigator window is displayed ([Figure 1-2, “SMS Remote Navigator Login Window”](#) (p. 1-5)).

**Figure 1-2 SMS Remote Navigator Login Window**



- 
- 2 Enter your **Admin ID** and **Password**. The Admin ID and password are the ones that were created during SMS installation, or those given to you by another administrator.

If you want to access the Status Monitor without logging into the rest of the SMS, you can check **Status Monitor Only Login**. This is useful if:

- You have a special monitoring room with large screens, and you want to display the graphs to monitor the health of the system, or
  - If you want to provide someone with the ability to monitor the system, but you do not want this person to be able to view or change the system's configuration.
- 

- 3 Enter the URL of the SMS or Compute Server. The URL is either:

`http://<IP_address>:<port_number>/LSMS`

— or —

`https://<IP_address>:<port_number>/LSMS`

where *<IP\_address>* is the IP address of the SMS or Compute Server and *<port\_number>* is the port the web server is listening on. Ports 80 and 443 are the standard ports for HTTP and HTTPS, respectively. The port your web server is using was assigned during installation; if another port was entered, use it instead.

Each URL you enter will be placed in the drop-down list in the URL field, so that each time you enter this URL after the initial entry, you can simply select it from the drop-down list instead of typing it in. You can store multiple URLs in this list in the event that you need to log into more than one SMS or Compute Server remotely.

---

- 4 Click **Connect**. When you have successfully logged in, the Navigator window will appear (refer to the section [“To Use the Navigator Window”](#) (p. 1-8)).

END OF STEPS

---

### Login to a “Locked” Navigator

Once you login to the SMS Navigator or the SMS Remote Navigator, your session will remain active until:

- You explicitly log out by clicking on **File ► Exit** from the menu bar  
-OR -
- The SMS Services are manually stopped.



However, after a period of inactivity, the SMS Navigator will automatically lock itself. The Idle Time interval is set through the SMS Configuration Assistant. For more information on this parameter, please refer to [Chapter 11, “Using the Configuration Assistant”](#).

If you attempt to use a locked SMS or CS Navigator, a window similar to the one shown in [Figure 1-3, “SMS Navigator Locked Window”](#) (p. 1-7) (depending on whether you are locked out of an SMS or CS) is displayed:

**Figure 1-3 SMS Navigator Locked Window**



Click the **Unlock LSMS Navigator** button. A password window is displayed. Enter the appropriate password for the administrator whose session is locked.

To log in as a different administrator, click the **Logout** button and initiate a new session.

□

## To Use the Navigator Window

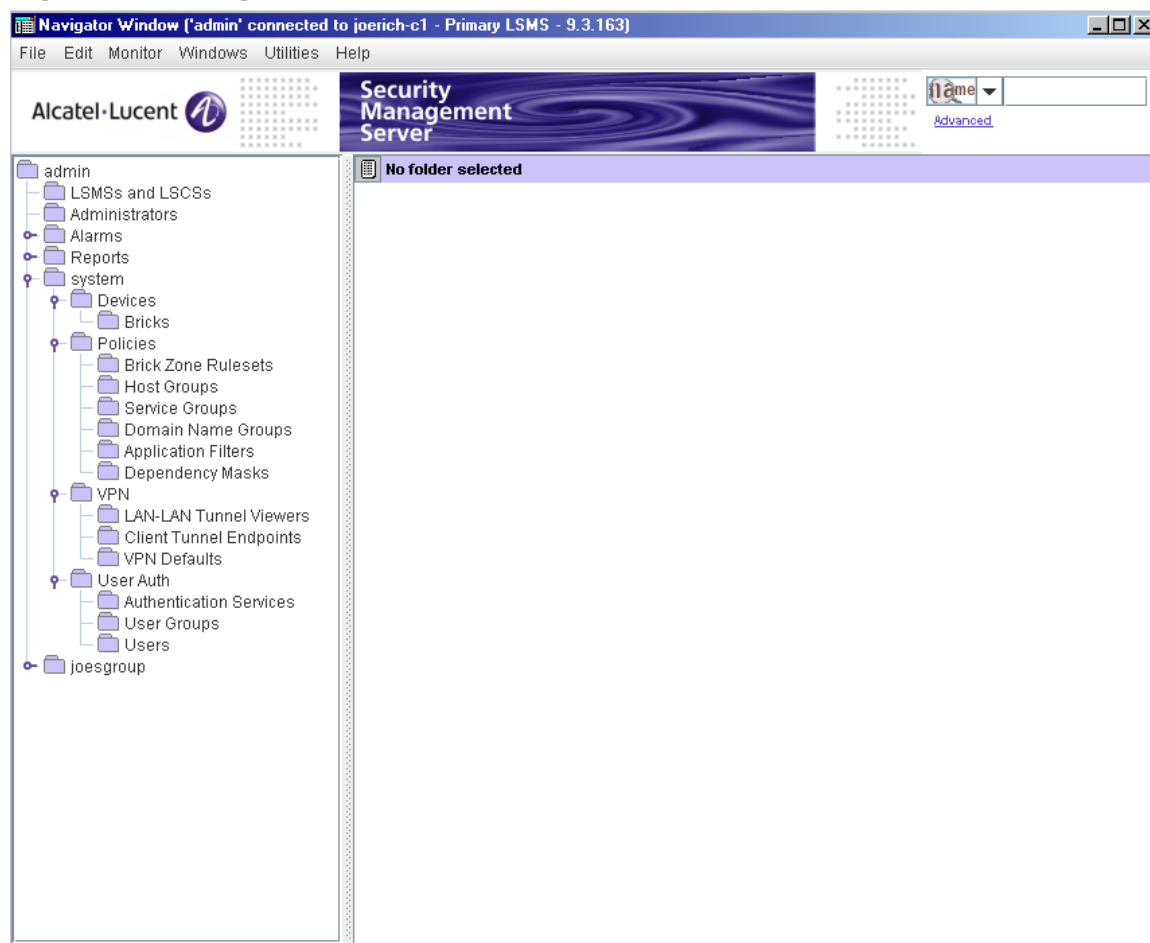
---

### When to use

The window that appears immediately after login is called the **Navigator window**. This window is your doorway to the SMS. Starting from this window, you will be able to centrally manage the Bricks in your network.

Figure 1-4, “Navigator Window” (p. 1-8) shows the Navigator window. The window work area is divided into two panels — a Folders panel on the left, and a Contents panel on the right.

**Figure 1-4 Navigator Window**



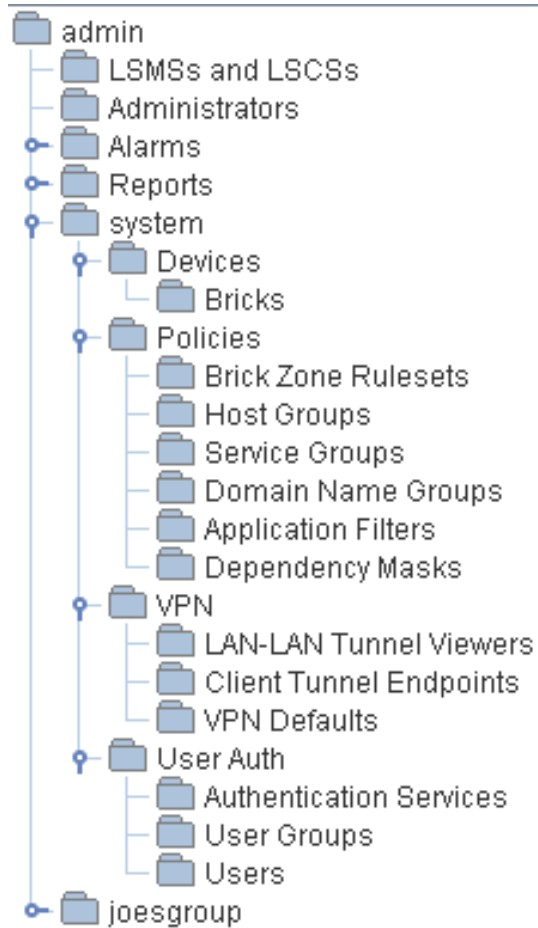
### Folders Panel

The Folders panel consists of a set of folders and subfolders organized into a hierarchical tree structure. Inside these folders, you will find the devices you are managing, the security policies and tunnel endpoints you have set up, and a variety of other system features and components.


**Important!** SMS Administrators see all folders. The folders that Group Administrators see depends on their privileges. For example, Group Administrators with full policy privileges but no device privileges will see all policy folders, but no device folders.

This is explained in detail in [Chapter 8, “Creating SMS Groups and Administrators”](#).

[Figure 1-5, “Folders Panel” \(p. 1-10\)](#) shows a close-up of a Folders panel.

**Figure 1-5 Folders Panel**



Note that the folder at the very top of the tree structure is the Admin ID of the Administrator currently logged in. Each Administrator always sees his or her own Admin ID.

One level down on the tree structure are the Administrators, Alarms, Reports, and System folders. Alarms and reports are not part of any group, but are specific to each Administrator. The Alarms and Reports folders have subfolders under them. You can tell by the  to their left.

The System folder is a group. This group is provided with the SMS application and automatically opens every time you log onto the SMS. If you create additional groups, these will appear below the System group at the same level of the hierarchy. The new groups will automatically have the same subfolders that are originally found in the System group (shown in [Figure 1-5, “Folders Panel”](#) (p. 1-10)). Groups you create will not expand automatically when you log on.

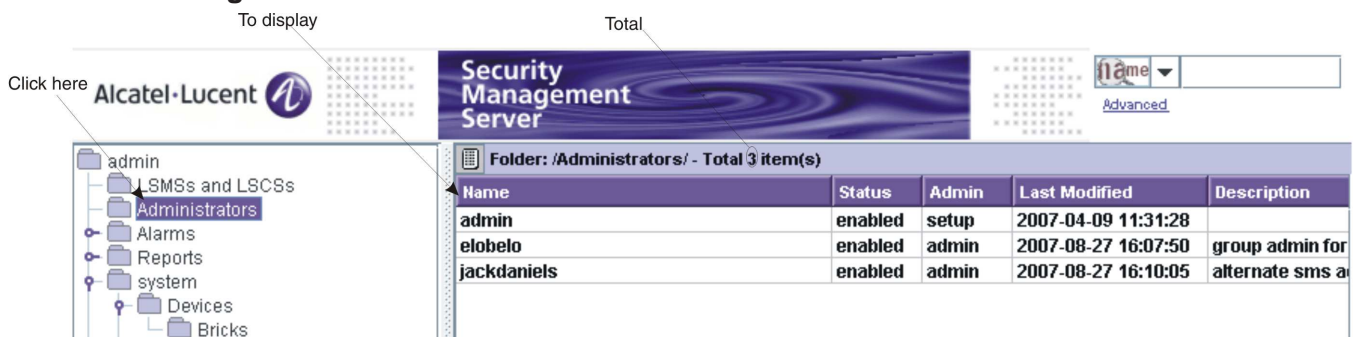
To open a folder that has subfolders, double-click the folder, or click  once.

## Contents Panel

The Contents panel displays the contents of the lowest level of folders. You can tell that you have reached the lowest level when a folder no longer has  or has a  to its left.

To display the contents of a folder, click the folder once. [Figure 1-6, “Contents Panel”](#) (p. 1-11) shows the contents of an Administrators folder. You will note that there are three entries in the Contents panel, and the total is always shown above the entries. The entries are sometimes referred to as *leaves*.

**Figure 1-6 Contents Panel**



## Find Name and Find IP Address tools

The Find Name and Find IP Address tools are available via a drop-down menu at the top right hand corner of the Navigator.

The Find Name tool allows you to perform a search for entities in the SMS database that match all or part of the entity name entered in the Search field.

The Find IP Address tool allows you to perform a search for entities in the SMS database that match the IP address entered in the Search field. The search results are displayed in the Contents panel of the Navigator.

For details about using the Find Name tool, refer to the section “ [Using the Find Name Tool](#)” (p. 1-23) in [Chapter 1, “Getting Started”](#).

For details about using the Find IP Address tool, refer to the section “[Using the Find IP Address Tool](#)” (p. 1-29) in [Chapter 1, “Getting Started”](#).



## To Operate the SMS

---

### Overview

To perform actions using the SMS, you have to manipulate the folders and their contents. There are several ways to do this:

- By using the menu bar at the top of each window.
- By using the mouse to select folders and leaves, and display a pop-up menu of actions.
- By using the buttons at the bottom of certain screens.

The method you choose to perform any given task does not matter. This redundancy has been deliberately built into the system to make it possible for you to perform any task from any screen in the manner that is easiest for you.

### Menu Bar

A menu bar appears across the top left of every major SMS screen. This allows you to perform almost all SMS functions from anywhere in the system, without the need to exit the current window and change functions.

The menu bar contains the following menus and commands:

- File
  - Sub-menu items:
    - New Group - allows you to create, save, and apply a new group
    - New - allows you to create, save, and apply any of the following new entries:
      - Administrator
      - Alarm (Triggers, Actions, TL1 Alarms (if enabled))
      - Report Filter (Closed Session Details, Sessions Logged, Administrative Events, VPN Events, Alarms Logged, User Auth, Audit Trail, Rule Statistics)
      - Device (Brick)
      - Policy (Brick Zone Ruleset, Host Group, Service Group, Domain Name Group, Application Filter, Dependency Mask)
      - VPN (LAN-LAN Tunnel, Client Tunnel Endpoint)
      - User Auth (Auth Service, User Group, User)
      - Group
    - Lock Navigator - locks the Navigator Window with password protection
    - Exit
  - Edit - provides access to a set of editing functions.
    - Sub-menu items:
      - Edit - allows you to edit the following entries:
        - Administrator
        - Alarm (Trigger, Action, TL1 Alarm)

- Report Filter (Closed Session Details, Sessions Logged, Administrative Events, VPN Events, Alarms Logged, User Auth, Audit Trail, Rule Statistics)
  - Device (Brick)
  - Policy (Brick Zone Ruleset, Host Group, Service Group, Domain Name Group, Application Filter, Dependency Mask)
  - VPN (VPN Defaults, LAN-LAN Tunnel, Client Tunnel Endpoint)
  - User Auth (Auth Service, User Group, User)
  - Group
- Move - allows you to move any of the following entries:
- Device (Brick)
  - Policy (Brick Zone Ruleset,, Host Group, Service Group, Domain Name Group, Application Filter, Dependency Mask)
  - User Auth (Auth Service, User Group, User)
- Copy - allows you to copy any of the following entries:
- Policy (Brick Zone Ruleset, Host Group, Service Group, Domain Name Group, Application Filter, Dependency Mask)
  - User Auth (Auth Service, User Group, User)
- Delete - allows you to delete any of the following entries:
- Administrator
  - Alarm (Trigger, Action, TL1 Alarm)
  - Report Filter (Closed Session Details, Sessions Logged, Administrative Events, VPN Events, Alarms Logged, User Auth)
  - Device (Brick)
  - Policy (Brick Zone Ruleset, Host Group, Service Group, Domain Name Group, Application Filter, Dependency Mask)
  - VPN (Client Tunnel Endpoint, LAN-LAN Tunnels)
  - User Auth (Auth Service, User Group, User)
  - Group
- Find IP Address - a tool that allows you to find all the instances in an SMS configuration where an IP address is used. It allows you to match a single address, a range of addresses, a subnet mask, a wildcard (\*), or one of the special keywords available in the pulldown. A match is defined as any overlap between the IP address input by the admin and any IP address found in the system. Since \* will match anything, there is an option, set by default, to ignore these matches so as to avoid having them clutter the output. Another option constrains matches to literal matches - no overlap matching is done when this option is set. Note that setting this option makes the Ignore Wildcard Matches option meaningless.
- Matches are retrieved and displayed in a tabular form in a new window that floats in the inner area. A series of different searches can be performed and displayed in separate windows while in the tool.



- Monitor - displays the SMS Status Monitor and all console alarms that have been configured to display an on-screen message. The Status Monitor provides the following views of your operation:

Sub-menu items:

- Status Overview - shows status of all Bricks, number of authenticated users, number of LAN-LAN tunnel endpoints, Brick packets, Brick sessions, Brick sessions by protocol type.
- Administrators - shows total number of administrators logged into an SMS or Compute Server.
- SMS/CS and Bricks - shows status of each SMS and Compute Server (CS) and the number of Bricks assigned to each server.
- Brick Status - shows Brick status by category (All Bricks assigned to, all Bricks, monitored Bricks, lost Bricks, Bricks up, Bricks not up, Bricks by Parent Folder, Single Brick status, single Brick ports, single Brick bandwidth statistics).

If you are an SMS Administrator, the Status Monitor shows the name of every SMS and Group Administrator currently logged in and the status of all configured Bricks.

If you are a Group Administrator, the Status Monitor shows your name and the status of all Bricks over which you have view or full privilege. You will also see the names of all SMS Administrators currently logged in, plus any other Group Administrators who have privileges for your group(s).

Sub-menu items:

- Console Alarms - accesses screen listing all console alarms with buttons to clear individual alarms or clear all alarms.

- Windows

Sub-menu items:

- Close All Open Windows - allows you to close all open window (except Navigator Window)
- Navigator Windows - lists all open windows and provides easy access to windows hidden behind other windows.

- Utilities

Provides access to the following system tools:

- Certificate Manager
- Configuration Assistant
- New Feature Setup
- Restart SMS Services
- SMS Service Status
- SMS Log Viewer

- Edit SMS Parameters
- View SMS Parameters
- Help - displays the following online help options:  
Sub-menu items:
  - Online Product Manuals
  - Error Codes
  - Subnet Mask Reference
  - About...The Brick Editor screen has the following additional menu item and commands:
- Brick Utilities (Software Download, Make Brick Boot Media, Open Brick Console, Initiate Failover, Reboot, Refresh MAC, Rehome To, View Brick Snapshot, Rule Statistics)

## Mouse Actions

You can use the right mouse button to perform most of the actions in the File and Edit menus, as well as many of the actions in the Utilities menu.

Right-click on a folder or subfolder in the Folders panel, and a menu will frequently pop up. If a menu does not pop up, no action can be taken on that particular folder, and you must look to a subfolder.

For example, if you right-click the System folder, a menu will pop-up and allow you to create a new group, edit an existing group, apply a group, delete a group, allocate client tunnel endpoint licenses, create the NOE template set, or delete the NOE template set.

You can right-click in the Contents panel, or on an entry in the panel, to display a pop-up menu. You can also double-click an entry in the Contents panel, and if it is editable, it will appear in the appropriate editor to allow you to make any necessary changes.

You can also right-click in many of the other SMS windows (those that have a viewing panel similar to the Contents panel). The procedures that are explained throughout this manual generally follow the right-click approach because this approach usually involves the least amount of mouse navigation.

## Buttons







Certain SMS windows provide special buttons that duplicate many of the menu and mouse functions. These include editing buttons, which appear on many windows and allow you to select an entry and perform an editing operation on it.

In addition, the Brick Editor Policy Assignment tab provides special buttons that you can use to view or terminate existing tunnels, or configure new tunnels.





The buttons always appear unlabeled at the bottom of the window. To display a button's label, the button must be active. If it is not active, you have to select an entry from above to activate it. Once it is active, position the cursor on it to display its label.





The tables below show the editing and tunnel buttons, and explain what each one does.

**Table 1-1 Editing Buttons**


Button	Label	Purpose
	New	Creates a new entry.
	Duplicate	Duplicates the selected entry.
	Edit	Edits the selected entry.
	Delete	Deletes the selected entry.
	Up/Down	Moves the selected entry one row up or down with each click.
	Activate/ Deactivate	Activates and deactivates a rule in a Brick zone ruleset.

### *Tunnel Buttons*

Button	Label	Purpose
	Client VPN	Displays the Client Tunnel Endpoint Editor. This window lets you configure a Brick to serve as the endpoint of a client tunnel.
	LAN-LAN VPN	Displays the LAN-LAN Tunnel Editor. This window lets you configure both endpoints of a LAN-LAN tunnel.
	ClearTunnel Viewer	Removes all entries from the LAN-LAN tunnel viewer.
	View Folder Tunnels	Displays a Browse window that allows you to select a Brick folder. All tunnels using the devices in the folder will then be displayed in the LAN-LAN tunnel viewer.

Button	Label	Purpose
	View Device Tunnels	Displays a Browse window that allows you to select a specific Brick. All tunnels using that Brick will then be displayed in the LAN-LAN tunnel viewer.
	Terminate All Sessions	Terminates all VPN client sessions.
	Terminate Session	Terminate the selected VPN client session.
	Refresh Tunnels	Refreshes the status of all the tunnels in a LAN-LAN tunnel viewer.

In addition, a Policy Snapshot button  appears on the Brick Interface Editor. It allows you to select a port and display a summary of the security policy associated with that port.

An Import Services Button  appears on the Service Group Editor. It allows you to import services from other services groups into a service group you are creating.

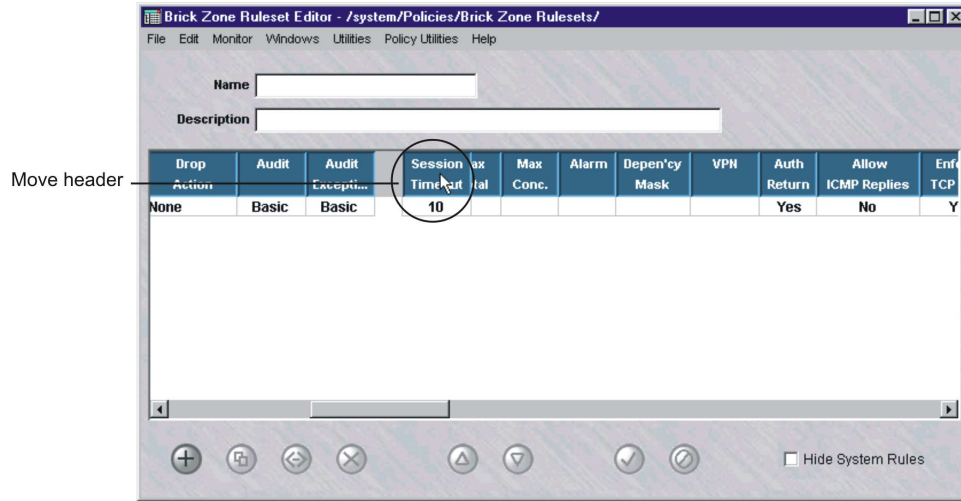
## Table Columns

Many SMS windows are formatted as tables, with columns and rows. In a number of cases, the tables contain more columns than can fit on one screen page, and so you must use the horizontal scrollbar at the bottom of the screen to display these columns.

For your convenience, you can rearrange the order of the columns to suit your needs. If a particular column contains information that is important, you may want to move it so that it displays when the screen first appears, without your having to resort to the scrollbar. You may also want to move certain columns next to each other because they provide information that is related.

To move a column in a table, simply position the mouse cursor on the column header, left-click the mouse to grab the column header, and then drag the column header left or right until it is positioned where you want. [Figure 1-7, “Move Column Header”](#) (p. 1-19) shows a column header being dragged to the right.

Figure 1-7 Move Column Header



## Organizing the SMS Interface

---

### Overview

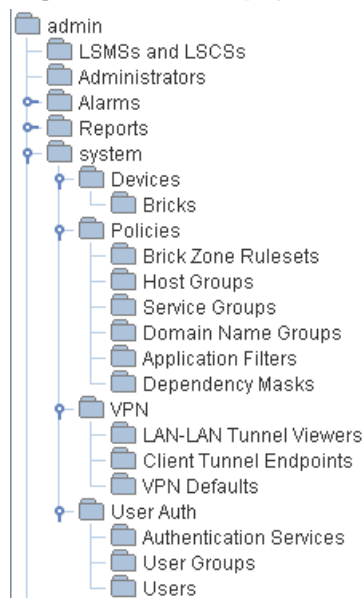
One of the first challenges facing an Administrator is to organize the various objects the SMS will be managing. These objects include devices, policies, tunnels and user authentication components.

These objects are what you see when you look at the screen — and by organizing them precisely and logically, you can make the system that much easier to use, and your network security that much easier to manage.

### Groups and Folders

The SMS provides two mechanisms for organizing objects — groups and folders. A group is a collection of objects that are managed together. These objects are represented on the screen as nested folders and subfolders. Every group contains the folders and subfolders shown in [Figure 1-8, “Group \(Folders and Subfolders\)”](#) (p. 1-20). However, you must have the appropriate privileges (either view or full) to see all folders.

**Figure 1-8 Group (Folders and Subfolders)**



In addition to the folders and subfolders shown above, it is possible to create additional levels of subfolders. You can create subfolders under the Bricks subfolder, and also under every Policies subfolder except Dependency Masks.

## system group

One group is provided with the SMS application. This group is called **system**, and whenever an SMS administrator logs in, it is automatically opened and displayed on screen.

The **system** group is different from any other groups you may create in two important ways:

- Rulesets from other groups can be applied to Bricks in the **system** group. This is to permit a Managed Service Provider to maintain control over all configured Bricks by managing them in the **system** group, while at the same time allowing each customer's Group Administrator to control the customer's security policy.

## Guidelines

The decision as to whether to place all your devices, policies, and tunnels in the **system** group, or whether to create additional groups, is at your discretion as an Administrator.

As a general rule, however, we recommend that only ISPs, and extremely large enterprises, create additional groups. ISPs in particular may find it useful to create groups for each customer, because each customer needs to be managed separately, and each customer may have a large internal organization.

It is important to keep in mind that — except for host groups, service groups and application filters, which can be given global status — objects such as devices and rulesets cannot be shared across groups. A tunnel can cross groups, but the host groups used in the tunnel definition cannot (unless they are made global). If, for example, you want to create a LAN-LAN tunnel from a device in one group to a device in another, you will not be able to take advantage of the ability of devices in the same group to easily share objects such as devices and rulesets.

Therefore, for most enterprises, we recommend using only the **system** group, and creating additional folders as needed. For example, if you are managing a large number of Bricks, you will probably want to create subfolders to organize the devices by location, department, and function. Similarly, if your security policies comprise many different rulesets, you can create subfolders to organize them logically.

An additional benefit of creating subfolders is that small subfolders generally display faster than large folders. This can be especially noticeable if you are logged onto the SMS remotely.

## Scenarios

The following are three possible scenarios for organizing the SMS interface:

1. *All components in the system group*

As indicated above, this is the preferred scenario for most organizations. If additional hierarchy is required — if, for example, you want to organize your Bricks by department — folders and even subfolders can be created.

2. *Devices in system group, policies in other groups*

In this scenario, all Brick devices are configured in the Bricks folder of the System group, but the Brick and router rulesets and other policy components are in the Policies folders of other groups.

This scenario is possible because Group Administrators with full policy privilege in their group can automatically apply policies and tunnels to Brick devices in the **system** group.

3. *All components in separate groups*

This scenario is primarily intended for ISPs, who need to keep the management of their individual customers' devices and policies completely separate.

Nonetheless, some ISPs may still prefer the second scenario, in which they maintain control over the Bricks — which are in the **system** group — while their customers maintain control over the policies and tunnels in their own groups.

## LSMSs and Compute Servers (LSCSs)

A folder in the Folder panel called **LSMSs and LSCSs** is accessed to view, edit, and create the secondary SMS(s) or Compute Server(s).





## Using the Find Name Tool

---

### Overview

The SMS application has a Find Name tool which allows you to search for any named entity in the SMS database by entering an entity name, partial name, or regular expression in a search field and display a list of entities that match the search criteria.

The Find Name tool can be used to perform a search for named entities such as:

- Brick devices
- SMSs and Compute Servers (CSs)
- Brick zone rulesets
- Host groups
- Service groups
- Domain name groups
- Application filters
- LAN-LAN tunnels
- Client tunnel endpoints
- Administrators and users
- Report filters
- Alarm triggers
- User Groups
- Authentication services

### Regular expressions in searches


The search field on the Find Entity tool window accepts an asterisk (\*) as a wildcard character to match zero or more characters of the name and all regular expression syntax supported by the *Java*<sup>TM</sup> language. For a description of *Java*<sup>TM</sup> regular expressions and their usage, refer to the *Java*<sup>TM</sup> URL <http://java.sun.com/j2se/1.4.2/docs/api/java/util/regex/Pattern.html>.

The meaning of the following special characters can be escaped and treated as literal characters in performing searches by preceding each character with a double-backslash (\\): [, ], {, }, ., \, +, ?, \*, ^, \$

**To perform a search using the Find Name tool**

Complete the following steps to perform a search using the Find Name tool:

.....

- 1 Click the down-arrow next to the  field icon to display a drop-down menu and choose **Find this name** (which is the default search on the Navigator), enter the name or partial name of the entity(ies) that you want to retrieve, and press the Enter key.

An asterisk (\*) can be used as a wildcard character to match zero or more characters of the entity name. Other regular expressions can be specified as search criteria (refer to the above section “Regular expressions in searches” (p. 1-23) ).

**Result** A list of entities that match the search criteria entered is displayed in tabular form in the Contents panel of the Navigator (Figure 1-9, “Find Name (Search Results Example)” (p. 1-25) provides a sample).

**Figure 1-9 Find Name (Search Results Example)**


The screenshot shows the Security Management Server interface. At the top left, it says "Security Management Server". On the right, there is a search bar with "smtp" entered and a dropdown menu showing "name". Below the search bar is a link for "Advanced". The main content area shows a search result summary: "Find: .\*smtp.\*, matching case - Total 4 item(s)". Below this is a table with the following data:

Name	Entity Type	Group	Subfolder
smtp	Service Group	system	
smtp	Service Group	joesgroup	
smtpDefault	Application Filter	system	
smtpDefault	Application Filter	joesgroup	

All searches that result in a partial match of the entity name are retrieved. For example, a search on abc matches 123abc4, except when anchor characters (^ or \$) are explicitly used.

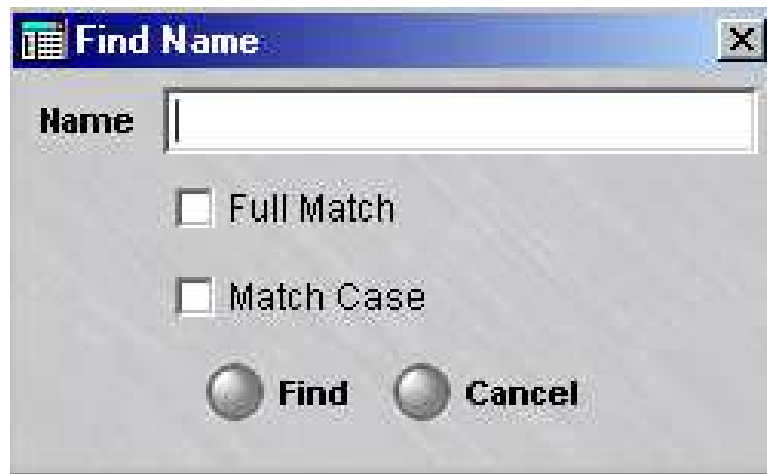
Once retrieved, you can right-click or on an entity to display a pop-up menu and select any of the maintenance functions available (such as **Edit**, **View**, **Copy**, **Move**, **Delete**, and so forth). You can also edit a retrieved entity by double-clicking on it to bring up the related Editor window.

To perform a new search, delete the existing entry in the Search field, enter new search criteria, and press the Enter key.

- 
- 2 To further refine your search criteria, click the [Advanced](#) hyperlink below the  search field icon at the top of the Navigator.

**Result** The Find Name dialog box is displayed (Figure 1-10, “Find Name Dialog Box” (p. 1-26)).

**Figure 1-10 Find Name Dialog Box**




Choose one or more of the following options in this search dialog box:

- **Name**— enter all or part of the entity name, using the same rules for entering a name and regular expressions already described in [Step 1](#). An entry in this field is required.
- **Full Match**— when this option is selected (checkbox is checked), the entity name(s) retrieved are only the ones that match the expression in the Name field from start to finish. Partial matches are not sufficient. The asterisk (\*) character has a different meaning here. Instead of matching 0 or more characters, it matches 0 or more of the character or regular expression that immediately precedes it. To match 0 or more characters here, you must use `.*`. For example, when this option is selected, an entry of `dyn.*1.*ers` will match `dynamicPppoe1DnsServers`, but an entry of `dyn.*1.*er` will not.
- **Match Case**—when this option is selected (checkbox is checked), the entity name(s) retrieved must match the case of the entity name entered exactly.

Selections made in the Advanced window are retained after the window is closed and in effect for searches done in the regular Find field at the top corner of the GUI, until the Advanced options are re-edited or you log out of the SMS.

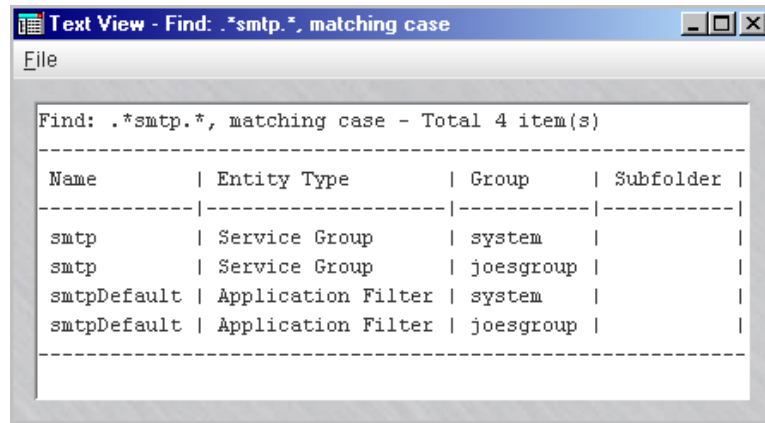
After specifying the search criteria, click the **Find** button.

**Result** A list of entities that match the entered search criteria is displayed in tabular form in the Contents panel of the Navigator ([Figure 1-9, “Find Name \(Search Results Example\)”](#) (p. 1-25) provides a sample).

- 
- 3 To view the contents of the current search retrieval in a text list, click the  icon in the left top corner of the list.

**Result** The list of retrieved entries is displayed as a text list in a separate window (Figure 1-11, “Text List of Name Search Retrieval Entries” (p. 1-28) shows an example).

**Figure 1-11 Text List of Name Search Retrieval Entries**



The contents of this window can be saved to a file by selecting **Save As** from the **File** menu, which brings up a Select File window to allow you to specify the name of the file and the folder in which it will be stored.

To close this window, click the Close () button at the top of the window.

END OF STEPS



## Using the Find IP Address Tool

---

### Overview


The **Find IP Address** tool allows you to search for any entities that use a specified IP address (Brick, host group, zone ruleset, tunnel endpoint, application filter, and so forth), and display the results of the search.

Optionally, you can also use this tool to find any nested entity, such as a host group, that contains the matching entity found, and, in turn, any entities where nested host group is being used.

### To perform a search using the Find IP Address tool

Complete the following steps to use the **Find IP Address** tool to find host groups and entities that contain an IP address.

---

- 1 Click the down-arrow next to the  field icon (located at the top right hand corner of the Navigator) to display a drop-down menu and choose **Find this IP address**.

**Result** An  icon is displayed next to the search field.

---

- 2 After specifying the search criteria, press the Enter key.

**Result** A list of entities that match the specified criteria is displayed in tabular form in a separate panel on the Navigator ([Figure 1-12, “Find IP Address Window \(Search Results\)”](#) (p. 1-30) provides a sample).

**Figure 1-12 Find IP Address Window (Search Results)**

Find: 135.112.248.28, ignoring wildcard matches, matching nested objects - Total 8 item(s)

Name	Entity Type	Group	SU...	Matches	Match Location
Salesgroup	Host Group	system		nycsales	nested in definition
joesbrick	Brick	system		nycsales	in hosts behind tunnel
lobrick	Brick	joesgr...		135.112.248.22/28	VLAN/IP assignment
nocgwzone	Brick Zone Ruleset	system		nycsales	in source in rule numb
nocgwzone	Brick Zone Ruleset	system		nycsales	in destination in rule n
nycsales	Host Group	system		135.112.248.28...	host addresses
nytola	Client Tunnel	system		nycsales	in hosts behind tunnel
udpmask	Dependency Mask	system		nycsales	in destination

Parent host group →

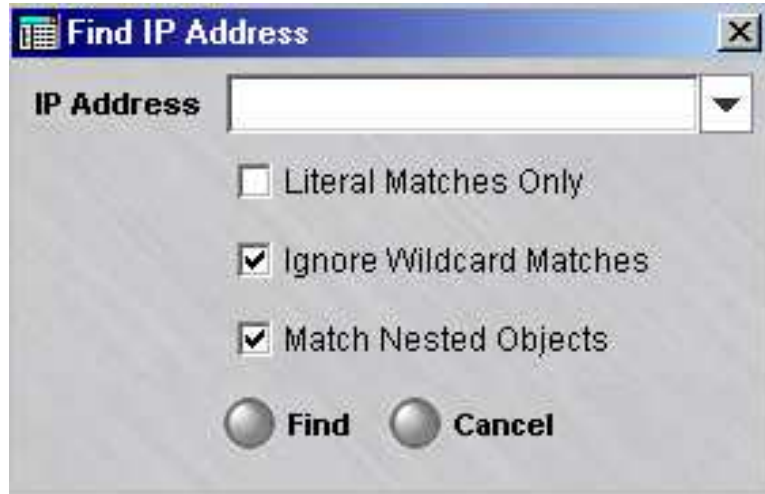
Host group nested in Salesgroup that contains IP address →

- To further refine your search criteria, click the [Advanced](#) hyperlink below the search field icon at the top of the Navigator.



**Result** The Find IP Address dialog box is displayed (Figure 1-13, “Find IP Address Dialog Box” (p. 1-31)).

**Figure 1-13 Find IP Address Dialog Box**



Choose one or more of the following options in this search dialog box:

- **IP Address**— enter the IP address of the host group or entity for which you want to perform a search. Alternatively, you can enter an asterisk (\*) as a wildcard character to find the IP addresses of any/all configured objects in the SMS database. This field is required.
- **Ignore Wildcard Searches**— when this option is selected (checkbox is checked), entities that contain an asterisk (\*) as a wildcard character in the address field in place of a specific IP address or address range are ignored in the search. This search option is checked, by default.
- **Match Nested Objects**— when this option is selected (checkbox is checked), the search results will include the entity(ies) that directly used the IP address, any host groups that nest these entities, and, in turn, all of the entities that use them (rulesets, tunnel endpoints, dependency masks, and so forth). This search option is checked, by default.

Selections made in the Advanced window are retained after the window is closed and in effect for searches done in the regular Find field at the top corner of the GUI, until the Advanced options are re-edited or you log out of the SMS.

After specifying the search criteria, click the **Find** button.

**Result** A list of entities that match the entered search criteria is displayed in tabular form in a separate panel on the Navigator ([Figure 1-12, “Find IP Address Window \(Search Results\)”](#) (p. 1-30) provides a sample).

Once an entity is retrieved and displayed, you can perform any of the available maintenance functions (edit, copy, move, and so forth) by right-clicking on the entity to display a pop-up menu and selecting the appropriate option.

.....  
E N D O F S T E P S



# Applying Changes

---

## Overview

Whenever an Administrator makes a change to information in the SMS that affects a configured device, that change has to be applied to the affected Brick. Although the changes may be saved in the SMS database, they will not take effect until they are applied to the device.

## When to Apply

As a general rule, you have to apply any updated information that has been downloaded to a Brick. For example, Brick zone rulesets are assigned to Brick ports; if you assign a new ruleset to a port, that change has to be applied to the Brick.

Similarly, if you add a new rule to a ruleset, or change an existing rule, that change has to be applied to every Brick to which the ruleset has been assigned.

If you create a new Brick zone ruleset, it is applied automatically when you apply the ruleset assignment.

Similarly, if you add a new user account or create a new user group, you do not have to perform an apply. However, when you create a rule that uses the new user group, then you have to apply the ruleset.

## What to Apply

There are five different types of apply actions that an Administrator with the appropriate privileges can perform. The type of apply you perform determines which devices are updated, and what information they are updated with.

When you perform the apply, the SMS always displays a window that indicates the Bricks that will be updated by the apply. The window does not allow you to select specific devices. If you only want to update some of the devices shown, you will have to cancel the apply and perform a different type of apply.

For example, as the table below indicates, a group apply updates every device in the group. If you only want to update one device in the group (such as single Brick), then you would have to perform a Brick apply instead. The table below explains:

Apply	Result
Group	Updates each Brick in the group with all device, policy, and tunnel changes that apply to that device.
Brick	Updates the selected Brick with all device, policy, and tunnel changes that apply to it.

<b>Apply</b>	<b>Result</b>
Brick Zone Ruleset	Applies the changes in the selected Brick zone ruleset to each Brick the ruleset has been assigned to.
LAN-LAN Tunnel	Applies the changes in the LAN-LAN tunnel configuration to the Brick that is functioning as the tunnel endpoint. Also applies the zone rulesets of the tunnel endpoints.
Client Tunnel	Applies the changes in the client tunnel configuration to the Brick that is functioning as the client tunnel endpoint. Also applies the zone rulesets of the tunnel endpoints.

## How to Apply

There are a number of ways to perform an apply. Regardless of which SMS window is displayed, you can perform any apply, except a LAN-LAN or client tunnel, from the Utilities menu. In addition, there are other ways to perform each of the apply actions. The table below explains:

<b>Apply</b>	<b>Do this...</b>
Group	Right-click the appropriate group folder and select <b>Apply</b> from the pop-up menu.
Brick	Right-click the Brick in the Navigator window and select <b>Apply</b> from the pop-up menu — or — Select <b>Save and Apply</b> from the File menu in the Brick Editor after making changes.
Brick Zone Ruleset	Right-click the ruleset in the Navigator window and select <b>Apply</b> from the pop-up menu — or — Select <b>Save and Apply</b> from the File menu in the Brick Zone Ruleset Editor after making changes.
LAN-LAN Tunnel	Select <b>Save and Apply</b> from the File menu in the LAN-LAN Tunnel Editor after making changes.
Client Tunnel	Select <b>Save and Apply</b> from the File menu in the Client Tunnel Endpoint Editor after making changes.

## Sarbanes Oxley (SOX) audit compliance

The SMS provides detailed auditing of configuration changes. This detailed auditing feature is always enabled. Any time that an administrator adds, deletes, or modifies an object, the event is recorded in the Audit Trail Log and a copy of the object is saved in an archive file for a specified number of days (which can be set via the Audit Trail Configuration Editor using the Configuration Assistant utility). For modification events, before and after images are available so that versions may be compared. A canned Audit Trail Report can be generated to view which objects have been changed over a specified time period, and who changed them.

For details about the Audit Trail parameter settings, refer to the Audit Trail section in [Chapter 11, “Using the Configuration Assistant”](#).

For details about the Audit Trail Log and Audit Trail Report, refer to the *SMS Reports, Alarms, and Logs Guide*.



# Concurrency Control

---

## Overview

The SMS application is a carrier grade centralized management system capable of managing a large number of objects (Bricks, zone rulesets, Host groups, tunnels, service groups, and so forth). The group-based model allows the creation of multiple management domains, where each group contains a set of resources. Multiple administrators may have access and the desire to modify the same object simultaneously. This raises the potential for problems caused by simultaneous changes to an object by multiple administrators, or editing of an outdated instance within an object by an administrator.

The Concurrency Control feature prevents changes from being made to a managed object, such as a Brick or zone ruleset, by more than one administrator at a time. With Concurrency Control enabled, an object opened for **Edit** by an administrator is “locked out” to other administrators until the managing administrator completes and saves the changes.

Multiple administrators can open the same object in **View** mode, but only one administrator can open the object in **Edit** mode.

## Edit mode

To make changes to an object, right-click on the name of the object in the Contents Panel and select **Edit** from the pop-up menu, or simply double-click on the object. The associated Editor window is opened, and the object is now in 'Edit' mode. Modifications can be made as needed.

If the Concurrency Control feature is enabled, the system prevents another administrator from opening the same object in 'Edit' mode and making changes at the same time. The operation is denied and a dialog box is displayed, informing the administrator that another administrator is currently editing the object. More detailed information, such as Admin Name, telephone number, and so forth are displayed if **Display Contact Information** is selected when enabling the Concurrency Control feature. Refer to the procedure [“To Enable Concurrency Control” \(p. 1-39\)](#) for instructions.

## View mode

To view the current configuration settings of an object, right-click on the name of the object in the Contents Panel and select **View**. The associated Editor window is opened in 'View' mode; the contents of the window display is shown in “view-only” mode and the parameter fields are greyed-out so no modifications can be made. An object can be opened in 'View' mode by multiple administrators at the same time

## Brick console

The SMS prohibits more than one Brick console to be opened for a particular Brick at the same time. However, it is possible to open another Brick console by directly connecting to the serial port on the Brick.

## Enabling concurrency control

By default, Concurrency Control is disabled. The feature is enabled via a dialog box that is accessed from the Utilities menu of the SMS Navigator. Refer to the procedure [“To Enable Concurrency Control”](#) (p. 1-39) for instructions.

## Displaying contact information

An option can be enabled to display detailed contact information about the administrator who currently has an object “out for edit” and a means to send an instant message to that administrator.

If another administrator attempts to edit the object at the same time, and the **Display Contact Information** option is enabled, the following information about the administrator who has the object “out for edit”:

- Full Name
- Telephone #
- Pager #
- Name and IP address of the device on which it is opened (such as Navigator, Remote Navigator or Compute Server)
- Amount of time that the object has been out for edit

**Important!** The **Telephone#** and **Pager #** fields must be provisioned in the Administrator profile; otherwise, these fields will be blank.

The informational display also includes a button to send an instant message to communicate and coordinate activities with the other administrator.

Refer to the procedure [“To Enable Concurrency Control”](#) (p. 1-39).

## Lock status timeout

In a multi-SMS/Compute Server environment, the amount of time needed to poll each device and determine the “out for edit” status of an object can be considerable. To avoid unnecessary lockouts, a timeout interval can be configured via the **Lock Status Timeout** field on the Concurrency Control Editor window. The default timeout interval value is **10** (seconds). When this time interval has elapsed, and the lockout information could be not retrieved in the time period, a warning message is issued to the SMS GUI that information on whether an object is out for edit could not be obtained from every networked device and that there could be a possible concurrency violation.

For instructions on how to enable this option, refer to the procedure [“To Enable Concurrency Control”](#) (p. 1-39).

### Force logout

As part of the Concurrency Control feature, the system provides an option for an SMS administrator to force the logout of any administrator from the SMS, including another SMS administrator. When the force logout feature is used, an AdminEventsLog record is created that shows the SMS administrator who forced the logout of an administrator and the administrator who was logged out. This option can be useful, for example, to log out an administrator who has an object out for edit and has locked out other administrators from being able to access the same object for editing.

For instructions on how to force logout of an administrator, refer to [“To Force a Logout of an Administrator”](#) (p. 1-41).





## To Enable Concurrency Control

---

### When to use

Use this procedure to enable the Concurrency Control feature and, optionally, configure display contact information and the lockout timeout interval for this feature.

### Task

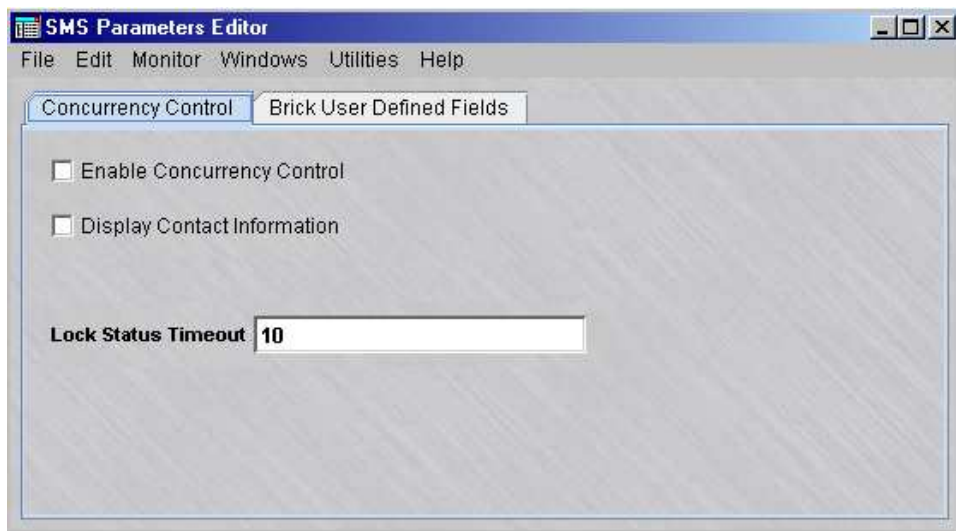
Complete the following steps to enable the Concurrency Control feature and configure the related options, as necessary.

---

- 1 From the menu bar, select **Utilities > Edit SMS Parameters**

**Result** The SMS Parameters Editor is displayed ([Figure 1-14, “SMS Parameters Editor”](#) (p. 1-39)).

**Figure 1-14 SMS Parameters Editor**



The SMS Parameters Editor has two tab panels:

- Concurrency Control
- Brick User Defined Fields

- 
- 2 On the Concurrency Control tab, configure the following options as needed:
- **Enable Concurrency Control**—click this checkbox to enable the Concurrency Control feature. The feature is disabled, by default.
  - **Display Contact Information**—click this checkbox to display detailed contact information about an administrator who has an object “out for edit” when the Concurrency Control feature is enabled.
  - **Lock Status Timeout**—change the lockout status timeout interval, as needed. The default value is **10** (seconds).
- 

- 3 When you are finished configuring the settings, select **Save and Close** from the File menu on the SMS Parameters Editor.

**Result** The settings are saved and the SMS Parameters Editor window is closed.

---

- 4 To just view (not edit) the current Concurrency Control feature settings, from the menu bar, select **Utilities > View SMS Parameters**

**Result** The Concurrency Control tab of the SMS Parameters Editor window is displayed in view-only mode. The fields on the Concurrency Control tab are greyed out and cannot be changed.

END OF STEPS

---



# To Force a Logout of an Administrator

---

## When to use

Use this procedure to force a logout of an administrator from the SMS.

**Important!** You must be an SMS administrator to log out another administrator.

## Task

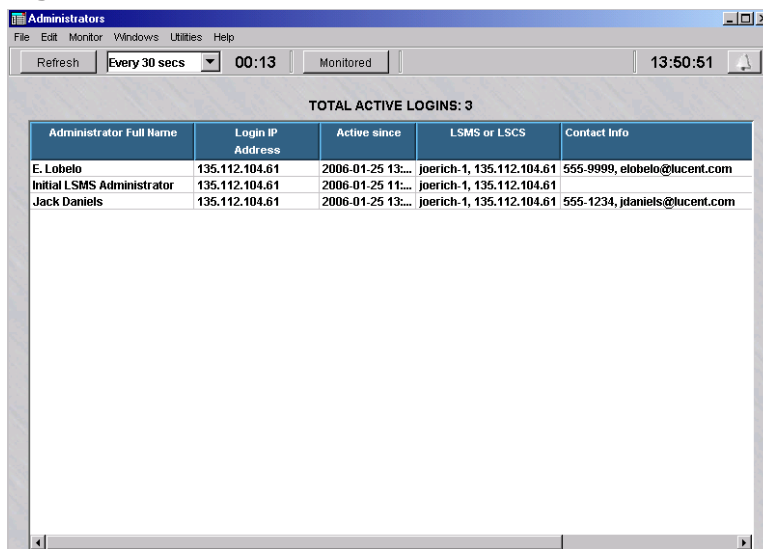
Complete the following steps to force a logout of an administrator from the SMS.

---

- 1 From the Menu bar, select **Monitor > Administrators**.

**Result** The Administrators Status window is displayed (Figure 1-15, “Administrators Status Window” (p. 1-41)).

**Figure 1-15 Administrators Status Window**



- 2 Right-click on the administrator to be logged out and select **Log Out** from the pop-up menu.

**Result** A confirmation dialog box is displayed, asking if you are sure that you want to log out the selected administrator.

---

- 3 Choose **Yes**.

**Result** The selected administrator is logged out of the SMS, and is removed from the Administrators Status window.

If the logged out administrator attempts to access the SMS GUI, a dialog box is displayed on that administrator's GUI instance with an error message Session Terminated by LSMS.

- 
- 4 To close the dialog box, the logged out administrator needs to click **Ok**.
- 

- 5 From the SMS administrator GUI instance, select **File > Close** to close the Administrators Status window.

END OF STEPS

---



# Basic Configuration Requirements

---

## Guidelines

At this point, you should have a sufficient grasp of the basic SMS functionality. At this point, you can begin configuring Brick devices to protect your network entities. The following steps are the suggested initial Brick configuration steps to take, with references to the section(s) in the in SMS documentation to which you can refer for additional procedural instructions:

---

**1** *Configure and install the Brick protecting the SMS host*

The first Brick you should install is the Brick that is protecting the SMS. This Brick is usually connected directly to the SMS.

Refer to [Chapter 3, “Configuring and Activating an Alcatel-Lucent VPN Firewall Brick™ Security Appliance”](#) in the *SMS Administration Guide*.

---

**2** *Configure and install any additional Bricks .*

Deploy the other Bricks in your network. Develop rulesets to determine which traffic will be permitted through them, and which will be dropped. Assign these rulesets to ports on the Bricks.

Refer to [Chapter 3, “Configuring and Activating an Alcatel-Lucent VPN Firewall Brick™ Security Appliance”](#) in the *SMS Administration Guide* and the

*Alcatel-Lucent VPN Firewall Brick® Zone Rulesets* chapter in the *SMS Policy Guide*

---

**3** *Configure any Bricks to be LAN-LAN or client tunnel endpoints*

Set up LAN-LAN and client tunnels. Provide tunnel endpoint addresses for the ports that will be used, and create the necessary ISAKMP/IPSec security associations.

Refer to the *LAN-LAN Tunnels* and *Client Tunnel Endpoints* chapters in the *SMS Policy Guide*

---

**4** *Set up user authentication*

If you will be setting up client tunnels, you have to authenticate the users. Decide whether to create a database on the SMS, or use an external database such as RADIUS or SecurID. Create the required authentication services.

Refer to the *User Authentication* chapter in the *SMS Policy Guide*

END OF STEPS

---



# 2 SMS Redundancy

## Overview

---

### Purpose

This chapter explains the concept of SMS Redundancy and describes how to configure Primary and Secondary SMSs in your operating environment.

### Contents

<a href="#">SMS Redundancy Concepts</a>	2-2
<a href="#">How Redundancy Works</a>	2-6
<a href="#">Redundant SMS Monitoring</a>	2-8
<a href="#">To Configure a Secondary SMS or Compute Server</a>	2-11



## SMS Redundancy Concepts

---

### Overview

To ensure the reliability, high availability, and data integrity of the network security environment, SMS supports the concept of redundancy. In its basic form, two SMSs can be installed and configured as a redundant pair. One SMS takes over the management of Alcatel-Lucent *VPN Firewall Brick*<sup>™</sup> Security Appliances and associated security policies in the network in the event that the other SMS fails for some reason.

In a basic redundant pair, one SMS is installed and designated the Primary SMS and the other SMS is installed and designated the Secondary SMS. Both SMSs are active and share the same database. Each SMS can be set up to manage its own set of Brick devices, security policies, and tunnels. While configuration of redundant SMSs is highly recommended, a single SMS can be installed and configured as a Primary SMS without a Secondary SMS.

The common database is built on the Primary SMS and replicated on the Secondary SMS. This database is updated periodically over the network, and any user-initiated zone ruleset or interface parameter modification is shown immediately on either SMS.

Heartbeat/keepalive messages are exchanged between the Primary SMS and Secondary SMS to establish connectivity. When connectivity is interrupted between redundant SMSs, each SMS keeps track of interim changes made in its own version of the database. When connectivity is restored, any interim changes made during the interruption in connectivity are reconciled in the common database.

### SMS redundancy in network design

The SMS redundancy concept can be extended beyond the basic redundant SMS pair to keep pace as the traffic volume and complexity of the network grows. A single Primary SMS can be connected with up to three Secondary SMSs, for added capacity and reliability, and to manage security for large-scale, multi-customer/multi-site networks, providing seamless redundancy and a single integrated view of the security policies and Bricks within the network to administrators.

#### Compute servers

To further enhance the capacity and security management capabilities of the SMS, one or more devices known as Compute Servers (CSs) can be linked to a Primary or Secondary SMS to serve as log collection points for Brick log data, which frees up the computing resources of the SMS for other activities. A Compute Server has all of the same basic firewall management functions of the an SMS, except it does not maintain a copy of the SMS database. A Brick can be accessed or configured from an SMS, Compute Server, or the Brick console.

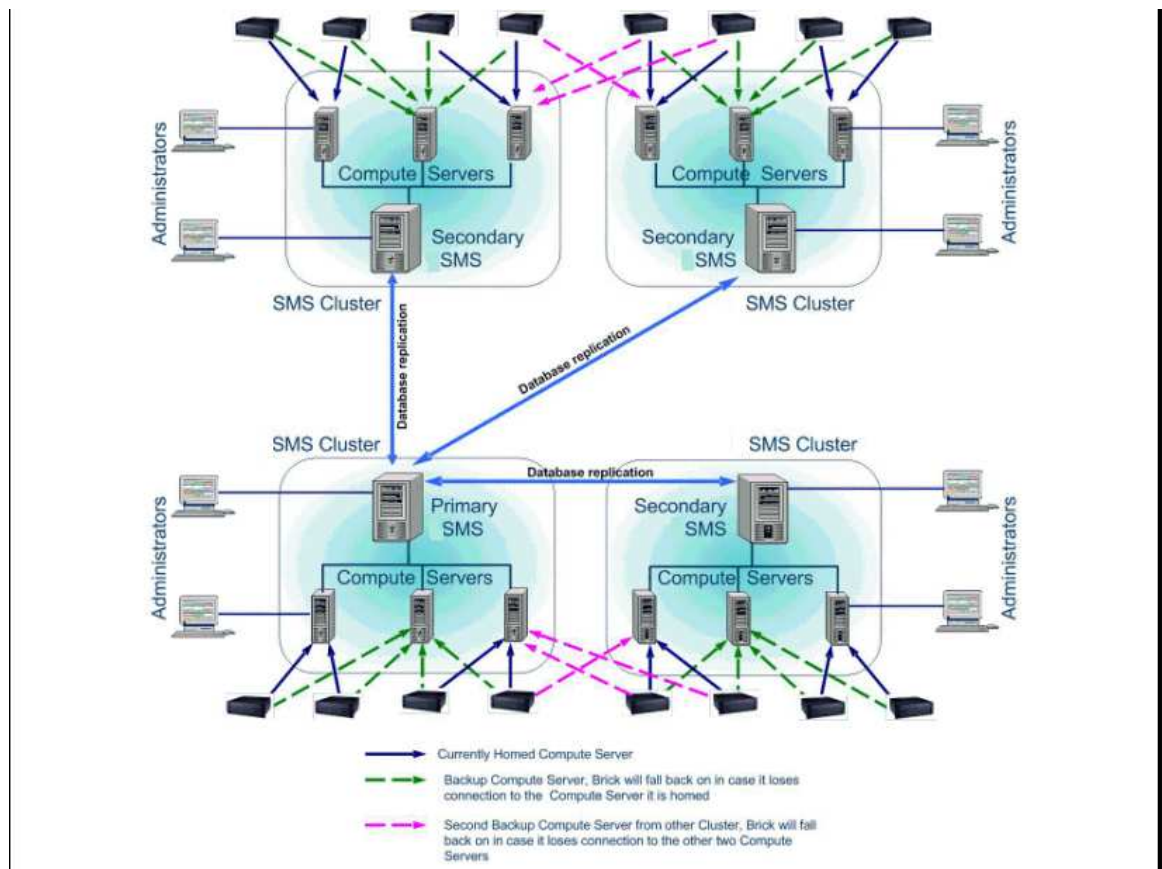


The SMS and its related Compute Servers can be configured as a unit or *cluster* of up to five Compute Servers, providing an additional level of redundancy for communications with a Brick.

For additional information about Compute Servers, refer to [Chapter 9, “Compute Servers”](#).

**Figure: scalability of the SMS network design**

A basic redundant SMS pair (Primary/Secondary SMS) can be installed and configured to ensure uninterrupted, secure traffic between the managed Bricks and protected devices. Additional Secondary SMSs and Compute Servers can be added later as network security requirements grow. The following figure illustrates how to optimize the use of redundant SMSs and Compute Servers for large scale, multi-site networks.



## Installation

When you install a Primary or Secondary SMS, the license key entered while running the installation program designates the SMS being installed as either a Primary or Secondary SMS.

Instructions for installing a Primary or Secondary SMS are provided in the *SMS Installation Guide*.

If you are installing a Primary SMS, the capability to manage additional Bricks or IPSec users, or optional new features can be added to the basic installation by using the New Feature Setup function described in [Appendix F, “New Feature Setup”](#). Any Secondary SMS installed and associated with the Primary SMS automatically receives the feature option keys from the Primary SMS.

If you are installing a Secondary SMS, the following general steps should be followed:

1. Install the Primary SMS, using the procedure for a *Microsoft®Windows®*, *Microsoft® Vista®*, *Sun Microsystems®Solaris®*, or Linux server platform provided in the *SMS Installation Guide*.
2. Log into the Primary SMS and add the Secondary SMS to the database, associating it with the Primary SMS, using the procedure [“To Configure a Secondary SMS or Compute Server” \(p. 2-11\)](#).
3. Install the Secondary SMS, using the procedure for a *Microsoft®Windows®*, *Microsoft® Vista®*, *Sun Microsystems®Solaris®*, or Linux server platform server platform provided in the *SMS Installation Guide*.

While installing the Secondary SMS, you must enter the same Secondary SMS Name that was used while adding the Secondary SMS on the Primary SMS. The installation program also prompts for the IP address of the Primary SMS so the Secondary SMS can communicate with the Primary SMS.

The above steps also apply for a Compute Server. To configure a Compute Server, follow the procedure [“To Configure a Compute Server” \(p. 9-5\)](#).

It is possible to install a Primary SMS and defer the installation of one or more Secondary SMSs to a later date. If this is done, however, all Bricks managed by the Primary SMS will require a manual update (save, apply, and reboot) when the Secondary SMS(s) is installed.

## Set SMS/CS priority

Once the Primary SMS, Secondary SMS(s), and Compute Server(s) have been installed and configured, the order, or priority in which Secondary SMSs or Compute Servers take over management of a Brick in the event that the main (Priority 1) SMS loses connection with the Brick or reboots can be defined via the Home LSMS/LSCS Priority Table of the Brick Editor.

Entries in the Priority Table can be edited, deleted, or rearranged.

The SMS from which the Brick is configured automatically becomes the Priority 1 SMS. This is the management device to which the Brick is initially *homed*. A Brick always attempts to home to its Priority 1 SMS after rebooting or after SMS services have been restarted.

If the Secondary SMS in a redundant pair has been configured on the Primary SMS and installed, its name and IP address appear automatically as the Priority 2 SMS in the Home SMS/LSCS Priority Table, unless you manually change the Priority 2 entry. Up to five SMSs or Compute Servers can be entered in the priority list.

If a Brick is currently homed to the first Compute Server in the list, and the connection to that Compute Server is lost, the Brick re-homes to the next available Compute Server or Primary/Secondary SMS in the priority list.

A Brick can be configured from any SMS (Primary, Secondary, or Compute Server). The SMS where the Brick is created is automatically configured as the Priority 1 SMS for the Brick. You can add to or reorder the priority list for a Brick as needed using the Home SMS/LSCS Priority Table in the Brick Editor.

By default, the Brick automatically rehomes to the Priority 2 device if communications is lost with the Priority 1 device. The **LSMS/LSCS Rehome Options** box on the Brick Editor determines what happens when the Brick re-establishes contact with the Priority 1 device.

If Compute Servers are used for logging purposes, it is recommended that one Compute Server be specified as the main logging server, a second Compute Server from the same SMS cluster be designated on the priority list as the first alternate, and another Compute Server from a different SMS cluster be designated as the second alternate.

Details about provisioning the rehome priority list and related parameters for a Brick are provided in the procedure [“To Configure a Brick Device on the SMS”](#) (p. 3-19).

□

## How Redundancy Works

---

### Overview

SMS redundancy requires database synchronization and a heartbeat between the Primary and Secondary SMS(s).

### Database Synchronization

The members of the SMS redundancy configuration synchronize their data with each other at the time that data is modified. The synchronization is initiated within five seconds of the time the change is made.

### Heartbeat

In a redundant SMS configuration, each SMS transmits *heartbeat* messages to the other across the network in both directions. Heartbeat messages indicate connectivity and the availability of each SMS to the other.

If a heartbeat request fails to complete within a specified period of time, the request is considered a time-out or missed heartbeat. The default is to transmit one heartbeat every second; if five heartbeats are missed, then failover occurs and an alarm is automatically generated.

Once connectivity is restored between the SMSs, the SMS that stayed active immediately copies any database changes that occurred during the failure to the SMS that has come back on-line.

### Load Sharing

An SMS and LSCS, in combination, share the load for Brick log data. Hence, the terms SMS and LSCS are synonymous in the context of the following discussion on load balancing.

SMS redundancy supports any degree of load sharing. Here, for example, are two possible scenarios:

- Home all the Bricks to one SMS, and use the other SMS for administrative duties
- Home half of the Bricks to one SMS and half to the other

In the first scenario, one SMS is the workhorse, attending to all the tasks required for normal firewall and VPN operations, such as log data storage.

The other SMS is used as a Brick maintenance platform from which administrators can provision new Bricks, apply policy or brick changes, add users, user groups, host groups and service groups, and perform all other tasks that require human intervention.

There are trade-offs with such an approach, however. If all Bricks are homed to one SMS, Brick provisioning tasks, performed from the other SMS, will be fast. However, if the SMS with all the Bricks homed to it fails, logging for all Bricks switches to the Priority 2 SMS.

While the load may be distributed across the two SMSs in various ways, there are more factors to consider than simply the number of Bricks in the network. The speed of the connections between multiple SMSs and many CSs, and between Brick devices and the SMS to which they are "homed" plays a role as well.

## Rehoming

A Brick rehomes when it loses connection with the SMS to which it is currently homed, or when an Administrator manually rehomes it. This rehoming arrangement is true even if the priority order of the SMSs is changed. A Brick also rehomes if it is homed to an SMS other than its priority 1 SMS and a higher priority SMS becomes available.

For example, suppose we have a situation in which a Brick is connected to a redundant pair of SMSs. SMS\_A is its Priority 1 SMS and SMS\_B is its Priority 2 SMS.

If an Administrator changes the priority order, so that SMS\_B is now the Priority 1 SMS, this will *not* cause the Brick to rehome. The Brick stays homed to its Priority 1 SMS, even though this SMS is now its Priority 2 SMS. The new priority order is applied only when the Brick connection to SMS\_A is broken, or if the Administrator manually rehomes the Brick.

When you change the priority order, and then save and apply the change, all that applies is specify the priority order that will be used the next time the Brick needs to rehome, either because of a loss of connectivity with the SMS to which it is currently homed or a Brick reboot.

If you manually rehome a Brick to its priority 2 SMS, it will stay homed to the priority 2 SMS until the connection is lost. Once the connection is lost, it will try to home to its Priority 1 SMS. Therefore, if you intend to permanently rehome a Brick, you must change its priority order as well.

**Important!** When a policy is applied by an Administrator, the SMS to which the administrator is logged in will try to apply the policy to all affected Bricks, whether they are homed to that SMS, or to the other member of the redundant pair.

The quickest way to determine which SMS a brick is homed to is to check the SMS Status Monitor. You can also issue the `display lsm` command from the a local or remote brick host. For details of brick host operation, refer to the *Introduction to the Alcatel-Lucent VPN Firewall Brick™ CLI* chapter in the *SMS Tools and Troubleshooting Guide*.

□

## Redundant SMS Monitoring

---

### Overview

You can use the Status Monitor and the Log Viewer to monitor the status of redundant of SMSs/CSs and their managed Bricks.

### Status Monitor

The Status Monitor provides a number of tools that you can use to monitor the status of redundant SMSs/CSs and their managed Bricks. For a more detailed discussion of the Status Monitor, refer to [Chapter 14, “Using the Status Monitor”](#).

### SMS/CS and Bricks window

The SMS/CS and Bricks window provides status information about the SMS/CS you are currently logged into and all of the other SMSs/CSs in your redundant network. Compute Servers are indented and grouped with their associated Primary or Secondary SMS. This window indicates whether each SMS is up or down, and has a **Display Bricks** option to display the name, IP address, SMS software version, and operational status of each Brick assigned (both assigned/homed and not assigned/homed) to each SMS/CS.

To display the LSMS/LSCS and Bricks window, open the Monitor Menu and select **SMS/CS and Bricks**.

### Status windows

The Status Monitor provides a number of windows that show Brick status. There is a Status Overview window, as well as a number of individual Brick Status windows that you can use to view different subsets of bricks (all Bricks, up Bricks, lost Bricks, and so forth). This information is accessible from the Monitor menu.

If a Brick is not homed to the SMS to which you are currently logged into, the only up-to-date information that will be provided in any status window is the Brick operational status (UP/LOST) and the SMS to which the Brick is currently or previously homed. The Proactive Monitoring (Promon) data of all managed Bricks across all SMSs/CSs is shared and can be displayed on the Status Monitor of the SMS to which you are currently logged in

### Log viewer

You can use the Log Viewer to view log records. To launch the Log Viewer on a *Windows*® or *Vista*® server platform, open the Start menu and select:

**Programs ► Alcatel-Lucent Security Management Server ► SMS LogViewer**

On a *Solaris*<sup>®</sup> or Linux server platform, make the installation directory (usually */opt/isms/lmf*) the present working directory, and enter the following command from the *Solaris*<sup>®</sup> or Linux command line: `./LogViewer`

For details on the operation and use of the SMS Log Viewer, refer to the *SMS Log Viewer* chapter in the *SMS Reports, Alarms, and Logs Guide*.

The various logs maintained by the SMSs/CSs can be merged by setting an option in the Reports Wizard to run a Bricks log report across all of the SMSs/CSs and merge the results.

The SMS/CS to which a Brick is homed keeps the log records for that Brick. Thus, if a Brick that is homed to its Priority 1 SMS loses connectivity and rehomes to its priority 2 SMS, the 1 SMS Administrative Events Log shows this as a **Brick Lost** event, and the Priority 2 SMS Administrative Events log shows it as a **Brick Up** event. Any other activity that occurs while the Brick is homed to the Priority 2 SMS is logged and remains in the Priority 2 SMS logs.

For a rehomed Brick, no data will be found in reports and logs of its priority 1 SMS. After rehoming, the Brick log data resides on the associated SMS.

Under normal circumstances, the primary SMS initiates a refresh to the Secondary SMS every five minutes, and messages about these periodic refreshes appear in the Administrative Events log on both SMS.

When a change is made on the Primary SMS, the Secondary SMS is immediately sent a message to synchronize the database with the Priority 1 SMS. This is logged in the Administrative Events log as log type **126, Refresh Status**, with the status **Initiated**, as shown below:

```
126:i:scheduler:013123::REFRESH INITIATED
```

On the Secondary SMS, whenever a database synchronization (refresh) succeeds, an event **126** is logged with status **Successful** in the Administrative Events log, as shown below:

```
126:i:scheduler:013125::REFRESH SUCCESSFUL
```

If a database synchronization fails on the Secondary SMS, an event **126** is logged with status **Failed** in the Administrative Events Log, as shown below:

```
126:i:scheduler:013126::REFRESH FAILED
```

When either Primary SMS or Secondary SMS loses connectivity with its peer an event **125, SMS Status**, is logged in the Administrative Events Log indicating the loss, as shown below:

```
125:i:scheduler:015913::SMS_TWO:LOST::
```

After the Primary or Secondary SMS re-connects with its peer, an event **125, SMS Status**, is logged in the Administrative Events Log indicating the SMS that was re-contacted. The version of the software on the peer is also a part of this log event. It is shown below:

```
125:i:scheduler:020115::SMS_TWO:CONTACTED:7.2.185:
```

During the time the Primary and Secondary SMS have different versions of the software, the database synchronization will be disabled, and when any change to the database is made, a SMS error **N9005** will be logged in the Administrative Events Log. The output message will be similar to the one shown below:

```
N9005 - WARNING - Secondary SMS (version 9.0.184) has a different
version than the Primary SMS (version 9.0.185) and needs upgrading.
Please Upgrade the Secondary SMS to version 9.0.185.
```

This event will be logged in the Administrative Events log each time a change is made on that SMS.

Whenever there is a change to the database and either SMS is unable to initiate a database synchronization, it will log an appropriate error message.

On the primary SMS, **N9007** will be logged to the Administrative Event Log with an appropriate **Reason** and on the secondary, **N9006** will be logged to the Administrative Event Log. This is shown below:

```
N9007 - WARNING - Changes made may not be visible on the Secondary SMS
(redundantNT_2). Reason - Could not connect to the Secondary SMS.
```

### Resynchronization of SMS database changes

If an SMS is unable to synchronize a database change with the other SMS(s) in a redundant configuration, an alarm is triggered.

□



## To Configure a Secondary SMS or Compute Server

---

### When to use

Use this task to configure a Secondary SMS or Compute Server.

### Before you begin

Before you begin this task, obtain the installation key of the type of SMS or Compute Server that you are configuring. For information about installation keys, refer to the *SMS Installation Guide*.

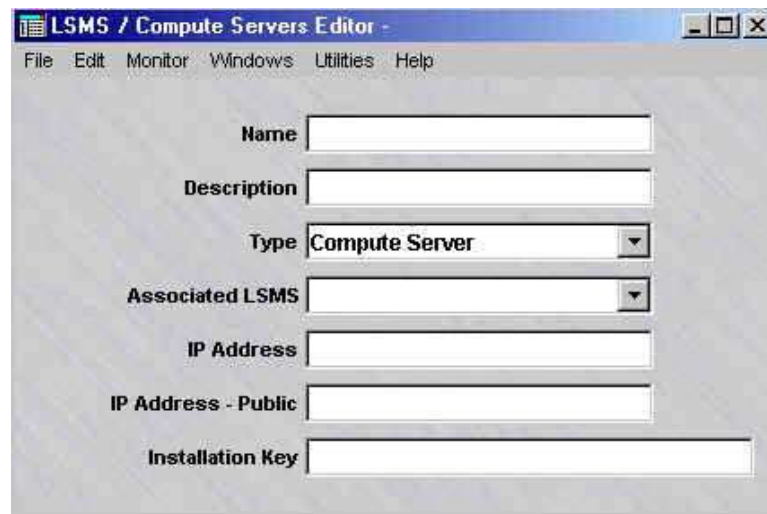
### Task

To configure a new Secondary SMS or Compute Server, follow the steps below:

---

- 1 With the Navigator window displayed, right-click the **LSMS and LSCSs** folder and select **New LSMS and Compute Servers** from the pop-up menu. The SMS / Compute Servers Editor window is displayed ( [Figure 2-1, “LSMS/Computer Servers Editor Window”](#) (p. 2-11) shows a sample window).

**Figure 2-1 LSMS/Computer Servers Editor Window**



- 2 Enter values in the following fields:
  - **Name** - The name of the Secondary SMS or Compute Server, 1-45 characters.
  - **Description** - A textual description of the SMS or Compute Server (Bricks supported, customer(s) supported, and so forth).

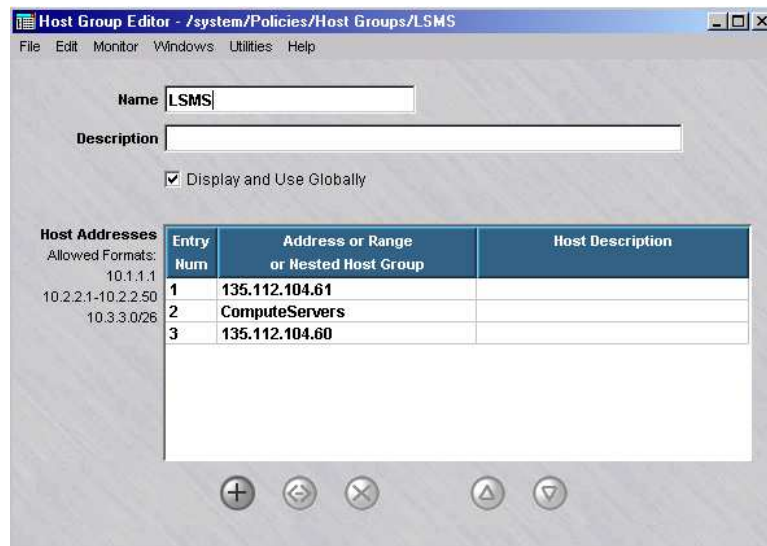
- **Type** - If a Secondary SMS is being added, click the down-arrow next to this field and select **Secondary SMS**  
If a Compute Server is being added, click the down-arrow next to this field and select **Compute Server**.
- **Associated LSMS** - For the Compute Server being added, click the down-arrow next to this field and select the associated SMS.
- **IP Address** - The real IP address of the SMS or Compute Server. On private networks, this is the real IP address of the SMS/CS that can be mapped to a virtual address using NAT.
- **IP Address - Public** - This is the Virtual Brick Address (VBA) of the Brick protecting the SMS/CS used for NAT. This field is optional.
- **Installation Key** - The license key used to install the SMS.

3 From the File menu, select **Save and Close**.

The new SMS or Compute Server is configured. If it is a Secondary SMS, an entry for the new SMS appears in the SMS Host Group. If it is a Compute Server, an entry is added to the ComputeServers Host Group.

Figure 2-2, “Host Group Editor window (SMS Host Group)” (p. 2-12) shows a sample Host Group Editor window.

**Figure 2-2 Host Group Editor window (SMS Host Group)**



END OF STEPS



# 3 Configuring and Activating an Alcatel-Lucent *VPN Firewall Brick*<sup>™</sup> Security Appliance

## Overview

---

### Purpose

This chapter explains how to configure and activate a Brick device. The process is the same regardless of the Brick model device being used. The process consists of the following activities:

- Using the SMS, create an instance of the Brick device and enter the required configuration parameters, such as Brick name and IP address
- Create a floppy disk or USB drive containing the configuration information and use the disk or USB drive to activate the Brick device, package the configuration files for remote floppy/USB drive creation using an external floppy drive or USB drive connected to the USB port of the Brick device (for certain models), or use the floppyless bootstrap method that copies a "boot image" to the Brick serial port

### Contents

<a href="#">Deployment Considerations for a Brick Device</a>	3-2
<a href="#">To Configure a Brick Device on the SMS</a>	3-19
<a href="#">Brick Device Failover</a>	3-38
<a href="#">To Set Up Brick Device Failover</a>	3-42
<a href="#">To Manually Initiate Failover</a>	3-48
<a href="#">To Migrate Model 1100 Bricks to a Model 1200 Bricks That Are in a Failover Pair</a>	3-50
<a href="#">To Activate a Brick Device</a>	3-52



## Deployment Considerations for a Brick Device

---

### Overview

All Brick devices have to go through the same configuration and activation process to become operational. However, before you begin the process of configuring and activating a Brick device, there are a number of questions you need to ask yourself about this Brick device and the purpose it serves in the network.

### Configuration of a Brick device as a bridge or router

**Important!** Do not attach two or more interfaces that are configured with the same VLAN/subnet to the same switched network unless that network is running spanning tree protocol.

A Brick device is essentially a bridging device. It passively “listens” on all its ports, in promiscuous mode. This means it accepts any traffic it “hears,” regardless of the destination MAC or IP address. One important advantage of having the Brick operate as a pure bridge is that it does not interact with surrounding network equipment directly, so no connected device has to be re-configured when a Brick is added to a network.

During the configuration process, you will be asked to provide the Brick with an IP address and subnet mask, which will then be automatically assigned to each of the Brick physical ports. If you make no changes to the addresses, the Brick will bridge all traffic on all ports.

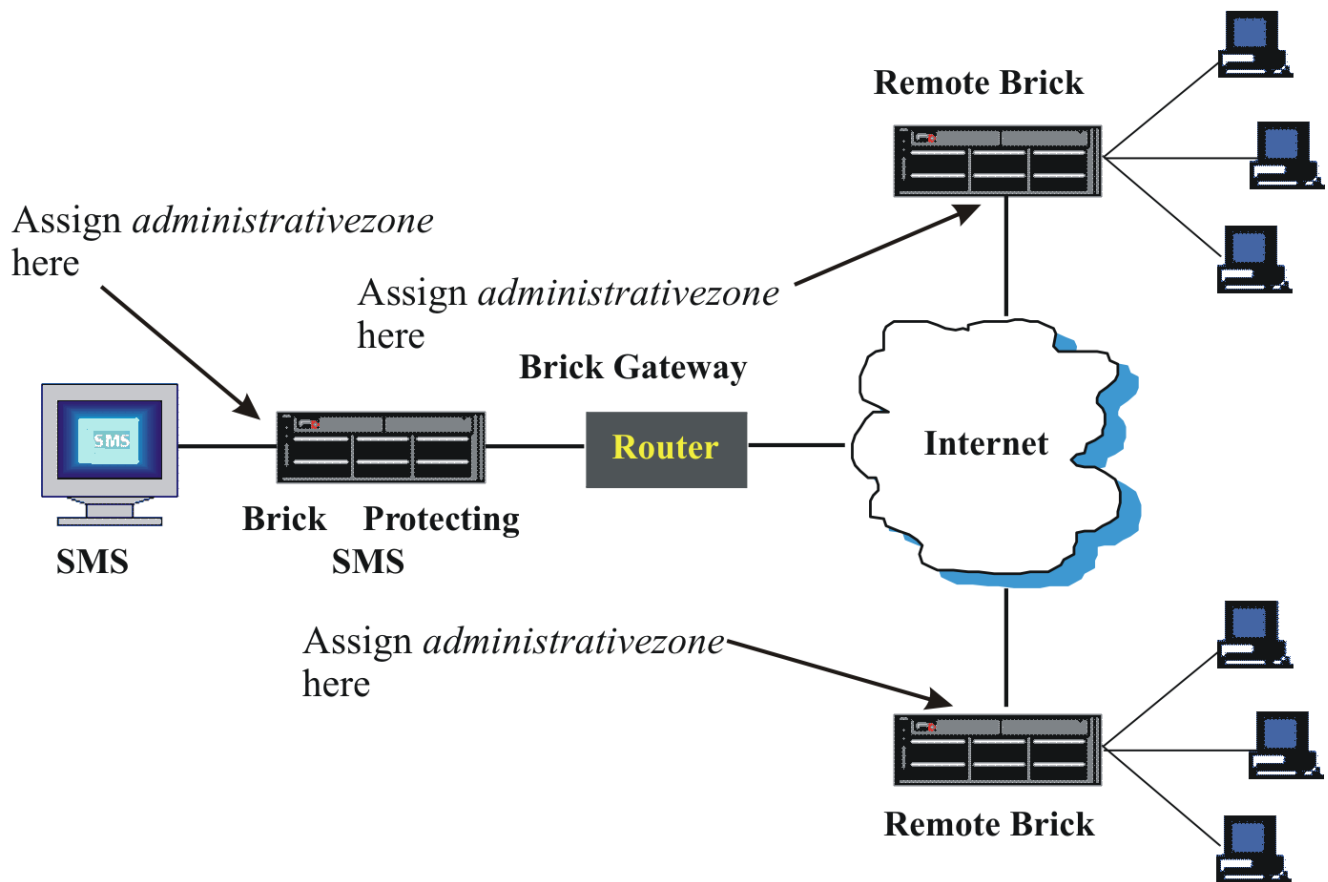
If you change the IP address of one or more of the physical ports — for example, if you assign one IP address to two of the Brick ports, and then assign a second IP address to the other two ports — and the Brick has VLAN enabled, the traffic within a single VLAN is bridged. However, if you also have bridge groups enabled, then traffic is bridged within a VLAN and between VLAN(s) with the same subnet IP address(es). If VLAN is not enabled, packets traveling between two ports with the same IP address are bridged, while packets traveling between two ports with different IP addresses will be routed from one subnet to another.

The Brick device does not participate in dynamic routing protocols. It can be configured to pass packets to other subnets that are not directly connected to it by creating static routes (refer to the procedure “[To Add a Static Route](#)” (p. 4-34) in [Chapter 4, “Configuring Alcatel-Lucent VPN Firewall Brick™ Security Appliance Ports”](#)).

### Direction connection of a Brick device to the SMS

It is strongly recommended that you connect at least one Brick device directly to the SMS host to prevent an attacker from gaining access to the SMS. [Figure 3-1, “Brick Configuration”](#) (p. 3-3) shows a configuration in which one Brick device is connected directly to the SMS, and two other Brick devices are connected to the SMS remotely.

**Figure 3-1 Brick Configuration**



If the Brick being configured protects the SMS, you should assign the pre-configured Brick zone ruleset *administrativezone* to the port connected to the SMS host (refer to [“To Assign a Security Policy to a Port”](#) (p. 4-9) for instructions). This is a ruleset provided with the SMS software specifically for this purpose. It contains rules that drop all traffic to the SMS except from the Bricks it is managing. (Refer to the *Pre-Configured Brick Zone Rulesets* appendix in the *SMS Policy Guide* for a detailed description of the *administrativezone* ruleset.)

If the Brick being configured is connected to the SMS remotely, you should still apply *administrativezone* to the port connecting it to the SMS. This is usually the port connected to the router that has been designated the Brick gateway during the configuration process.

When assigning *administrativezone* to a port, you also have to indicate the IP addresses connected to the port that will be protected by this ruleset (the ruleset along with the IP addresses is referred to as a *zone*). It is best if the SMS is the only host connected to the Brick on its port. If this is the case, enter an asterisk in the **Zone IP Addresses** field when assigning *administrativezone* to the port. If other hosts are connected, enter the IP address of the SMS host instead.

This configuration will prevent an administrator from creating a policy on that port that disallows access from the Brick to the SMS host, thereby rendering that Brick unmanageable. (If this does accidentally happen, simply change the policy on the SMS and reboot the Brick to allow it to recollect its policy from the SMS. If it is a Brick failover pair, you may have to reload the policy from a USB drive, floppy drive, or from a serial port to recover it)

## A Brick device functioning as a firewall

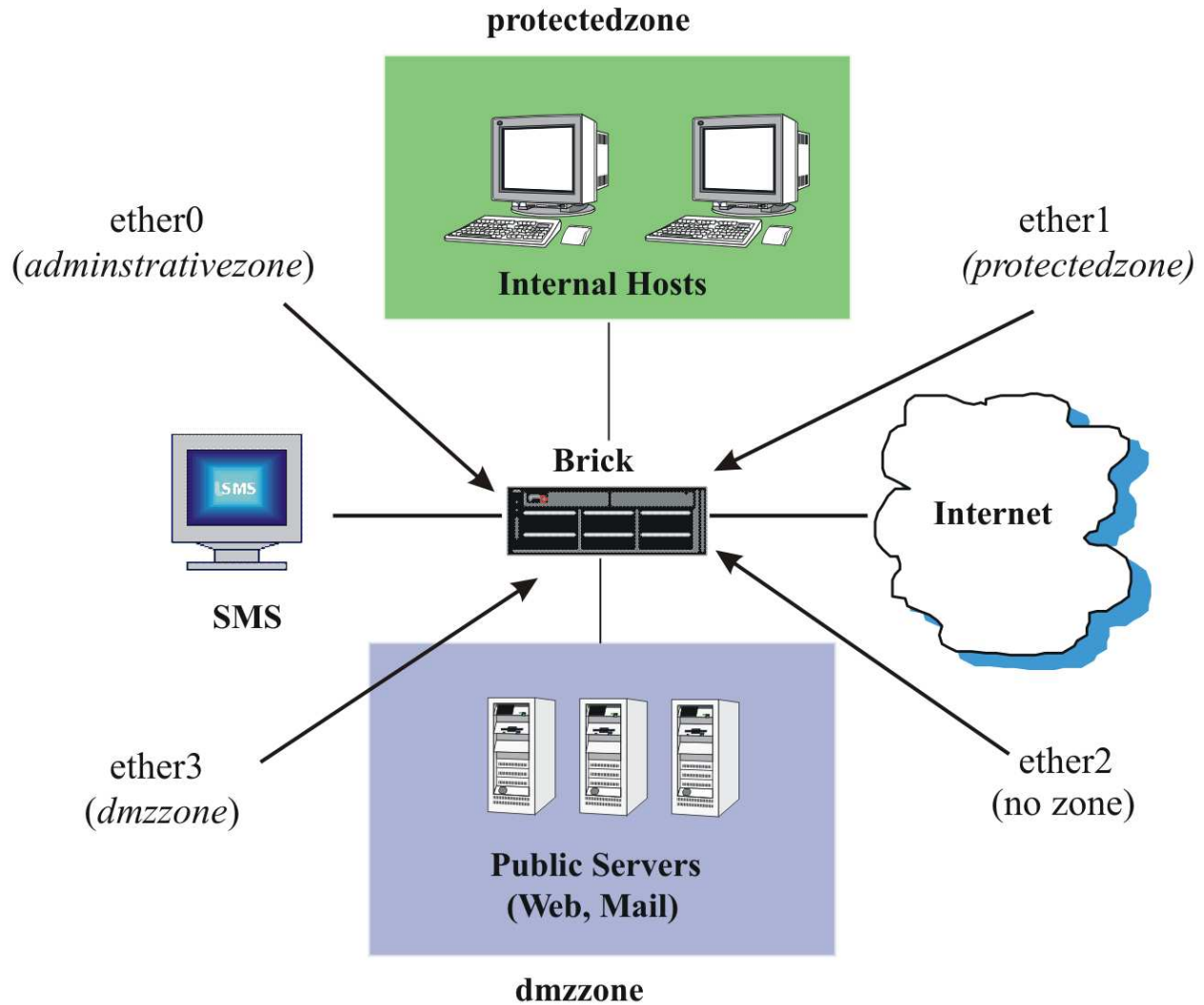
If the Brick device is being deployed as a firewall to protect internal LANs from attack via the Internet, you have to configure the Brick appropriately. [Figure 3-2, “Firewall Configuration” \(p. 3-5\)](#) shows a Brick device configured as a firewall.

In this example, the Brick device is deployed between the Internet and an internal LAN consisting of two zones (Brick zone rulesets). All communication between the Internet hosts in the two zones is monitored by the *protectedzone* and *dmzzone* rulesets that were assigned to ethers1 and 3.

Since this Brick device is also protecting the SMS, the *administrativezone* ruleset is applied to ether0, the port connecting the Brick and SMS. No ruleset is applied to ether2, since it is connected to the Internet.

Deploying the Brick device at the port to the Internet protects the internal network from external intrusion and attack. Attacks between hosts in the internal network can also be mitigated by connecting them to separate ports on the Brick. This ensures that all communication between these hosts must pass through the Brick so that their traffic is also scrutinized by the rulesets on the Brick.

Figure 3-2 Firewall Configuration



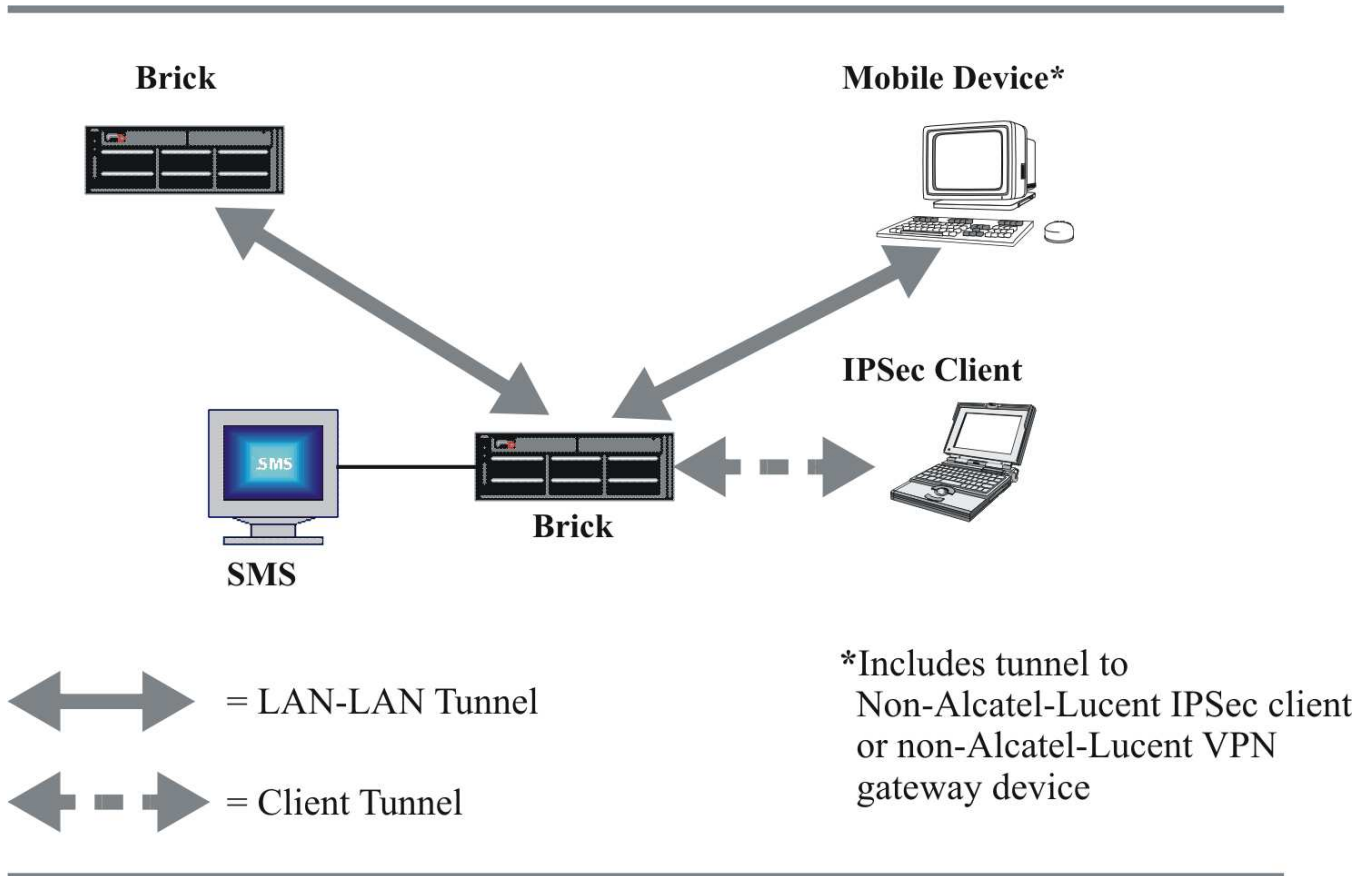
### A Brick device functioning as a tunnel endpoint

If the ports on this Brick device will be terminating LAN-LAN or client tunnels, you have to assign tunnel endpoint addresses to the ports when configuring the Brick device.

Figure 3-3, “LAN-LAN and Client Tunnels” (p. 3-6) shows the different kinds of tunnels that can terminate on a Brick device port. LAN-LAN tunnels include tunnels from the Brick to another Brick device or to an unmanaged device. A client tunnel is a tunnel from a host running the Alcatel-Lucent IPsec Client to the Brick device.

**Important!** The tunnel endpoint address is also the Virtual Brick Address (VBA). The VBA can be used when performing network address translation (refer to the *Network Address Translation* chapter in the *SMS Policy Guide*).

**Figure 3-3 LAN-LAN and Client Tunnels**



### Assignment of a “dynamic” IP address to a Brick device

In some environments, such as a home office or branch office, a service provider may only grant users a single dynamic IP address, which may change from time to time. Also, in a DSL network environment, dynamic IP addresses are assigned by DSL modems using PPPoE. A Brick device can operate in such settings in either of three different modes: with a static, private IP address in which the router performs a Network Address Translation function, or in which the Brick itself obtains the dynamic address via either DHCP or PPPoE.

When the Brick device is provisioned with a static IP address, there are any number of low-end routers on the market that provide a DHCP client operating on their “outside address”. These devices have the ability to source address translate any outbound TCP or UDP connection so that their public addresses may be shared by inside “private” sources. In addition, the external device must support mapping inbound connections to



specific private addresses. Typically, this configuration would involve a Model 50 Brick device with a small office router such as the Linksys Etherfast router. The router performs Network Address Translation (NAT) on the inbound and outbound packets from the Brick while the SMS “learns” about any IP address change for the Brick device.

When the Brick device is provisioned as a DHCP client or as PPPoE, the Brick device communicates with the DHCP server itself or the DSL modem itself and obtains a dynamic IP address, netmask, and gateway from them. In these cases, any outside router does not typically perform NAT. The Brick device may perform NAT or VPN for the network “behind” it, using this public address.

### **Configuration of a Brick device as a base station router (BSR) voice gateway and/or packet gateway**

The Base Station Router (BSR), developed by Alcatel-Lucent, streamlines and simplifies the IP-based mobile network architecture by combining key components of third-generation (3G) mobile networks—base station, radio network controller, core network router—into a single, compact unit that can be easily installed to expand cellular services in hotspots and buildings, without the major cost and effort involved in deploying or upgrading additional base stations or radio network controllers, while improving coverage and maintaining quality of service over a secure connection.

A Brick device can be configured to serve as a BSR Voice Gateway (BVG) and/or BSR Packet Gateway (BPG) in an IP-based mobile network, thereby providing inherent security features and firewall protection.

A Brick device, with the BVG feature enabled, can consolidate and map the voice traffic from many BSRs into a single source UDP port on the Brick device for passing on to a Mobile Switching Center (MSC) or Media Gateway (MGW) in the mobile service provider’s Circuit Switched Core Network.

Similarly, with the BPG feature enabled, a Brick device can consolidate and map the data traffic from many BSRs (the number dependent on the size of the BSR cluster) into a single UDP port on the Brick device for passing on to a Serving GPRS Support Node (SGSN) and Gateway GPRS Support Node (GGSN) in the mobile service provider’s Packet Switched Core Network. When passing data traffic, the BPG acts a virtual Radio Network Controller (VRNC) towards the SGSN and as a virtual SGSN towards the BSR(s).

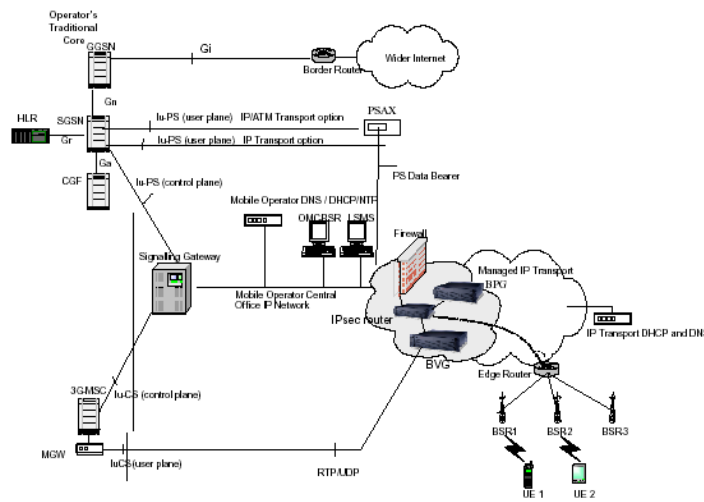
The Brick, serving as a BVG or BPG, can support up to 120 MSC or SGSN IP addresses.

The Brick device, serving as the BVG and/or BPG, establishes LAN-LAN tunnels or client tunnels between itself and the BSR(s), using IPSec to receive, consolidate, and encrypt the voice and/or data packets. The BVG and/or BPG function(s) is co-located on the same device platform as the IPSec router in the network design. A Brick device,

acting as either a BVG or BPG, can support simultaneous tunnels to up to 20,000 BSRs, depending on the volume of voice and/or data traffic (for example, if there are less than 5,000 simultaneous voice calls per BSR cluster).

Figure 3-4, “Deployment of Brick device as BVG/BPG in BSR-based mobile network” (p. 3-8) depicts the deployment of a Brick device as a BVG and/or BPG in a BSR-based mobile network architecture.

**Figure 3-4 Deployment of Brick device as BVG/BPG in BSR-based mobile network**



When a Radio Access Bearer (RAB) session is set up for transfer of voice traffic, the matching VMSC and VRNC address/port information is returned by the BVG (Brick device) to the BSR for transmission of the voice IP data packets to the BVG and delivery to their destination. The DPAT protocol allows voice RTP packets from many BSRs to be consolidated at the BVG so as to provide a single lu-CS user plane interface towards the MSC/MGW.

When an RAB session is set up for transfer of data traffic, the matching VSGSN address and VRNC User Plane tunnel endpoint address is returned by the BPG (Brick device) to the BSR for transmission of the data packets to the BPG and delivery to their destination. The DPAT protocol allows data RTP packets from many BSRs to be consolidated at the BPG so as to provide a single lu-PS user plane interface towards the SGSN.

**Important!** If the SGSN supports an ATM interface only for the lu-PS user plane, an IP-to-IP/ATM converter box is required between the BPG (Brick device) and the SGSN to provide IP-to-IP/AAL5/ATM conversion.

A typical exchange between a BSR and the BVG (Brick) for a cellular service call session is as follows:

1. The BSR sends a request message to the BVG (Brick device) that contains a MSC/MGW IP address and port number, the BSR's IPsec tunnel address, and a BSR port number for the call session.  
This exchange invokes the BVG to set up a mapping between the BSR IP address and BVG UDP port number for voice packet transfer.
2. The BVG responds to the request sent by the BSR with a Virtual RNC Address (VRA) and port number, a UDP port number, and a Virtual MSC Address (VMA) and port number to be used in addressing the voice data packets to be sent.  
In the current version of the BVG feature, the VRA and VMA addresses are the same as the Virtual Brick Address (VBA) or Tunnel Endpoint Address assigned to the Brick device serving as the BVG.
3. The BVG receives a UDP data packet from the BSR. If the VMSC/MGW IP address and port number match a corresponding entry in its port mapping table, the BVG creates and encrypts a UDP packet with the destination IP address and port number and forwards it to the BSR for delivery and completion of the cellular service call. If the data packet has been handed over from one BSR to another one, the port entry in the mapping table is revised via a DPAT protocol message, the new mapping goes into effect immediately, and the packet is forwarded to the updated BSR for delivery and completion of the cellular service call.

A typical exchange between a BSR and the BPG (Brick) for mobile-based data packet transfer is as follows:

1. The BSR sends a request message to the BPG (Brick device) that contains an SGSN IP address and GTP-U tunnel endpoint identifier (TEID), and the BSR's IPsec tunnel address. This exchange invokes the BPG to set up a mapping between the BSR IP address and the BPG Virtual Radio Controller (VRNC) GTP-U tunnel endpoint address.
2. The BPG responds to the request sent by the BSR with a VRNC IP address, VRNC User Plane TEID, and VSGSN IP address to be used in addressing the data packets to be sent. In the current version of the BPG feature, the VRNC address is the same as the VBA or tunnel endpoint address assigned to the Brick device serving as the BPG.
3. The BPG receives a UDP data packet from the BSR. If the VSGSN IP address matches a corresponding entry in its binding table, the BPG replaces the VSGSN IP address (if it is not the actual SGSN IP address) with the SGSN IP address, the BSR's source address with the BPG's VRNC IP address, and then forwards the data packet to the SGSN.
4. If a data packet is received from the SGSN by the BPG, the BPG uses the VRNC tunnel endpoint identifier (TEID) to look up the BSR IP address in its binding table, replaces the VRNC IP address with the BSR's IP address, and then forwards the data packet to the BSR for delivery and completion of the mobile data transfer.

The BVG and/or BPG feature(s) can be enabled or disabled for a Brick device via the **BVG/BPG** tab on the Brick Policy Assignment Editor. As part of the BSR voice and packet gateway features, an administrator can specify the DPAT port number for collection of UDP packets from multiple BSRs, enable/disable a clean-up process for hung-up or failed BSR/BVG port table mappings, and configure a BPG inactivity timer to terminate the binding session between the BSR and Brick device if there has been no user traffic activity for a set amount of time (in minutes).

**Important!** The BVG and BPG features are optional features that must be purchased and installed together using a separate installation key via the New Feature Setup utility. If the BVG and BPG features have not been installed, the **BVG/BPG** tab is not displayed on the Brick Policy Assignment Editor.

For details about the New Feature Setup utility, refer to [Appendix F, “New Feature Setup”](#) in the *SMS Administration Guide*.

For instructions on how to enable or disable the BVG and/or BPG feature(s), refer to the procedure [“To Enable or Disable the BSR Voice Gateway \(BVG\) And/Or BSR Packet Gateway \(BPG\) Feature\(s\)”](#) (p. 4-21) in [Chapter 4, “Configuring Alcatel-Lucent VPN Firewall Brick™ Security Appliance Ports”](#).

### **Deployment of a Brick device as an application layer gateway (ALG) for VoIP/NOE phone communications**

A Brick device can be deployed as an application layer gateway (ALG) in a service provider’s IP-based telecommunications network, providing virtual firewall protection and secure Voice over IP (VoIP) communications between the various network elements, specifically the call server(s), Media Gateway (MGW), and IP phone devices, such as a New Office Environment (NOE) IP Touch phone.

When the Application Layer Gateway (ALG)/NOE feature is enabled on a Brick device in a VoIP network environment, the Brick performs application layer filtering on all transmission protocol services used for data exchanges between IP Touch phones and the other network elements. In this capacity, the Brick can also translate and secure IPlink signaling protocol messages exchanged between a MGW supporting telecommunication devices behind the Brick firewall zone and call servers outside of the Brick zone.

Serving as a security gateway device in a VoIP environment, the Brick manages and monitors the voice and data traffic at all levels (media plane, control plane, management plane). The Brick device also decodes the Universal Alcatel (UA) proprietary signaling protocol between the communication endpoints, and dynamically controls the opening of the exact pinhole (UDP port) needed for a specific communication session (such as a telephone conversation between two IP Touch phone users), thereby minimizing the potential for compromise of service or breach of security by intruders. A security optimization option can be enabled, which restricts the

opening of pinholes to VoIP traffic (RTP flows) between IP phone devices that crosses the firewall (Brick device). With this security optimization option enabled, if a phone call is placed between IP phones in a Branch office that are behind the Brick, no pinholes are opened.

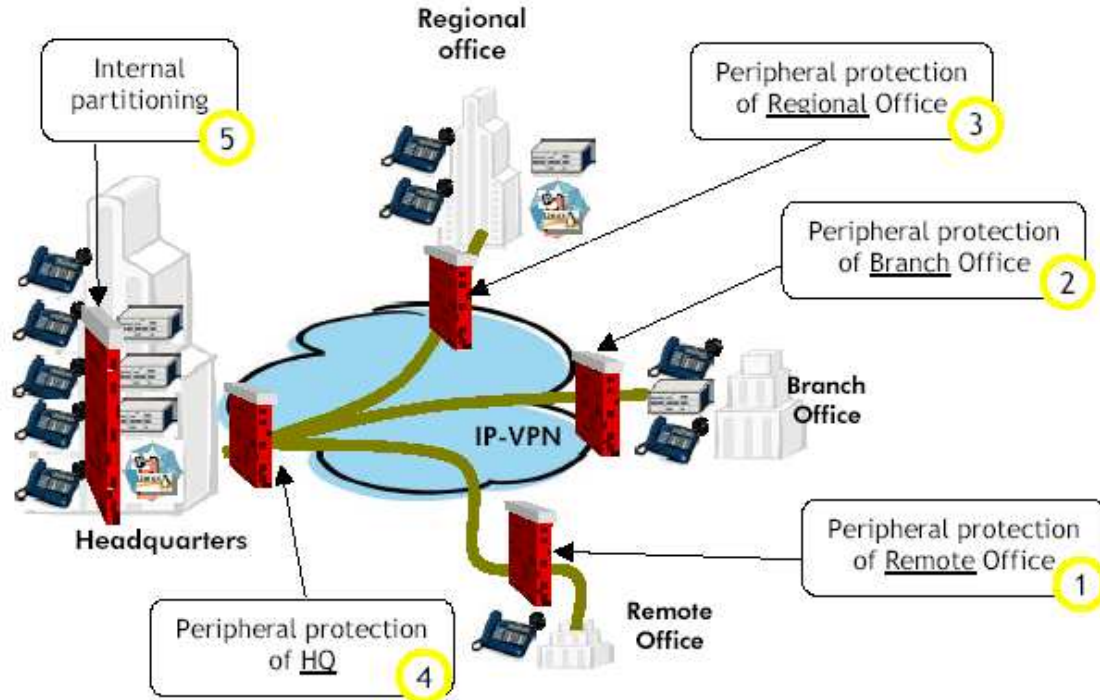
A Brick, acting as a VoIP ALG, supports up to 2,000 IP phones per zone.

A Brick can be deployed to serve as an ALG at any logical vantage point in a customer's enterprise VoIP network, including:

- Headquarters where the call server and MGW are located
- Regional office connected to a corporate Headquarters through IP-VPN or IPSec VPN. The call server and MGW may be deployed in the Regional office
- Branch office connected to a corporate Headquarters office through IP-VPN or IPSec VPN. Call server and MGW may be deployed in the Regional office
- Branch office connected to a corporate Headquarters office through IP-VPN or an IPSec VPN. A Branch office may host MGW with terminals
- Remote office connected to a corporate Headquarters office through IP-VPN or an IPSec VPN. Only terminals are installed in the remote office. No call servers or MGWs are onsite

Figure 3-5, “Deployment of Brick devices in a customer's enterprise VoIP network” (p. 3-12) depicts the possible deployment strategies for a Brick device in securing a typical customer's enterprise VoIP phone network, which is being managed by Alcatel-Lucent's OmniPCX Enterprise (OXE) communications server(s).

**Figure 3-5 Deployment of Brick devices in a customer's enterprise VoIP network**



As shown above, the type of VoIP traffic that could be monitored by the deployed Brick device(s) varies, based on the deployment scenario:

- In Scenario 1, the Brick device deployed at a Remote office would provide peripheral protection and monitors local data traffic and VoIP traffic between IP hardphones/softphones and communications applications
- In Scenario 2, a Brick device deployed at a Branch office would provide peripheral protection and monitors local data traffic, VoIP traffic between IP hardphones/softphones, and the media and control flows to the MGW(s)
- In Scenario 3, a Brick device deployed at a Regional office would provide peripheral protection and monitor the flows exchanged between the call servers in addition to all of the typical data flows of a Branch office
- In Scenario 4, a Brick device deployed to provide peripheral protection of the corporate Headquarters office LAN would monitor the data traffic and VoIP traffic, depending on other network elements that could be located in a Branch office (IP hardphones/softphones, MGWs, other call servers)
- In Scenario 5, a Brick device deployed to internally partition the Headquarters LAN would monitor the same type of traffic as if it were placed at the periphery as described in Scenario 4

**Important!** In Brick deployments where there are multiple call servers handling VoIP phone traffic, call server failover is *not* supported by the Brick device when the call servers are on different subnets (as in the Regional Office case). Typically,

there is a separate Brick device protecting each call server, and Brick devices currently cannot share state information about each call server should one go down. During a phone call, an IP phone establishes a data link with only one of the call servers; only the Brick protecting that call server will have the dynamic rules in place for the call session in progress. If a call server goes down for some reason and failover to another call server occurs, the data link(s) will go down and come up again, reconnecting to the new call server and Brick.

During the initialization phase, when an IP Touch phone (NOE) is first installed and set up (following the IEEE 802.1X authentication process where the IP phone device is given LAN port access to the network), the IP phone device is manually configured with a password and default identity, which can be changed to differentiate some NOE phone devices and offer customers additional control and security over equipment connected to their network. The Brick manages the retrieval of a configuration file *lanpbx.cfg* by the IP phone device from the call server, using Trivial File Transfer Protocol (TFTP), which contains the type, version, and IP address of the call server involved in the phone's initialization (and software updates), and, optionally, the IP address of a call server for future transmissions. A second call server IP address will be specified for redundant operations. These optional call server IP addresses are later used by the Brick (if specified in the configuration file) to authorize traffic to/from the call server(s) to the IP phone device. The Brick manages UA signaling traffic for start/end of transmission messages between the IP phone device and call server.

An IP hardphone/softphone communicates with another network entity (such as another IP phone, MGW, voice mailbox system) by sending a UA message to the call server that it is ready to begin transmission. The call server sets up a Real Time Protocol (RTP) session between the IP phone and the entity by sending a *START\_RTP* UA message, which contains the destination IP address and UDP port to be used for the transfer of the RTP packets during the call or data stream. The UA message passes through the Brick, and the Brick detects, from this message, which source and destination UDP ports will be used for this particular RTP session. The Brick restricts the valid UDP ports and IP addresses for RTP transmissions to those specified in the TFTP application filter and defined in the Brick zone rule for NOE traffic. The call or data transfer is terminated when the call server sends a *STOP\_RTP* UA message back to the IP phone signaling that the call/data transfer is completed.

HTTP URLs may be transmitted to the IP Touch phone through UA/NOE signaling. The IP Touch phone acts as an HTTP client that retrieves the HTTP content of the page designated by the URL. The Brick opens a configurable destination port which allows the IP phone to retrieve HTTP output.

The Brick also supports remote debugging of an IP Touch phone by allowing a UA message to be sent from any host to the phone device, opening a telnet service port (tcp/23) for debugging purposes for a specified period of time. The telnet service port will be opened between the host and the IP phone for a period of time (none null) as specified in the message.

To enable the ALG/NOE functionality of a Brick device, the NOE application filter option is activated within a TFTP application filter which, in turn, is assigned to a TFTP service group and defined in a Brick zone rule to allow TFTP traffic to/from the call server(s), specified either by individual IP address or within a call server host group (up to two call server IP address entries are recognized by the Brick in this type of host group). The call server host group entries are compared with the call server IP addresses that were downloaded in the IP Touch phone's initialization file (if they were specified). If the call server host group addresses match the call server addresses in the initialization file, the Brick allows traffic to/from the call server(s). If there is no match, the Brick blocks communication with the call server(s) and reports an error in the log file. For additional details about creating host groups, refer to the *Host Groups* chapter in the *SMS Policy Guide*.

When the NOE application filter option is activated within a TFTP application filter, the Brick dynamically creates other rules for the other types of service traffic involved in call activity and IP phone maintenance (RTP sessions, UA signaling messages, telnet debug sessions). A static rule must be created within the assigned Brick zone ruleset to allow HTTP URLs to be passed to/from the IP phone to a presentation server.

For details about creating an NOE application filter and applying an NOE application filter within a TFTP application filter, refer to the TFTP Application Filter and NOE Application Filter sections of the *Application Filters* chapter in the *SMS Policy Guide*.

The SMS application provides a set of pre-defined Brick zone ruleset, application filter, service group, and host group templates to assist you with configuring the Brick to handle VoIP/NOE traffic in most OXE/NOE deployment arrangements. These pre-defined templates are named to make it easy to identify which application filter(s), service group(s), host group(s), and zone ruleset(s) are being applied, based on the deployment location of the Brick, as shown in [Figure 3-5, "Deployment of Brick devices in a customer's enterprise VoIP network"](#) (p. 3-12) (in a Headquarters or Branch Office, for example) and/or the equipment being protected (NOE/IP hardphones/softphones, MGW, call servers). The correct pre-defined application filters, service groups, host groups, and rules are already pre-configured in each Brick zone ruleset. All that is required is for you to input the IP address(es) of the equipment (IP phones, call servers, MGW) in the host groups called by the NOE application filter and rule(s) within the appropriate zone ruleset and then apply this zone ruleset to a physical port on the Brick.



For a listing and samples of the pre-defined application filter templates provided with the SMS application for VoIP/NOE traffic, refer to the *Application Filters* chapter in the *SMS Policy Guide*.

For a listing and samples of the pre-defined service groups provided with the SMS application for VoIP/NOE traffic, refer to the *Service Groups* chapter in the *SMS Policy Guide*.

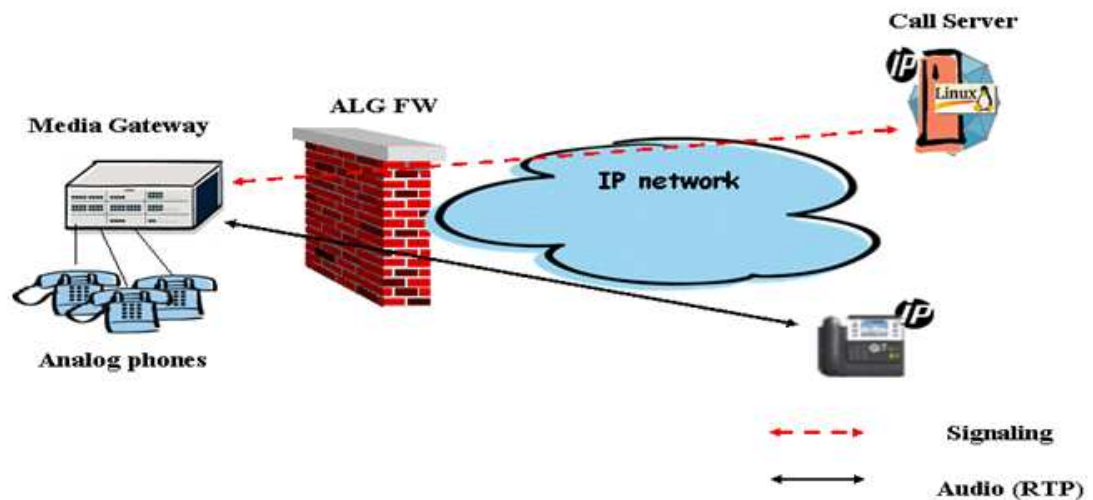
For a listing and samples of the pre-defined host groups provided with the SMS application for VoIP/NOE traffic, refer to the *Host Groups* chapter in the *SMS Policy Guide*.

For a listing and samples of the pre-defined Brick zone rulesets provided with the SMS application for VoIP/NOE traffic, refer to the *Alcatel-Lucent VPN Firewall Brick® Security Appliance Zone Rulesets* chapter in the *SMS Policy Guide*.

For step-by-step instructions and illustrations on how to set up a Brick device to serve as an Application Layer Gateway (ALG) in various VoIP deployment scenarios (Headquarters site, Branch Office site, Remote Office site, NATed configurations) using the pre-defined templates provided with the SMS application, refer to the *Configuring the Brick for VoIP/NOE Traffic Using Pre-Defined SMS Templates* appendix in the *SMS Policy Guide*.

A Brick, deployed as an ALG in a Branch office setting, as shown in [Figure 3-5, “Deployment of Brick devices in a customer’s enterprise VoIP network”](#) (p. 3-12) (Scenario 2), protects and monitors VoIP traffic between IP hardphones/softphones, and also secures IPlink signaling protocol messages exchanged between the Media Gateway (MGW) unit and the call server (CS), as shown in [Figure 3-6, “Brick/ALG Firewall Protection of MWG-CS Communications”](#) (p. 3-15).

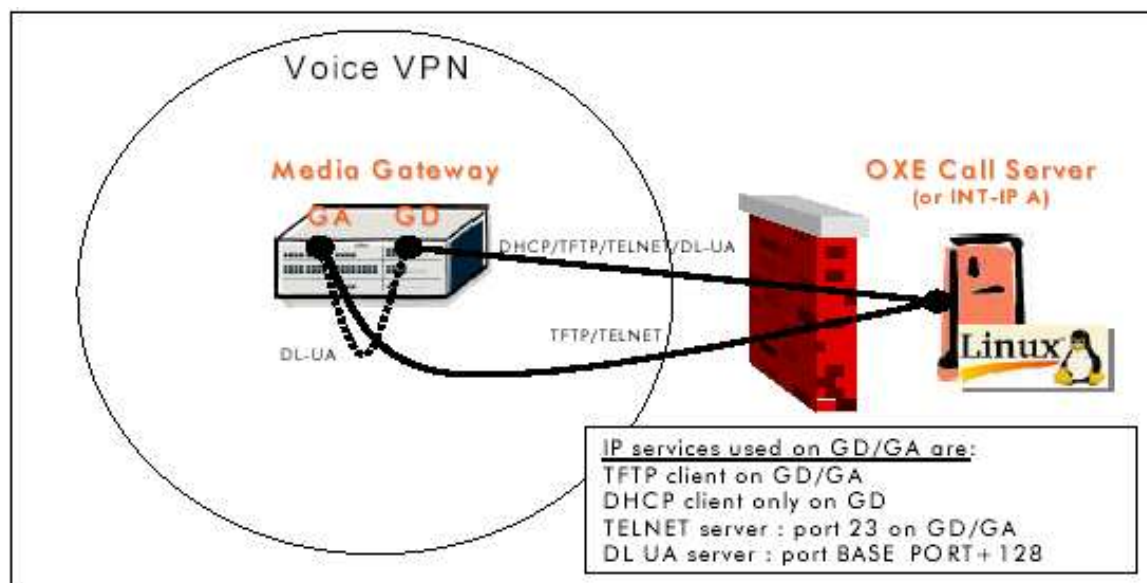
**Figure 3-6 Brick/ALG Firewall Protection of MWG-CS Communications**



The MGW, serving as a translation unit between different telecommunications networks, converts call and data traffic carried over the Public Switched Telephone Network (PSTN) to VoIP so it can be transmitted to IP hardphones/softphones and, conversely, translates VoIP call traffic originating from IP hardphones/softphones to Time Division Multiplexing (TDM) voice traffic to be received by phones over the PSTN. A signaling data link is established between the MGW and the call server, which sets up the call or data session and handles call control activities. The MGW and CS exchange port and addressing information for the duration of the call/data session over the data link, using IPlink protocol signaling messages. The Brick, acting as an intermediary device, protects and monitors these IPlink message exchanges.

The IP flows between the MGW and CS for initialization of the data link for data/call setup and Telnet maintenance port are depicted in [Figure 3-7, “Media Gateway - Call Server Initialization and Maintenance Flows”](#) (p. 3-16).

**Figure 3-7 Media Gateway - Call Server Initialization and Maintenance Flows**



The Brick supports static mode of MGW initialization. In this mode, all parameters are configured in the GD gateway. The GD starts initialization by requesting application file `<binm***>` from the TFTP server, followed by downloading `<startemsg>`, and then establishing a data link (DL) with the CS. The Brick opens a pinhole for the DL.

RTP/RTCP pinholes are opened and closed dynamically (by monitoring the IPlink messages).

The Brick also permits maintenance requests from a Telnet (call server) to be passed to the MGW for debugging purposes for a specified period of time.

To protect the private IP space of the MGW behind the firewall zone, the Brick performs source Network Address Translation (NAT), converting the private IP address of the MGW GD board to a public IP address before the Uplink signaling message is routed to the CS. In turn, the Brick performs destination NAT for incoming signaling messages from the CS, mapping the public IP address of the MGW/GD board contained in the message to the private IP address of the MGW/GD board. Direct (one-to-one mapping) NAT is used by the Brick for IPlink protocol messaging between the MGW and CS. For more information about NAT, refer to the *Network Address Translation* chapter in the *SMS Policy Guide*.

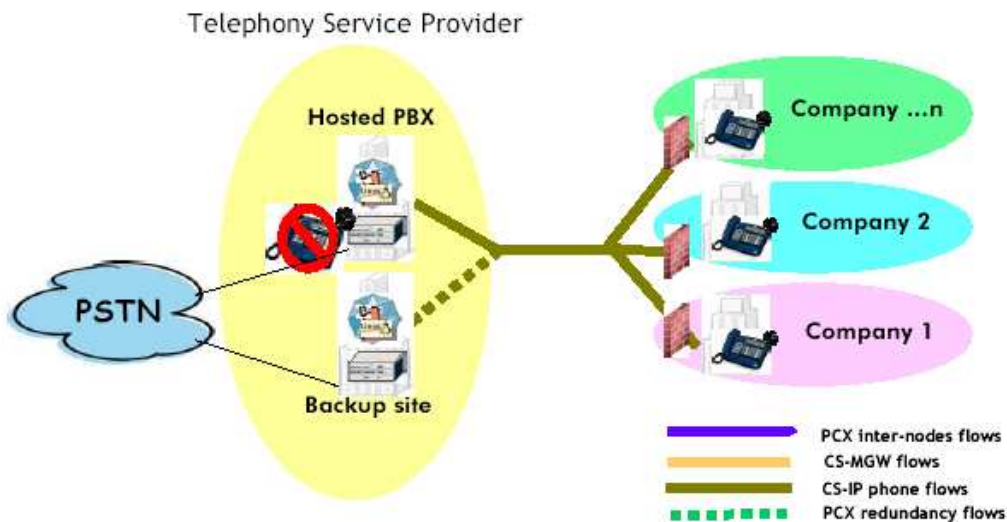
Before the data link has been established and ports identified for IPlink messaging, the Brick uses the Virtual Brick Address (VBA) for exchanges between the MGW/GD board and CS. Once the data link has been brought up, the Brick switches to the mapped IP address of the MGW/GD board.

Host groups of private and public IP addresses used by the Brick for NATing IPlink protocol message exchanges between the MGW and call server(s) are specified in an NOE application filter, which is activated within a TFTP application filter, and, in turn, assigned to a TFTP service group and defined in a rule of the Brick zone ruleset that is protecting the MGW. A separate Brick device is usually deployed to protect the CS, with its own set of rules for allowing/prohibiting TFTP traffic to/from the CS.

**Important!** When an NOE application filter is being used for MGW NATing, it cannot be used in another zone ruleset that has also been configured for NAT, since this filter has designated host groups that contain public and private IP addresses to be used by the Brick to perform NAT between the MGW and CS.

A Brick can also be deployed to serve as an ALG for NOE traffic if the other network elements (MGW, call servers) are “hosted” at the Telephony Service Provider’s premises and are connected to its Telephony Network (PSTN), providing full VoIP service in a multi-company environment, as depicted in [Figure 3-8, “Telephone service provider hosting private communication exchange \(PCX\) equipment with full VoIP deployment”](#) (p. 3-18).

**Figure 3-8 Telephone service provider hosting private communication exchange (PCX) equipment with full VoIP deployment**



In the above network configuration, VoIP traffic from different companies is being handled by the call server(s) and MGW equipment situated at the TSP's site, rather than in a secure environment behind a Brick in one company's network. To protect the private IP addresses of hardphones/softphones in outbound calls going outside of the Brick zone, the Brick device must be set up to perform source Network Address Translation (NAT), converting the private IP addresses of the source NOE devices in the outgoing TFTP message to a public IP address before the call is transmitted to the TSP's call server for routing to its destination/endpoint (for more information about NAT and setting up source address mapping, refer to the *Network Address Translation* chapter in the *SMS Policy Guide*).

The Brick device, acting as a NATing device, intercepts every phone TFTP request and sends, instead, a specially crafted TFTP read request to the TSP's call server, with an added sub-address byte (which varies between 1 and 255) to identify a particular IP hardphone/softphone device, for setting up the UA/NOE signaling link between the IP phone device and the call server. Up to 255 NOE (hard and soft) phones can be handled per public address by the Brick, and the Brick NAT function can be performed with multiple public IP addresses, using this sub-address byte indexing method, for deployments that must handle more than 255 IP hardphones/softphones.

The Brick device also transmits a unique MAC address for each IP phone device to the call server, which is matched against the original MAC address assigned to the phone device by the call server, as an added security measure.

□

## To Configure a Brick Device on the SMS

---

### When to use

Once you have addressed all of the preceding questions, you are ready to begin configuring the Brick device. To configure a Brick device, you have to display the Brick Editor and enter the configuration information requested. This information is then saved in the SMS database.

The basic information required to configure a Brick device is entered on the Brick tab of the Brick Editor.

The basic configuration can include any additional fields that you define for logical details or other information about the Brick. Refer to the section [“Adding user-defined fields when configuring a Brick”](#) (p. 3-19).

[“To configure basic information on the Brick tab”](#) (p. 3-23) explains how to configure the information on the Brick tab.

### Adding user-defined fields when configuring a Brick

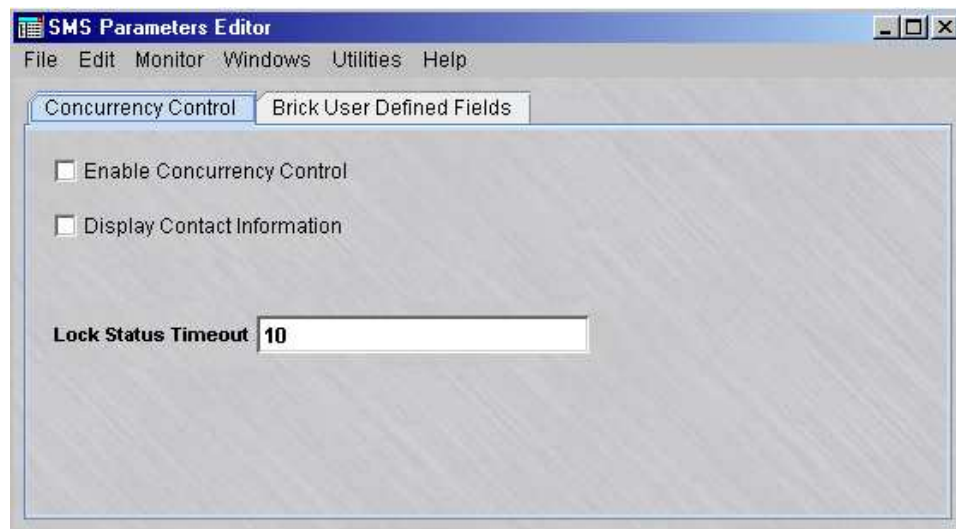
When configuring a Brick device on the SMS, certain basic key information is entered to uniquely identify the Brick, such as the Brick Name, IP address, associated SMS(s)/CS(s), Brick type/version, individual Brick ports/statuses, and a general textual description (if desired). This Brick data is saved and stored in the SMS database, and is later reported as part of the details about each Brick device in a Brick snapshot report, and on the various Brick Status windows of the Status Monitor. In addition to the basic configuration fields for a Brick device, the SMS allows you to create up to 5 user-defined, customized fields to label and store additional information about a Brick device, such as Serial Number, Rack Location, Contact Information, Provisioned status (yes/no), and so forth. Once created, these user-defined fields will appear on the Brick tab of the Brick Editor for input, unless they are disabled via the SMS Parameters window. Information can be then be entered into these fields when you configure each Brick device, and edited as needed. When user-defined fields are created, you have the option of choosing whether or not to display them on the All Bricks Status windows of the Status Monitor.

Complete the following steps to add user-defined fields to a Brick configuration:

- 
- 1 From the menu bar, select **Utilities > Edit SMS Parameters**

**Result** The SMS Parameters Editor is displayed (Figure 3-9, “SMS Parameters Editor” (p. 3-20)).

**Figure 3-9 SMS Parameters Editor**



The SMS Parameters Editor has two tab panels:

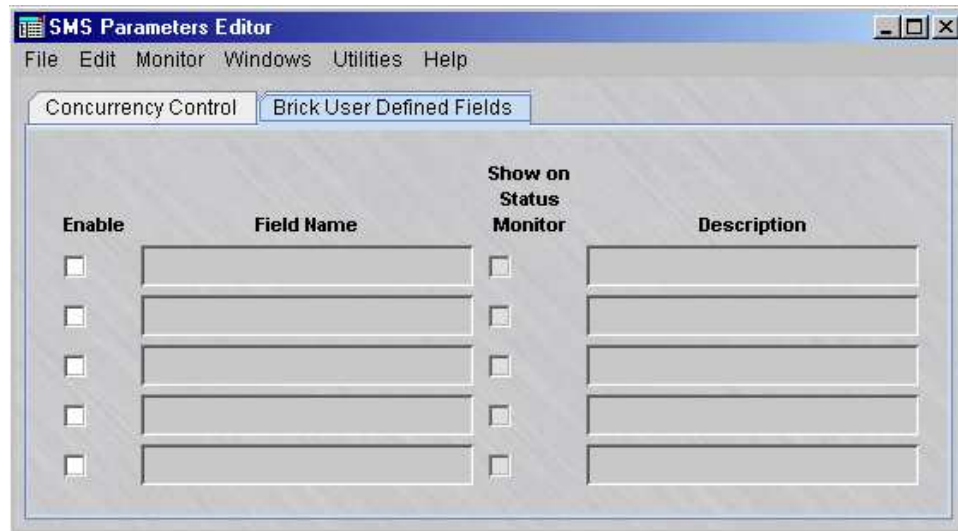
- Concurrency Control
- Brick User Defined Fields

---

**2** Click on the **Brick User Defined Fields** tab.

**Result** The Brick User Defined Fields panel of the SMS Parameters Editor is displayed (Figure 3-10, “SMS Parameters Editor (Brick User Defined Fields Tab)” (p. 3-21)).

**Figure 3-10 SMS Parameters Editor (Brick User Defined Fields Tab)**

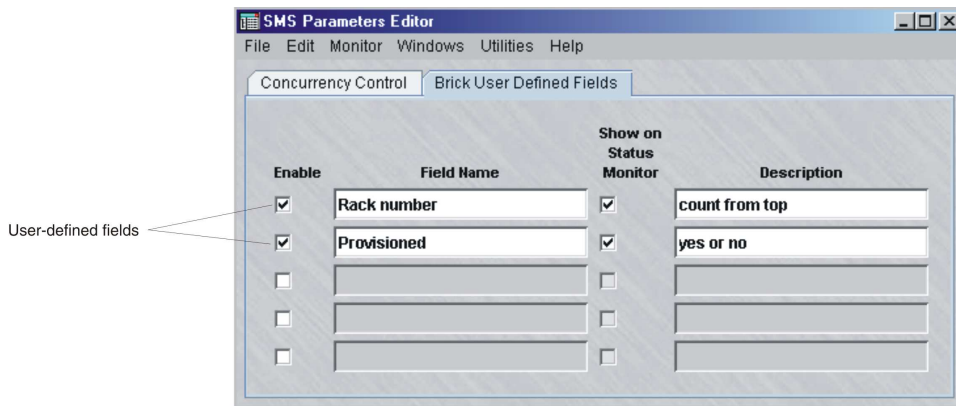


- 3 For each user-defined field, provision the following fields:
- **Enable**— click the checkbox to enable the user-defined field. When this checkbox is checked, the field becomes active and will appear on the Brick Editor when a Brick device is configured. To enable the field at another time, leave the checkbox blank. If the checkbox is left blank (the default), the new field is not displayed on the Brick tab of the Brick Editor when configuring a new Brick device.
  - **Field Name**— enter the name of the field (label) for the additional information that you want to record about a Brick device when it is configured. Some examples of fields that can be defined are: **Serial number, Rack Number, Contact information, Provisioned**. You can create any additional field(s) needed to track or record pertinent details about a Brick device. This field name/label will appear on the Basic tab of the Brick Editor when a new Brick device is configured or when you are editing the Brick device configuration using the Brick Editor. Information entered into each user-defined field on the Brick Editor will also eventually be reported and displayed on the Brick snapshot screen and the All Bricks Status windows of the Status Monitor. For information about how to view a Brick snapshot, refer to the “[To View a Brick Snapshot](#)” (p. 5-3) section in [Chapter 5, “Maintaining an Alcatel-Lucent VPN Firewall Brick™ Security Appliance Configuration”](#). For more information about the Status Monitor, refer to [Chapter 14, “Using the Status Monitor”](#).

- **Show on Status Monitor**— click this checkbox (place a check in it) if you want this field to be displayed on the All Bricks Status windows of the Status Monitor and a Brick Snapshot view of the configuration. By default, the field is not displayed on the Status Monitor windows or Brick Snapshot view.
- **Description**— enter additional textual description about the field, such as acceptable values that can be entered, expanded definition of the field, and so forth. This information is recorded internally and is not displayed on the Brick tab of the Brick Editor. This field is optional.

Figure 3-11, “SMS Parameters Editor (sample user-defined field entries)” (p. 3-22) shows an example of some user-defined field entries on the SMS Parameters Editor window.

Figure 3-11 SMS Parameters Editor (sample user-defined field entries)



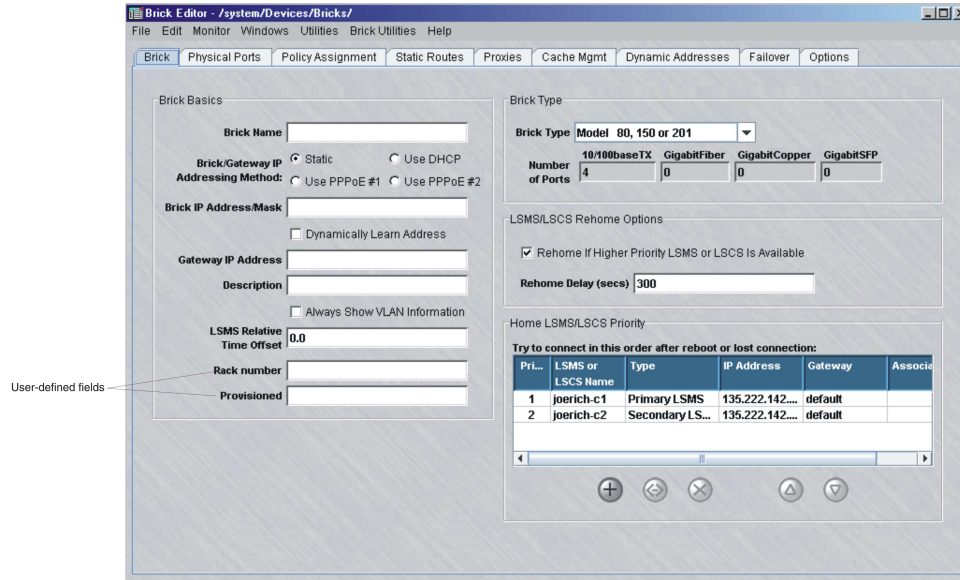
- 4 When you are done with creating new fields to be used when configuring a Brick device (up to 5 fields can be defined), select **Save and Close** from the File menu on the SMS Parameters Editor.

**Result** The field entries are saved and the SMS Parameters Editor is closed.

The field(s) that you defined will be displayed on the Brick tab of the Brick Editor to be used when configuring a Brick device (Figure 3-12, “Brick Editor (Brick Tab, sample user-defined fields for configuring a Brick)” (p. 3-23) shows the sample user-defined field entries that were just defined, on the Brick tab of the Brick Editor).



**Figure 3-12 Brick Editor (Brick Tab, sample user-defined fields for configuring a Brick)**



- To just view (not edit) the current user-defined field entries, from the menu bar, select **Utilities > View SMS Parameters**.

The SMS Parameters Editor is displayed. Click on the **Brick User Defined Fields** tab.

**Result** The Brick User Defined Fields tab of the SMS Parameters Editor is displayed in view-only mode. The user-defined field entries and settings are greyed out and cannot be changed.

END OF STEPS

### To configure basic information on the Brick tab

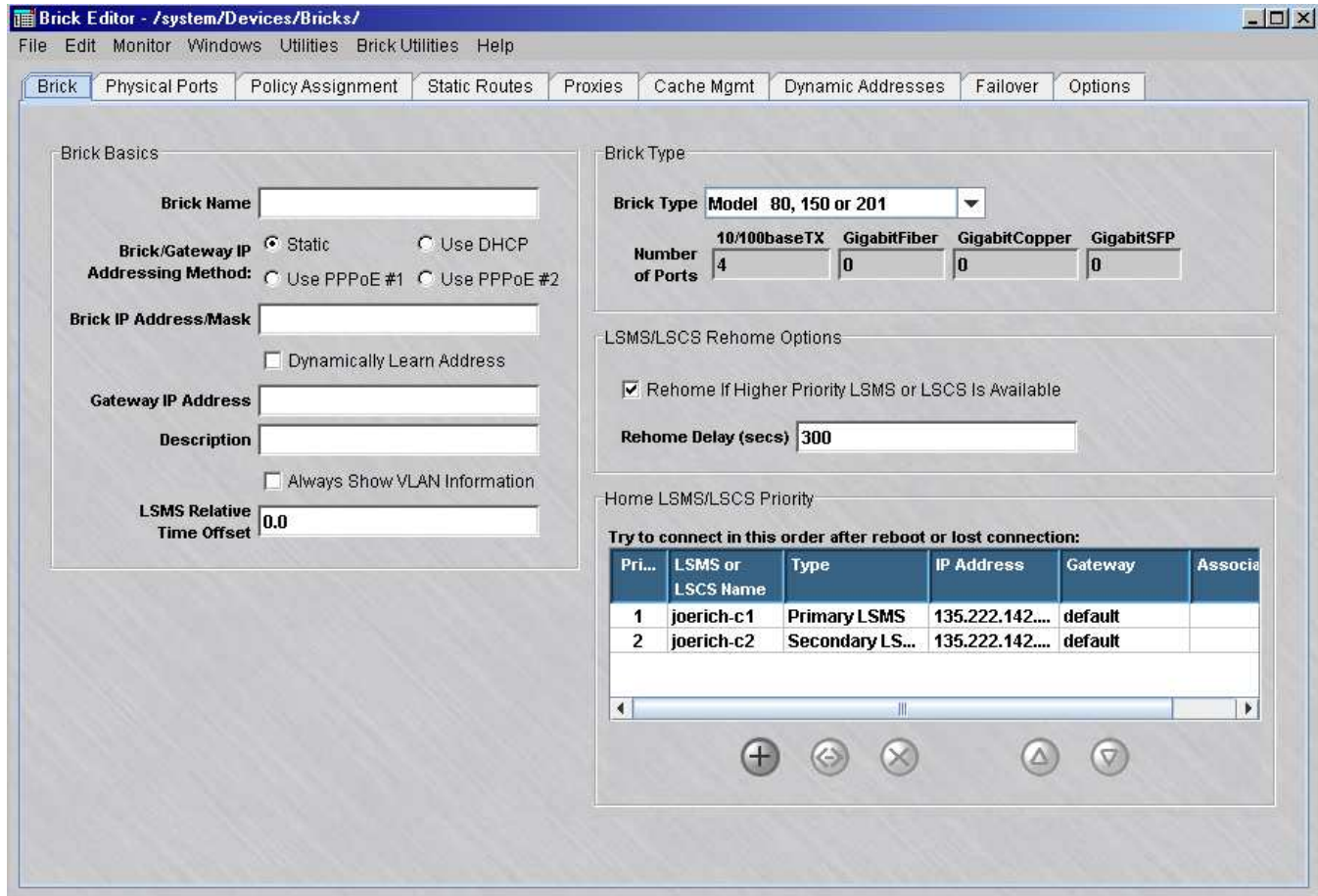
**Important!** You can define up to 5 additional fields for inputting basic configuration information about the Brick on the Brick tab. These fields may or may not be displayed, depending on the **Enable** setting on the SMS Parameters Editor. Refer to the previous section [“Adding user-defined fields when configuring a Brick”](#) (p. 3-19).

Complete the following steps to configure basic information about a Brick on the Brick tab:

- Open the folder of the group in which you want to put the Brick and open the **Devices** folder.

- Right-click the **Bricks** folder and select **New Brick** from the pop-up menu. The Brick Editor (Brick Tab) is displayed (see [Figure 3-13, “Brick Editor \(Brick Tab\)”](#) (p. 3-24)).

**Figure 3-13 Brick Editor (Brick Tab)**



- In the **Brick Name** field, enter the name to be used to identify this Brick. This field is required. The name of the Brick must be unique and can contain 1 to 62 lowercase alphanumeric characters.
- To assign a static IP address to the Brick and a static gateway that the Brick will use to talk to the SMS, click the **Static** radio button. In the **Brick IP Address/ Mask** field, enter both the IP address and subnet mask of the Brick device. In the **Gateway IP Address** field, you can also enter the address of a default gateway for the Brick device to contact the Primary SMS after it boots or loses connection (go to [Step 5](#)).

Alternatively, you may dynamically assign these addresses. This can be accomplished by either using DHCP or PPPoE. Your service provider can tell you if DHCP is required. If your network uses DSL lines installed on DSL modems that require the CPE side equipment to talk with the modem, then PPPoE is most likely required.

Click the **Using DHCP** radio button to enable DHCP. Click the **Using PPPoE#1** or **Using PPPoE#2** radio button to enable Point-to-Point Over Ethernet #1 (PPPoE#1) or PPPoE #2.

Checking any of the dynamic address radio buttons causes the **Dynamically Learn Address** box to be checked. The **Gateway IP Address** field will also be grayed out.

PPPoE #1 and #2 indicate two different PPPoE sessions that are configured on the Dynamic Addresses tab of the Brick Editor based on the following configurations:

- A single port on the Brick device connecting to a single PPPoE modem with a single PPPoE session (#1 or #2) active.
- A single port on the Brick device connecting to a single PPPoE modem with two PPPoE sessions (#1 and #2) active.
- Two ports on the Brick device connecting to a different PPPoE device.
- A single port on the Brick device connecting to two PPPoE devices simultaneously.

Click the **Dynamically Learn Address** checkbox if:

- The Brick device itself does not acquire its management address dynamically.
- The Brick device is in a home office / branch office setting.
- The service provider grants only a single IP address which is updated periodically.
- There is a device somewhere between the Brick and the SMS that performs a Network Address Translation (NAT) function on the Brick address using an address that may change over time. This is often (but not always) a low end router immediately in front of the Brick.
- The router has been specifically configured to allow the following inbound connections from the SMS to the Brick:
  - TCP 910 (administrative channel and asynchronous commands)
  - UDP 1024 (reflection channel for SMS-based user authentication proxy)

If the **Dynamically Learn Address** checkbox is checked, the SMS does not attempt to contact the Brick device until it has made first contact with the SMS.

The SMS automatically assigns the address and mask to each of the Brick physical ports. You can view this on the Physical Ports tab of the Brick Editor. If the ports are not changed, the Brick functions as a "pure" bridge on all ports.

To change the IP address and subnet mask for any of the ports, display the Brick Ports Editor. If you change one or more ports, the Brick routes packets on those ports. (It may also be necessary to add static routes to reach other subnets.) For more information, refer to the “[Static Routes](#)” (p. 4-32) section in [Chapter 4, “Configuring Alcatel-Lucent VPN Firewall Brick™ Security Appliance Ports”](#).

Once the configuration is saved, the mask will be dropped from this field. It still can be seen by displaying the Brick Ports Editor.

- 
- 5** In the **Gateway IP Address** field, enter the IP address of the device (usually a router) that will serve as the *default static route* to the Brick device at boot time. This is where the Brick will send all traffic not destined for a local subnet. Once a Brick policy has been applied, if there is a default route in the Static Routes tab on the Brick, it will override the value in this field. Static routes to a particular SMS can be overridden in the Home LSMS/LSCS Priority portion of the Brick Editor.

If the SMS is on a different subnet than the Brick, you have to enter the IP address of the router that the Brick uses to communicate with the SMS in this field. This is the only route that the Brick can use to contact the SMS when the Brick first boots. The gateway address must fall within the IP range of one of the Brick ports.

If you enter a conflicting route in the Static Routes Table, it may override this **Gateway IP Address** field (see Important Note below).

**Important!** The default gateway on the SMS should be set to the address of whatever device is the “next hop.” If the SMS is directly connected to the Brick, use the Brick IP address for the gateway. If there is a router between the SMS and the Brick, use the router IP address for the gateway on the Brick.

If the SMS host is running *Windows*® or *Vista*®, make sure that the *Default Gateway* field is properly set in the TCP/IP protocol properties.

If the SMS host is running *Solaris*® or Linux, make sure that the */etc/defaultrouter* setting is correct.

- 
- 6** In the **Description** field, enter a brief description of this Brick. The description is optional. It can contain up to 80 characters (letters, numbers and certain special characters).

**Important!** *ALWAYS SHOW VLAN INFORMATION*

If you will be configuring the Brick to recognize, forward and filter VLAN traffic, you must check the **Always Show VLAN Information** checkbox (see Figure 3-5). This will add two new tabs (*VLAN/IP Assignment and Partitions*) to the row of

tabs in the Brick Editor, and it will add a number of VLAN-related columns to the table in the Physical Ports tab. It will also add several VLAN fields onto the Brick Ports Editor and Policy Assignment Editor.

Once you check this checkbox and save the configuration, you will not be able to return to the pre-VLAN view. The VLAN/IP Assignment tab and the changes to the Physical Ports tab will remain in effect, regardless of whether you actually make use of the VLAN feature or not.

If you plan to use the VLAN feature, turn to *Chapter 6. Configuring VLANs on Bricks* for an explanation of how to configure the Brick's physical ports and assign policies to the ports to handle VLAN traffic.

---

**7** The **SMS Relative Time Offset** field, is only used if:

- The Brick is in a different time zone than the SMS
- AND-
- You need to add time and day restrictions to the rules.

Enter the time offset value in hours, with a "+" or "-" to indicate whether the time zone for the Brick is "ahead" or "behind" the time on the SMS.

For example, if the Brick is in Los Angeles and the SMS is in New York, the Brick is three hours behind the SMS. The offset value is "-3.0". Similarly, if a Brick is in a time zone 8 1/2 hours ahead of the SMS, the offset is "+8.5".

The SMS and Brick synchronize their times once an hour.

For additional details, refer to the *To Add Time and Day Restrictions to a Rule* procedural section in the *SMS Policy Guide*.

---

**8** In the **Brick Type** field, select the Brick device model from the drop-down list. The options are:

- Model 20 or 50
- Model 150
- Model 350
- Model 700 (0/0/2/6)
- Model 700 (0/0/8/0)
- Model 1100 (7/0/13)
- Model 1100 (7/4/1)
- Model 1100 (7/6/1)
- Model 1200 (0/0/14/6)
- Model 1200 (0/0/8/2)

- UNSUPPORTED - Model 300
- UNSUPPORTED - Model 500
- UNSUPPORTED - Model 1000 (3/4/0)
- UNSUPPORTED - Model 1000 (5/4/0)
- UNSUPPORTED - Model 1000 (7/2/0)
- UNSUPPORTED - Model 1000 (9/2/0)

**Important!** The Brick models labeled as **UNSUPPORTED** in the Brick Type drop-down list have been discontinued and are no longer available for purchase from Alcatel-Lucent. Alcatel-Lucent does not warrant that the SMS software will work on Brick models labeled as **UNSUPPORTED**.

When you select the Brick device model type, the **Number of ports** section of the Brick tab (which is read-only) displays the number of configurable 10/100baseTX, Gigabit Fiber, GigabitCopper, and GigabitSFP ports available for that Brick model type.

Refer to the *User's Guide* of the respective Brick model for complete details about the hardware configuration.

- 
- 9** The **Home SMS/LSCS Priority** panel shows a list of each SMS and CS that can be used to manage this Brick device. Each entry in the list has a priority number. The Brick device uses the priority number to decide which SMS/CS to contact so that it can perform logging and user authentication. Initially, the Brick device attempts to contact the priority 1 SMS/CS. If it cannot contact the priority 1 SMS/CS, it tries to contact the priority 2 SMS/CS, and so on.

The SMS that you are logged into when you create a Brick is automatically configured as the *priority 1* SMS, and the Brick is said to be *homed* to this SMS. All Primary and Secondary (if any) SMSs are automatically included in the list. Compute Servers (if any) may be manually added. The list may contain up to five entries. Any SMS/CS in the list can manage the Brick device, regardless of where the Brick device is currently homed.

Care should be taken when assigning Brick devices to Compute Servers. A Compute Server is dependent on its associated SMS for database access, so if the associated SMS goes down, so will its Compute Server(s). For this reason, if a Brick device is configured with an SMS and a CS, it is recommended to choose a CS that is associated with a different SMS than the one it is associated with, if possible.

- 10 To change the priority of the management SMSs and/or CSs for the Brick device in the **Home SMS/LSCS Priority** panel, select the server (SMS or CS) and click the **Down** (▼) button to lower its priority of connectivity with the Brick, or select the server and click the **Up** (▲) button to raise its priority of connectivity with the Brick. The SMS priority can be changed when you are initially configuring the Brick.
- 11 To add an SMS or CS to the **Home LSMS/LSCS Priority** management priority queue for the Brick device, click the **New** (+) button.

### Result

The LSMS/LSCS Priority Editor is displayed (Figure 3-14, “LSMS/LSCS Priority Editor” (p. 3-29)).

**Figure 3-14 LSMS/LSCS Priority Editor**



Click the down arrow to the right of the **LSMS/LSCS Name** field to display a drop-down list, and select a new SMS or CS to add to the management priority queue for this Brick device.

The **LSMS/LSCS IP Address** field normally displays the private IP address to be used by the Brick device to contact this SMS or CS after it reboots or it loses connection with the SMS/CS. To specify the public IP address for the connection, click the down arrow next to this field to display a drop-down list, and select the public IP address (if one has been entered) for the SMS/CS.

To specify a different public IP address to be used by the Brick device to contact this SMS/CS after reboot or loses connection with the server, other than the IP address already defined (for example, the Virtual Brick Address (VBA) of a Brick device protecting the SMS if Network Address Translation (NAT) is being used), click the **Use modified address** checkbox and enter an IP address in the field to the right of the checkbox.

If a gateway device other than the one specified in the **Gateway IP Address** field is required for the Brick to contact this SMS/CS, click the **Use modified gateway** checkbox and enter the address in the field to the right of the checkbox.

After specifying the entry(ies), click the **OK** button.

- 
- 12** To remove an SMS or CS from the Brick homing priority list, select the server and click the **Delete** (X) button.
- 

- 13** If a Brick device is currently connected to a lower priority SMS/CS, and connectivity is lost, and a high priority SMS/CS becomes available, the Brick device will automatically rehome to the higher priority SMS/CS if the **Rehome If Higher Priority LSMS or LSCS Is Available** checkbox is checked.

If this box is not checked, the Brick device will remain homed to the lower priority SMS/CS until one of the following occurs:

- The Brick device is manually rehomed to another SMS/CS
- The Brick device is rebooted
- The Brick device loses contact with the SMS/CS(s) (if, for example, the services on that SMS/CS are restarted)

**Important!** Brick log records are sent to the SMS to which the Brick device is currently connected. If the Brick loses connectivity to its priority 1 SMS/CS, all new log records will be sent to the priority 2 SMS/CS. To keep the majority of the log records in one place (such as the priority 1 SMS), it is recommended to keep the **Rehome if Higher Priority LSMS or LSCS** checkbox checked.

---

- 14** The **Rehome Delay (secs)** field is used in conjunction with the **Rehome if Higher Priority LSMS or LSCS** checkbox. It specifies the amount of time that the Brick will wait (in seconds) before it rehomes to the higher priority SMS/CS when it becomes available. The default is 300 seconds.
- 

- 15** Display the File menu and select **Save**.

You have just entered the basic information necessary to activate a Brick device. However, there are certain optional configuration parameters you should consider before activating the Brick. Refer to the [“Configuration options” \(p. 3-32\)](#) section for instructions on how to configure these optional parameters.

**Important!** If you open the Monitor menu and select **Status Overview** to display the Status Monitor, the Brick device being activated appears in the Brick Status graph as *LOST*. Once the activation process is complete, the status changes to *UP*, indicating that the Brick and the SMS are communicating.



LOST and CONTACTED alarms are generated after a transition from CONTACTED to LOST or from CONTACTED to LOST back to CONTACTED.

END OF STEPS

---

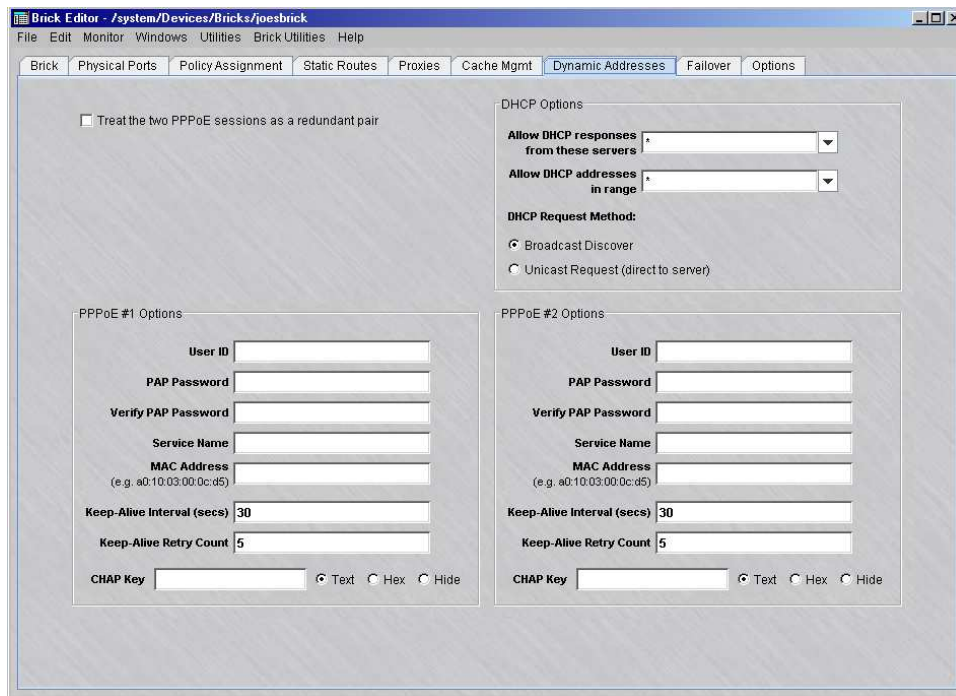
## To configure dynamic addressing options

Complete the following steps for configuring dynamic addressing options for the Brick device

---

- 1 Click **Dynamic Addresses** to display the Dynamic Addresses tab of the Brick Editor (Figure 3-15, “Brick Editor (Dynamic Addresses Tab)” (p. 3-31)).

**Figure 3-15 Brick Editor (Dynamic Addresses Tab)**



- 2 Click the **Treat the two PPPoE sessions as a redundant pair** checkbox to indicate that wherever a PPPoE (#1 or #2) session is used in the Brick configuration, the one actually used is the first session that becomes available. Both PPPoE sessions are kept open at all times; only one session is used at a time.

When this box is checked, the use of PPPoE #1 or PPPoE #2 is equivalent everywhere, except in the VLAN assignment and interface assignment. For example, using PPPoE #1 as a VBA and PPPoE #2 as the target of a static route means the same thing. The Brick will use the address/route associated with the link that is currently selected as active.

.....

3 If you are acquiring any Brick device address via DHCP, you may need to change one or more of the following settings:

- **Allow DHCP responses from these servers** - This allows you to select an IP address or host group list of IP addresses that the Brick will allow to serve its requests. By default, the Brick will accept a reply from any IP address.
- **Allow DHCP addresses in range** - This allows you to restrict the addresses that the Brick will accept for its own addresses. It prevents someone from spoofing the DHCP reply and, for example, assigning an address that really belongs to another interface. By default, the Brick will accept any IP assignment.
- **Broadcast Discover/Unicast Request(direct to server)** - Typically, DHCP operates in **Broadcast Discover** mode; this option should remain selected. However, in a sensitive environment where the DHCP request addresses should not be broadcast all over the network, select **Unicast Request (direct to server)**, which invokes the Brick to solicit in sequence every IP address specified in the **Allow DHCP responses from these servers** field. This list could be extensive.

.....

4 Configuration options for setting up the PPPoE #1 and #2 sessions are displayed in the bottom portion of the tab.

All fields are optional except the **Keep Alive Interval (secs)** and **Keep-Alive Retry Count** fields per session. If a User ID is entered, either a **PAP Password** or **CHAP Key** is required. The **MAC Address** field identifies which physical device to use, and must be entered as six pairs of hex characters, delimited by colons. The **CHAP Key** can be entered as text or hex characters.

.....

END OF STEPS

.....

## Configuration options

Once the information requested in the Brick tab has been entered and saved, the Brick can be activated. However, before you activate the Brick, you should decide whether or not to enable certain optional features found in the Brick. These options, which are enabled from the Options tab of the Brick Editor, are the same, regardless of whether you have a Primary SMS or redundant SMS pair. In addition, the Options tab allows

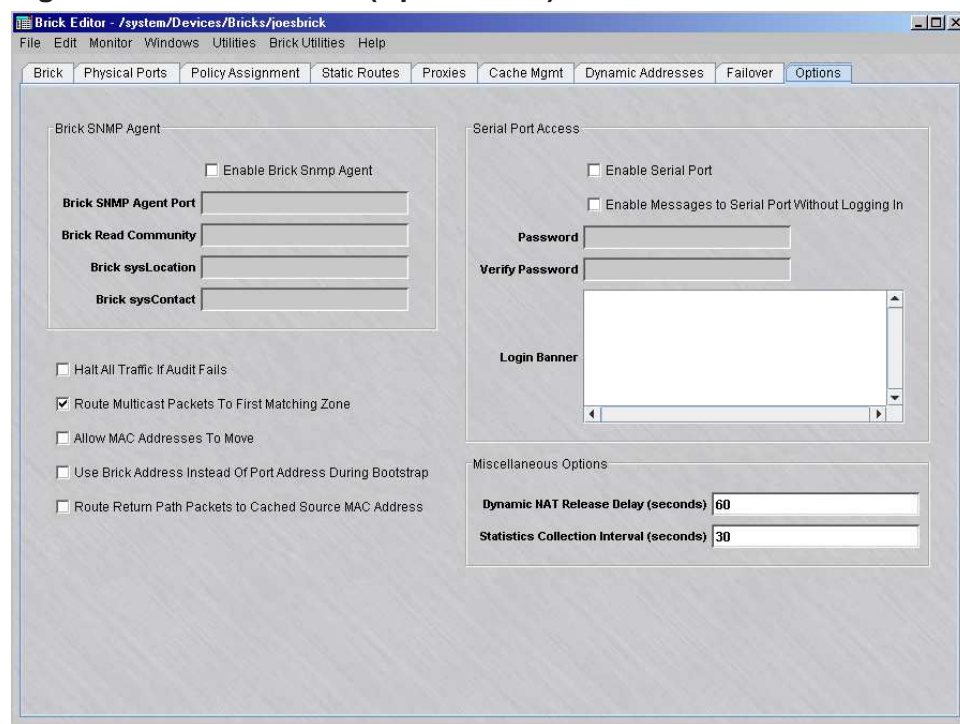
you to create a password that you can use to log into the serial port of the Brick. The Options tab also allows you to enable Brick failover, if this Brick is part of a failover pair.

Complete the following steps to configure options on the Options tab:

- 1 Click **Options** to display the Options tab of the Brick Editor (Figure 3-16, “Brick Editor (Options Tab)” (p. 3-33)).

**Result** The Options tab of the Brick Editor is displayed (Figure 3-16, “Brick Editor (Options Tab)” (p. 3-33)).

**Figure 3-16 Brick Editor (Options Tab)**



- 2 Configure the Brick SNMP Agent options if the SNMP on the Brick feature is being used (for details about SNMP and how to configure these options, refer to [Chapter 15, “Simple Network Management Protocol \(SNMP\)”](#)).

- 3 Click the options checkboxes that you want to enable.

The following explains what each checkbox accomplishes.

1. **Halt All Traffic If Audit Fails**

This checkbox determines how the Brick responds if it loses communication with the SMS and cannot perform its logging function. The following explains:

- If the checkbox is *unchecked*, the Brick continues to permit traffic through, and will fully enforce all security policies, but will perform no auditing.
- If the checkbox is *checked*, the Brick stops all traffic until communication with the SMS is re-established.

The SMS and Brick actively maintain a heartbeat on the audit channel, and can detect failures almost immediately.

By default, this checkbox is unchecked, which means traffic will continue in the event of loss of communication with the SMS. To stop all traffic, click once to check the checkbox.

## 2. **NOC Gateway**

This checkbox has to be checked if this Brick is to serve as the NOC Gateway Brick to manage routers securely.

To be the NOC Gateway, this Brick has to be directly connected to the SMS, and it has to be the endpoint for the management tunnels that the SMS uses to manage routers securely.

## 3. **Route Multicast Packets to First Matching Zone**

Normal (unicast) traffic is addressed to a specific host. The Brick determines which zone that host is a member of, and applies that policy. Multicast traffic may be delivered to multiple hosts. If more than one zone has been assigned to a port, hosts in each zone may receive the traffic. If one zone has a rule passing such traffic and another zone has a rule requiring it to be dropped, there is a conflict. This checkbox determines how the Brick resolves such conflicts. The following explains:

- If this checkbox is *unchecked*, the Brick processes multicast sessions in all zones assigned to the port. This means there must be a rule allowing the session in each of these zones for the session to pass through the Brick, even if the session is only intended for one of the zones.
- If this checkbox is checked, the Brick processes multicast sessions in individual zones. This means there must be a zone that protects the multicast address — either explicitly or with the wildcard asterisk. (Refer to [“To Assign a Security Policy to a Port”](#) (p. 4-9)).

## 4. **Allow MAC Addresses to Move**

This checkbox has to be checked to allow MAC addresses to float from one Brick port to another. Allowing MAC addresses to float means that when a Brick that has a MAC address associated with a particular port receives an Ethernet frame *from that same MAC address on a different port*, it automatically moves the MAC address assignment and associated firewall sessions to the new port, and marks that MAC entry with the time it was assigned.

### 5. Use Brick Address Instead of Port Address During Bootstrap

This checkbox allows you to specify that the Brick should use the address specified in the Brick IP Address/mask field to communicate with the SMS while loading the policy. This is sometimes required when the Brick has only one (public) address for management and for the VBA, but the interfaces on the Brick are all assigned to be private in order to enable more traffic (such as DHCP) to be bridged. After the Brick has loaded its policy from the SMS, this checkbox has no further effect. This checkbox is not available if the **Dynamically Learn Address** checkbox is checked and the **Brick/Gateway IP Addressing Method** is a static IP address. To enable this feature, you have to check this checkbox, and then you have to set the Brick IP address to the VBA of the Brick zone ruleset assigned to the port that is serving as the tunnel endpoint (see "How to Configure a Physical Port" on page 4-1).

### 6. Route Return Path Packets to Cached Source MAC Address

This checkbox affects how the reverse direction packets are routed in the firewall (in other words, the packets that are routed from the session destination back to the session originator).

This checkbox *only* affects packets that are not bridged. Packets that are bridged are routed according to the destination MAC address and VLAN in the packet. When the checkbox is not checked and the traffic is routed, then the return packets are routed using the ARP table and, possibly, the static route table. When the checkbox is checked and the traffic is routed, then the Brick simply routes the return traffic back to the same interface, VLAN, and MAC address from which the first packet in the session arrived.

However, there is an exception to this handling of return packets. If the Brick has detected that the MAC address should not be used for this purpose (for example, it is a VRRP or HSRP router, then the MAC address is not used for this purpose (regardless of the checkbox setting). The Brick makes this determination by looking at the inner and outer MAC addresses on ARP packets, and, if they are different, marks the outer MAC address as being a VRRP/HSRP MAC address.

Subsequently, the Brick does not return packets back these devices. Unfortunately, experience has shown that this test does not work for all routers.

When this checkbox should be used:

In most cases, the checkbox should be left unchecked. The checkbox should be checked only if traffic is being routed (using static routes) and one of the following applies:

- There is no static route that takes traffic back to the source address
- A session with a particular IP address may arrive at the Brick from more than one router or interface and there is a need to have the return traffic routed the same way

- 
- 4 If you intend to use the Brick serial port to access the out-of-band (OOB) command line interface, click the **Enable Serial Port** checkbox, and enter a password twice — once in the **Remote Password** field and again in the **Verify Password** field. The password can be from 6 - 72 characters (letters and numbers). The password is case sensitive, so capitalization must be consistent.

To access the command line interface, you can connect a terminal or a modem to the Brick serial port. Refer to the *SMS Tools and Troubleshooting Guide* for instructions on how to log into the Brick and use the OOB command line interface. (Serial port parameters are 115,200 baud, no parity, 8 data bits and 1 stop bit.)

Note that for a Model 50 Brick, flow control for the serial port should be set to **None** or **Xon/Xoff** instead of **Hardware**. The flow control setting can be configured or modified by connecting your PC to the Brick and running a terminal emulation program (such as HyperTerminal) that is used to set up a local serial port connection. For instructions on how to set up a local serial port connection and configure the flow control setting, refer to the *Set Up a Direct Serial Port Connection* appendix in the *SMS Tools and Troubleshooting Guide*.

If the serial port is enabled, then the console command line will also require the password to log in and access its functions. If the serial port is disabled (and hence no password is given), then the console command will not require the password.

The **Enable Messages to Serial Port Without Logging In** checkbox allows Bricks to send messages to the serial port without having to log in first.

To add a login banner to be displayed when logging into the Brick via the serial port, refer to the procedure [“To Activate a Login Banner on the Brick Serial Port Console”](#) (p. 4-41) in Chapter 4, “Configuring Alcatel-Lucent VPN Firewall Brick™ Security Appliance Ports”.

---

**5** In the **Miscellaneous Options** portion of the window, provision or change the following timer settings as needed:

- **Dynamic NAT Release Delay (seconds)**— this field allows you to set the amount of time to wait before releasing a dynamically assigned IP address back to the Dynamic NAT pool after all outbound sessions have terminated and no new outbound sessions have been created for this period of time. The default value is **60** (seconds). A value of zero (**0**) causes the mapped IP address (and any remaining inbound sessions) to be released immediately after the last outbound session has terminated.

For more details about the Dynamic NAT feature, refer to the *Network Address Translation* chapter in the *SMS Policy Guide*.

- **Statistics Collection Interval (seconds)**— this field allows you to set the reporting interval for collection of Proactive Monitoring (ProMon) statistics. The default is **30** (seconds). You can change or reduce the reporting interval for this Brick to less than 30 seconds. The value entered must be greater than zero (**0**). For more information about Brick Proactive Monitoring parameters that are logged by the SMS or Compute Server, refer to the *SMS Reports, Alarms, and Logs Guide*.

---

**6** When you are finished, display the File menu and select **Save**.

END OF STEPS

---



# Brick Device Failover

---

## Overview

Brick device failover is based on a simple model: two Brick devices, each connected to the same set of LANs, can share the same identity, including IP address and name. The two Brick devices are administratively treated as one. The first Brick device to boot becomes the active Brick device and behaves like a normal Brick device. The other Brick device is the standby, and waits to take over should the active Brick device fail.

Brick device failover can be set up to be invoked automatically, or it can be performed manually from the SMS GUI or via the Brick device command line interface (CLI).

## How Brick device failover works

In a Brick device failover configuration, both Brick devices issue heartbeats, or keepalive messages, at regular intervals to indicate their operational “health” and the integrity of each of their Ethernet links. (For additional details, refer to the [“Brick device failover protocol and heartbeats”](#) (p. 3-38) section.) A lack of incoming heartbeat messages from the Brick device itself or one of its links can invoke failover to the standby Brick device.

The active Brick device may also yield to the standby if it detects that the standby has better LAN connectivity, or the other Brick is designated to be the *Primary* Brick device in a failover pair. For details about designation of a Primary Brick device, refer to the [“Primary Brick device”](#) (p. 3-40) section. Failover Brick device pairs employ state-sharing to maintain sessions despite the failure of one Brick device in the pair.

In addition to heartbeat messages issued by the Brick device, the SMS provides an option to configure the active Brick device to ping a router or other device on the LAN, at a specified time interval and frequency, to determine if it still has LAN connectivity. In the event that no response is received for the specified number of iterations, the currently active Brick device will initiate a failover if the standby Brick is operational and has link integrity. The standby Brick device must be operational for at least 30 seconds before initiating a failover (to allow state-sharing to occur).

## Brick device failover protocol and heartbeats

Both the active and standby Brick devices regularly issue heartbeats. The active Brick device generates ten heartbeats per second for each link. The standby Brick device is adaptive. During changing conditions, the standby beats once; during stable times, it beats once every 800 milliseconds per link.



Heartbeats serve several functions:

- The heartbeat indicates the presence of an active Brick device. A lack of incoming heartbeats causes the standby Brick device to become active.
- Heartbeats allow Brick devices to determine the relative health of each of their Ethernet links. Without heartbeat messages or some other configured flow, the Brick devices would have to rely on simple link integrity to give a local view of the health of their ports.
- Heartbeats allow Brick devices to share health, status, and priority information with each other. This information is used to make failover and state-sharing decisions.
- Heartbeats also verify that the corresponding ports on each Brick device are connected to the same LANs, essentially for implementing security policies that are based on connection to specific ports.

Heartbeat messages carry authentication and anti-replay information to prevent a local host from shutting down a Brick device by generating forged or previously recorded heartbeats.

### Brick device failover states

In terms of operational status and failover response, a Brick device can be in one of the following states:

- *Active*— The operational status is up, has link integrity with its LAN connections, and is available for carrying traffic. Only one Brick device in the failover pair can be in the active state at any time. The currently active Brick device owns the virtual MAC address of the failover pair.
- *Standby*— The Brick is device waiting to take over should the currently active Brick device fail or lose connectivity. This is also the initial operational state on boot-up of the Brick device.
- *X-Wired* — Each of the Ethernet ports of each Brick device must each be assigned to the same LANs. When this is not the case, the standby Brick device goes to the cross-wired state until the situation is resolved. Failover will not work while the two Brick devices are in the cross-wired state.

The `display failover` command, issued from a local or remote Brick device console, can be used to show the failover status of a specific Brick device. Refer to the *SMS Tools and Troubleshooting Guide* for details on the Brick device CLI and the `display failover` command.

### Brick device redundancy for failover

The Brick device failover or redundancy feature has the following characteristics: two Brick devices can be deployed as a failover pair. The Brick devices are identically configured, and share a single IP address.

The Brick device that boots first becomes the *active* Brick device. The other Brick device remains in *standby* state, ready to take over should the active Brick device fail or yield to it. The active Brick device reports to the SMS on the state of the failover pair. The standby does not have an IP address and therefore cannot report its own state.

When a Brick device that is configured for failover boots, there is a delay while it listens to be sure it does not have a counterpart that is already active. If it finds that the other Brick device in the failover pair to be active, it remains in standby state.

To create a failover pair, the second Brick device is attached to the same LAN as the first one. Each interface on the second Brick device must be attached to the same LAN as the matching interface on the first Brick device.

Both Brick devices must be installed from the same floppy, using the same name, configuration, and authentication credentials. The failover pair is configured as a single Brick device in the Brick Editor, with the **Enable Brick Failover** option checked on the Failover tab. If both Brick devices are not created from the same floppy, they perform as independent devices and form Layer 2 loops.

### Primary Brick device

One of the Brick devices in a failover pair can be designated as the *Primary* Brick device. The Primary Brick device will be the active Brick device at all times, unless it has experienced some failure or has lost its LAN connectivity. If the Primary Brick device is currently in standby state, and the currently active Brick device detects that the Primary Brick device has been up and running and has LAN connectivity, the active Brick device will initiate failover to the designated Primary Brick device after a provisionable Failback Delay time period has elapsed.

The exception to the above is if the Primary Brick initiated failover to the secondary Brick as a result of an IP tracking failure. In this case, the currently active Brick (the secondary Brick) will *not* yield control back to the Primary Brick after the Primary Brick reboots, unless some other failure occurs, IP tracking recovers and then fails again, or the failover is initiated manually.

### Link health monitoring

Each Brick device in the failover pair continually monitors the health of its network interfaces.

Each Ethernet link can be in one of the following states:

- **Down**— No link integrity.
- **Up - no data**—Link integrity exists between the active and standby Brick in a failover pair but the active Brick is not receiving any frames. Also indicates that the active and standby Brick are not connected to the same switch or hub.
- **Receiving**— Receiving non-heartbeat frames.

- **Unverified** — Receiving heartbeats that do not acknowledge the heartbeats sent on this link.
- **Verified**— Receiving heartbeats that do acknowledge the heartbeats sent.  
In a Brick failover pair, if the standby Brick is powered down, the ports showing a state of **Verified** switch over to a state of **Receiving**
- **Disabled**—Not capable of receiving frames.

Note that the heartbeats provide a measure of Brick-to-Brick health checking. The unverified state can come about if the Ethernet link is partially broken and is passing traffic in one direction only.

The default wait period before Brick device failover takes place as a result of a link failure is configured in the **Yield Time** field. If link integrity is restored before the end of the configured wait period, failover is cancelled.

### LAN connectivity

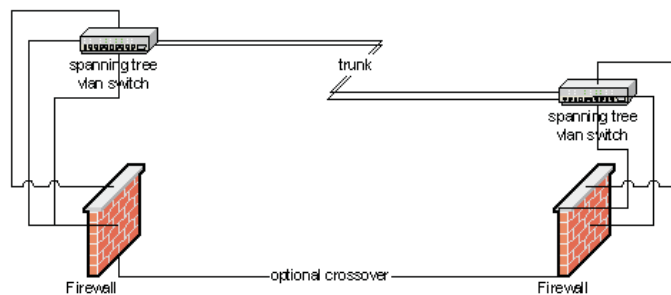
Any hub or switch can be used to implement the LANs. Note however, that for optimum failover performance, any switches used should be IEEE 802.1 Spanning Tree-enabled.

Note that if switches are used without enabling spanning tree, after a failover occurs, these switches will continue to send traffic out on the link where the active Brick device used to reside until packets are detected arriving from the opposite direction. This could potentially result in a long period of network inactivity

### Figure: physical Brick device failover topology

Figure 3-17, “Example of Brick Device Failover Physical Topology” (p. 3-41) shows a physically connected redundant Brick device pair that can be configured for failover.

Figure 3-17 Example of Brick Device Failover Physical Topology



No dedicated link between the Brick devices is required. However, a dedicated link is recommended for state-sharing, and can be added, if there is a spare port available. Providing such a link improves redundancy and tolerance of extremely heavy load.

## To Set Up Brick Device Failover

---

### When to use

Use this task to set up Brick device failover to be invoked automatically.

### Before you begin

Before you begin this task, make sure that you have cabled the Bricks to the network in a failover configuration.

Be aware that policies will not be loaded unless this procedure is performed in the proper order. If the active Brick device fails and the SMS is unreachable, the newly active Brick device may apply an outdated set of policies to network traffic. In a new installation, the failover Brick device may have no policies loaded.

### Task

Complete the following steps to set up Brick device failover to be invoked automatically:

- 
- 1 Configure the first Brick device in failover pair by performing Steps 1 to 5 of the task [“To Configure a Brick Device on the SMS”](#) (p. 3-19).

Make sure that the following fields are completed:

- **Brick Name**
  - **Brick IP Address**
  - **Gateway IP Address**
- 

- 2 Click **Options** on the Brick Editor.

**Result** The Options tab of the Brick Editor is displayed ([Figure 3-16, “Brick Editor \(Options Tab\)”](#) (p. 3-33)).

---

- 3 Click the **Allow MAC Addresses to Move** checkbox. This field is a security measure that prevents MAC addresses for local clients from being seen on more than one Brick interface. If this option is checked, the Brick will allow a MAC address to be moved from one interface to another.
- 

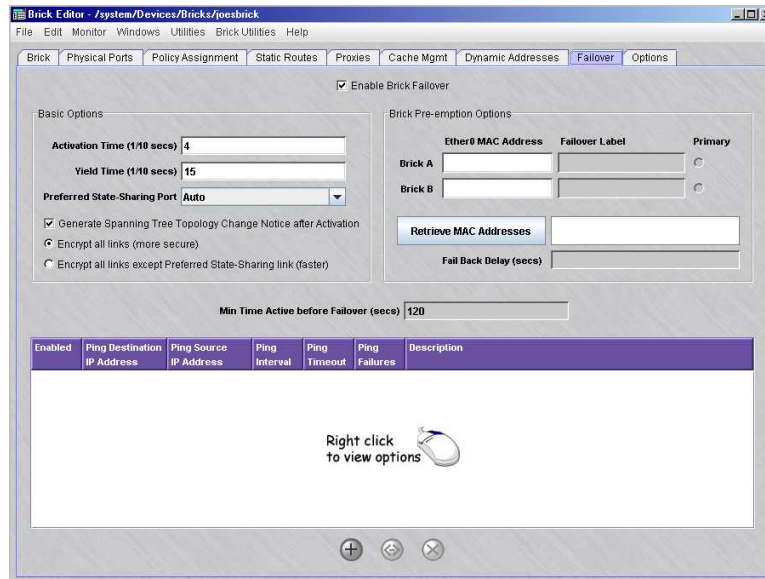
- 4 Click **Failover** on the Brick Editor.

**Result** The Failover tab of the Brick Editor is displayed.

- 5 Click the **Enable Brick Failover** checkbox to enable the Brick Failover feature.

**Result** The associated fields for the Failover feature are displayed on the Failover tab (Figure 3-18, “Brick Editor (Failover Tab, Brick Failover Enabled)” (p. 3-43)).

**Figure 3-18 Brick Editor (Failover Tab, Brick Failover Enabled)**



- 6 If the Brick Failover feature was enabled in [Step 5](#), complete the following fields:
  - **Activation Time (1/10 secs)**— this field specifies the amount of time (in 1/10 seconds) that must transpire after a missed heartbeat by the active Brick before failover to the standby Brick occurs. The default value is **4** (tenths of a second).
  - **Yield Time (1/10 secs)**— this field specifies the amount of time (in 1/10 seconds) that the active Brick must wait before failover to the standby Brick as a result of a link failure. The default value is **15** (tenths of a second, or 1.5 seconds).
  - **Preferred State Sharing Port**— click the down arrow next to this field and select the Brick port to be used for state-sharing. It is recommended that the default value **Auto** be used, unless a dedicated crossover connection to one of the Brick ports is being used. If the crossover connection port is not the same on each Brick, you can specify one as the preferred state-sharing port.

- **Generate Spanning Tree Topology Change Notification after Activation**— a Brick failover pair may be situated between switches running Multiple Spanning Tree (MST) mode. During a failover, the newly activated Brick issues two Topology Change Notifications (TCNs) to notify the switches of the failover. If a switch in MST mode that is also configured to run Rapid Spanning Tree Protocol (RSTP) receives a TCN, the switch's ports connected to the Brick change over to STP mode, thereby disrupting the MST domain and interrupting the flow of MST topology information between the switches.

This checkbox allows you to control whether an activated Brick issues any TCNs during failover.

If this checkbox is checked (the default), the newly active Brick generates two TCNs when it is activated during failover. If this checkbox is unchecked, the Brick does not generate the TCNs.

The SMS issues a warning message when this setting is changed, indicating that the Brick must be rebooted twice for the change to take effect.

- **Encrypt all links (more secure)**— by default, this radio button is selected. For additional speed, click the **Encrypt all links except Preferred State Sharing links (faster)**, which can be used when a particular link between Bricks is the preferred state-sharing link and is completely trusted.

- 
- 7 To designate a Primary Brick in the failover pair, enter a MAC address in the related **Ether0 Mac Address** field of both **Brick A** and **Brick B**.

Each MAC address must be specified in hexadecimal octets, separated by a colon (:). (Example: a1:10:04:00:0d:36). A minimum of 2 octets must be specified. Both MAC address fields must be completed and the MAC address of each Brick must be different to designate a Primary Brick.

To obtain the MAC address(es) of the Brick(s), click the **Retrieve MAC Addresses** button. *Note: The Retrieve MAC Addresses button cannot be used during initial provisioning of the failover pair. It will only work after the Bricks have been flopped/booted.* One or two MAC addresses for the Brick pair is displayed in the text area to the right of the button; each address is displayed on a separate line. The first line displays the MAC address of the active Brick, and, if available, the second line displays the MAC address of the standby Brick. Either MAC address can be copied and pasted into the **Ether0 Mac Address** field of **Brick A** or **Brick B**.

**Result** The **Primary** radio buttons for each Brick and the **Failback Delay** field are activated on the tab.

- 
- 8 To designate a Primary Brick in a failover pair, click the **Primary** radio button for **Brick A** or **Brick B** in the Brick Pre-emption Options portion of the tab.

- .....
- 9 If a Primary Brick was designated in [Step 8](#), in the **Fail Back Delay (secs)** field, enter a time (in seconds) to wait before initiating failover to the designated Primary Brick. The valid range is **20** to **9999**.

**Important!** This field is required when you designate a Primary Brick.

.....

- 10 Enter a label for each Brick to be used for logging failover messages. The default label is the last four hexadecimal digits of the Brick Ether0 MAC address.
- .....

- 11 In the **Min Time Active Before Failover (secs)** field, enter the amount of time (in seconds) that the active Brick must be up and running and has link integrity before failover can be initiated. The default value is **120**.
- .....

- 12 Optionally, IP address information can be entered in the IP Tracking table section to test link connectivity to designated links to the currently active Brick. If the designated links are not working, failover to the standby Brick is initiated.

In the IP Tracking table section of the tab, right-click and select **New** from the pop-up menu.

**Result** The Ping Failover Editor is displayed ([Figure 3-19, “Ping Failover Editor” \(p. 3-45\)](#)).

**Figure 3-19 Ping Failover Editor**



- 
- 13** In the **Ping Failover Editor**, complete the following fields:
- In the **Enabled** field, choose **Yes** to activate the ping/connectivity verification options (this is the default).
  - In the **Ping Destination IP Address** field, enter the IP address of a router or other device to be pinged by the Brick to determine if the associated link is still working.
  - In the **Ping Source IP Address** field, enter the source IP address of the Brick interface from which the ping will originate (either a VBA for the Brick, interface/VLAN address, **PPPoE#1**, **PPPoE#2**, or **DHCP**).
  - In the **Ping Interval (secs)** field, enter the time interval for sending a ping, in seconds. The default value is **10** seconds.
  - In the **Ping Timeout** field, enter the maximum time to wait for a ping response, in seconds. The default value is **1** second.
  - In the **Ping Failures for Failover** field, enter the number of consecutive responses to fail before failover is initiated. The default value is **10**.
  - If the Brick is configured to show VLAN information (the **Always Show VLAN Information** checkbox is checked on the Brick tab of the Brick Editor), in the **Ping Partition** field, enter the partition from which to initiate the ping. The default value is the partition with local as the VLAN ID.
  - In the **Description** field, enter a textual description of this Brick failover configuration. This field can be left blank.

- 
- 14** Click **OK**.

**Result** The link entry is displayed in the IP Tracking table section of the tab.

- 
- 15** Repeat steps 12 through 14 for each link to be pinged to determine if failover should be initiated to the standby Brick.

- 
- 16** Save and apply the changes to the Brick.

- 
- 17** Reboot the Brick to put the failover settings into effect. An additional reboot may be necessary.

**Important!** Steps 18-23 are only required the first time that you set up a Brick failover pair. If any changes are made to the Brick failover configuration after the initial setup, save and apply the Brick changes and reboot the modified Brick to make the changes take effect.



- 
- 18** Open the Brick Utilities menu and select **Make Brick Boot Media**.

Note that this step and the preceding steps are only performed once for the failover pair.

---

- 19** Follow the steps in the task [“To make a Brick boot floppy or USB drive on the SMS host”](#) (p. 3-53)
- 

- 20** When the Make Floppy or USB Drive task is completed, insert the boot floppy or boot USB drive in the floppy drive or USB drive and follow the steps in the task [“To boot the Brick device”](#) (p. 3-62).
- 

- 21** Check the SMS Status Monitor to verify that the Brick is able to connected to the SMS.

**Result** When the Brick connects, it synchronizes its clock with the SMS clock and downloads policies.

---

- 22** Insert the floppy or USB boot floppy into the floppy or USB boot drive of the second Brick of the failover pair, and power up the second Brick to install the software from the floppy.

**Result** The second Brick boots up and remains in standby state.

---

- 23** Reboot the Brick and verify that the second Brick can contact the SMS.

**Result** The second Brick synchronizes its clock with the SMS clock and downloads policies.

---

- 24** Power up the first Brick and verify that it enters the standby state.

END OF STEPS

---



## To Manually Initiate Failover

---

### When to use

Use this task to manually initiate failover on a Brick in a failover pair.

### Related information

A manual failover can also be performed on a Brick by issuing the `failover yield` command through the Brick CLI using the local or remote Brick console. For information about the `failover yield` command and the Brick, refer to the *SMS Tools and Troubleshooting Guide*.

### Before you begin

Before you begin this task, make sure that you have cabled the Bricks to the network in a failover configuration.

### Task

Complete the following steps to manually initiate failover of a Brick in a failover pair.

---

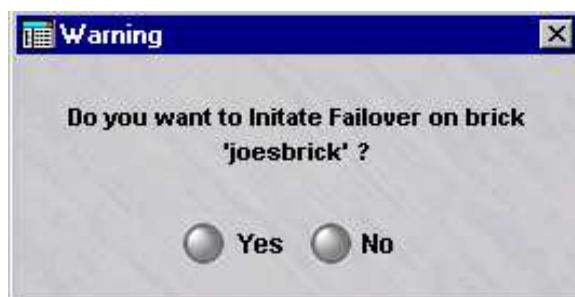
- 1 Click the Bricks folder in the Navigator.

**Result** The list of currently configured Bricks is displayed in the Contents panel.

---

- 2 Right-click on the Brick and select **Initiate Failover** from the pop-up menu.

**Result** The following confirmation dialog box is displayed.



- 3 Click **Yes**.

**Result** The currently active Brick reboots and becomes the standby Brick.

Once failover has been manually initiated, the Brick pair remain in this arrangement until a failure event occurs or another manual failover is performed.

.....  
E N D O F S T E P S



## To Migrate Model 1100 Bricks to a Model 1200 Bricks That Are in a Failover Pair

---

### When to use

Use this procedure to migrate Model 1100 Bricks to Model 1200 Bricks that are in a failover pair.

### Task

Complete the following steps to migrate Model 1100 Bricks to Model 1200 Bricks that are set up as a failover pair.

- 1 In the Brick Editor, clear out the Brick Pre-emption Options fields on the Failover tab.  
.....
- 2 Choose **Save** from the File menu to save the changes.  
.....
- 3 Make a boot floppy.  
.....
- 4 Floppy the Model 1200 Bricks as Model 1100 Bricks.  
.....
- 5 Move the links from the standby Model 1100 Brick to the new standby Model 1200 Brick.  
.....
- 6 Verify that the failover status is UP/UP.  
.....
- 7 Apply the policy to the active Model 1100 Brick and the new standby Model 1200 Brick.  
.....
- 8 Do a failover of the Model 1200 Brick. Verify that traffic is not impacted.  
.....
- 9 Move the links from the remaining Model 1100 Brick to the other Model 1200 Brick.  
.....
- 10 Verify that the failover status is UP/UP.

.....  
**11** Apply the policy to the Model 1200 Bricks.

.....  
**12** Perform a manual failover to the standby 1200 Brick. Verify that traffic is not impacted.

Once both 1200 Bricks are in a failover configuration:

.....  
**13** Edit the Model 1200 Bricks and change the Model Type to 1200.

.....  
**14** Configure the Bricks for preemption, if desired.

.....  
**15** Choose **Save and Apply** from the File menu.

Preemption requires a failover/reboot of both Model 1200 Bricks.

.....  
E N D O F S T E P S  
.....



## To Activate a Brick Device

---

### When to use

Once the Brick device is configured on the SMS, it is ready to be activated. Essentially, the configuration information for the Brick device must be copied to the Brick device flash memory. When that is done, the Brick device is booted with the information in its flash memory. There are four different options available to accomplish this:

1. You can create a floppy disk with the Brick configuration information on the local SMS host.
2. You can create a Brick boot USB drive with the Brick configuration information on the local SMS host or from a remote host logged into the SMS. The remote host must be a *Windows*® PC, while you may be logged into a *Windows*®, *Vista*®, *Solaris*®, or Linux SMS.

It should be noted that the USB flash drive must be one that is 1) less than 128MB in size (up to a 1GB drive is allowed for releases 9.1.210 or later) and 2) guaranteed from the manufacturer to be able to function as a bootable device when formatted as FAT. If you want to use a flash drive larger than 128 MB to create the Brick boot USB drive, you can download an upgraded version of the `makeBrickfloppy` utility by selecting the **Downloads** link from the OLCS or VPN Product Registration and Support website. Due to the variety of USB flash drives that are commercially available, and the internal differences between flash drives that seem to be identical from an external view - Alcatel-Lucent only qualifies that the USB flash drive orderable from Alcatel-Lucent will work properly. The user assumes all liability when using any USB flash drive other than the one available from Alcatel-Lucent. Contact your sales representative for further information.

3. You can create a floppy disk or USB drive with the Brick configuration information from a remote host logged into the SMS. The remote host must be a *Windows*® PC, while you may be logged into a *Windows*®, *Vista*®, *Solaris*®, or Linux SMS.

In addition, you can use this remote host procedure to create an encrypted file that can be securely sent to another network administrator to create the floppy or USB drive. This feature is particularly useful if you want to outsource the floppy/USB drive creation/activation function to staff who are not SMS or Group Administrators; these individuals are able to create the floppy or USB drive without actually accessing the SMS.

The `mkfloppy` process transfers the following files to the floppy disk or USB drive:

- *typc.zip*— the Brick operating system
- *inferno.ini*— an ASCII configuration file that contains the Brick name, Brick IP address, and SMS IP address

- *authinfo*— the ASCII certificate file, which contains the Brick private and public keys and SMS public key
- *b.com*— the bootstrap loader executable

In addition, the boot sector on the disk is overwritten with the Brick boot loader code. For this reason, the above files cannot simply be copied to a disk using the operating system's copy function.

4. If you have a connection to the serial port on the Brick (through a terminal server or modem), you can activate the Brick without a floppy disk or USB drive.

### To make a Brick boot floppy or USB drive on the SMS host

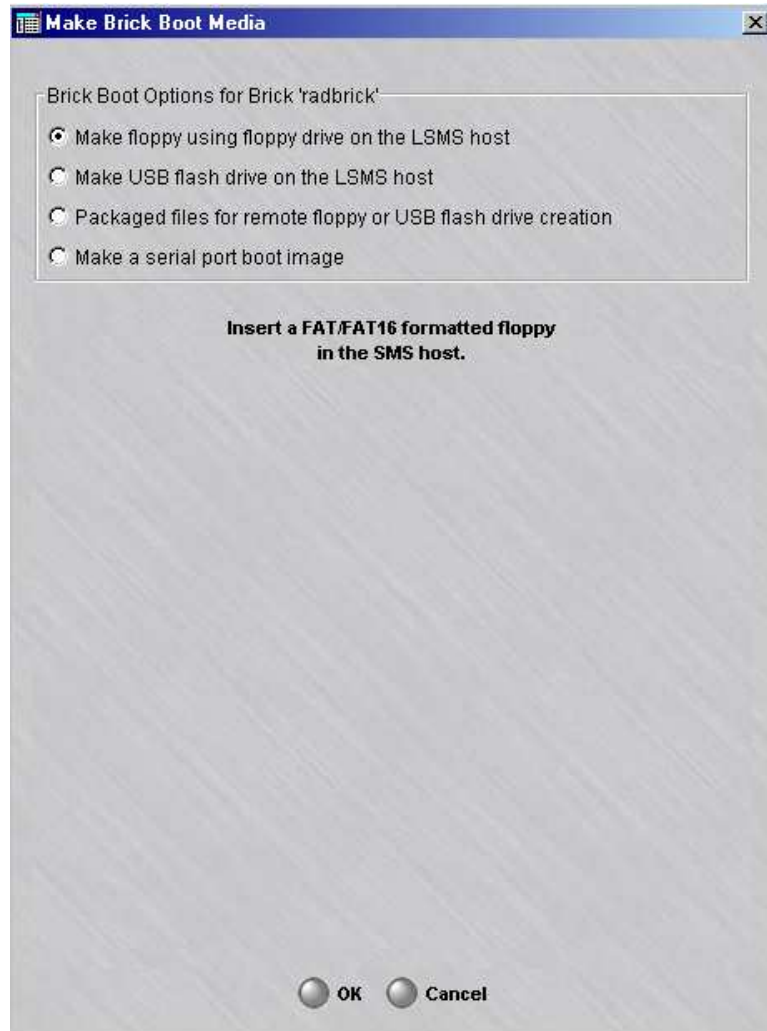
If you are sitting at the SMS host, follow the steps below to create the floppy disk or boot USB drive:

- 
- 1 If the Brick is currently displayed in the Brick Editor, open the Brick Utilities menu and select **Make Brick Boot Media**.

If the Navigator window is displayed, open the appropriate group and Devices folders, and click the **Bricks** folder to display all configured Bricks. Right-click the Brick to be activated, and select **Make Brick Boot Media** from the pop-up menu.

**Result** The Make Brick Boot Media window is displayed (Figure 3-20, “Make Brick Boot Media Window” (p. 3-54)).

**Figure 3-20 Make Brick Boot Media Window**



- 
- 2 If you have selected the option **Make floppy using floppy drive on the LSMS host** (the default), insert a formatted floppy disk into the disk drive of the SMS host.

If you have selected the option **Make USB flash drive on the LSMS host**, insert the USB drive into the USB port of the SMS host machine.

*Additional Information for Creating Brick Boot Media on a Linux SMS*

On a Linux SMS, the procedure for making bootable Brick media requires some additional steps, and the Linux SMS version of the Make Brick Boot Media window is slightly different (refer to the sample windows shown in Figure 3-21,



“Make Brick Boot Media Window (Linux SMS floppy drive creation)” (p. 3-55)  
and Figure 3-22, “Make Brick Boot Media Window (Linux SMS flash drive  
creation)” (p. 3-56).

**Figure 3-21 Make Brick Boot Media Window (Linux SMS floppy drive creation)**

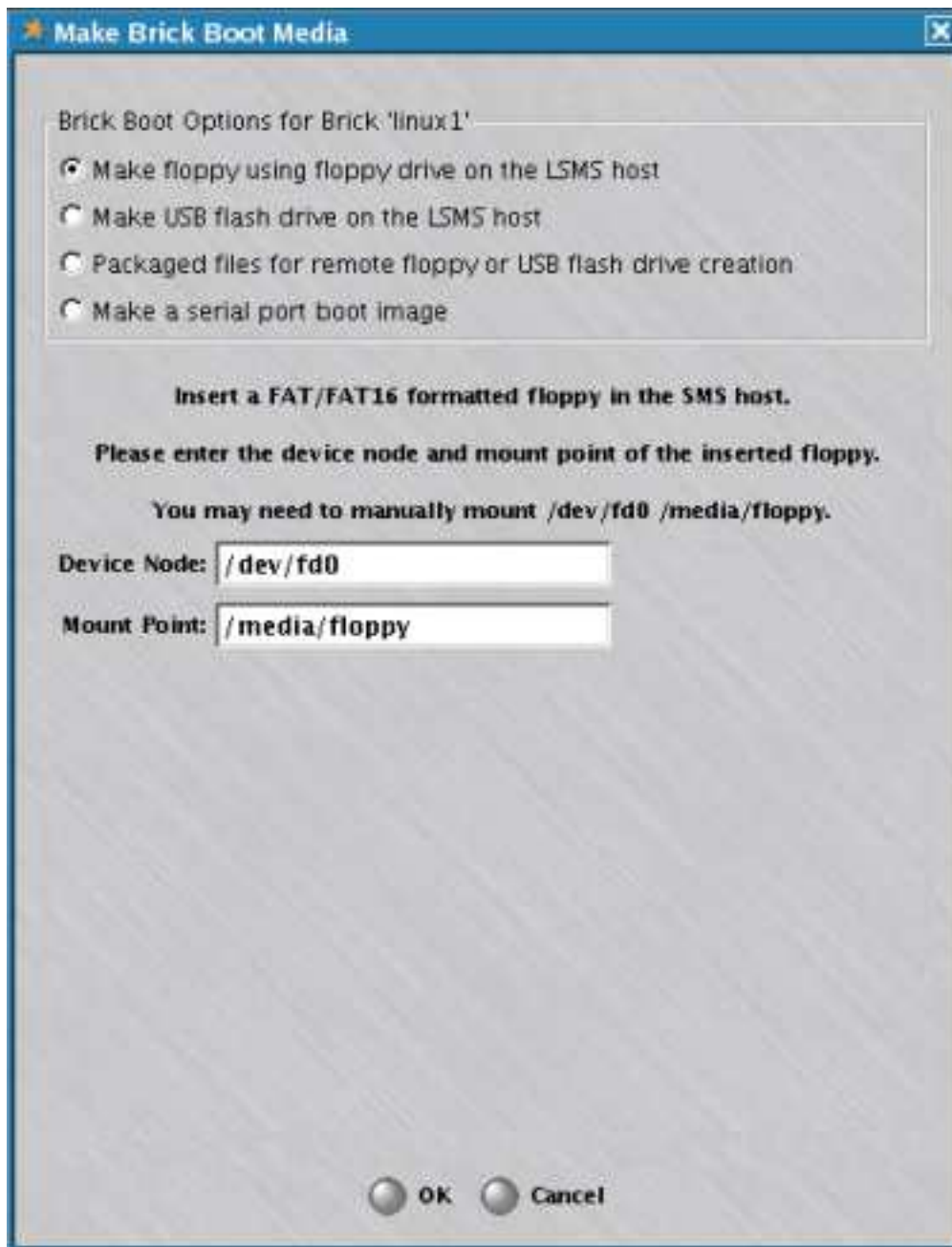
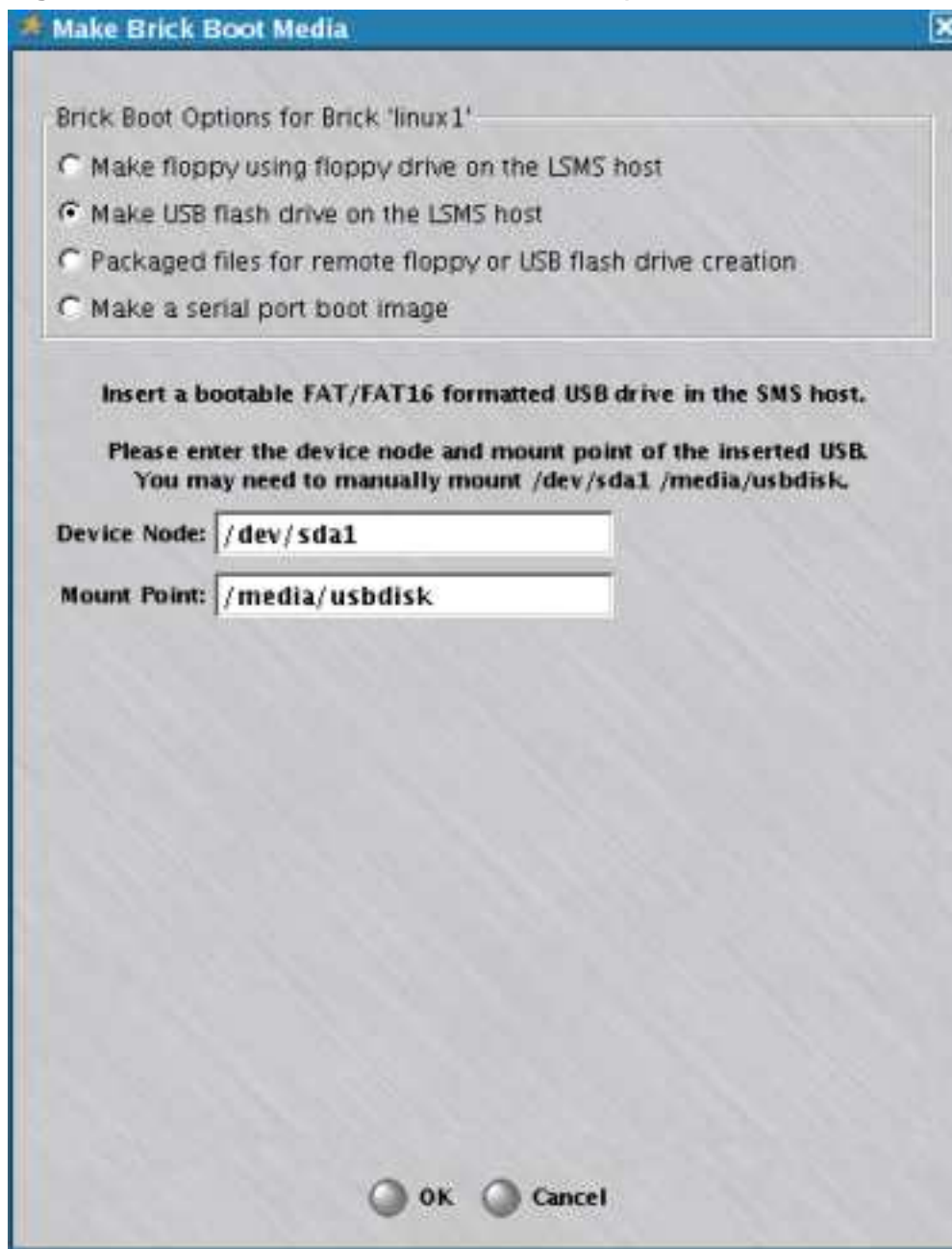


Figure 3-22 Make Brick Boot Media Window (Linux SMS flash drive creation)



Two additional input fields, **Device Node** and **Mount Point**, are displayed on the Linux SMS version of the Make Brick Boot Media window. These fields must be populated correctly to match the mounted device in order to successfully copy the Brick boot files to the media for a Linux SMS.

When creating floppy boot media on a Linux SMS, a 3.5 inch floppy will not auto-mount because Linux does not poll such devices. Before kicking off the floppy creation process ([Step 3](#)), you must manually mount the floppy device by logging in as root at the Linux system prompt and entering the following

command: `mount /dev/fd0 /media/floppy.` /dev/fd0 and /media/floppy are the default mount points that are set in the mkfloppy backend process of the SMS GUI.

After the floppy creation process has completed (Step 4), you must manually unmount the floppy by entering the following command at the Linux system prompt: `umount /media/floppy`

When creating flash drive boot media on a Linux SMS, the USB flash drive will auto-mount when inserted, and the SMS will auto-unmount the device when the process of creating the bootable USB flash drive has completed (Step 4). The default **Device Node** is /dev/sda1 and the default **Mount Point** is /media/usbdisk. The default Mount Point is valid if the USB flash device does not have a label. If the device does have a label (for example, USBFLOPPY), the entry in the **Mount Point** field must be modified accordingly (in other words, to /usb/USBDISK), since this is how the flash drive will be mounted by Linux.

- 
- 3 Click **OK**. The SMS downloads the configuration information to the disk or USB drive. The process takes approximately three minutes.  
A pop-up confirmation window is displayed.
  - 4 When the download is complete, click **OK** in the pop-up window and remove the disk from the SMS host.

END OF STEPS

---

### To make a Brick boot floppy or USB drive on a remote host

If you are logging into the SMS from a remote host, complete the following steps to create the floppy disk or Brick boot USB drive:

- 
- 1 Log into the SMS from the remote host using the SMS Remote Navigator.
  - 2 Open the appropriate group and **Devices** folders, and click the **Bricks** folder to display all configured Bricks.
  - 3 Right-click the Brick to be activated, and select **Make Brick Boot Media** from the pop-up menu.

If you configured the Brick from the remote SMS, and the Brick is displayed in the Brick Editor, open the Brick Utilities menu and select **Make Brick Boot Media**.

**Result** The Make Brick Boot Media window is displayed (Figure 3-23, “Make Brick Boot Media Window” (p. 3-58)).

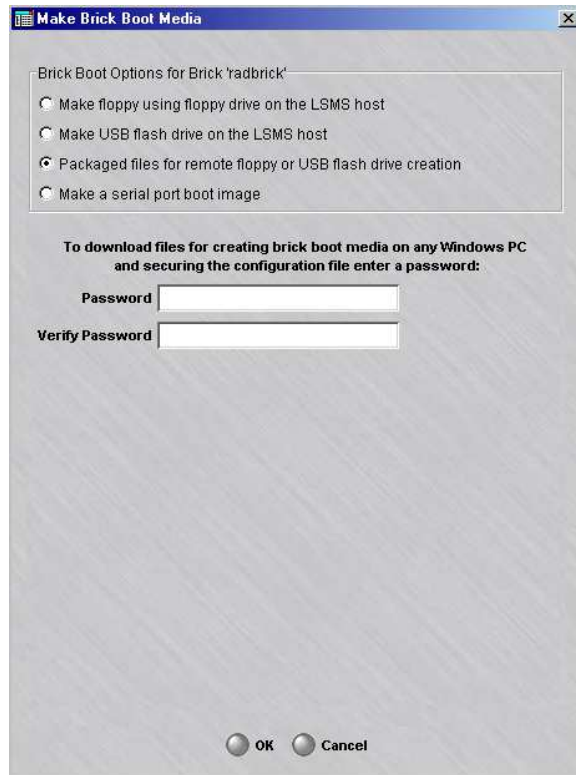
**Figure 3-23 Make Brick Boot Media Window**



- 
- 4 Click the radio button labeled **Packaged files for remote floppy or USB drive creation**.

**Result** The Make Brick Boot Media window prompts you to create a password (see [Figure 3-24, “Make Brick Boot Media Window \(with Password Fields\)”](#) (p. 3-59)).

**Figure 3-24 Make Brick Boot Media Window (with Password Fields)**



- 
- 5 Enter a password in the **Password** field, and then again in the **Verify Password** field. The password must be at least six characters.

Do not use an existing password. Make up a new password specifically for this purpose, and be sure to remember it. This password is used to encrypt and hash the configuration information, and you will need it later to decrypt the information.

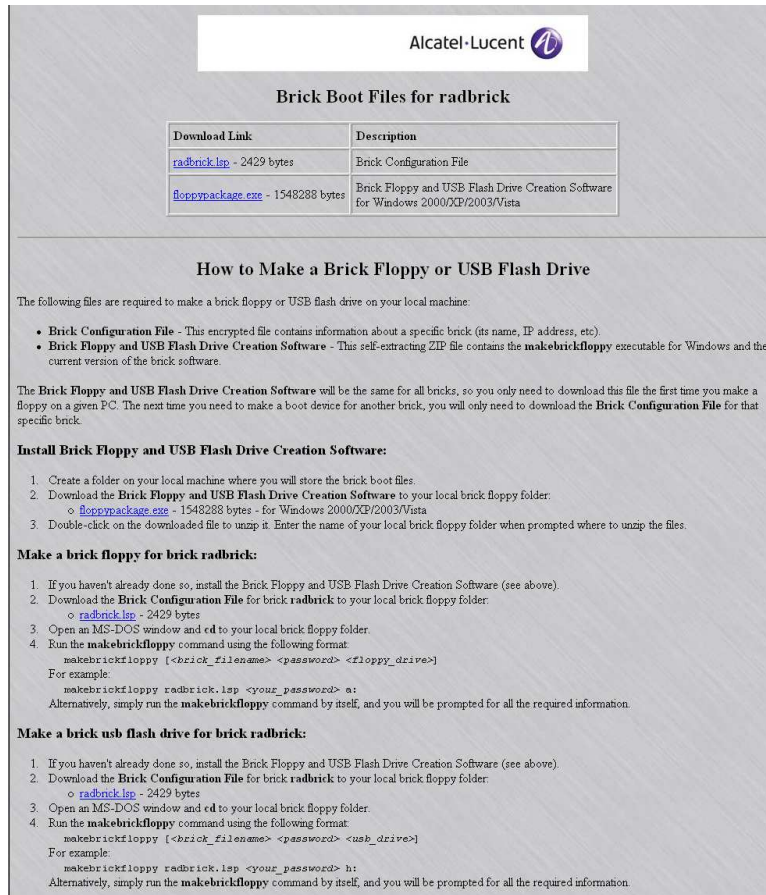
If you will be sending the encrypted file to another administrator to make the floppy and boot the Brick, you will have to give that administrator this password.

- 
- 6 Click **OK**.

**Result** A browser window will appear with instructions for making the boot floppy or USB drive (Figure 3-25, “Browser Window” (p. 3-60)).

The browser window contains links to all the files you need to make a boot floppy or USB drive.

**Figure 3-25 Browser Window**



- 7 If this is the first time you are making a floppy/USB drive on this host, you have to download the Brick floppy/USB drive creation software. This only needs to be done once on a host, so if you have made boot drive files on this host before, you can skip this step and proceed directly to [Step 8](#).

To download this file:

1. Create a folder on the host to store the floppy/USB drive creation file.
2. Click **floppypackage.exe** in the browser window. Then, download the file to the directory you just created. The file is a self-extracting Zip file.
3. Double-click the Zip file and extract the files to the folder you created in Step 1.

- 
- 8 Download the Brick configuration file to the directory containing the Brick floppy/USB drive creation software. This file is already encrypted, so it can be transferred without additional security measures.

Note that:

- If *Microsoft*® Internet Explorer is the default browser, click the **<Brick name>.lsp** file in the browser window and download the file to the appropriate directory.
- If Firefox or Netscape Navigator is the default browser, right-click the file, select **Save link as** from the pop-up menu, and save the file to the appropriate directory.

**Important! SEND AN ENCRYPTED FILE**

The next two steps explain how to make a floppy/USB drive on the machine you are now using. If your intention is to send the encrypted configuration file to another administrator to create the floppy and boot the Brick, you can stop here.

Instead, email the floppy/USB drive creation executable (*floppypackage.exe*) and the *<Brickname>.lsp* files to the person who will be creating the floppy/USB drive. Make sure that person is also in possession of the password you created in Step 4 — but do not include the password in the email message, as this defeats the purpose of encrypting the file.

- 
- 9 Open a Command Prompt window and cd to the directory containing the software you downloaded.
- 
- 10 Open the command line prompt and click the *.exe* file to unzip the files in it.
- 
- 11 Insert a formatted disk into the disk drive, or insert the USB drive in the USB port of the SMS host machine, and enter this command:

```
makeBrickfloppy <Brick filename><password><drive>:
```

where:

- *<Brick name>*= the name of the Brick configuration file
- *<password>*= the password you created in Step 4
- *<drive>*= the USB drive or floppy disk drive a.

If you enter *makeBrickfloppy* without the three parameters mentioned above, you will be prompted to enter them.

END OF STEPS

---

## To boot the Brick device

Complete the following steps to copy the files from the floppy disk or USB drive to the Brick flash memory, and then boot the Brick device from the flash memory.

- 1 Insert the disk into the disk drive of the Brick device, or insert the USB drive into the USB port of the Brick (for Model 50, Model 150, 700, and 1200 Bricks only). The disk drive of Models 201, 350, 1000 and 1100 is located on the front panel; the disk drive of Models 300 and 500 is located on the back panel; and the disk drive of Models 50, 80, and 150 is an external attachment. Refer to the *User's Guide* for the respective Brick model or contact your Alcatel-Lucent customer support team representative.

- 2 Power up the Brick by flipping the power switch. The configuration information will be automatically transferred to the Brick flash disk.

You will hear three beeps during the transfer process:

- A short beep will sound as the process begins,
- A second short beep will sound approximately 10 seconds later, and a
- Triple beep will sound within 2.5 minutes, indicating the transfer is complete.

- 3 When the transfer process is complete, remove the floppy disk from the disk drive, close the front panel, and flip the power switch off and on a second time to re-boot the Brick device from the flash disk. If a USB drive was used to boot the Brick device, remove it from the USB port of the Brick.

Once booted, the Brick attempts to contact its SMS and download its security policy and advanced configuration.

**Important!** When booting a Model 700 or 1200 Brick device from a USB Flash Drive that has a USB keyboard connected, a message may display indicating that no keyboard is present. The keyboard can still be used; just press any key on the keyboard and it will function.

- 4 If the Status Monitor is not displayed, open it now (see Note above). There should be an entry for the Brick, and within one minute, the Brick status should go from *LOST* to *UP*.



**Important!** The Certificate Authority (CA) is created on the SMS when the Brick is initially installed. The certificate for the Brick contains both the public key and private key of the Brick. If an intruder is able to spoof the Brick public address and connect with the SMS, the Brick policies, including VPN preshared keys and information about addresses/privilege levels might be obtained illegally.

Therefore, if a Brick floppy disk is compromised, the Brick should be deleted from the SMS and the Brick name should not be reused.

.....  
E N D O F S T E P S  
.....

### To activate the Brick device without a floppy disk

In order to activate the Brick without using a floppy disk, you must have a connection to the serial port located on the rear of the Brick. For more information on the exact location of the serial port, please review the appropriate User's Guide for your Brick model. The DB9-DB9 serial cable should be wired for null modem. The Brick port is configured for 115200 baud, no parity bits, 8 data bits and 1 stop bit. Note that for a Model 50 Brick, flow control for the serial port should be set to **None** or **Xon/Xoff** instead of **Hardware**. The flow control setting can be configured or modified by connecting your PC to the Brick and running a terminal emulation program (such as HyperTerminal) that is used to set up a local serial port connection. For instructions on how to set up a local serial port connection and configure the flow control setting, refer to the *Set Up a Direct Serial Port Connection* appendix in the *SMS Tools and Troubleshooting Guide*. Newly manufactured Bricks are packaged with software that, when powered up for the first time, allows them to come up to the "bootstrap" state. By using this procedure, an administrator can load a "boot image" (an encrypted version of the configuration files) to the Brick. Once the image is loaded, the Brick will then automatically reboot and connect to the SMS via its LAN connection. When connected to the SMS, the Brick will download the latest version of Brick software to itself, and automatically reboot one more time. At that point, the Brick is in the same state as if you had loaded it with a floppy disk.

Assuming that you have already configured the Brick on the SMS and that you are connected to the serial port on the Brick, follow these steps:

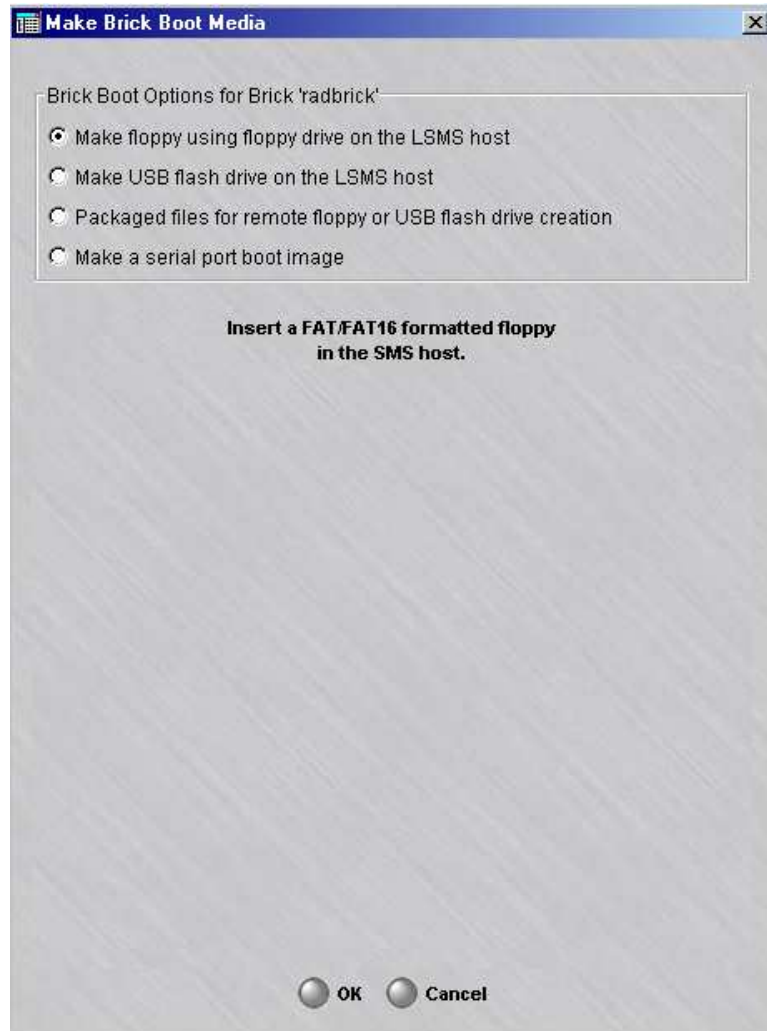
- .....
- 1 If the Brick is currently displayed in the Brick Editor, open the Brick Utilities menu and select **Make Brick Boot Media**.

If the Navigator window is displayed, open the appropriate group and Devices folders, and click the **Bricks** folder to display all configured Bricks. Right-click the Brick to be activated, and select **Make Brick Boot Media** from the pop-up menu.

In either case, the Make Brick Boot Media window is displayed.

**Result** The Make Brick Boot Media window is displayed (Figure 3-26, “Make Brick Boot Media Window” (p. 3-64)).

**Figure 3-26 Make Brick Boot Media Window**



- 
- 2 Select the last radio button labelled **Make a serial port boot image**. The “boot image” is the encrypted version of the Brick configuration files.

As shown in Figure 3-27, “Make Brick Boot Media Window (Make Serial Port Boot Image Option Selected)” (p. 3-65), there are several fields to be completed before the boot image is created. You must enter and verify a password to be used during the Brick bootstrap. Optionally, you may choose to enter a **User Defined Header**.

**Figure 3-27 Make Brick Boot Media Window (Make Serial Port Boot Image Option Selected)**



- 3 You can choose the **Browser** or **FTP** option depending on the accessibility of the Brick serial connection to the SMS server.

If you can connect to the Brick serial port from your SMS Navigator or SMS Remote Navigator, you should elect to display the boot image string in your **Browser**. Or, you may choose to **FTP** the boot image string to a more convenient location on another machine.

- 
- 4 If you select **Browser** and click **OK**, the default browser for your platform will come up and display several fields of information as well as a long encrypted string surrounded by !BEGIN! and !END! (examples are shown in [Figure 3-28, “Serial Port Boot Image Output \(1 of 2\)”](#) (p. 3-66) and [Figure 3-29, “Serial Port Boot Image Output \(2 of 2\)”](#) (p. 3-67) .

**Figure 3-28 Serial Port Boot Image Output (1 of 2)**

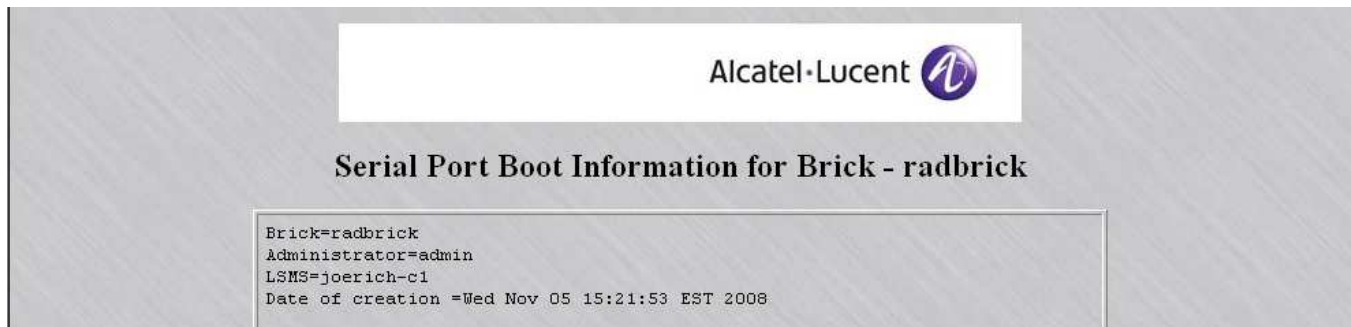
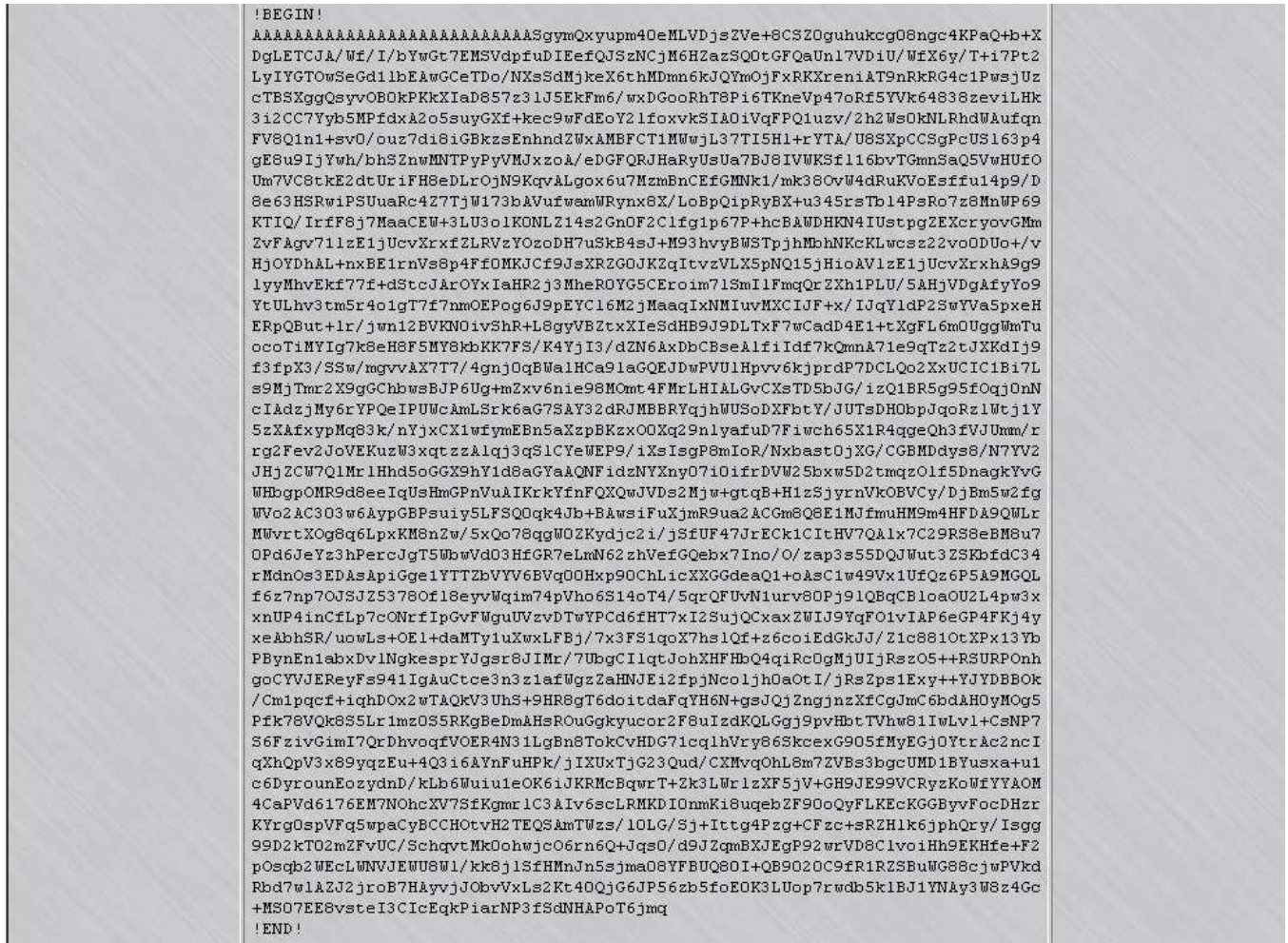
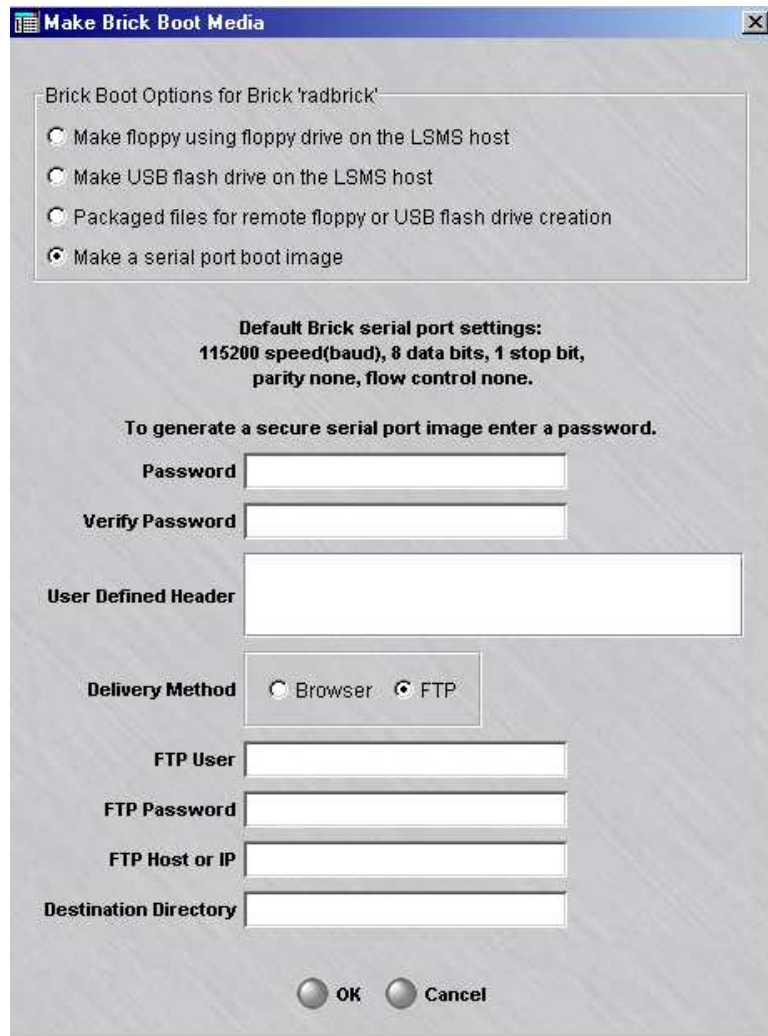


Figure 3-29 Serial Port Boot Image Output (2 of 2)



- 5 If you select **FTP**, additional fields will appear on the lower half of the window, as shown in Figure 3-30, “Make a Serial Port Boot Image (FTP Option)” (p. 3-68):

**Figure 3-30 Make a Serial Port Boot Image (FTP Option)**



You will need to supply valid input for all four fields in order for the ftp transaction to be successful. When you click OK, the SMS will create the boot image, save it to a "txt" file, and ftp it to the specified location.

- 
- 6 Now we are ready to bring up a session (either telnet or hyperterm) to the Brick serial port. Once connected to the Brick, the following message is displayed:

```
brick> - This Brick is in factory-ship state. Bootstrap the brick
```

- 
- 7 Press the **Enter** key three times.

**Result** The `brick>` command prompt is displayed.

- .....
- 8 Enter `bootstrap xxxxxx` where "xxxxxxx" is the password that you defined for the boot image. The Brick will respond:

OK. Waiting for config file on serial port... (^D to abort)

.....

- 9 At this point, you need to paste in the long boot image string. You must include `!BEGIN!` and `!END!`; if you happen to copy and paste any of the data prior to `!BEGIN!`, it will be ignored. You may copy and paste the string from either the browser or from the file that you ftp-ed in Step 5.
- .....

- 10 When you have pasted the boot image string successfully, the Brick will reboot and attempt to connect to the SMS via its LAN connection. Once it is communicating with the SMS, the Brick will automatically download the latest version of the Brick software to itself. The Brick reboots itself one more time to ensure that it is running with the latest software.

After the last reboot, the Brick is in the same state as if you had activated it from a floppy disk.

**Important!** If you want to create a floppy disk that allows the Brick to be restored to the original factory ship mode, there are tools available on the CD to create such a floppy disk.

Go to the "Tools\Floppyless Boot" directory on the CD and view the *readme.solaris.txt* file on how to create such a floppy disk on Solaris®, the *readme.linux.txt* file on how to create a floppy disk on Linux, or the *readme.windows.txt* file on how to create such a floppy disk on Windows®.

END OF STEPS

.....







# 4 Configuring Alcatel-Lucent *VPN Firewall Brick*<sup>™</sup> Security Appliance Ports

## Overview

---

### Purpose

This chapter explains how to:

- Configure the Brick physical ports if you want the Brick device to perform routing or to set the ports to a specific speed and mode
- Disable a Brick physical port
- Assign security policies to the ports where necessary (this includes assigning a special policy to the port connecting the Brick and SMS)
- Enable or disable the BSR Voice Gateway (BVG) and/or BSR Packet Gateway (BPG) feature(s)
- Create any necessary static routes so that the Brick can send traffic to LAN segments that are not directly connected to any of its ports
- Configure the Brick intelligent cache management feature so that the Brick automatically frees up additional memory when its cache usage approaches a pre-set threshold.

### Contents

<a href="#">To Configure a Physical Port</a>	4-3
<a href="#">To Assign a Security Policy to a Port</a>	4-9
<a href="#">To Enable or Disable the BSR Voice Gateway (BVG) And/Or BSR Packet Gateway (BPG) Feature(s)</a>	4-21
<a href="#">Static Routes</a>	4-32
<a href="#">To Add a Static Route</a>	4-34
<a href="#">To Modify a Static Route</a>	4-38
<a href="#">To Activate or Deactivate a Static Route</a>	4-39
<a href="#">To Delete a Static Route</a>	4-40

<a href="#">To Activate a Login Banner on the Brick Serial Port Console</a>	4-41
---	------

## To Configure a Physical Port

---

### When to use

When the Brick was initially configured, the SMS automatically assigned the IP address and subnet mask of the Brick to each of its ports (refer to the procedure [“To Configure a Brick Device on the SMS”](#) (p. 3-19)). If you make no changes to the addresses, the Brick will operate in a pure bridge mode.

### Routing

If you want the Brick device to perform routing, you can change the IP address\\subnet mask of any of the ports, and enter a different LAN segment. You can also change the Brick port mode from auto-sensing to either half or full duplex.

### Disabling a Brick device port

You can also disable a port (interface) on a Brick device. Disabling a Brick device port (interface) through the SMS GUI is equivalent to disconnecting the wire/fiber attached to the Brick device port. This can be done to ensure that the behavior of the Brick device does not change if someone inadvertently connects that port to a LAN. When a Brick port is disabled, no traffic is allowed to pass in or out of the Brick device through that port.

A Brick port can be disabled by selecting the Physical Ports tab on the Brick Editor, and then selecting the **Disabled** option from the **Mode** field pull-down menu on the Brick Ports Editor.

A Brick port cannot be disabled if the *administrativezone* zone ruleset is assigned to it. The *administrativezone* zone ruleset protects the SMS that is managing the Brick. A zone ruleset other than the *administrativezone* can be assigned to the disabled port, but if the assigned zone ruleset does not have a VBA, the Brick device is not accessible through that port and a warning message is issued, indicating that the zone rule assignment has no effect.

The **Send/Receive DHCP request on this port** checkbox cannot be checked if a port is disabled. The DHCP interface is typically used by the SMS to manage the Brick device.

If a Brick is part of a Brick failover pair, at least one Brick port in the pair must be enabled and the **Ignore heartbeat failures on this link** checkbox must be *unchecked*. For additional details about Brick device failover, refer to the [“Brick Device Failover”](#) (p. 3-38) section in [Chapter 3, “Configuring and Activating an Alcatel-Lucent VPN Firewall Brick™ Security Appliance”](#).

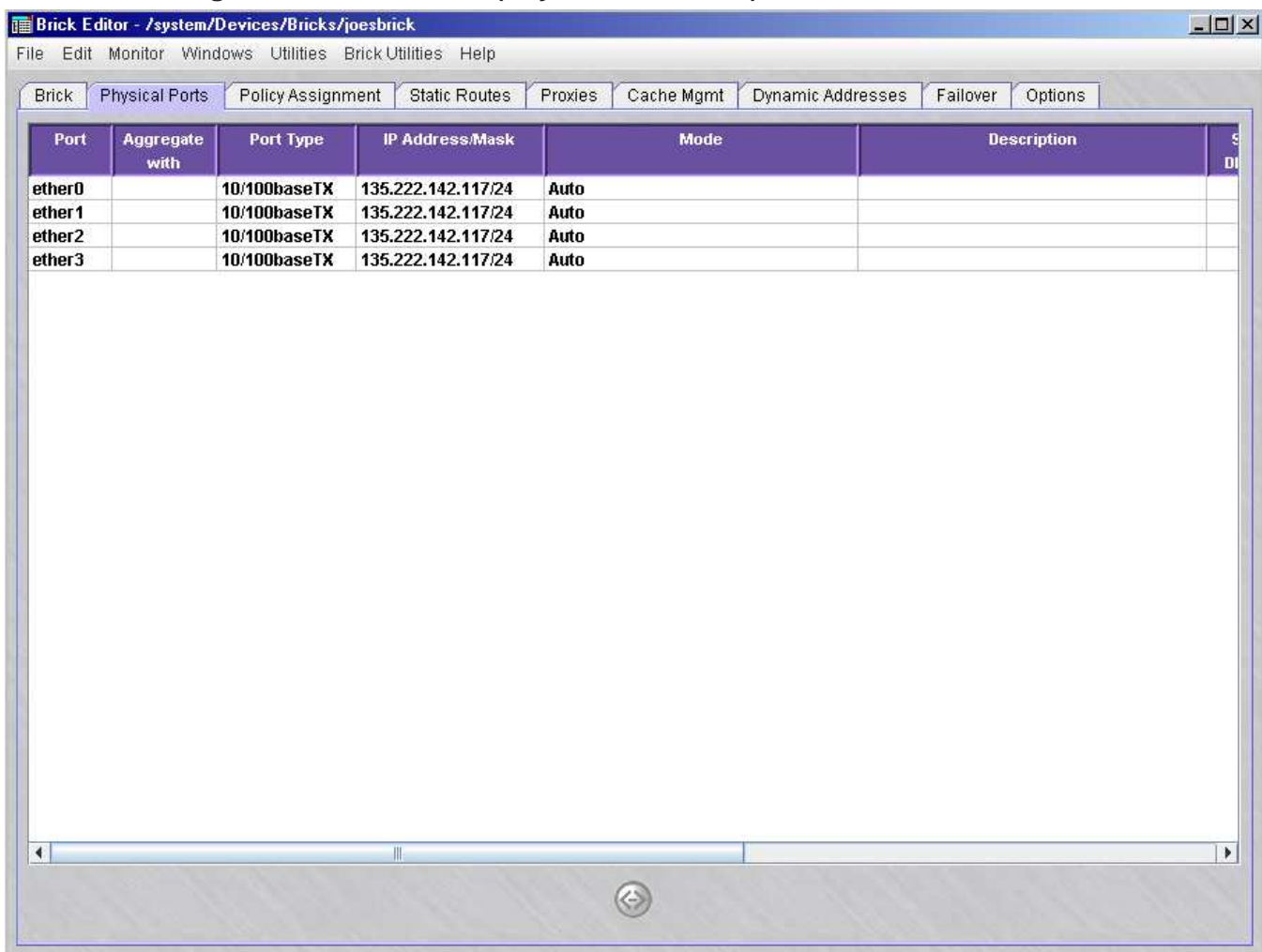
If the disabled port is being used for Brick device state-sharing, the currently active Brick device switches to a different port before the selected port is disabled. If that port is later switched from being disabled to enabled, the Brick device will resume using that port once it returns to the verified state.

**Task**

Complete the following steps to configure a port on a Brick device.

- 1 With the Brick Editor open, click **Physical Ports** to display the Physical Ports tab (see Figure 4-1, “Brick Editor(Physical Ports Tab)” (p. 4-4)) .

**Figure 4-1 Brick Editor(Physical Ports Tab)**

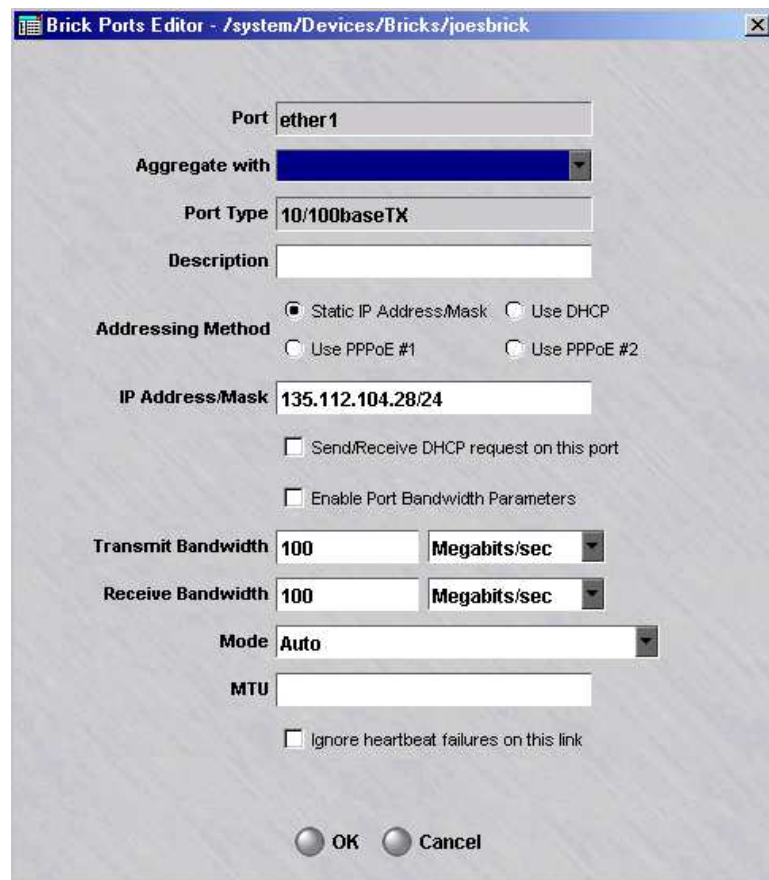


Note that the number of ports shown depends upon the Brick model or port configuration of a Brick model.

- 2 Double-click the port you want to configure.

The Brick Ports Editor is displayed (Figure 4-2, “Brick Ports Editor” (p. 4-5)).

**Figure 4-2 Brick Ports Editor**



### **Important! VLAN Information**

If you clicked the **Always Show VLAN Information** checkbox on the Brick tab of the Brick Editor, the Brick Ports Editor will contain additional fields for you to enter the VLAN domain, VLAN default ID, VLAN membership, and receive/transmit formats.

In addition, the Physical Ports tab will not show the IP Address/Mask for each port, but will show the VLAN domain, VLAN default ID, VLAN membership, and receive/transmit formats instead.

Both of these windows are shown with the VLAN information in [Chapter 6, “Configuring VLANs on Alcatel-Lucent VPN Firewall Brick™ Security Appliances”](#). Refer to this chapter if you are configuring one or more ports to handle VLAN traffic.

- 
- 3 The Brick supports link aggregation, where two or more physical ports are combined into one logical port so that the logical port handles more bandwidth. To aggregate this port with a logical port, select a logical port with the **Aggregate with** pull-down. When this is done, the port being edited is said to be a *child aggregate*, and the logical port in the **Aggregate with** field is said to be a *parent aggregate*. The ports in the pull-down are restricted to ones having the same **Port Type** as this one, and ones that have not yet been assigned as child aggregates. A child aggregate becomes assimilated with its parent, taking on the policy assignment attributes, MTU attributes, QoS, and VLAN/IP address assignments of the parent port (child aggregates will not appear as choices on the Policy Assignment screen). Port attributes can be changed only in the parent aggregate. A parent aggregate may have more than one child, but a child only one parent.

A blank choice under the **Aggregate with** pull-down allows you to undo link aggregation, at which point both ports have the same values for all attributes. Ports that were previously child aggregates take on the values of its previous parent aggregate for entries in the Policy Assignment screen.

Link aggregation *cannot* be made hierarchical beyond parent and child; parent aggregates may not serve as child aggregates of some other parent. The **Brick Type** may not be changed if any ports are aggregated.

- 
- 4 *Optional:* In the **Description** field, enter a textual description of the port.

- 
- 5 To have the interface address assigned dynamically, check either **Use DHCP**, **Use PPPoE #1**, or **Use PPPoE #2**, whichever is the appropriate Addressing Method for your environment, otherwise check the Static IP Address/Mask.

- 
- 6 To allow the Brick DHCP requests to go out this particular port and replies to come back in, check the **Send/Receive DHCP request on this port** checkbox. By allowing the DHCP request to go out only the port on which the DHCP server is located, you can prevent possible DHCP server spoofing from the other ports. At least one port must have this checkbox checked if a DHCP address is used anywhere on the Brick.

- 
- 7 Click the **Enable Port Bandwidth Parameters** checkbox to obtain and display statistics about data packets passing in and out of this Brick port.

This option must be enabled to display Brick port data packet statistics on the Single Brick Zones monitor window, which is accessed by selecting **Monitor > Brick Status > Single Brick Bandwidth Statistics**.

For details about the Status Monitor windows, refer to [Chapter 14, “Using the Status Monitor”](#).

- 8 If you are not assigning the interface address dynamically, then enter the IP address and subnet mask in the **IP Address/Mask** field.
- 9 **Transmit Bandwidth** and **Receive Bandwidth** are the “total” bandwidth in each direction. These values limit the total throughput that the Brick will allow out and into the interface.  
If you are not using the quality of service features, you can ignore these fields.
- 10 If this is a GigabitFiber port, you can configure the port to handle jumbo frames. To do this, select **Yes** from the drop-down list in the **Enable Jumbo Frames** field. If this is not a Gigafiber port, you will not see this field.
- 11 The default for the **Mode** field drop-down menu is **Auto**, which will automatically sense the correct speed for a port; however, you can specify the speed and whether traffic should be evaluated in full duplex or half duplex mode.  
To disable a port, select **Disabled** from the **Mode** field drop-down menu.
- 12 **MTU** (Maximum Transmission Unit) is the largest size IP packet that the Brick will transmit on the interface. If left blank, it defaults to 1500 bytes.
- 13 You can also decide whether or not to ignore heartbeat failures between redundant Bricks on this link by clicking the **Ignore heartbeat failures on this link** checkbox. By default, this box is not checked. This box should only be checked if a known topology exists which prevents heartbeats from reaching the other Brick.
- 14 Click **OK** to dismiss the Brick Ports Editor and return to the Physical Ports tab of the Brick Editor. The changes you just made will appear in the appropriate column.
- 15 Repeat Steps 2 — 14 for each additional port you want to re-configure.

.....  
**16** Display the File menu and select **Save**.

.....  
E N D O F S T E P S  
.....





## To Assign a Security Policy to a Port

---

### When to use

Once a Brick device has been configured and activated, and the ports properly configured, you can begin to assign security policies — in the form of a Brick zone rulesets — to the ports on the Brick device. The rules in the ruleset determine which traffic will be permitted through each port, and which will be dropped. No packets will be permitted through the Brick unless they have been examined by at least one ruleset.

The first ruleset you will want to assign to a port is the pre-configured ruleset *administrativezone*. This ruleset is provided with the SMS application, and its purpose is to protect the SMS while allowing it to communicate with the Bricks it is managing. The *administrativezone* also prevents accidentally blocking Brick - SMS intercommunication.

This ruleset should be applied to the port connecting the Brick and SMS (if the Brick is not directly connected to the SMS, this is the port connected to the router identified in the **Gateway IP Address** field on the Basic tab of the Brick Editor).

You do not have to assign a ruleset to every port that is in use. For example, administrators typically do not assign a ruleset to the port connecting the Brick to the Internet. Instead, they rely on the rulesets applied to the ports connecting the internal LANs to the Brick to filter out any unwanted traffic. As long as traffic is processed by at least one zone, it can pass through the Brick. However, if traffic is processed by more than one zone, it must pass all security policies in order to be retransmitted by the Brick.

If a port will be serving as a tunnel endpoint, you also have to enter a Virtual Brick Address (VBA). This address can also be used for network address translation purposes. You can also assign IPSec Client tunnel users an address on a local LAN.

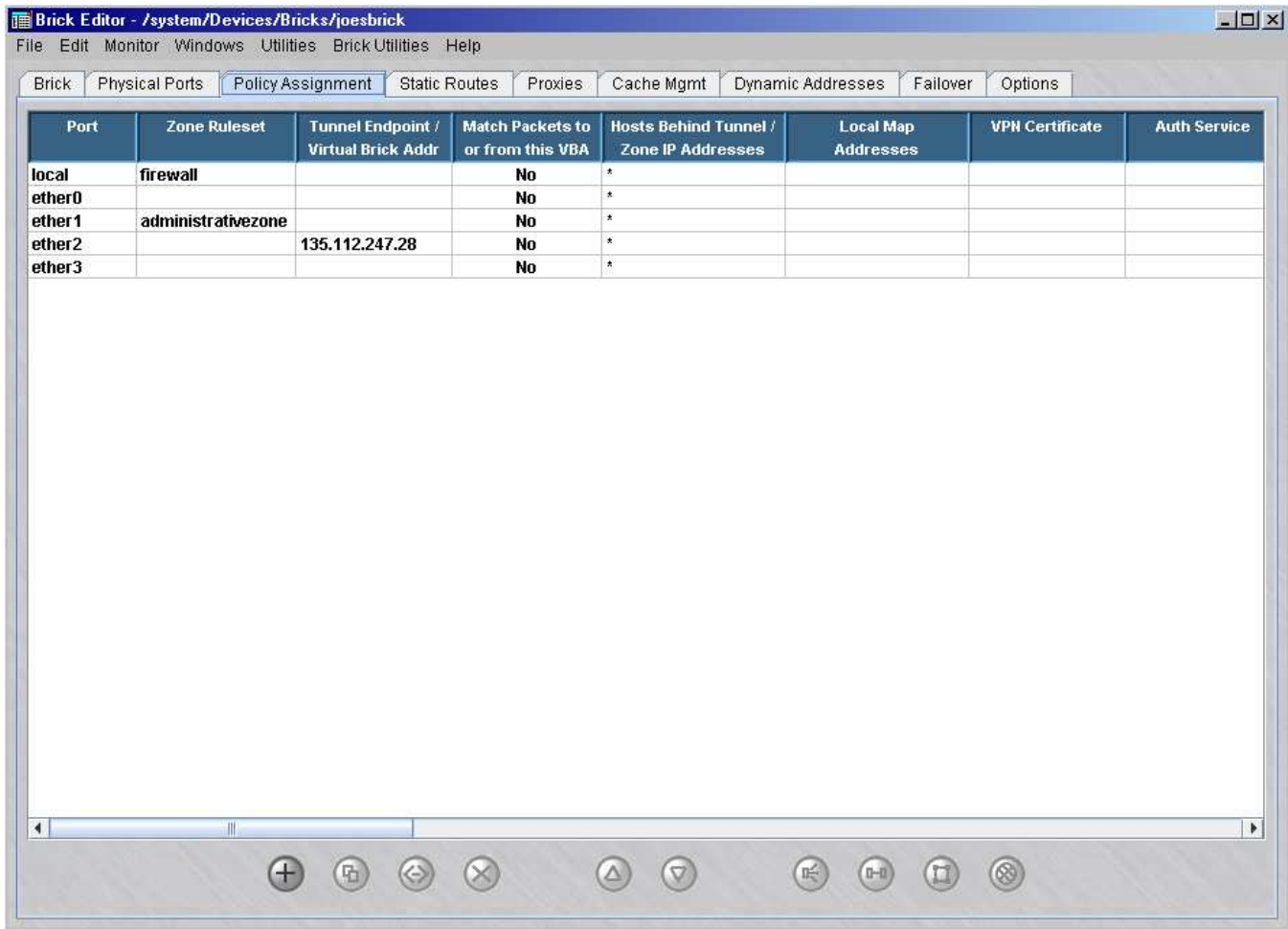
### Task

Complete the following steps to assign a policy to a port.

---

- 1 With the Brick Editor open, click **Policy Assignment** to display the Policy Assignment tab (see [Figure 4-3, “Brick Editor \(Policy Assignment Tab\)”](#) (p. 4-10)).

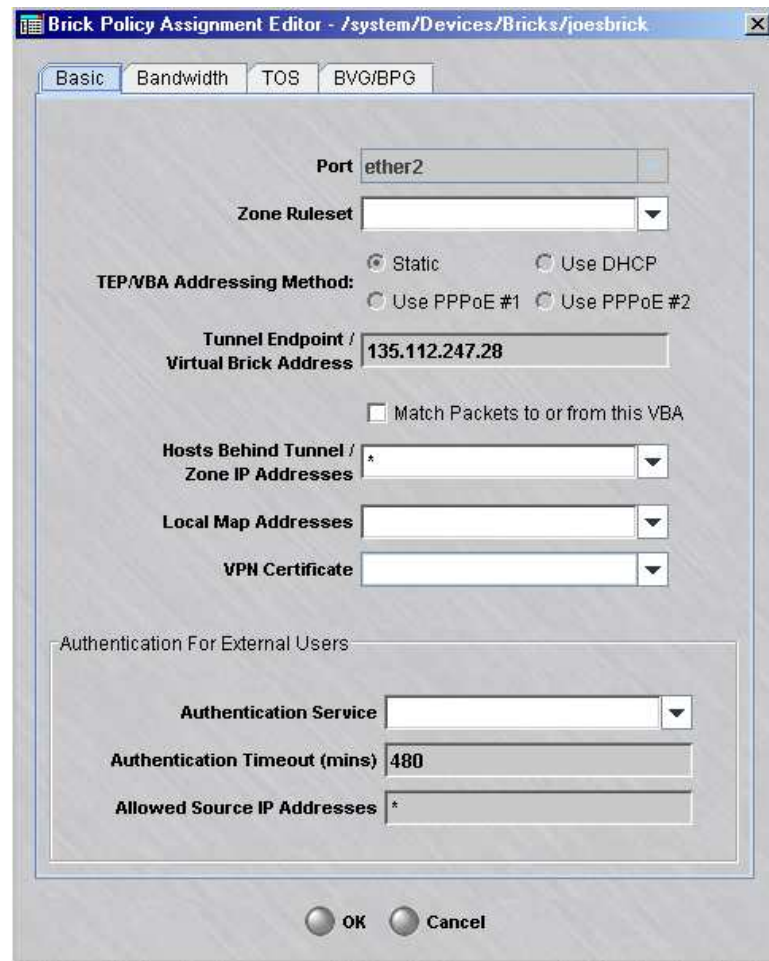
Figure 4-3 Brick Editor (Policy Assignment Tab)



- 2 Double-click the port to which the policy will be assigned.

**Result** The Brick Policy Assignment Editor is displayed ( [Figure 4-4, “Brick Policy Assignment Editor \(Basic Tab\)”](#) (p. 4-11)).

**Figure 4-4 Brick Policy Assignment Editor (Basic Tab)**



If you clicked the **Always Show VLAN Information** checkbox on the Brick tab of the Brick Editor, the Brick Policy Assignment Editor will contain a Zone VLAN IDs field, in addition to the fields shown above. In addition, the Policy Assignment tab will have an additional column showing the Zone VLAN IDs. Refer to [Chapter 6, “Configuring VLANs on Alcatel-Lucent VPN Firewall Brick™ Security Appliances”](#) for a more detailed discussion of VLANs.

- 
- 3 In the **Zone Ruleset** field, display the drop-down list and select a Brick zone ruleset, or select **Browse** and then select a ruleset from the Browse window. Here are a few guidelines to assist you:

**Important! Ruleset Guidelines:**

1. If this Brick is connected to the SMS via this port, select the *administrativezone* ruleset. This is a pre-configured ruleset provided for this purpose. (Refer to the *Pre-Configured Brick Zone Rulesets* appendix in the *LSMS Policy Guide* for details about all pre-configured Brick zone rulesets).
2. If this port will be used primarily as a firewall, protecting the LAN connected to it from attack via the Internet, select a ruleset you have created. This ruleset should reflect the desired security policy.
3. If this port will be used primarily as a tunnel endpoint, select the *vpnzone* ruleset. This is a pre-configured ruleset that contains all the rules required to quickly establish a tunnel. If you apply it to the ports on both Bricks, you have a functioning tunnel that securely passes all traffic. You can then edit this ruleset to add any additional security rules you require.
4. Select the *dhcpzone\_on\_inside* and *dhcpzone\_on\_outside* rulesets default zone rulesets. These rulesets are designed for routers using DHCP or PPPoE to get their public facing address. The first zone is used if it is applied on the side of the protected hosts and the second zone ruleset is used if it is applied on the interface connected to the WAN side.

- 
- 4 If the **TEP/VBA Address** should be dynamically assigned rather than fixed, check either **Use DHCP**, **Use PPPoE #1**, or **Use PPPoE #2**, whichever is the appropriate Addressing Method for your environment, otherwise check the **Static IP Address/Mask**. Note that only one Zone on a Brick may use a DCHP address, and only one Zone on a Brick may use the same PPPoE address.

If this port will terminate a LAN-LAN or client tunnel, this address is required. This is the address users of the Alcatel-Lucent IPSec Client will enter to enable their tunnels.

If this port will only function as a firewall, this address still may be required if you will be doing network address translation (refer to the *Network Address Translation* chapter in the *SMS Policy Guide*).

- 
- 5 In the **Host Behind Tunnel/Zone IP Addresses** field, enter the IP addresses of hosts that the ruleset will protect. If multiple rulesets are assigned to the same port, the Brick uses this field to determine which ruleset to apply to each incoming and outgoing packet. If the port will be terminating a LAN-LAN tunnel, the Brick uses this field to determine which hosts can send and receive encrypted traffic through the tunnel.

There are several ways to complete this field:

- Leave the default asterisk (\*) in place. This means all hosts connected to the port are protected. The advantage of using the asterisk is that if additional hosts are added to the port, they will automatically be protected by the Brick zone ruleset. If multiple rulesets are assigned to this port, you can leave the asterisk in the *last* ruleset shown in the Policy Assignment tab (in this instance, it means "everything else").
- Display the drop-down list, and select a host group from the list, or select **Browse** and select a host group that is not on the list (because, for example, it is in a subfolder).
- Enter a specific IP address, a range of IP addresses (in the format 1.1.1.1-1.1.1.10) or an address and subnet mask (Example: 1.1.1.0/24).

If none of the zone assignments matches the address(es) in a packet, the Brick device drops the packet and generates an error in the administrative events log, indicating error in zone table configuration. Hence, anti-spoofing often can be implemented easily by simply entering the subnet(s) of the devices behind this interface.

For additional recommendations for prevention of spoofing attacks, refer to the *Preventing Spoofing Attacks* section in the *Alcatel-Lucent VPN Firewall Brick® Zone Rulesets* chapter of the *SMS Policy Guide*.

- 
- 6 In certain situations, you may find it necessary to create a pool of IP addresses that will be used to provide client tunnel users with an address on a local LAN. This feature is especially useful if the client users applications that require opening sessions back to towards the clients (such as X-Windows) or in an environment where routing back to the TEP can only be guaranteed by assigning them from an address pool associated with that TEP.

This is done by entering one or more IP addresses in the **Local Map Addresses** field. This field only becomes active after you enter an IP address in the **Tunnel Endpoint** field. Enter a single IP address, an IP address with subnet mask, or a range of IP addresses. These are the addresses that will be set aside for client tunnel users.

Note that the **Local Map Address** field may also be used when you would like the Brick to respond to certain proxy ARP requests. For more information on this feature, refer to the *Network Address Translation* chapter in the *SMS Policy Guide*.

For more detailed information on local presence, including instructions on how to set it up, refer to the *Local Presence* appendix in the *SMS Policy Guide*.

- 
- 7 If this port will be used for user authentication (either firewall or tunnel users) and you will be using a database of user accounts that does *not* reside on the SMS host, you will have to enter an authentication service in the **Authentication Service for External Users** box.

If the port will not be terminating a client tunnel, or if the user database resides on the SMS host, you can skip this field.

Refer to the *User Authentication* chapter in the *SMS Policy Guide* for a detailed explanation of user authentication.

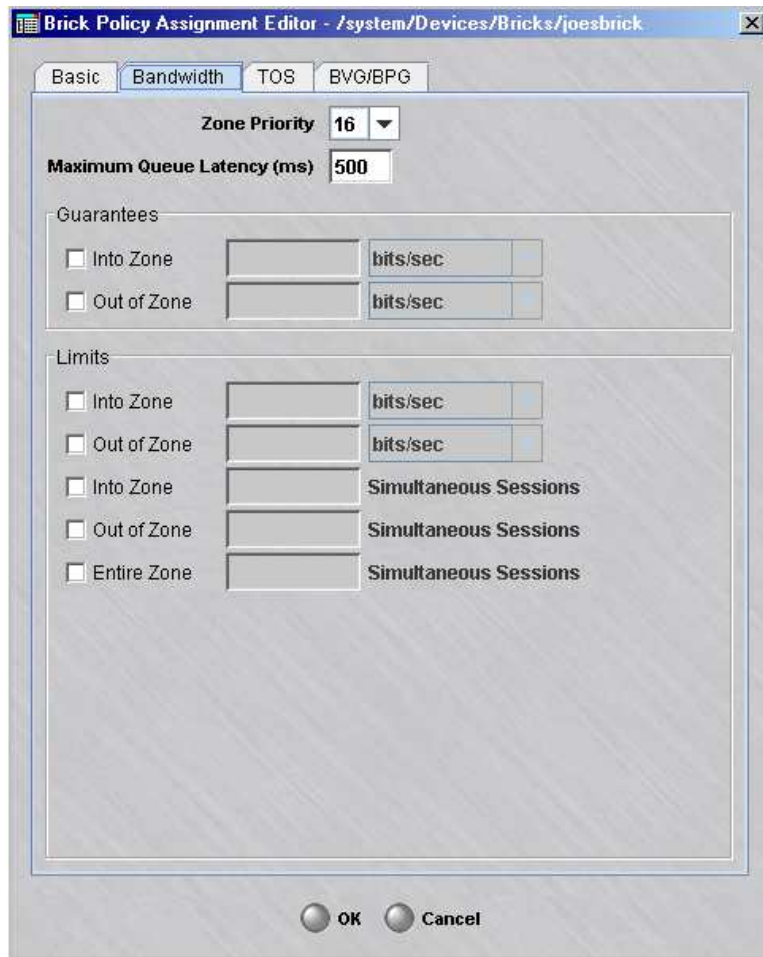
- 
- 8 If a digital certificate is being used to authenticate users who will be enabling tunnels to this tunnel endpoint or for LAN-LAN tunnels, click the down arrow to display a drop-down list and select the name of the digital certificate in the **VPN Certificate** field.

If you do not see the certificate in the list, bring up the Certificate Manager, click the Group Assigns tab, and assign the VPN Certificate to the Group of the Zone that is assigned to the Brick interface.

Refer to the *Digital Certificates* chapter in the *SMS Policy Guide* for an explanation of the procedure to obtain and install a digital certificate.

- 
- 9 Click on **Bandwidth** to display the Bandwidth tab of the Brick Policy Assignment Editor ( [Figure 4-5, “Brick Policy Assignment Editor \(Bandwidth Tab\)”](#) (p. 4-15)). The purpose of this tab is to configure bandwidth parameters for this port.

**Figure 4-5 Brick Policy Assignment Editor (Bandwidth Tab)**



The parameters on this screen establish the criteria for bandwidth through this zone on this port. They can be set as bit rate guarantees, bit rate limits, and limits on simultaneous sessions. A guarantee sets the minimum acceptable bandwidth when traffic must be reduced here to accommodate higher traffic demands elsewhere. A limit caps the allowable bandwidth or number of simultaneous sessions under high traffic loads. The checkboxes enable or disable a parameter while preserving its configured value.

Note that the total guaranteed bandwidth specified for all zones on a particular physical port must not be greater than the value assigned for 'Transmit Bandwidth' and 'Receive Bandwidth' in the Brick Ports Editor. If there is more than one zone assigned to the same port, the total of the guaranteed bandwidth specified for all of the zones on that port must not be greater than the value assigned for **Transmit Bandwidth** and **Receive Bandwidth** in the Brick Ports Editor.

A limit for the number of simultaneous sessions for the entire zone is provided to allow directionally skewed values (a high value in one direction and a low value in the other), while prohibiting high values in both directions at once.

**Zone Priority parameter** In order to set the **Zone Priority** parameter, a few things need to be explained about how bandwidth allocation is performed. For the purposes of this discussion, consider a class as some entity with bandwidth criteria placed on it. Classes can either be at the session, rule, zone, or physical port level. The physical port level is considered the highest level. **Zone Priority** controls which zone class(es) get any available excess bandwidth once their guarantees are satisfied.

More generally, when two classes are competing for bandwidth, both are under their limits, and some higher level class is over its limit, the following are the rules:

- When both classes are under the guarantee, available bandwidth is allocated on a round robin basis.
- When one class is over guarantee and one is under guarantee, available bandwidth is allocated to the class that is under guarantee first.
- When both classes are over guarantee, the bandwidth is allocated to the class with the better priority (the lower value).

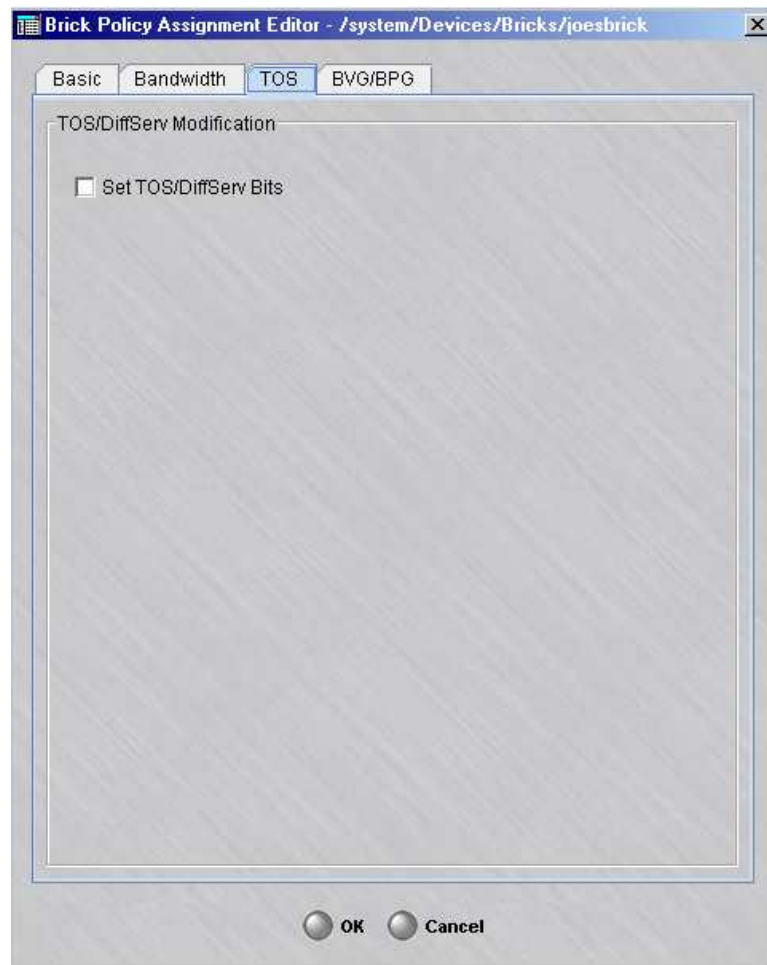
**Maximum Queue Latency parameter** This parameter controls the maximum amount of time a packet will be queued in the Brick. Setting this value appropriately prevents stale packets from being forwarded after they are no longer useful (i.e., lower values are usually better) and allows better bandwidth sharing (higher values are better). A value of 0 completely inhibits queuing which harms some applications. Tuning this value is, at best, empirical and guesswork in many applications (especially TCP-based ones). For applications like H.323, this is fairly simple because any latency over 50 msec is considered undesirable.

For additional details, refer to the *To Add Bandwidth Management to a Rule* section in the *SMS Policy Guide*.

- 
- 10 Click **TOS** to display the TOS tab of the Brick Policy Assignment Editor ( [Figure 4-6](#), “[Brick Policy Assignment Editor \(TOS Tab\)](#)” (p. 4-17)). The purpose of this tab is to edit the TOS/DiffServ parameters.



**Figure 4-6 Brick Policy Assignment Editor (TOS Tab)**



DiffServ is a method (defined in RFCs 2474/2475) that intermediate systems like routers can use to prioritize IP traffic depending on the precedence portion of the ToS field (bits 0, 1, 2) and bits 3, 4, 5 of the ToS field. This tab provides the option for the Brick to change the default priority of an outbound packet as it traverses the public backbone.

These parameters inform the Brick how to set the TOS/DiffServ bits in the second byte of the IP header for packets passing through the port. Several equivalent representations of the ToS byte are presented for user convenience. There are separate settings for packets within the guarantee and those exceeding the guarantee. The **Set TOS/DiffServ Bits** feature can be disabled while still preserving the configuration.

Note that the TOS/Diffserv settings at the Brick level will override the TOS/Diffserv settings in the Brick zone rulesets for a given port. If the settings within the individual rules for TOS/Diffserv are more important, do not enter TOS/Diffserv information for that Brick port.

For additional details, refer to the *To Add ToS/Alarm Capability to a Rule* section in the *SMS Policy Guide*.

- 11 Click **OK** to save the changes and dismiss the Brick Policy Assignment Editor.
- 12 Display the File menu in the Brick Editor and select one of the **Save** options.

END OF STEPS

### To assign multiple rulesets to a port

You can assign more than one Brick zone ruleset to a single Brick port. When a port has more than one Brick zone ruleset assigned to it, the Policy Assignment tab of the Brick Editor has multiple entries for the same port. Figure 4-7, “Policy Assignment Tab (Two Rulesets Assigned to Ether1)” (p. 4-18) shows a Policy Assignment tab with two entries for ether1.

**Figure 4-7 Policy Assignment Tab (Two Rulesets Assigned to Ether1)**

Port	Zone Ruleset	Tunnel Endpoint / Virtual Brick Addr	Hosts Behind Tunnel / Zone IP Addresses
local	firewall		*
ether0			*
ether1	sales_zone		100.10.10.1/24
ether1	clerical_zone		*
ether2			*
ether3			*

The hosts in two zones connected to the same port can communicate freely because their traffic does not pass through a Brick port. Both are, however, protected from all other traffic.

If the Zone IP address or range associated with rulesets assigned to the same port is a range of IP addresses, the order of the entries becomes important. This is because the Brick looks at the ports in order and uses the first match found when directing a packet to a Brick zone ruleset.

If the **Match Packets to or from this VBA** option is checked on the Brick Policy Assignment Editor, you can assign multiple rulesets to the same interface when all of the traffic is VPN-based and addressed to/from the Brick VBA.

Therefore, the entry that is a *subset of the larger entry must appear first*. Otherwise, the Brick will direct packets to the Brick zone ruleset with the larger range first, and packets intended for the Brick zone ruleset with the smaller range will never arrive there.

If one of the Brick zone rulesets is assigned to a port and has its IP address set to the wildcard asterisk (\*) — the entry for that zone *must be the last entry for that port*. The asterisk stands for all hosts, and so by definition is the largest range.

To re-order an entry, right-click it and select **Up** or **Down** from the pop-up menu. Repeat until the order is correct.

### Assign the Same Ruleset to Multiple Ports

It is possible to assign the same zone ruleset to multiple ports. This allows you to configure your network with redundant paths for VPN traffic.

When multiple ports have the same ruleset, all the other policy parameters for those ports (for example, Brick zone ruleset, hosts behind tunnel, local map address, and so forth) must be the same. Therefore, the easiest way to assign the zone ruleset to both ports is to:

1. Assign the zone ruleset to the first port, as described above (refer to the task “[To Assign a Security Policy to a Port](#)” (p. 4-9)).
2. Right click the port in the Policy Assignment tab and select **Duplicate** from the pop-up menu (or click the **Duplicate** button).
3. When the Brick Policy Assignment Editor appears, enter the second port in the **Port** field and click **OK**.
4. Repeat Steps 2 and 3 for each additional port to which this ruleset will be assigned.
5. If necessary, move the new port assignments up or down to ensure that the ports are in correct, ascending order, beginning with *ether0*.

If you attempt to edit the policy associated with one of the ports, you will receive an error message. The text of the message indicates that all fields must be the same for ports with the same ruleset, and it offers you two choices of action: (1) restore the values of this port to the ones used by the other ports, or (2) overwrite the other ports with the new values of this port.

### To modify a policy assignment

Complete the following steps to change an existing policy assignment.

1. With the Policy Assignment tab displayed (see Figure 3-3), double-click the port you want to edit. The Brick Policy Assignment Editor is displayed, with the policy assignment displayed.
2. Make any changes to the information shown, as necessary.

3. Click **OK** to dismiss the Brick Policy Assignment Editor.
4. Display the File menu and select one of the **Save** options.

### To delete a policy assignment

You can only delete a policy assignment if more than one policy has been assigned to the same port. In other words, if there are two entries for a given port, one can be deleted. If you have only assigned one policy to a port, and you want to remove the policy, you can only do this by modifying the assignment and removing all the values you entered (zone ruleset, hosts behind tunnel, and so forth).

Complete the following steps to delete an existing policy assignment.

1. With the Policy Assignment tab displayed, right-click the port you want to delete and select **Delete** from the pop-up menu. A confirmation window is displayed.
2. Click **Yes** to dismiss the confirmation window. The port entry will no longer appear in the Policy Assignment tab of the Brick Editor.

### To re-order the policy assignment entries

If the entries in the Policy Assignment tab get out of ascending order — for example, if the entry for ether3 precedes ether2 — you should re-arrange the entries so that the ports and policy assignments are in the proper ascending order. If multiple zones assigned to the same port get out of order — for example, if a zone with an asterisk for its IP address range precedes a zone with a specific address range — you should rearrange the entries. If the entries are not in their proper order, problems can result.

Complete the following steps to re-order existing port entries.

1. With the Policy Assignment tab displayed, right-click the port entry you want to reorder and select **Up** or **Down** from the pop-up menu. The entry will move one row with each click.
2. Repeat as necessary until the port entries are in the correct order.



## To Enable or Disable the BSR Voice Gateway (BVG) And/Or BSR Packet Gateway (BPG) Feature(s)

---

### When to use

Use this task to enable or disable the BSR Voice Gateway (BVG) and/or BSR Packet Gateway (BPG) feature(s).

When the BVG feature is enabled, the Brick device (BVG) consolidates and encrypts voice packets from a cluster of BSRs and provides a single lu-CS interface towards the Mobile Switch Center (MSC)/Media Gateway (MGW) in the service provider's Core Circuit Switched Network.

When the BPG feature is enabled, the Brick device (BPG) consolidates and encrypts data packets from a cluster of BSRs and provides a single lu-PS interface towards the Serving GPRS Support Node (SGSN) in the service provider's Core Packet Switched Network.

### Before you begin

**Important!** The BVG/BPG features are an optional feature package that must be purchased and installed using a separate installation key via the New Feature Setup utility. If the BVG/BPG feature package has not been installed, the **BVG/BPG** tab is not displayed on the Brick Policy Assignment Editor.

For details about the New Feature Setup utility, refer to [Appendix F, "New Feature Setup"](#) in the *SMS Administration Guide*.

Before enabling the BVG and/or BPG feature(s), a service group must be created and assigned to a rule within the assigned zone ruleset to allow UDP traffic at the Dynamic Port Address Translation (DPAT)-provisioned port (default 9898) to pass through. The Brick device (acting as the BVG and/or BPG) will dynamically create rules to allow the RTP traffic associated with a successful DPAT binding to pass through.

Before enabling the BPG feature, a GTP Version 1 application filter should be created and assigned to a service group, which, in turn, is assigned to a set of rules within a Brick zone to process GTP packets between the BSR and SGSN.

As an example:

1. Create a GTP Version 1 application filter called `bpg_gtpv1_filter`.  
Use all default options for the filter.
2. Create a service group called `bpg_service`.  
Provision the service group with the following parameters: `prot=udp, dest port=2152, src port range=*`, App Filter=`bpg_gtpv1_filter`
3. Create a service group called `DPAT_service`  
Provision the service group with the following parameters: `prot=udp, dest port range=9898(default), src port range=*`  
Define rules to process RTP packets between the BSR and BPG to the SGSN.

The following table provides general guidelines for creating rules in a zone ruleset for the BPG functionality, assuming the BPG is provisioned on a zone assigned to the Brick interface facing the SGSN. If the BPG is provisioned on a zone assigned to an interface facing the BSR, only the direction of the ruleset would change.

SRC	DEST	DIR	SERVICE <sup>1</sup>	ACTION	Description
BSR/ Active VPN users	VBA/ (BPG)	IN	DPAT_service	VPN	process DPAT protocol
BSR/ Active VPN users	VSGSN	IN	bpg_service	VPN	process pre-mapped GTP pkts, BSR to VSGSN(BPG)
VBA	SGSN	IN	bpg_service	PASS	process post-mapped GTP pkts, BPG to SGSN
SGSN	VBA(BPG)	OUT	bpg_service	PASS	process pre-mapped GTP pkts, SGSN to BPG
VSGSN	BSR	OUT	bpg_service	VPN	process post-mapped GTP pkts, SGSN to BSR

**Notes:**

1. The service group names used in this column are only examples.

In addition, the administrator should create regular rules to allow/drop the other traffic that the Brick device is expected to handle, according to the customer-specific policy.

**Important!** When the BPG feature is enabled, each rule that is created to process GTP packets by the BPG (Brick device) to/from the BSR and SGSN *must* have the **Authorize Return Channel** option *enabled* (checkbox checked). The **Authorize Return Channel** option is enabled via the Advanced tab of the Brick Zone Rule Editor.

For details about creating a Brick zone ruleset, refer to the *Alcatel-Lucent VPN Firewall Brick® Security Appliance Zone Rulesets* chapter in the *SMS Policy Guide*. For details about assigning a zone ruleset to a Brick device port, refer to the [“To Assign a Security Policy to a Port”](#) (p. 4-9) task in the *SMS Administration Guide*. For details about configuring a GTP application filter and assigning it to a service group, refer to the *Application Filters* chapter in the *SMS Policy Guide*.

Before you begin this task, you must assign a Virtual Brick Address (VBA) or Tunnel Endpoint Address to the Brick device port on the **Basic** tab of the Brick Policy Assignment Editor. This address will be used as the Virtual Mobile Switching Center (VMSC) or Virtual Radio Network Controller (VRNC) address in exchanges between the BSR(s) and Brick device to map voice or data packets to the correct destination.

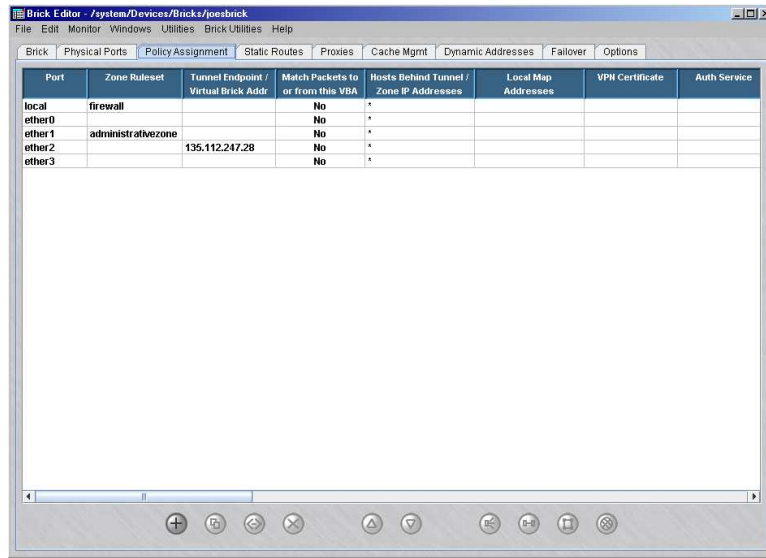
For details about assigning a VBA and using Network Address Translation (NAT) on a Brick device, refer to the *Network Address Translation* chapter in the *SMS Policy Guide*.

## Task

Complete the following steps to enable or disable the BVG and/ or BPG feature(s).

- 1 With the Brick Editor open, click **Policy Assignment** to display the Policy Assignment tab (see [Figure 4-8, “Brick Editor \(Policy Assignment Tab\)”](#) (p. 4-24)).

Figure 4-8 Brick Editor (Policy Assignment Tab)

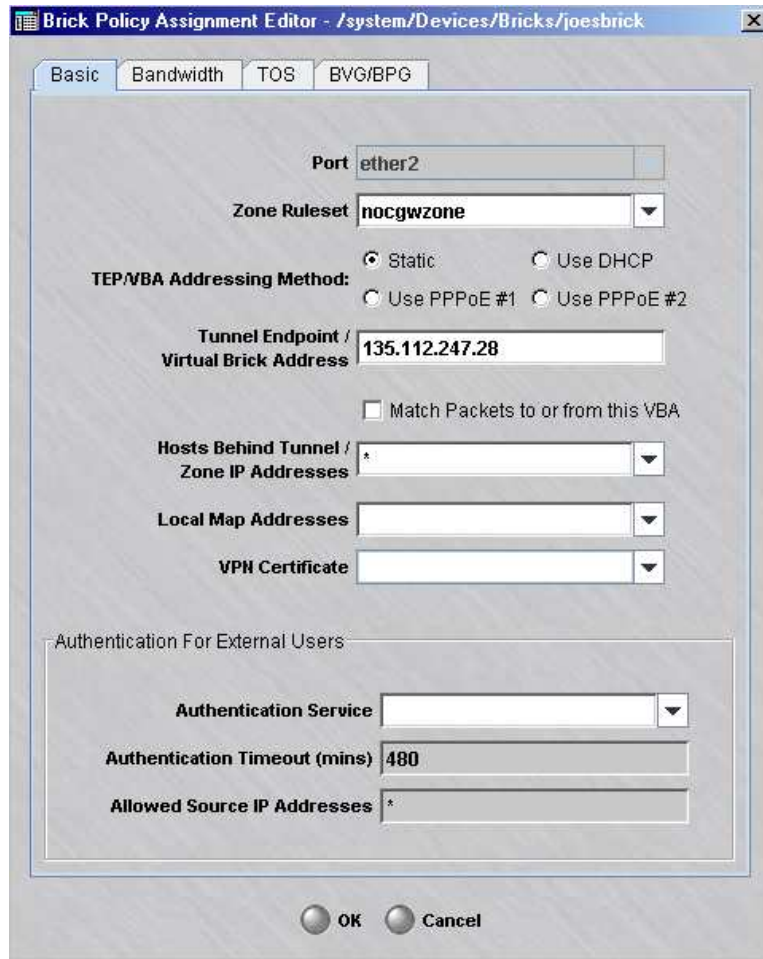


- 2 Double-click on the port for which you want to enable or disable the BVG/BPG feature(s).



**Result** The Brick Policy Assignment Editor is displayed (Figure 4-9, “Brick Policy Assignment Editor” (p. 4-25)).

**Figure 4-9 Brick Policy Assignment Editor**

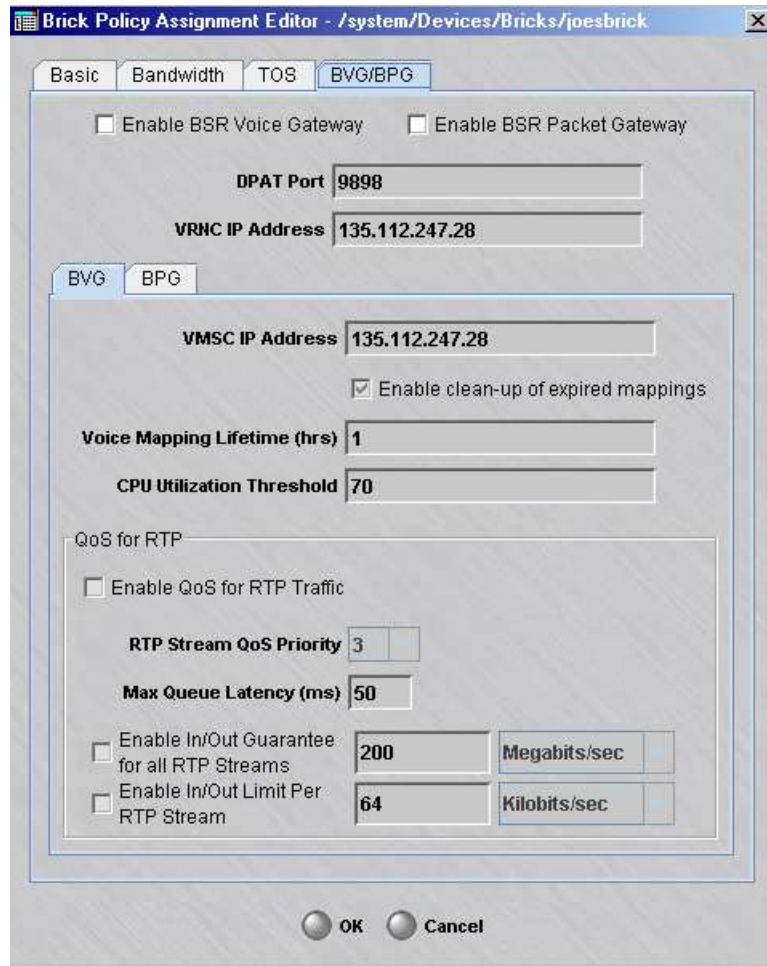


If you originally clicked the **Always Show VLAN Information** checkbox on the Brick tab of the Brick Editor, the Brick Policy Assignment Editor will also contain a Zone VLAN IDs field, in addition to the fields shown above. In addition, the Policy Assignment tab will have an additional column showing the Zone VLAN IDs. Refer to the *Configuring VLANs on Alcatel-Lucent VPN Firewall Brick® Security Appliances* chapter in this Guide for a more detailed discussion of VLANs.

- 
- 3 Click on the **BVG/BPG** tab.

**Result** The BVG/BPG tab panel is displayed (Figure 4-10, “Brick Policy Assignment Editor (BVG/BPG Tab)” (p. 4-26)).

**Figure 4-10 Brick Policy Assignment Editor (BVG/BPG Tab)**



- 
- 4 To enable the BVG feature, click the **Enable BSR Voice Gateway** checkbox to check it (the feature is disabled and the checkbox is unchecked, by default).

To enable the BPG feature, click the **Enable BSR Packet Gateway** checkbox to check it (the feature is disabled and the checkbox is unchecked, by default).

If either feature is enabled, go to [Step 5](#).

- 
- 5 In the **DPAT Port** field, specify the UDP port number that will be used to accept data packets from the BSR. The default value is **9898**.

The **VRNC IP Address** field is a read-only field that contains the Virtual Brick Address (VBA) or Tunnel Endpoint Address assigned to the Brick device serving as the BVG/BPG.

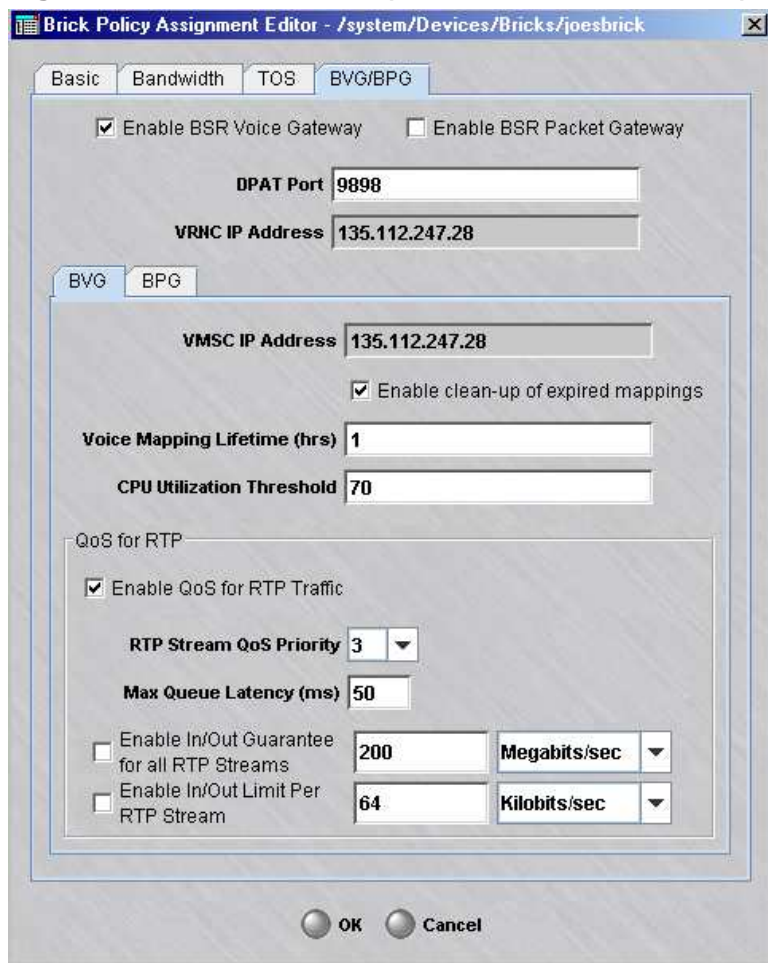
If the BVG feature was enabled in [Step 4](#), go to [Step 6](#).

If the BPG feature was enabled in [Step 4](#), click the BPG sub-tab and go to [Step 12](#).

- 
- 6** On the **BVG** sub-tab, the **VMSC IP Address** is a read-only field that contains the Virtual Mobile Switching Center (VMSC) address which is sent to the BSR by the BVG (Brick device) for voice data packet transport when the BSR's IPsec tunnel address and port number map to a corresponding MSC/MGW IP address and port number in the BVG's port mapping table.
- 
- 7** To enable the clean-up of failed or hung-up port mappings between the BVG (Brick device) and BSR(s), click the **Enable clean-up of expired mappings** checkbox to place a check in it. This option is enabled by default.
- If the **Enable clean-up of expired mappings** is checked, click the checkbox again to disable the option and remove the check.
- 
- 8** If the clean-up process was enabled in [Step 7](#), in the **Voice Mapping lifetime (hrs)** field, specify the time duration of a port mapping session, in hours. The minimum value is 1 hour.
- 
- 9** In the **CPU Utilization Threshold** field, enter a threshold value (percentage) for BVG mapping requests. By default, the CPU Utilization Threshold for BVG mapping requests is 70%. When this threshold value is reached, the BVG denies new port mapping requests.
- Requests to change existing mapping requests or delete existing mappings are not rejected if the threshold value is reached.
- 
- 10** To configure Real Time Protocol (RTP) Quality of Service (QoS) settings for the BVG, click on the **Enable QoS for RTP Traffic** checkbox.
- If you are not configuring RTP QoS settings for the BVG, skip to [Step 16](#).

**Result** If the RTP QoS option is enabled (**Enable QoS for RTP Traffic** checkbox is checked), the QoS for RTP parameter fields are activated (Figure 4-11, “BVG Sub-Tab (QoS for RTP Parameters)” (p. 4-28)).

**Figure 4-11 BVG Sub-Tab (QoS for RTP Parameters)**

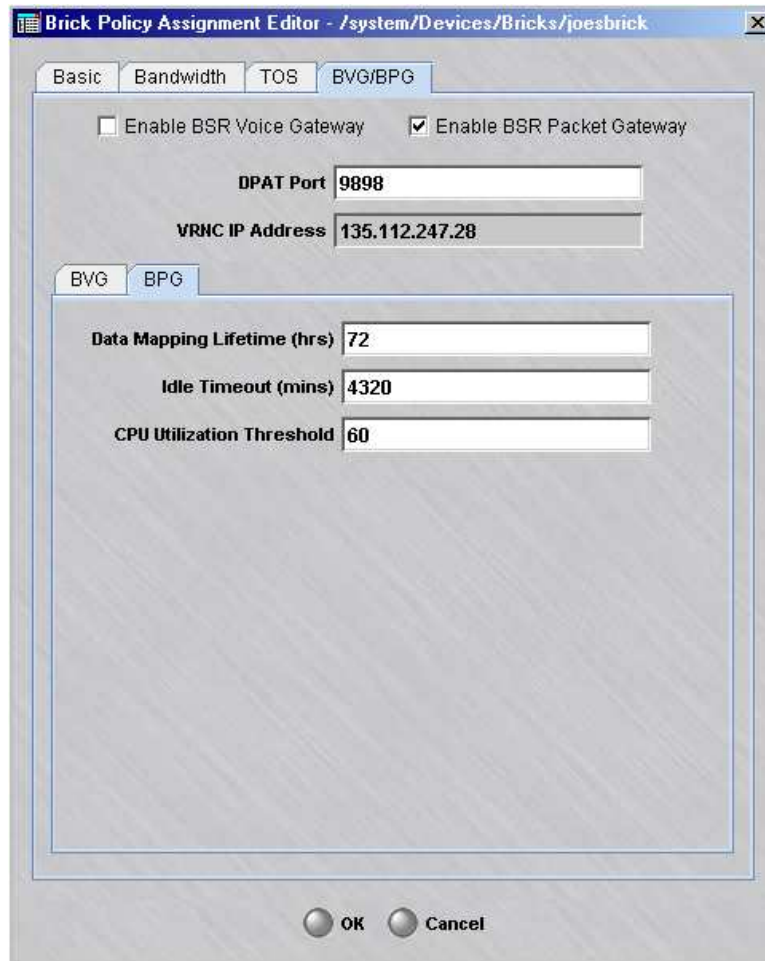


- 11 If the QoS for RTP Traffic option was enabled in Step 10, enter values for the following fields:
- **RTP Stream QoS Priority**—Click the down arrow next to this field to display a drop-down list and select the priority for BVG data packets over other traffic.
  - **Maximum Queue Latency (ms)**—enter the time limit (in milliseconds) for the BVG to queue congested RTP packets before discarding them (typically set to 40-60 ms). The maximum value for this field should be 100 to be consistent with the BSR jitter buffer size.

- **Enable In/Out Guarantee for all RTP Streams**—to set a minimum guaranteed QoS level for all incoming and outgoing BVG RTP traffic, click this checkbox, enter a value in the field to the right of the checkbox, and select the unit measurement from the drop-down list.  
*Note:* If the **Enable In/Out Guarantee for all RTP Streams** checkbox is unchecked, the configured value and unit measurement fields are greyed out and the option is disabled. The last configured value and unit measurement settings are retained so they can be re-applied if this option is reactivated at some later point.
  - **Enable In/Out Limit Per RTP Stream**—to set a maximum limit for each BVG RTP stream, click this checkbox, enter a value in the field to the right of the checkbox, and select the unit measurement from the drop-down list.  
*Note:* If the **In/Out Limit Per RTP Stream** checkbox is unchecked, the configured value and unit measurement fields are greyed out and the option is disabled. The last configured value and unit measurement settings are retained so they can be re-applied if this option is reactivated at some later point.
- 

- 12** If the BSR Packet Gateway (BPG) feature was enabled in [Step 4](#) and the BPG sub-tab was selected in [Step 5](#), the BPG sub-tab fields are displayed ([Figure 4-12, “BVG/BPG Tab, BPG Sub-Tab”](#) (p. 4-30)).

Figure 4-12 BVG/BPG Tab, BPG Sub-Tab



Go to [Step 13](#) to configure the BPG-related parameters.

- .....
- 13** In the **Data Mapping lifetime (hrs)** field, specify the time duration of a BPG/BSR port mapping session, in hours.

If the value of this field is zero or blank, the process to clean up expired mappings between the BPG and BSR(s) is disabled.

.....

- 14** In the **Idle Timeout (mins)** field, specify the period of inactivity (in minutes) that must transpire between the BPG (Brick device) and BSR(s) before the mapping session for data transfer is terminated.

If the value of this field is zero or blank, the process to clean up expired mappings between the BPG and BSR(s) is disabled.

.....

- 
- 15** In the **CPU Utilization Threshold** field, enter a threshold value (percentage) for BPG mapping requests. By default, the CPU Utilization Threshold for BPG mapping requests is 60%. When this threshold value is reached, the BPG denies new port mapping requests.

Requests to change existing mapping requests or delete mappings are not rejected if the threshold value is reached.

If you have finished setting parameters for the BPG feature ([Step 13](#) through [Step 15](#)), go to [Step 16](#).

- 
- 16** Click **OK** to activate your choices.

**Result** The BVG and/or BPG feature settings are activated.

END OF STEPS

---



## Static Routes

---

### Overview

The Brick device operates primarily as a bridging device, connecting two pieces of the same LAN segment. However, the Brick device has a Static Routing Table, and you can add routes to this table so that the Brick will send traffic to LAN segments that are not directly connected to any of its ports. A static route consists of the network address of the remote LAN and the source address of the next hop segment of the route.

### Brick device access to the static routing table

A Brick device cannot access its Static Routing Table until it is fully booted, is communicating with the SMS, and has downloaded its policies from the SMS. If the Brick is not directly connected to the SMS when it is booting, it must use the value in the **Gateway IP Address** field to route packets to the SMS.

The Static Routing Table can be loaded from the SMS or from the Brick flash memory, if the SMS cannot be contacted.

### Default static route

After the Brick has booted and downloaded its policies and static routes from the SMS, if there is no "default route" entry (0.0.0.0) in the Static Route Table, the Brick uses the **Gateway IP Address** as the default route. If there is a default route entry in the Static Route Table, the Brick uses this static route as the default route for all traffic, including traffic to the SMS.

### Cost-based routing

When multiple routes to the same destination can be defined, the SMS allows you to assign a cost-weighting value to each of these routes in the Static Route Table. The Brick routes traffic to this destination using the lowest cost available route. Route availability is determined by configuring an IP address to ping at a specified interval to test the route. If a ping to a device on the primary route fails after a specified number of attempts, that route is treated as no longer active and traffic is rerouted by the Brick device to the secondary route until that one fails, and so on. This method of defining static routes can be useful for dual PPPoE configurations or for load sharing between static routes.

If multiple routes in a given partition specify the same ping target, the same source address, and the same ping interval, only one ping is sent to the target device.

If a lower cost route is restored, the Brick device only switches to this route if the higher cost route becomes unavailable.



When there are two or more routes in the same partition with the same destination subnet and an identical cost value, but different next hop addresses, the Brick device transmits data on a round-robin basis across all of these routes, unless one of the routes fails.



## To Add a Static Route

---

### When to use

Use this procedure to add a route to a Brick Static Routes Table.

### Task

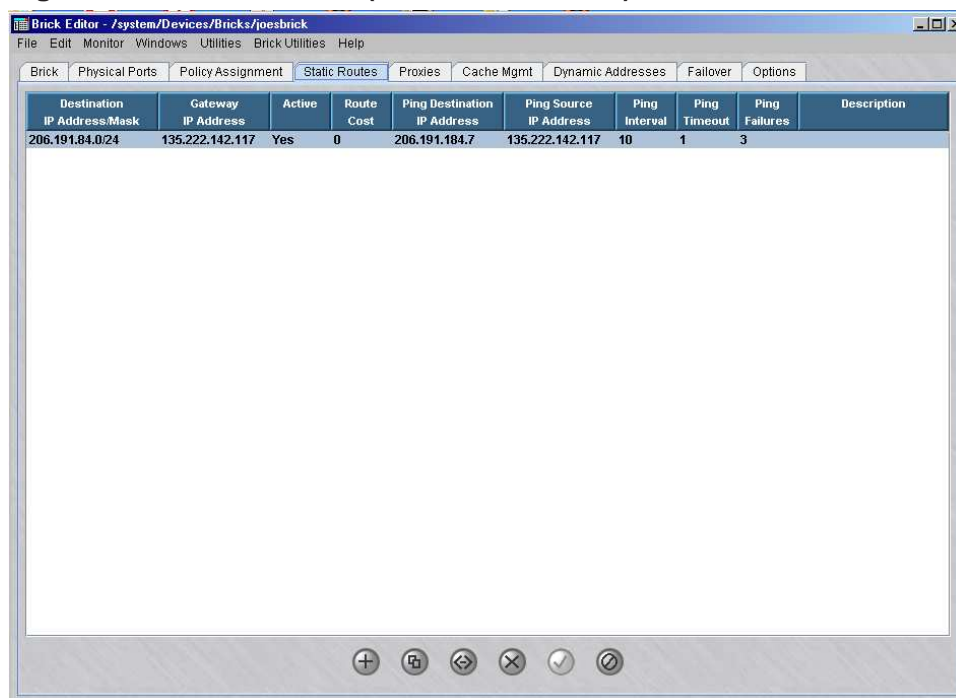
Complete the following steps to add a route to a Brick Static Routes Table.

---

- 1 If the Brick is currently displayed in the Brick Editor, click **Static Routes** to display the Static Routes tab (Figure 4-13, “Brick Editor (Static Routes Tab)” (p. 4-34)).

If the Navigator window is displayed, open the appropriate Group and Devices folders, and click the **Bricks** folder to display all configured Bricks. Double-click the desired Brick and click **Static Routes** to display the Static Routes tab.

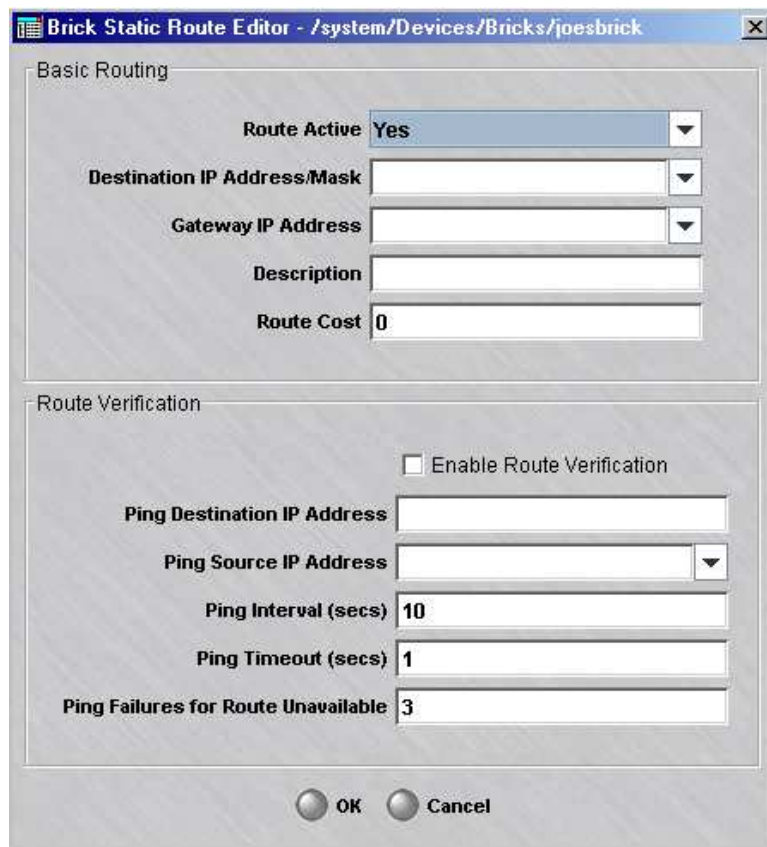
**Figure 4-13 Brick Editor (Static Routes Tab)**



- 2 To add a route, right-click in the Routes panel and select **New** from the pop-up menu.

**Result** The Brick Static Route Editor is displayed (Figure 4-14, “Brick Static Route Editor” (p. 4-35)).

**Figure 4-14 Brick Static Route Editor**



- 
- 3 Click the down arrow next to the **Route Active** field and select **Yes** to make this route active or **No** to define the route but leave it inactive. New routes are active by default.
- 
- 4 In the **Destination IP Address/Mask** field, enter the IP address for a single destination network, or click the down arrow to the right of the field to display a drop-down list, and select a host group from the list. Selection of a host group allows you to add a new static route for every IP address defined in that host group. Only host groups that are defined in the Brick’s group are available to be selected, and only those host groups with individual IP address entries can be used (wildcard character asterisks and comma-separated IP addresses in a host group will be ignored; IP address ranges in a host group will generate an error message).

A subnet/mask can be entered for an IP address but is not required. If a subnet/mask is not specified, the mask is /32.

- 
- 5 If the Gateway should be the Gateway obtained from the DHCP server or one of the two PPPoE sessions, then use the **Gateway IP Address** pull-down to fill in either *DHCP*, *PPPoE1*, or *PPPoE2*, whichever is appropriate. Otherwise, in the **Gateway IP Address** field, enter the IP address of the router that represents the first hop toward the destination. The Gateway address must fall within the IP range of one of the Brick ports.
- 
- 6 In the **Description** field, enter a textual description of the route. This field is optional.
- 
- 7 In the **Route Cost** field, enter a value (non-negative integer). The value of this field is zero, by default. This field is *required*.
- 
- 8 To enable route verification, click the **Enable Route Verification** checkbox. This feature is optional and disabled by default.
- 
- 9 If route verification was enabled in [Step 8](#), complete the following fields:
- In the **Ping Destination IP Address** field, enter the IP address of the router or other device to be pinged by the Brick to determine if this route is still available.
  - In the **Ping Source IP Address** field, enter the source IP address of the Brick interface from which the ping will originate (either a VBA for the Brick, interface/VLAN address, **PPPoE#1**, **PPPoE#2**, or **DHCP**).
  - In the **Ping Interval (secs)** field, enter the time interval for sending a ping, in seconds. The default value is **10** seconds.
  - In the **Ping Timeout** field, enter the maximum time to wait for a ping response, in seconds. The default value is **1** second.
  - In the **Ping Failures for Route Unavailable**, enter the number of consecutive responses to fail before the route is declared to be unavailable. The default value is **3**
- 
- 10 Click **OK** to dismiss the Brick Static Route Editor.
- Result** The new route is displayed in the Static Routes Table of the Brick Editor.
- 
- 11 Display the **File** menu in the Brick Editor and select **Save** or **Save and Apply**.

**Important!** Modified route entries do not become active until a Brick is applied.

END OF STEPS

---



## To Modify a Static Route

---

### When to use

Use this procedure to modify an existing static route.

### Task

Complete the following steps to modify an existing static route.


---

- 1 With the Static Routes tab of the Brick Editor displayed (see [Figure 4-13, “Brick Editor \(Static Routes Tab\)”](#) (p. 4-34)), double-click the route you want to modify.

**Result** The Brick Static Route Editor is displayed, with the destination network and gateway displayed.

---

- 2 Change either field in the window, as necessary.
- 

- 3 To duplicate an existing route and modify its parameters, select the route on the Static Routes tab of the Brick Editor and click the Duplicate () button.

**Result** The Brick Static Route Editor is displayed, with the destination network and gateway displayed. Make any modifications needed.

---

- 4 Click **OK**. The modified route will appear in the Brick Editor.
- 

- 5 Display the **File** menu in the Brick Editor and select **Save** or **Save and Apply**.

**Important!** Modified route entries do not become active until a Brick is applied.

END OF STEPS

---

□

## To Activate or Deactivate a Static Route

---

### When to use

Use this procedure to activate or deactivate an existing static route.

### Task

Complete the following steps to activate or deactivate an existing static route.

- 1 With the Static Routes tab of the Brick Editor displayed (see [Figure 4-13, “Brick Editor \(Static Routes Tab\)”](#) (p. 4-34)), select the route.  
.....
- 2 To activate the route, right-click to display a pop-up menu and select **Activate**, or simply click the Activate button at the bottom of the window.  
.....
- 3 To deactivate the route, right-click to display a pop-up menu and select **Deactivate**, or simply click the Deactivate button at the bottom of the window.  
.....
- 4 Select **Save and Apply** from the File menu to activate your choices.

.....  
E N D O F S T E P S  
.....



## To Delete a Static Route

---

### When to use

Use this procedure to remove a route from the routing table.

### Task

Complete the following steps to remove a route from the routing table.

---

- 1 With the Static Routes tab of the Brick Editor displayed (see [Figure 4-13, “Brick Editor \(Static Routes Tab\)”](#) (p. 4-34)), right-click the route you want to delete and select **Delete** from the pop-up menu.

**Result** A confirmation window is displayed ( [Figure 4-15, “Confirm Deletion Window”](#) (p. 4-40)).

**Figure 4-15 Confirm Deletion Window**



- 
- 2 Click **Yes** to confirm deletion of the row and dismiss the confirmation window. The route will no longer appear in the Static Routes tab of the Brick Editor.
  - 3 Display the **File** menu in the Brick Editor and select **Save** or **Save and Apply**.

**Important!** Changes do not become active until a Brick is applied.

END OF STEPS

---

□



## To Activate a Login Banner on the Brick Serial Port Console

---

### When to use

Use this task to activate a Login Banner on the Brick Serial Port Console.

You must reboot the Brick to enable the serial port.

### Task

Complete the following steps to activate a Login Banner on the Brick Serial Port Console.

---

- 1 Double-click on the desired Brick.

**Result** The Brick Editor is displayed.

---

- 2 Select the Options tab.

**Result** The Options tab is displayed.

---

- 3 Check the **Enable Serial Port** checkbox.
- 

- 4 In the **Password** field, enter a password. Passwords must be a minimum of six alphanumeric characters.
- 

- 5 Re-enter the password in the **Verify Password** field.
- 

- 6 In the **Login Banner** dialog window of the tab, enter the desired login text.

For example:

```
THIS SYSTEM IS RESTRICTED SOLELY TO AUTHORIZED USERS  
FOR LEGITIMATE BUSINESS PURPOSES ONLY. THE ACTUAL  
OR ATTEMPTED UNAUTHORIZED ACCESS, USE, OR  
MODIFICATION OF THIS SYSTEM IS STRICTLY PROHIBITED.  
UNAUTHORIZED USERS ARE SUBJECT TO COMPANY  
DISCIPLINARY PROCEDURES AND/OR CRIMINAL AND CIVIL  
PENALTIES UNDER APPLICABLE DOMESTIC AND FOREIGN  
LAWS.
```

---

- 7 From the File menu, choose **Save and Apply**.

**Result** The Apply Brick window is displayed.

.....

**8** Click the **OK** button.

.....

**9 Reboot** the Brick to activate the changes.

To disable the Serial Port Banner, repeat Steps 1 and 2 of this procedure and remove the Login Banner text. Reboot the Brick after saving and applying the changes. It is not necessary to disable the Serial Port to disable the Login Banner.

END OF STEPS

.....



# 5 Maintaining an Alcatel-Lucent *VPN Firewall Brick*<sup>TM</sup> Security Appliance Configuration

## Overview

---

### Purpose

This chapter explains how to maintain a Brick device configuration. Once a Brick device has undergone its initial configuration, you have to maintain the Brick device on the SMS to ensure its configuration and software remain up-to-date.

You can modify certain parameters of a Brick device configuration, or delete the Brick device altogether if it is no longer operational. It is also possible to move Brick devices, in case you create additional groups or folders, and want to reorganize the SMS interface.

You can also reboot the Brick device and refresh its MAC table from the SMS. Finally, if new software is released, you can download it to the Brick device from the SMS.

### Contents

<a href="#">To View a Brick Snapshot</a>	5-3
<a href="#">To Modify a Brick</a>	5-6
<a href="#">To Apply Changes to a Brick Device</a>	5-7
<a href="#">To Delete a Brick Device</a>	5-11
<a href="#">To Move a Brick Device</a>	5-12
<a href="#">To Reboot a Brick Device</a>	5-13
<a href="#">To Reboot a Brick Device via the SMS</a>	5-14
<a href="#">To Refresh the MAC Table</a>	5-16
<a href="#">ARP and MAC Handling in the Brick</a>	5-18
<a href="#">Static MAC and ARP Assignments</a>	5-20
<a href="#">To Initiate a Ping or Traceroute from a Brick Device</a>	5-22
<a href="#">To Download Software to a Standalone Brick</a>	5-24

<a href="#">To Download Software to a Failover Brick</a>	<a href="#">5-26</a>
<a href="#">To Download Software to Multiple Bricks</a>	<a href="#">5-27</a>
<a href="#">To Configure Intelligent Cache Management</a>	<a href="#">5-29</a>



## To View a Brick Snapshot

---

### When to use

Use this procedure to view a snapshot of the current configuration of a selected Brick.

### Task

Complete the following steps to view a snapshot of the current configuration of a selected Brick.

- 
- 1 Click on the **Bricks** folder in the Folders panel.

**Result** A list of currently configured Bricks is displayed in the Contents panel.

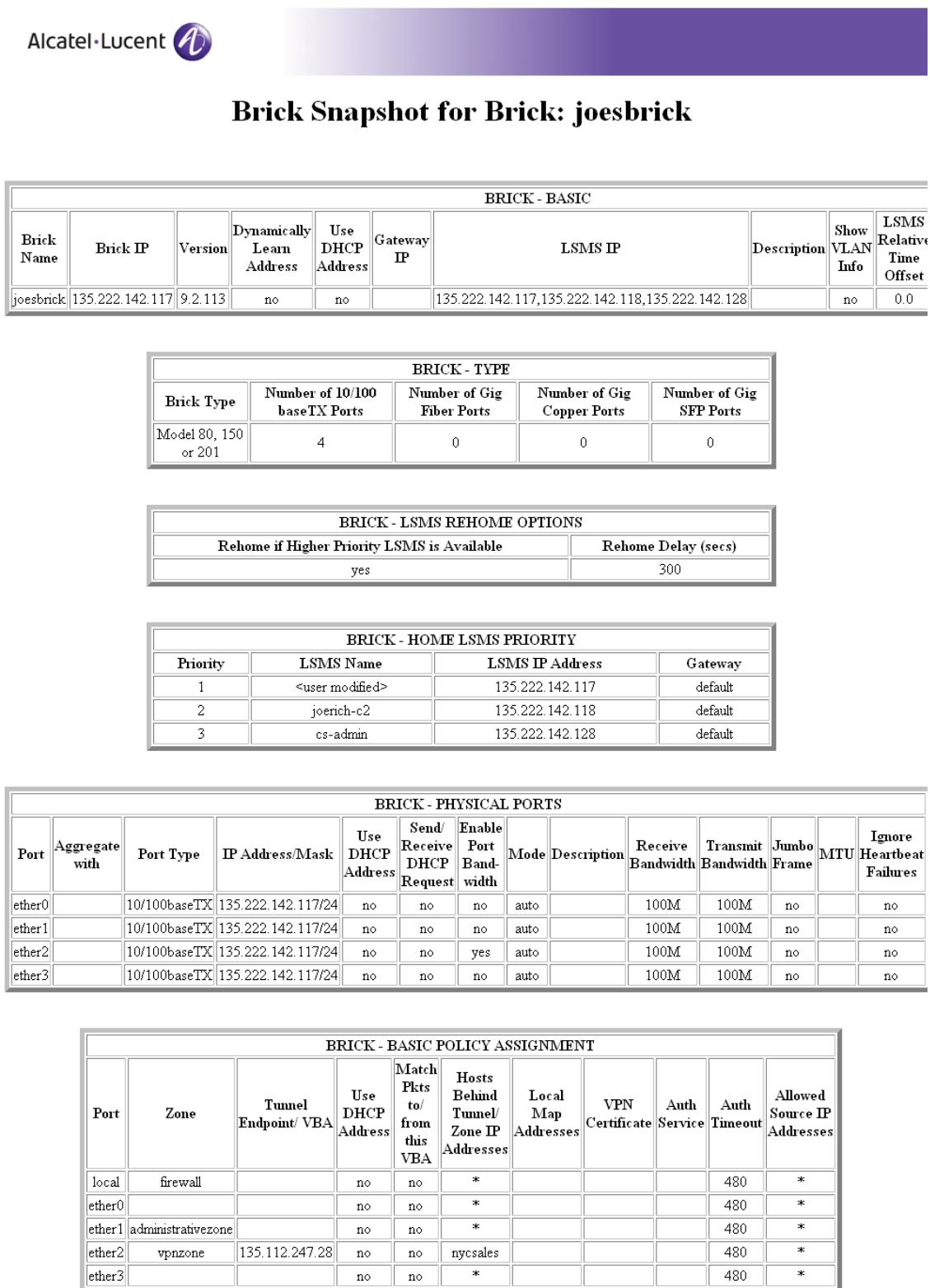
---

- 2 Right-click on a Brick and select **View Brick Snapshot**.

**Result** A snapshot of the selected Brick's current configuration is displayed.

[Figure 5-1, "Brick Snapshot" \(p. 5-4\)](#) shows an example of a portion of a Brick snapshot.

Figure 5-1 Brick Snapshot



Any additional user-defined fields that are part of a Brick's configuration and have been enabled via the SMS Parameters Editor are also displayed in the Brick snapshot view. For more details about user-defined fields in a Brick configuration, refer to the [“Adding user-defined fields when configuring a Brick”](#) (p. 3-19) section in Chapter 3, *“Configuring and Activating an Alcatel-Lucent VPN Firewall Brick™ Security Appliance”*.

.....  
E N D O F S T E P S



## To Modify a Brick

---

### When to use

Use this task to modify a Brick device configuration.

You cannot change a Brick device name or IP address. To change either of these, you have to delete the Brick device and re-enter it with the modified information. Then, you have to make a floppy and activate the Brick device again, as you did initially.

To change any other configuration information, follow the steps below. After certain changes (for example, changing the *halt all traffic if audit fails* parameter on the Options tab), you will be prompted to reboot the Brick device for the changes to take effect.

Procedurally:

1. With the Navigator window displayed, open the appropriate Group and Devices folders, and click the Bricks folder to display all configured Bricks.
2. Double-click the Brick to be modified. The Brick Editor is displayed with the configuration of the selected Brick.
3. Make any necessary changes to any of the tabs.
4. Display the File menu and select **Save**.





## To Apply Changes to a Brick Device

---

### Task

Whenever you make a change to a Brick device configuration, you have to apply the changes to the device. To do this, follow the steps below:

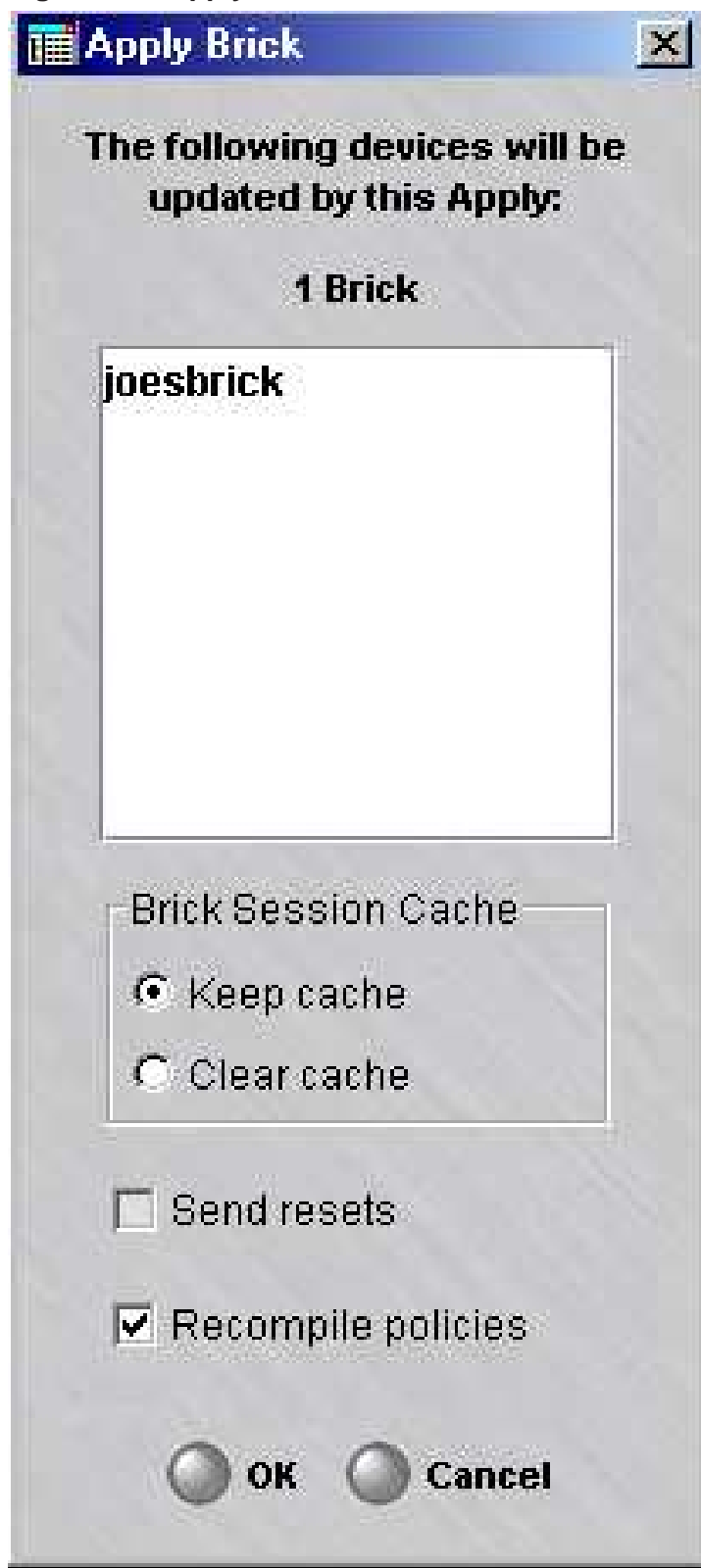
---

- 1 If the Brick device is currently displayed in the Brick Editor, display the Utilities menu and select **Brick▶Apply**.

If the Bricks are displayed in the Navigator window, right-click the Brick you want and click **Apply** from the pop-up menu.

The Apply Brick window is displayed ([Figure 5-2, “Apply Brick Window” \(p. 5-8\)](#)). Note that the Brick you are applying (updating) appears in the left panel on top.

Figure 5-2 Apply Brick Window



- 
- 2 When performing the apply, you have the option of keeping or clearing the Brick session cache. The default is to keep the cache. To clear the cache, click the **Clear Cache** radio button.

The **Keep cache** option will preserve all active sessions while applying the Brick and policy changes to the Brick. Any rule changes will not affect current sessions until the cache timeout value for that rule is reached. New sessions will be processed using the new ruleset.

The **Clear cache** option kills all active sessions and immediately implements any policy changes. Some sessions may be reestablished automatically. However, strict TCP enforced sessions and other session types may not be reestablished without user intervention. In addition, some client tunnels may be disrupted or lost. You will have to contact the client users and instruct them to re-enable their tunnels. You could also disrupt some sessions in progress, including FTP sessions and sessions allowed by rules with dependency masks.

- 
- 3 If you select **Clear Cache**, the **Send Resets** checkbox, which was grayed-out, becomes active and is checked by default. If you keep this box checked, the Brick will send TCP resets to all TCP sessions it is clearing. The Brick sends two resets per session: one to each endpoint, using the other endpoint as the source address. This makes it appear to each endpoint that the other endpoint has aborted the connection.

If the resets are not sent, the endpoint will continue to retransmit any outstanding (unacknowledged) packets it was sending for some number of minutes. If TCP strict enforcement is in effect, these retransmissions will be dropped. By sending the resets, the Brick forestalls these retransmissions.

Also, depending on the application, the end user may be given timely notification that the connection has been broken.

- 
- 4 You have the option of recompiling the policies associated with this Brick before applying the Brick. The default is to recompile the policies. If you do not want to recompile them, uncheck the **Recompile Policies** checkbox.

If you recompile the policies, all changes to the policies will be applied to the Brick. Therefore, if you want to update the Brick configuration, but *not apply any policy changes at this time*, uncheck the **Recompile Policies** checkbox.

- 
- 5 When you are ready to begin the apply, click **OK** to dismiss the Apply Brick window. The apply will take place.

**Important!** If, for some reason, the SMS is unable to contact the Brick device (as during a network outage, for example), the policy is automatically applied when connectivity between the Brick and SMS is restored.

END OF STEPS

---



## To Delete a Brick Device

---

### Before you begin

If you intend to delete a Brick device configuration, you first have to delete any tunnels that terminate on any of the Brick ports. If you do not do this, you will get a message indicating that the SMS cannot delete this Brick, because something depends on it.

Complete the following steps to delete a Brick device.

---

- 1 With all configured Bricks displayed in the Navigator window, right-click the Brick you want to delete and select **Delete** from the pop-up menu. The confirmation window shown below is displayed.

**Figure 5-3 Confirmation Window**



- 2 Click **Yes** to dismiss the confirmation window. The Brick will no longer appear in the Navigator window.

END OF STEPS

---



## To Move a Brick Device

---

### When to use

You can move a Brick device from one folder to another in the same group, or to a folder in another group. If you move a Brick device to a folder in a different group, all the policy components associated with the Brick device are copied to the appropriate folders in the new group. This includes Brick zone rulesets, host groups, service groups, application filters, dependency masks, LAN-LAN and client tunnels, and authentication services.

Complete the following steps to move a Brick device.

- 
- 1 With the **Bricks** folder displayed in the Navigator window, right-click the Brick device you want to move, and select **Move** from the pop-up menu.

**Result** A Browse window is displayed.

---

- 2 Select the folder in the Browse window to which the Brick device is being moved and click **OK** to dismiss the Browse window.

**Result** The Brick device and its associated policy components are moved to the appropriate folder.

---

- 3 Use the Navigator window to verify the move.

END OF STEPS

---



## To Reboot a Brick Device

---

### Methods of rebooting a Brick

There are two ways to reboot a Brick device. One way is to power the Brick on and off by toggling the power switch on the Brick device itself. To do this, someone has to be physically present at the Brick location.

The second way to reboot the Brick device is to do it remotely from the SMS.

**Important!** Whenever you reboot the Brick device, you should alert any Administrators who are overseeing client tunnels so that they can advise the Alcatel-Lucent IPSec Client users to re-establish their secure connections, which will be terminated by the reboot.



## To Reboot a Brick Device via the SMS

---

### Task

Complete the following steps to reboot a Brick device via the SMS.

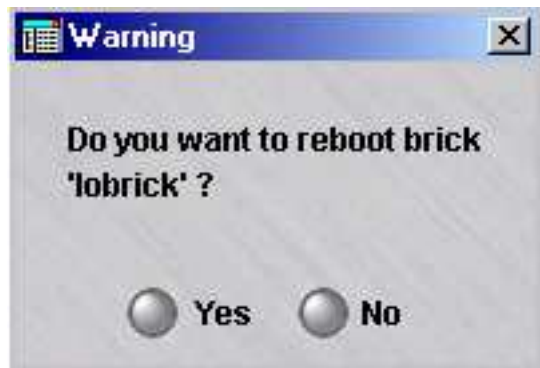
---

- 1 If the Brick device is currently displayed in the Brick Editor, open the Brick Utilities menu and select **Reboot**.

If the Navigator window is displayed, open the appropriate Group and Devices folders, and click the Bricks folder to display all configured Brick devices. Right-click the Brick device you want to reboot and select **Reboot** from the pop-up menu.

**Result** If it is a standalone Brick device, a dialog box similar to the following is displayed (Figure 5-4, “Warning Window for Rebooting Standalone Brick Device” (p. 5-14)).

**Figure 5-4 Warning Window for Rebooting Standalone Brick Device**



If the Brick device is part of a failover pair, a dialog box similar to the following is displayed (Figure 5-5, “Warning Window for Rebooting Brick Device in Failover Pair” (p. 5-15)).



Figure 5-5 Warning Window for Rebooting Brick Device in Failover Pair



- 
- 2 If the Brick device is part of a failover pair, and you want to reboot either the Active Brick device or the Standby Brick device, select the one to be rebooted (the Active Brick is the default selection) and click **Yes** to proceed with the reboot.

If it a standalone Brick device, just click **Yes** to proceed with the reboot.

---

- 3 When the reboot is complete, click **OK** to return to the Brick Editor.

**Important!** The *reboot* function should not be confused with the *make floppy* function. When you initially installed and configured the Brick, you went through the process of making a floppy disk, transferring the information from the floppy disk to the Brick's flash disk, and then booting the Brick from the flash disk.

The purpose of the make floppy function is to transfer encryption and authentication information (the security certificate) to the Brick so that it can communicate with the SMS.

The make floppy function generally needs to be performed only once, when the Brick is initially installed.

END OF STEPS

---



## To Refresh the MAC Table

---

### Overview

Media Access Control (MAC) addresses are hardware addresses that are hard-coded in all network interface cards. The Brick contains a table that keeps track of the MAC addresses of the hosts associated with each Brick port. For security reasons, the Brick will not allow you to move a MAC address from one port to another without refreshing the MAC table — unless you have checked the **Allow MAC Addresses to Move** checkbox on the Options tab of the Brick Editor. This prevents spoofing.

Complete the following steps to refresh the MAC table:

- 1 If the Brick is currently displayed in the Brick Editor, open the Brick Utilities menu and select **Refresh MAC**.
- 2 If the Navigator window is displayed, open the appropriate Group and Devices folders, and click the Bricks folder to display all configured Bricks. Right-click the Brick you want and select Refresh MAC from the pop-up menu.

**Result** A warning window similar to the one shown in [Figure 5-6, “Warning Window”](#) (p. 5-16) will appear.

Figure 5-6 Warning Window



- 3 Click **Yes** to confirm the refresh.

**Result** The table will be refreshed.

---

- 4** When the refresh is complete, click **OK** to return to the Brick Editor.

END OF STEPS

---



## ARP and MAC Handling in the Brick

---

### Overview

MAC addresses are stored when the Brick first receives a packet from a given source MAC address. If that packet is tagged, the MAC address is associated with the VLAN on which the packet is received. The size of the Brick MAC table varies with the Brick model, from several hundred thousand MAC addresses down to several hundred MAC entries. Though MAC addresses can be refreshed manually, or allowed to move, the MAC cache is never flushed. Once the MAC table is full, the Brick must be rebooted to clear the table.

An internal process starts to age MACs when they have not been used in a cache session or route for an extended period of time (about 9 hours). If a MAC address has not been referenced in that period of time, it is removed from the table, regardless of whether the MAC table is full. If the MAC table becomes full, an unreferenced MAC address will be removed immediately.

The Brick performs discovery of MAC addresses as well as ARP bindings when necessary, for packet forwarding purposes. This occurs in three different ways, using the Address Resolution Protocol (ARP):

### 1 HOST DISCOVERY

The Brick will transmit a broadcast ARP request in response to a need to forward a packet to a Layer-2 (MAC) address with no information about the location of that MAC address. Since the Brick will cache inbound source MAC addresses, this condition should occur only once for each new host added to the networks directly connected to the Brick.

If the Brick does not know what physical port or VLAN to use to transmit a packet, it drops that packet (under the assumption that upper-layer retransmits will recover it), and instead broadcasts an ARP Request to stimulate the destination host to identify and locate itself. Once a response is received, the MAC address of the recipient will be associated with a particular physical port (and VLAN, if the port is tagged), thereby allowing future packets to that host to be properly forwarded.

This ARP Request will only be sent on the appropriate subnet for that destination IP. Additionally, this ARP request will NOT be sent out on the physical port (and VLAN, if the port is tagged) on which the original packet was received. There is no need to forward the ARP Request out the original port: if both hosts are on that port, then they can communicate directly without the Brick being able to stop them.)

ARP entries used to stimulate MAC discovery will be timed out of the ARP cache. However, the MAC address of the host will be updated if a packet with that MAC address appears on another physical port, and the "Allow MAC addresses to move" checkbox is checked.

## 2 LOCAL GATEWAYS AND SPECIAL HOSTS

The Brick transmits a broadcast ARP Request when it needs to send a packet to a Gateway (router) to perform Layer-3 packet forwarding. This ARP request will contain the source IP address of the interface or VLAN directly connected to that Gateway, and the source MAC address of the associated physical port.

This ARP request will be sent out over all interfaces on the same subnet as the configured Gateway, or all VLANs containing that subnet. These ARP requests are performed initially when the Brick is booted, and then continuously refreshed afterwards. This action is also performed for any SMS hosts or LPA hosts on a directly-connected subnet.

ARP Requests of this type will be refreshed periodically using a unicast ARP Request, followed by a broadcast ARP Request later if unanswered. This process continues as long as that address remains statically provisioned in the Brick as a Gateway.

## 3 LOCAL HOSTS

The Brick transmits a broadcast ARP Request when it needs to send a packet to a locally-connected Host and has performed Layer-3 packet forwarding itself. This ARP request will contain the source IP address of the interface of the VLAN directly connected to that Host.

This ARP Request will be sent out all interfaces on the same subnet as the destination host, or all VLANs containing that subnet.

ARP entries used for local hosts will be timed out of the ARP cache. However, the MAC address of the host will be updated if a packet with that MAC address appears on another physical port. The "Allow MAC addresses to move" checkbox must be checked.

□

## Static MAC and ARP Assignments

---

### Overview

The Brick attempts to learn MAC and ARP binding information automatically based on information available in the surrounding network. However, since the protocols used to do so are inherently insecure, it is possible to attempt to cause the Brick to improperly learn the local network topology. To do so is fairly difficult, since it requires administrator-level access to a directly-connected host, but it is possible. Note that this possibility applies not only to the Brick, but to any network device (such as routers or switches) that rely on MAC addresses or the ARP protocol to help make packet forwarding decisions.

To help mitigate this possibility, the Brick has the ability to create "static" MAC and ARP assignments, which may not be overridden by observed network traffic. If you are concerned that your network may be of such a trust level that hosts directly connected to the Brick may be compromisable, creating static MAC and ARP assignments for directly connected routers (and/or SMS and LPA hosts) can help.

### Task

To create a static ARP or MAC assignment for a given Brick, you need to edit a file on the SMS host. This requires SMS operating system host access; therefore, this ability should only be given to the most trusted administrators. Follow these steps:

---

- 1 In the inferno.ini text file, create a new text line, using the following format:

```
staticXX=mac=AA:AA:AA:AA:AA:AA ip=BBB.BBB.BBB.BBB ether=C [vid=D] [soft={y | n}][badSrcMac={y|n}]
```

where

XX is an arbitrary number from 0-99 inclusive used to make this entry unique

AA:AA:AA:AA:AA:AA is the MAC address

BBB.BBB.BBB.BBB is the IP address

C is the physical port number (range depends on Brick type)

D is the VLAN ID (1-4094)

A static ARP entry is created by specifying the MAC and IP parameters. A static MAC entry is created by specifying the MAC and port parameters. The two may be combined in a single entry.

The soft parameter specifies whether or not the assignment may be updated if new information is discovered. If being used for security purposes, soft should be set to *n*, or omitted from the assignment.

The default for `vid` for static ARP entries is the VLAN ID in the default partition whose subnet includes the IP parameter address. In the case of static MAC entries, the default is the port default VLAN ID.

When the "Route Return Path Packets to Cached Source MAC Address" checkbox on the Brick editor is checked, the Brick will use the source MAC address on the first packet of a session to determine the routing for the return packets of that session. In some cases, such as with some VRRP and HSRP routers, this behavior may cause undesirable routing. The Brick supports the ability to disable this behavior for specific MAC addresses by creating a static MAC address and giving it the "badSrcMac=y" option.

Examples:

1. a static MAC assignment, assigning MAC 01-02-03-04-05-06 to ether3.  
`static1=mac=01-02-03-04-05-06 ether=3`
2. a static MAC assignment, assigning MAC 01-02-03-04-05-06 to ether3 and VLAN ID 27, allowed to be overridden  
`static5=mac=01-02-03-04-05-06 ether=3 vid=27 soft=y`
3. a static ARP binding MAC 01-02-03-04-05-06 to IP 10.1.1.1  
`static7=mac=01-02-03-04-05-06 ip=10.1.1.1`
4. a static combined MAC and ARP binding MAC 01-02-03-04-05-06 to IP 10.1.1.1 on ether4 and VLAN ID 36  
`static22=mac=01-02-03-04-05-06 ip=10.1.1.1 ether=4 vid=36`

- 
- 2 Change some option in the Brick. Save and Apply the Brick. Change the option back to its original value. Save and Apply the Brick again.

- 
- 3 Reboot the Brick.

END OF STEPS



## To Initiate a Ping or Traceroute from a Brick Device

---

### When to use

This feature allows an administrator to initiate an outbound ping or traceroute from a Brick to another device. To do this, you must first open a console window on the Brick, either by directly accessing the Brick or by using the SMS remote console or the SMS Remote Navigator console. You do not have to add any rules or make other policy modifications for the ping and traceroute to work.

### Ping

To execute a ping, you must include the IP address of the target device in the ping command. The Brick will report each success or failure individually in real-time, with round-trip time (in ms), plus an overall success rate as a count and percentage, including average round-trip time.

The syntax of the ping command is

```
ping [options] target_ip
```

where *target\_ip* is the IP address of the target device and the available options are:

- t ttl
- w timeout
- c (for continuous)
- n number of requests
- v vlantag
- i interface# to send ping to
- I interval between pings (in seconds)
- l data size (in bytes)
- s source IP
- o make packet come OUT of the zone
- ! (to bypass rule processing)

The ping command will default to a 64-byte packet sent every second for five seconds.

### Traceroute

To execute a traceroute, you must include the IP address of the target device in the traceroute command. The Brick will report each probe round-trip time with increasing TTL until the target is reached, in real-time.



The syntax of the traceroute command is

```
traceroute [options] target_ip
```

where *target\_ip* is the IP address of the target device and the available options are:

- t max ttl
- q max queries per hop
- w timeout
- v vlantag
- i interface# to send traceroute to
- U use UDP instead of ICMP
- l data size
- s source IP
- o make packet come OUT of the zone
- ! (to bypass rule processing)

The traceroute command will default to 3 x 64-byte ICMP ping packets sent to every TTL increment, with a one-second timeout.



## To Download Software to a Standalone Brick

---

### When to use

SMS upgrades, point releases, and patches will be released periodically via a CD-ROM or from a website. An administrator has to load the new software on the SMS, using the installation procedures provided with the software.

### Task

Once this has been done, the administrator has to update the software of each Brick connected to the SMS. To do this, follow the steps below:

- 1 If the Brick is currently displayed in the Brick Editor, open the Brick Utilities menu and select **Software Download**.

If the Navigator window is displayed, open the appropriate Group and Devices folders, and click the Bricks folder to display all configured Bricks. Right-click the Brick you want and select **Software Download** from the pop-up menu.

A warning window similar to the one shown in [Figure 5-7, “Warning Windows \(Standalone Brick\)”](#) (p. 5-24) will appear.

**Figure 5-7 Warning Windows (Standalone Brick)**



- 2 Click **Yes** to confirm the download. The software will be downloaded to the Brick. The download is carried out over an encrypted link.

- 
- 3** When the download is complete, click **OK** to return to the Brick Editor. A reboot is required to make the new software operational.

END OF STEPS

---



## To Download Software to a Failover Brick

---

### When to use

If you are downloading the software to a Brick that is part of a failover pair, you have the option of downloading the software to the active Brick only, to the standby Brick only, or to both the active and standby Bricks.

The procedure is the same as described above for a standalone Brick, except you will see the following message displayed (Figure 5-8, “Warning Window (Failover Brick)” (p. 5-26)).

Figure 5-8 Warning Window (Failover Brick)



Click **Yes-Only Active** to download the software to the active Brick, **Yes-Only Standby** to download the software to the standby Brick, **Yes-Both Active and Standby** to download the software to both Bricks, or **No** to terminate the download.

If the **Yes-Only Standby** option is selected, the software is downloaded to the Active Brick, copied to the Standby Brick, and then deleted from the Active Brick. Messages that the software is being downloaded appear on both Brick consoles, but only the Standby Brick software is updated.

□

## To Download Software to Multiple Bricks

---

### When to use

If you need to download software to more than one Brick, you can do this one Brick at a time, as described above, or you can download the software to all the Bricks in one operation. Since it is necessary to reboot a Brick after the software has been successfully downloaded, you can also include reboot instructions in the operation, so that all the Bricks are automatically rebooted after the download.

When performing the download and reboot, you can specify the Bricks in three ways:

- All the Bricks in a folder
- All the Bricks in a group
- All the Bricks in all groups for which you have full device permission

### Task

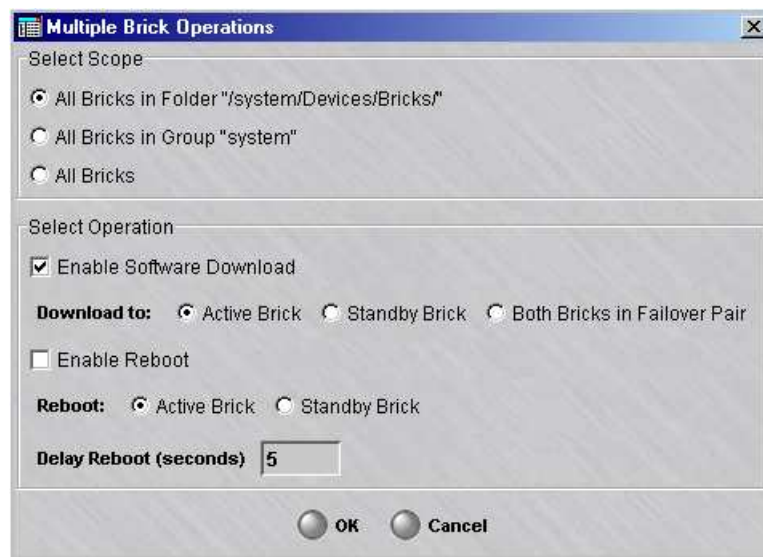
The following explains the procedure:

---

- 1 With the Navigator window displayed, right-click the Bricks folder and select **Software Download for Multiple Bricks** from the pop-up menu.

**Result** The Multiple Brick Operations Window is displayed ([Figure 5-9, “Multiple Brick Operations Window”](#) (p. 5-27)).

**Figure 5-9 Multiple Brick Operations Window**



You can also select **Software Download then Reboot Multiple Bricks** from the pop-up menu. The only difference is that the screen shown in [Figure 5-9, “Multiple Brick Operations Window”](#) (p. 5-27) is displayed with the **Reboot** checkbox already checked.

- 
- 2 When the Multiple Brick Operations Window first appears, the **All Bricks in Folder “/system/Devices/Bricks”** checkbox is checked. This means all Bricks in this folder will be rebooted. You can change this to all Bricks in the system group, or all Bricks that you have full device permission on, simply by clicking the appropriate checkbox.

---

  - 3 By default, the software will only be downloaded to active Bricks. If you have one or more failover pairs, and you want the software downloaded to both Bricks in the pairs, click the **Both Bricks in Failover Pairs** checkbox.

---

  - 4 If you want the Bricks to be automatically rebooted after the software has been downloaded, click the **Reboot** checkbox, and then indicate the delay time in the appropriate field (default = 5 seconds).

The delay time determines how long after the download the Bricks will wait before rebooting themselves. This allows the reboot command to apply to all Bricks before any of them actually begin the reboot process. This is important when one of the Bricks is a gateway, and you want to avoid the problem of having this Brick reboot before all the reboot commands reach the Bricks behind the gateway.

For failover Bricks, only the active Brick will be rebooted. If you intend to reboot the Bricks selectively, you may leave the **Reboot** checkbox unchecked.

END OF STEPS



## To Configure Intelligent Cache Management

---

### When to use

The SMS provides a patented intelligent cache management (ICM) feature that allows you to configure the Brick device so that if cache usage approaches a preset threshold, the Brick device automatically purges less important sessions to clear cache memory for new sessions.

The purpose of this feature is to help prevent denial-of-service attacks — in which attackers attempt to flood your network with a sustained stream of high-bandwidth traffic — from flooding the session cache and tying up valuable network resources. (A “session” is not just a TCP connection. The Brick device also treats UDP and ICMP packets as sessions. Some services (such as FTP) require multiple sessions.)

The intelligent cache management feature is one of three features built into the Brick device to protect against denial of service attacks. These features are described in greater length in the *Denial of Service Attacks* appendix.

### Determine the Threshold Levels

Some considerations when determining the threshold levels are:

---

- 1 The challenge in determining effective threshold levels for ICM is picking levels that will allow ICM to activate if the network is under attack, while making sure that ICM will not activate under a “normal” traffic load.

The challenge is to determine what a “normal” traffic load is. A reasonable approach is to monitor network traffic for some period of time and attempt to determine how much memory is needed (or how many sessions are created) during that period — particularly at peak traffic times. There are a number of things that can be done to shed light on that question:

- Look in the Proactive Monitor logs to find out what the peak cache memory usage is.
- Attach a protocol analyzer (a “packet sniffer”) to the network, capture packets, and analyze the captured packets to find out how many ICMP, UDP, and TCP packets there were over a period of time. Use that information (perhaps coupled with reports from the session logs) to determine how the cache class thresholds should be set.

Ideally, the thresholds should be set a little bit above what the expected peak memory usage is. With such settings in place, the Brick should be able to handle normal peak traffic flow without activating ICM; and if an attack causes cache memory usage to exceed the expected levels, ICM will activate to protect the Brick and the network.

END OF STEPS

---

## To set the threshold levels

To use the intelligent cache management feature to set global and session thresholds, follow the steps below:

- 1 If the Brick is currently displayed in the Brick Editor, click **Cache Mgmt** to display the Cache Management tab (Figure 5-10, “Brick Editor (Cache Management Tab)” (p. 5-31)).

If the Navigator window is displayed, open the appropriate Group and **Devices** folders, and click the **Bricks** folder to display all configured Bricks. Double-click the Brick you want and click **Cache Mgmt** to display the Cache Management tab.

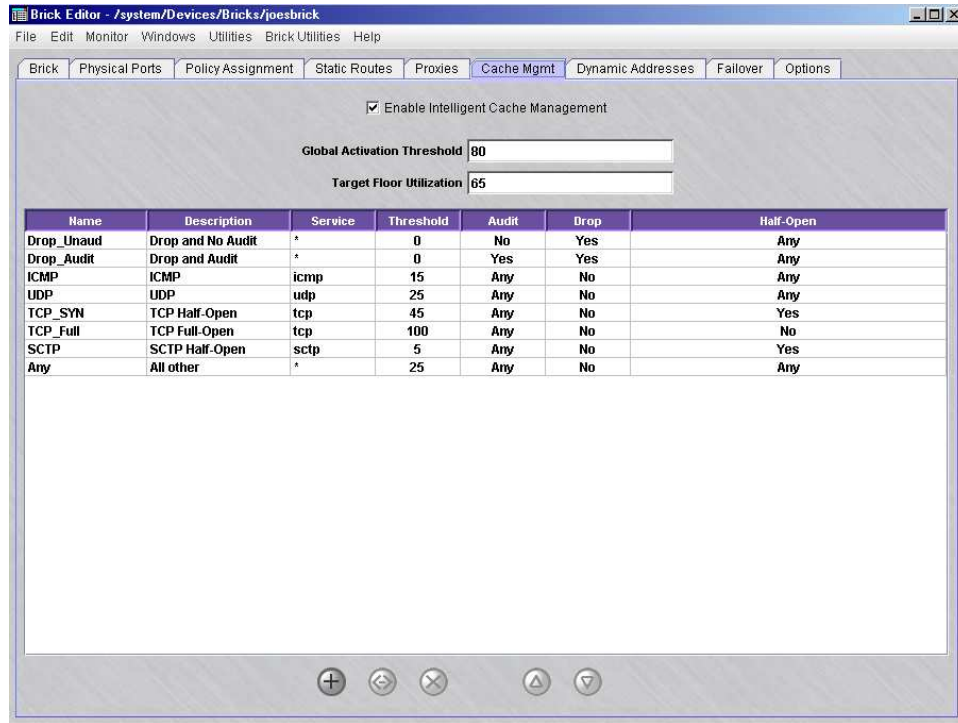
- 2 The **Enable Intelligent Cache Management** checkbox is checked by default. This causes the two global parameters and the session classes to become active. To disable this feature, uncheck this box.

- 3 Change the values in the **Global Activation Threshold** and **Target Floor Utilization** fields, if necessary. The defaults are 80% and 65%, respectively. These figures represent a percent of total cache capacity.

When the global activation threshold is reached, the intelligent cache management feature will begin scanning the session cache to identify sessions that can be cleared.



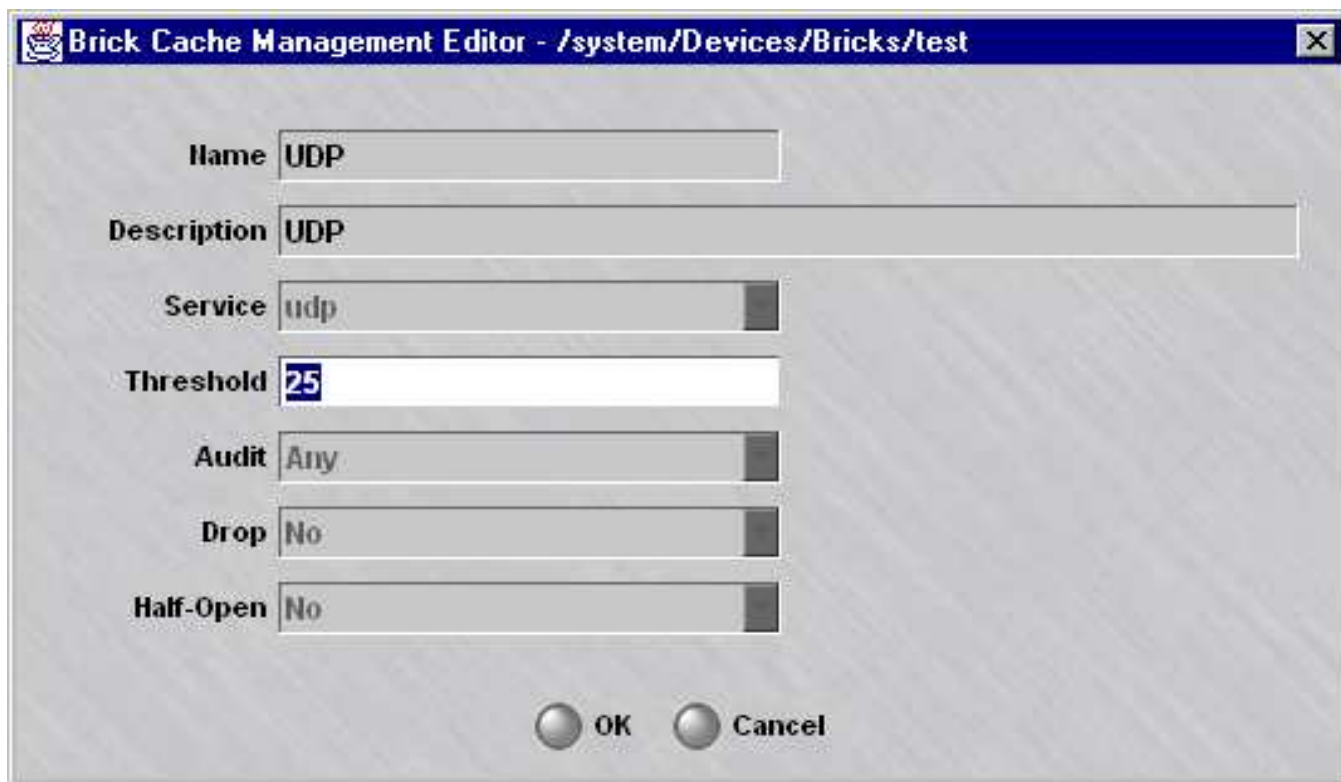
**Figure 5-10 Brick Editor (Cache Management Tab)**



- 4 Change the threshold for any of the five session classes, as necessary. To change a threshold, double click the session class to display the Brick Cache Management Editor (refer to [Figure 5-11, “Brick Cache Management Editor”](#) (p. 5-32)), and enter a value (percentage of cache capacity) in the **Threshold field**. Then, click **OK** to dismiss the Brick Cache Management Editor.

When the threshold is reached for a given session class, the intelligent cache management feature will begin clearing those types of sessions from cache.

Figure 5-11 Brick Cache Management Editor



- 
- 5 Display the **File** menu and select **Save**.

END OF STEPS

---

### Add an Entry to the Table

To add an entry to the Intelligent Cache Management Table, follow the steps below:

- 1 Right-click in the Cache Management tab of the Brick Editor and select **New** from the pop-up menu.

**Result** The Brick Cache Management Editor will appear. It is shown in [Figure 5-12, “Brick Cache Management Editor”](#) (p. 5-33).

**Figure 5-12 Brick Cache Management Editor**

The screenshot shows a window titled "Brick Cache Management Editor - /system/Devices/Bricks/internet\_brick". The window contains the following fields and controls:

- Name:** A text input field.
- Description:** A text input field.
- Service:** A drop-down menu.
- Threshold:** A text input field.
- Audit:** A drop-down menu with "Any" selected.
- Drop:** A drop-down menu with "Any" selected.
- Half-Open:** A drop-down menu with "Any" selected.
- Buttons:** "OK" and "Cancel" buttons at the bottom.

- 2 In the **Name** and **Description** fields, enter a name and brief description of this entry. The description is optional.
- 3 In the **Service** field, select a service from the drop-down list.
- 4 In the **Threshold** field, enter the threshold.
- 5 In the **Audit**, **Drop**, and **Half-Open** fields, select the appropriate value from the drop-down list. The values are **Yes**, **No** and **Any**.
- 6 Click **OK** to save the new entry and return to the Cache Management tab of the Brick Editor.

- .....
- 7 Open the File menu and select one of the **Save** options to save the new entry.

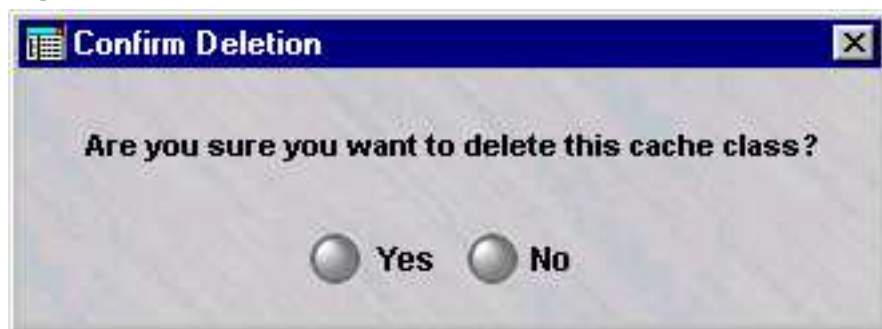
.....  
E N D O F S T E P S  
.....

### To delete an entry

Complete the following steps to delete an entry from the Intelligent Cache Management Table:

- .....
- 1 In the Intelligent Cache Management Table, right-click the entry you want to delete and select **Delete** from the pop-up menu. The confirmation window shown in [Figure 5-13, “Confirmation Window”](#) (p. 5-34) will appear.

**Figure 5-13 Confirmation Window**



- .....
- 2 Click **Yes**. The entry will be deleted from the table.

.....  
E N D O F S T E P S  
.....

□

# 6 Configuring VLANs on Alcatel-Lucent *VPN Firewall Brick*<sup>™</sup> Security Appliances

## Overview

---

### Purpose

This chapter explains how to configure a Brick to recognize, forward and filter VLAN-tagged frames.

### Contents

What is a VLAN?	6-2
Why Build VLANs?	6-4
Forwarding Packets and VLAN Boundaries	6-5
To Configure and Activate the Brick	6-6
To Configure the Brick Physical Ports for VLAN-Tagged Traffic	6-7
To Assign a Policy to the Ports	6-12
To Associate a Network with a VLAN	6-15
What are VLAN Bridge Groups?	6-18
To Enable a Brick to Support VLAN Bridge Groups	6-19
Configuring Bridging Between Specific VLANs	6-20
Save and Apply the VLAN Configuration	6-21



## What is a VLAN?

---

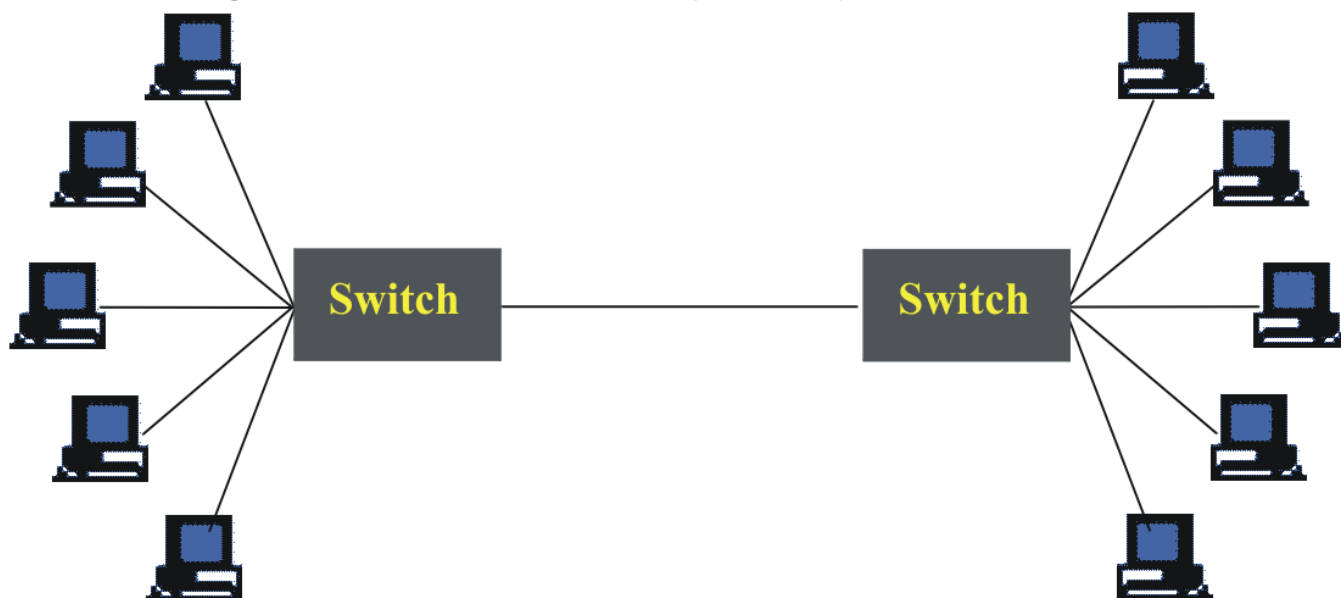
### Definition

A VLAN is a collection of hosts on different physical segments of a switched network that communicate with each other as if they were on the same segment. VLANs allow network administrators to define multiple LANs on a single collection of switches.

One useful way to think of VLANs is that the combination of the VLAN and the physical port form a virtual port. From this point of view, a trunk port is simply a collection of many virtual ports

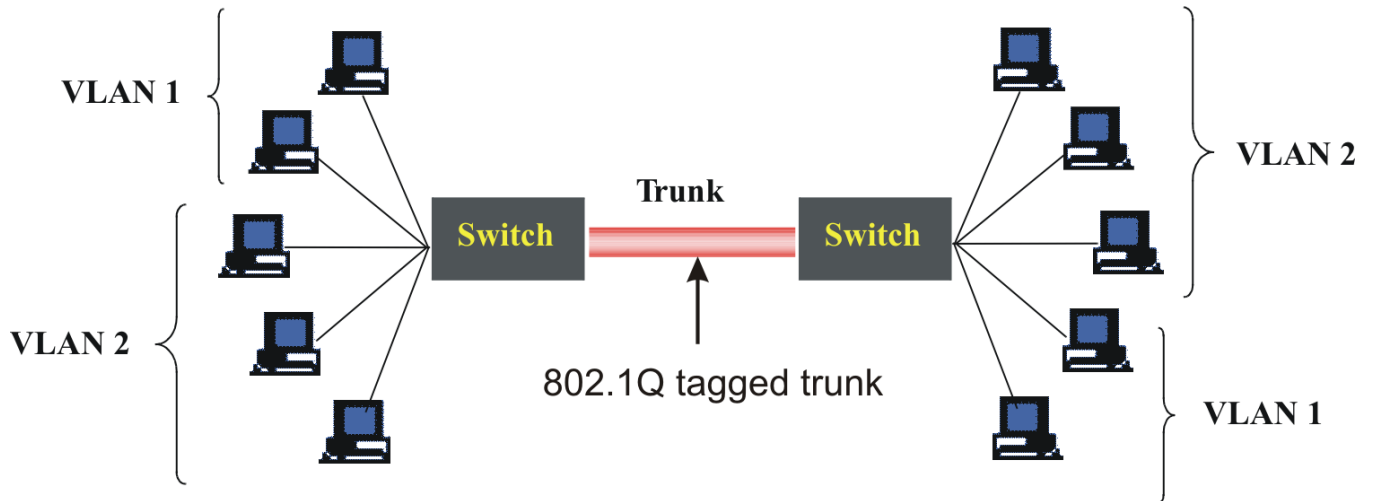
The diagram in [Figure 6-1, “Flat Switched Network \(no VLANs\)”](#) (p. 6-2) shows a typical flat, switched network with no VLANs implemented.

**Figure 6-1 Flat Switched Network (no VLANs)**



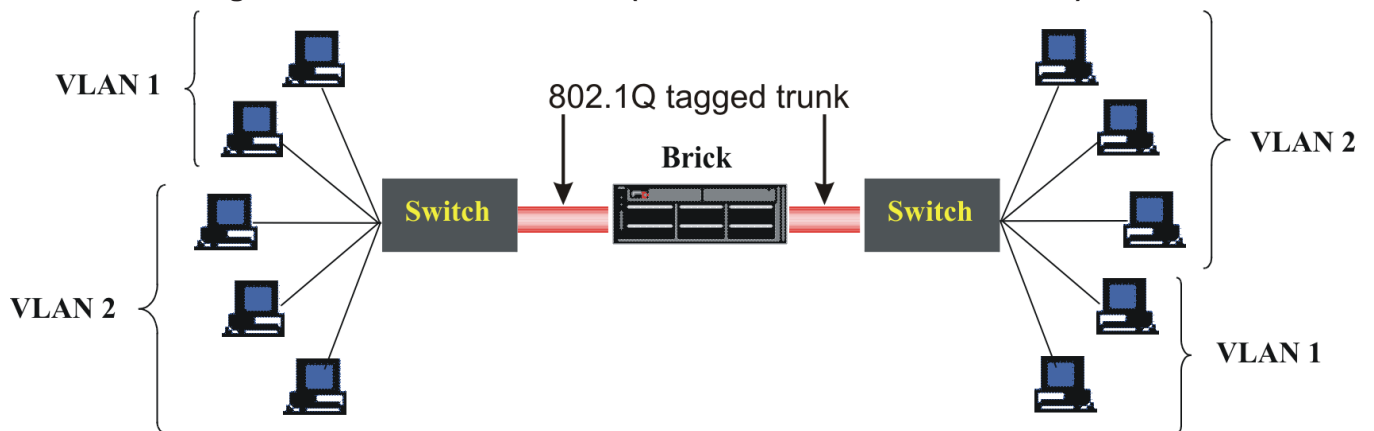
The diagram in [Figure 6-2, “Switched Network \(with two VLANs\)”](#) (p. 6-3) shows the same network after it has been subdivided into two VLANs. The VLANs allow network administrators to organize network resources by department, function etc., rather than physical connection.

Figure 6-2 Switched Network (with two VLANs)



The diagram in [Figure 6-3, “Switched Network \(with VLANs and Brick on trunk\)”](#) (p. 6-3) shows a Brick situated on a VLAN trunk between two switches. The Brick is able to apply security policies based on VLAN-tagged traffic as it passes between the two switches.

Figure 6-3 Switched Network (with VLANs and Brick on trunk)



□

## Why Build VLANs?

---

### The purpose of VLANs

A flat network, as illustrated in [Figure 6-1, “Flat Switched Network \(no VLANs\)”](#) (p. 6-2), is characterized by a large, unsegmented IP space. This architecture differs from a traditional routed IP infrastructure, where networks and subnets define a tree-like hierarchical topology, segregated by routers.

In a VLAN environment, specific ports on each switch are dedicated to specific VLANs, with trunk ports configured to handle traffic between the switches. Traffic on the trunk ports is tagged with a unique VLAN identifier. The switch that initially receives the frame from the host applies the tag to the frame and puts the frame on the trunk, where it is forwarded to the port on another switch that is assigned to that VLAN.

VLANs allow a network administrator to design a logical network so that hosts on physically diverse segments can be given the appearance of sharing a single broadcast segment. Switches on separate floors of a building can be connected by 802.1Q tagged trunks, which allows broadcast traffic to be transmitted on the correct ports of the correct switches, and nowhere else. Contrast this with ordinary switches or hubs where broadcast traffic is repeated on all ports of all devices.

Service providers use VLAN tagging on their internal backbone to enable them to identify packets inbound from a particular customer. This is enabled by routers that convert untagged inbound frames to 802.1Q tagged frames, which traverse the internal ISP backbone tagged by an identifier that can be traced back to a single port on a router. This differs significantly from using the IP address to track down the path of a packet, since IP relies on the sender to correctly fill in its own address. The VLAN tag is supplied by the router, and is based on the inbound port.

When service providers are hosting customers who use the same private addresses, the Brick partition feature can be used to keep the IP address space of each customer distinct. See [Chapter 7, “Configuring Alcatel-Lucent VPN Firewall Brick™ Security Appliance Partitions”](#) for details.

□



## Forwarding Packets and VLAN Boundaries

---

### Overview

When packets enter the Brick, those packets are always associated with a VLAN. If the packets are tagged (using 802.1Q), they are associated with the VLAN ID contained within the VLAN tag, provided that the VLAN ID is configured for the physical port. Otherwise, the packets are associated with the default VLAN assigned to the physical port at which they arrived. Default VLAN assignment occurs even if the Brick window is set not to display VLAN information (the LSMS creates VLANs automatically for the user).

The Brick forwards packets according to Layer-2 information (MAC addresses) where possible, and using Layer-3 information (IP addresses and routes) otherwise. broadcast packets (such as ARP requests) are restricted to the VLAN or VLAN bridge group on which they entered the Brick.

Normally, packets can only traverse or change VLANs via Layer-3 forwarding. That is, they must be routed using IP information associated with the Brick, either in the Static Routes table, or by using local VLAN or Interface IP addresses. While this is reasonable to set up, it requires allowing the Brick to participate in routing a packet at Layer-3, which may necessitate a large static routing table.

It may sometimes be advantageous to allow the packet to enter the Brick on a given VLAN, and be moved to a different VLAN before forwarding, without static IP routing. VLAN bridge groups allow this to occur. This process further enhances the Brick functioning as a transparent bridge, since it allows the Brick to facilitate passing packets at Layer-2, even when moving packets across VLANs. (See [“What are VLAN Bridge Groups?”](#) (p. 6-18) on [“What are VLAN Bridge Groups?”](#) (p. 6-18) for a description of VLAN bridge groups).

□

## To Configure and Activate the Brick

---

### When to use

To set up a Brick to process frames bearing VLAN tags, the first thing you have to do is configure and activate the Brick, just as you would any Brick.

If this has not already been done, refer to [Chapter 3, “Configuring and Activating an Alcatel-Lucent VPN Firewall Brick™ Security Appliance”](#) for complete instructions on how to configure and activate a Brick, and ensure it is communicating with the SMS.



## To Configure the Brick Physical Ports for VLAN-Tagged Traffic

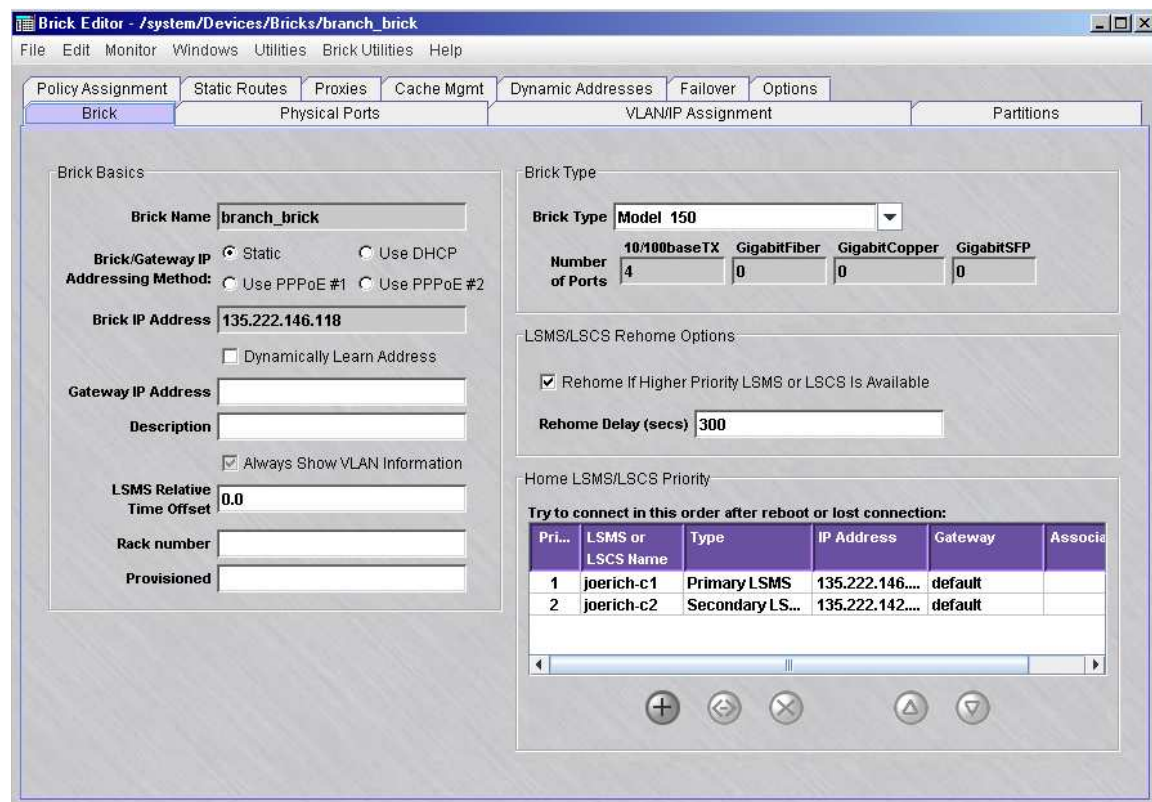
### Task

Complete the following step to configure the ports on the Brick that will be accepting VLAN-tagged traffic.

- 1 With the Navigator window displayed, open the appropriate group, Devices and Bricks folders, and double-click the Brick you want. The Brick Editor (Brick tab) will appear, with the configuration of the Brick you selected displayed.
- 2 Click the **Always Show VLAN Information** checkbox. Additional columns will now be added to the tables in the Physical Ports, Policy Assignment and Static Routes tabs, and two new tabs entitled **VLAN/IP Assignment** and **Partitions** will appear.

Figure 6-4, “Brick Editor (VLAN View)” (p. 6-7) shows the Brick tab of the Brick Editor after the checkbox has been selected.

**Figure 6-4 Brick Editor (VLAN View)**



**Important!** By default, the **Always Show VLAN Information** checkbox is unchecked. This is so those administrators who do not use VLANs will not see the VLAN fields and the VLAN/IP Assignment tab.

If you save the Brick configuration with the checkbox checked, VLAN information will be permanently displayed for that Brick. The checkbox will be grayed-out (as in [Figure 6-4, “Brick Editor \(VLAN View\)”](#) (p. 6-7)), and you will not be able to uncheck it.

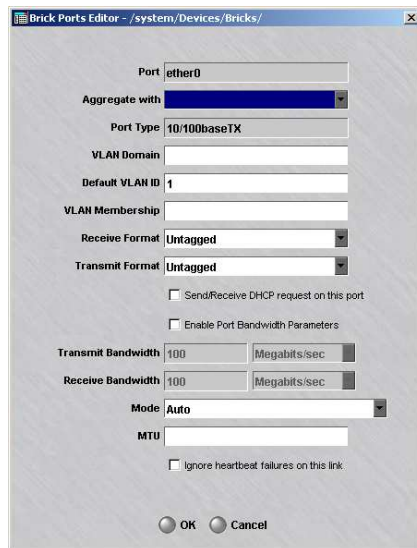
As long as no **save** operation is performed while this box is checked, you can toggle back and forth between a VLAN and non-VLAN view. Therefore, if you do not want to permanently view VLAN information, close without saving.

The fact that you are viewing VLAN information does not mean you are committed to using VLAN's, only that you are committed to viewing the VLAN fields and VLAN/IP Assignment tab.

Once this box has been checked, you must delete and re-create the Brick to not display VLAN information.

- 
- 3 Click **Physical Ports** to display the Physical Ports tab, and double-click a port that will be receiving VLAN traffic. The Brick Ports Editor will appear. It is shown in [Figure 6-5, “Brick Ports Editor”](#) (p. 6-8).

**Figure 6-5 Brick Ports Editor**



4 Enter the following information in the Brick Ports Editor.

Field	Description
Aggregate With	Select the port to be aggregated with this port. The aggregate port will become the parent port of the port receiving VLAN traffic; the child port assumes the policy assignment attributes, MTU attributes, QoS, and VLAN/IP assignments of the parent port.
Description	Enter a textual description of the port.
VLAN Domain	<p>The purpose of the domain identifier is to distinguish the VLANs assigned to this port. It allows the Brick to treat identical VLANs from different trunks differently.</p> <p>Leave this field blank unless the Brick is positioned between two switches with different VLAN numbering schemes.</p> <p>If this is the case, enter a lower-case letter from <b>a</b> to <b>n</b> to identify the VLAN domain associated with this port.</p>
Default VLAN ID	<p>The default VLAN ID is the ID number that will be assigned to all untagged frames entering this port.</p> <p>The default is <b>1</b>. You can change the default to any number from 0 — 4094.</p>
VLAN Membership	<p>Identifies all the incoming VLAN tags that will be permitted to access this port. The default VLAN ID for this port is automatically included in the VLAN membership, and should not be manually entered.</p> <p>You can leave this field blank, or you can enter any of the following:</p> <ul style="list-style-type: none"> <li>• A single VLAN ID</li> <li>• Multiple VLAN IDs separated by commas (1,2,3)</li> <li>• A range of VLAN IDs using a dash, with individual ranges separated by commas (1-3, 7-10)</li> <li>• An asterisk (*), indicating all VLAN IDs are acceptable</li> </ul> <p>If both the receive and transmit formats (see below) are untagged, you must leave this field blank.</p>
Receive Format	The frame format to be allowed into this port. The choices are <b>Untagged</b> (default), <b>802.1Q</b> , or <b>Any</b> .

Field	Description
Transmit Format	<p>The frame format the Brick will send out of this port. The choices are <b>Untagged</b> (default), <b>802.1Q</b>, <b>802.1Q Except Default</b>, or <b>Preserve</b>.</p> <p>Only certain combinations of receive and transmit formats are supported:</p> <ul style="list-style-type: none"> <li>• When the receive format is <b>Untagged</b>, the transmit format must be <b>Untagged</b>.</li> <li>• When the receive format is <b>802.1Q</b> or <b>Any</b>, the transmit format can be any of the above <i>except</i> <b>Untagged</b>.</li> </ul> <p>The normal setting for untagged links is Untagged, Untagged. The normal setting for tagged links is Any, Preserve.</p> <p><b>802.1Q Except Default</b> specifies that frames on the port default VLAN will be sent untagged, while frames on any of the other VLAN members for the port will be sent with 802.1Q tags.</p> <p><b>Preserve</b> means that when a frame is bridged (forwarded based on its MAC address), it will be sent as it was received (with or without a tag). If the frame is forwarded based on its IP address (i.e., is "routed"), this option behaves the same as <b>802.1Q Except Default</b>.</p>
Send/Receive DHCP request on this port	<p>Check this box to allow the Brick's DHCP requests to go out this particular port and replies to come back in. By allowing the DHCP request to go out only the port on which the DHCP server is located, you can prevent possible DHCP server spoofing from the other ports. At least one port must have this checkbox checked if a DHCP address is used anywhere on the Brick.</p>
Transmit Bandwidth Receive Bandwidth	<p><b>Transmit Bandwidth</b> and <b>Receive Bandwidth</b> are the "total" bandwidth in each direction.</p> <p>The value entered here restricts the maximum throughput that the Brick will transmit/accept on the interface. If the value is equal to or higher than the physical capacity of the link, then it serves only to bound the guarantees on the zones assigned to this physical port..</p>
Mode	<p>By default, a port will auto-sense the correct speed. However, you can specify the speed of the port and whether traffic should be configured in full duplex or half duplex mode on that port. Gigabit Fiber and SFP optic links are fixed at 1000 Gbps Full duplex, but autonegotiation may be disabled and flow control may be enabled or disabled with this option.</p>
MTU	<p>Maximum Transmission Unit is the largest size IP packet that the Brick will transmit on the interface. If left blank, it defaults to 1500 bytes.</p>

Field	Description
Ignore heartbeat failures on this link	Checking this box results in ignoring heartbeat failures between redundant Bricks on this link. It should be checked only if a known topology exists which prevents heartbeats from reaching the other Brick.

- .....
- 5 When you have finished entering the information above, click **OK** to dismiss the Brick Ports Editor and return to the Physical Ports tab of the Brick Editor. The information you entered will appear in the appropriate columns.

- .....
- 6 Repeat [Step 3](#) — [Step 5](#) for each additional port you need to configure.

.....

END OF STEPS

.....



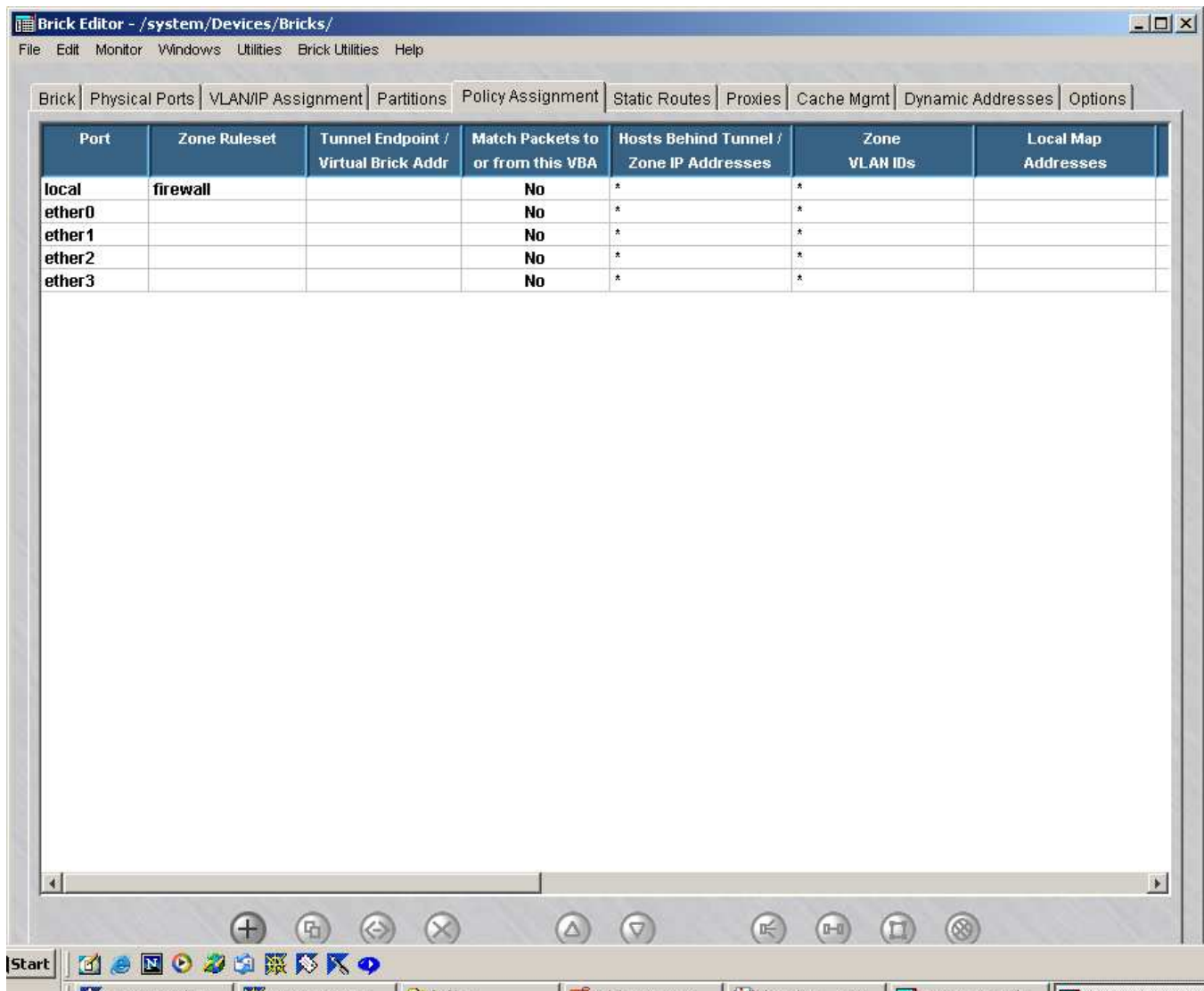
## To Assign a Policy to the Ports

### Task

Once the physical ports have been configured to recognize VLAN-tagged frames, you need to assign a security policy to the VLANs on each port. To do this, follow the steps below:

- 1 With the Brick Editor displayed, click **Policy Assignment** to display the Policy Assignment tab. It is shown in [Figure 6-6, “Brick Editor \(Policy Assignment Tab\)”](#) (p. 6-12).

**Figure 6-6 Brick Editor (Policy Assignment Tab)**



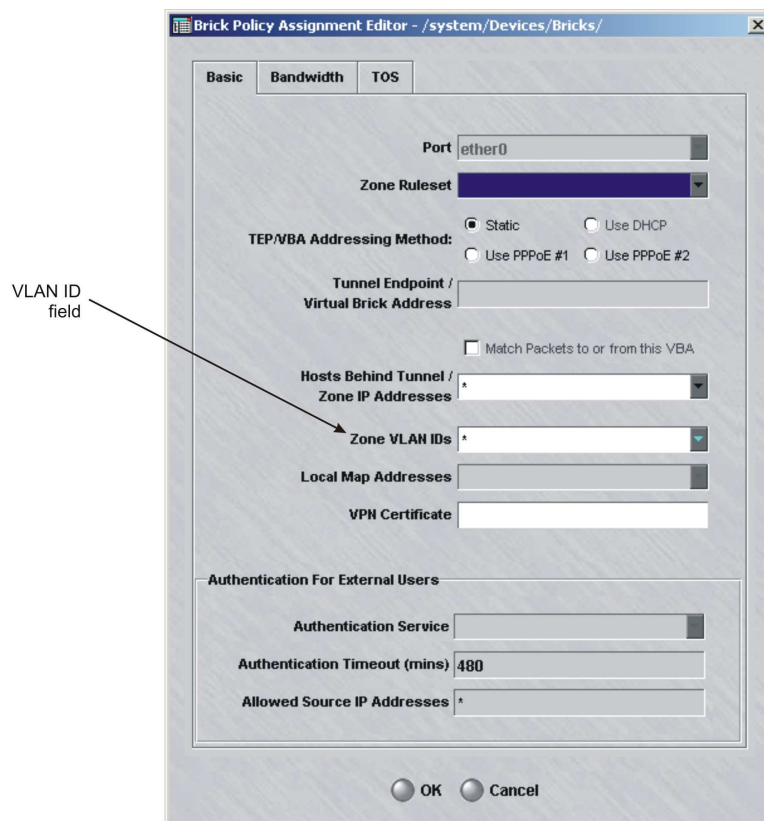


- 2 Double-click a port that will be receiving VLAN traffic. The Brick Policy Assignment Editor is displayed.

This is the window you use to assign a security policy (i.e. a Brick zone ruleset) to a Brick port (see ““To Configure a Physical Port” (p. 4-3)” in Chapter 3, “Configuring and Activating an Alcatel-Lucent VPN Firewall Brick™ Security Appliance”).

When the **Show VLAN View** checkbox is checked, this window has a VLAN ID field. The Editor and field are shown in Figure 6-7, “Brick Policy Assignment Editor” (p. 6-13).

**Figure 6-7 Brick Policy Assignment Editor**



- 3 Fill in all the fields as you ordinarily would when assigning a ruleset to a port, as explained in Chapter 4, “Configuring Alcatel-Lucent VPN Firewall Brick™ Security Appliance Ports”. In the **Zone VLAN ID** field, enter all the VLAN IDs on this port to which you want to assign this Brick zone ruleset. You can enter a single VLAN ID directly into the field, or a range of VLAN IDs separated by a dash. You can also enter a comma-separated list of single VLAN IDs or ranges of VLAN IDs.

The IDs you enter must be IDs defined for this port. IDs defined for this port include the default VLAN ID and all IDs in the VLAN membership. You can choose the entire membership, or you can enter a subset of the membership. For example, if the membership is 1—99, you could enter 1—10 in this field.

You can also select **Port Default** and the "asterisk" from the drop-down list. Port default is the default VLAN ID for this physical port as defined on the Physical Ports tab of the Brick Editor (see [Chapter 4, "Configuring Alcatel-Lucent VPN Firewall Brick™ Security Appliance Ports"](#), [Figure 5-2, "Apply Brick Window"](#) (p. 5-8)). The asterisk means the policy applies regardless of the VLAN ID.

Note that the drop-down arrow is blue, indicating that more than one entry can be selected for this field.

**Important!** Only one VLAN ID can be associated with a zone ruleset. Therefore, if there is a ruleset defined for this port, make sure no more than one VLAN ID is selected in this field.

- 
- 4 When you have finished entering the information above, click **OK** to dismiss the Brick Policy Assignment Editor and return to the VLAN Policy Assignment tab of the Brick Editor. The information you entered will appear in the appropriate columns.

END OF STEPS

---



## To Associate a Network with a VLAN

---

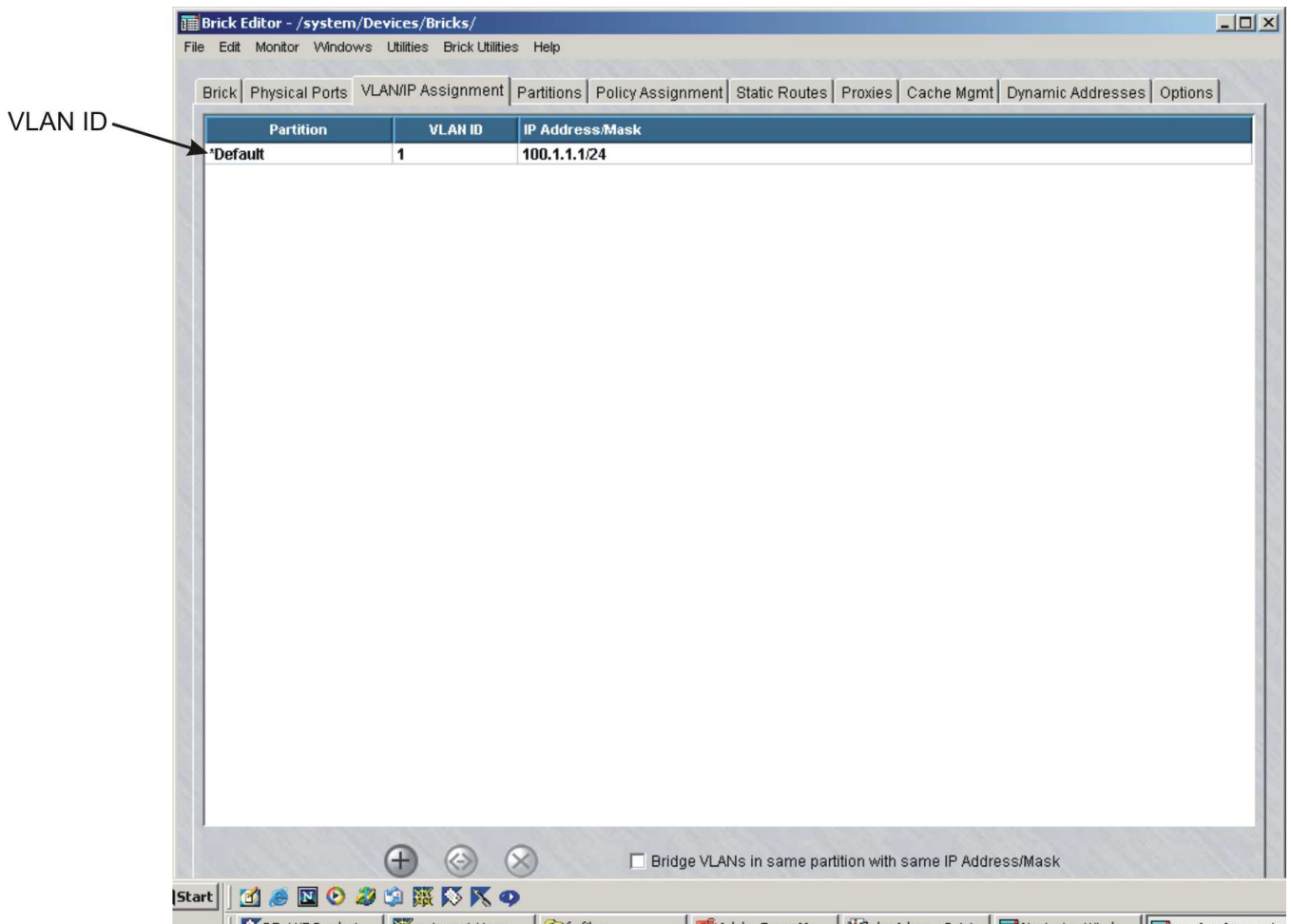
### Task

To assign a network (IP address/mask) to a VLAN (identified by its VLAN ID), follow the steps below:

---

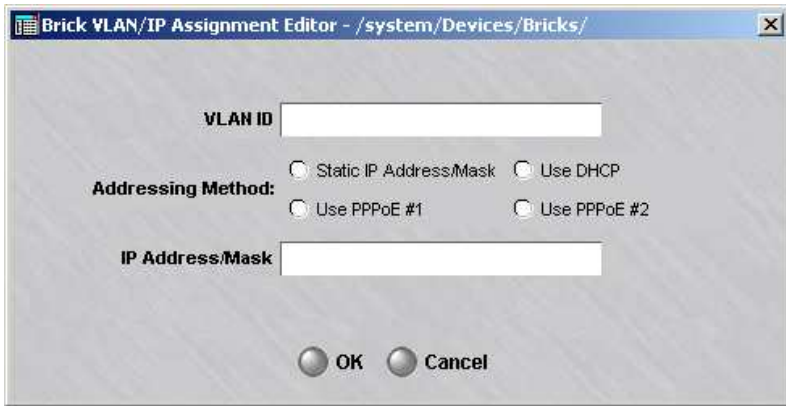
- 1 With the Brick Editor displayed, click **VLAN/IP Assignment** to display the VLAN/IP Assignment tab. It is shown in [Figure 6-8, “Brick Editor \(VLAN/IP Assignment Tab\)”](#) (p. 6-15). As this figure shows, the VLAN ID is automatically displayed and assigned the IP address of the Brick (including the appropriate subnet mask).

**Figure 6-8 Brick Editor (VLAN/IP Assignment Tab)**



- 2 To add a new VLAN ID and IP address/mask, right-click in the display area and select **New**. The Brick/VLAN IP Assignment Editor will appear. It is shown in [Figure 6-9](#), “Brick/VLAN IP Assignment Editor” (p. 6-16).

**Figure 6-9 Brick/VLAN IP Assignment Editor**



- 3 Enter the following information in the Brick/VLAN IP Assignment Editor. Multiple subnets can be assigned to the same VLAN by adding multiple entries with the same VLAN ID.

Field	Description
VLAN ID	Enter the domain and VLAN ID. Use the letter of the domain followed by a dot and the number of the VLAN ID (0 — 4094). The domain is optional.

Field	Description
IP Address/Mask	If the Address is statically assigned, then enter the IP address and mask to be associated with this VLAN ID. The mask is required.
Addressing Method	Check either the Use DHCP, Use PPPoE #1, or Use PPPoE #2 box (whichever is appropriate) if the Brick address on this VLAN is to be acquired dynamically rather than statically assigned.

**Important!** VLAN/IP assignment entries may now contain network addresses, in addition to host entries. This is useful if you want the Brick to be aware of the networks to which it is attached, but without using an IP address on the Brick itself. Network addresses are those that have a zero in the host portion of the address; for example: 10.1.1.0/24 is a network address, whereas 10.1.1.15/24 is a host address. Also, 192.168.15.128/28 is a network address, whereas 192.168.15.130/28 is a host address (since the host piece of the address with a 28-bit mask is the last 4 bits)

- 
- 4 When you have finished entering the information above, click **OK** to dismiss the Brick/VLAN IP Assignment Editor and return to the VLAN IP Assignment tab of the Brick Editor. The information you entered will appear in the appropriate columns.

END OF STEPS



## What are VLAN Bridge Groups?

---

### Definition

A VLAN Bridge Group is a set of VLAN IDs that can mutually bridge packets. That is, Layer-2 forwarding can be used among all members of a VLAN Bridge Group to cause packets to forward from one VLAN ID to another, without requiring Layer-3 routing.

Packets are routed using their destination MAC address. The Brick looks in its MAC cache to determine if the destination MAC address is known, and to determine to which virtual port that MAC address is bound. If that virtual port happens to be a different VLAN ID than the one on which the packet already exists, the Brick will modify the VLAN ID information on that packet such that it will be associated with the correct destination VLAN ID.

All members of a VLAN Bridge Group must have one or more addresses and IP subnets in common, since the Bridge Group essentially functions as a single VLAN. Layer-2 Broadcast packets and multicast packets are also sent to all members of a VLAN Bridge Group.

VLAN Bridge Groups are mostly used when separating security domains using VLANs on external devices connected to the Brick via 802.1Q tagged VLAN trunks. Note this may involve as few as one switch, with the Brick acting as a "one-legged firewall", scaling up to as many switches as necessary. (It is necessary to configure such attached switches to prevent packets from crossing VLAN boundaries; consult your switch vendor to determine the correct configuration for your switch, if applicable.)

Once enabled, VLAN Bridge Groups are created implicitly in the VLAN/IP Assignment tab, by simply assigning the same IP address and mask to multiple VLAN IDs. There are NO explicit VLAN Bridge Group objects that appear in the SMS Navigator.

VLAN Bridge groups never include a VLAN whose address is assigned via DHCP or PPPoE.



## To Enable a Brick to Support VLAN Bridge Groups

---

### Task

To enable a Brick to support VLAN bridge groups as well as configuring bridge groups themselves, follow the steps below:

- 1 With the Navigator window displayed, open the appropriate group, Devices and Bricks folders, and double-click the Brick you want. The Brick Editor (Brick tab) will appear, with the configuration of the Brick you selected displayed.
- 2 Click **VLAN/IP Assignment to** display the VLAN/IP Assignment tab. Click the **Bridge VLANs in same partition with same IP/Mask** checkbox. This step needs only be performed once, regardless of the number of VLAN bridge groups set up on a given Brick. Once the checkbox is checked, you can skip this step.

END OF STEPS



## Configuring Bridging Between Specific VLANs

---

### Task

A VLAN bridge group is configured implicitly in the VLAN/IP Assignment screen, once the feature is enabled.

---

- 1 In the VLAN/IP Assignment tab, either choose an existing VLAN entry or create a new one by following the standard procedure.

---

- 2 To add a new VLAN bridge group, simply create a new VLAN/IP assignment with the same network or networks as specified in the chosen VLAN/IP assignment entry, and a different VLAN ID. IP address/mask pairs must match precisely. An error condition will result if an identical IP address is entered with a different subnet mask. If some, but not all, of the networks are identical, only packets destined to the identical networks will be part of the Bridge Group. Also note that all VLAN IDs in a VLAN Bridge Group must be in the same Brick Partition.

---

- 3 Repeat Step 2 for as many VLAN groups as required in the VLAN Bridge Group.

---

- 4 You may also create as many different VLAN Bridge Groups. Each VLAN Bridge Group is identified by the shared IP networks that span it.

END OF STEPS

---





## Save and Apply the VLAN Configuration

---

### Task

Once the ports have been configured for VLAN traffic, you have to save and apply the configuration. Open the File menu and select **Save and Apply**.





# 7 Configuring Alcatel-Lucent *VPN Firewall Brick*<sup>™</sup> Security Appliance Partitions

## Overview

---

### Purpose

Brick partitions allow true virtual firewalls to be implemented on the Brick device. Each virtual firewall has its own routing information, its own set of IP addresses, its own firewall policies, and so forth. In fact, each partition maintains its own session table, to ensure complete uniqueness and isolation for the virtual firewall.

For example, in a service provider environment, it is frequently necessary to ensure that packets *cannot* cross VLANs unless they are explicitly allowed. This circumstance may arise when a set of conflicting or "overlapping IP addresses" are used by two disjointed networks connected to two different physical or virtual interfaces. In this case, Brick Partitions ensure that sessions are distinct, regardless of IP addressing, as well as ensuring that packets CANNOT cross from one VLAN to another, unless an explicit route is created.

Brick partitions are created using the VLAN capabilities inherent to the LVF Brick. Each partition is created by choosing a set of VLANs that belong to it, and giving the Partition a name. (It is NOT necessary to use 802.1Q VLAN tagging to support Brick Partitions, since the Brick always relates packets to VLANs internally.)

The Brick partition feature requires that the Brick be displaying VLAN information. This is accomplished by checking the **Always Show VLAN Information** checkbox (see "[To Configure a Brick Device on the SMS](#)" (p. 3-19)" in Chapter 3, "[Configuring and Activating an Alcatel-Lucent VPN Firewall Brick<sup>™</sup> Security Appliance](#)").

### Contents

<a href="#">What are Brick Partitions?</a>	7-3
<a href="#">Configure Brick Partitions</a>	7-4
<a href="#">Use Static Routes with Partitions</a>	7-6

Allow Partitions to Intercommunicate with Static Routes	7-7
Save and Apply the Brick Configuration	7-10
Interpreting IP Addresses When Brick Partitions Are Configured	7-11



## What are Brick Partitions?

---

### Definition

Brick partitions are used to create true virtual firewalls, with no potential of confusion or ambiguity in rulesets or session cache entries. Brick partitions are also designed to allow traffic to only traverse VLANs where explicitly allowed. Without Brick partitions, packets in a given VLAN are free to route to other VLANs where policy and configuration allows.

For example, it is possible to conceive of a network where a service-provider edge connects to two different customers. Both customers use the 10.0.0.0/8 network internally, though they have legal, registered addresses externally.

Brick partitions allows the Brick to treat each entity as completely separate at Layer-2, regardless of the fact that their IP address ranges overlap. With Brick partitions, traffic from one customer's host 10.1.2.3 is treated as completely distinct from traffic on the other customer's host 10.1.2.3, even if they are accessing the same destination server, on the same TCP ports.

Once a zone is assigned to a VLAN on one or more ports on a Brick, it is effectively assigned to that VLAN's partition as well. The same zone may not be assigned to more than one partition on a Brick. There is a restriction on Virtual Brick Addresses (VBAs). VBAs must be unique on the Brick. Therefore the same VBA cannot be used for different zones even if the zones are in different partitions.

Brick partitions must be used in conjunction with static routes to allow partitions to intercommunicate. Additionally, network address translation must be configured if the partitions contain overlapping IP addresses, as in the above example.

Brick partition objects are created per-Brick, and not shared across Bricks.



## Configure Brick Partitions

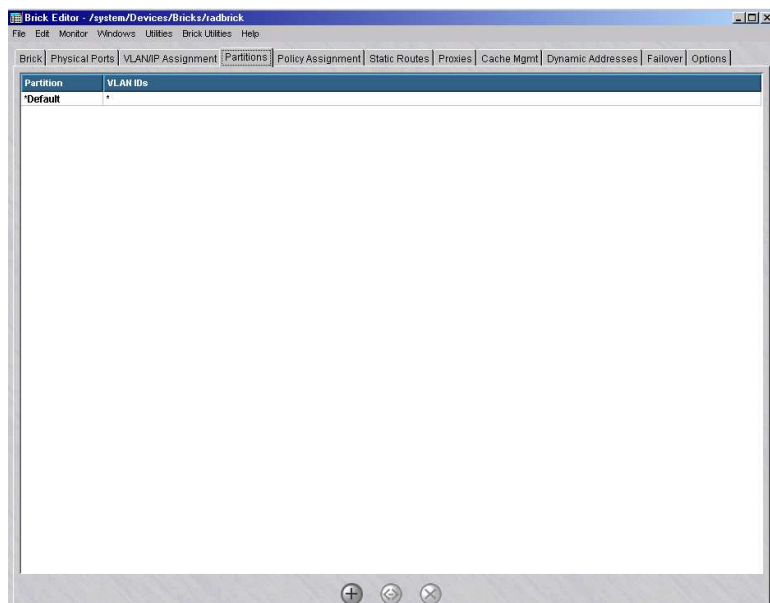
---

### When to use

Brick partitions are configured as named objects. Each set of Brick partitions is created for a given Brick. For each Brick, you must configure the desired set of Brick partitions, along with appropriate static routing information. To do this, follow the steps below:

- 1 With the Navigator window displayed, open the appropriate group, Devices and Bricks folders, and double-click the Brick you want. The Brick Editor (Brick tab) will appear, with the configuration of the Brick you selected displayed.
- 2 Click the **Partitions** tab to display a list of Brick partitions currently configured for that Brick. [Figure 7-1, “Brick Editor \(Partition Tab\)”](#) (p. 7-4) shows this display.

**Figure 7-1 Brick Editor (Partition Tab)**



Note that in [Figure 7-1, “Brick Editor \(Partition Tab\)”](#) (p. 7-4), the only entry is “\*Default.” If no partitions are configured, a single entry called “\*Default” with a “\*” assignment will appear in the Partitions tab. This indicates that all VLANs are in the *Default* partition; with this configuration, the Brick is “unpartitioned.”

The entry for the default partition is not editable. It is there as a reminder that any VLAN ID not mentioned explicitly in the Partitions table belongs to the default partition.

- 3 To add a Brick partition, right-click in the display area and select **New** from the pop-up menu. The Brick VLAN Partition Editor will appear. It is shown in [Figure 7-2, “Brick VLAN Partition Editor”](#) (p. 7-5).

**Figure 7-2 Brick VLAN Partition Editor**



- 4 In the **Name** field, enter a name for the partition. The name must be unique for each Brick.
- 5 In the **VLAN ID List** field, enter the VLAN IDs that will be included in the partition. A given VLAN ID may be assigned to only one partition. If a given VLAN ID is not explicitly assigned to a given Brick partition, it is implicitly a member of the *Default* partition.
- 6 Check the **Local Partition for LSMS Communication** checkbox if this partition is to be used for LSMS — Brick communication. Exactly one partition must be used for this purpose. If this checkbox is not checked on any partition, the *Default* partition is assumed.
- 7 Click the **OK** button to return to the Partitions tab of the Brick Editor ([Figure 7-1, “Brick Editor \(Partition Tab\)”](#) (p. 7-4)).

END OF STEPS



## Use Static Routes with Partitions

---

### Overview

Each static route has a partition indicator. This is the partition to which that route applies. In other words, any packet in a given partition can *only* use the static routes for *that* partition. When static routes are created, it is important to pay attention to the partition in which the route is created, since that route will only apply to packets within that partition.

Default routes are also applied per-partition. It is frequently useful to have a 0.0.0.0/0 route for each partition, to specify a default gateway so that partition can get to the outside if all else fails.

To create a static route, follow the procedure outlined in the section [“To Add a Static Route”](#) (p. 4-34) in Chapter 4, [“Configuring Alcatel-Lucent VPN Firewall Brick™ Security Appliance Ports”](#).





## Allow Partitions to Intercommunicate with Static Routes

---

### Overview

By default, traffic on VLANs in one partition cannot traverse to VLANs in any another partition. To allow traffic from one partition to another, a static route must be created.

### Create Static Routes with a Partition as Gateway

Each static route you create can now have a partition as its gateway, as well as a VBA. Using a partition as the next hop causes the Brick to change the current partition of the packet and to continue searching for a static route using the entries for the new partition. Such a route may be helpful in directing a packet from another partition to an initial zone within this partition.

All communication between partitions should be bi-directional: If partition "A" has a static route with partition "B" as its next hop, then there must be one or more static routes with "A" as their next hop. If there is no return route, then packets from partition B are only able to return to partition A if the **Route Return Path Packets to Cached Source MAC Address** option is checked. Even in this case, return traffic may be halted if the cache for Partition B is cleared or if a MAC is moved. A warning message is displayed if you omit the return route.

The address for returning packets back to the sourced MAC must also be defined in a ruleset on the Brick using the Rules-based Routing feature. For details about the Rules-based Routing feature, refer to the *SMS Policy Guide*.

Using a VBA as the next hop causes the packet to be processed by the zone associated with that VBA, then forwarded.

Figure 7-3 Brick Static Route Editor

**Brick Static Route Editor - /system/Devices/Bricks/radbrick**

Basic Routing

**Route Active** Yes

**Partition** \*Default

**Destination IP Address/Mask**

**Next Hop**  Gateway IP Address  Partition

**Gateway IP Address**

**Description**

**Route Cost** 0

Route Verification

Enable Route Verification

**Ping Destination IP Address**

**Ping Source IP Address**

**Ping Interval (secs)** 10

**Ping Timeout (secs)** 1

**Ping Failures for Route Unavailable** 3

OK  Cancel

To create a static route, follow the procedure described in the [“To Add a Static Route”](#) (p. 4-34) section in [Chapter 3, “Configuring and Activating an Alcatel-Lucent VPN Firewall Brick™ Security Appliance”](#).

## Examples

In the simplest case of inter-partition communication, all the hosts that need to communicate have unique public addresses. In this case all that is needed is to add static routes in each partition pointing to the hosts in the other partition.

As a more complicated case, consider a service provider who hosts two customers, one in Partition1, the other in Partition2. Each customer uses addresses in the 10.0.0.0/8 subnet, but they wish to set up a private application between them. One way to do this is pick two other subnets, one for each partition — for example, 192.168.1.0/24 for Partition1 and 192.168.2.0/24 for Partition2.

The first address in each subnet will be arbitrarily reserved for a VBA. Zone1 in Partition1 will be assigned VBA 192.168.1.1 and Zone2 in Parttion2 will be assigned VBA 192.168.2.1. To allow clients in Partition1 to originate traffic to servers in Partition2, you must do the following:

1. Add outbound rules in Zone1 with destination addresses in the 192.168.2.0/24 subnet. These rules should source NAT to the VBA for Zone1.
2. In the static route table, add these two static routes:  
Partition: Partition1 Destination: 192.168.2.0/24 Next hop: Partition2  
Partition: Partition2 Destination: 192.168.2.0/24 Next hop: VBA 192.168.2.1
3. For return traffic, add these static routes:  
Partition: Partition2 Destination: 192.168.1.0/24 Next hop: Partition1  
Partition: Partition1 Destination: 192.168.1.0/24 Next hop: VBA 192.168.1.1
4. Add inbound rules in Zone2 that perform destination network address translation (NAT) to map the relevant 192.168.2.0/24 addresses to the appropriate addresses in the 10.0.0.0/8 space of Partition2.

At this point host 10.10.10.10 can have a dialogue with host 10.10.10.10. The 10.10.10 client in Zone1 thinks it is connecting to, say 192.168.2.134, while the 10.10.10 server in Zone2 thinks it is being contacted by 192.168.1.1.

If there are hosts in Partition2 that must originate traffic to hosts in Partition1, then perform the corresponding steps 1 and 4 for this direction. The static route table does not have to change.

□

## Save and Apply the Brick Configuration

---

### Task

Once Brick partitions and static routes are created, you have to save and apply the configuration. Open the File menu and select **Save and Apply**.



## Interpreting IP Addresses When Brick Partitions Are Configured

---

### Overview

Whenever you look at an IP address in a Brick configuration, you must bear in mind what partition is applicable. If you see an IP address that you recognize, you must be careful to ask yourself if it refers to the endpoint you are thinking of, or to a totally different endpoint in another partition.

For example, in the VLAN/IP assignment table, the same Brick address can be assigned to two different VLAN IDs. If both VLAN IDs belong to the same partition, then these entries form a bridge group (and the "Bridge VLANs in same partition with same IP/Mask" checkbox must be checked). If they are in different partitions, however, there is no relationship between the addresses.





# 8 Creating SMS Groups and Administrators

## Overview

---

### Purpose

This chapter discusses the concept of a group, describes the **system** group (a special group provided with the SMS), and explains how to create new groups.

This chapter also describes the two types of administrators, SMS Administrators and Group Administrators, and explains how to create new administrator accounts. It describes the different privileges that can be given to Group Administrators.

### Contents

What is a Group?	8-2
To Create a Group	8-5
To Maintain Groups	8-7
SMS and Group Administrators	8-9
To Create Administrator Accounts	8-10
To Assign Groups and Privileges	8-17
To Maintain Administrator Accounts	8-21
To Use the SMS Messenger	8-25



## What is a Group?

---

### Definition

A group is a collection of objects that are managed as a whole. In general, no object can exist in more than one group. However, some objects can be made globally visible to all the other groups. In addition, a LAN-LAN tunnel may have endpoints in two different groups.

If you are a Managed Service Provider, groups typically represent all devices, policies, tunnels, and users of a specific customer. (Refer to [Chapter 1, “Getting Started”](#) for a more detailed discussion of group characteristics.)

### Organization

The objects in a group are organized into folders and subfolders. The folders and subfolders that comprise each group are:

- Devices
  - Subfolders
    - Bricks
- Policies
  - Subfolders
    - Brick zone rulesets
    - Host groups
    - Service groups
    - Application filters
    - Dependency masks
- VPNs
  - Subfolders
    - LAN-LAN tunnels
    - Client tunnel endpoints
    - VPN Defaults
- User Authentication
  - Subfolders
    - Users
    - User groups
    - Authentication services



## New Groups

SMS Administrators have the choice of using the **System** group that is provided with the SMS application, or creating additional groups.

The *System* group is a special group. It is the home of the NOC gateway Brick, and it is automatically populated with five pre-configured Brick zone rulesets, two router main rulesets and two router tunnel rulesets. In addition, three host groups are also included. (Refer to the *Pre-Configured Brick Zone Rulesets* appendix in the *SMS Policy Guide* for a detailed description of these rulesets).

Each new group you create will have the same folder/subfolder structure as the **system** group, but it will only contain four Brick zone rulesets, one router tunnel ruleset, and two host groups.

The names of the rulesets will be different in each new group you create. The SMS will automatically add the @ symbol and the group's name after the name of the ruleset. So, for example, if you created a group called XYZ, you would see these rulesets: administrativezone@xyz and main-encrypt@xyz.

## Administration

Groups can be administered by both SMS Administrators and Group Administrators. SMS Administrators have full privileges over all groups, which means they can access all folders in all groups and make any additions, modifications, or deletions they deem necessary.

Group Administrators, on the other hand, can only access the specific groups to which they are assigned. In addition, Group Administrators can be given three levels of privilege over the folders in their groups: None, View and Full.

This means you can create multiple Group Administrators for a group, each with different privileges, to administer different aspects of the group's operations. For example, one Group Administrator could have Full privileges over devices, but only View privileges over policy, while a second Group Administrator could have View privileges over devices and Full privileges over policy.

All valid SMS and Group Administrators must have an administrator account in the SMS. When creating new groups, you can create the Group Administrator account first, and then create the group, or you can create the group first, and then create the administrator account. The following explains the difference:

- *Create Group First*

If you create a new group before any Group Administrator accounts have been created, you simply enter a name and optional description in the Group Editor, and the group is created. The complete procedure is given in "How to Create a Group" below.

You must then create a Group Administrator account, and assign the administrator to the group you just created. If you edit the group after creating and assigning the new administrator, you will see the administrator's account listed in the Group Editor.

- *Create Administrator First*

If you create a Group Administrator account before creating the new group, you will be asked to enter the administrator in the Group Editor when creating the group. You will also be able to indicate the administrator's privileges over the group.

If you then edit the administrator's account, you will see the new group listed in the Administrator Editor. If you later delete the administrator's account, it will automatically be removed from the Group Editor.



## To Create a Group

---

### Task

Complete the following steps to create a new group.

---

- 1 With the Navigator window displayed, right-click any group folder and select **New Group** from the pop-up menu.

**Result** The Group Editor window is displayed (Figure 8-1, “Group Editor Window” (p. 8-5)).

**Figure 8-1 Group Editor Window**



- 2 In the **Group Name** field, enter a unique name. The name can contain 1 to 25 characters.
- 3 In the **Description** field, you can enter an optional description of the group. The description can contain up to 80 characters.

- .....
- 4 The License Limit field is a read-only field that shows the number of licenses allocated to the Group. The value of this field can be changed by right-clicking on a Group folder and selecting **Allocate Licenses**.

- .....
- 5 At this point, you can display the File menu and select one of the **Save** options to save the new group.

If Group Administrator accounts have already been created and the Privileges panel is displayed, you can assign administrators to this group before performing the save operation. Right-click in the **Group Administrator Privileges** box and select **New** from the pop-up menu.

.....  
E N D O F S T E P S  
.....



## To Maintain Groups

---

### When to use

SMS administrators can edit and delete existing groups. You cannot change a group's name, but you can change its description, the administrators, and their privileges. For example:

- You can add a new Group Administrator or delete an existing one.
- You can change the privileges of an existing administrator.

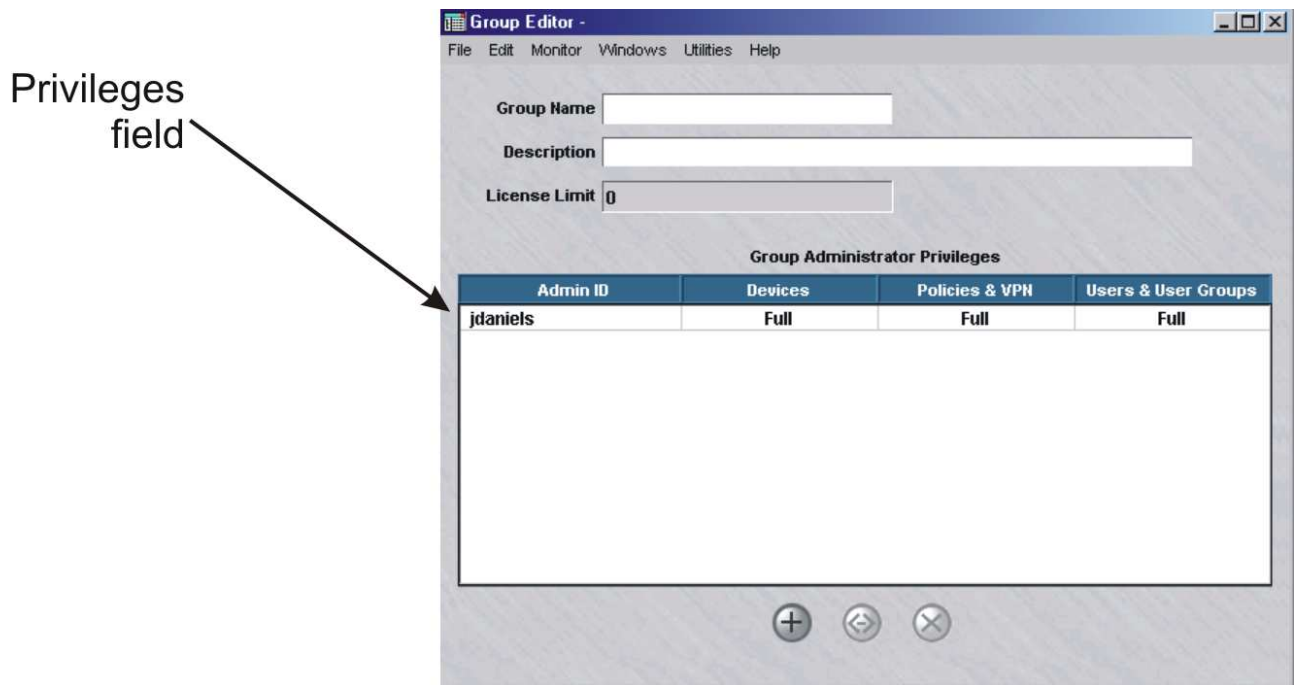
### To edit a group

To edit an existing group, follow the steps below:

---

- 1 With the Navigator window displayed, right-click the group folder and select **Edit Group** from the pop-up menu. The Group Editor window is displayed, as shown in Figure 8-2.

**Figure 8-2 GroupEditor Window**



- 2 The **Group Name** field is greyed-out and cannot be changed, but you can change the privileges.

- 
- 3 You can assign a new Group Administrator, modify the privileges of an existing administrator, or delete an administrator.

To do this:

- To assign a new administrator, right-click in the Privileges panel and select **New**. Then, enter the administrator ID and privileges, and click **OK**.
- To modify an administrator’s privileges, right-click the administrator in the Privileges panel and select **Edit**. Change the administrator’s privileges and click **OK**.
- To delete an administrator, right-click the administrator in the Privileges panel and select **Delete**. Click **Yes** in the pop-up window to confirm the deletion. The administrator will no longer appear in the Privileges panel. However, the administrator’s account is not deleted, only the administrator’s ability to manage this group. The account can still be seen by clicking **Administrators** on the Navigator window.

END OF STEPS

---

### To delete a group

An SMS administrator can only delete a group if the group is empty. This means you must remove all devices in the Devices folders, all administrator-created rulesets in the Policies folders, and all LAN - LAN tunnels before deleting the group. Related objects such as host groups, service groups, user authentication components, and the pre-configured rulesets will be automatically removed.

Once the group is ready, complete the following steps to delete it.

- 
- 1 With the Navigator window displayed, right-click the group and select **Delete Group** from the pop-up menu.
- 
- 2 Click **Yes** in the pop-up box to confirm the deletion. The group will be removed from the Navigator window.

END OF STEPS

---



# SMS and Group Administrators

---

## Overview

The SMS supports two types of administrators — SMS Administrators and Group Administrators. There can be multiple SMS Administrators and Group Administrators. Every administrator must have a valid administrator account in the SMS.

Only SMS Administrators can create other SMS Administrators and Group Administrators, and assign privileges to Group Administrators.

Administrator logins may be authenticated in one of three ways:

- Local Password
- RADIUS Server
- RSA SecurID Server

## SMS Administrators

An initial SMS administrator account is created during installation of the SMS application. This account can then be used to log onto the SMS and begin setting things up.

A SMS administrator has full privileges over *all* folders in all groups. This set of privileges entitles them to create, edit, delete, and apply all devices, rulesets and tunnels, as well as set up and maintain user authentication.

## Group Administrators

Group Administrators are created by SMS administrators and assigned to one or more groups. The functions that Group Administrators can perform in their groups are determined by the privileges they have been assigned by the SMS administrator.

Group Administrator functions are broken down into three areas:

- Devices (Bricks)
- Policies (rulesets, tunnels, authentication services)
- Users and user groups

For each area, Group Administrators can be assigned one of three privilege categories:

- Full (Create, Edit, Delete, and Apply).
- View (Display but not Create, Edit, or Delete)
- None (the folders will not be visible)

In addition, Group Administrators can view their assigned privileges and change their name, password, e-mail, phone number, and pager information.



## To Create Administrator Accounts

---

### Task

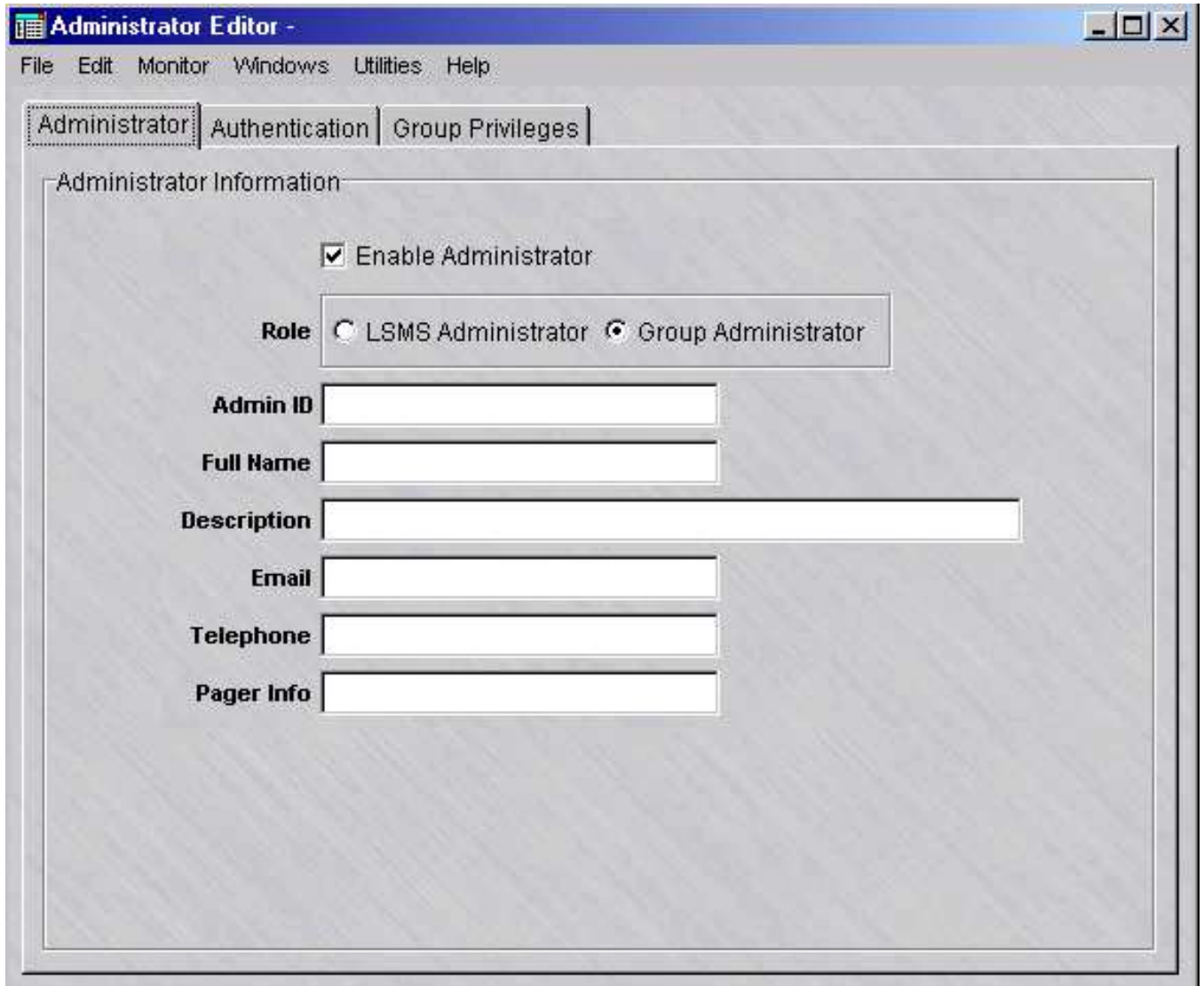
To create a new SMS or Group Administrator, you have to create an account in the SMS. If the account is for a Group Administrator, you also have to assign groups and privileges to the account for it to take effect.

To create an administrator account, follow the steps below:

- 
- 1 With the Navigator window displayed, right-click the **Administrators** folder and select **New Administrator** from the pop-up menu. The Administrator Editor will appear with the Administrator tab highlighted, as shown in [Figure 8-3, “Administration Editor \(Administrator Tab\)”](#) (p. 8-11).
  - 2 By default, the **Group Administrator** radio button is clicked in the **Role** box. This means this account is for a Group Administrator. If you intend this administrator to be an SMS Administrator, click the SMS **Administrator** radio button.



**Figure 8-3 Administration Editor (Administrator Tab)**



- 
- 3 Enter the information requested in the fields. **Admin ID** and **Full Name** are required fields. The **Enable Administrator** field is checked by default. An LSMS Administrator can modify this checkbox for any user but himself / herself, while a Group Administrator cannot modify this checkbox.

The table below describes each field under the Administrator tab:

Field	Description
Admin ID	The administrator login. Can contain 1 to 16 characters (letters and numbers) and must be lowercase. This is a required field.
Full Name	The administrator's name. Can contain 1 to 80 upper and lower case characters (letters and numbers).  This is a required field, but it does not appear on-screen when you display administrators in the Navigator window.
Description	A description of the administrator. Can contain 1 to 80 upper and lower case characters (letters and numbers).  It is displayed in the Navigator window, so you can enter the administrator's name, role (SMS/Group), or any other information that might be helpful to see in the Navigator window.
E-mail Address	The administrator's e-mail address.  The contents of this field is used in the e-mail alarm action. Refer to the <i>SMS Reports, Alarms, and Logs Guide</i> .
Telephone Number	The administrator's office telephone number.
Pager Info	The PIN of the administrator's paging service (Examples: SkyTel, PageNet, MetroCall).  The contents of this field is used in the Direct Page alarm action. Refer to the <i>SMS Reports, Alarms, and Logs Guide</i> .

---

4 Click on the Authentication tab.

- **Authentication Service** - Default choice is "Local Password". If you have already configured a RADIUS or SecurID server to provide authentication for your firewall or VPN users in the *system* group, it will be also listed here as an option. You may initially create a user with a local password and update it later to use a different authentication method.

The choice of Authentication Service affects the options available under the Authentication tab. If you chose RADIUS or RSA SecurID, proceed to Step 5. If you selected Local Password, you will see the following screen:

Figure 8-4 Administrator Editor (Authentication Tab)



The table below describes each field listed for Local Password:

- **Disable Administrator After** - You have the option to disable an administrator after "n" number of failed logins.
- **Active From** - By default, a user is active from the time of creation until 12/31/2099. You may redefine that period as desired. This only applies to Group Administrators.
- **Allowed Source IP Addresses** - By default, this field is set to "\*" (allow any source IP). You may narrow the scope of allowed addresses as desired. If you are using the LSMS Remote Navigator, you can only connect to the LSMS from addresses listed in this field.

- **Password** - The password required to validate the login. The password is case-sensitive. The minimum password length is six characters (or the minimum password length setting for the **Local Password** Authentication Service) and the maximum length is 42 characters long. This is a required field if you are using a local password.

When a new password is set for an administrator that is authenticated using Local Password authentication, or an existing local password is changed, if the strong password (SOX compliance) option is enabled (the default) via the Configuration Assistant, stricter password requirements would apply. In this case, the password:

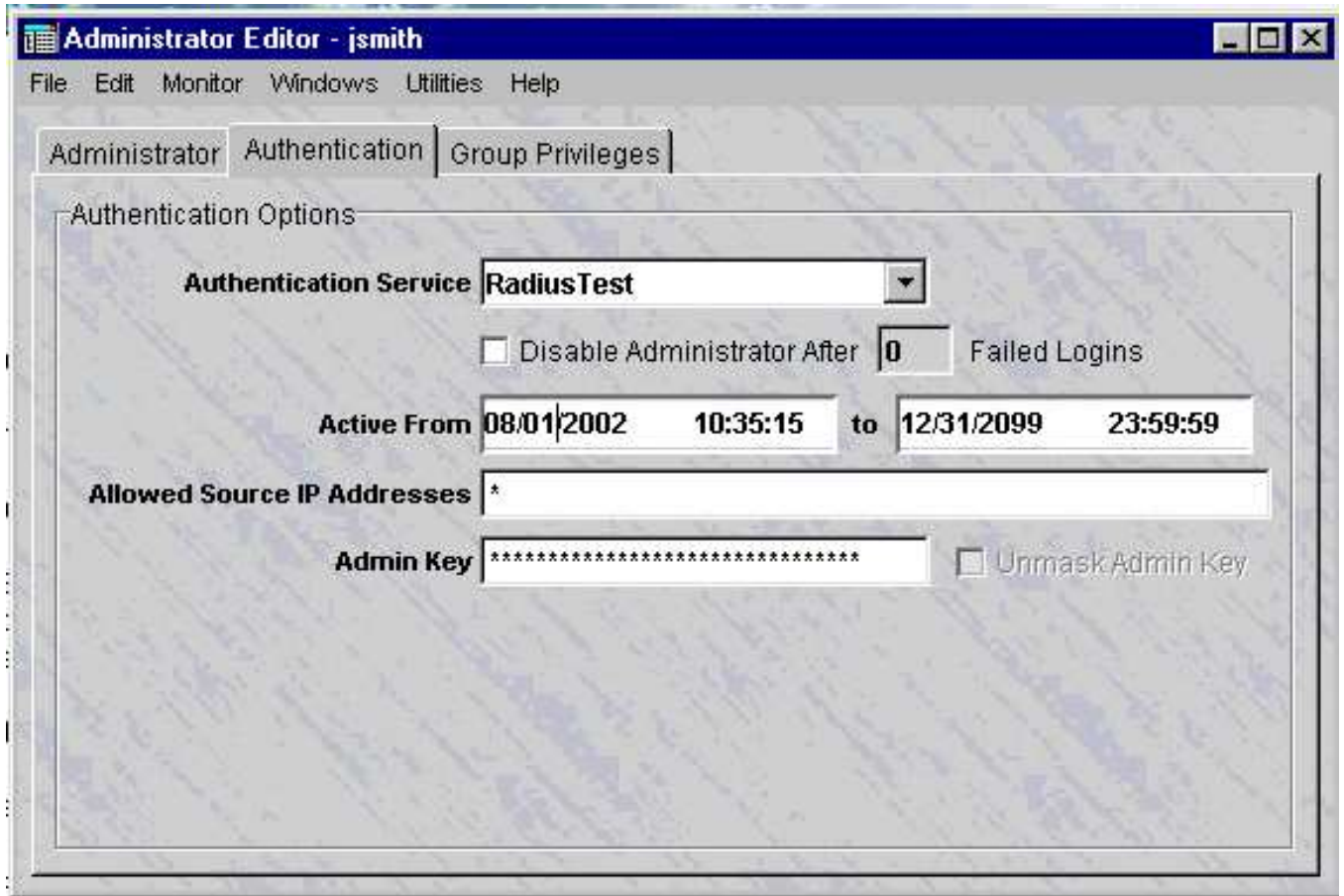
- Must be a minimum of eight characters, or the **Minimum Password Length** set for the **Local Password** Authentication Service, whichever is greater
- Must contain at least one alpha character and one non-alpha character (0-9, special characters, no restrictions)
- Cannot contain three or more repeated alphanumeric characters in a row
- Cannot contain three or more consecutive, ascending or descending, alphanumeric characters in a row
- Not contain the User Account name or its mirror (reverse character format)
- Not be one of the previous three passwords most recently used

For details about enabling or disabling the strong password (SOX compliance) option, refer to the description of the User Authentication Parameters settings of the Configuration Assistant in [Chapter 11, “Using the Configuration Assistant”](#).

- **Verify Password** - The password, entered exactly as above. If using capital letters, ensure that you are capitalizing consistently. Also a required field for local password admins.
- **Require Administrator to Change Password on Next Login** - Check off if desired.
- **Password Expiration Options** - If “Enable Password Expiration” is checked, you may define the length of time before a password expires, and also choose the **Action on Expiration** - whether to prompt the user for a new password or to disable the administrator.

- 
- 5 Under the Authentication tab, if you selected an Authentication Service of “RADIUS” or SecurID”, you will see the following screen:

Figure 8-5 Administration Editor (Authentication Service)



The list below describes each field shown:

- **Disable Administrator After** — You have the option to disable an administrator after "n" number of failed logins.
- **Active From** — By default, a user is active from the time of creation until 12/31/2099. You may redefine that period as desired. This only applies to Group Administrators.
- **Allowed Source IP Addresses** — By default, this field is set to "\*" (allow any source IP). You may narrow the scope of allowed addresses as desired. If you are using the SMS Remote Navigator, you can only connect to the LSMS from addresses listed in this field.

- **Admin Key** — During the login process, this key must be provided, either automatically via a RADIUS attribute, or entered manually by the user, to authenticate the administrator. See "Administrator Authentication with RADIUS and SecurID" on page 8-14.
- **Unmask Admin Key** — While the Admin Key is initially created, if this box is checked, the admin can see the key as it is typed. If left unchecked, each keystroke is masked by a "\*". However, administrators cannot see the key of other administrators once it is created.

- 
- 6 If you are creating an SMS Administrator account, display the File menu and select one of the **Save** options.

If this is a Group Administrator account, you have to assign this administrator to at least one group and specify the administrator's privileges before you save the account. The procedure is described in the next section.

END OF STEPS



## To Assign Groups and Privileges

---

### When to use

Group Administrators have to be assigned to the groups they will manage, and they have to be given privileges.

### Privileges

Privileges determine the extent of a Group Administrator's control over the group and its components. Group administration is broken down into three functional areas:

- Devices (Bricks)
- Policies & VPN (rulesets, tunnels, authentication services)
- Users and user groups

For each functional area, a Group Administrator can be assigned one of three privilege categories:

- Full
- View
- None

The table below shows the result of assigning each privilege to the three functional areas.

Area	Privilege	Result
Devices	None	Does not see Devices folder
	View	Sees all configured Bricks. Can make no additions, deletions, or changes.
	Full	Can configure Bricks. Can edit and delete configured devices. Can apply devices.
Policies & VPN	None	Does not see Policies folder, VPN folder, and Authentication Services folder
	View	Sees all configured rulesets, host groups, and service groups. Sees all configured tunnels and authentication services. Can make no additions, deletions, or changes.
	Full	Can create, edit, and delete Brick rulesets, host groups, and service groups. Can configure LAN-LAN tunnels and client tunnel endpoints. Can apply policy, LAN-LAN tunnels, and client tunnel endpoints.

Area	Privilege	Result
Users & User Groups	None	Does not see Users and User Groups folders.
	View	Sees all user accounts and user groups that have been created. Can make no additions, deletions, or changes.
	Full	Can create, edit, and delete user accounts and user groups.

**To assign groups and privileges**

Complete the following steps to assign groups and privileges to a Group Administrator account.

- 1 Proceed to the Group Privileges tab in the Administrator Editor. Right click in the white area and select **New** from the pop-up menu. The Group Administrator Privileges window is displayed (Figure 8-6, “Group Administrator Privileges Window” (p. 8-18)).

**Figure 8-6 Group Administrator Privileges Window**



- 2 In the **Group** field, select a group from the drop-down list.
- 3 In the **Privileges** field, enter the privileges this administrator will have over the group you selected. You must select one of the privilege combinations on the drop-down list.

The table below explains each combination:

Privilege Combination	Description
Full, Full, Full	Can manage all aspects of the group’s operations.



Privilege Combination	Description
Full, Full, View	Can manage devices and policies, including all tunnels and user authentication services. Can only see user accounts and user groups.
Full, View, View	Can manage devices, but can only see policies, user accounts, and groups. Can only apply devices.
View, Full, Full	Can view all configured devices. Can create policies, user accounts, and user groups. Can apply policy, LAN-LAN tunnels, and client tunnel endpoints.
View, Full, View	Can view all configured devices, and all user accounts and user groups. Can manage policies, including LAN-LAN tunnels, client tunnel endpoints, and authentication services. Can apply policy, LAN-LAN tunnels, and client tunnel endpoints.
View, View, Full	Can view all configured devices and all policies. Can manage user accounts and user groups. Cannot apply.
View, View, View	Can view all aspects of a group's operations. Can make no changes. Cannot apply.
None, Full, Full	Can manage policies, user accounts, and user groups. Does not see Devices folder in Navigator window. Can apply policy, LAN-LAN tunnels, and client tunnel endpoints.
None, Full, View	Can manage policies. Can view user accounts and user groups. Does not see Devices folder in Navigator window. Can apply policy, LAN-LAN tunnels, and client tunnel endpoints.
None, View, Full	Can manage user accounts and user groups. Can view policies. Does not see Devices folder in Navigator window. Cannot apply.
None, View, None	Can view the Policies and VPN folders. Cannot view the Devices or User Auth folders in Navigator window. Cannot apply.
None, None, Full	Can manage user accounts and user groups. Does not see Devices or Policies folders. Cannot apply.

.....

**4** When you are finished, click **OK** to dismiss the Group Administrator Privileges window and return you to the Administrator Editor. The new administrator's privileges will appear in the Administrator Editor.

.....

**5** Display the File menu and select one of the **Save** options.

END OF STEPS

.....

## Administrator Authentication with RADIUS and SecurID

If SMS or Group Administrators using Local Password authentication enter the correct password as stored in the SMS database, they are able to login successfully.

If an administrator is authenticating via an external RADIUS server, there are several scenarios to consider:

- If the RADIUS authentication service in the LSMS is configured with the Admin Key attribute, the users in RADIUS must be configured to return the attribute, otherwise the login will fail. The value of the Admin Key that is returned from RADIUS must match the value that is entered for that administrator in the Administrator Editor, in order for the login to succeed.
- If the authentication service in the SMS is *not* configured for Admin Key, then the administrator will be prompted to enter the Admin Key during the login process.

If an administrator is authenticating through a SecurID server, this is similar to RADIUS authentication where the SMS parameter "Admin Key" has NOT been configured. After the SecurID authentication is complete, the user will be prompted to enter their Admin Key. If the SecurID authentication was successful and the Admin Key is correct, the user is authenticated and the SMS or Group Administrator login is successful.

## Administrators and SMS Installations and Upgrades

Although LSMS and Group Administrators have the option to authenticate through external RADIUS or SecurID servers, it is imperative to ensure that at least one SMS Administrator could log into the SMS Navigator *if all external servers are unavailable*.

The initial SMS administrator created during the installation of the SMS application will be assigned the Local Password authentication service. To ensure that there is always an administrator account available to install software upgrades, the initial SMS administrator account created during installation cannot be deleted although the password for this account can be set up to expire after a set period of time. This account is assigned the Local Password authentication service, and the authentication service cannot be changed.

When upgrading the SMS application, an SMS administrator ID and password must be provided. The login ID and password of any administrator that is assigned to the Local Password authentication service may be used to install upgrade software. Even if a Local Password administrator is disabled via the **Disable Administrator after x Failed Logins** checkbox on the Administrator Editor, and they can no longer log in to the GUI to administer the SMS, that login ID and password may still be used to upgrade the SMS application.

□

## To Maintain Administrator Accounts

---

### When to use

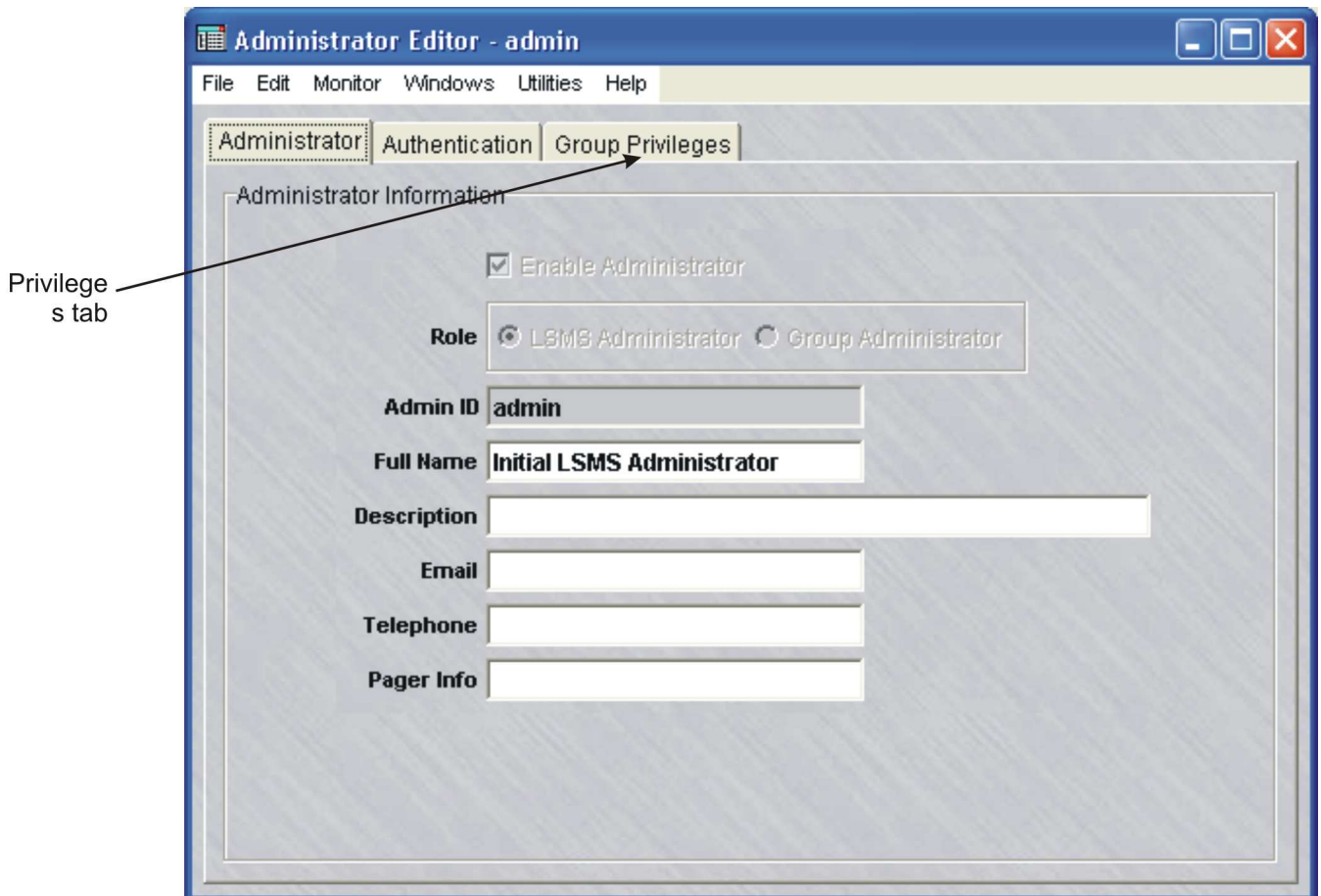
Once an administrator has been created, an SMS administrator can edit the account when information or privileges change, or delete it when it is no longer necessary.

### To edit an administrator account

Complete the following steps to edit an administrator account.

- 1 With the Navigator window displayed, click the **Administrators** folder to display all administrator accounts in the Contents panel.
- 2 Highlight and right-click or double-click the account you want to edit. It will appear in the Administrator Editor ([Figure 8-7, “Administrator Editor \(Edit Mode\)”](#) (p. 8-21)).

**Figure 8-7 Administrator Editor (Edit Mode)**



- 
- 3 Make any changes to the information shown. You cannot change the Admin ID. The password can be changed under the Authentication tab, but it never displays.
  - 4 If this is a Group Administrator account, you can add groups to the account, and delete groups. You can also change the administrator's privileges for an existing group. The following explains how:

To do this:

- To add a new group, proceed to the Group Privileges tab, right-click in the Privileges panel and select **New** from the pop-up menu. Enter the group and privileges, and click **OK**.
- To delete a group, right-click the group and select **Delete** from the pop-up menu. Click **Yes** to confirm the deletion.
- To change the administrator's privileges, double-click the entry in the Privileges panel, enter the new privileges and click **OK**.

- 
- 5 Display the File menu and select one of the **Save** options.

**Important!** *When Changes Take Effect*

If a Group Administrator is currently logged in, and the privileges are changed by an SMS administrator, the changes will not take effect until the Group Administrator logs out and logs back in again.

The current session of the Group Administrator is not terminated when changes are made.

END OF STEPS

---

### To view the status of an administrator account

---

- 1 To view the status of an Administrator account, follow the steps below, with the Navigator window displayed, click the **Administrators** folder to display all administrator accounts in the Contents panel (see [Figure 8-8, "Contents Panel \(Administrators folder\)"](#) (p. 8-23)).

**Figure 8-8 Contents Panel (Administrators folder)**

Folder: /Administrators/ - Total 4 item(s)				
Name	Status	Admin	Last Modified	Description
admin	enabled	setup	2004-11-08 15:47:07	
elobelo	enabled	admin	2004-12-07 14:00:41	Isms administrat
jdaniels	enabled	admin	2005-06-03 10:42:24	group administrat
tbanks	disabled	admin	2005-06-03 10:42:34	group administrat

The list below describes each field shown:

- **Name** — The Admin ID of the administrator.
- **Status** — A field that shows whether the administrator account is currently **enabled** or **disabled**. The status of an administrator can be changed only by an SMS administrator by checking/unchecking the **Enable Administrator** checkbox on the Main tab of the Administrator Editor window. For details about the **Enable Administrator** checkbox, refer to the section [“To Create Administrator Accounts”](#) (p. 8-10).
- **Last Modified** — A field that shows the date and time that any changes were made to the administrator account.
- **Description** — A text field that can be used to provide any additional descriptive information about the administrator account.

.....  
 END OF STEPS

### To delete an administrator account

Complete the following steps to delete an existing administrator account.

- 1 With the Navigator window displayed, click the **Administrators** folder to display all administrator accounts in the Contents panel.
- 2 Right-click the administrator and select **Delete** from the pop-up window.
- 3 Click **Yes** in the pop-up window to confirm the deletion.

**Important!** The initial SMS administrator account created during installation cannot be deleted. Only accounts created afterwards can be deleted.

Group Administrators cannot delete accounts, but they can edit information in their own account.

.....  
 END OF STEPS



## To Use the SMS Messenger

---

### Overview

The SMS Messenger is a feature that allows SMS and Group administrators to send short messages to other administrators who are already logged in. Using this feature, an administrator can send a message to one or more specific administrators or to all active administrators.

If you have a redundant or multi-site SMS configuration, or a Compute Server configuration, you can send messages to administrators logged into the Primary SMS, Secondary SMS, or CSs.

### Send messages using the SMS Messenger

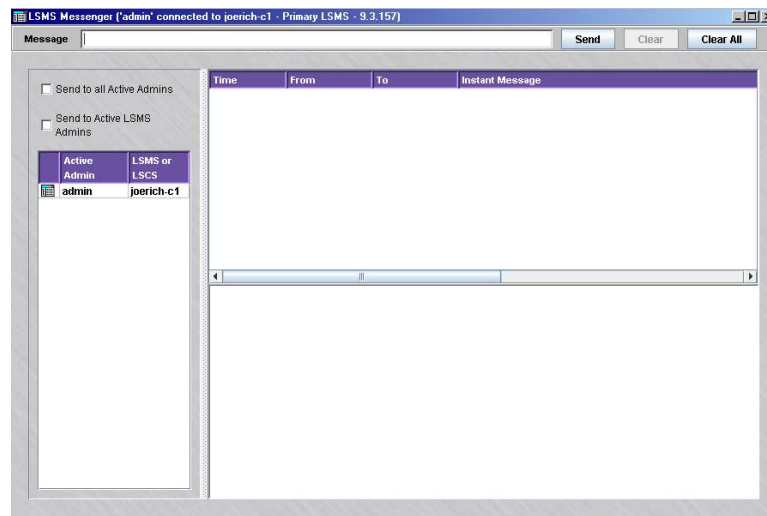
Complete the following steps to send a message to one or more administrators using the SMS Messenger.

---

- 1 From any SMS window, select **Utilities > SMS Messenger**.

**Result** The SMS Messenger is displayed ([Figure 8-9, “SMS Messenger” \(p. 8-25\)](#)).

**Figure 8-9 SMS Messenger**



- 2 Type the message in the **Message** field at the top of the window.  
To enter a multi-line message, type \t wherever you want a line break.

*Example:*

the system will be going down in 5 minutes\tplease terminate all  
activities\tthe system will be back up at 22:00

---

**3** In the left-hand panel, indicate the recipient of the message.

There are three ways to do this:

- Click **Send to all Active Admins** to send the message to all active administrators (both LSMS and Group Administrators).
  - Click **Send to Active LSMS Admins** to send the message to all active LSMS Administrators (not Group Administrators)
  - Select one or more administrators, which are displayed under the checkboxes. You can select multiple administrators by holding down the **[Ctrl]** key and clicking each one, or by holding down the **[Shift]** key and clicking two administrators (all administrators between the two will also be selected).
- 

**4** Click the **Send** button.

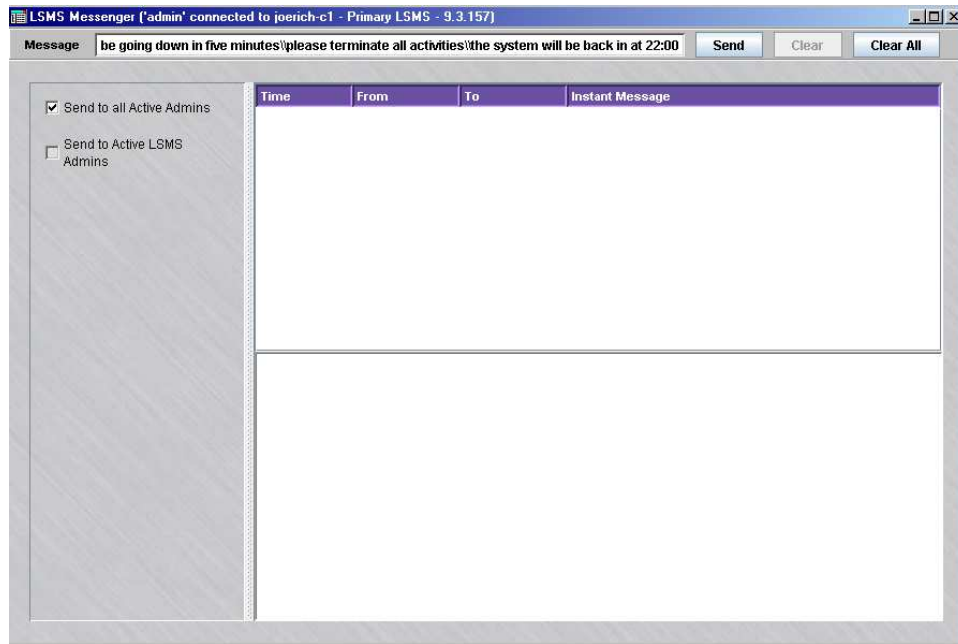
**Result** The message is sent to the selected administrator(s).

A record of the message sent is displayed in the main panel of the SMS Messenger. The record includes the time the message was sent, the administrator who sent the message, the intended recipients of the message, and the text of the message.



Figure 8-10, “Records of Sent Message” (p. 8-27) shows a typical display of a message that can be sent.

**Figure 8-10 Records of Sent Message**



To clear the display, click the **Clear All** button.

END OF STEPS .....

**To receive messages using the SMS Messenger**

Complete the following steps to receive a message sent using the SMS Messenger.

.....

- 1 Log onto the SMS using one of the procedures described in “To Log On and Off the SMS Server or Compute Server” (p. 1-2) in Chapter 1, “Getting Started”.

**Result** If a message has been sent to you using the SMS Messenger, the system displays an envelope icon that opens repeatedly at the top right portion of the Navigator (Figure 8-11, “Messenger Envelope” (p. 8-27) shows an example).

**Figure 8-11 Messenger Envelope**



This is the same area where a bell icon is displayed when an SMS or Brick alarm condition has been detected.

---

- 2 Click on the envelope icon or select **Utilities > SMS Messenger**.

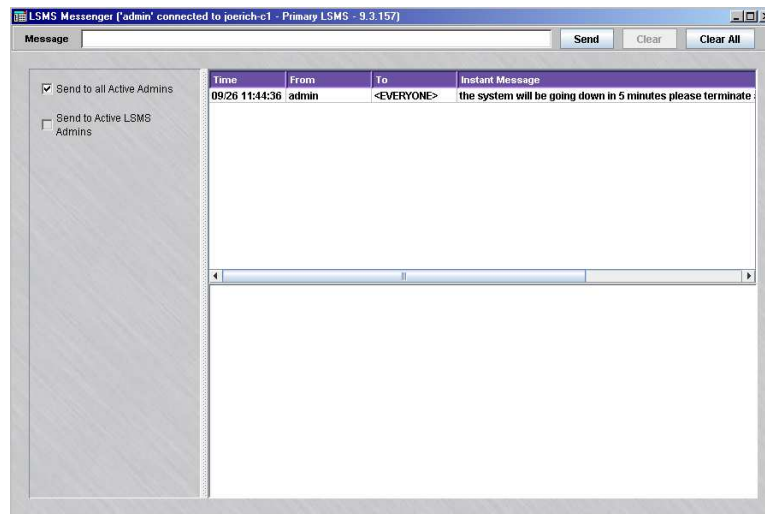
**Result** The SMS Messenger is displayed (see [Figure 8-10, “Records of Sent Message”](#) (p. 8-27)).

---

- 3 Click on the record of the message displayed in the **Instant Message** portion of the window.

**Result** The message sent is displayed in the bottom panel of the window [Figure 8-12, “SMS Messenger \(Message Sent\)”](#) (p. 8-28) shows an example).

**Figure 8-12 SMS Messenger (Message Sent)**



To clear the display, click the **Clear All** button.

END OF STEPS

---



# 9 Compute Servers

## Overview

---

### Purpose

This chapter discusses the concept of Compute Servers as an alternative means of collecting log information from Alcatel-Lucent *VPN Firewall Brick*<sup>TM</sup>Security Appliances that are managed by the SMS. It also describes how to configure Compute Servers.

### Contents

<a href="#">What is a Compute Server?</a>	9-2
<a href="#">To Configure a Compute Server</a>	9-5



## What is a Compute Server?

---

### Overview

To maximize the scalability of the SMS/Brick security solution, SMS provides the option of adding a separate set of servers called Compute Servers (CSs), which are associated with an SMS server or redundant pair of SMSs and act as collection points for Brick log traffic. Using a CS to collect Brick log data frees up computing resources on the SMS itself and extends the number of Bricks and total log traffic that can be handled. Each Brick managed by the SMS can be homed to one of the associated CSs or the managing SMS for logging purposes.

A CS provides most of the same functionality as an SMS, but does not have its own database. The database is centrally located on the Primary SMS. The Brick log data is collected and stored in files on the associated CS.

### Quantity of Compute Servers (CSs) and Bricks supported by an SMS

One SMS server can support up to five CSs. Each CS can collect log data from up to 1,000 Bricks. A redundant pair of SMSs, in a Primary SMS/Secondary SMS arrangement, can support up to 10 CSs and manage up to 10,000 Bricks.

### Redundancy

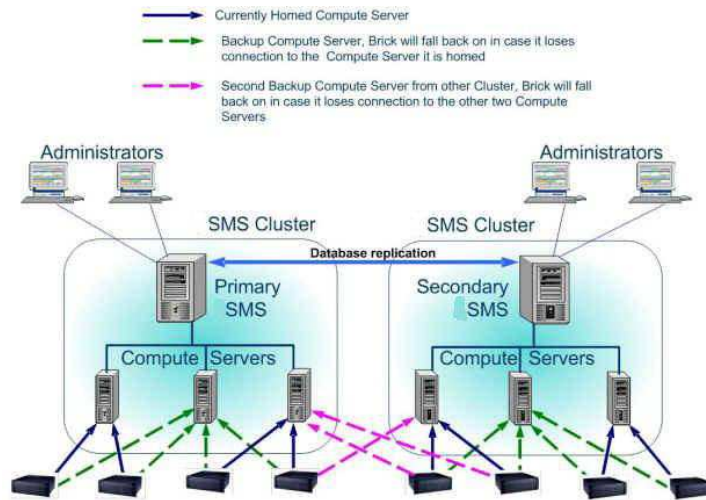
If a group of CSs has been added and configured, a Brick can be homed to one of the CSs to serve as the logging server, with the remaining CSs configured as backup log collection points in the event that the Brick connection to the first CS fails. The failover priority of CSs can be defined for a Brick, using the Brick Editor window (refer to [Chapter 3, “Configuring and Activating an Alcatel-Lucent VPN Firewall Brick™ Security Appliance”](#) for details on how to configure a Brick).

CSs can be configured to work with a single Primary SMS, but a redundant SMS pair is recommended for a large network of Bricks to evenly distribute the collection of log data and to maintain connectivity.

A CS can be associated with either the Primary or Secondary SMS in a redundant pair. The SMS can still be used to collect log data and perform configuration functions on the associated Brick regardless of which SMS is currently active.

[Figure 9-1, “SMS Cluster Arrangement of Computer Servers and Redundant SMS Pair” \(p. 9-3\)](#) depicts a typical cluster arrangement of Compute Servers (CSs) employed in collecting Brick log data managed by redundant SMS servers.

**Figure 9-1 SMS Cluster Arrangement of Computer Servers and Redundant SMS Pair**



Compute Servers can be geographically dispersed and still communicate securely with the SMS. A single Compute Server or group of Compute Servers should be protected by a Brick to ensure that only authorized traffic reaches the SMS cluster.

**Accessing a compute server**

A CS need to be configured on the SMS by an SMS Administrator before it can be brought up. For instructions on how to configure a CS, refer to the procedure [“To Configure a Compute Server”](#) (p. 9-5).

**Logging into a compute server**

SMS Administrators can log into a CS from the SMS console or remotely using the Remote Navigator. Only SMS Administrators have access permissions to add, modify, or delete CSs. Group Administrators do not have access permissions to CSs and can only view these servers through the Brick Editor window.

An SMS Administrator can reconfigure a CS while logged into the server directly from the SMS console or through the Remote Navigator.

**SMS tools on compute servers**

Most of the functions that are available on the managing SMS can be performed while logged into a CS, including creation and update of Bricks and Policies on the Bricks that are associated with the CS.

## Alarms and logs

Alarms that are generated on a specific SMS or Compute Server can be viewed by all Administrators logged into all SMSs/CSs in the network. Distributed reports can also be run to obtain a consolidated picture of all SMS/CS activities.

To view the raw logs on a CS, an SMS Administrator must log into that server and view the Brick data rows in a flat file or use the local Log Viewer (SMS function).

## SMS services

The DataBase service does not run on a CS. The CS communicates over the network with its associated SMS for DB access.

## Status Monitor

An Administrator can monitor the activity and status of a CS using the Status Monitor window.

On the Status Monitor window, the status of each CS is shown on a separate, indented line below it associated SMS and provides the following details:

- Name
- IP Address
- Status (Up, Down, Lost)
- Version (SMS software version)
- SMS association
- Number of Bricks assigned
- Number of Bricks assigned and homed to the CS
- Number of Bricks not assigned but homed to the CS

For complete information about the SMS Status Monitor window, refer to [Chapter 14, "Using the Status Monitor"](#).

## Operating system

CSs supported by the SMS run on the *Microsoft® Windows®* operating system. A CS can communicate with an SMS running on a *Microsoft® Windows®, Microsoft® Vista®, Sun® Solaris®,* or Linux operating system, since it is a separate server that resides in front of the SMS and is protected by a Brick.

□

## To Configure a Compute Server

---

### Task

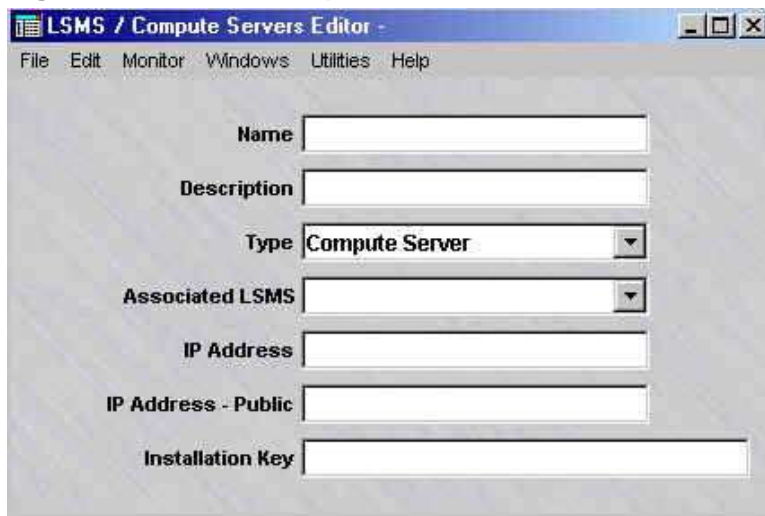
Complete the following steps to configure a new Compute Server.

---

- 1 With the Navigator window displayed, right-click the **LSMS and LSCSs** folder and select **New LSMS and Compute Servers** from the pop-up menu.

**Result** The LSMS / Compute Servers Editor window is displayed ( [Figure 9-2, “LSMS/Computer Servers Editor Window”](#) (p. 9-5)).

**Figure 9-2 LSMS/Computer Servers Editor Window**



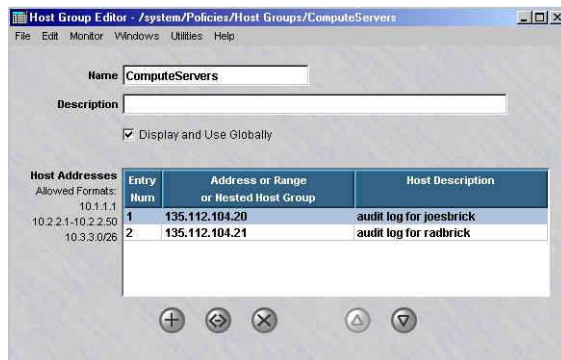
- 2 Enter values in the following fields:
  - **Name** - The name of the Compute Server, 1-45 characters.
  - **Description** - A textual description of the Compute Server (Bricks supported, types of logging data collected, and so forth).
  - **Type** - Click the down-arrow next to this field and select **Compute Server** from the drop-down list.
  - **Associated LSMS** - Click the down-arrow next to this field and select the Primary or Secondary SMS associated with this Compute Server.
  - **IP Address** - The real IP address of the Compute Server. On private networks, this is the real IP address of the server that can be mapped to a virtual address using NAT.

- **IP Address - Public** - This is the Virtual Brick Address (VBA) of the Brick protecting the Compute Server. This field is optional.
- **Installation Key** - The license key used to install the Compute Server and associate it with an SMS.

3 From the File menu, select **Save and Close**.

The new Compute Server is configured. A entry for the new Compute Server appears in the ComputeServers Host Group (Figure 9-3, “Host Group Editor window (ComputeServers Host Group)” (p. 9-6) shows a sample Host Group Editor window).

**Figure 9-3 Host Group Editor window (ComputeServers Host Group)**



END OF STEPS





# 10 Remote Administration

## Overview

---

### Purpose

This chapter will explain all the steps needed and options available to administer the SMS from a remote PC or workstation, including:

- Installation and supported platforms
- SMS policy changes needed to permit remote administrator access
- Login procedure
- Tasks that may be performed remotely

### Contents

The SMS Remote Navigator	10-2
To Install the Remote Navigator on <i>Microsoft®Windows®</i> or <i>Vista®</i>	10-3
To Install the Remote Navigator on <i>Solaris®</i>	10-7
Permitting Remote Administration on the SMS	10-10
To Create the Host Group	10-11
To Create the Security Rules	10-12
To Log In from a Remote Host	10-15
Remote Administrator Capabilities	10-18



# The SMS Remote Navigator

---

## Overview

The SMS Remote Navigator application allows you to run the SMS application from a remote host instead of the SMS console. It is provided on the SMS CD-ROM, and may also be retrieved remotely from the SMS via a browser.

An Administrator can log into the SMS remotely using a host running *Microsoft®Windows®*, *Vista®*, or *Sun®Solaris®*, and Linux operating systems; a Linux host can only be accessed remotely by a *Windows®* or *Solaris®* server that has the Remote Navigator software installed. Interoperability across platforms is supported, so *Windows®*Windows remote clients can access a *Solaris®* SMS, and *Solaris®* remote clients can connect to a *Windows®* or *Vista™* SMS. The following gives the software requirements for both platforms.

### ***Microsoft®Windows® or Vista®***

The remote host must be running the following software:

- *Windows®* XP Professional with Service Pack 2 (SP2) or Service Pack 3 (SP3), *Windows®* 2003 *Server®* with Service Pack 2 (SP2). or *Vista®*
- Internet Explorer 5.5 or later, Netscape Communicator 4.7 or greater, Firefox 2.0 or later. Browser software is needed to view SMS reports and display the on-line help.
- Adobe Acrobat Reader 8.0 or above, to read the on-line documentation.

### ***Solaris® 9 or 10***

The remote host must be running the following software:

- *Solaris®*9 or 10
- Adobe Acrobat Reader 8.0 or above, to read the on-line documentation.



# To Install the Remote Navigator on *Microsoft® Windows®* or *Vista®*

---

## Overview

There are two ways to install the SMS Remote Navigator— directly from the SMS CD-ROM, or by downloading the software from the SMS.

## From the CD-ROM

Complete the following steps to install the SMS Remote Navigator from the CD-ROM.

---

- 1 With the SMS CD in the CD-ROM drive, open the Windows Explorer and locate this directory on the CD-ROM:

*\windows\RemoteNavigator*

---

- 2 Double-click the file

*lsmremnav-9.4.xxx.exe*

where *xxx* is the version number of the software. This is the installation program. The installation process will begin.

**Important!** If you are upgrading from an earlier release of the Remote Navigator, a window will pop up and indicate that an earlier release is loaded on the host you are using. Click **Yes** to overwrite the older release.

---

- 3 The first window to appear is the Welcome window. Read the text in the Welcome window, and when you are finished, click **Next** to continue with the installation.
- 

- 4 The Choose Destination Location window will appear. This window allows you to specify where the SMS Remote Navigator software will be installed. The default is:

*c:\LSMSRemNav9.4*

We recommend you accept the default. Click **Next** to do this, or click the **Browse** button and enter a new destination location before clicking **Next**.

---

- 5 The Select Program Folder window will appear. This window allows you to select the folder in which the SMS Remote Navigator program selections appear on the Windows Start menu, Programs. The default is:

*Alcatel-Lucent Security Management Server*

---

We recommend you accept the default. Click **Next** to do this, or select another folder from the Existing Folders panel before clicking **Next**.

---

- 6 Installation of the files will now begin. When the installation is finished, the Setup Complete window will appear. Click **Finish** to complete the installation. It is not necessary to reboot your machine. The SMS Remote Navigator may be run immediately.

.....  
E N D O F S T E P S  
.....

## From the SMS

To download the SMS Remote Navigator from the SMS, follow the steps below:

---

- 1 Create a temporary directory on the hard drive of your computer to hold the downloaded file.
- 2 Open a browser and enter the URL of the SMS. The URL consists of the SMS IP address, its port number, and the directory in which the SMS application is stored. Depending on whether the SMS web server is HTTP or HTTPS, the URL will look like one of the following:

*http://<ip\_address>:<port>/LSMS*

— or —

*https://<ip\_address>:<port>/LSMS*

**Important!** Before the browser is displayed with the link to download the Remote Navigator software, you may be required to enter an "Authentication Key." For additional information about configuring this key, see the SMS web server parameter in [Chapter 11, "Using the Configuration Assistant"](#).

**Result** The How to Install the Remote Navigator window is displayed (Figure 10-1, “How to Install the Remote Navigator Window (*Windows®* Version)” (p. 10-5).

**Figure 10-1** How to Install the Remote Navigator Window (*Windows®* Version)



- 
- 3** Click the **lsmsremnav.exe** link. You may want to leave the How to Install the Remote Navigator window up as a reference.

**Result** The File Download window is displayed. The **Save this program to disk** option is the default and should already be selected.

- 
- 4** Click **OK** to save the program.

**Result** The File Download window is displayed. The **Save this program to disk** option is the default and should already be selected.

- 
- 5** Click **OK** to save the program.

**Result** A Save As dialog box is displayed.

- 
- 6** Navigate to the temporary directory you created, and click the **Save** button.

**Result** A progress indicator dialog box is displayed.

.....

- 7** When the dialog box indicates that the download is complete, click **Open** to begin the installation process.

**Result** When the installation is finished, the Setup Complete window is displayed.

.....

- 8** Click **Finish** to complete the installation. It is not necessary to reboot your machine. The SMS Remote Navigator may be run immediately.

END OF STEPS

.....



## To Install the Remote Navigator on *Solaris*®

---

### Methods of installation

There are two ways to install the SMS Remote Navigator — directly from the SMS CD-ROM, or by downloading the software from the SMS.

#### From the CD-ROM

Complete the following steps to install the SMS Remote Navigator from the CD-ROM.

---

- 1 Create a temporary directory on the hard drive of the your computer to hold the installation file.  

---
- 2 With the CD-ROM in the CD-ROM drive, locate this directory on the CD-ROM:  
*/Solaris/RemoteNavigator*  

---
- 3 Copy the file  
*LSMSRemNav.tar*  
to the temporary directory.  

---
- 4 Make the temporary directory the present working directory and issue the command:  
`tar xvf LSMSRemNav.tar`  

---
- 5 When you have successfully untarred the files, change directories to the */lmf* directory created by the tar extraction process and enter the following to install the program:  
*./install*

END OF STEPS

---

#### From the SMS

To download the SMS Remote Navigator from the SMS, follow the steps below:

---

- 1 Create a temporary directory on the hard drive of your computer to hold the downloaded file.

- 
- 2 Open a browser and enter the URL of the SMS. The URL consists of the SMS IP address, its port number, and the directory in which the SMS application is stored. Depending on whether the SMS web server is HTTP or HTTPS, the URL will look like one of the following:

*http://<ip\_address>:<port>/LSMS*

— or —

*https://<ip\_address>:<port>/LSMS*

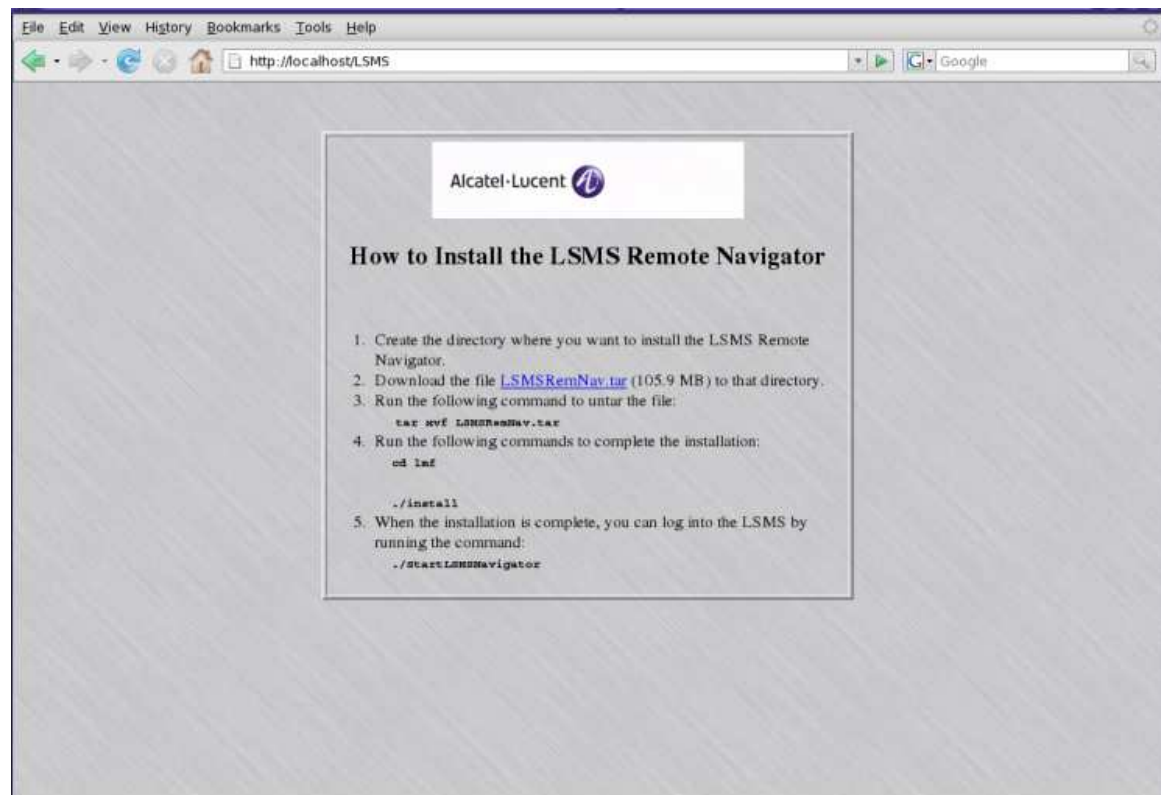
**Result** The SMS login window is displayed.

---

- 3 Enter your Admin ID and password in the appropriate fields, click the checkbox labeled **Download the LSMS Remote Navigator** and click the **OK** button.

**Result** The How to Install the Remote Navigator window is displayed (Figure 10-2, “How to Install the Remote Navigator (Solaris® Version)” (p. 10-8)).

**Figure 10-2 How to Install the Remote Navigator (Solaris® Version)**





- 
- 4 . Click the **LSMSRemNav.tar** link and download the .tar file that contains the LSMS Remote Navigator software to the temporary directory. You may want to leave the How to Install the Remote Navigator window up as a reference.

---

  - 5 Make the temporary directory the present working directory and issue the command:  
`tar xvf LSMSRemNav.tar`

---

  - 6 When you have successfully untarred the files, change directories to the /lmf directory created by the tar extraction process and enter

*./install*

to install the program.

END OF STEPS

---



## Permitting Remote Administration on the SMS

---

### Purpose

This section explains how to enable Administrators to log into the SMS remotely when the SMS is protected by a Brick device.

To set up remote administration, you have to modify the security policy of the Administrative Zone. This zone ruleset is created automatically during the installation of the SMS software. For details, refer to the *Pre-Configured Brick Zone Rulesets* appendix in the *SMS Policy Guide*.

One of these policies has to be changed to allow Administrators to log into the SMS from remote hosts outside one or more of these Bricks. This involves creating two new rules and a host group, and adding them to the security policy.

This section provides information to perform the following:

1. Create a host group containing the IP addresses of all the hosts that will be permitted to access the SMS remotely.
2. Create two rules allowing sessions to and from these remote hosts to pass through the Brick.



## To Create the Host Group

---

### When to use

The first thing you should do to set up remote administration is to create a host group that contains the IP addresses of the remote hosts that each Administrator will be using to log into the SMS.

If you do not create this host group, you will have to create separate security rules for each Administrator. However, with this host group, you will need only two rules to cover all Administrators.

If a new Administrator is introduced, or an existing Administrator leaves, you simply add the new IP address to, or delete the old IP address, from the host group. The security rules are not affected.

### Task

Complete the following steps to create a new host group.

---

- 1 Open the Policies folder.  

---
- 2 Right-click the Host Groups folder and select **New Host Group**.  

---
- 3 The Host Group Editor appears.  

---
- 4 Enter a name that uniquely identifies this host group for example, *remote\_admins*, in the **Name** field. The name can contain up to 45 alphanumeric characters.  

---
- 5 Enter a brief description of the host group in the **Description** field. The description is optional. It can contain up to 80 alphanumeric characters.  

---
- 6 Enter the IP addresses of the Administrators. Enter each IP address on a single line, or enter a range of addresses.  

---
- 7 Display the File menu and choose one of the **Save** options.

END OF STEPS

---



## To Create the Security Rules

---

### When to use

Two rules must be added to the security policy of the Administrative Zone to permit the hosts in the host group you just created to access the SMS from outside a Brick.

The two rules are needed to allow two-way communication between the remote hosts and the SMS. One rule allows the Administrator's remote session *into* the Administrative Zone and the other rule allows a session initiated by the SMS *out of* the Administrative Zone.

**Important!** If the computer the Administrator is using to log in remotely is on a LAN in a zone that is assigned to another port on the Brick, these same rules have to be added to the security policy of that zone — *with the directions reversed*.

### Create the First Rule

The first rule to be considered is the rule that allows sessions initiated by the remote Administrators to pass through a Brick into the Administrative Zone. To create this rule, follow the steps below:

- 1 Open the Policies folder.  

---
- 2 Open the Brick Zone Rulesets folder and double-click **administrativezone**.  

---
- 3 In the Brick Zone Ruleset Editor, right-click any rule and select **New**.  

**Result** The Brick Zone Rule Editor is displayed.

---
- 4 In the **Direction** field, select **IN TO ZONE** from the drop-down list. This rule will now apply to sessions initiated outside the Administrative Zone.  

---
- 5 In the **Source** field, click **Host** and select the host group from the drop-down list that contains the IP addresses of the Administrators who will be logging in remotely.  

This ensures that only sessions initiated by those IP addresses are permitted to pass through the Brick.

---
- 6 In the **Destination** field, click **Host** and enter the LSMS host group. You could also enter an asterisk, since the SMS should be the only host in the Administrative Zone.

- 
- 7 In the **Service or Group** field, select **\*\*BROWSE\*\***. In the Browse: Select a Service Group window, select:

**secure\_remote\_admin\_to\_SMS**

from the drop-down list. This is a Service Group (tcp/7000/\* and tcp/443/\*) provided with the SMS specifically for this purpose.

**Important!** The entry 'tcp/443/\*' implies that the SMS web server has been configured for HTTPS. An entry of 'tcp/80/\*' can be added to this service group if the SMS web server is set up for HTTP. However, using HTTPS is preferred because it is more secure.

- 
- 8 In the **Action** field, select **Pass** from the drop-down list.

- 
- 9 In the **Description** field, enter an optional description, if necessary.

- 
- 10 Click the **Advanced** tab and increase the value for "Session timeout".

It is recommended that the default value of 300 seconds be increased because the Remote Navigator session will be removed from the Brick after five minutes of idle time. The administrator login will still be active, but when the user attempts to reuse the GUI after, say, 30 minutes, the Brick no longer has an entry for this session. The resumed interaction looks to the Brick like a new session, but one that is starting without the normal TCP connection "handshake. The new TCP validations (configured under the Advanced tab) will block the session.

With the session timeout set to a more convenient threshold, the Remote Navigator session can be preserved for a longer period with the protection afforded by the Brick's strict TCP enforcement. For example, if you set the timeout to 3600 seconds, you will have one hour of idle time.

- 
- 11 Click the **OK** button to temporarily store the rule on the SMS.

END OF STEPS

---

## Create the Second Rule

The purpose of the second rule is to permit a session initiated by the SMS out of the Administrative Zone. This rule is the same as the first rule, except:

- **Direction** is *out of* the zone
- **Source** is the LSMS host group
- **Destination** is the host group containing the IP addresses of the remote Administrators
- **Service or Group** is *secure\_remote\_admin\_from\_SMS*.

Click the **Advanced** tab, and ensure that all TCP validations are unchecked. Otherwise if the Remote Navigator is logged in and idle for awhile, its session cache will time out. The next time the administrator attempts to use the Remote Navigator, it will need to (transparently) open a new session, and the TCP validation may block it.

Create this rule as you created the first rule, and then click the **OK** button to close the Editor. From the File menu in the Brick Zone Ruleset Editor, select **Save and Apply** to apply them to the Brick.



## To Log In from a Remote Host

---

### When to use

**Important!** It is possible to install the SMS Remote Navigator on the SMS host so that you are running both the SMS Navigator and the SMS Remote Navigator on the same machine. The only reason to do this is if you intend to use the SMS host to log into another SMS remotely.

### Task

Complete the following steps to log in from a remote host using the SMS Remote Navigator.

---

- 1 If the remote host is running *Microsoft®Windows®* or *Vista®*, click the **Start** menu and select:

**Programs > Alcatel-Lucent Security Management Server > SMS Remote Navigator**

If the remote host is running *Solaris®*, go to the installation root directory (*/opt/isms/lmfif* if you used the defaults during installation) and enter:

```
./StartLSMSNavigator [<valid URL>]
```

from the command line. The [<valid URL>] is optional. If the URL of the SMS is provided on the command line, it pre-populates the **LSMS/LSCS URL** field on the SMS Remote Navigator Login window.

In either case, the Remote Navigator Login window is displayed ([Figure 10-3, “LSMS Remote Navigator Login Window”](#) (p. 10-16)).

Figure 10-3 LSMS Remote Navigator Login Window



- 
- 2 Enter your **Admin ID** and **Password**. The Admin ID and password are the ones that were created during SMS installation, or those given to you by another administrator.

If you want to access the Status Monitor without logging into the rest of the SMS, you can check **Status Monitor Only Login**. This is useful if:

- You have a special monitoring room with large screens, and you want to display the graphs to monitor the health of the system, or
  - If you want to provide someone with the ability to monitor the system, but you do not want this person to be able to view or change the system's configuration.
- 

- 3 Enter the URL of the SMS or CS. The URL is either:

*http://<IP\_address>:<port\_number>/LSMS*

— or —

*https://<IP\_address>:<port\_number>/LSMS*

where *<IP\_address>* is the IP address of the SMS or LSCS and *<port\_number>* is the port the web server is listening on. Ports 80 and 443 are the standard ports for HTTP and HTTPS, respectively. The port your web server is using was assigned during installation; if another port was entered, use it instead.



Each URL you enter will be placed in the drop-down list in the LSMS or LSCS URL field, so that each time you enter this URL after the initial entry, you can simply select it from the drop-down list instead of typing it in. You can store multiple URLs in this list in the event that you need to log into more than one SMS remotely.

---

- 4 Click **Connect**. Initially, the remote host and the SMS will exchange keys to set up a 3DES tunnel. Once the tunnel is in place, the SMS will authenticate the administrator ID and password. If the ID and password are valid, another 3 DES tunnel is enabled to maintain maximum security throughout the session.

When you have successfully logged in, the Navigator window is displayed.

END OF STEPS

---



# Remote Administrator Capabilities

---

## Overview

Once an administrator has successfully logged into the SMS Remote Navigator, everything that an SMS administrator (LA) or group administrator (GA) can do from a local SMS - provision new Bricks, apply policy changes, create VPN tunnels, and so forth, can be done from the Remote Navigator.

The remote administrator can benefit from a number of options through the **Utilities** menu bar on the Navigator. The options are:

1. Certificate Manager - (SMS Administrators only) - This utility allows an administrator to obtain and import digital certificates issued by a Certificate Authority (CA) for user authentication. For more information, refer to the *Digital Certificates* chapter in the *SMS Policy Guide*.
2. Configuration Assistant - (SMS Administrators only) - This tool allows an administrator to easily configure a number of system wide parameters. For more information, refer to [Chapter 11, "Using the Configuration Assistant"](#).
3. New Feature Setup - (SMS Administrators only ) - The New Feature Setup utility allows an administrator to install a new license key for optional features or to increase the management capacity of the SMS. For more information, refer to [Appendix F, "New Feature Setup"](#).
4. Restart Services - (SMS Administrators only) - This tool stops and starts SMS Services on the SMS that you are remotely logged into.
5. SMS Service Status - (SMS Administrators only) - This utility presents a graphical summary of all LSMS services. This may be helpful for system monitoring or for troubleshooting purposes. For more information, refer to the *SMS Tools and Troubleshooting Guide*.
6. SMS Log Viewer - (SMS Administrators only) - The remote administrator may monitor a variety of SMS activities in "real time". This utility is particularly helpful for troubleshooting. For more information, refer to the *SMS Reports, Alarms and Logs Guide*.
7. SMS Messenger- (All Administrators) - All administrators currently logged in may now exchange short messages with this tool. It can be used for a two way exchange or a broadcast to all administrators. For more information, refer to the *Creating Groups and Administrators* chapter in this Guide.

Often it is important to monitor the status of individual Bricks. In this release, SMS administrators can access the Brick console directly from the Navigator. Once the "remote Brick console" is displayed, the admin can issue any of the commands that can be executed from a local Brick console. For more information, refer to Chapters 9 through 14 in the *SMS Tools and Troubleshooting Guide*.

When a Brick is first created on the SMS, its initial configuration must be loaded on the device. In this release, the user has the three choices to transfer the information to the Brick:

- Create a floppy with the Brick configuration on the local LSMS and load the floppy on the device.
- Create a floppy with the Brick configuration on any remote PC or workstation and load the floppy on the device.
- If a serial connection on the Brick is available from the network (as via a terminal server), the Brick configuration may be loaded onto the device without a floppy.

Of course, once the floppy has been loaded on the Brick, the SMS and Brick can communicate directly for subsequent configuration updates, new software downloads, policy changes, etc. For more information on configuring and loading Bricks, refer to the *Configuring Alcatel-Lucent VPN Firewall Brick™ Security Appliances* chapter in this Guide.

8. Edit SMS Parameters (SMS Administrators only) - this utility allows an administrator to enable or disable the Concurrency Control feature and configure additional options related to this feature. For more information, refer to the section [“Concurrency Control” \(p. 1-36\)](#) in [Chapter 1, “Getting Started”](#).
9. View SMS Parameters (SMS Administrators and Group administrators) - this utility allows an administrator to view the current Concurrency Control feature settings. For more information, refer to the section [“Concurrency Control” \(p. 1-36\)](#) in [Chapter 1, “Getting Started”](#).





# 11 Using the Configuration Assistant

## Overview

---

### Purpose

This chapter explains how to use the Configuration Assistant to set a number of parameters that affect the system's operation and performance.

The Configuration Assistant may be accessed either directly at the local SMS host or remotely while logged in via the SMS Remote Navigator. In order to run the Configuration Assistant from the Remote Navigator, you must be logged in as an SMS Administrator.

### Contents

<a href="#">The SMS Configuration Assistant</a>	11-3
<a href="#">Alarms</a>	11-9
<a href="#">Audit Trail</a>	11-11
<a href="#">Direct Paging</a>	11-13
<a href="#">FIPS</a>	11-15
<a href="#">GUI and Status Monitor Parameters</a>	11-17
<a href="#">Log Files</a>	11-19
<a href="#">Log Transfer</a>	11-22
<a href="#">Login Banner</a>	11-25
<a href="#">LSMS Web Parameters</a>	11-27
<a href="#">Reports</a>	11-29
<a href="#">SNMP Agent</a>	11-31
<a href="#">Software Download</a>	11-34
<a href="#">Strong Passwords</a>	11-40

<a href="#">TL1 Alarms</a>	<a href="#">11-42</a>
<a href="#">Tunable Parameters</a>	<a href="#">11-44</a>
<a href="#">User Authentication</a>	<a href="#">11-46</a>



## The SMS Configuration Assistant

---

### Definition

*Configuration Assistant* is the name given to the software that is used to set a variety of parameters that affect the way the overall system operates.

The installation software for the SMS gives you the opportunity to display the Configuration Assistant immediately after the SMS software has been installed. If you choose to do this, you can set any of the parameters at this time.

An alternative is to operate the system for awhile using the default parameters, and then decide whether or not to change any of the parameters. The Configuration Assistant can be activated at any time to make changes.

### Starting the Configuration Assistant - *Microsoft®Windows®* or *Vista®* Procedure

The Configuration Assistant can be started from either the local SMS host or while logged into the SMS Navigator or SMS Remote Navigator. The following explains how to do this on both the *Microsoft®Windows®* or *Vista®* and *Solaris®* platforms:

On a *Windows®* or *Vista®* platform:

---

- 1 Click **Start** on the Windows taskbar and select:

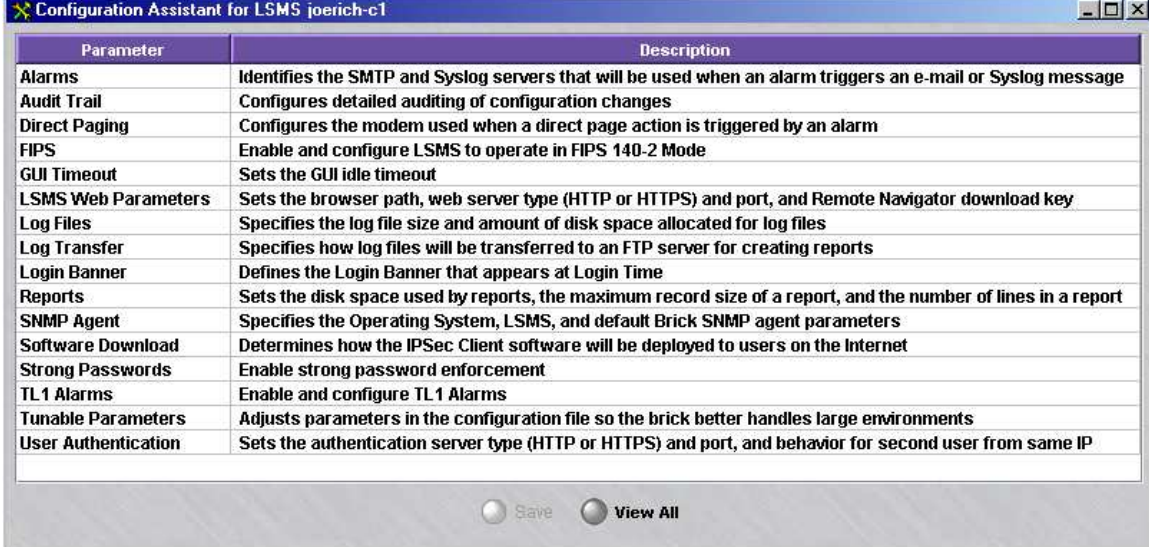
**Programs-> Alcatel-Lucent Security Management Server-> Utilities-> Configuration Assistant**

-OR -

Log into either the SMS Navigator or Remote Navigator as an SMS administrator. From the Utilities Menu Bar, click on System Utilities, then select the Configuration Assistant.

**Result** The Configuration Assistant window is displayed (Figure 11-1, “Configuration Assistant Window” (p. 11-4)).

**Figure 11-1 Configuration Assistant Window**



Parameter	Description
<b>Alarms</b>	Identifies the SMTP and Syslog servers that will be used when an alarm triggers an e-mail or Syslog message
<b>Audit Trail</b>	Configures detailed auditing of configuration changes
<b>Direct Paging</b>	Configures the modem used when a direct page action is triggered by an alarm
<b>FIPS</b>	Enable and configure LSMS to operate in FIPS 140-2 Mode
<b>GUI Timeout</b>	Sets the GUI idle timeout
<b>LSMS Web Parameters</b>	Sets the browser path, web server type (HTTP or HTTPS) and port, and Remote Navigator download key
<b>Log Files</b>	Specifies the log file size and amount of disk space allocated for log files
<b>Log Transfer</b>	Specifies how log files will be transferred to an FTP server for creating reports
<b>Login Banner</b>	Defines the Login Banner that appears at Login Time
<b>Reports</b>	Sets the disk space used by reports, the maximum record size of a report, and the number of lines in a report
<b>SNMP Agent</b>	Specifies the Operating System, LSMS, and default Brick SNMP agent parameters
<b>Software Download</b>	Determines how the IPSec Client software will be deployed to users on the Internet
<b>Strong Passwords</b>	Enable strong password enforcement
<b>TL1 Alarms</b>	Enable and configure TL1 Alarms
<b>Tunable Parameters</b>	Adjusts parameters in the configuration file so the brick better handles large environments
<b>User Authentication</b>	Sets the authentication server type (HTTP or HTTPS) and port, and behavior for second user from same IP

Save     View All

END OF STEPS



## Starting the Configuration Assistant -Solaris® procedure

On a *Solaris* platform:

---

- 1 Open a window and enter

```
cd <install_directory>
```

where <install\_directory> is the directory in which the SMS application was installed (*/opt/isms/lmf* if you used the default directory during installation).

This makes the installation root directory the present working directory.

---

- 2 Enter

```
./configurationAssistant
```

to display the Configuration Assistant window (Figure 11-1, “Configuration Assistant Window” (p. 11-4)).

- OR -

Log into either the SMS Navigator or Remote Navigator as an SMS administrator. From the Utilities Menu Bar, click on System Utilities, then select the Configuration Assistant.

**Result** The Configuration Assistant window is displayed (Figure 11-1, “Configuration Assistant Window” (p. 11-4)).

The Viewer Panel of the Configuration Assistant window contains 16 groups of parameters. The following is a brief explanation of each group:

- **Alarms**  
Identifies the SMTP and Syslog servers that will be used when an alarm triggers an e-mail or Syslog message.
- **Audit Trail**  
Allows the SMS to store archive copies of changes to Brick devices, rulesets, alarm triggers/actions, users, administrators, SMSs, and other managed objects.
- **Direct Paging**  
Configures the modem used when a direct page action is triggered by an alarm.
- **FIPS**  
Allows you to enable and configure the SMS to operate in FiPS 140-2 mode.
- **GUI and Status Monitor Parameters**  
Sets the GUI timeouts, with and without an active Status Monitor. Permits real time Brick status to be displayed on the Status Monitor for both SMSs in a redundant pair.

- **LSMS Web Parameters**  
Sets the path to the web browser executable, web server type (HTTP or HTTPS) and port, and the Remote Navigator download key.
- **Log Files**  
Sets the log file size and the amount of disk space allocated for log files. Can also define an alternate directory to store log files, as well as specify the maximum number of users that can simultaneously use the Log Viewer.
- **Log Transfer**  
Specifies how log files will be transferred to a designated FTP server for creating reports.
- **Login Banner**  
Specifies an optional text message that is displayed to administrators after a successful login to the SMS. The message can be a legal notice, security policy notification, disclaimer, etc.
- **Reports**  
Sets the disk space used by reports, the maximum record size of a report, and the number of lines on a report in both portrait and landscape formats.
- **SNMP Agent**  
Sets configuration parameters for the Operating System, SMS, and Brick SNMP Agents.
- **Software Download**  
Determines how the Alcatel-Lucent IPsec Client software will be deployed to users across the public Internet.
- **Strong Passwords**  
Enforces stricter password creation rules that comply with Sarbanes-Oxley (SOX) requirements.
- **TL1 Alarms**  
Allows you to enable and configure TL1 alarms.
- **Tunable Parameters**  
Allows you to adjust certain *maxHeap* parameters in the configuration file (*config.ini*) so that the Brick better handles environments with large numbers of Bricks, client tunnels, and audit records.
- **User Authentication**  
Sets the authentication server type (HTTP or HTTPS), and the port.

.....  
E N D O F S T E P S  
.....

## To set Configuration Assistant parameters

Using the Configuration Assistant window, you can set the individual parameters that are part of each parameter group. After setting a parameter, you will be instructed to stop and restart services, if necessary, to activate your changes.

Complete the following steps when setting a parameter:

- 1 Double-click on the the parameter group in the Configuration Assistant window.  
**Result** The parameter group is highlighted, and the related parameters are displayed in a separate window for editing. If a parameter has a default value, it is displayed in the field and can be changed if desired.
- 2 Make any necessary additions or changes to the fields shown.
- 3 Click the **OK** button to temporarily store the changes on the SMS.  
Click the **Cancel** button to cancel the edit operation and return to the Configuration Assistant window.  
**Result** If you click the **OK** button, the parameter change(s) is temporarily stored, the editing window is removed, and the system returns to the Configuration Assistant window.
- 4 Click the **SAVE** button on the Configuration Assistant window to permanently save the parameter change(s) on the SMS.

END OF STEPS

### To view all settable parameters

To view the values of all the parameters in one window, click the **VIEW ALL** button on the Configuration Assistant window to display the Configuration Parameters window. An example of this window is shown in [Figure 11-2, “Configuration Parameters Window” \(p. 11-8\)](#) .

The Configuration Parameters window has a scrollbar which allows you to scroll through the remaining list of parameters that are not immediately visible on the window.

Figure 11-2 Configuration Parameters Window

Parameter	Value
<b>Alarms</b>	
SMTP Host	
Account Name	
Syslog Host	
Syslog Port	
Trigger Alarm Code	no
<b>Audit Trail</b>	
Keep Archived Files for (days)	5
<b>Direct Paging</b>	
Modem Port	
Initialization String	ATE0
Reset String	ATZ
Dial String	ATDT
Modem to CPU Speed (Baud)	9600
<b>FIPS</b>	
Enable FIPS 140-2 Mode	no
LSMS Web Server HTTPS Cipher Suites	SSL
User Auth HTTPS Cipher Suites	SSL
<b>GUI Timeout</b>	
GUI Idle Timeout (secs)	3600
<b>LSMS Web Parameters</b>	
Browser Path	
LSMS Web Server Type	http
LSMS Web Server Port	80
Authentication Key	
<b>Log Files</b>	
Root Directory for Log Files	C:\isms\lmf
Max simultaneous Remote Log Viewer Connecti...	10
Session : LogFile Rollover Interval (mins)	
Session : Max LogFile Size (MB)	10
Session : Max Alloc(MB)	1000
Session : Halt Logging if Log Full	no
Admin Events : LogFile Rollover Interval (mins)	
Admin Events : Max LogFile Size (MB)	1

OK

Click the **OK** button to close the window.

The remainder of this chapter explains in greater detail how to set any of the parameters shown.



# Alarms

---

## Overview

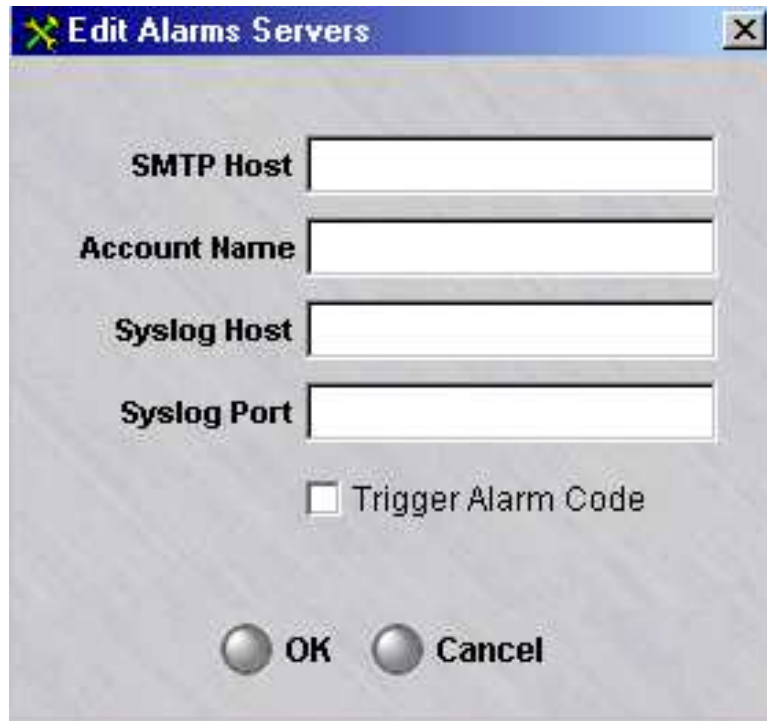
The Alarms parameters allow you to indicate the SMTP and Syslog servers that will be used when an alarm triggers an e-mail or Syslog message.

If you modify any of these parameters, you will have to stop and then restart all the SMS services.

## Default Values

There are no default values provided for the Alarms parameters. As the [Figure 11-3, “Edit Alarms Servers”](#) (p. 11-9) window shows, you have to enter the appropriate information for the first time.

**Figure 11-3 Edit Alarms Servers**



## SMTP Host

The **SMTP Host** field identifies the Simple Mail Transport Protocol server(s) that will process e-mail requests generated by alarms that have been configured to trigger e-mail messages.

You can enter one SMTP host in this field, or you can enter multiple hosts, separating each host with a comma.

If DNS is accessible from the SMS, you can enter the machine name(s) of the SMTP host(s). If not, you have to enter the IP address(es).

### Account Name

The **Account Name** field identifies the sender of the e-mail message that is triggered by an alarm. This e-mail address is used to allow the SMS to send e-mail to the specified server.

You can only enter one account in this field.

### Syslog Host

The **Syslog Host** field identifies the Syslog server that will process the Syslog messages generated by alarms that have been configured to trigger Syslog messages.

You can only enter one Syslog host in this field.

If DNS is accessible from the SMS, you can enter the machine name of the Syslog host. If not, you have to enter the IP address.

### Syslog Port

The **Syslog Port** field identifies the port on which the Syslog server will be listening to receive Syslog messages.

Typically, the Syslog server listens on port 514.

### Trigger Alarm Code

Click this checkbox to turn the alarm code feature on. When it is on, you can include an alarm code in a rule, so that when the rule is invoked by an inbound or outbound session, an alarm is triggered (refer to the *Alcatel-Lucent VPN Firewall Brick™ Security Appliance Zone Rulesets* chapter in the *SMS Policy Guide*).

When the alarm code feature is turned on, the SMS has to parse all of the session log records, which can possibly cause a degradation in performance.



# Audit Trail

---

## Overview

The Audit Trail feature, which is always enabled, allows you to preserve archive copies in the SMS installation directory of all changes made (additions, modifications, deletions) to the following managed objects:

- Bricks
- Brick zone rulesets
- Host groups
- Service groups
- Application filters
- Client tunnels
- Client tunnel defaults
- LAN-LAN tunnel defaults
- LAN-LAN tunnels
- Domain name groups
- Dependency masks
- Alarm triggers
- Alarm actions
- TL1 alarms
- Report settings
- Users
- User groups
- Administrators
- Groups
- Authentication services
- SMSs/CSs
- Certificates
- CRLs
- VPN certificate group assignments
- Proxies for CRL updates

This feature also tracks Start, Stop, and Restart Services events.

**Figure 11-4 Edit Audit Trail Configuration Window**



### **Keep Archived Files For (Days)**

You can specify how many days you wish to keep the archive files of changes made. Valid values are 1 to 365 days. The default value is 5 days. If no value is entered, the archive files are kept indefinitely.





## Direct Paging

---

### Direct paging parameters

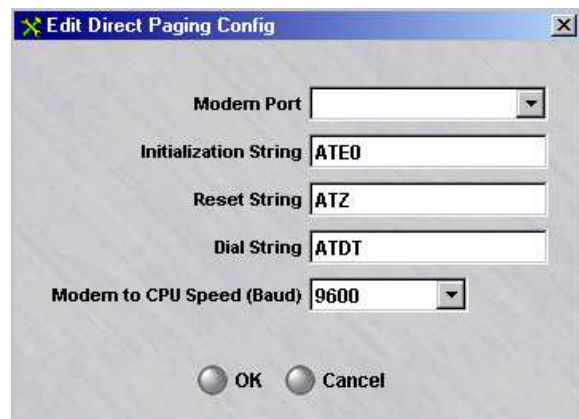
The Direct Paging parameters allow you to configure the modem that will be used when an alarm is set up to page an administrator.

The page is sent via a PSTN/modem-based connection that is made to a wireless pager service provider, such as SkyTel.

### Default Values

Figure 11-5, “Edit Direct Paging Configuration Window” (p. 11-13) shows an example of the Edit Direct Paging Configuration window with any default values for the Direct Paging parameters.

Figure 11-5 Edit Direct Paging Configuration Window



### Modem Port

The **Modem Port** field specifies the physical port on the SMS to which the modem is connected.

- For *Windows*<sup>®</sup> and Vista server platforms, a COM port is used.
- For *Solaris*<sup>®</sup> server platforms, the modem is a serial device in the *Unix*<sup>®</sup> file system. The default is */dev/cua/a*.

### Initialization String

The **Initialization String** field contains a Hayes-modem string that is used to initialize the modem every time a direct page is transmitted.

Refer to the Hayes Command Set documentation of your modem manufacturer for the exact syntax of this string.

This string is not required and can be left blank or the default (ATE0) can be accepted.

### Reset String

The **Reset String** field contains a string that is sent to the modem if the modem is unresponsive.

For example, if the modem does not respond to the SMS commands, the reset string will be sent.

This string is not required and can be left blank or the default (ATZ) can be accepted.

### Dial String

The **Dial String** field contains a string that is sent to the modem to cause the modem to dial. It defaults to Hayes touch-tone dial command.

Examples include:

- ATDT \*nnn,  
Where nnn is an access code. Used for touch-tone dialing to dial-out.
- ATDP \*9,  
Used for pulse-signaling. The \*9 is included to dial-out.

### Modem Speed

The **Modem to CPU Speed (baud)** field specifies the speed at which the CPU of the SMS talks to the modem.

This string is not required and can be left blank, or the default, 9600 bits per second, can be entered.

**Important!** You may need to set the **Modem to CPU Speed (baud)** field to match the speed of the paging service provider. This may be especially necessary if the value is very low (300 bps) or very high (56K).



# FIPS

---

## Overview

All communications between an SMS and a Brick device are encrypted. Many US government agencies require that the SMS and devices communicate with each other in compliance with several Federal Information Processing Standards (FIPS):

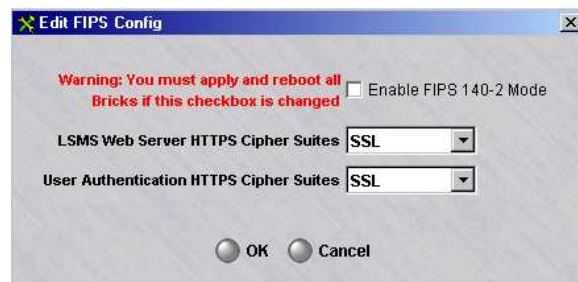
- FIPS Pub 180-1 (Secure Hash Algorithm, SHA-1)
- FIPS Pub 140-1 (Security Requirements for Cryptographic Modules)
- FIPS Pub 186-2 (Digital Signal Standard)

If you are a US government department, it is recommended that you click the **Enable FIPS 140-2 Mode** checkbox. When FIPS is enabled, it is enabled for the SMS and all managed Bricks. If the value of this checkbox is changed, all Bricks must be applied and rebooted.

## Default Values

Figure 11-6, “Edit FIPS Configuration Window” (p. 11-15) shows an example of the Edit FIPS Parameters Configuration window with any default values.

**Figure 11-6 Edit FIPS Configuration Window**



## LSMS Web Server HTTPS Cipher Suites

If FIPS 140-2 Mode is enabled, the cipher suites for the SMS Web Server HTTPS is set to the FIPS-compliant value **TLS** (Transport Layer Security). **SSL** (Secure Sockets Layer) is not FIPS-compliant, but is provided as a choice for customers that prefer to use this option. When FIPS is enabled, HMAC MD5 is not available as a choice for ISAKMP and IPsec Proposal Authentication Type for Client tunnel Endpoints and LAN-LAN Tunnels.

## User Authentication HTTPS Cipher Suites

If FIPS 140-2 Mode is enabled, the cipher suites for the User Authentication HTTPS is set to the FIPS-compliant value **TLS** (Transport Layer Security). **SSL** (Secure Sockets Layer) is not FIPS-compliant, but is provided as a choice for customers that prefer to use this option. When FIPS is enabled, HMAC MD5 is not available as a choice for ISAKMP and IPsec Proposal Authentication Type for Client tunnel Endpoints and LAN-LAN Tunnels.



## GUI and Status Monitor Parameters

---

### Overview

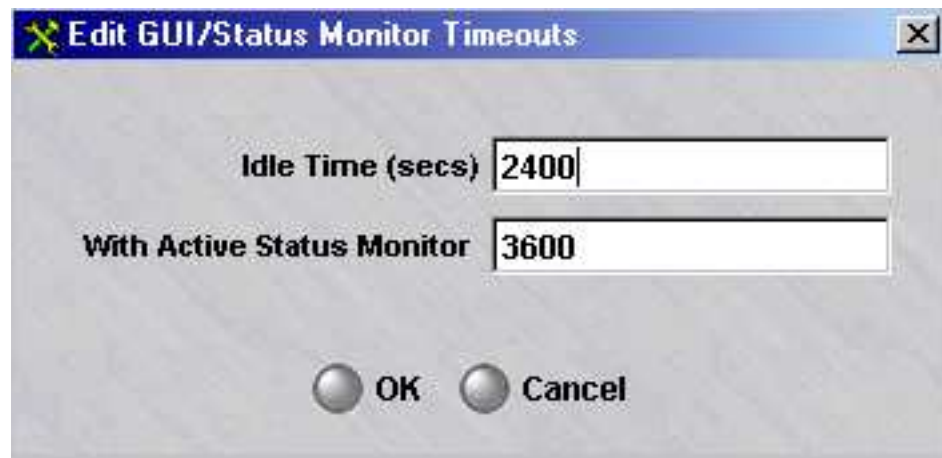
The GUI Timeout parameters allow you to set the Idle Timeout period for inactivity on the SMS GUI before an administrator is “locked out” of the session. Note that when the GUI times out, the SMS session is still active, but in a “locked” state.

If you modify any of these parameters, you will have to stop and then restart all the SMS services.

### Default Values

Figure 11-7, “Edit GUI/Status Monitor Timeouts Window” (p. 11-17) shows an example of the Edit GUI/Status Monitor Timeouts window with any default values.

Figure 11-7 Edit GUI/Status Monitor Timeouts Window



### Idle Time

The **Idle Time** field determines the length of time that must elapse without GUI activity before an administrator’s session is locked.

The default is 2400 seconds.

### With Active Status Monitor

The purpose of the **With Active Status Monitor** field is to allow you to set a second GUI timeout that only applies when the Status Monitor is active.

This allows an administrator to remain logged in for a longer period of time when performing only monitoring duties, such as when keeping an eye on the Status Monitor but not initiating any GUI-related activities.

For this reason, the value of this field should always be equal to or greater than the value in the **Idle Time** field. The default is 3600 seconds.



# Log Files

---

## Log files parameters

The Log Files parameters allow you to determine four sets of parameters:

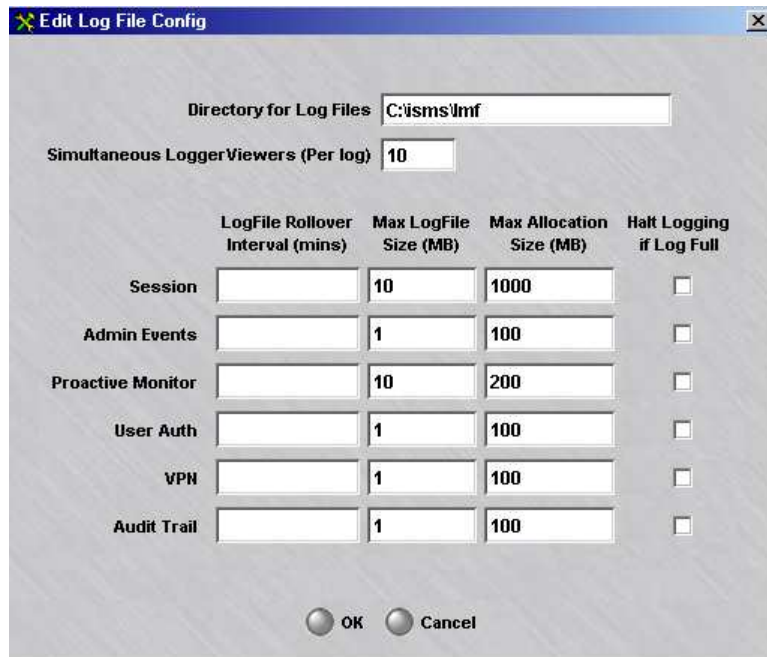
- The directory used to store SMS log files
- The maximum number of users that can simultaneously access the SMS Log Viewer
- The log file rollover interval, based on a specified time interval or filesize constraint
- The maximum size of the various log files and the amount of disk space to be allocated for log files. These parameters also allow you to indicate whether or not you want all collection of log data by the SMS stopped when the disk space allocated for log files is exhausted.

If you modify any of these parameters, you will have to stop and then restart all SMS services.

## Default Values

[Figure 11-8, “Edit Log File Configuration Window” \(p. 11-19\)](#) shows the Edit Log File Configuration Window with the default values for the Log Files parameters.

**Figure 11-8 Edit Log File Configuration Window**



## Directory for log files

If you wish to store all of the SMS log files on the SMS but not in the default SMS installation directory (for *Windows*® `c:\isms\lmf`, and for *Solaris*® and Linux `/opt/isms/lmf`), specify the new directory path here.

If you would like to store the SMS log files on a remote machine, please review the *Log Transfer* parameter later in this chapter.

## Simultaneous logger viewers (per log)

Administrators may review real time system activity using the SMS Log Viewer. When the stand-alone SMS Log Viewer is used, it accesses the log files directly. This is the most efficient and least performance impacting way of monitoring the logs. For convenience, the SMS Log Viewer is also available from the local and remote Navigator. When accessed in this fashion, log files are monitored by the SMS Admin service and data is transmitted over the link between the SMS and the Navigator. If multiple administrators access the logs in this fashion, SMS performance and network bandwidth will be adversely impacted.

This configuration option allows you to limit the number of simultaneous Log Viewers that can be started via the Navigator to help preserve performance and bandwidth.

By default, this value is set to 10 users.

## Logfile rollover interval (min)

If an interval is specified (in minutes), log files will rollover to a new file name after the elapsed time interval or the maximum log file size is met, whichever comes first.

## Maximum log file size

The SMS maintains five logs, and for each of these logs, the **Max LogFile Size** fields determine how large each log file will be permitted to grow before a new file is begun.

The old log files are saved until the maximum disk space allocated for that log is reached (see below). At that time, the SMS begins to delete the files to free up space, with the oldest files deleted first.

The following shows each log and its default maximum file size:

Log File	Maximum File Size
Session Log	10 Mb
Admin Events Log	1 Mb
Proactive Monitor Log	10 Mb
VPN Log	1 Mb



Log File	Maximum File Size
User Auth Log	1 Mb
Audit Trail	1 Mb

### Maximum disk allocation

The **Max Allocation** field determines the amount of disk space that will be allocated to each log.

The following shows each log and its default disk allocation:

Log	Maximum Disk Allocation
Session Log	1000 Mb
Admin Events Log	100 Mb
Proactive Monitor Log	200 Mb
VPN Log	100 Mb
User Auth Log	100 Mb
Audit Trail	100 Mb

If you have upgraded the SMS software from an earlier version, the default allocations will be based on the allocations you were using in the earlier version.

### Halt logging if log full

A checkbox labeled **Halt Logging if Log Full** appears to the right of each log.

By default, the checkbox is not checked. If the checkbox is unchecked, the SMS deletes old log file(s) to free up space, and continues logging.

If the checkbox is checked, the SMS stops logging for the associated log type when the log is full (**Maximum Allocation Size** is reached).

**Important!** To stop the Brick device from passing traffic when the log is full, make sure that the checkbox labeled **Halt All Traffic if Audit Fails** on the Options tab of the Brick Editor is checked.

The Brick Editor is the window that is used to configure a Brick (refer to [Chapter 3, “Configuring and Activating an Alcatel-Lucent VPN Firewall Brick™ Security Appliance”](#)).

□

## Log Transfer

---

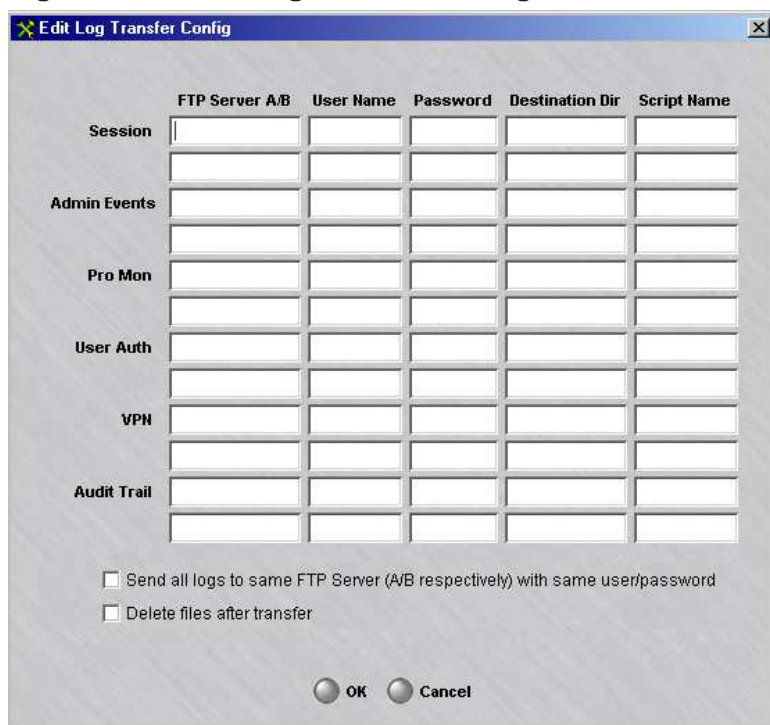
### Log transfer parameters

The Log Transfer parameters allow you to specify where and how the various log files will be transferred for use in creating reports.

### Default Values

There are no default values provided for the Log Transfer parameters. As [Figure 11-9, “Edit Log Transfer Configuration Window”](#) (p. 11-22) shows, you have to enter the appropriate information for the first time.

**Figure 11-9 Edit Log Transfer Configuration Window**



### FTP Server

For each of the five logs, the **FTP Server A/B** field indicates the host(s) that will receive the transferred log files. The host(s) must be an FTP server. Up to two hosts per log can be entered.

If DNS is accessible from the SMS, you can enter the machine name of the host. If not, you have to enter the IP address.

**User Name**

The user name must be a valid user account on the FTP server.

**Password**

The password must be the valid password for the user account entered in the **User Name** field.

**Important!** Even if you log on as anonymous, you must still enter a password.

**Destination Directory**

The destination directory is the directory on the FTP server in which the log files will be placed.

Enter either an absolute path name or a path name that is relative to the user's home directory.

**Script Name**

Scripts can be created to pre-process the log files before they are transferred to the FTP server. You could, for example, create a script to compress the files to make the transfer more efficient.

If you will be making use of a script, enter the path and name of the file that contains the script for each log in the **Script Name** field.

**Same FTP Server**

If you want to send all the logs to the same FTP server and account, the Configuration Assistant provides an easy way to do this.

Click the checkbox labeled **Send all logs to same FTP server with same user/password**.

This will cause the **FTP Server A/B**, **User Name**, and **Password** fields for the last four logs to become greyed-out, as shown in [Figure 11-10, "Same FTP Server" \(p. 11-24\)](#).

Figure 11-10 Same FTP Server



Enter an FTP server, user name, and password for the Session log. The other three logs will automatically be sent to the same FTP server, using the same user name and password.

Note that you must enter a different destination directory and script for each of the four logs.

### Delete Files

If you want to delete the log files after they are transferred, click the checkbox labeled **Delete files after transfer**.

# Login Banner

---

## Overview

When this feature is enabled, a login banner is displayed immediately after an administrator successfully logs into the SMS Navigator. Refer to [Figure 11-12, “Sample Login Banner Window”](#) (p. 11-26) for the default notice (computer misuse act notice). The feature is enabled by placing a check mark in the check box labeled **Enable Login Banner** on the Edit Login Banner Configuration Window. The notice can be edited by clicking on **Edit** and editing the text in the edit box (An example is shown in [Figure 11-11, “Edit Login Banner Configuration Window \(With Default Banner Text\)”](#) (p. 11-25)).

## Default Values

**Figure 11-11 Edit Login Banner Configuration Window (With Default Banner Text)**

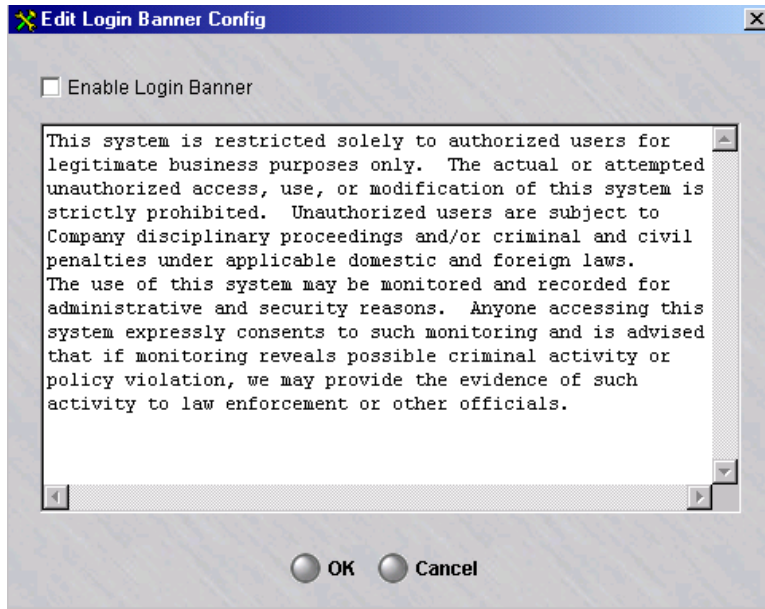
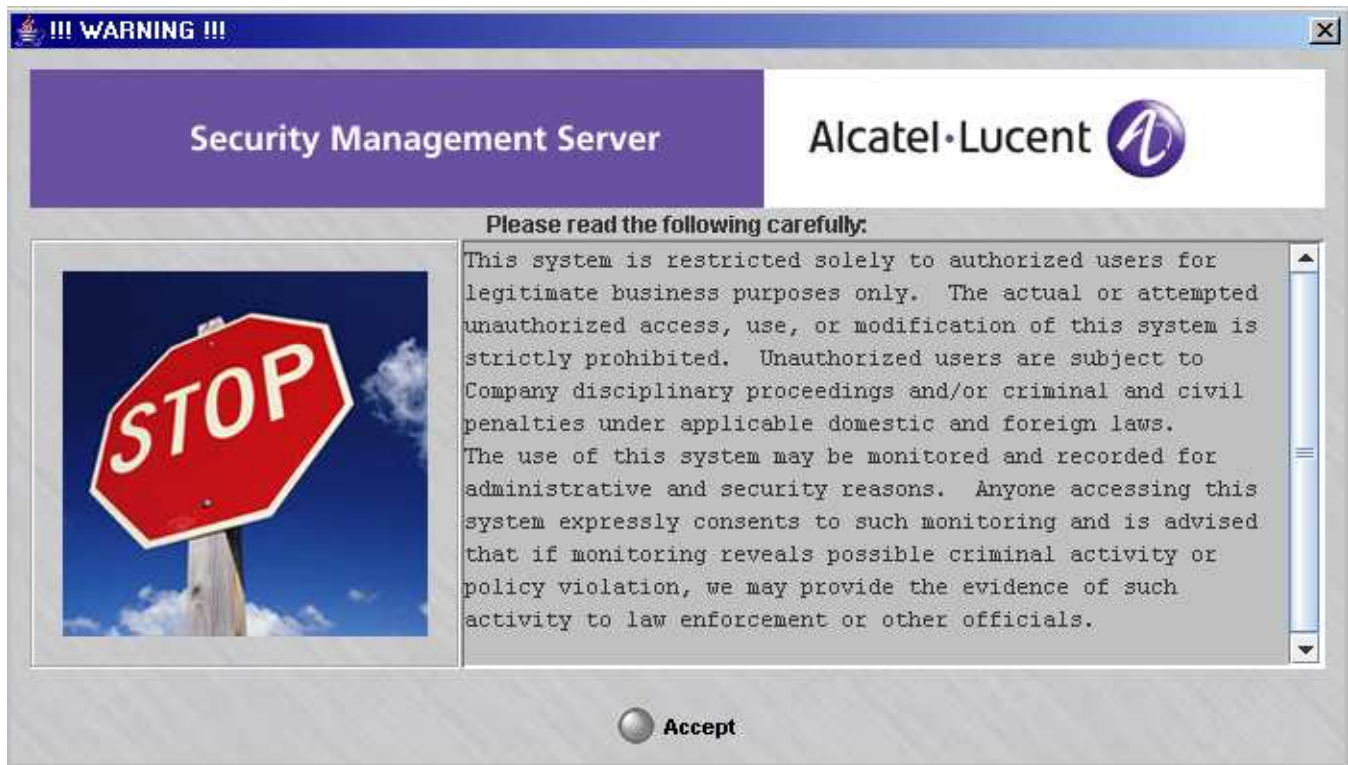


Figure 11-12 Sample Login Banner Window



□

## LSMS Web Parameters

---

### LSMS web parameters

The LSMS Web parameters allow you to indicate the default path to browser software, the type of Web server (HTTP or HTTPS) running in the SMS, and the port on which it is listening.

If you have obtained a digital certificate from Verisign or another certificate authority, the Web server should be HTTPS; if you have not, the Web server should be HTTP.

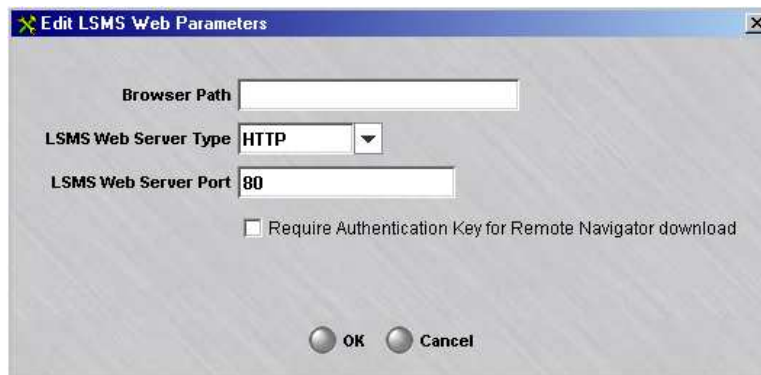
If you modify any of these parameters, you will have to stop and then restart all the SMS services.

### Default values for web server, listening port

The default values for the web server and listening port are determined during the installation of the SMS software.

[Figure 11-13, “Edit LSMS Web Parameters Window” \(p. 11-27\)](#) shows a sample of the Edit SMS Web Parameters window with default values for the LSMS Web Server type and LSMS Web Server Port. The default is a HTTP Web server listening on port 80, the standard HTTP port.

**Figure 11-13 Edit LSMS Web Parameters Window**



### Browser Path

This field allows you to store the default path to a browser for viewing SMS reports and online help files of error codes and subnet masks. If this field is not populated, a pop-up window is displayed when you initially access a report or online help, prompting you to enter a temporary path to browser software for the login session.

## LSMS Web Server Type

The type of web server will either be HTTP or HTTPS, depending on the type that was entered during the installation of the SMS software.

If you will be accessing the SMS remotely, you need to consider the security of the SMS web server. The Remote Navigator provides secure, encrypted access to the SMS.

The Remote Navigator does not use the SMS web server during login, or to perform SMS administration. However, the web server is used to view reports, online help, and download Brick floppy packages and new Remote Navigator software. Of these, the only one that may contain sensitive information is reports.

If you need to view reports remotely over the public internet, and you will not be using the Alcatel-Lucent IPsec Client to establish a secure encrypted tunnel, it is strongly recommend that you set up the SMS web server for HTTPS.

## LSMS Web Server Port

The port number will be the port that was entered during the installation of the SMS software.

Port 443 is standard for HTTPS and port 80 is standard for HTTP. However, non-standard ports can be entered.





# Reports

---

## Reports parameters

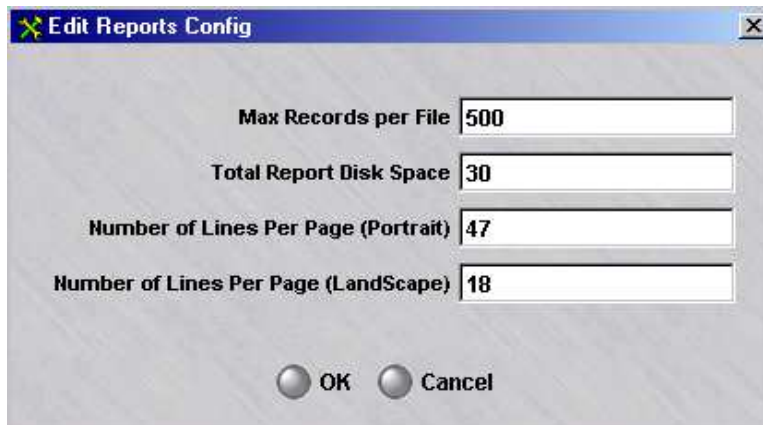
The Reports parameters allow you to specify the maximum number of records in a report file and the total amount of disk space to be allocated for reports.

They also allow you to set the number of lines per page in both portrait and landscape formats.

## Default Values

Figure 11-14, “Edit Reports Configuration Window” (p. 11-29) shows the default values for the Reports parameters.

**Figure 11-14 Edit Reports Configuration Window**



## Maximum Records Per File

The **Max Records per File** field specifies the maximum number of records permitted in any HTML report file.

The default is 500. The minimum value is 50.

## Total Report Disk Space

The **Total Report Disk Space** field specifies the amount of disk space (in megabytes) to be allocated for report output.

The default is 30 megabytes.

## Lines Per Page

The **Number of Lines per Page (Portrait)** and **Number of Lines per Page (Landscape)** fields specify the number of lines per printed page in each format.

The default for portrait is 47 and for landscape 18.



## SNMP Agent

---

### SNMP agent parameters

The SNMP Agent Parameters window allows you to configure the Operating System SNMP Agent port, the SMS SNMP Agent port and read community string, and the default values for the Brick SNMP Agent.

The Brick SNMP Agent default values configured here are populated on the Options tab of the Brick Editor when the SNMP agent on the Brick is enabled for the first time, or the Brick SNMP agent is enabled and the related fields on the Brick Editor are blank.

The SNMP agent runs continuously on the SMS and responds to queries initiated by a Network Management Station (NMS) administrator. It is optional to enable the SNMP agent software on a Brick, which allows an NMS to query a Brick directly for SNMP configuration and status information.

For details about the SNMP on the SMS and SNMP on the Brick features, refer to [Chapter 15, “Simple Network Management Protocol \(SNMP\)”](#).

If you modify the Operating System or SMS SNMP Agent parameters via the Configuration Assistant, the SMS services must be restarted. If you modify the Brick SNMP Agent defaults, you must restart the SMS Navigator to see the new defaults.

### Default Values

[Figure 11-15, “Edit SNMP Configuration Window”](#) (p. 11-32) shows the default values for the SNMP Agent parameters.

Figure 11-15 Edit SNMP Configuration Window



The screenshot shows a window titled "Edit SNMP Config" with three main sections:

- Operating System SNMP Agent:** Contains a single text input field labeled "Operating System SNMP Agent Port".
- LSMS SNMP Agent:** Contains two text input fields: "LSMS SNMP Agent Port" with the value "161" and "LSMS Read Community" with the value "public".
- Defaults for Brick SNMP Agent:** Contains four text input fields: "Brick SNMP Agent Port", "Brick Read Community" with the value "public", "Brick sysLocation", and "Brick sysContact".

At the bottom of the window are "OK" and "Cancel" buttons.

### Operating System SNMP Agent Port

If you have the Operating System SNMP Agent enabled, or have other SNMP Agent software running on the host machine where SMS is installed, all SNMP GET requests for objects that are not defined in the SMS MIB will be forwarded to the port that you designate here.

You can change the port in the **Operating System SNMP Agent Listening Port** field. The port that you enter in this field must be different from the value specified for the **LSMS SNMP Agent Port**.

### LSMS SNMP Agent Port

This field displays the default UDP port that the SMS SNMP agent is listening on. This port value is set to 161 if you selected the default value during SMS installation. If you selected a different port during installation, that port is displayed as the default in this field.

You can change the port in the **LSMS SNMP Agent Listening Port** field. The port that you enter in this field must be different from the value specified for the **Operating System SNMP Agent Port**.

### LSMS Read Community

While the SNMP agent on the SMS allows read-only access to the SNMP reporting information by the NMS, this “community string” (which is similar to a password) is used as an additional security mechanism to authenticate NMS hosts who access the SMS for SNMP data. By default, this field is set to `public`.

### Brick SNMP Agent Port

This field displays the default UDP port that the Brick SNMP agent is listening on. This value is used to populate the Brick SNMP Agent Port field on the Options tab of the Brick Editor when SNMP agent is enabled on the Brick for the first time and can be changed.

If the default value of this UDP port is changed, the pre-existing rule in the *firewall* zone for NMS-to-Brick SNMP traffic must also be edited to specify the new port, or a new rule must be created with the new port value.

### Brick Read Community

While the SNMP agent on the Brick allows read-only access to the SNMP reporting information by the NMS, this “community string” (which is similar to a password) is used as an additional security mechanism to authenticate NMS hosts who access the Brick for SNMP data. By default, this field is set to `public`.

### Brick sysLocation

This text field is used to record specific details about the location of a Brick device, such as rack number, floor, host name, and so forth. This field allows up to 256 characters. Commas are not allowed.

### Brick sysContact

This text field is used to record specific contact details about the Brick, such as a person’s name, title, office location, telephone number, and so forth. This field allows up to 256 characters. Commas are not allowed.



## Software Download

---

### Alcatel-Lucent IPsec Client CD-ROM

The Alcatel-Lucent IPsec Client CD-ROM provides software that can be directly installed on a client user's laptop or distributed to many Alcatel-Lucent IPsec Client users across the public Internet.

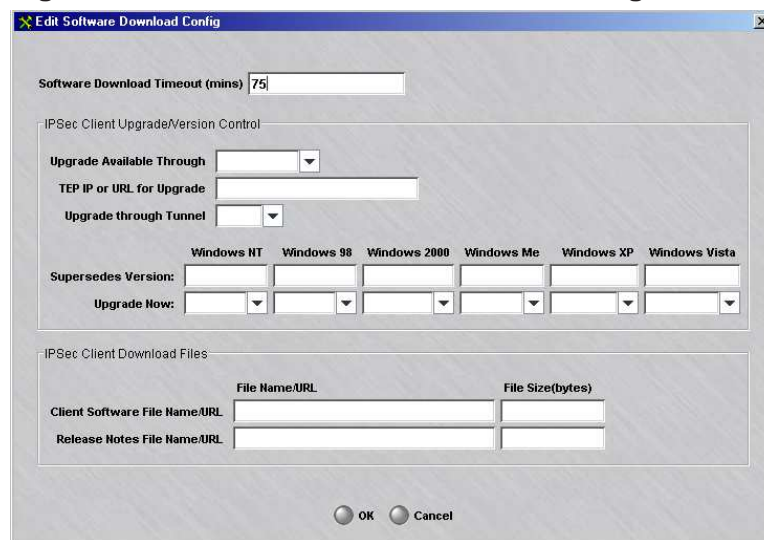
When distributing the software across the Internet, the software on the CD-ROM must be copied to either the SMS, an FTP server, or a Web server. If you suspect that simultaneous downloads from the SMS may degrade performance, you may want to consider distributing the software from an FTP server or Web server instead.

If you modify any of these parameters, you may have to stop and then restart all the SMS services.

### Default Values

There is one default value provided for the Log Transfer parameters (software download timeout). As [Figure 11-16, "Edit Software Download Configuration Window"](#) (p. 11-34) shows, for the rest of the parameters you have to enter the appropriate information for the first time.

**Figure 11-16 Edit Software Download Configuration Window**



### LSMS Software Download

When distributing the software from the SMS that is "behind a Brick", rules need to be applied to the interfaces of the Brick devices through which the software must pass.

Examples of the required rules are provided in the *vpnzone* Brick zone ruleset. Rules #305 and #306 can be used as a template when the software is distributed through a tunnel. Rule #310 can be used as a template when the software is distributed outside of a tunnel.

### FTP/Web Server Download

To provide a level of security when distributing software from publicly accessible FTP server or Web servers, you should force the Alcatel-Lucent IPsec Client users to be authenticated.

When distributing the software from an FTP server or Web server that is "behind a Brick", a rule needs to be applied to the interfaces of the Brick devices between the FTP server or Web server and the client. For example, the rule could be defined as follows:

- Source = All\_Users
- Destination = <FTP/Web Server>
- Service = FTP
- Action = Pass

### Before You Begin

To set up the Alcatel-Lucent IPsec Client software so it can be distributed from the SMS, an FTP server, or a Web server, do the following:

- 1 Insert the Alcatel-Lucent IPsec Client CD-ROM into the disk drive on the SMS.
- 2 Copy the *clientSWversion.info* file into the <LSMS Root>/fac/docroot directory on the SMS.
- 3 If distributing the software from the SMS, copy the *9.4.xxx.exe* file (where *xxx* is the build number) and the *releasenotes.txt* file into the <LSMS Root>/fac/docroot directory on the SMS.  
 For example, if you accepted the default directory during installation, on a Windows® SMS, copy the above files to  
*c:\isms\lmf\fac\docroot.*
- 4 If distributing the software from an FTP server or Web server, insert the Alcatel-Lucent IPsec Client CD-ROM into the disk drive on the FTP server or Web server and copy the *9.4.xxx.exe* file (where *xxx* is the build number) and the *releasenotes.txt* file into a

directory.

END OF STEPS

---

### Software Download Timeout (minutes)

The **Software Download Timeout** field sets the amount of time that is allocated for downloading the software to the Alcatel-Lucent IPsec Client host. The timer starts after the Alcatel-Lucent IPsec Client user has successfully been authenticated and downloading the software has been initiated.

If the period of time expires and the software download is not complete, the download will terminate. The Alcatel-Lucent IPsec Client user will then have to be re-authenticated.

The default timeout is 75 minutes. This should provide an ample amount of time for downloading the software (~7 MB) using a 14.4 kbps modem connection. However, if necessary, you can increase the timeout.

**Important!** This timeout value overrides the authentication timeout value (refer to the *User Authentication* chapter in the *SMS Policy Guide* for details).



## Alcatel-Lucent IPSec Client Upgrade/Version Control

Specify values for the fields, as the following table explains:

Field	Selection	Description
Upgrade Available Through	Specific TEP	Applicable for both methods of download. Implies the software will be downloaded from a specific tunnel endpoint (TEP) associated with a Brick interface. Enter the IP address of the TEP in the <b>TEP IP or URL for Upgrade</b> field.  This address was entered when the ruleset containing the rules establishing the tunnel is assigned to a Brick interface (refer to <a href="#">Chapter 4, “Configuring Alcatel-Lucent VPN Firewall Brick™ Security Appliance Ports”</a> ).
	Any TEP	Applicable for both methods of download. Implies the software will be downloaded from the currently active tunnel endpoint being used by the client.  In this case, entering the IP address of the TEP in the <b>TEP IP or URL for Upgrade</b> field is not required.
	URL	Applies only when the software will be downloaded from an FTP server or Web server.  This requires entering the full pathname (including the file name) in the <b>TEP IP or URL for Upgrade</b> field as described below.
TEP IP or URL for Upgrade	If <b>Specific TEP</b> was selected...	Enter the IP address of the TEP.
	If <b>Any TEP</b> was selected...	This field is not editable and “any” is displayed.
	If <b>URL</b> was selected...	Then enter the full pathname of the Web server or FTP server (including the file name). For example: <i>ftp://105.39.90.100/Upgrade/9.4.0.160.exe</i> <i>http://www.your_company.com/ipsec_client/upgrade.html</i>

Field	Selection	Description
Upgrade Through Tunnel	Yes	If the software can be upgraded through a tunnel, the Alcatel-Lucent IPsec Client user is informed of the availability of new software at the end of tunnel establishment.
	No	If the software cannot be upgraded through a tunnel, the Alcatel-Lucent IPsec Client user is informed of the availability of new software at the end of disabling the tunnel.

### Supersedes Version

For each platform, the version of software that can be superseded by the new software on the SMS, an FTP server, or Web Server is displayed.

The versions of software that are displayed are pulled from the *clientSWversion.info* file that was copied to the SMS as explained in "Before You Begin".

For each platform, decide if you want client users to be notified that the new software is available. Choose either:

- **Yes**  
After a user has successfully been authenticated, they will immediately receive notification when new software is available.
- **No**  
After a user has successfully been authenticated, they will NOT receive notification when new software is available.

### Alcatel-Lucent IPsec Client Download Files

In these fields, enter the name and size of the software to be downloaded and optionally, the release notes that may accompany it.

These fields only require values if the software will be distributed from the SMS.

- **Client Software Name/URL**

Note that:

- In the **File Name/URL** field, enter the name of the software file to be downloaded from the SMS. For example, 9.4.160.exe.

This file must reside in the *<LSMS Root>/fac/docroot* directory, for example, *c:\users\isms\lms\fac\docroot*, and must match the name that was copied from the CD-ROM as explained in "Before You Begin".

- In the **File Size(bytes)** field, enter the size of the file.

For example, 800000 indicates that the file size is approximately 8 MB.

- **Release Notes File Name/URL**

Note that:

- In the **File Name/URL** field, optionally enter the name of the Release Notes file that will accompany the software. For example, *releasenotes.txt*.

This file must reside in the *<LSMS Root>/fac/docroot* directory, for example, *c:\users\isms\lmf\fac\docroot*, and must match the name that was copied from the CD-ROM as explained in "Before You Begin".

Even though this is optional, it is recommended to provide Release Notes so that users are aware of the new features and bug fixes that are included in the upgrade software.

- In the **File Size(bytes)** field, enter the size of the file.  
For example, 1000 indicates that the file size is approximately 1 K.



## Strong Passwords

---

### Strong passwords

The Strong Password option, when enabled, provides access to a set of password restrictions that can be applied when creating new passwords or modifying existing passwords in the SMS, to comply with Sarbanes-Oxley (SOX) password requirements.

The Strong Passwords feature is disabled, by default.

When the Strong Passwords feature is enabled via the Configuration Assistant, a series of checkboxes are activated, which allow you to choose which password requirement(s) will be enforced when creating or modifying passwords. One or more password requirements can be chosen. You can choose to enforce the requirement(s) that a password:

- Must be a minimum of eight characters, or the **Minimum Password Length** set for the **Local Password** Authentication Service, whichever is greater (this option is checked, by default)
- Must contain at least one alpha character (this option is checked, by default)
- Must contain at least one non-alpha character (0-9, special characters, no restrictions) (this option is checked by default)
- Cannot contain three or more repeated characters in a row (this option is checked by default)
- Cannot contain three or more consecutive, ascending or descending, characters in a row (this option is checked, by default)
- Cannot contain the User Account name or its mirror (reverse character format) (this option is checked, by default)
- Cannot be one of the previous three password most recently used (this option is checked, by default)
- Must contain at least one non-alpha character not in the first or last position. When this option is enabled, for example, “5letmein” and “allowmein2” would be invalid passwords, while “ready2go” and “m4testing” would be valid passwords. (this option is disabled, by default)

The strong password (SOX) requirement(s), when enabled, apply to new or changed passwords for:

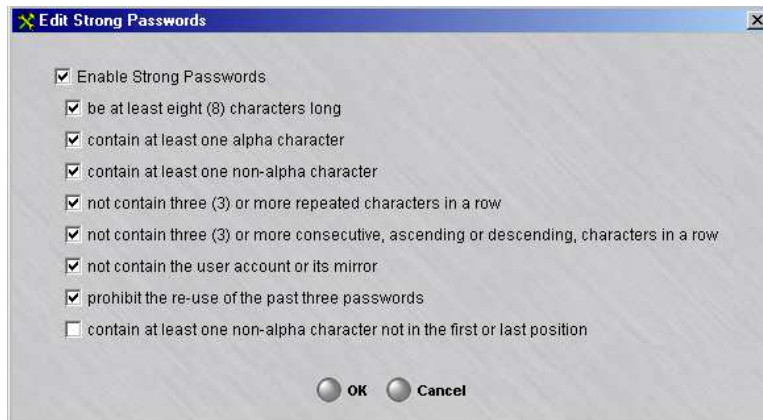
- A clean installation password of the master user
- Local passwords
- User passwords
- Administrator passwords

- User login passwords for the Brick device console
- Admin key (additional key) which is needed when SecurID or RADIUS authentication methods are used

### Edit strong passwords window

Figure 11-17, “Edit Strong Passwords Window” (p. 11-41) shows an example of the Strong Passwords window with the Enable Strong Passwords feature enabled (checkbox is checked).

**Figure 11-17 Edit Strong Passwords Window**



### Enable strong passwords

The **Enable Strong Passwords** feature is disabled, by default (checkbox is unchecked). To enable this feature, click the checkbox to place a check in it. To disable the feature, click the checkbox again to remove the check.

When the Strong Passwords feature is enabled, a series of password restriction options (checkboxes) are activated to allow you to choose which restriction(s) will be applied.

### Strong passwords restrictions

The password restrictions are a series of options (checkboxes) that can be enabled or disabled. To enable a restriction, click the checkbox to place a check in it (if it is not already enabled). To disable a restriction, click the checkbox again to remove the check.

Click **OK** to activate your selections.



## TL1 Alarms

---

### Overview

The TL1 Alarms parameters allow you to enable and configure the Transaction Language 1 alarm reporting interface.

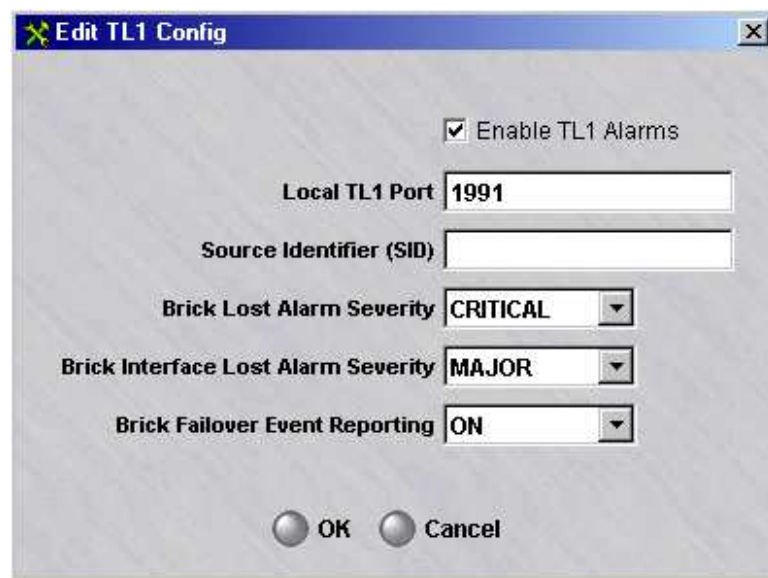
If you modify any of these parameters, you will have to stop and then restart all the SMS services.

To activate this feature, click on the **Enable TL1 Alarms** checkbox on the Configuration Assistant screen (Figure 11-18, “Edit TL1 Alarms Configuration Window” (p. 11-42)).

### Default Values

TL1 Alarms are disabled as the default. Figure 11-18, “Edit TL1 Alarms Configuration Window” (p. 11-42) shows the default values for the *TL1Alarm* parameters when it is enabled.

**Figure 11-18 Edit TL1 Alarms Configuration Window**



### Local TL1 Port

The **Local TL1 Port** field identifies the port on which the TL1 server will be listening to receive TL1 Alarm session requests.

By default, the TL1 Server listens on port 1991. If you wish to change the default value, you should run a networking command, like *netstat -a*, on the SMS computer to ensure the port you are designating is not already in use.

### Source Identifier (SID)

The **Source Identifier** field is used to specify the name of the SMS in TL1 command responses and autonomous messages.

It is recommended that for traditional telecommunications applications, the **Source Identifier** should include the Common Language Location Identifier for the LSMS.

### Brick Lost Alarm Severity

The **Brick Lost Alarm Severity** field specifies the TL1 alarm severity for Brick Lost alarms.

A choice of **CRITICAL**, **MAJOR**, **MINOR**, and **NONE** is given. If **NONE** is chosen, no Brick Lost alarms will be sent. The default value is **CRITICAL**.

### Brick Interface Lost Alarm Severity

The **Brick Interface Lost Alarm Severity** field specifies the TL1 alarm severity for Brick Interface Lost alarms.

A choice of **CRITICAL**, **MAJOR**, **MINOR**, and **NONE** is given. If **NONE** is chosen, no Brick Interface Lost alarms will be sent. The default value is **MAJOR**.

### Brick Failover Event Reporting

The **Brick Failover Event Reporting** field specifies whether Brick Failover events will be reported via the TL1 Alarms interface.

A choice of **ON** and **OFF** is given. The default value is **ON**.



## Tunable Parameters

---

### Overview

The Tunable parameters allow you to adjust certain *maxHeap* parameters in the configuration file (*config.ini*) so that the SMS better handles environments in which there are:

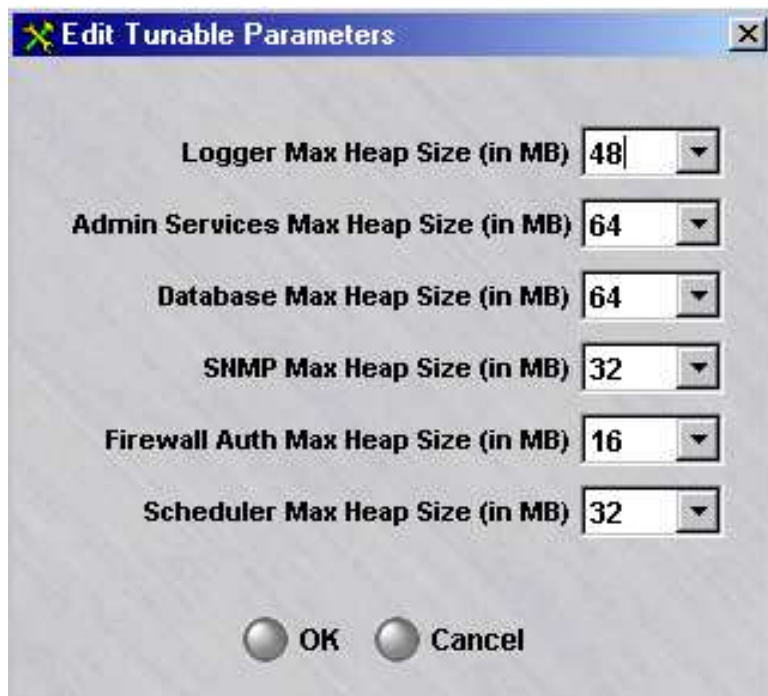
- A large number of Brick devices managed by the SMS,
- A large number of Alcatel-Lucent IPsec Client users enabling client tunnels to Brick devices managed by the SMS, and/or
- A large number of audit records being generated per Brick/per second.

A single SMS can manage up to 1000 Brick devices and handle up to 10,000 client tunnels (a Sunfire V210 with at least 512 MB of RAM or an equivalent platform is required to manage such a load). If your environment approaches these high-end figures, you need to re-set certain *maxHeap* parameters. The following explains.

### Default Values

Figure 11-19, “Edit Tunable Parameters Window” (p. 11-44) shows the default values for the *maxHeap* parameters.

Figure 11-19 Edit Tunable Parameters Window





**Logger Max Heap Size**

The **Logger Max Heap Size** parameter is set by default to 48 Mb. If this SMS will be managing between 200-400 Bricks, set this parameter to 64 Mb. If it will be managing between 400-600 Bricks, set the parameter to 80 Mb. If it will be managing more than 600 Bricks, set the parameter to 96 Mb.

**Admin Services Max Heap Size**

The **Alarms Max Heap Size** parameter is set by default to 32 Mb. If this SMS is managing more than 400 Bricks, set this parameter to 48 Mb. Add 1 MB for every 2,500 IPSec clients to be managed.

**Other Max Heap Size Parameters**

The defaults of the other max heap size parameters should generally not be changed.



## User Authentication

---

### User authentication

User Authentication is used to authenticate remote users whose IP addresses are unknown, allowing them access. The User Authentication parameters allow you to define the protocol (HTTP or HTTPS) and port that will be used by the authentication server.

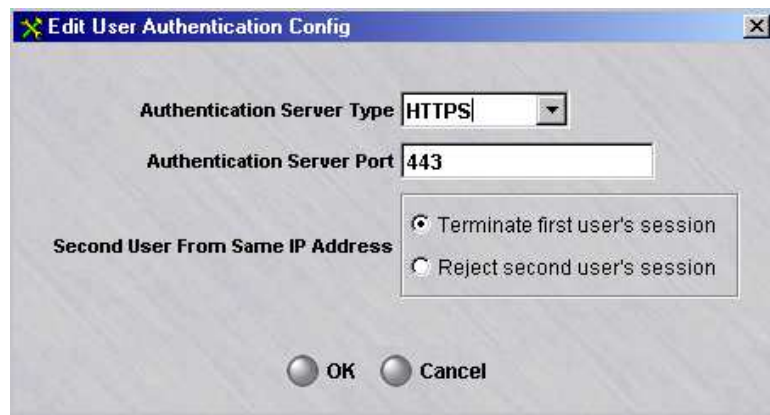
The authentication server is the SMS web server that is used for user authentication. The authentication server is only used for firewall Authentication, not VPN authentication

If you modify any of these parameters, you will have to stop and then restart all the SMS services.

### Default Values

Figure 11-20, “Edit User Authentication Configuration Window” (p. 11-46) shows the default values for the User Authentication parameters.

**Figure 11-20 Edit User Authentication Configuration Window**



### Authentication Server Type

The **Authentication Server Type** field determines whether the connection to the authentication server will be HTTPS (secure) or HTTP (non-secure).

### Authentication Server Port

The **Authentication Server Port** field identifies the port to which the end users connect for application user authentication. (Refer to the *User Authentication* chapter in the *SMS Policy Guide* for additional details.)

If the authentication server is HTTPS (as highly recommended), the port is usually 443.

### Second User From Same IP Address

This set of options defines the action to be taken if a second user tries to authenticate from the same IP address. This could happen, for example, if there is a shared workstation, and user1 is authenticated and then leaves the workstation without ending the authenticated session by logging off. If a second user comes to the workstation and attempts to log in, this option defines what should be done.

There are two options for the action to be taken:

- **Terminate first user's session.** This is the default option. If the second user is successfully authenticated, the first user's session is terminated. The IP address of the workstation is removed from any User Groups to which user1 belongs and is added to any User Groups to which user2 belongs. User Groups are used in Brick Zone Rulesets to allow or deny access to authenticated users for certain resources protected by the Brick device. Also, any active sessions in the Brick cache for user1 are terminated.
- **Reject second user's session.** The second user's login will be rejected, even if they enter the correct password. For security reasons, they are not told why their authentication fails. A message will be logged to the User Auth Log, which is viewable by the SMS Administrator, which indicates that the authentication failed because another user already has an active session from that IP address. If this option is chosen, user1's session remains active until user1 logs out or until the authentication times out, whichever comes first.





# 12 Backing Up and Restoring Data

## Overview

---

### Purpose

This chapter explains how to back up and restore data on both a Primary SMS and a redundant pair of SMSs (Primary and Secondary).

The SMS data that has to be backed up consists of a database and a number of configuration files. The database contains the configuration data that is managed by the SMS, such as devices, policies, VPN tunnels, and certificates. The configuration files are certain “flat” files, such as *config.ini* and *inferno.ini*, which contain information not residing in the database.

### Contents

<a href="#">Automatic Backup</a>	12-2
<a href="#">Manual Backup</a>	12-3
<a href="#">Scheduled Backups</a>	12-6
<a href="#">To Restore SMS Data on a Primary SMS</a>	12-7
<a href="#">To Restore SMS Data on a Secondary SMS</a>	12-9
<a href="#">Restore Scenarios on Redundant SMSs</a>	12-11
<a href="#">Other Restore Scenarios</a>	12-12



## Automatic Backup

---

### Overview

By default, all standalone and primary SMS automatically back up their databases and configuration files each night at 2:00 am. Backups for the last seven days are stored under the directory in which the SMS application was installed, in subdirectories named */db/backups/1-7*. The first backup is stored in subdirectory 1, the second in subdirectory 2, and so forth. After a week's time, directory 1 is overwritten. The subdirectory with the most recent backup can be identified by the timestamp on the directory.

The SMS Login Banner content is backed up during automatic backups, so that any customized login banner display is preserved.

After the nightly backup, a copy of the backup is written to the secondary SMS under *installdir/db/primary\_backups*. It is to be used in the event that there is a failure on the primary SMS and its nightly database backup is not available.

No automatic backup is performed on a secondary SMS because it is not necessary to back up the database on a secondary SMS. Whenever the secondary SMS is upgraded or restored, you must run the *dbsetup* utility on the Secondary SMS, which copies the database from the primary SMS and re-syncs the Secondary SMS database. A manual backup should be performed on the Secondary SMS to back up configuration files after new software is installed or after making changes with the Configuration Assistant.



# Manual Backup

---

## Overview

The automatic backup ensures that the database on each standalone and primary SMS is backed up at least once a day. However, you can also perform manual backups so that your database is backed up more frequently.

This is important, because each administrative change (add, modify or delete) alters all or portions of the configuration data in the database. The ability to restore the database becomes critical if you make a change and later discover that the change has to be reversed — especially if it creates a security violation.

The SMS Login Banner content is backed up during manual backups, so that any customized login banner display is preserved.

Do not back up your files to a directory in *installdir* tree (or to any subdirectory under the installation directory). This is a precaution, so that your backup is not inadvertently lost if you need to uninstall and reinstall the SMS application. You might also consider moving the backup to a tape or another machine.

For the backup to be complete, do not back up the database when the SMS is being used to add, modify, or delete configuration data. Otherwise, the backup will not have integrity. Also, the system is collecting real-time session statistics and should not be taken off-line to perform backups.

If you need to obtain an estimate of the disk space that is required for the backup, look at the */db/LSMS* directory under the installation root directory. This will be the approximate amount of disk space required for the backup.

Even though other configuration data from other directories are included in the backup, they are minor compared to this directory that holds the database.

## To manually back up the SMS database

Even though the SMS services can be running while backing up, the backup process should not be done during a period of system change, such as adding or deleting Brick devices or users. Manual backups should be performed during off-peak hours, when there is a light processing load on the SMS.

Complete the following steps to manually back up the SMS database.

---

- 1 Open a command prompt window.

---

**2** Change directories to the installation directory as follows:

- On *Windows*<sup>®</sup> or *Vista*<sup>™</sup> platform servers, the default installation directory is *c:\users\isms\lmf* if you upgraded from an earlier SMS release (such as R9.1) to R9.4. If it is a clean installation of R9.4, the default installation directory is *c:\isms\lmf*.
  - On *Solaris*<sup>®</sup>, this is */opt/isms/lmf* if you selected the default. You also need root privileges on the *Solaris*<sup>®</sup> hosts.
- 

**3** At the command prompt, enter

```
local/bin/backup <backup_directory>
```

where:

<backup\_directory> is the mountable destination directory used to record the database. This directory will be created for you if it does not already exist. It can be a mapped directory. It can include fully-qualified path names or be relative to the installation root directory.

**Important!** When entering the command on a *Windows*<sup>®</sup> platform, you have to include the letter indicating the disk drive, as in the example below:

```
c:\backups\2000-05-22
```

On a *Solaris*<sup>®</sup> platform, you do not have to include the disk drive letter. The following is an example:

```
../backups/2000-05-22
```

---

**4** During the course of the backup, the following messages will appear on the screen:

- *Primary SMS Backup*

```
# ./local/bin/backup /export/home/tmp/backup_0726
Backing up database...
Backing up non-database files...
Backup is complete and successful #
```

- *Secondary SMS Backup*



```
# ./local/bin/backup /export/home/tmp/sec_backup_0726  
Backing up non-database files only...  
Backup is complete and successful #
```

.....  
E N D O F S T E P S



## Scheduled Backups

---

### **SMS task scheduler**

The SMS Task Scheduler allows you to run a database backup command on a scheduled basis through a separate GUI function. A database backup can be scheduled to be run once, a specific number of times, or periodically at a set time (hourly, daily, weekly, monthly, or yearly).

For details about how to use the Task Scheduler, refer to [Chapter 13, “Task Scheduler”](#)

.



## To Restore SMS Data on a Primary SMS

---

### When to use

Use this procedure to restore SMS data on a Primary SMS.

The restore utility, when run on a Primary SMS, restores certain “flat” configuration files and the Primary SMS database.

Before restoring the Primary SMS database using the restore utility, the SMS services must be stopped.

The restore process should not compete with other processes for CPU and memory resources. It is recommended that the restoral of files should only be performed during off-peak hours.

### Task

Complete the following steps to restore SMS data on a Primary SMS.

---

- 1 Stop the SMS services as follows:
  - On *Windows*® and *Vista*™ platform servers, click the **Start** menu and select **Programs ► Alcatel-Lucent Security Management Server ► Stop Services**
  - On *Solaris*® platform servers, from the installation root directory enter `./stopServices`.

---
- 2 Open a command prompt window.

---
- 3 Change directories to the installation root directory as follows:
  - On *Windows*® or *Vista*™ platform servers, the default installation directory is `c:\users\isms\lmf` if you upgraded from an earlier SMS release (such as R9.1) to R9.4. If it is a clean installation of R9.4, the default installation directory is `c:\isms\lmf`.
  - On *Solaris*® platform servers, this is `/opt/isms/lmf` if you selected the default directory. You also need root privileges on *Solaris*® hosts.

---
- 4 At the command prompt, enter  
`local/bin/restore <backup_directory>`  
where:

<*backup\_directory*> is the source directory where the database was backed up. It can be a mapped directory. It can include fully-qualified path names or be relative to the installation root directory. Examples include:

*D:\backups\2000-05-22*

*../bkup/2000-05-22*

- 5 During the course of the restore, the following message will appear on the screen:

```
# ./local/bin/restore /export/home/tmp/bu_test1
Be sure the SMS Services are not running.
If they are running, STOP THEM NOW.
When they are stopped, hit 'Enter'

Restoring database...
Restoring non-database files...
Removing old publication...This may take a few
minutes...

Database Schema is up-to-date...no changes made...

Creating updated publication...This may take a few minutes...

Done with successful restore
- Please re-start SMS services
- Then run restore on the secondary SMS #
```

- 6 Restart the SMS services as follows:

- On *Windows*<sup>®</sup> and *Vista*<sup>™</sup> platform servers, Click **Start** and select **Programs > Alcatel-Lucent Security Management Server > Start Services**.
- On *Solaris*<sup>®</sup> platform servers, from the installation root directory enter `./startServices`.

END OF STEPS



## To Restore SMS Data on a Secondary SMS

---

### When to use

Use this procedure to restore SMS data on a Secondary SMS.

The restore utility, when run on a Secondary SMS, restores the “flat” configuration files but does *not* automatically restore the Secondary SMS database. After running the restore utility on a Secondary SMS, the dbsetup utility must also be run manually. dbsetup re-syncs the two databases by copying the Primary SMS database to the Secondary SMS.

Before restoring data on a Secondary SMS using the restore and dbsetup utilities, the SMS services must be stopped.

The restore process should not compete with other processes for CPU and memory resources. It is recommended that the restoral of files should only be performed during off-peak hours.

After the dbsetup utility is run on the Secondary SMS, you must restart the SMS services.

For details about the dbsetup utility, refer to the *Database Utilities* chapter in the *SMS Tools and Troubleshooting Guide*.

### Task

Complete the following steps to restore SMS data on a Secondary SMS.

---

- 1 Stop the SMS services as follows:
  - On *Windows*<sup>®</sup> and *Vista*<sup>™</sup> platform servers, click the **Start** menu and select **Programs ► Alcatel-Lucent Security Management Server ► Stop Services**
  - On *Solaris*<sup>®</sup> and Linux platform servers, from the installation root directory enter `./stopServices`.

---
- 2 Open a command prompt window.

---
- 3 Change directories to the installation root directory as follows:
  - On *Windows*<sup>®</sup> or *Vista*<sup>™</sup> platform servers, the default installation directory is `isc:\users\isms\lmf` if you upgraded from an earlier SMS release (such as R9.1) to R9.4. If it is a clean installation of R9.4, the default installation directory is `c:\isms\lmf`.
  - On *Solaris*<sup>®</sup> and Linux platform servers, this is `/opt/isms/lmf` if you selected the default directory. You also need root privileges on *Solaris*<sup>®</sup> and Linux hosts.

---

- 
- 4 At the command prompt, enter

```
local/bin/restore <backup_directory>
```

where:

*<backup\_directory>* is the directory where the configuration files were backed up. It can be a mapped directory. It can include fully-qualified path names or be relative to the installation root directory. Examples include:

```
D:\backups\2000-05-22
```

```
../bkup/2000-05-22
```

---

- 5 After the restore utility completes, run the dbsetup utility.

At the command prompt, enter

```
local/bin/dbsetup
```

---

- 6 Restart the SMS services as follows:

- On *Windows*<sup>®</sup> and *Vista*<sup>™</sup> platform servers, Click **Start** and select **Programs > Alcatel-Lucent Security Management Server > Start Services**.
- On *Solaris*<sup>®</sup> and Linux platform servers, from the installation root directory enter `./startServices`.

END OF STEPS

---



## Restore Scenarios on Redundant SMSs

---

### Overview

There are several possible scenarios that you have to be aware of when performing a restore procedure on a redundant pair of SMSs:

- *Scenario #1:* Restore has been performed on a primary SMS.  
When the services on the primary SMS are restarted, the primary and secondary SMS are not "connected" because their database certificates are not in sync. These are the certificates required to encrypt the transfer of the database between the two machines to ensure their security.  
The restore utility must be run on the Secondary SMS to restore the "flat" configuration files. Then, the dbsetup utility must be run manually to re-sync the two databases. By running dbsetup, the database is copied from the primary SMS to the secondary SMS. It is important to keep in mind that any changes made on the secondary SMS since it lost connection with the primary SMS will be lost once dbsetup is run and copies the Primary SMS database to the Secondary SMS.
- *Scenario #2:* The Primary SMS database has not changed, but a restore is needed on the Secondary SMS.  
Before doing a restore on the Secondary SMS, you must issue the following command from the installation directory on the Primary SMS:  
`local/bin/allowSecondarySetup`  
This command resets the database certificate on the primary SMS to the default and allows the secondary SMS to copy the database from the Primary SMS. Run the restore command on the Secondary SMS to restore the "flat" non-database configuration files and execute the dbsetup command, which copies the database from the Primary SMS to the Secondary SMS.  
Please note that this is the only way to restore the database on the Secondary SMS. *Do not* attempt to restore the backup from the Primary SMS directly onto the Secondary SMS.  
For details about the allowSecondarySetup utility, refer to the *Database Utilities* chapter in the *SMS Tools and Troubleshooting Guide*.
- *Scenario #3:* The user does not need to restore the configuration files on the Secondary SMS, but needs to copy the database from the Primary SMS.  
This situation could arise if the Primary and Secondary SMS have not been connected for more than a week. As in Scenario #2, you have to issue the allowSecondarySetup command on the primary SMS. On the Secondary SMS, you have to stop services and then run  
`local/bin/dbsetup`  
to copy the database from the Primary SMS to the Secondary SMS. After dbsetup is run, you have to restart the SMS services.

□

## Other Restore Scenarios

---

### Overview

The following additional scenarios are also possible:

- *Scenario #4:* The user has recently upgraded their Primary SMS with an SMS patch. After the patch upgrade, the user has discovered a need to restore the database, but only an older version of the database backup is available. The restore utility will automatically upgrade an older version of a database to the current release on the Primary SMS, if needed. After the restore utility completes on the Primary SMS, and services have been restarted, you must resync the Secondary SMS database. On the Secondary SMS, stop services, then run `local/bin/dbsetup` to copy the database from the Primary SMS to the Secondary SMS. After the `dbsetup` utility completes, restart the SMS services.
- *Scenario #5:* The user has decided to move an existing Primary SMS onto a different machine. Prior to restoring the Primary SMS database onto the new machine, the SMS application must already be installed. The SMS installation paths must be the same on both machines. After the restore has been completed, other steps may be necessary before the SMS services can be restarted on the new machine. If the IP address on the new SMS is different than the old SMS, you must run the `changeIP` utility and update the Brick devices. For more information, refer to *Appendix D* in the *SMS Administration Guide*. If the machine name on the new SMS is different than the old SMS, you must run the `changeName` utility. For more information, refer to the *Database Utilities* chapter in the *SMS Tools and Troubleshooting Guide*. If the new SMS is a primary SMS, you must run the `restore` and `dbsetup` utilities on the secondary SMS to synchronize the two environments. See the steps mentioned earlier in Scenario #1.
- *Scenario #6:* The Secondary SMS needs to be reinstalled and is running a patch version of the SMS software. The first step in performing a *clean* install on a Secondary SMS is to uninstall the existing version of the SMS and to delete the `lmf` directory (by default, `\users\isms\lmf` on Windows® or Vista™ if it is an upgrade installation from an earlier release to R9.4, `\isms\lmf` on Windows® or Vista™ if it is a clean installation of R9.4, or `/opt/isms/lmf` on Solaris® and Linux). The user needs to install the *gold* version of the SMS on the Secondary SMS first. The difficulty arises when the database is copied from the Primary SMS. Since the Primary SMS is running the SMS patch version, by definition, its database version will be out of sync with the Secondary SMS. Therefore, the database cannot be copied from the Primary SMS to the Secondary SMS.



As a workaround, the administrator must execute the following steps:

- Install the gold version of the SMS on the Secondary SMS. The Secondary installation key can be found on the Primary SMS using the SMS Navigator. The key is displayed in the SMS/Compute Servers Editor.
- The error for connection refused by the Primary SMS may occur when the Secondary SMS tries to perform a handshake with the Primary SMS. On the Primary SMS, from a DOS or terminal window, cd to the SMS installation directory. Type `local/bin/allowSecondarySetup`. This temporarily resets the database encryption certificate used for communication between the Primary and Secondary databases. You can also right-click the Primary SMS in the LSMSs and LSCSs window in the Navigator Window of the Primary and run the Allow Secondary Setup utility.
- Continue with the installation process even though there will be an error message warning about the Primary and Secondary having different releases.
- When the Secondary *gold* installation process is finished, install the same patch version on the Secondary SMS that is running on the Primary SMS. A message may be displayed, indicating that the Secondary SMS cannot communicate with the Primary SMS and advising you to run the `allowSecondarySetup` utility on the Primary SMS.
- On the Primary SMS, from a DOS or terminal window, cd to the SMS installation directory. Type `/local/bin/allowSecondarySetup`. This temporarily resets the database encryption certificate used for communication between the Primary and Secondary SMS databases. You can also right-click the Primary SMS in the LSMSs and LSCSs window in the Navigator Window of the Primary SMS and run the Allow Secondary Setup utility.
- Restore the Secondary SMS flat files if a backup was performed. On the secondary, stop all SMS services. From a DOS or terminal window, cd to the SMS installation directory. Type `local/bin/restore<backup>` where *<backup>* is the directory in which the Secondary SMS backup was saved.
- Start the SMS services on the Secondary SMS.
- Verify Primary SMS - Secondary SMS communication using the SMS\CS and Bricks status window under the **Monitor > SMS\CS and Bricks** options in the Navigation Window.

□



# 13 Task Scheduler

## Overview

---

### Purpose

This chapter discusses the SMS Task Scheduler.

### Contents

<a href="#">What is the Task Scheduler?</a>	<a href="#">13-2</a>
<a href="#">Schedule Editor</a>	<a href="#">13-3</a>



## What is the Task Scheduler?

---

### Definition

The SMS Task Scheduler allows you to run commands (perform tasks), such as database backups or log transfers, at scheduled times via a GUI window. A command (task) can be scheduled to run once, a specific number of times, or periodically at a set time (hourly, daily, weekly, monthly, or yearly).

The SMS Task Scheduler is installed with just one task scheduled (backing up the SMS database), but you can schedule other commands (tasks) such as FTP transfer of log files.

For additional details about scheduling FTP transfer of log files, refer to the *Transferring Log Files via FTP* appendix in the *SMS Reports, Alarms, and Logs Guide*.



# Schedule Editor

---

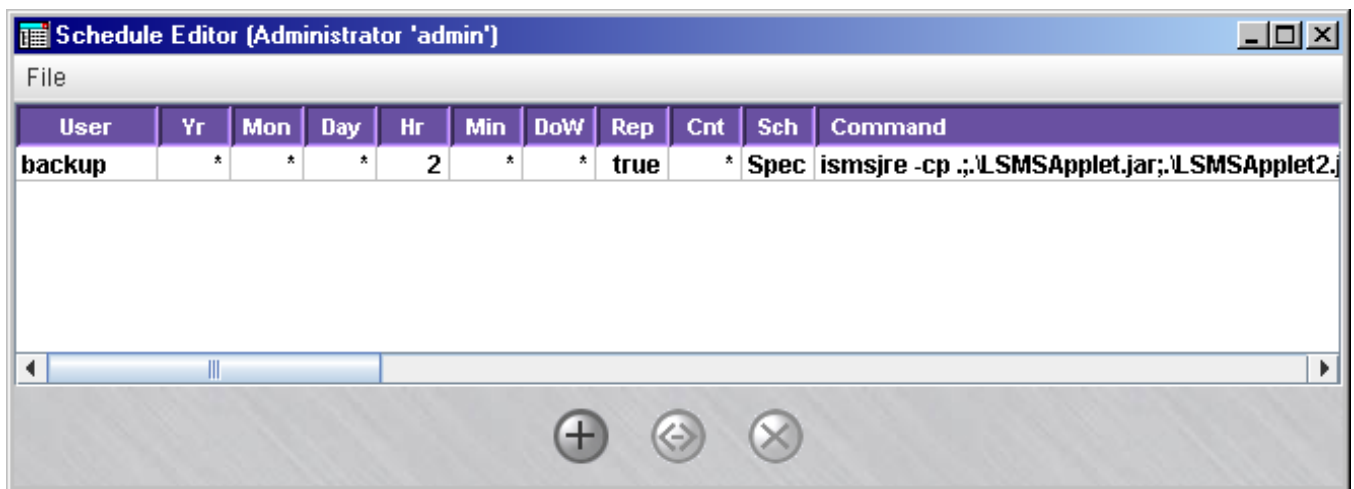
## Overview

The Schedule Editor, which is the editing window accessible through this tool, allows you to modify the actions of the Task Scheduler without disrupting the system by stopping and restarting SMS services. It also provides a less error-prone method of modifying the scheduler configuration files than editing them manually using a text editor.

## Schedule Editor Window

Figure 13-1, “Schedule Editor Window (Initial View)” (p. 13-3) shows a sample of the Schedule Editor window..

**Figure 13-1 Schedule Editor Window (Initial View)**



Each tabular row in the window displays a task and the details about when it is scheduled to be performed, as follows:

- **User** - identifies the user account who scheduled the command.
- The **Yr** (year), **Mon** (month), **Day**, **Hr** (hour), **Min** (minute) and **DoW** (day of the week) fields provide the scheduling particulars of the task.
- The **Rep** (repeat) and **Cnt** (count) fields specify how many times the command is to be executed. If the Rep entry is true, then the command is run repeatedly the number of times shown in the **Cnt** field. A non-numeric or entry of **0** in the **Cnt** field indicates that the command will be run indefinitely.
- The **Sch** field indicates whether the time fields indicate a specific date/time (**Spec**) for the command to be run or a time interval (**Freq**) between execution of the command, if it has been scheduled to be performed repeatedly.

## Scheduling a Command

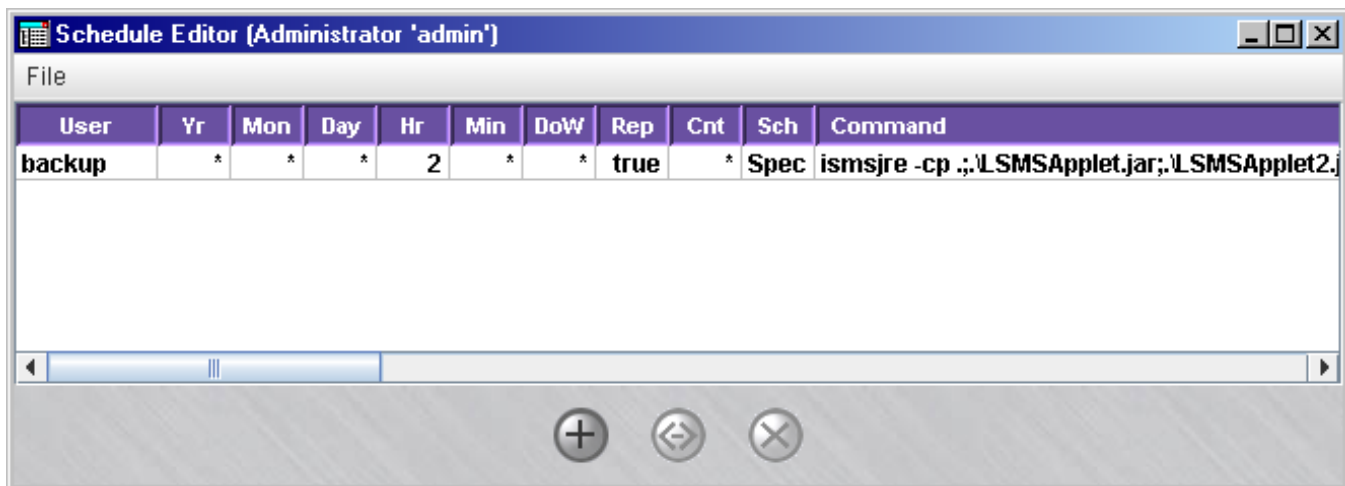
- 1 To schedule a command (task), follow the steps below. If the remote host is running *Windows*® or *Vista*™, click the **Start** menu and select:


**Programs > Alcatel-Lucent Security Management Server > Utilities > SMS  
Schedule Editor**

A login window is displayed to enter your SMS Admin ID and password.

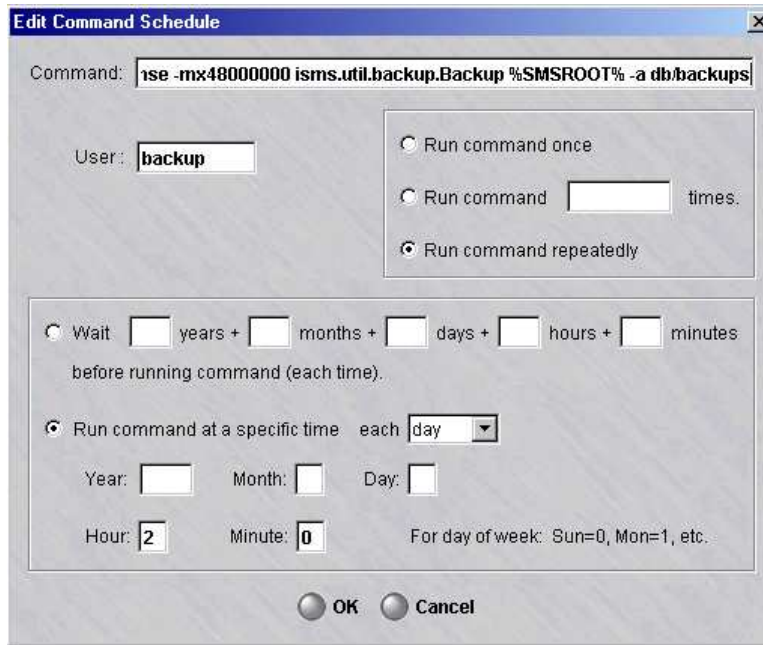
The SMS Schedule Editor window is displayed, with the backup task pre-selected in the task list, which is pre-set when the SMS software is installed ([Figure 13-2, “Schedule Editor Window \(Initial View\)”](#) (p. 13-4) shows a sample window).

**Figure 13-2 Schedule Editor Window (Initial View)**



- 2 To schedule a backup, or any other command to be run, click the Edit (  ) button, or just double-click on the backup task in the task list.

The Edit Command Schedule window is displayed ([Figure 13-3, “Edit Command Schedule Window”](#) (p. 13-5) shows a sample window).

**Figure 13-3 Edit Command Schedule Window**

If you want to still execute the scheduled database backup (command), and add another command as a new scheduled task, click the New (+) button on the Scheduler Window.

The New Command Schedule window is displayed (Figure 13-4, “New Command Schedule” (p. 13-6)).

Figure 13-4 New Command Schedule

- 3 To schedule the backup (or another command) to run, edit the fields as follows:
- **Command** - this field is pre-set with the command to run an SMS database backup. If you want to schedule a backup, leave the contents of this field as is. To schedule a different command, enter the complete command line of the task to be scheduled to run.
  - **User** - Enter the user login who is scheduling the command/task.
  - **Run command once** - click this radio button to run the command only once at the scheduled time interval.
  - **Run command n times** - click this radio button and specify the number of times to run the command at the scheduled time interval.



- **Run command repeatedly** - click this radio button to run the command repeatedly at the scheduled time interval.  
If the option is selected to run the command repeatedly, specify the waiting time (number of years, months, days, hours, minutes) between each command run.
  - **Run command at specific time** - If the command is being run only once, specify the exact time to run the command (year in yyyy format; month in mm format; day, 0=Sunday, 1=Monday, and so forth; hour, in hh format, minutes, in mm format)
- 

**4** After making your schedule settings, click the **OK** button.

The Schedule Editor window is displayed, showing the newly scheduled command on the tasklist. The command/task will be scheduled to run at the selected frequency or time interval.

**Important!** Whenever the Schedule Editor is used to schedule a new task or modify an existing one, you must restart the SMS services to make the change effective.

END OF STEPS

---





# 14 Using the Status Monitor

## Overview

---

### Purpose

This chapter explains how to use the SMS Status Monitor. The Status Monitor provides a mechanism for monitoring the status of all Alcatel-Lucent *VPN Firewall Brick*<sup>™</sup> Security Appliances, VPN tunnels, and SMSs at varying levels of summary and detail. In addition, it shows all SMS and Group Administrators currently logged into the SMS you are logged into, and it displays all console alarm messages.

Administrators can use the Status Monitor to:

- Monitor the current health of all SMS-related network components to ensure that they are operating smoothly
- Track and analyze long range traffic patterns through all installed Bricks and tunnels
- Compare different time periods' worth of network activity and analyze the differences.

### Contents

<a href="#">To Access the Status Monitor</a>	14-2
<a href="#">How to Interpret the Status Monitor</a>	14-3
<a href="#">Status Overview Window</a>	14-6
<a href="#">Administrators Window</a>	14-14
<a href="#">SMS/CS and Bricks Status Window</a>	14-16
<a href="#">Brick Status Windows</a>	14-19
<a href="#">Console Alarms Window</a>	14-35



## To Access the Status Monitor

---

### Methods of access

You can access the Status Monitor using either the SMS Navigator or the SMS Remote Navigator.

### Display the Status Monitor

There are two ways to display the Status Monitor:

- *Status Monitor Only*  
This method allows you to log into the Status Monitor without also logging into the SMS. To display the Status Monitor without opening the SMS, click the **Status Monitor Only Login** checkbox on the Login window when logging into the SMS. (The Status Overview window is displayed instead of the SMS Navigator window.) This method is *not* recommended for SMS or Group Administrators. It is intended primarily for use in network operations centers, or to enable an individual to view network status without having the ability to view or change any of the configuration parameters.
- *Status Monitor and SMS*  
To display the Status Monitor from the SMS, log into the SMS without clicking the **Status Monitor Only Login** checkbox. Then, open the **Monitor** menu on any SMS window and select the Status Monitor component that you want.

### Status Monitor Components

The Monitor menu has four options on it, each of which corresponds to one of the components of the Status Monitor. The Status Monitor consists of these components:

- Status Overview window
- Administrators window
- LSMS/LSCS and Bricks window
- Brick Status window
- Console Alarms window.

An administrator can keep more than one Status Monitor window open at the same time. For example, you could keep the Status Overview window open to provide a high-level view of network operations, and at the same time keep open windows displaying individual Brick status, as well as a window listing the Bricks that are lost.



# How to Interpret the Status Monitor

---

## Overview

The Status Monitor provides a variety of data in both tabular and graphical form.

## Status Monitor Data

The bulk of the data displayed in all Status Monitor windows except the Console Alarms window is gathered from the Proactive Monitoring Log. This log contains information about Brick events, logger events, and Firewall Authentication Controller (FAC) events. (For a more detailed explanation of the Proactive Monitoring Log, refer to the *Audit Logs* chapter in the *SMS Reports, Alarms and Logs Guide*.)

By default, the SMS automatically refreshes the Status Monitor windows every 30 seconds to ensure the data displayed is current. However, you can change the refresh interval according to your requirements. This is done from the window's toolbar (see "[Toolbar](#)" (p. 14-4)" on "[Toolbar](#)" (p. 14-4) for an explanation of how to change the refresh interval.)

If you cannot wait until the next system refresh, you can perform a manual refresh at any time. You can also turn off the system refresh feature, so that the Status Monitor only refreshes itself when you perform a manual refresh. This is also done from the toolbar.

**Important!** Every 30 seconds, a new batch of data is taken from the Proactive Monitoring Log and held by the SMS. The last 30 seconds worth of data that was collected is the data that is sent to the Status Monitor when a refresh (either system or manual) is performed.

Each SMS/CS between the administrator and the data source (the Brick in particular) does this caching, possibly causing up to two minutes of delaying in collecting the data.

Hence, when a refresh is performed, it is not the last 30 seconds worth of "real-time" data that is displayed, but the last 30 second interval that was cached by the SMS.

## Brick States

The Status Monitor indicates the current status of a Brick device by giving the current state of the Brick device. The state of a Brick device depends on the condition of the Brick device itself, as well as the condition of the standby Brick device, if the Brick device has been configured as part of a failover pair.

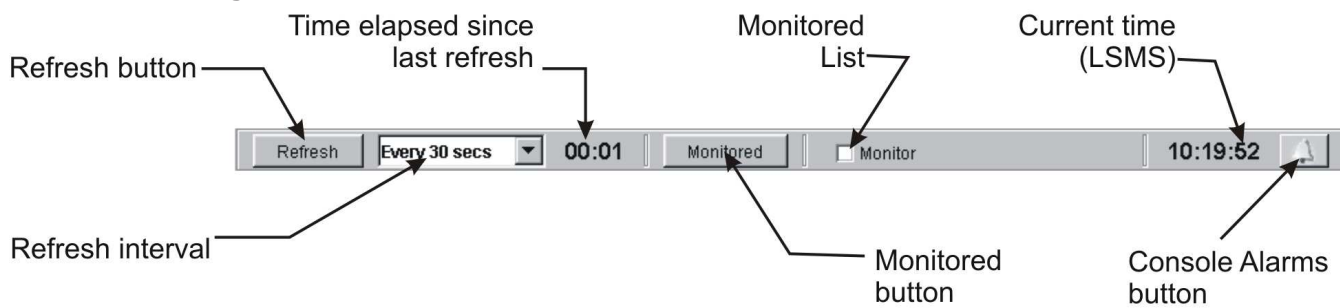
If the Brick device is *not* part of a redundant pair, it can be in one of two states : *Up* (the Brick device is healthy) or *Lost* (the Brick device is down). If the Brick device *is* part of a redundant pair, it can be in one of four states. The table below describes these states.

State	Active	Standby	Explanation
Up-Up	Up	Up	Both Brick devices are up, equivalently healthy, and communicating with each other
Up-Lost	Up	Lost	The active Brick device is up and the standby has either not transitioned into ready mode yet or is down.
Up-Unhealthy	Up	Unhealthy	Both Brick devices are up, but the active or standby Brick device is reporting suboptimal health.
Up-X-wired	UP	X-wired	Both Brick devices are up, but the standby is cross-wired

### Toolbar

Every Status Monitor window except the Console Alarms window has a toolbar across the top, directly below the menubar. [Figure 14-1, “Status Window Toolbar” \(p. 14-4\)](#) below shows the toolbar with each component labeled.

**Figure 14-1 Status Window Toolbar**



The following table explains how to use the components of the toolbar:

Component	What it does
Refresh button	Manually refreshes the data in the Status Monitor window.

Component	What it does
Refresh interval	<p>Determines the amount of time between system refreshes. The alternatives are:</p> <ul style="list-style-type: none"> <li>• Manual only</li> <li>• Every 30 second (default)</li> <li>• Every 1 minute</li> <li>• Every 2 minutes</li> <li>• Every 5 minutes</li> <li>• Every 10 minutes</li> <li>• Every 15 minutes</li> <li>• Every 30 minutes</li> </ul>
Time elapsed since last refresh	<p>Displays the amount of time in minutes and seconds since the last refresh (either system or manual). The counter returns to 00:00 after each refresh.</p>
Monitored button	<p>Displays the list of monitored Brick.</p> <p>The Bricks in the Monitored Bricks List are those that you chose to include. You can use this list to monitor any Bricks that you want to keep an eye on. See <a href="#">“Brick Lists” (p. 14-19)</a> on <a href="#">“Brick Lists” (p. 14-19)</a> for additional details.</p>
Monitored list checkbox	<p>This checkbox only appears on Brick Status windows.</p> <p>To add a Brick device to the Monitored Bricks List, select the Brick in any Brick Status window and click this checkbox. To remove a Brick device from the list, select the Brick device and uncheck the checkbox.</p> <p>If you are not sure if a particular Brick device has been added to the list, select the Brick device in any Brick Status window and see if this checkbox is checked.</p>
Current time	<p>Displays the current time, according to the SMS clock. This time will most likely differ from your own PC time.</p>
Console Alarms button	<p>Opens the Console Alarms window.</p> <p>The bell becomes yellow when a new alarm has been recorded.</p>



## Status Overview Window

---

### Overview

The Status Overview window displays summary information for all Brick devices, SMS(s), and Compute Servers that you have permission to view.

If you are an SMS Administrator, you will see all Brick devices in all groups. If you are a Group Administrator, you will only see Brick devices in groups over which you have permission, and you must have at least *Device/View* permission (see [“To Assign Groups and Privileges”](#) (p. 8-17) for an explanation of administrative permissions).

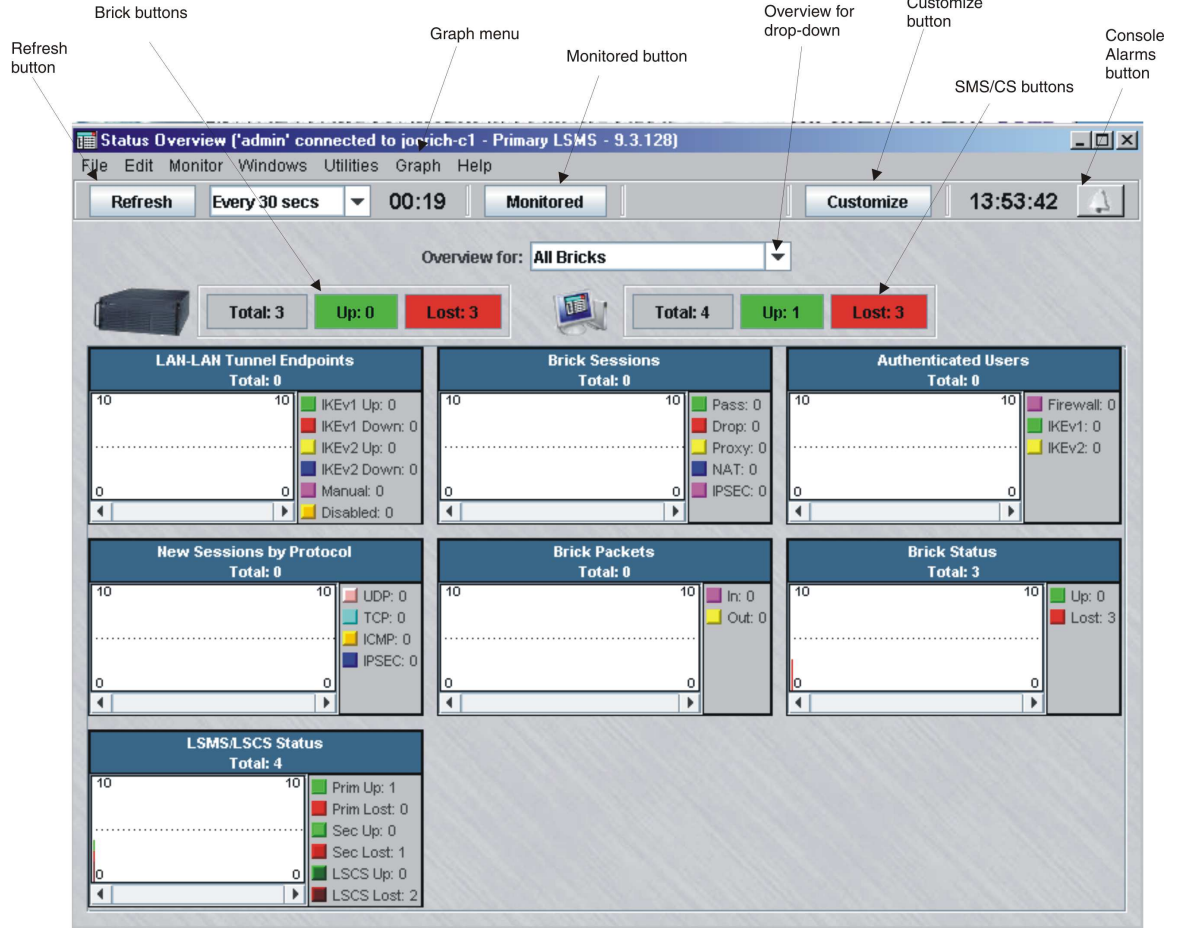
### Window Components

To display the Status Overview window, open the Monitor menu and select **Status Overview**. (If you clicked the **Status Monitor Only Login** checkbox when logging in, this is the first window that appears.)

[Figure 14-2, “Status Overview Window”](#) (p. 14-7) shows a typical Status Overview window, with its major components labeled.



Figure 14-2 Status Overview Window



## Brick Buttons

The first set of buttons that appear at the top of the Status Overview window allow you to access status information about Brick devices by each of the following categories:

- Total (gray button)
- Up (green button)
- Lost (red button)

The number on each button corresponds to the number of Brick devices currently configured in all groups in that category (such as total, up, or lost). When you click one of the three buttons, a Brick Status window (also known as a "Brick List") appears with the appropriate Bricks listed in the window (refer to the "[Brick Status Windows](#)" (p. 14-19)" section for a more detailed description of Brick Status windows and Brick Lists).

## SMS/CS buttons

The second set of buttons that appear at the top of the Status Overview window allow you to access status information about the configured SMS(s) and CS(s) by each of the following categories:

- Total (grey button)
- Up (green button)
- Lost (red button)

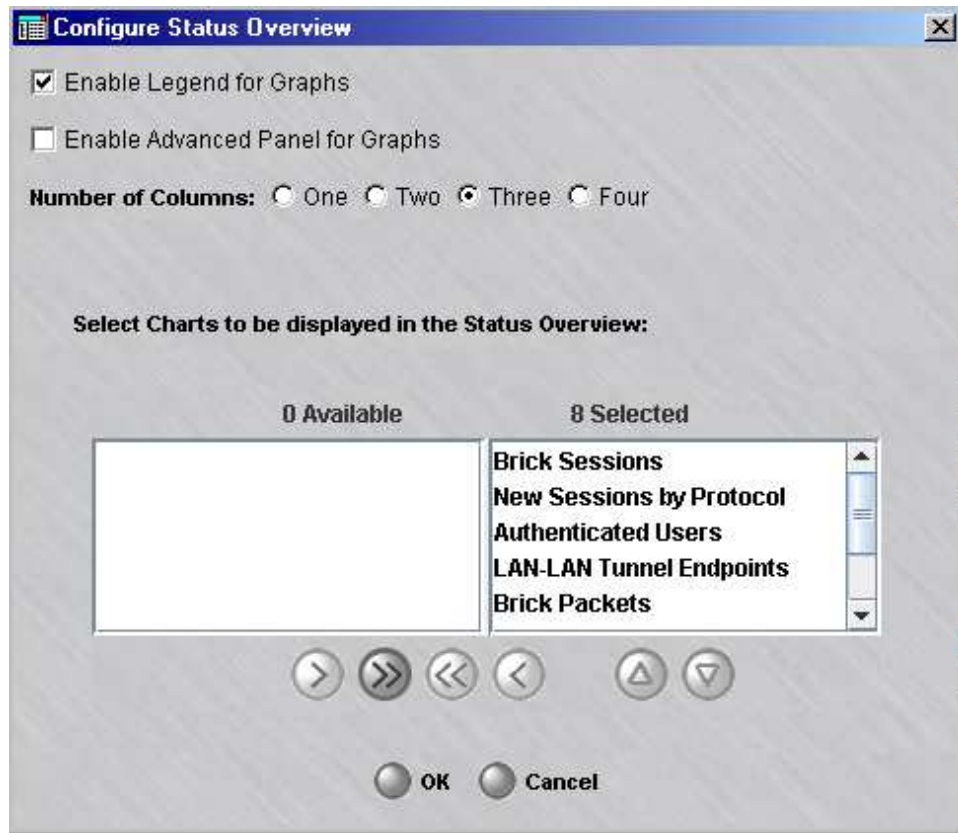
The number on each button corresponds to the number of SMS(s) and CS(s) in that category (such as total, up, or lost). When you click one of the three buttons, the SMS/CS and Bricks status window is displayed with additional details about the SMS(s) and CS(s) in that operational status category (refer to the [“SMS/CS and Bricks Status Window”](#) (p. 14-16) for more information about this status window).

## Customize layout of Status Overview window

The layout of the Status Overview window can be customized to suit your needs, including selection of the number of graphs and columns to display and the showing or hiding of graph legends.

Clicking the **Customize** button on the Status Overview toolbar brings up the Configure Status Overview window ([Figure 14-3, “Configure Status Overview Window”](#) (p. 14-9)).

Figure 14-3 Configure Status Overview Window



This window allows you to select which graphs of the Status Overview to display, by moving the selected graph(s) from the Selected column (the graphs that are displayed) to the Available column (the graphs that are suppressed) using the arrow keys. You can select more than one graph at a time in the column by clicking the Ctrl key and left mouse keys simultaneously.

You can also select the number of columns in the Status Overview display, as well as choosing whether to show or hide the graph legends and the advanced panel tabs of each graph (the date and time display captions).

After the customized selection(s) made, click the **OK** button. The layout change(s) made to the Status Overview is applied across every administrative login and SMS, and the latest layout of the Status Overview is shown each time an administrator logs into the SMS.

The Status Overview is automatically adjusted if the number of graphs selected for display is less than the number of columns selected in the view.

## Overview For Drop-Down

The **Overview For** drop-down list lets you select the Bricks you want displayed in the Status Overview window. The default is **All Bricks**.

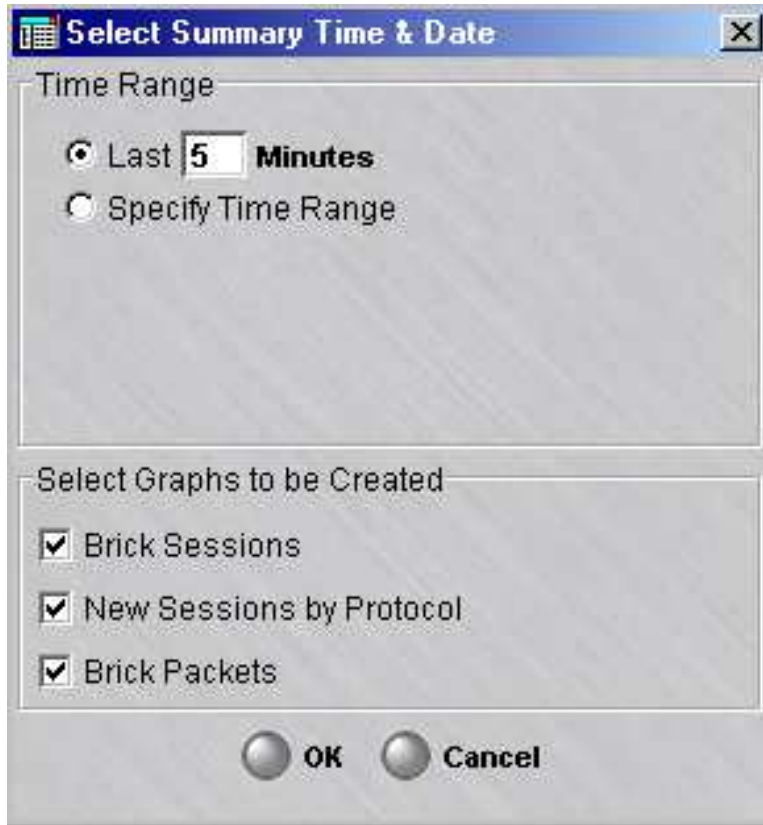
You can change the default by selecting **Browse** from the drop-down list, and then selecting another Bricks folder. Once you select a folder this way, it will be permanently added to the drop-down list, so that in the future you will be able to access this folder directly from the list, without having to browse. In addition, all the data in the graphs will be re-drawn.

## SMS and CS status graph

The Status Overview allows you to access summary data on the operational status of each SMS and CS in a single graph, indicating the number of Primary SMSs, Secondary SMSs (if installed and configured), and Compute Servers (CSs) (if installed and configured) that are up, down, or lost.


To access the SMS and CS summary graph, choose **Summarize...** from the Graph menu on the Status Overview menu bar.

The Select Summary Time & Date window is displayed for you to choose the date and time range for the summary ([Figure 14-4, “Select Summary Time & Date window” \(p. 14-11\)](#)).

**Figure 14-4 Select Summary Time & Date window**

After making your choice(s), click the **OK** button.

The SMS/CS summary status graph is displayed.


The total for each SMS category is the total for the last datapoint displayed in the graph. A legend appears to the right of each graph that explains the color coding on the graph. Click the Legend button (  ) that appears below the graph to hide the legend.

A graph depicting the Brick statistics for each selection made for the specified time period is displayed..

### Brick graphs

The Status Overview window allows you to access seven Brick device graphs that provide different views of network activity.

To access each of the Brick graphs, select **Graph** from the Status Overview menu bar and choose the Brick graph to be displayed ( [Table 14-1, “Brick Graphs from Status Overview Window”](#) (p. 14-12) describes each Brick graph).

The title of each graph is shown in a grey bar across the top of the graph, along with the total for that graph. The total is the total for the last datapoint displayed in the graph. A legend appears at the bottom of each graph, which explains the color coding used on the graph. Click the Legend button (  ) below the graph to hide the legend if you wish.

The graphs are stacked bar graphs in that the values for each point at a given time are stacked on top of one another. The graph region contains the graphic representation of all of the data points in the history of this graph.

If the data point is the first data point in the history, its width will be all the remaining visible space to the left of the graph. As a new data point is received, it is added at the right of the graph, pushing the oldest point (on the left of the graph) out of the viewable area.



You can modify the width of the bars and the spacing between the bars by right-clicking on a graph and selecting an option from the pop-up menu. The width of the bars has no meaning other than cosmetic.

The table below describes what each graph shows. The Brick Status graph shows all Bricks managed by your SMS, regardless of whether the SMS is a Primary SMS, Secondary SMS, or Compute Server.

**Table 14-1 Brick Graphs from Status Overview Window**

Graph	What it shows
Brick Status	Shows the number of up and lost Bricks
Authenticated Users	Shows the number of firewall and Client VPNs (IKEv1 and IKEv2)
LAN-LAN Tunnels	Shows the number of IKEv1 tunnels Up/Down, IKEv2 tunnels Up/Down, Manual key tunnels, and Disabled tunnels. <i>Note: the Disabled counter is a count of disabled LAN-LAN IKE tunnels. The Brick has no knowledge of disabled manual tunnels, therefore they are not included in this count.</i>
Brick Sessions	Shows all sessions that were passed, dropped, proxied, NATed and IPsec (tunneled)
New Sessions by Protocol	Shows all new sessions through the Brick devices
Brick Packets	Shows the number of packets passing through the Brick devices within the last reporting interval

Each graph has two buttons to the right of the date:

- The **Legend** button  on the left acts as a toggle. Click it once to remove the legend from a graph so there is a larger graph area to view. Click it again to return the legend.
- The **Print** button  on the right allows you to print the graph. You must have a printer defined for the print operation to work.

In addition, you can right-click on any graph to display a menu that allows you to customize the graph. You can select more than one data point by holding down the [Shift] key and selecting each point with the mouse cursor. The table below explains each option on the menu.

Option	What it does
Display Selected Point Details	Launches a separate window that shows the current date, time and details for the data point on the graph that you selected
Clear Selected Points	Removes the data point you selected from the graph.
Clear All Points	Removes all data points from the graph
Space Between Bars	Inserts spaces between the bars in the graph. This option, and the option below, allow you to view the graph with spaces and without.
No Space Between Bars	Removes spaces between the bars in the graph
Thin Bars	Makes the bars thinner than the default size
Standard Bars	The default size of the bars in all graphs
Wide Bars	Makes the bars thicker than the default size



# Administrators Window

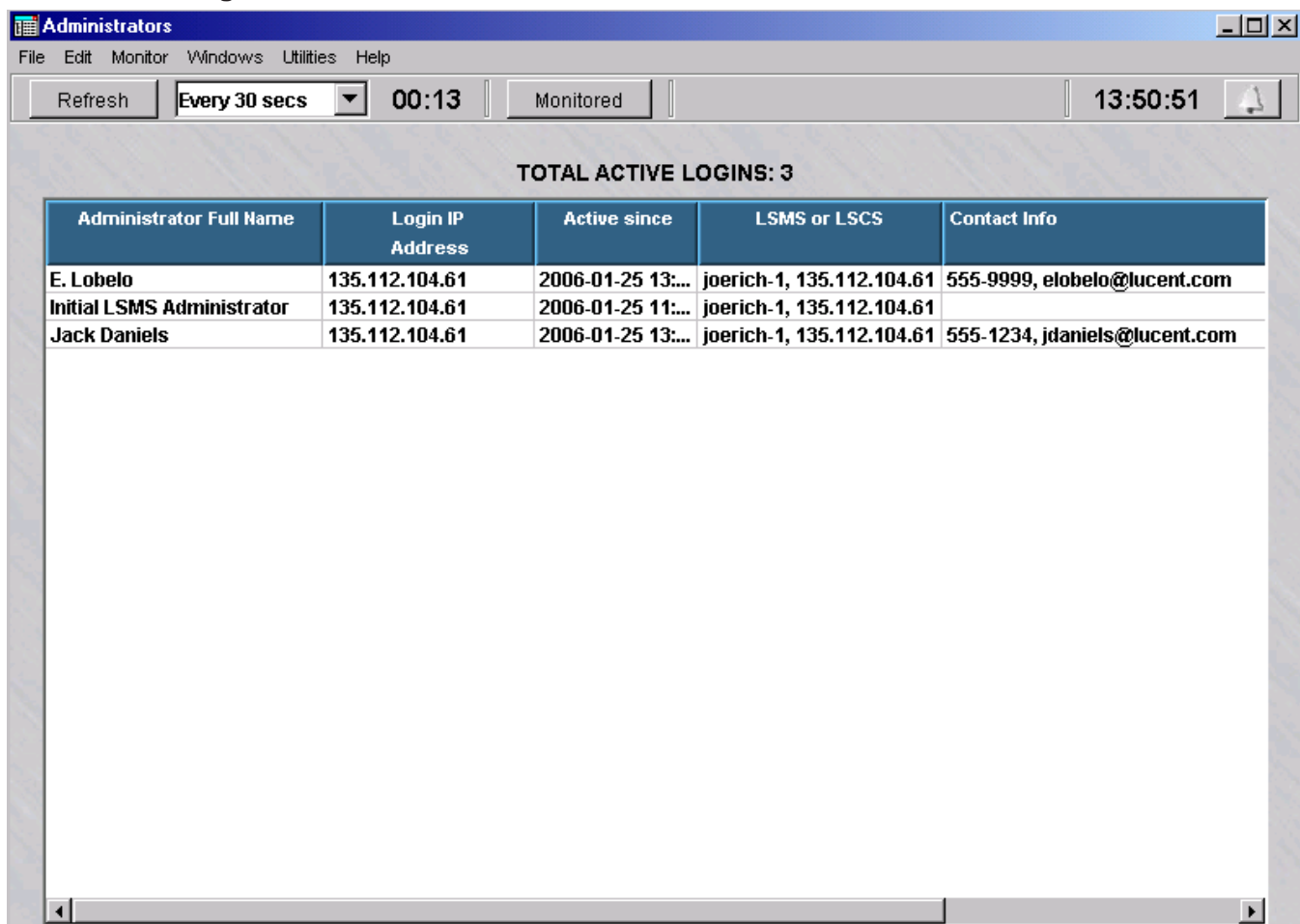
## Overview

The Administrators window provides status information about each administrator who is currently logged in.

## Window Components

To display the Administrators status window, open the **Monitor** Menu and select **Administrators**. Figure 14-5, “Administrators Status Window” (p. 14-14) shows a sample of the Administrators status window.

**Figure 14-5 Administrators Status Window**



The Administrators status window displays the status of all administrators currently logged into the SMS you are logged into. This includes both SMS and Group Administrators.



The total number of administrators currently logged in is given at the top of the table. For each administrator logged in, the Administrator table provides the following information:

<b>Field</b>	<b>Description</b>
Administrator	The full name of the administrator that was entered in the <b>Full Name</b> field when the administrator account was created
Login IP Address	The IP address of the administrator
Active Since	The date and time the administrator logged in
SMS	The name and IP address of the SMS this administrator is logged into
Contact Info	The telephone number and email address of the administrator, if this information was entered when the administrator account was created



## SMS/CS and Bricks Status Window

---

### Overview

The SMS/CS and Bricks status window displays the status of the Primary SMS into which you are currently logged, any associated Compute Servers (CSs ) (if installed and configured), and any Secondary SMS(s) (if installed and configured). Details about each SMS or CS are presented on a separate line on the screen.

### Access to associated Bricks status

Optionally, you can click the **Display Bricks** checkbox to display a list of Brick devices that are homed to each SMS or Compute Server in the SMS cluster. If the **Display Bricks** option is chosen, and the list of Brick devices associated with each SMS or Compute Server is displayed, you can double-click on a specific Brick device in the list, which brings up a Single Brick Status window with additional details about the traffic and tunnel activity of the selected Brick device. Refer to [“Single Brick Status Window”](#) (p. 14-24) for additional information about the Single Brick Status window.

### Figure: sample SMS/CS and Bricks status window

Figure 14-6, [“SMS/CS and Bricks Status Window \(with Display Bricks option selected\)”](#) (p. 14-17) shows a sample of the SMS/CS and Bricks Status window with the **Display Bricks** option selected, showing a hierarchical view of the SMS, supported Brick devices, and associated Compute Servers in a typical SMS cluster.

**Figure 14-6 SMS/CS and Bricks Status Window (with Display Bricks option selected)**

LSMS/LSCS or Brick Name	Type	IP Address	Status	Version	Associated With	Bricks Assigned	Assigned Homed	Not Assigned Homed
joerich-c1	Primary	135.222.146....	Up	9.4.157		4	0	0
hq_brick	Brick	135.222.146....	Lost	9.4.146	joerich-c1			
regional_...	Brick	111.111.111....	Lost	9.4.146	joerich-c1			
remote_...	Brick		Lost	9.4.146	joerich-c1			
branch_b...	Brick	135.222.146....	Lost	9.4.146	joerich-c1			
cs-log	Compute Server	135.222.142....	Lost		joerich-c1	0	0	0
joerich-c2	Secondary	135.222.142....	Lost			0	0	0
cs-admin	Compute Server	135.222.142....	Lost		joerich-c2	0	0	0

**Explanation of fields**

The total number of SMSs and LSCSs, and the number currently up and lost, is given at the top of the table. For each SMS or LSCS, the Administrator table provides the following information:

Field	Description
SMS	The name of the SMS or Compute Server
Type	The type of monitored device. Possible values are <b>Primary</b> (Primary SMS), <b>Secondary</b> (Secondary SMS), <b>Compute Server</b> , or <b>Brick</b> (only displayed if the <b>Display Bricks</b> option is chosen).
IP Address	The IP address of the device.

Field	Description
Status	Up or lost
Version	The product version of the SMS or monitored device
Associated with	For a monitored CS, the name of the associated SMS. For a monitored Brick device, the name of its priority 1 SMS.
Bricks Assigned	The number of Bricks assigned to the SMS or CS.
Assigned Homed	The number of Bricks for which this SMS or CS is <i>priority 1</i> that are currently homed to this SMS. This field is blank if the status of the SMS or CS is lost.
Not Assigned Homed	The number of Brick devices for which this SMS or CS is <i>priority 2</i> that are currently homed to this SMS or CS. This field is blank if the status of the SMS or CS is lost. If you have a standalone SMS, this field is always <b>0</b> .



## Brick Status Windows

---

### Overview

The Status Monitor provides ten distinct Brick Status windows. Seven of these windows are Brick Lists, which show different groupings of Bricks (such as all Bricks, only Bricks with a current status of *up*, or only Bricks in a certain folder), and information about each Brick in the list. The other three Brick Status windows are a Single Brick Status window, a Single Brick Ports window, and a single Brick Bandwidth Statistics window.

### Brick Lists

To display a Brick List, open the Monitor menu, select **Brick Status**, and then select the list you want from the submenu. The table below indicates the Brick Lists that are provided and briefly describes each one:

Brick List	Description
All Bricks Assigned to	Lists all Bricks that are assigned to a specific administrator
All Bricks	Lists all Brick devices over which you have device/view privileges, regardless of their current status
Monitored Bricks	Lists the specific Brick device you have added to the Monitored Bricks list
Lost Bricks	Lists all Brick devices with a current status of <i>lost</i>
Not Up Bricks	Lists all Brick devices with a current status of <i>lost</i> or <i>unhealthy</i>
Up Bricks	Lists all Brick devices with a current status of <i>up</i>
Bricks by Parent Folder	Lists all Brick devices in the folder you select
Single Brick Status	Displays traffic and tunnel statistics for a selected Brick device
Single Brick Ports	Displays data performance statistics for all configured ports of a selected Brick device
Single Brick Bandwidth Statistics	Displays statistics about data packet traffic for the selected Brick device  <i>Note: The Enable Port Bandwidth Parameters checkbox must be checked on the Brick Ports Editor for one or more of the Brick ports to display this status information.</i>

The Brick devices that are included in all of the Brick Lists except the Monitored Bricks List are determined by the current state of the Brick or parent folder. The Brick devices in the Monitored Bricks List, however, are manually selected by the administrator. This is a convenience for administrators, who frequently find it useful to have a special list of Brick devices that they want, for any of a number of reasons, to keep an eye on.

To create the list, select a Brick device in any window that has the toolbar and click the **Monitored** checkbox in the toolbar. Repeat until all the Brick devices you want are in the list.

To display the Monitored Bricks List, click the **Monitored** button in the toolbar of any Status Monitor window. To delete a Brick device from the list, select the Brick device and uncheck the **Monitored** checkbox.

You can also highlight a Brick device in the list, right-click the Brick device and select one of the following two options:

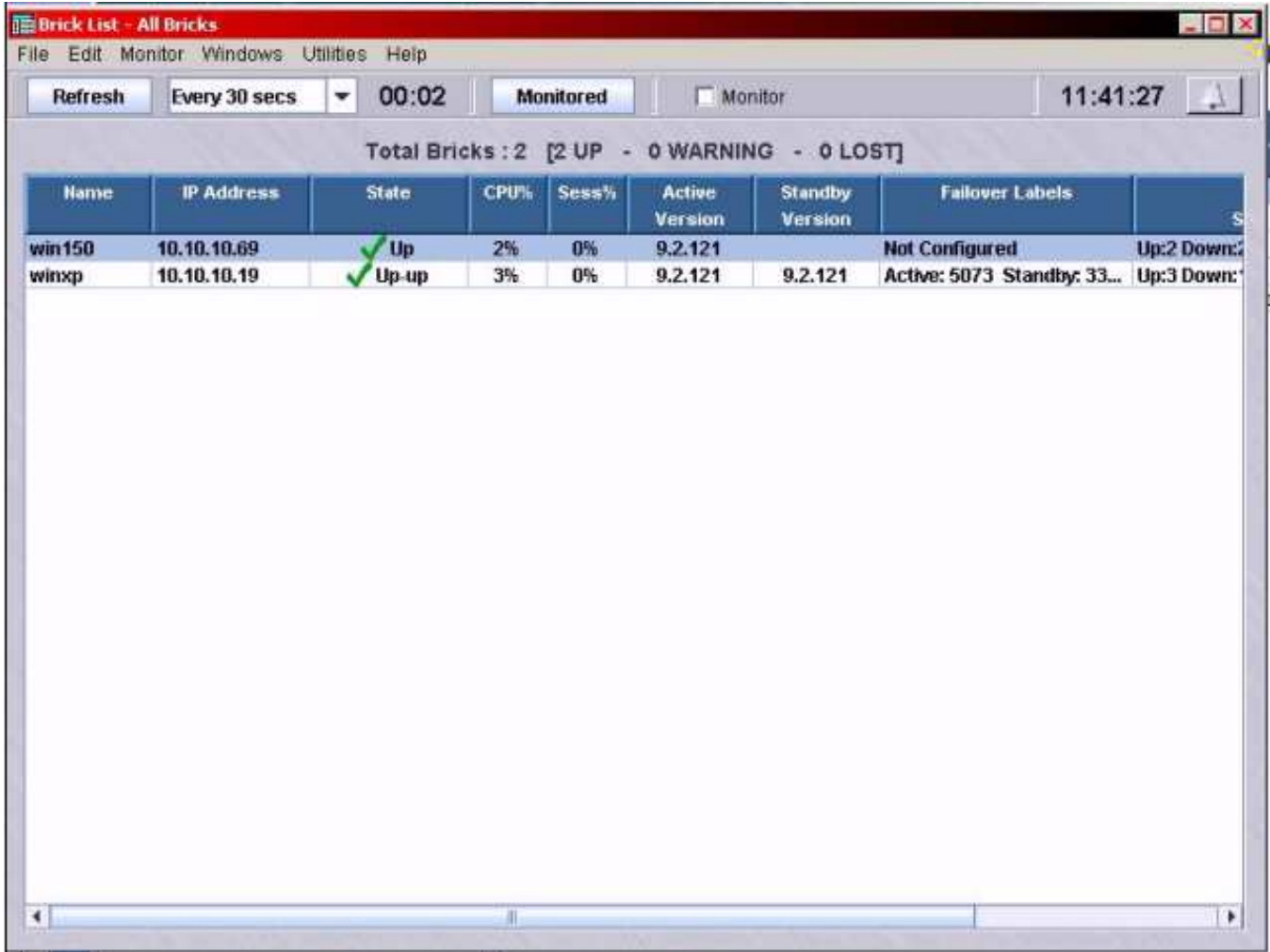
- Open Single Brick Window
- Open Single Brick Ports Window

These options display the same data that is displayed when you select Single Brick Window and Single Brick Ports Window from the Monitor menu.

## Format and Contents

[Figure 14-7, “Brick Lists \(All Bricks\)”](#) (p. 14-21) shows a typical Brick List (All Bricks). All the Brick Lists share this same format.

Figure 14-7 Brick Lists (All Bricks)



For each Brick device in the list, the following information is provided:

Field	Description
Name	The name of the Brick device
IP Address	The IP address of the Brick device

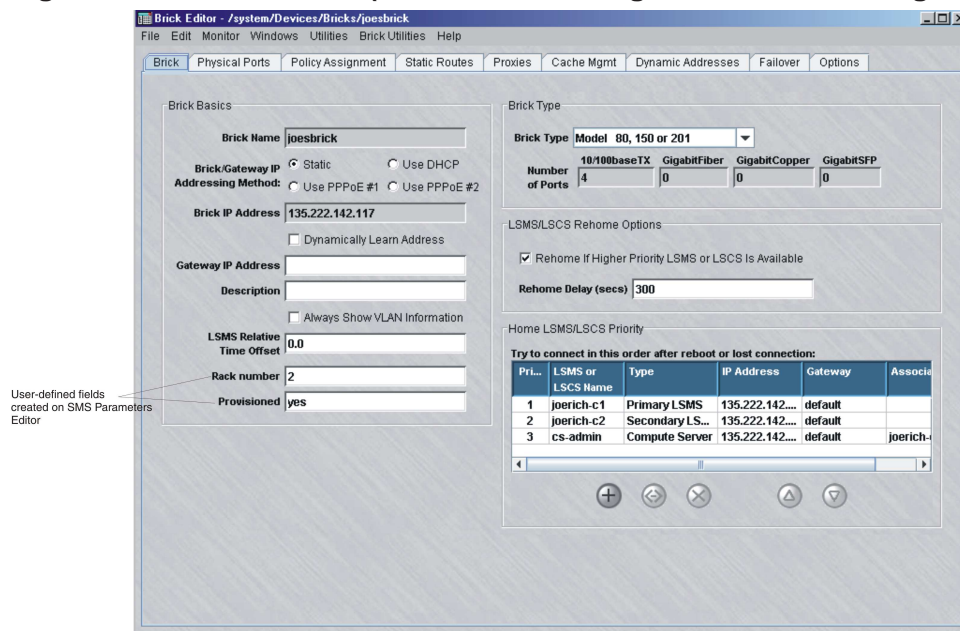
Field	Description
State	Up, Lost, or Unhealthy. The Unhealthy state indicates a hardware fault and can be given for either the active or standby Brick in a failover pair. The State field displays a green checkmark if the State is Up, a red "x" if the State is Lost, and a yellow checkmark if the State is unhealthy; a yellow checkmark is displayed if either the active or standby Brick in a failover pair is unhealthy. If the Brick is the standby Brick of a failover pair, it shows the current operational state of the active and standby Brick in the pair (such as Up-Up or Up-Unhealthy).
CPU%	The percentage of the Brick device CPU currently in use
Sess%	The percentage of the Brick device session cache currently in use
Active Version	If the Brick device is a standalone, this is the version of the Brick device operating system. If the Brick device is part of a failover pair, this is the version of the active Brick operating system.
Standby Version	If the Brick device is part of a failover pair, this is the version of the standby Brick operating system.
Failover Labels	If this Brick device is part of a failover pair, the label consists of the last two octets of each Brick device MAC address, or the values configured by the administrator on the Failover tab of the Brick Editor. The label also indicates which Brick device is active and which is standby. If this Brick device is not configured as part of a failover pair, the failover label is <i>Not Configured</i> .
Port Status	The number of ports up, down, and disabled
Mgmt Server	The name of the SMS to which this Brick is currently homed
Roaming	Indicates whether this Brick is "roaming" from its priority 1 SMS: <ul style="list-style-type: none"> <li>• No means it is currently connected to its priority 1 SMS</li> <li>• Yes means it is currently connected to a lower priority SMS</li> </ul>



### User-defined fields

Along with the standard Brick configuration information provided on the All Bricks status windows, an administrator can add up to 5 user-defined fields, which can be used to record and track other details about each Brick, as needed. These fields are defined using the SMS Parameters Editor and, when enabled, are displayed for inputting Brick configuration data on the Brick tab of the Brick Editor (Figure 14-8, “Brick Editor (Brick Tab, showing user-defined configuration fields)” (p. 14-23) shows an example) and on the All Bricks Assigned to and All Bricks status windows (Figure 14-9, “All Bricks Status Window (showing user-defined configuration fields)” (p. 14-24) shows an example).

**Figure 14-8 Brick Editor (Brick Tab, showing user-defined configuration fields)**



**Figure 14-9 All Bricks Status Window (showing user-defined configuration fields)**

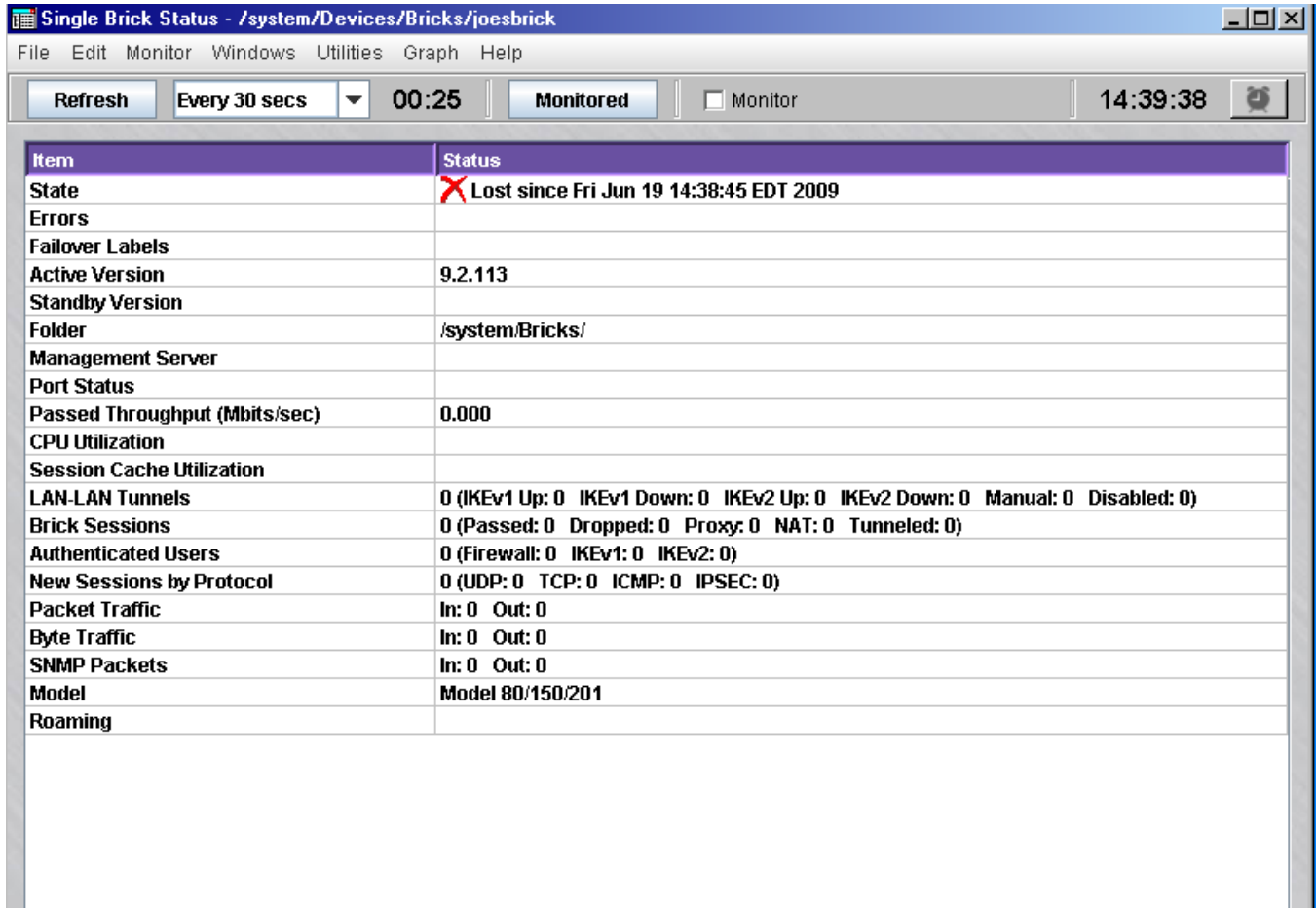
s	State	CPU%	Sess%	Active Version	Standby Version	Failover Labels	Port Status	Mgmt Server	Roaming	Rack num...	Provisioned
117	Lost			9.2.113			Up:0 Down:0 Disabled:0			2	yes
22	Lost			9.3.124			Up:0 Down:0 Disabled:0				
118	Lost			9.2.113			Up:0 Down:0 Disabled:0				

### Single Brick Status Window

The Single Brick Status window provides information about a specific selected Brick. To display the Single Brick Status window, open the Monitor menu, select **Brick Status**, and then select **Single Brick Status** from the submenu.

Figure 14-10, “Single Brick Status Window” (p. 14-25) shows a typical Single Brick Status Window.

Figure 14-10 Single Brick Status Window



For the Brick shown, the following information is provided:

Field	Description
State	Up, Lost, or Unhealthy. The Unhealthy state indicates a hardware fault and can be given for either the active or standby Brick in a failover pair. The State field displays a green checkmark if the State is Up, a red “x” if the State is Lost, and a yellow checkmark if the State is unhealthy; a yellow checkmark is displayed if either the active or standby Brick in a failover pair is unhealthy.
Errors	Dot3, collision or frame errors.

Field	Description
Failover Labels	<p>If this Brick is part of a failover pair, the label consists of the last two octets of each Brick's MAC address. The label also indicates which Brick is active and which is standby.</p> <p>If this Brick is not configured as part of a failover pair, this field is blank.</p>
Active Version	<p>If the Brick is a standalone Brick, this is the version of the Brick's operating system.</p> <p>If the Brick is part of a failover pair, this is the version of the active Brick's operating system.</p>
Standby Version	<p>If the Brick is part of a failover pair, this is the version of the standby Brick's operating system.</p>
Folder	<p>The folder in which the Brick is found.</p>
Management Server	<p>The name of the SMS to which this Brick is currently homed.</p>
Port Status	<p>The number of ports up, down, and disabled.</p>
CPU Utilization	<p>The percentage of the Brick CPU currently in use.</p>
Session Cache Utilization	<p>The percentage of the Brick's session cache currently in use.</p>
LAN-LAN Tunnels	<p>The total number of LAN-LAN tunnels of which this Brick is an endpoint, divided into categories [IKEv1 Up, IKEv1 Down, IKEv2 Up, IKEv2 Down, Manual, Disabled].<i>Note: details about disabled manual tunnels are not downloaded from the SMS to the Brick. As a result, the Disabled counter does not include a count of disabled manual tunnels.</i></p>
Brick Sessions	<p>The total number of sessions through this Brick, divided into categories (Passed, Dropped, Proxy, NAT, Tunneled).</p>
Authenticated Users	<p>The total number of authenticated users, divided into Firewall, IKEv1, and IKEv2 categories.</p>
New Sessions by Protocol	<p>The total number of new sessions, divided into categories by protocol (examples: UDP, TCP, ICMP, IPSec)</p>
Packet Traffic	<p>The total number of packets handled by the Brick in the last refresh cycle, divided into <i>In</i> and <i>Out</i> categories.</p> <p>This makes it possible to view the activity on a port, as well as the total of all the ports.</p>

Field	Description
Byte Traffic	The total number of bytes handled by the Brick, divided into <i>In</i> and <i>Out</i> categories.  This makes it possible to view the activity on a port, as well as the total for all ports.
SNMP Packets	The total number of incoming and outgoing SNMP packets handled by the Brick, if the SNMP on the Brick feature is enabled. If the feature is disabled, both totals are zero (0).
Model	The Brick model.
Roaming	Indicates whether this Brick is "roaming" from its priority 1 SMS: <ul style="list-style-type: none"> <li>• <i>No</i> means it is currently connected to its priority 1 SMS</li> <li>• <i>Yes</i> means it is currently connected to its priority 2 SMS</li> </ul>

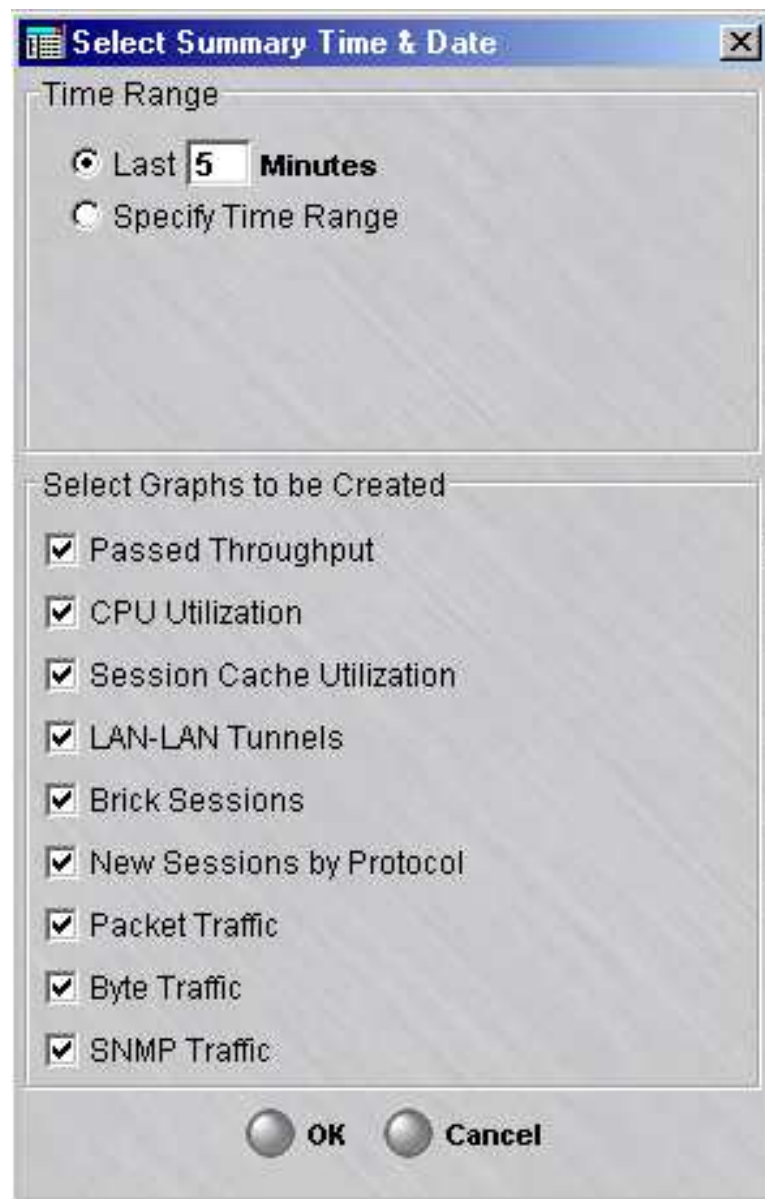
The Single Brick Status window also has a Graph menu on the menubar at the top. This menu allows you to display graphs of the following:

- Throughput
- CPU utilization
- Session cache utilization
- LAN-LAN tunnels (showing up, down, manual and foreign tunnels)
- Brick sessions (showing passed, dropped, proxied, NATted and tunneled sessions)
- Authenticated users (showing firewall and Client VPN users)
- New sessions by protocol (showing UDP, TCP, ICMP and IPSec protocols)
- Packet traffic (showing in and out traffic)
- Byte traffic (showing in and out traffic)
- SNMP packets (showing incoming and outgoing packets)

If you want these graphs to reflect current Brick activity, select the appropriate graph from the Graph menu (or right-click in the Single Brick Status window and select the graph).

If you want the graph to display historical information, select **Summarize** from the Graph menu. The window shown in [Figure 14-11, "Select Summary Time and Date Window"](#) (p. 14-28) will appear. Indicate how many minutes previously you want the summary to cover (the default is 5), or click **Select Time Range** and enter a start date/time and end date/time.

Then, indicate which of the eight graphs you want created. By default, all checkboxes are checked, so all graphs will be created. When you click **OK**, a separate graph will be generated for each option checked.

**Figure 14-11 Select Summary Time and Date Window**

### Single Brick Ports Window

The Single Brick Ports window provides information about the ports for the selected Brick. To display the Single Brick Ports window, open the Monitor menu, select **Brick Status**, and then select **Single Brick Ports**.

[Figure 14-12, “Single Brick Ports Window” \(p. 14-29\)](#) shows a typical Single Brick Ports window for a standalone Brick.

Figure 14-12 Single Brick Ports Window

Single Brick Ports - /system/Devices/Bricks/attila

File Edit Monitor Windows Utilities Graph Help

Refresh Every 30 secs 00:05 Monitored  Monitor 15:14:58

TOTAL INTERFACES: 4 [4 UP - 0 DOWN]

Interface	State	Bytes In	Bytes Out	Packets In	Packets Out	Error Packets In	Error Packets ...	Dot 3 Errors	Collision Errors	Frame Errors
ether0	✓ Up	4224	11404	66	110	0	0	0	0	0
ether1	✓ Up	2404	2404	31	31	0	0	0	0	0
ether2	✓ Up	2184	0	28	0	0	0	0	0	0
ether3	✓ Up	11514	7044	96	66	0	0	0	0	0

For each port, the window indicates whether it is up or down and displays the following information:

- Bytes in/out
- Packets in/out
- Error packets in/out
- Dot 3, collision and frame errors.

If the Brick is part of a failover pair, the Single Brick Ports window shows the byte/packet/error counts for each port of the currently active Brick for the selected monitoring period.

Figure 14-13, “Single Brick Ports Window (Brick Failover Pair)” (p. 14-30) shows a sample Single Brick Ports window for a Brick failover pair.

Figure 14-13 Single Brick Ports Window (Brick Failover Pair)

Single Brick Ports - /system/Devices/Bricks/twin-1200

File Edit Monitor Windows Utilities Graph Help

Refresh Every 30 secs 00:08 Monitored Monitor 16:51:28

TOTAL PORTS: 20 [12 UP - 7 DOWN - 1 DISABLED]

Port	State	Bytes In	Bytes Out	Packets In	Packets Out	Error Packets In	Error Packets Out	Dot 3 Errors	Collision Errors	Frame Errors
ether0	✓ Verified	488388	94841	2001	704	0	0	0	0	0
ether1	✓ Verified	65263	87767	530	455	0	0	0	0	0
ether2	✓ Verified	15760	80788	129	391	0	0	0	0	0
ether3	✗ Down	0	0	0	0	0	0	0	0	0
ether4	✓ Verified	84212	116951	601	627	0	0	0	0	0
ether5	✗ Down	0	0	0	0	0	0	0	0	0
ether6	✓ Up - no data	0	30240	0	280	0	0	0	0	0
ether7	✗ Down	0	0	0	0	0	0	0	0	0
ether8	✓ Receiving	0	30240	0	280	0	0	0	0	0
ether9	✗ Down	0	0	0	0	0	0	0	0	0
ether10	✗ Disabled	0	0	0	0	0	0	0	0	0
ether11	✗ Down	0	0	0	0	0	0	0	0	0
ether12	✗ Down	0	0	0	0	0	0	0	0	0
ether13	✓ Verified	4428	30304	41	281	0	0	0	0	0
ether14	✗ Down	0	0	0	0	0	0	0	0	0
ether15	✓ Verified	169269	99603	411	607	0	0	0	0	0
ether16	✓ Verified	4428	30240	41	280	0	0	0	0	0
ether17	✓ Verified	4428	30240	41	280	0	0	0	0	0
ether18	✓ Verified	4428	30240	41	280	0	0	0	0	0
ether19	✓ Verified	170068	412083	1486	1111	0	0	0	0	0

The **State** field of the Single Brick Ports window shows the link integrity (health) of each Brick interface, either for a standalone Brick or the active and standby Brick in a failover pair.

The link integrity states of each interface on a standalone Brick are as follows:

State	Meaning
Up	Link integrity but not receiving any frames
Down	No link integrity
Disabled	Not capable of receiving frames



The link integrity states of each interface on a Brick failover pair (active and standby) are as follows:

State	Meaning
<b>Up - no data</b>	Link integrity exists between the active and standby Brick on this interface but the active Brick is not receiving any frames. Also indicates that the active and standby Brick are not connected to the same switch or hub.
<b>Down</b>	No link integrity
<b>Receiving</b>	Receiving non-heartbeat frame
<b>Unverified</b>	Receiving heartbeats that do not acknowledge the heartbeats sent on this link
<b>Verified</b>	Receiving heartbeats that do acknowledge the heartbeats sent. In a Brick failover pair, if the standby Brick is powered down, the ports showing a state of <b>Verified</b> switch over to a state of <b>Receiving</b>
<b>Disabled</b>	Not capable of receiving frames

Note that when a standby Brick is powered down in a failover pair, the **State** of the link between the active and standby Brick for a port is shown on this window as either **Receiving** or **Up - no data**

The Single Brick Ports window also has a Graph menu on the menu bar at the top. This menu allows you to display graphs of the following:

- Byte traffic
- Packet traffic
- Error traffic
- Errors



If you want these graphs to reflect current port activity, select the appropriate graph from the Graph menu (or right-click in the Single Brick Status window and select the graph).

If you want the graph to display historical information, select **Summarize** from the Graph menu. A window similar to the one shown in [Figure 14-11, “Select Summary Time and Date Window”](#) (p. 14-28) will appear. Indicate how many minutes previously you want the summary to cover (the default is 5), or click **Select Time Range** and enter a start date/time and end date/time.

Then, indicate which of the four graphs you want created. By default, all checkboxes are checked, so all graphs will be created. When you click **OK**, a separate graph will be generated for each option checked.

At the bottom of each graph, there is a drop down list that lets you decide whether you want the graph to show all ports (the default), or one specific port.

In addition, each graph has two buttons to the right of the date:

- The **Legend** button  on the left acts as a toggle. Click it once to remove the legend from a graph so there is a larger graph area to view. Click it again to return the legend.
- The **Print** button  on the right allows you to print the graph. You must have a default printer defined for the print operation to work.

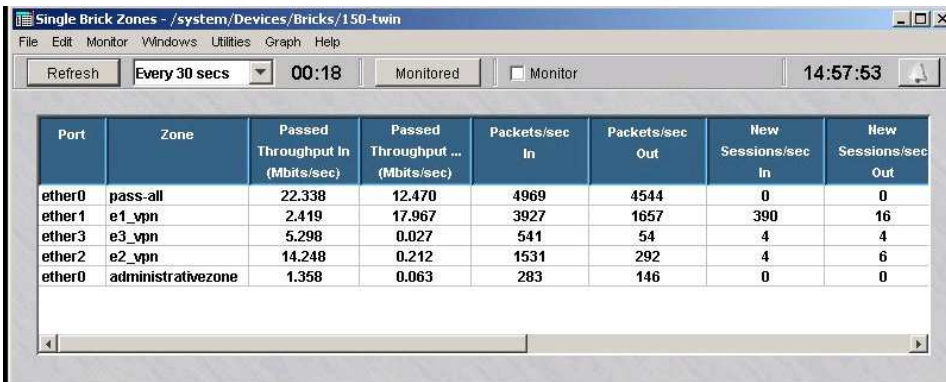
## Single Brick Bandwidth Statistics Window

The Single Brick Bandwidth Statistics provides traffic statistics and performance information for each port of the selected Brick.

**Important!** The **Enable Port Bandwidth Parameters** checkbox must be checked on the Brick Ports Editor for each Brick port to display the port bandwidth statistics on this window. For instructions on how to configure Brick ports, refer to [Chapter 4, “Configuring Alcatel-Lucent VPN Firewall Brick™ Security Appliance Ports”](#).

Figure 14-14, “Single Brick Zones Window” (p. 14-32) shows a sample Single Brick Bandwidth Zones window, displaying the bandwidth statistics for each Brick port.

**Figure 14-14 Single Brick Zones Window**



Port	Zone	Passed Throughput In (Mbits/sec)	Passed Throughput ... (Mbits/sec)	Packets/sec In	Packets/sec Out	New Sessions/sec In	New Sessions/sec Out
ether0	pass-all	22.338	12.470	4969	4544	0	0
ether1	e1_vpn	2.419	17.967	3927	1657	390	16
ether3	e3_vpn	5.298	0.027	541	54	4	4
ether2	e2_vpn	14.248	0.212	1531	292	4	6
ether0	administrativezone	1.358	0.063	283	146	0	0

For each port, the window displays the following information by zone:

- Data packet throughput into the Brick (Mbits/sec)
- Data packet throughput out of the Brick (Mbits/sec)
- Packets per second into the Brick

- Packets per second out of the Brick
- New sessions per second into the Brick
- New sessions per second out of the Brick
- Megabit guarantee into the Brick
- Megabit limit into the Brick
- Session limit into the Brick
- Megabit guarantee out of the Brick
- Megabit limit out of the Brick
- Session limit out of the Brick

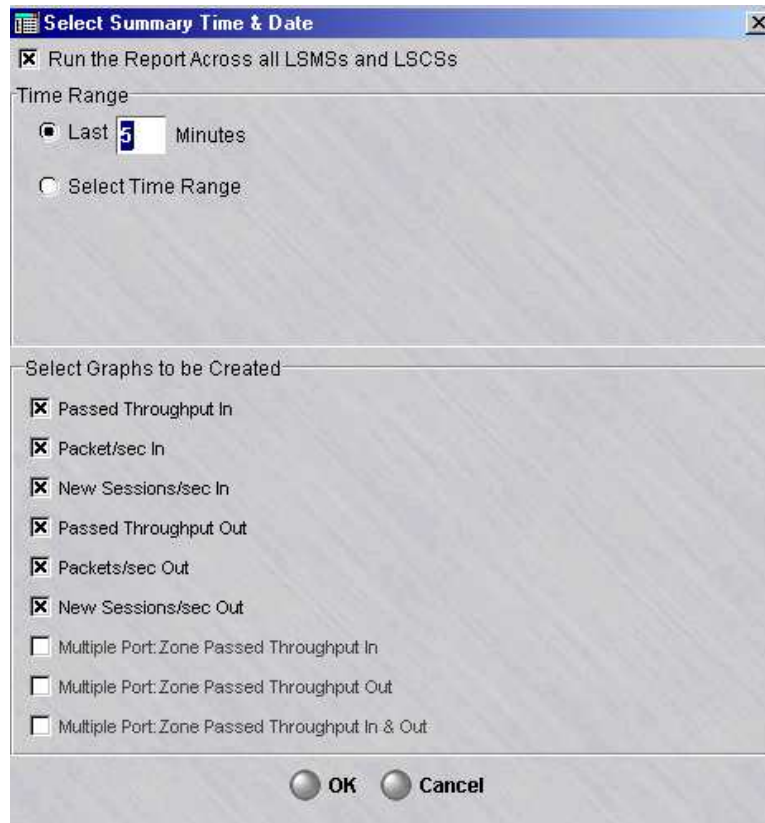
The Single Brick Zones window also has a Graph menu on its menu bar, to display a graphical representation of the data, according to user-specified criteria.

To select a graph that shows current Brick activity, select the appropriate graph from the Graph menu or right-click in the Single Brick Zones window and select the graph.

To display historical data graphically, select **Summarize** from the Graph menu.

The Select Summary Time & Date window is displayed ([Figure 14-15, “Select Summary Time and Date Window \(Brick Bandwidth Statistics\)”](#) (p. 14-34)).

**Figure 14-15 Select Summary Time and Date Window (Brick Bandwidth Statistics)**



Indicate the prior time period for the summary (default is five minutes), or click **Select Time Range** and enter a start and end date/time.

Indicate which graphs that you want to display, and click **OK**. A separate graph is generated for each option checked.

□

## Console Alarms Window

---

### Console alarms window display

The Console Alarms window displays all alarms that have been configured to send a message to the SMS console. To display the Console Alarms window, open the Monitor menu and select **Console Alarms**.

The bell shown below will appear at the top of the SMS window currently open when a new console alarm has been triggered. You can display the Console Alarms window by clicking this icon:



Figure 14-16, “Console Alarms Window” (p. 14-36) shows a typical Console Alarms Window. For each alarm, the window shows the data and time, and the text of the console message.

Figure 14-16 Console Alarms Window

Time	Alarm Text
Tue May 29 14:22:11 EDT 2001	Secondary LSMS - secondary_nt - LSMS has contacted peer LSMS again
Tue May 29 14:21:42 EDT 2001	<2k_brick2> LSMS has contacted Brick again.
Tue May 29 14:18:47 EDT 2001	<2k_brick2> LSMS cannot contact Brick.
Tue May 29 14:18:47 EDT 2001	Secondary LSMS - secondary_nt - LSMS unable to contact peer LSMS
Tue May 29 14:13:36 EDT 2001	Lan To Lan Tunnel DownFireWall: 2k_brick1 Reason: missing Source Host: 10.20.30.23 Destination Host: 10.20.30.101Time: 991160...
Tue May 29 14:13:36 EDT 2001	Lan To Lan Tunnel DownFireWall: 2k_brick1 Reason: missing Source Host: 10.20.30.23 Destination Host: 10.20.30.101Time: 991160...
Tue May 29 14:13:35 EDT 2001	Lan To Lan Tunnel DownFireWall: 2k_brick2 Reason: missing Source Host: 10.20.30.101 Destination Host: 10.20.30.23Time: 991160...
Tue May 29 14:13:35 EDT 2001	Lan To Lan Tunnel DownFireWall: 2k_brick2 Reason: missing Source Host: 10.20.30.101 Destination Host: 10.20.30.23Time: 991160...
Tue May 29 14:08:02 EDT 2001	Secondary LSMS - secondary_nt - LSMS has contacted peer LSMS again
Tue May 29 14:07:19 EDT 2001	<2k_brick2> LSMS has contacted Brick again.
Tue May 29 14:04:41 EDT 2001	<2k_brick2> LSMS cannot contact Brick.
Tue May 29 14:04:36 EDT 2001	Secondary LSMS - secondary_nt - LSMS unable to contact peer LSMS
Tue May 29 14:04:48 EDT 2001	Lan To Lan Tunnel DownFireWall: 2k_brick1 Reason: missing Source Host: 10.20.30.23 Destination Host: 10.20.30.101Time: 991159...
Tue May 29 14:04:48 EDT 2001	Lan To Lan Tunnel DownFireWall: 2k_brick1 Reason: missing Source Host: 10.20.30.23 Destination Host: 10.20.30.101Time: 991159...
Tue May 29 14:02:36 EDT 2001	Lan To Lan Tunnel DownFireWall: 2k_brick1 Reason: missing Source Host: 10.20.30.23 Destination Host: 10.20.30.101Time: 991159...
Tue May 29 14:02:36 EDT 2001	Lan To Lan Tunnel DownFireWall: 2k_brick1 Reason: missing Source Host: 10.20.30.23 Destination Host: 10.20.30.101Time: 991159...
Tue May 29 14:00:24 EDT 2001	Lan To Lan Tunnel DownFireWall: 2k_brick1 Reason: missing Source Host: 10.20.30.23 Destination Host: 10.20.30.101Time: 991159...
Tue May 29 14:00:24 EDT 2001	Lan To Lan Tunnel DownFireWall: 2k_brick1 Reason: missing Source Host: 10.20.30.23 Destination Host: 10.20.30.101Time: 991159...
Tue May 29 13:58:12 EDT 2001	Lan To Lan Tunnel DownFireWall: 2k_brick1 Reason: missing Source Host: 10.20.30.23 Destination Host: 10.20.30.101Time: 991159...
Tue May 29 13:58:12 EDT 2001	Lan To Lan Tunnel DownFireWall: 2k_brick1 Reason: missing Source Host: 10.20.30.23 Destination Host: 10.20.30.101Time: 991159...
Tue May 29 13:56:00 EDT 2001	Lan To Lan Tunnel DownFireWall: 2k_brick1 Reason: missing Source Host: 10.20.30.23 Destination Host: 10.20.30.101Time: 991158...
Tue May 29 13:56:00 EDT 2001	Lan To Lan Tunnel DownFireWall: 2k_brick1 Reason: missing Source Host: 10.20.30.23 Destination Host: 10.20.30.101Time: 991158...
Tue May 29 13:53:48 EDT 2001	Lan To Lan Tunnel DownFireWall: 2k_brick1 Reason: missing Source Host: 10.20.30.23 Destination Host: 10.20.30.101Time: 991158...
Tue May 29 13:53:48 EDT 2001	Lan To Lan Tunnel DownFireWall: 2k_brick1 Reason: missing Source Host: 10.20.30.23 Destination Host: 10.20.30.101Time: 991158...
Tue May 29 13:51:25 EDT 2001	Lan To Lan Tunnel DownFireWall: 2k_brick1 Reason: missing Source Host: 10.20.30.23 Destination Host: 10.20.30.101Time: 991158...
Tue May 29 13:51:25 EDT 2001	Lan To Lan Tunnel DownFireWall: 2k_brick1 Reason: missing Source Host: 10.20.30.23 Destination Host: 10.20.30.101Time: 991158...
Tue May 29 13:50:12 EDT 2001	Secondary LSMS - secondary_nt - LSMS has contacted peer LSMS again
Tue May 29 13:49:49 EDT 2001	<2k_brick2> LSMS has contacted Brick again.
Tue May 29 13:47:45 EDT 2001	Lan To Lan Tunnel DownFireWall: 2k_brick1 Reason: missing Source Host: 10.20.30.23 Destination Host: 10.20.30.101Time: 991158...
Tue May 29 13:47:45 EDT 2001	Lan To Lan Tunnel DownFireWall: 2k_brick1 Reason: missing Source Host: 10.20.30.23 Destination Host: 10.20.30.101Time: 991158...
Tue May 29 13:46:49 EDT 2001	<2k_brick2> LSMS cannot contact Brick.
Tue May 29 13:46:47 EDT 2001	Secondary LSMS - secondary_nt - LSMS unable to contact peer LSMS
Tue May 29 13:45:22 EDT 2001	Lan To Lan Tunnel DownFireWall: 2k_brick1 Reason: missing Source Host: 10.20.30.23 Destination Host: 10.20.30.101Time: 991158...
Tue May 29 13:45:22 EDT 2001	Lan To Lan Tunnel DownFireWall: 2k_brick1 Reason: missing Source Host: 10.20.30.23 Destination Host: 10.20.30.101Time: 991158...
Tue May 29 13:43:42 EDT 2001	Secondary LSMS - secondary_nt - LSMS has contacted peer LSMS again
Tue May 29 13:43:40 EDT 2001	<2k_brick2> LSMS has contacted Brick again.

# 15 Simple Network Management Protocol (SNMP)

## Overview

---

### Purpose

This chapter describes the Simple Network Management Protocol (SNMP) application layer protocol and its use by a Network Management System (NMS) to monitor and collect configuration, status, statistical, and alarm information from the SMS and its managed Brick devices.

### Contents

<a href="#">Basic SNMP Concepts</a>	15-2
<a href="#">SNMP on the SMS</a>	15-6
<a href="#">SNMP on the Brick</a>	15-9
<a href="#">To Configure the SNMP on the Brick Feature</a>	15-10



## Basic SNMP Concepts

---

### Definition

SNMP is part of the internet protocol suite defined by the Internet Engineering Task Force (IETF). SNMP is used by Network Management Systems (NMSs) to monitor and collect key administrative data from network-connected devices and systems, such as the Alcatel-Lucent *VPN Firewall Brick*<sup>TM</sup> Security Appliances and the SMS itself. It consists of a set of standards for network management, which include an application layer protocol, a database schema for classifying the managed object data, which is referred to as a Management Information Base (MIB), and a set of data object types.

SNMP exposes management data, in the form of variables, about the configuration and performance of the managed device or system. These variables can then be queried or modified and configured by the NMS. For security reasons, the SMS and Brick only support SNMP queries. Variable modification and configuration via SNMP is not allowed.

The key components of an SNMP-managed network are:

- Managed devices (in this case, the SMS and Bricks)
- SNMP agents
- Network Management Systems (NMSs)

### SNMP agent

An SNMP agent is a network management software module that resides on the SMS and each managed Brick. The SMS SNMP Agent is built-in to the SMS application and is stopped and started along with the rest of the SMS application services. The Brick SNMP Agent is an optional feature that can be enabled or disabled individually on each Brick. The SNMP agents allow the NMS to access and collect management data from the Brick devices and the SMS. An NMS can actively poll and retrieve management data about the Brick devices or SMS through GET, GETNEXT, and GETBULK protocol operations, or the SNMP agent on the SMS notifies the NMS and sends the data through a TRAP protocol operation without being polled (when, for example, an alarm condition is triggered on a Brick).

### SNMP protocol versions supported

SNMPv1 and SNMPv2c are supported, only over User Datagram Protocol (UDP), by the Alcatel-Lucent *VPN Firewall Brick*<sup>TM</sup> Security Solution. SNMPv3 is currently not supported.



## Management information base (MIB)

To define which information (variables) is available and retrievable by an NMS, the SNMP concept of a Management Information Base (MIB) is used. An MIB is a hierarchical definition of all of the categories of information that are available about a managed device, similar to a database schema. The hierarchical structure of an MIB is analogous to a tree, with individual data items making up the leaves of the tree. The leaf, or object instance, holds a value that is collected by an NMS.

Management data is organized in a MIB into a table, and classified and grouped into related classes of managed objects, each uniquely identified by an object identifier (OID) or object name (such as 1.3.6.1.2.1.1.5 or brkDevName). An NMS uses the OID to search for and retrieve a specific object instance from the SMS or Brick, such as the IP address assigned to a tunnel endpoint on a Brick, or a specific metric, such as the number of frames received that exceeded the frame size in a packet.

The Alcatel-Lucent MIBs are private, but based on MIB-II. Many parameters found in MIB-II are supported in the Alcatel-Lucent MIBs under private OIDs. These MIBs, which are provided on the SMS CD-ROM, comprise two basic types of retrievable information: configuration and statistical. Local procedures for copying the MIBs from the SMS CD-ROM and installing them on the NMS server vary by server type; consult the appropriate documentation for your NMS for details. Generally, configuration and statistical data objects are defined in separate MIBs. The MIBs are as follows:

MIB Name	MIB Description
<i>svs-global-reg.mib</i>	<p>LUCENT-SECURE-VPN-SOLUTIONS-GLOBAL-REG</p> <p>The Global Registration module contains the assigned numbers for all other modules, as well as entry points for conformance, capabilities, requirements, and experimental sections to be added.</p> <p>It also contains OIDs for current products including Bricks, the SMS, and so forth. All modules depend on the Global Registration Module.</p>

MIB Name	MIB Description
<i>svs-Brick-mib.mib</i>	<p data-bbox="659 254 1305 281"><b>LUCENT-SECURE-VPN-SOLUTIONS-Brick-MIB</b></p> <p data-bbox="659 302 1425 443">The Brick module is the most complex of all the modules. Since there can be many Brick devices in the system, and each Brick device has multiple interfaces, there needs to be several layers of hierarchy to accommodate all information.</p> <p data-bbox="659 464 1422 527">However, since SNMPv2c does not allow nesting of tables, the data is arranged in the following six related tables:</p> <ul data-bbox="659 548 1187 800" style="list-style-type: none"> <li data-bbox="659 548 964 575">• Brick Configuration</li> <li data-bbox="659 596 902 623">• Brick Statistics</li> <li data-bbox="659 644 1084 672">• Brick Interface Configuration</li> <li data-bbox="659 693 1024 720">• Brick Interface Statistics</li> <li data-bbox="659 741 1008 768">• Brick Tunnel Endpoints</li> <li data-bbox="659 789 1187 816">• Brick VLAN IP Address Assignments</li> </ul> <p data-bbox="659 837 1438 1220">A separate private <i>brkDevEntry</i> branch, which contains all of the above Brick MIB objects, plus LAN-LAN tunnel information, is defined to allow an NMS to retrieve this information directly from each Brick that has been upgraded to R9.4 and has the SNMP Agent on the Brick feature enabled (via the Brick Editor in SMS). In addition, those objects that map directly to a standard MIB object are also reported using that OID. Data is retrieved by the NMS from each Brick, instead of collectively from a group of Bricks (listed as separate entries in a table) from the SMS. The SNMP agent on the SMS does not report OIDs from this branch.</p>
<i>svs-lsms-mib.mib</i>	<p data-bbox="659 1245 1295 1272"><b>LUCENT-SECURE-VPN-SOLUTIONS-SMS-MIB</b></p> <p data-bbox="659 1293 1438 1434">The SMS module contains basic configuration and statistical information about the SMS, as well as all objects related to notifications (traps). The SMSEvents object is contained in the SMS module.</p> <p data-bbox="659 1455 1438 1629">This MIB also contains a table of up to six alarms, so if the NMS believes it may have missed a notification due to network packet loss, it may query the SMS alarms table. Each entry in the table contains the same information that is sent in the notification.</p>

MIB Name	MIB Description
<i>svs-lsms-notification-mib.mib</i>	<p data-bbox="699 254 1279 321"><b>LUCENT-SECURE-VPN-SOLUTIONS-SMS-NOTIFICATIONS-MIB</b></p> <p data-bbox="699 338 1468 478">The Notifications module contains one notification-type for every SMS alarm type that exists in the SMS. All notifications are sent with respect to objects in the SMS MIB.</p> <p data-bbox="699 495 1479 636">Each notification contains the date/time it was triggered and a plain-text explanation as to what happened. Since each notification has its own type, no type information is included within the notification body.</p> <p data-bbox="699 653 1149 684">There are no tables in this module.</p>
<i>svs-auditsvr-mib.mib</i>	<p data-bbox="699 705 1430 737"><b>LUCENT-SECURE-VPN-SOLUTIONS-AUDITSVR-MIB</b></p> <p data-bbox="699 753 1479 894">The Audit Server module is designed to allow the NMS to query the Audit Server process to determine the number and type of audit logs currently in service on that host, as well as current statistics regarding free space and usage rates.</p> <p data-bbox="699 911 1344 942">There is no ability to view log records via SNMP.</p> <p data-bbox="699 959 1446 1062">This module contains a table with information about each audit log on the device (such as the AdminEvents log and Proactive Monitoring log).</p>
<i>svs-authsvr-mib.mib</i>	<p data-bbox="699 1083 1422 1115"><b>LUCENT-SECURE-VPN-SOLUTIONS-AUTHSVR-MIB</b></p> <p data-bbox="699 1131 1451 1272">The Authentication Server module gives statistics and configuration regarding the Authentication Server process. Currently, the Auth Server must be co-located on the SMS host.</p> <p data-bbox="699 1289 1443 1356">This module only has a very small number of parameters. There are no tables in this module.</p>



## SNMP on the SMS

---

### Overview

The SNMP agent on the SMS reports configuration information for all Bricks, management status and hardware alarm status for all Bricks, and statistical information for Bricks that are homed to that SMS. The SMS SNMP Agent also reports information about the SMS itself, including statistics on the Audit and Authentication Server subsystems.

The SNMP agent obtains statistical information about Bricks primarily from the Proactive Monitoring log. This log contains information reported by each Brick in the system and is updated every 30 seconds. Therefore, the NMS can be set up to poll the SMS in 30 second intervals. If all Bricks are homed to a Primary SMS, information for every Brick can be obtained by polling that SMS. If some Bricks are currently homed to a Secondary SMS in a Primary/Secondary SMS redundant pair or one of the Compute Servers (CSs) connected to the SMS, only information about Bricks that are currently homed to a given SMS is available on that host.

### Default SNMP UDP port

When installing the SMS application for the first time (a “clean” installation), the installation program prompts you for the SMS SNMP Agent port. This is the UDP port where the SMS Agent listens for queries from the NMS. The default value is 161, which is the standard port for SNMP. During installation, you can accept the default port or change it to another port number if port 161 is being used by another SNMP application.

You should only change the default port if you are already using or planning to use a third-party SNMP agent and assign it to port 161 (refer to the [“Multiple SNMP agents” \(p. 15-6\)](#) section).

After the SMS application is installed, you can change the SMS SNMP agent port by using the Configuration Assistant to change the SNMP Configuration parameters. Refer to the *Using the Configuration Assistant* chapter for details.

### Multiple SNMP agents

The SNMP agent on the SMS does not provide information about the SMS host or operating system.

If information about the host or operating system must be retrieved, you must install a separate third-party SNMP agent software module on the SMS host (not provided with the SMS software) or configure/enable the SNMP agent that comes with the operating system (such as the SNMP Agent Service on *Microsoft® Windows®*).

Any third-party SNMP agent must be configured to use a different UDP port on the SMS than the SMS SNMP agent; both SNMP agents cannot use the default UDP port 161. Use the Configuration Assistant to define which UDP ports will be used by the Operating System SNMP agent, the SMS SNMP agent, and the Brick SNMP agent. Refer to the *Using the Configuration Assistant* chapter for details on how to provision the SNMP Agent parameters.

## SNMP traps

In the SMS environment, SNMP traps are associated with an alarm action. The **SNMP Trap** alarm action can be associated with any alarm trigger type. When a particular alarm is triggered, and the assigned alarm action is **SNMP Trap**, the SNMP agent on the SMS sends the SNMP trap to the NMS. SNMP traps and alarm data are always forwarded by the SMS, regardless of whether the SNMP Agent is activated on the SMS, on the Brick, or on both.

Once the SNMP trap is received on the NMS, and the NMS administrator is notified, the NMS administrator logs into the SMS and analyzes the situation by viewing log files or generating reports, using the details provided in the trap.

Each alarm trigger type (such as Unauthorized LSMS Login Attempt, Brick Lost) has a unique SNMP Object Identifier (OID), which allows the NMS to associate the trap with a specific alarm type. A network administrator can then determine exactly what type of fault condition exists in the network, and information forwarded in the trap message can be used to determine where exactly the problem occurred.

Each SNMP trap contains data elements that are specific to the alarm type. These data elements are defined in the MIB. In addition to the alarm-specific information forwarded, each trap includes the:

- Alarm Index
- Alarm Trigger Time
- Alarm Details (unparsed)
- Alarm Log Entry
- Alarm Trigger Name

SMS alarms include the SMS name, while Brick alarms include the Brick name.

## Brick zone rules

In a normal network configuration, where a Brick is protecting the SMS, security rules must be added to the zone between the SMS and NMS to allow SNMP traffic to pass. Typically, this will be the *administrativezone*. One rule must be created in a Brick zone ruleset to pass SNMP requests from the NMS to the SMS; a pre-defined service group **snmp** for UDP traffic on port 161 already exists for SNMP Requests and can be assigned to this rule. Another rule must be created in a Brick zone ruleset to pass

SNMP traps from the SMS to the NMS; a pre-defined service group **snmp\_trap** for UDP traffic on port 162 already exists for SNMP traps and can be assigned to this rule.

For details about how to create security rules, refer to the *SMS Policy Guide*.



## SNMP on the Brick

---

### Overview

The SNMP agent on the Brick, when enabled, allows an NMS to monitor and retrieve management data directly from a Brick without having to go through the SMS proxy.

The SNMP on the Brick feature is enabled/disabled and configured on the Options tab of the Brick Editor (refer to the procedure [“To Configure the SNMP on the Brick Feature”](#) (p. 15-10)).

When enabled, the SNMP agent on the Brick reports configuration information, operational status, and statistical information for that Brick.

The SNMP agent software on the Brick does not permit write or SET protocol operations to set or modify a Brick configuration for security reasons.

### SNMP traps

SNMP traps are still generated and sent by the SMS on an alarm action to the NMS. Traps are always sent from SMS, not the Brick, even if the SNMP agent on the Brick is enabled.

### Brick zone rule

When the SMS is upgraded to R9.4 and installed on a Brick, a new rule (Rule 250) is automatically added to the *firewall* zone ruleset, which allows SNMP requests to be passed from the specified NMS host(s) to the Brick, and read by the SNMP agent on the standard UDP port 161. The NMS hosts can be specified in the host group **SNMP\_Managers**, which is the source host group in Rule 250, or the rule can be edited to specify a different host group or IP address to configure the hosts that are allowed to send SNMP queries to the Brick.

The UDP port used by the SNMP agent on the Brick can be changed from port 161 via the Brick SNMP Agent options on the Brick Editor to a different port, but then this port specified in Rule 250 must also be manually changed, or another rule using the new port must be created in the Brick *firewall* zone ruleset to allow this traffic (refer to the procedure [“To Configure the SNMP on the Brick Feature”](#) (p. 15-10) for more details).

For details about how to create security rules, refer to the *SMS Policy Guide*.

### Configuring Brick IP address on the NMS

The SNMP monitoring system (NMS) must be configured with the IP address of each Brick to be contacted for SNMP data. The IP address to be used is the physical IP address of the Brick or one of its interfaces.

□

## To Configure the SNMP on the Brick Feature

---

### When to use

Use this procedure to enable or disable the SNMP agent on the Brick and configure the related options.

The Brick SNMP Agent options are set on the Options tab of the Brick Editor.

### Using the Configuration Assistant to set default values

Default settings for the SNMP on the Brick feature (Brick SNMP Agent port, read community string, system location, and system contact) can be set using the Configuration Assistant.

These default values will appear in the Brick SNMP Agent options on the Brick Editor when the SNMP Agent on the Brick is brought up or enabled for the first time on a Brick.

Refer to the *Using the Configuration Assistant* chapter for details on how to provision the SNMP Agent parameters.

### To enable/disable the SNMP agent on the Brick and configure related options

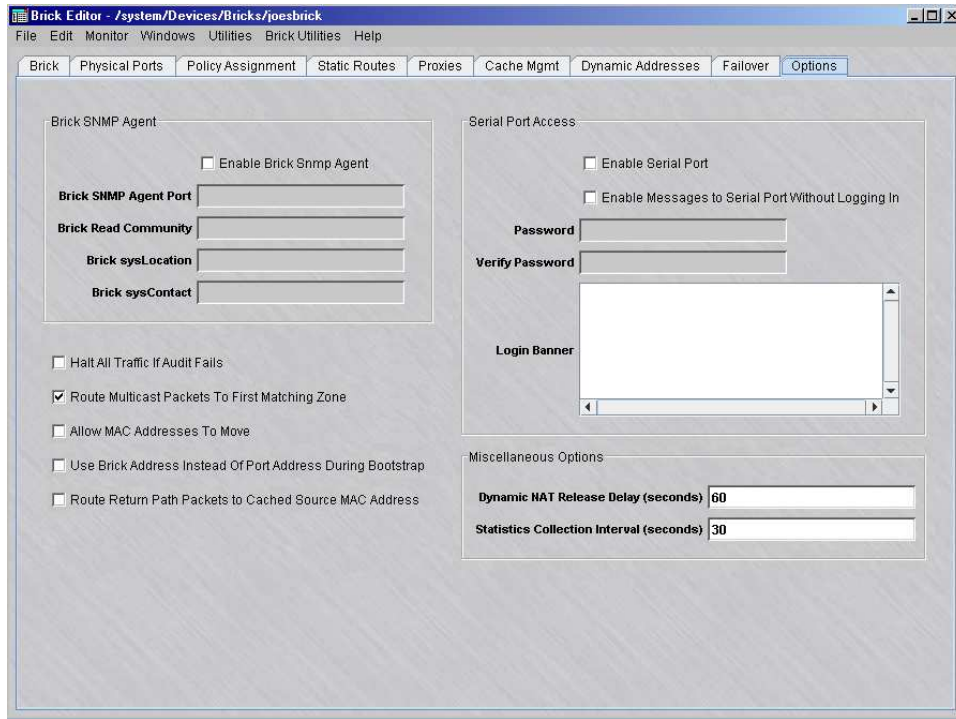
Complete the following steps to enable/disable the SNMP agent on the Brick and configure related options:

- 
- 1 Follow the steps in the procedure [“To configure basic information on the Brick tab”](#) (p. 3-23) in Chapter 3, [“Configuring and Activating an Alcatel-Lucent VPN Firewall Brick™ Security Appliance”](#) to configure the basic information for a Brick device.
- 

- 2 Click **Options** to display the Options tab of the Brick Editor.

The Options tab of the Brick Editor is displayed ([Figure 15-1, “Brick Editor \(Options Tab\)”](#) (p. 15-11)).

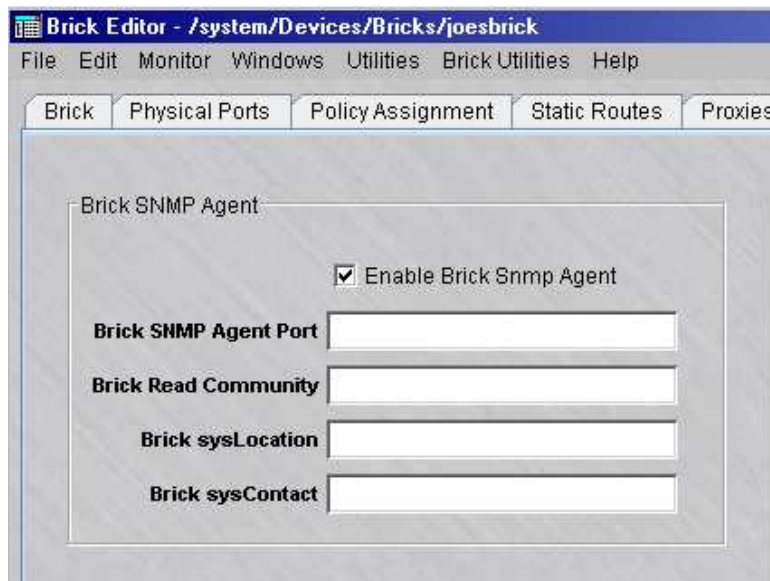


**Figure 15-1 Brick Editor (Options Tab)**

- 
- 3 Click the **Enable Brick Snmp Agent** checkbox to enable the SNMP on the Brick feature (to place a check in it). This feature is disabled by default. To disable the feature, click the checkbox again to remove the check.

**Result** If the SNMP on the Brick feature is enabled, the other fields in the Brick SNMP Agent portion of the tab are activated and available for input (Figure 15-2, “Brick Options Tab - SNMP Brick Agent Option Fields Activated” (p. 15-12)).

**Figure 15-2 Brick Options Tab - SNMP Brick Agent Option Fields Activated**



*Note: These fields will be initially populated with default values if they were previously entered on the SNMP Parameters window of the Configuration Assistant. Any default values entered can be changed on the Options tab for a Brick device.*

- 
- 4 Enter (or change) values for the following fields:
- **Brick SNMP Agent Port**— this field defines the UDP port that is used by the SNMP agent on the Brick to listen to SNMP requests for information from the Brick. The default port value is 161. Valid values are 1-65535. The pre-defined rule (Rule 250) in the Brick *firewall* zone ruleset is automatically configured to use port 161 (the default). If you configure the NMS to use a different port number for requests to the Brick SNMP agent, you must manually edit the port number in this rule or create a new rule in the *firewall* zone ruleset to allow SNMP traffic.
  - **Brick Read Community**— while the SNMP agent allows read-only access to the SNMP reporting information, this “community string” is used as an additional security mechanism to authenticate NMS hosts who access the Brick for SNMP data. The read-only community string is initially set to `public`.

- **Brick sysLocation**— this text field is used to populate the MIB-II *sysLocation* object.
  - **Brick sysContact**— this text field is used to populate the MIB-II *sysContact* object.
- 

- 5 Select **File** from the main menu bar and choose **Save and Apply** to activate SNMP on the Brick.

END OF STEPS

---





# Appendix A: Administer an Alcatel-Lucent *VPN Firewall Brick*<sup>TM</sup> Security Appliance Over the Internet from an Unregistered SMS

## Overview

---

### Purpose

This appendix explains how to enable an SMS with an unregistered IP address to administer a Brick over the Internet.

### Contents

<a href="#">Background</a>	<a href="#">A-2</a>
<a href="#">To Configure the Brick</a>	<a href="#">A-3</a>
<a href="#">To Assign the Administrative Zone and Enter a VBA</a>	<a href="#">A-4</a>
<a href="#">To Add NAT Rules to the administrativezone Ruleset</a>	<a href="#">A-5</a>
<a href="#">To Activate the Remote Brick</a>	<a href="#">A-8</a>



## Background

---

### Remote administration of Bricks

There are a number of circumstances in which an SMS with a private address might have to administer a Brick remotely over the Internet. For example, an SMS may have been initially set up to manage several Bricks that were connected directly to its ports. In this case, the private address would not prevent the SMS from communicating with these Bricks.

However, network growth could require the deployment of Bricks in other geographic locations. In this case, the SMS would need to use the Internet to administer these Bricks, and the unregistered address would be a problem.

The solution is to employ the Brick network address translation (NAT) capability to convert the private address of the SMS to a registered address that can be used on the Internet.

To do this, you must first obtain a registered IP address for the SMS to use. Once this is done you have to:

- Configure the remote Brick, making sure to enter the *registered* IP address as the SMS IP address instead of the private IP address that you have been using
- Assign the *administrativezone* ruleset to the port connecting the Brick to the SMS, and enter a virtual Brick address (VBA)
- Add three NAT rules to the *administrativezone* ruleset
- Modify the SMS host group to include the registered address you will now be using for the SMS
- Activate the remote Brick.

□

## To Configure the Brick

---

### Task

To configure the remote Brick, follow the steps below. (For a more detailed explanation of the configuration process, refer to [Chapter 3, “Configuring and Activating an Alcatel-Lucent VPN Firewall Brick™ Security Appliance”](#).)

---

- 1 From the Navigator window, right-click the Bricks folder and select **New** from the pop-up menu. The Brick Editor is displayed, with the Brick tab shown.
  - 2 Enter the Brick name, IP address and, if necessary, gateway IP address. The unregistered address you have been using will appear in the **SMS IP Address** field if this is a standalone SMS. Replace the unregistered address with the registered address.
  - 3 Open the File menu and select **Save** to save the configuration.
  - 4 Open the Brick Utilities men, and select **Make Brick Boot Media**. Follow the on-screen instructions to make a USB floppy disk or USB flash drive on the SMS host, or to package the files for remote floppy or USB flash drive creation. *However, do NOT load the USB floppy disk into the Brick until you are instructed to do so.*
- 

END OF STEPS

---

□

## To Assign the Administrative Zone and Enter a VBA

---

### When to use

The *administrativezone* ruleset is a pre-configured ruleset that allows the Bricks and SMS to communicate, while protecting the SMS from attack.

You will have to apply this ruleset to the port on the Brick that connects the Brick to the SMS. You will also have to create a Virtual Brick address (VBA) and make the VBA the registered address you will now be using for the SMS. Complete the following steps to do this:

- 1 With the Brick Editor displayed, click **Policy Assignment** to display the Policy Assignment tab.
- 2 Double-click the port connecting the Brick and SMS. Since this Brick will be administered remotely, that should be the port connected to the router that Brick will use to communicate with the SMS. The Brick Policy Assignment Editor is displayed.
- 3 In the **Zone Ruleset** field, select **administrativezone** from the drop-down list.
- 4 In the **Tunnel Endpoint Address/Virtual Brick Address** field, enter the registered IP address you will be using. If this is a standalone SMS, this must be the same address you entered in the **SMS IP Address** field when configuring the Brick.
- 5 Click **OK** to dismiss the Brick Policy Assignment Editor. You can ignore the other fields on the Brick Policy Assignment Editor for now.
- 6 Open the File menu and select **Save** to save the assignment.

END OF STEPS





## To Add NAT Rules to the *administrativezone* Ruleset

---

### When to use

Once the *administrativezone* ruleset has been assigned to a port and the VBA has been entered, you have to enable and edit three rules in the ruleset to perform the required address translation:

- Rule 209
- Rule 210
- Rule 211

The first rule (209) performs destination address mapping. These rules will instruct the Brick to map all inbound sessions destined for the VBA ( the registered IP address) to the unregistered IP address of the SMS.

The second and third rules (210, 211) perform source address mapping. These rules instruct the Brick to map the source address of all outbound sessions (the unregistered IP address) to the VBA, so that the return sessions automatically have the VBA as their destination.

### Task

To enable and edit these rules, follow the steps below. These rules will be made active in the *administrativezone* ruleset.

- 1 With the Navigator window displayed, click the appropriate Brick Zone Rulesets folder to display all existing Brick zone rulesets, and double-click **administrativezone**. The Brick Zone Ruleset Editor will appear, with the *administrativezone* rules displayed.
- 2 Double-click on Rule 209 in the rules table.

The Brick Zone Rule Editor is displayed with the Basic tab for Rule 209. Configure the rule as follows and make sure that it is active:

Direction	Source	Destination	Service	Action
In To Zone	brickRemoteAd- dresses	Virtual Brick Address	brick_to_SMS_ Services	Pass

*brickRemoteAddresses* is a host group that can be selected from the drop-down list in the **Source** field. *Virtual Brick Address* is a keyword that can be selected from the drop-down list in the **Destination** field. *brick\_to\_SMS\_Services* is a service group that can be selected from the drop-down list in the **Service or Group** field.

This rule will allow the Brick to send audit data to the SMS and request policy downloads from the SMS, using the registered address (the VBA) instead of the unregistered address that had been used previously.

- 3 Click **Address Translation** to display the Address Translation tab. Then, enter the SMS' unregistered IP address in the **Destination Address Mapping** box (you may leave the mapping type as pool). Click **OK** to dismiss the Brick Zone Rule Editor and return to the Basic Tab of the Brick Zone Ruleset Editor.

- 4 Double-click on Rule 210.

The Brick Zone Rule Editor is displayed with the Basic tab for Rule 210. Configure the rule as follows and make sure that it is active:

Direction	Source	Destination	Service	Action
Out of Zone	SMS	brickLocalAddresses	brick_from_SMS_Services	Pass

SMS is a host group that can be selected from the drop-down list in the **Source** field. *brickLocalAddresses* is a host group that can be selected from the drop-down list in the **Destination** field. *brick\_from\_SMS\_Services* is a service group that can be selected from the drop-down list in the **Service or Group** field.

This rule allows the SMS to upload policy and configuration information to the SMS, using the registered address (the VBA) instead of the unregistered address that had been used previously.

- 5 Double-click on Rule 211.

The Brick Zone Rule Editor is displayed with the Basic tab for Rule 211. Configure the rule as follows and make sure that it is active:

Direction	Source	Destination	Service	Action
In To Zone	brickRemoteAddresses	Virtual Brick Address	tcp/*/910	Pass

This is the same as the rule you just created, except that the service is different. The purpose of this rule is to allow policy download replies from the Brick to the SMS when the Clear Cache option is invoked.

You also have to perform the same destination address mapping for this rule that you did for the Rule 209. Open the Address Translation tab and enter the SMS unregistered IP address in the **Destination Address Mapping** box, as was done in Step 3.

.....

- 6 Click **Address Translation** to display the Address Translation tab. Then, select the key word **Virtual Brick Address** from the drop-down list in the **Source Address Mapping** box (you may leave the mapping type as pool). Click **OK** to dismiss the Brick Zone Rule Editor and return to the Basic Tab of the Brick Zone Ruleset Editor.
- .....

- 7 Open the File menu and select **Save and Apply**, and then dismiss the Brick Zone Ruleset Editor.

.....  
E N D O F S T E P S  
.....



## To Activate the Remote Brick

---

### Task

You are now ready to activate the Brick, using the USB flash drive or floppy you created on the SMS host or on a remote host. To do this, follow the steps below:

- 1 Insert the floppy disk into the disk drive of the Brick or USB flash drive into the USB port of the Brick.
- 2 Power up the Brick by toggling the Brick power switch. The configuration information on the disk will be transferred to the Brick flash disk. The transfer process takes about 2.5 minutes.
- 3 When the transfer is complete, remove the floppy disk from the disk drive and power the Brick off and on to boot the Brick from its flash disk. The Brick is now ready to be deployed.

**Important!** If additional Bricks will be administered by this SMS over the Internet, do the following:

1. Add the IP addresses of the new Bricks to the *BrickRemoteAddresses* host group.
2. Apply the policy to the new Brick.
3. Configure the new Brick, create a floppy or USB flash drive, and activate the Brick using the floppy or USB flash drive.

END OF STEPS

---



# Appendix B: Sizing Guidelines

## Overview

---

### Purpose

To determine the proper size of the PC or host machine that is required to efficiently run the SMS software, you need to understand the following:

- Resource utilization and behavior of the software
- Performance of the computer hardware
- Maximum user response time requirements
- How the system will be used.

### Contents

Sizing Tool	B-2
Determine CPU Capacity	B-4
Memory Utilization	B-6
Disk Capacity for Log Files	B-7
Disk Configuration	B-8



## Sizing Tool

---

### Purpose of sizing tool

The SMS includes a sizing tool that shows the current status of all SMS processes. This is a very useful tool to help size the capacity of the hardware the SMS is running on.

For example, if the amount of memory used for a particular service is nearing its maximum, you may need to go to the Tunable Parameters in the Configuration Assistant and increase the memory allocation for this service. For a more detailed discussion of the Configuration Assistant, see [Chapter 11, “Using the Configuration Assistant”](#) (in particular, ““TL1 Alarms” (p. 11-42)”).

### Sun®Solaris® and Linux Platform

On *Solaris*® and Linux server platforms, there are two versions of this tool, a graphical version and a command line version. The only difference between the two is that the information is presented in graphical format on the graphical version.

The invocation method for each version is as follows:

- *Command Line*  
To invoke the command line version, go to the directory `<ISMSHOME>` and enter `./lsmsStatus`
- *Graphical*  
To invoke the graphical version, display the **Desktop** menu, select **Utilities**, and select the tool, or go to the directory `<ISMSHOME>` and enter `./StartLSMSStatus`

### Microsoft®Windows® or Vista® Platform

On *Microsoft*®*Windows*® and *Microsoft*®**Vista** server platforms, only the graphical version of the tool is available. To invoke it, open the **START** menu, select **Utilities**, and select the tool.

### Contents

The command line and graphical versions of the tool provide the following information:

Field	Description
LSMS Service	Name of the SMS service
jre PID	Process ID of the service
Threads	Number of threads currently in the service

Field	Description
Active DB Conns	Current number of open database connections used by the service
Active Trans	Number of active database transactions in progress at the time the screen refreshed
Max Active Trans	Maximum number of active database transaction in progress at one time since the services were started
% CPU	Percent CPU utilization of this service
Maximum Heap	Maximum allocation for the heap memory of this service
Allocated Heap	Heap memory currently allocated by this service
Used Heap	Heap memory currently used by this service
Total CPU Time	Total CPU time used up by this service since it started
Last Started At	The last time this service was started (only available on graphical version)
Heap Snapshot At	Last time this service's allocated heap memory information was refreshed (only available on graphical version)

In addition, the tool also displays:

- Records logged by Brick devices to this SMS
- Number of Bricks connected to this SMS
- The time the SMS Status window was invoked (this window can remain up even if you've stopped services)
- The last time that the number of Bricks connected to this SMS changed.



## Determine CPU Capacity

---

### Overview

To determine the processor required by the SMS application, analyze the following choices and choose the one that has the highest value.

- *Windows*<sup>®</sup> or *Vista*<sup>®</sup>— 800 MHz Pentium processor, *Solaris*<sup>®</sup> — 500 MHz Sparc processor, Linux —2 GHz dual-core processor
- Calculate the result of this formula: (2 MHz \* the number of Bricks).  
For example, if you have 350 Bricks, then a machine offering 700 MHz may best suit your needs. Acquire a machine that provides this processing power (or comes the closest) and is available on the market today.
- Calculate the result of this formula:
  - *For Solaris, Sparc:* if you are using HTTP, then:  
CPU Speed (MHz) = (L \* 0.55) + (U \* 50) + (V \* 40\*) + (A \* 10)
  - *For Windows/Linux:* if you are using HTTP, then:  
CPU Speed (MHz) = (L \* 0.55) + (U \* 50) + (V \* 30\*) + (A \* 10)
  - *For Solaris, Sparc:*if you are using HTTPS, then:  
CPU Speed (MHz) = (L \* 0.55) + (U \* 133) + (V \* 40\*) + (A \* 10)
  - *For Windows/Linux:*if you are using HTTPS, then:  
CPU Speed (MHz) = (L \* 0.55) + (U \* 133) + (V \* 30\*) + (A \* 10)

\* If using RADIUS, Local Password, or SecurID, the number is 170. If using a digital certificate, this number then becomes 250.

where:

L = Total network traffic through all Bricks to be logged in megabits/second—e.g., 200.
---

U = User authentications per second during "busy" time.
---

V = VPN negotiations per second during "busy" time.
---

A = Maximum simultaneous Administrators logged in.
--

### Example

If your configuration includes 10 Bricks supporting 4 T3's and 12 T1's and each connection operates at an average of 50% utilization (full duplex), then the total network traffic is just under 200 Mbps.



User authentications and VPN negotiations include both initiated and failed. For this example, suppose you are using HTTPS and estimate 2 authentications per second and 1 VPN negotiation per second and you have two Administrators who can log in simultaneously.

In this example, the processor required for the machine running the SMS software is 566 MHz.

Since 566 MHz exceeds a 400 MHz Pentium II processor, acquire a machine that provides this processing power (or comes the closest) and that is available on the market today.

processor =  $(200 * 0.55) + (2 * 133) + (1 * 40) + (2 * 10)$  566 MHz = 110 + 266 + 40 + 20

## Summary

The above guidelines should be sufficient for most installations.

Naturally, they will depend on the amount of administrator activity and network traffic mix.

**Important!** *Logging DROPS only*

Logging dropped traffic only dramatically reduces the amount of log traffic. Many Administrators find this sufficient.



## Memory Utilization

---

### Overview

To determine the amount of RAM required by the machine running the SMS software, analyze the following choices and choose the one that has the highest value.

- 256 MB
- Calculate the result of this formula:  
Physical Memory (MB) =  $(170 + F/4) + (L * .05) + R/25 + (\# \text{ tunnels} * .004)$

where:

F = Number of Brick(s) in the network.
L = Network traffic through a Brick to be logged in megabits/second — Example: 200.
R = Number of routers.

### Example

If your configuration includes 10 Bricks supporting 4 T3's and 12 T1's and each connection operates at an average of 50% utilization (full duplex), then the total network traffic is just under 200 Mbps.

In this case, the memory required by the machine running the SMS software is **182.5 MB** =  $172.5 + 10$ .

If you are using Internet Explorer as your browser, assume you will need approximately 32 MB more of memory.

**Important!** *Virtual Memory*

Virtual memory should be at least twice the size of physical memory.



## Disk Capacity for Log Files

---

Use the following guidelines to determine how much disk space you need to allocate for the audit logs:

- Each log record occupies 120 bytes of disk space.
- Each megabit of traffic that is audited typically generates about 35 session records per second if every event is logged and there are no significant attacks.  
If the traffic travels through a VPN tunnel, an additional five records per second are audited.  
If only drops are audited, the session records will drop significantly.
- Each user authentication request generates 1 to 2 records.
- Each VPN session generates 2 to 6 records.
- Proactive monitoring traffic amounts to 20 records per Brick per minute, or about 2KB per Brick per minute.
- Allow an extra 10 percent to minimize fragmentation and an extra 10 percent for administrative events.



## Disk Configuration

---

Use the following chart for guidelines on how to configure your disk given a logging records-per-second range:

<b>Records per Second</b>	<b>Windows<sup>®</sup>, Vista<sup>®</sup>, Solaris<sup>®</sup> (May Require a tune of the file system), Linux</b>
< 30,000	Single drive
30,000 - 50,000	Logs should be configured on a separate physical disk from everything else - especially swap
50,000+	For logging rates about 50,000 records per second, a high performance disk subsystem is recommended, including disk arrays, high speed individual disks, and/or striping. This must be done with care as an inadequate disk subsystem can put the SMS in a state in which it cannot catch up with incoming data. Running frequent reports against session logs can greatly increase the load on the disk.

General disk configuration guidelines include:

- When the FTP scheduler is used at a high data rate, it should be scheduled either:
  - for times when no one is expected to be logged in
  - or
  - to run very frequently (every 1 to 2 minutes) so that the data is still in the memory cache.
- For rates above 30,000 records per second, faster disk drives are highly desirable (e.g., 10,000 RPM or better).
- Use defragmentation with care. Some tools may interfere with the normal operation of the SMS by running at too high a priority level.



# Appendix C: Changing the IP Address of the SMS

## Overview

---

### Purpose

This appendix explains how to change the IP address of the SMS on the *Windows*<sup>®</sup> *Vista*<sup>®</sup>, *Solaris*<sup>®</sup>, and Linux server platforms. A change in the IP address of the SMS may be necessary if you are rearranging the elements of your network.

A utility called *changeIP* simplifies the process. The procedure is the same for *Solaris*<sup>®</sup>, *Windows*<sup>®</sup>, and *Vista*<sup>®</sup> server platform SMSs. However, the steps differ slightly, depending on whether the SMS is a Primary SMS or part of a redundant SMS pair.

Follow the procedures exactly as described in this appendix, and you will not have to reboot Brick devices or interrupt service to your user community.

### Contents

To Change the IP Address of an SMS (Primary SMS Only)	C-2
To Change the IP Address of a Primary SMS (Primary/Secondary SMS Pair)	C-4
To Change the IP Address of a Secondary SMS (Primary/Secondary SMS Pair)	C-6
After the Update	C-8



## To Change the IP Address of an SMS (Primary SMS Only)

---

### Task

Complete the following steps to change the IP address of a Primary SMS. To perform this procedure, you must log into the SMS Navigator *directly from the SMS host for which the IP address change will be made*.

---

- 1 In the Folder panel of the Navigator, open the **Bricks** folder to display the list of currently configured Bricks in the Contents panel.
- 

- 2 Right-click on a Brick and select **Edit**.

**Result** The Brick Editor is displayed.

---

- 3 In the Home LSMS/LSCS Priority table, double-click on the Primary SMS.

**Result** The LSMS/LSCS Priority Editor is displayed.

---

- 4 In the **LSMS/LSCS IP Address** field, change the IP address shown to the new IP address and click **OK**.

**Result** The system returns to the Brick Editor.

---

- 5 From the File menu, select **Save and Apply** to save and apply the changes to the Brick.

**Result** A warning dialog box is displayed, indicating that there is No LSMS at this address.

---

- 6 Click **OK** to acknowledge the warning message.

If there are multiple Bricks, repeat steps 2 through 6 until all Bricks have been modified. *If there are multiple Bricks, change the Brick that is directly in front of the SMS last.*

---

- 7 In the Folders panel, open the **LSMSs and LSCSs**. In the Contents panel, right-click on the SMS to be changed and select **Change LSMS IP Address**.

**Result** A warning dialog box is displayed.

.....

- 8 Click **Yes** to acknowledge the warning message.

**Result** The Change LSMS IP Address dialog box is displayed.

.....

- 9 In the **New LSMS IP Address** field, enter the new IP address of the SMS.
- .....

- 10 Click **OK** to save the IP address change.

**Result** A dialog box is displayed, indicating that the SMS IP address change has taken effect.

.....

- 11 Click **OK** to acknowledge the message.
- .....

- 12 Exit the SMS Navigator.
- .....

- 13 Stop the SMS Services.
- .....

- 14 Change the IP address of the SMS host network interface card so it can communicate with the Brick.
- .....

- 15 Start the SMS Services.
- .....

- 16 Reboot all Bricks.

END OF STEPS

.....



## To Change the IP Address of a Primary SMS (Primary/Secondary SMS Pair)

---

### Task

Complete the following steps to change the IP address of a Primary SMS in a Primary SMS/Secondary SMS pair. To perform this procedure, you must log into the SMS Navigator *directly from the SMS host for which the IP address change will be made.*

---

- 1**     **Important!** *The procedure assumes that Brick devices that are connected to this SMS are rehomed to the Secondary SMS while the Primary SMS IP address is being modified. In any case, where a Brick device is homed solely to the Primary SMS, and cannot rehome to the Secondary SMS, the Brick device must be re-flopped after changing the IP address.*

*On the Primary SMS:*

In the Folders panel, open the **LSMSs and LSCSs**. In the Contents panel, right-click on the SMS to be changed and select **Change LSMS IP Address**.

**Result** A warning dialog box is displayed.

---

- 2**     Click **Yes** to acknowledge the warning message.

**Result** The Change LSMS IP Address dialog box is displayed.

---

- 3**     In the **New LSMS IP Address** field, enter the new IP address of the SMS.
- 

- 4**     Click **OK** to save the IP address change.

**Result** A dialog box is displayed, indicating that the SMS IP address change has taken effect.

---

- 5**     Exit the SMS Navigator.
- 

- 6**     Stop the SMS Services.



**Result** When the SMS Services are stopped, any Bricks "homed" to the Primary SMS for which the address is being changed will lose contact and "rehome" to the Secondary SMS in the redundant pair.

---

- 7 Change the IP address of the SMS host network interface card so it can communicate with the Brick(s).
- 

- 8 Start the SMS Services.

**Result** If the Primary SMS for which the address has been changed is the higher-priority SMS in the redundant pair, the Brick(s) will now "rehome" to this SMS when the SMS Services are re-started.

---

- 9 Run the AllowSecondarySetup utility on the Primary SMS.

For details about the AllowSecondarySetup utility, refer to the *SMS Tools and Troubleshooting Guide*.

---

- 10 *On the Secondary SMS:*

1. Stop the SMS Services.

2. Run the dbsetup utility.

For details about the dbsetup utility, refer to the *SMS Tools and Troubleshooting Guide*.

3. Start the SMS Services.

END OF STEPS

---



## To Change the IP Address of a Secondary SMS (Primary/Secondary SMS Pair)

---

### Task

Complete the following steps to change the IP address of a Secondary SMS in a Primary SMS/Secondary SMS pair. To perform this procedure, you must log into the SMS Navigator *directly from the SMS host for which the IP address change will be made*.

---

- 1**     **Important!** *The procedure assumes that Brick devices that are connected to this SMS are rehome to the Secondary SMS while the Primary SMS IP address is being modified. In any case, where a Brick device is homed solely to the Primary SMS, and cannot rehome to the Secondary SMS, the Brick device must be re-flopped after changing the IP address.*

*On the Primary SMS:*

In the Folders panel, open the **LSMSs and LSCSs**. In the Contents panel, right-click on the SMS to be changed and select **Change LSMS IP Address**.

**Result** A warning dialog box is displayed.

---

- 2**     Click **Yes** to acknowledge the warning message.

**Result** The Change LSMS IP Address dialog box is displayed.

---

- 3**     In the **New LSMS IP Address** field, enter the new IP address of the SMS.
- 

- 4**     Click **OK** to save the IP address change.

**Result** A dialog box is displayed, indicating that the SMS IP address change has taken effect.

---

- 5**     Apply all Bricks.
- 

- 6**     Run the AllowSecondarySetup utility on the Primary SMS.

For details about the AllowSecondarySetup utility, refer to the *SMS Tools and Troubleshooting Guide*.

---

**7** *On the Secondary SMS:*

1. Stop the SMS Services.
  2. Change the IP address of the SMS host network interface card so it can communicate with the Brick(s).
  3. Run the changeIP utility and enter the new IP address for the Secondary SMS. For details about the changeIP utility, refer to the *SMS Tools and Troubleshooting Guide*.
  4. Run the dbsetup utility. For details about the dbsetup, refer to the *SMS Tools and Troubleshooting Guide*.
- 

**8** Change the IP address of the SMS host network interface card so it can communicate with the Brick(s).

---

**9** Start the SMS Services.

**Result** If the Primary SMS for which the address has been changed is the higher-priority SMS in the redundant pair, the Brick(s) will now "rehome" to this SMS when the SMS Services are re-started.

---

**10** Run the AllowSecondarySetup command on the Primary SMS.

For details about the AllowSecondarySetup command, refer to the *SMS Tools and Troubleshooting Guide*.

---

**11** *On the Secondary SMS:*

1. Stop the SMS Services.
2. Run the dbsetup command. For details about the dbsetup command, refer to the *SMS Tools and Troubleshooting Guide*.
3. Start the SMS Services.

END OF STEPS

---



## After the Update

---

### Post-update activities

Once you have updated the Bricks and the SMS database and the SMS services have been restarted, what else needs to be done?

The remaining things to be done are:

- **Primary SMS** — Once services have been restarted, the Bricks that are normally "homed" to the Primary SMS should start "rehomeing" from the Secondary SMS to the primary. This will depend on the settings on the Brick under **LSMS/LSCS Rehome Options** on the Brick tab of the Brick Editor.  
In addition, the database on the Primary SMS can no longer synchronize with the database on the Secondary SMS. On the Secondary SMS, from the SMS installation directory, you must run a `dbsetup`. This will reinitialize the database on the secondary and copy the database from the primary to the secondary.  
For more information on the `dbsetup` utility, refer to the *Database Utilities* chapter in the *SMS Tools and Troubleshooting Guide*.
- **Secondary SMS**— Once services have been restarted, the Bricks that are normally "homed" to the Secondary SMS should start "rehomeing" from the Primary SMS to the Secondary SMS. This will depend on the settings on the Brick under **LSMS/LSCS Rehome Options** on the Brick tab of the Brick Editor.  
The database on the secondary will automatically update the database on the primary with the change to its SMS IP address.

□

# Appendix D: Support for Non-IP Protocols

## Overview

---

### Purpose

The Alcatel-Lucent *VPN Firewall Brick*<sup>™</sup> Security Appliance is originally designed to work with IP packets. Information within the IP packet is used to make access control decisions, such as whether or not to allow this packet to pass through the Brick.

In addition to handling IP packets, a Brick can be also be configured to pass packets from non-IP protocols, for example, AppleTalk, Novell IPC, and Decnet/LAT. For example, you may have a Brick between an Apple client and server that need to talk to one another.

### Non-IP protocol packets

#### **Important! CAUTION**

Filtering is not performed on these individual packets. Either they ALL are entirely allowed or denied.

To pass non-IP protocol packets, you need to edit a file on the SMS host. The file then needs to be applied to the Brick that will be passing the non-IP packets.

### Contents

<a href="#">Ethertype and DSAP Files</a>	<a href="#">D-2</a>
<a href="#">Procedure for Passing Non-IP Packets</a>	<a href="#">D-3</a>



## Ethertype and DSAP Files

---

### Non-IP protocol file editing

To support the passing of non-IP protocols, you need to edit one or both of these files:

- *ethertype*  
The *ethertype* file is used to support EV2 ethertype protocols. These protocols are represented by a four-digit hexadecimal number.
- *dsap*  
The *dsap* file supports 802.2 DSAP protocols. These protocols are represented by a two-digit hexadecimal number.

### File Location

For each Brick in your network, the *ethertype* and *dsap* files reside in a folder under the root installation directory.

- On *Windows*<sup>®</sup> and *Vista*<sup>®</sup> typically the folder is:  
`c:\isms\lmf\firewalls\Brick_name`
- On *Solaris*<sup>®</sup> and Linux, typically the folder is:  
`/opt/isms/lmf/firewalls/Brick_name`

### Obtain Hexadecimal Number

Before editing the *ethertype* or *dsap* file, you need to identify the hexadecimal number that represents the protocol you need to support. You can either:

- Access this URL to obtain a current list of ethertypes:  
<http://www.iana.org>  
The reference for this site is RFC 1700, "Assigned Numbers", J. Reynolds, J. Postel, October 1994.
- Attach a packet sniffer to your network and examine the packets that are generated when attempting to pass packets of the protocol.



## Procedure for Passing Non-IP Packets

---

### Task

To pass non-IP protocol packets (for example, AppleTalk packets), you must:

---

- 1 Edit a file named *ethertype* on the SMS. Save and exit the file.
  - 2 Apply the changes to the Brick. Refer to [Chapter 3, “Configuring and Activating an Alcatel-Lucent VPN Firewall Brick™ Security Appliance”](#) for details on applying changes to a Brick.
- 

END OF STEPS

---

### Edit ethertype File on LSMS

Use the following procedure to edit a file so that the Brick will pass AppleTalk packets:

---

- 1 For each Brick that needs to pass non-IP protocol packets, you need to navigate to a folder under the installation root directory folder.
    - On *Windows*® and *Vista*® typically the folder is:  
*c:\isms\lmf\firewalls\<Brick\_name>*
    - On *Solaris*® and Linux, typically the folder is:  
*/opt/isms/lmf/firewalls/<Brick\_name>*
  - 2 Open the *ethertype* file with an ASCII editor on the platform you are using, for example, Notepad on *Windows*® or *Vista*®, or *vi* on *Solaris*® and Linux.
  - 3 To support AppleTalk packets, enter the following two four-digit hexadecimal numbers on separate lines in the *ethertype* file:
- 

809B

80F3

**Important!** *DSAP Values*

Since AppleTalk generates AA DSAP types, you do not need to edit the dsap file. This applies to all non-IP protocols that generate AA types for ethertypes 0x5FE or greater. For these ethertypes or for any other DSAP other than AA, you must explicitly enter them in the dsap file in the format dsap, ethertype1, ethertype2, etc.

---

4 Save and exit the file.

---

5 Repeat Steps 1 - 4 for each Brick that needs to pass AppleTalk packets.

---

END OF STEPS

---

### Apply Changes to the Brick

Perform the steps below to load the new configuration information to a Brick:

---

1 Log onto the SMS host.

For details, refer to *Chapter 2. Getting Started*.

---

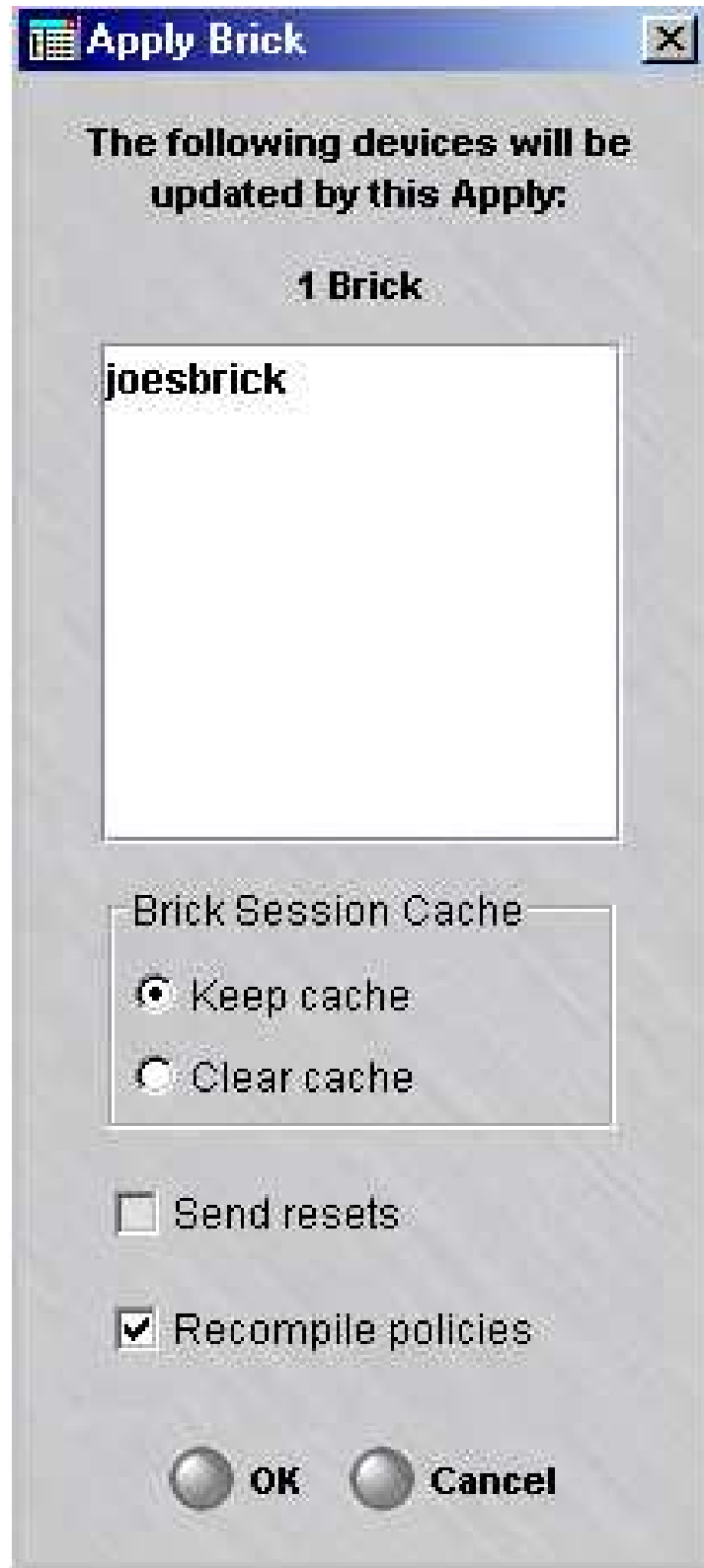
2 If the Brick is currently displayed in the Brick Editor, display the Utilities menu and select **Brick ► Apply**.

If the Bricks are displayed in the Navigator window, right-click the Brick you want and click **Apply** from the pop-up menu.

The Apply Brick window will appear. It is shown in Figure D-1. Note that the Brick you are applying (updating) appears in the left panel on top.



Figure D-1 Apply Brick Window



- 
- 3** When performing the apply, you have the option of keeping or clearing the Brick session cache. The default is to keep the cache. To clear the cache, click the **Clear Cache** radio button.

If you decide to clear the cache, you will terminate any client tunnels currently established to this Brick. You will have to contact the client users and instruct them to re-enable their tunnels.

You could also disrupt some sessions in progress, for example, FTP sessions or sessions allowed by rules with dependency masks.

- 
- 4** You have the option of recompiling the policies associated with this Brick before applying the Brick. The default is to recompile the policies. If you do not want to recompile them, uncheck the **Recompile Policies** checkbox.

If you recompile the policies, all changes to the policies will be applied to the Brick. Therefore, if you want to update the Brick configuration, but *not apply any policy changes at this time*, uncheck the **Recompile Policies** checkbox.

- 
- 5** When you are ready to begin the apply, click **OK** to dismiss the Apply Brick window. The apply will take place.

- 
- 6** Repeat steps 2 - 5 for each Brick that needs to pass non-IP protocol packets.

END OF STEPS



# Appendix E: VPN Firewall Solution Ports

## Overview

---

### Purpose

This appendix provides a list of ports that are used by various components of the VPN Firewall Solution (SMS, Alcatel-Lucent *VPN Firewall Brick*<sup>™</sup> Security Appliance, client server, SMS Remote Navigator) to communicate with each other.

### Ports used by VPN Firewall Solution

The following table is a list of ports that are used by various components of the VPN Firewall Solution to communicate with each other.

Destination Port	Protocol	Service	Configurable?	Initiator/Receiver	Description
900	TCP	administration	no	Brick -> SMS	Updates, "save and apply" configuration changes, etc.
910	TCP	administration	no	SMS -> Brick	Configuration updates
911	TCP	VPN client authentication	no	Brick -> SMS	VPN client authentication
1024	UDP	administration	no	SMS -> Brick	Configuraton updates
7000	TCP	administration	no	client -> SMS	Remote Navigator GUI (SMS)
9000	TCP	audit	no	Brick -> SMS	Log information, heartbeats, RADIUS, etc.
9041	TCP	administration	no	client -> SMS	Remote Navigator GUI (SMS)
n/a	ICMP	audit	no	SMS -> Brick	ping

Destination Port	Protocol	Service	Configurable?	Initiator/Receiver	Description
7001	TCP	administra- tion	yes	SMS -> SMS	Application-level communication channel between Primary, Secondary SMS and Compute Servers
8161	UDP	patrol-snmp	yes	client -> SMS	Used as the alternate SNMP port for this configuration because a system SNMP agent was running on the default SNMP port 161
9004	TCP	audit	yes	client -> SMS	Application-level internal audit
9007	TCP	administra- tion	no	SMS -> SMS	Used by internal User Authentication Engine
9008	TCP	administra- tion	no	SMS -> SMS	Used by internal User Authentication Engine
9009	TCP	administra- tion	no	SMS -> SMS	Used by internal scheduling application
9011	TCP	administra- tion	yes	SMS -> SMS	Internal Firewall Access Control Application
9012	TCP	administra- tion	yes	SMS -> SMS	Internal Firewall Access Control Application
9019	TCP	administra- tion	yes	SMS -> SMS	used by Command Line Interface
9090	TCP	Synchroniza- tion	yes	SMS -> SMS	Application level communication channel between Primary, Secondary SMS and Compute Servers

Destination Port	Protocol	Service	Configurable?	Initiator/Receiver	Description
9091	TCP	Synchroniza- tion	yes	SMS -> SMS	Application level communication channel between Primary, Secondary SMS and Compute Servers
9092	TCP	Synchroniza- tion	yes	SMS -> SMS	Application level communication channel between Primary, Secondary SMS and Compute Servers

**Notes:**

1. Traffic on all ports is bidirectional.
2. Port is no longer used.





# Appendix F: New Feature Setup

## Overview

---

### Purpose

By default, when you purchase SMS R9.4, your installation key(s) will provide you with the ability to manage up to five Alcatel-Lucent *VPN Firewall Brick™* Security Appliances as well as up to 100 Alcatel-Lucent IPSec Client users.

If you wish to expand the number of Bricks or IPSec users to be managed through your SMS, you must purchase a separate options license key. Certain optional features may require a separate license key to be installed in order to activate the feature(s).

The New Feature Setup utility allows an administrator to install a new key to provide additional SMS management capacity or new optional features as required.

### Contents

<a href="#">Determining Current SMS Feature Setup</a>	<a href="#">F-2</a>
<a href="#">To Use the New Feature Setup Utility</a>	<a href="#">F-3</a>



## Determining Current SMS Feature Setup

---

### Overview

To determine how many licenses that you currently have, open the SMS Navigator or SMS Remote Navigator. Then, choose **Help** from the menu bar and click **About** from the list of options. The screen that is displayed shows the SMS software version, the Brick software version, and an Enabled Features section, indicating the number of Alcatel-Lucent IPsec Client users and Bricks that your SMS can currently manage. Additional application information such as the SMS name, SMS type (such as Primary SMS), and installation key is also shown in the window.





## To Use the New Feature Setup Utility

---

### Task

Once you have purchased the additional key, follow the instructions below:

---

- 1 Obtain an installation key by registering your new feature option license key. Contact your Alcatel-Lucent customer support team representative for information about how to register license keys. To register your license key you will need to know the Installation Key for your Primary SMS that is displayed in the LSMS Editor.  

---
- 2 After obtaining the installation key, return to the SMS console and bring up **New Feature Setup**.
  - For *Windows*<sup>®</sup> and *Vista*<sup>™</sup> users, click **Start => Programs => Alcatel-Lucent Security Management Server => Utilities => New Feature Setup**  
The New Feature Setup window is displayed.
  - For *Solaris*<sup>®</sup> and Linux users, "cd" to your SMS installation directory (default choice is */opt/isms/lmf*), and type:  
*./newFeatureSetup*  
The New Feature Setup window is displayed.  

---
- 3 Click on the **Enter New Key** button  
**Result** The Enter New Option Key window is displayed.  

---
- 4 In the **Install Key** field, enter the new key.  

---
- 5 Click the **OK** button.  
**Result** The new license limits and/or installed feature(s) are displayed on the New Feature Setup window.

If your entered options key is not accepted, it is usually because the key was not registered for the proper SMS. When registering your options key, make sure that the **Installation Key** field in the LSMS / Compute Servers Editor for the Primary SMS matches the Primary SMS Installation Key on the registration website or the one that you provided to your customer support representative.

END OF STEPS

---

□



# Index

- A** Activate
  - Brick device, [3-52](#)
  - Activate a Brick, [3-63](#)
  - Add
    - Static route, [4-34](#)
  - Admin ID, [1-4](#), [1-8](#), [10-14](#)
  - Administer a brick over the Internet from an unregistered SMS, [A-1](#)
  - Administer a Brick over the Internet from an unregistered SMS, [A-8](#)
    - Activate the remote brick, [A-8](#)
    - Add NAT rules to the administrativezone ruleset, [A-5](#)
    - Assign the Administrative Zone, [A-4](#)
    - Configure the Brick, [A-3](#)
    - Enter a VBA, [A-4](#)
  - Administrator account
    - Create, [8-10](#)
    - Delete, [8-24](#)
    - Edit, [8-21](#)
    - Explained, [8-1](#)
    - Maintain, [8-21](#)
  - Administrators & LSMS window, [14-14](#), [14-19](#)
  - Alarms parameters, [11-9](#)
  - Alcatel-Lucent Netcare Professional Services, [xxv](#)
  - ALG
    - See: Application Layer Gateway (ALG)
  - Allow MAC addresses to move, [3-34](#)
  - AppleTalk, [D-1](#)
  - Application Layer Gateway (ALG)
    - Brick device as, [3-10](#)
  - Apply, [1-33](#), [1-33](#), [1-33](#), [1-34](#)
    - Brick, [5-7](#)
    - How to apply, [1-34](#)
    - What to apply, [1-33](#)
    - When to apply, [1-33](#)
  - Assign
    - Groups, [8-17](#)
  - Assign multiple rulesets to a port, [4-18](#)
  - Assign the same VBA to multiple ports, [4-19](#)
  - Audience
    - Audience:Network Administrators, [xxi](#)
- B** Backing up and restoring data, [12-1](#), [12-12](#)
  - Automatic backup, [12-2](#)
  - Manual backup, [12-3](#), [12-3](#)
  - Restore scenarios, [12-11](#)
  - Restoring data, [12-7](#), [12-9](#)
- Base station router (BSR), [3-7](#)
- BPG
  - See: BSR Packet Gateway (BPG) feature
- Brick
  - rehomeing options, [2-7](#)
- Brick device failover, [3-38](#)
- Brick device redundancy
  - See: Brick failover
- Brick devices
  - supported, [xxiv](#)
- Brick failover
  - manually initiate, [3-48](#)
  - migrate Model 1100 Bricks to Model 1200 Bricks in a failover pair, [3-50](#)
  - primary Brick and, [3-40](#)
  - set up, [3-42](#)
- Brick serial port
  - activate login banner, [4-41](#)

Brick Status windows, [14-19](#), [14-35](#)

- Brick lists, [14-19](#)
- Single Brick Bandwidth Statistics window, [14-32](#)
- Single Brick Ports window, [14-28](#)
- Single Brick Status window, [14-24](#)

Bricks

- activate, [3-52](#)
- Apply changes, [5-7](#)
- boot, [3-62](#)
- Bridge or router, [3-2](#)
- Configuration options, [3-32](#)
- Configure a physical port, [4-3](#)
- Configuring, [3-1](#), [4-1](#)
- configuring, [5-1](#)
- Configuring, [5-29](#)
- configuring the SNMP on the Brick feature, [15-10](#)
- Delete, [5-11](#)
- Directly connected to the SMS, [3-2](#)
- disable BPG feature, [4-21](#)
- disable BVG feature, [4-21](#)
- Download software, [5-24](#)
- enable BPG feature, [4-21](#)
- enable BVG feature, [4-21](#)
- failover, [3-38](#)
- Firewall, [3-4](#)
- heartbeat messages and, [3-38](#)
- Intelligent cache management, [4-1](#)
- Make floppy, [3-57](#)

- Modify, [5-6](#)
- Move, [5-12](#)
- Reboot, [5-13](#)
- Refresh the MAC Table, [5-16](#)
- status, [14-16](#)
- Tunnel endpoint, [3-5](#)
- user-defined fields for, [3-19](#)
- view snapshot of configuration, [5-3](#)

Bricks host group, [8-3](#)

BSR

- See: Base station router (BSR)

BSR Packet Gateway (BPG) feature, [3-7](#)

- disable, [4-21](#)
- enable, [4-21](#)

BSR Voice Gateway (BVG) feature, [3-7](#)

- configuring Quality of Service (QoS) parameters, [4-27](#)
- disable, [4-21](#)
- enable, [4-21](#)
- Real Time Protocol (RTP), [4-27](#)

Buttons, [1-16](#)

- Editing buttons, [1-16](#)
- Tunnel buttons, [1-17](#)

.....

**C** Change the IP address of the SMS, [C-1](#), [F-1](#)

Compute servers

- redundancy and, [2-2](#)
- status, [14-16](#)

Concurrency control, [1-36](#)

- enable, [1-37](#), [1-39](#)
- Force a logout of administrator, [1-41](#)
- force logout of an administrator, [1-38](#)
- lock status timeout, [1-37](#)

Configuration Assistant, [11-1](#), [11-29](#), [11-44](#)

- Alarms parameters, [11-9](#)
- Direct paging parameters, [11-13](#)
- FIPS parameters, [11-15](#)
- Log files parameters, [11-19](#)
- Log transfer parameters, [11-22](#)
- LSMS server parameters, [11-27](#)
- set parameters using, [11-6](#)
- SNMP agent parameters, [11-31](#)
- Software download parameters, [11-34](#)
- Start Configuration Assistant from the LSMS host, [11-3](#)
- strong passwords feature, [11-40](#)
- User authentication parameters, [11-46](#)
- View parameters, [11-7](#)

Configuration options, [3-32](#)

- Allow MAC addresses to move, [3-34](#)
- Halt all traffic if audit fails, [3-33](#)
- NOC Gateway, [3-34](#)
- Route multicast packets to first matching zone, [3-34](#)

- Configure a physical port, [4-3](#), [4-9](#)
- Configuring, [3-1](#)
- Configuring Brick devices, [5-1](#)
- Configuring Bricks, [4-1](#), [5-29](#)
- Configuring bricks
  - Configurations options, [3-32](#)
- Configuring Bricks
  - dynamic addressing options, [3-31](#)
  - Primary SMS, [3-23](#)
- Console Alarms window, [14-35](#)
- Contents panel, [1-11](#)
- CPU capacity, [B-4](#)
- Create
  - Administrator accounts, [8-10](#)
  - Groups, [8-5](#)

---

- D** Decnet/LAT, [D-1](#)
- Delete
  - Administrator account, [8-24](#)
  - Brick, [5-11](#)
  - Group, [8-8](#)
  - Policy assignment, [4-20](#)
  - Static route, [4-40](#)
- Direct paging parameters, [11-13](#)
- Disk capacity for log files, [B-7](#)
- Download software to a Brick, [5-24](#)
- dsap file, [D-2](#)

---

- E** Edit
  - Administrator account, [8-21](#)
  - Group, [8-7](#)

---

- Editing buttons, [1-16](#)
- Enable
  - strong passwords feature, [11-40](#)
- ethertype file, [D-2](#)

---

- F** Failover
  - Brick heartbeat messages and, [3-38](#)
- Federal Information Processing Standards (FIPS), [11-15](#)
- Find IP Address tool, [1-29](#)
- Find Name tool, [1-23](#)
- FIPS
  - See: Federal Information Processing Standards (FIPS)
- FIPS parameters, [11-15](#)
- Folders, [1-20](#)
  - Of a group, [8-2](#)
- Folders panel, [1-8](#)
- Force a logout of administrator, [1-41](#)
- Force logout of an administrator, [1-38](#)

---

- G** Group
  - Create, [8-5](#)
  - Defined, [8-2](#)
  - Delete, [8-8](#)
  - Edit, [8-7](#)
  - Folders, [8-2](#)
  - Subfolders, [8-2](#)
- Group administrator, [8-3](#), [8-9](#)
  - Privileges, [8-3](#), [8-17](#)
- Group Administrators, [1-8](#)

---

- Groups, [1-20](#)
  - Assign privileges, [8-17](#)
  - Maintain, [8-7](#)
  - New, [8-3](#)

---

- H** Halt all traffic if audit fails, [3-33](#)
- Halt Logging if Log Full checkbox, [11-21](#)
- Heartbeat messages
  - redundant SMS configuration, [2-6](#)
- Heartbeats
  - SMS Failover, [2-6](#)
- Host group
  - Bricks, [8-3](#)

---

- I** Intelligent cache management, [4-1](#)
  - Set the threshold levels, [5-30](#)

---

- L** Log files
  - Disk capacity, [B-7](#)
- Log files parameters, [11-19](#)
- Log in, [1-2](#), [1-3](#), [1-4](#), [1-4](#), [10-15](#)
  - Log in from a remote host, [1-4](#)
  - Log in from the SMS host, [1-3](#)
  - Status monitor only login, [1-4](#), [10-15](#)
- Log off, [1-2](#)
- Log transfer parameters, [11-22](#)

Login banner  
 Brick serial port, [4-41](#)  
 LSMS Administrators, [1-8](#)  
 LSMS host, [10-14](#)  
 LSMS web parameters, [11-27](#)  
 .....

**M** Maintain  
 Administrator accounts, [8-21](#)  
 Groups, [8-7](#)  
 Make floppy, [3-57](#)  
 SMS host, [3-57](#)  
 Management Information Base (MIB), [15-2](#)  
 Media Gateway (MGW), [3-10](#)  
 Memory utilization, [B-6](#)  
 Menu bar, [1-13](#)  
 Messages  
 send to administrators, [8-25](#)  
 mgmt-tunnel ruleset, [8-3](#)  
 MGW  
 See: Media Gateway (MGW)  
 Modem port, [11-13](#)  
 Modify  
 Brick, [5-6](#)  
 Policy assignment, [4-19](#)  
 Static route, [4-38](#)  
 Mouse actions, [1-16](#)  
 Move  
 Brick, [5-12](#)  
 .....

**N** Navigator  
 Status Monitor via, [14-2](#)

Navigator window, [1-8](#)  
 Contents panel, [1-11](#)  
 Folders panel, [1-8](#)  
 Network administrators, [xxi](#)  
 New feature setup, [2-3, F-1](#)  
 New groups, [8-3](#)  
 New Office Environment (NOE) phone device, [3-10](#)  
 NOC Gateway, [3-34](#)  
 nocgwzone, [8-3](#)  
 Non-IP protocols, [D-1](#)  
 Non-IP Protocols, [D-4](#)  
 Non-IP protocols  
 Edit the ethertype and dsap files, [D-2](#)  
 Novell IPC, [D-1](#)  
 .....

**P** Parameters  
 Alarms, [11-9](#)  
 Direct paging, [11-13](#)  
 FIPS, [11-15](#)  
 Log files, [11-19](#)  
 Log transfer, [11-22](#)  
 LSMS web, [11-27](#)  
 Reports, [11-29](#)  
 SNMP agent, [11-31](#)  
 Software download, [11-34](#)  
 Tunable, [11-44](#)  
 User authentication, [11-46](#)  
 Ports, [4-3, 4-9, 4-18, 4-19, 4-19, 4-20, 4-20](#)  
 Assign a security policy, [4-9](#)  
 Assign multiple rulesets, [4-18](#)

Assign the same VBA to multiple ports, [4-19](#)  
 configure, [4-3](#)  
 Delete a policy assignment, [4-20](#)  
 disable the BPG feature, [4-21](#)  
 disable the BVG feature, [4-21](#)  
 enable the BPG feature, [4-21](#)  
 enable the BVG feature, [4-21](#)  
 Modify a policy assignment, [4-19](#)  
 Re-order the policy assignment entries, [4-20](#)  
 SMS application, [E-1](#)  
 Primary Brick  
 failover and, [3-40](#)  
 Primary SMS  
 installation, [2-3](#)  
 Privileges  
 Of a group administrator, [8-17](#)  
 .....

**R** Real Time Protocol (RTP)  
 and BVG feature, [4-27](#)  
 Reboot a Brick, [5-13](#)  
 Redundancy  
 Compute servers and, [2-2](#)  
 load sharing, [2-6](#)  
 Logging and, [2-8](#)  
 monitoring and, [2-8](#)  
 SMS, [2-1](#)  
 Redundancy, Brick device  
 See: Brick device failover

- Refresh the MAC Table, [5-16](#)
- Remote administration, [10-14](#), [10-14](#)
  - Create the host group, [10-11](#)
  - Create the rules, [10-12](#)
  - Prepare the remote host, [10-11](#)
- Remote login See Remote administration, [10-10](#)
- Remote Navigator
  - Status Monitor via, [14-2](#)
- Reports parameters
  - Reports parameters, [11-29](#)
- Restoring data, [12-1](#)
- Route multicast packets to first matching zone, [3-34](#)
- RTP
  - See: Real Time Protocol (RTP)
- ruleset
  - mgmt-tunnel, [8-3](#)
- .....
- S** Sarbanes-Oxley (SOX) password compliance
  - enable password restrictions for, [11-40](#)
- Secondday SMS
  - installation, [2-3](#)
- See Backing up and restoring data, [12-1](#)
- Set
  - Alarms parameters, [11-9](#)
  - Direct paging parameters, [11-13](#)
  - FIPS parameters, [11-15](#)
  - Log files parameters, [11-19](#)
- Log transfer parameters, [11-22](#)
- LSMS web parameters, [11-27](#)
- Reports parameters, [11-29](#)
- SNMP agent parameters, [11-31](#)
- Software download parameters, [11-34](#)
- System wide parameters, [11-1](#)
- Tunable parameters, [11-44](#)
- User authentication parameters, [11-46](#)
- Simple Network Management Protocol (SNMP), [15-1](#)
  - agent parameters, [11-31](#)
  - definition, [15-2](#)
  - protocol versions supported, [15-2](#)
- Simple Network Management Protocol (SNMP) agent
  - on the Brick, [15-9](#)
  - on the SMS, [15-6](#)
- Sizing guidelines, [B-1](#), [B-8](#)
  - Determine CPU capacity, [B-4](#)
  - Determine memory utilization, [B-6](#)
  - Disk capacity for log files, [B-7](#)
  - Sizing tool, [B-2](#)
- Sizing tool, [B-2](#)
- SMS administrator, [8-3](#), [8-9](#)
- SMS host, [1-2](#), [1-4](#)
- SMS Messenger, [8-25](#)
- SMS Navigator, [1-3](#)
- SMS Remote Navigator, [1-4](#)
- SMS status, [14-16](#)
- SMS/CS and Brick Status window, [14-16](#)
- SMTP host, [11-9](#)
- SNMP
  - See: Simple Network Management Protocol (SNMP)
- Software download parameter, [11-34](#)
- SOX password compliance
  - See: Sarbanes-Oxley (SOX) password compliance
- Static routes, [4-32](#)
  - activate, [4-39](#)
  - add, [4-34](#)
  - Add, [4-34](#)
  - cost-based selection of, [4-32](#)
  - deactivate, [4-39](#)
  - delete, [4-40](#)
  - Delete, [4-40](#)
  - modify, [4-38](#)
  - Modify, [4-38](#)
- Status Monitor, [14-1](#), [14-35](#)
  - access, [14-2](#)
  - Administrators & LSMS window, [14-14](#)
  - Brick states, [14-3](#)
  - Brick Status windows, [14-19](#)
  - Console Alarms window, [14-35](#)
  - Display the Status Monitor, [14-2](#)
  - SMS/CS and Bricks Status window, [14-16](#)

Status Monitor data, [14-3](#)

Status Overview window, [14-6](#)

  Toolbar, [14-4](#)

Status monitor only login, [1-4](#), [10-15](#)

Status Overview window, [14-6](#), [14-14](#)

  Brick buttons, [14-7](#)

  Brick graphs, [14-11](#)

  Customize button, [14-8](#)

  customize layout of, [14-8](#)

  LSMS and Compute Server status, [14-10](#)

  LSMS/LSCS buttons, [14-7](#)

  Overview For drop-down, [14-9](#)

Strong passwords feature

  enabling, [11-40](#)

Subfolders

  Of a group, [8-2](#)

Syslog port, [11-10](#)

System group, [1-20](#)

  Defined, [8-1](#)

System wide parameters, [11-1](#)

.....

**T** Technical support, [xxv](#)

TFTP application filter

  VoIP services, [3-10](#)

Trigger Alarm Code checkbox, [11-10](#)

Tunabile parameters

  Tunable parameters, [11-44](#)

Tunnel buttons, [1-17](#)

Tunnel endpoint, [3-5](#)

.....

**U** UA

  See: Universal Alcatel (UA)

UAC

  See: User Account Control (UAC)

Universal Alcatel (UA)

  Alcatel-Lucent proprietary signaling protocol, [3-10](#)

User Account Control, [1-2](#)

User authentication parameters, [11-46](#)

User-defined fields

  Brick devices and, [3-19](#)

.....

**V** *Vista*<sup>®</sup>

  User Account Control (UAC), [1-2](#)

VLANs, [6-1](#), [6-21](#)

  Always Show VLAN Information checkbox, [6-7](#), [6-7](#)

  Assign a policy to a port, [6-12](#)

  Associate a network with a VLAN, [6-15](#)

  Configure Brick physical ports and, [6-7](#)

  Default VLAN ID, [6-9](#)

  Receive format, [6-9](#)

  Transmit format, [6-10](#)

  VLAN domain, [6-9](#)

  VLAN membership, [6-9](#)

  What is a VLAN?, [6-2](#)

  Why build VLANs?, [6-4](#)

  Zone VLAN ID field, [6-12](#)

Voice over IP (VoIP)

  communications, [3-10](#)

VoIP

  See: Voice over IP (VoIP)