Release 12.0 R2 | May 2014 | 3HE 08861 AAAB TQZZA Edition 01

Alcatel-Lucent 5620

SERVICE AWARE MANAGER

SYSTEM ADMINISTRATOR GUIDE

Alcatel-Lucent Proprietary
This document contains proprietary information of Alcatel-Lucent and is not to be disclosed
or used except in accordance with applicable agreements.
Copyright 2014 © Alcatel-Lucent. All rights reserved.

Alcatel·Lucent

Alcatel-Lucent assumes no responsibility for the accuracy of the information presented, which is subject to change without notice.

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

Copyright 2014 Alcatel-Lucent.
All rights reserved.

Disclaimers

Alcatel-Lucent products are intended for commercial uses. Without the appropriate network design engineering, they must not be sold, licensed or otherwise distributed for use in any hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life-support machines, or weapons systems, in which the failure of products could lead directly to death, personal injury, or severe physical or environmental damage. The customer hereby agrees that the use, sale, license or other distribution of the products for any such application without the prior written consent of Alcatel-Lucent, shall be at the customer's sole risk. The customer hereby agrees to defend and hold Alcatel-Lucent harmless from any claims for loss, cost, damage, expense or liability that may arise out of or in connection with the use, sale, license or other distribution of the products in such applications.

This document may contain information regarding the use and installation of non-Alcatel-Lucent products. Please note that this information is provided as a courtesy to assist you. While Alcatel-Lucent tries to ensure that this information accurately reflects information provided by the supplier, please refer to the materials provided with any non-Alcatel-Lucent product and contact the supplier for confirmation. Alcatel-Lucent assumes no responsibility or liability for incorrect or incomplete information provided about non-Alcatel-Lucent products.

However, this does not constitute a representation or warranty. The warranties provided for Alcatel-Lucent products, if any, are set forth in contractual documentation entered into by Alcatel-Lucent and its customers.

This document was originally written in English. If there is any conflict or inconsistency between the English version and any other version of a document, the English version shall prevail.

When printed by Alcatel-Lucent, this document is printed on recycled paper.

Alcatel-Lucent License Agreement

SAMPLE END USER LICENSE AGREEMENT

1. LICENSE

1.1 Subject to the terms and conditions of this Agreement, Alcatel-Lucent grants to Customer and Customer accepts a nonexclusive, nontransferable license to use any software and related documentation provided by Alcatel-Lucent pursuant to this Agreement ("Licensed Program") for Customer's own internal use, solely in conjunction with hardware supplied or approved by Alcatel-Lucent. In case of equipment failure, Customer may use the Licensed Program on a backup system, but only for such limited time as is required to rectify the failure.

1.2 Customer acknowledges that Alcatel-Lucent may have encoded within the Licensed Program optional functionality and capacity (including, but not limited to, the number of equivalent nodes, delegate workstations, paths and partitions), which may be increased upon the purchase of the applicable license extensions.

1.3 Use of the Licensed Program may be subject to the issuance of an application key, which shall be conveyed to the Customer in the form of a Supplement to this End User License Agreement. The purchase of a license extension may require the issuance of a new application key.

2. PROTECTION AND SECURITY OF LICENSED PROGRAMS

2.1 Customer acknowledges and agrees that the Licensed Program contains proprietary and confidential information of Alcatel-Lucent and its third party suppliers, and agrees to keep such information confidential. Customer shall not disclose the Licensed Program except to its employees having a need to know, and only after they have been advised of its confidential and proprietary nature and have agreed to protect same.

2.2 All rights, title and interest in and to the Licensed Program, other than those expressly granted to Customer herein, shall remain vested in Alcatel-Lucent or its third party suppliers. Customer shall not, and shall prevent others from copying, translating, modifying, creating derivative works, reverse engineering, decompiling, encumbering or otherwise using the Licensed Program except as specifically authorized under this Agreement. Notwithstanding the foregoing, Customer is authorized to make one copy for its archival purposes only. All appropriate copyright and other proprietary notices and legends shall be placed on all Licensed Programs supplied by Alcatel-Lucent, and Customer shall maintain and reproduce such notices on any full or partial copies made by it.

3. TERM

3.1 This Agreement shall become effective for each Licensed Program upon delivery of the Licensed Program to Customer.

3.2 Alcatel-Lucent may terminate this Agreement: (a) upon notice to Customer if any amount payable to Alcatel-Lucent is not paid within thirty (30) days of the date on which payment is due; (b) if Customer becomes bankrupt, makes an assignment for the benefit of its creditors, or if its assets vest or become subject to the rights of any trustee, receiver or other administrator; (c) if bankruptcy, reorganization or insolvency proceedings are instituted against Customer and not dismissed within 15 days; or (d) if Customer breaches a material provision of this Agreement and such breach is not rectified within 15 days of receipt of notice of the breach from Alcatel-Lucent.

3.3 Upon termination of this Agreement, Customer shall return or destroy all copies of the Licensed Program. All obligations of Customer arising prior to termination, and those obligations relating to confidentiality and nonuse, shall survive termination.

4. CHARGES

4.1 Upon shipment of the Licensed Program, Alcatel-Lucent will invoice Customer for all fees, and any taxes, duties and other charges. Customer will be invoiced for any license extensions upon delivery of the new software application key or, if a new application key is not required, upon delivery of the extension. All amounts shall be due and payable within thirty (30) days of receipt of invoice, and interest will be charged on any overdue amounts at the rate of 1 1/2% per month (19.6% per annum).

5. SUPPORT AND UPGRADES

5.1 Customer shall receive software support and upgrades for the Licensed Program only to the extent provided for in the applicable Alcatel-Lucent software support policy in effect from time to time, and upon payment of any applicable fees. Unless expressly excluded, this Agreement shall be deemed to apply to all updates, upgrades, revisions, enhancements and other software which may be supplied by Alcatel-Lucent to Customer from time to time.

6. WARRANTIES AND INDEMNIFICATION

6.1 Alcatel-Lucent warrants that the Licensed Program as originally delivered to Customer will function substantially in accordance with the functional description set out in the associated user documentation for a period of 90 days from the date of shipment, when used in accordance with the user documentation. Alcatel-Lucent's sole liability and Customer's sole remedy for a breach of this warranty shall be Alcatel-Lucent's good faith efforts to rectify the nonconformity or, if after repeated efforts Alcatel-Lucent is unable to rectify the nonconformity, Alcatel-Lucent shall accept return of the Licensed Program and shall refund to Customer all amounts paid in respect thereof. This warranty is available only once in respect of each Licensed Program, and is not renewed by the payment of an extension charge or upgrade fee.

6.2 ALCATEL-LUCENT EXPRESSLY DISCLAIMS ALL OTHER WARRANTIES, REPRESENTATIONS, COVENANTS OR CONDITIONS OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, WARRANTIES OR REPRESENTATIONS OF WORKMANSHIP, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, DURABILITY, OR THAT THE OPERATION OF THE LICENSED PROGRAM WILL BE ERROR FREE OR THAT THE LICENSED PROGRAMS WILL NOT INFRINGE UPON ANY THIRD PARTY RIGHTS.

6.3 Alcatel-Lucent shall defend and indemnify Customer in any action to the extent that it is based on a claim that the Licensed Program furnished by Alcatel-Lucent infringes any patent, copyright, trade secret or other intellectual property right, provided that Customer notifies Alcatel-Lucent within ten (10) days of the existence of the claim, gives Alcatel-Lucent sole control of the litigation or settlement of the claim, and provides all such assistance as Alcatel-Lucent may reasonably require. Notwithstanding the foregoing, Alcatel-Lucent shall have no liability if the claim results from any modification or unauthorized use of the Licensed Program by Customer, and Customer shall defend and indemnify Alcatel-Lucent against any such claim.

6.4 Alcatel-Lucent Products are intended for standard commercial uses. Without the appropriate network design engineering, they must not be sold, licensed or otherwise distributed for use in any hazardous environments requiring fail safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life-support machines, or weapons systems, in which the failure of products could lead directly to death, personal injury, or severe physical or environmental damage. The Customer hereby agrees that the use, sale, license or other distribution of the Products for any such application without the prior written consent of Alcatel-Lucent, shall be at the Customer's sole risk. The Customer also agrees to defend and hold Alcatel-Lucent harmless from any claims for loss, cost, damage, expense or liability that may arise out of or in connection with the use, sale, license or other distribution of the Products in such applications.

7. LIMITATION OF LIABILITY

7.1 IN NO EVENT SHALL THE TOTAL COLLECTIVE LIABILITY OF ALCATEL-LUCENT, ITS EMPLOYEES, DIRECTORS, OFFICERS OR AGENTS FOR ANY CLAIM, REGARDLESS OF VALUE OR NATURE, EXCEED THE AMOUNT PAID UNDER THIS AGREEMENT FOR THE LICENSED PROGRAM THAT IS THE SUBJECT MATTER OF THE CLAIM. IN NO EVENT SHALL THE TOTAL COLLECTIVE LIABILITY OF ALCATEL-LUCENT, ITS EMPLOYEES, DIRECTORS, OFFICERS OR AGENTS FOR ALL CLAIMS EXCEED THE TOTAL AMOUNT PAID BY CUSTOMER TO ALCATEL-LUCENT HEREUNDER. NO PARTY SHALL BE LIABLE FOR ANY INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES, WHETHER OR NOT SUCH DAMAGES ARE FORESEEABLE, AND/OR THE PARTY HAD BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7.2 The foregoing provision limiting the liability of Alcatel-Lucent's employees, agents, officers and directors shall be deemed to be a trust provision, and shall be enforceable by such employees, agents, officers and directors as trust beneficiaries.

8. GENERAL

8.1 Under no circumstances shall either party be liable to the other for any failure to perform its obligations (other than the payment of any monies owing) where such failure results from causes beyond that party's reasonable control.

8.2 This Agreement constitutes the entire agreement between Alcatel-Lucent and Customer and supersedes all prior oral and written communications. All amendments shall be in writing and signed by authorized representatives of both parties.

8.3 If any provision of this Agreement is held to be invalid, illegal or unenforceable, it shall be severed and the remaining provisions shall continue in full force and effect.

8.4 The Licensed Program may contain freeware or shareware obtained by Alcatel-Lucent from a third party source. No license fee has been paid by Alcatel-Lucent for the inclusion of any such freeware or shareware, and no license fee is charged to Customer for its use. The Customer agrees to be bound by any license agreement for such freeware or shareware. CUSTOMER ACKNOWLEDGES AND AGREES THAT THE THIRD PARTY SOURCE PROVIDES NO WARRANTIES AND SHALL HAVE NO LIABILITY WHATSOEVER IN RESPECT OF CUSTOMER'S POSSESSION AND/OR USE OF THE FREEWARE OR SHAREWARE.

8.5 Alcatel-Lucent shall have the right, at its own expense and upon reasonable written notice to Customer, to periodically inspect Customer's premises and such documents as it may reasonably require, for the exclusive purpose of verifying Customer's compliance with its obligations under this Agreement.

8.6 All notices shall be sent to the parties at the addresses listed above, or to any such address as may be specified from time to time. Notices shall be deemed to have been received five days after deposit with a post office when sent by registered or certified mail, postage prepaid and receipt requested.

8.7 If the Licensed Program is being acquired by or on behalf of any unit or agency of the United States Government, the following provision shall apply: If the Licensed Program is supplied to the Department of Defense, it shall be classified as "Commercial Computer Software" and the United States Government is acquiring only "restricted rights" in the Licensed Program as defined in DFARS 227-7202-1(a) and 227.7202-3(a), or equivalent. If the Licensed Program is supplied to any other unit or agency of the United States Government, rights will be defined in Clause 52.227-19 or 52.227-14 of the FAR, or if acquired by NASA, Clause 18-52.227-86(d) of the NASA Supplement to the FAR, or equivalent. If the software was acquired under a contract subject to the October 1988 Rights in Technical Data and Computer Software regulations, use, duplication and disclosure by the Government is subject to the restrictions set forth in DFARS 252-227.7013(c)(1)(ii) 1988, or equivalent.

8.8 Customer shall comply with all export regulations pertaining to the Licensed Program in effect from time to time. Without limiting the generality of the foregoing, Customer expressly warrants that it will not directly or indirectly export, reexport, or transship the Licensed Program in violation of any export laws, rules or regulations of Canada, the United States or the United Kingdom.

8.9 No term or provision of this Agreement shall be deemed waived and no breach excused unless such waiver or consent is in writing and signed by the party claimed to have waived or consented. The waiver by either party of any right hereunder, or of the failure to perform or of a breach by the other party, shall not be deemed to be a waiver of any other right hereunder or of any other breach or failure by such other party, whether of a similar nature or otherwise.

8.10 This Agreement shall be governed by and construed in accordance with the laws of the Province of Ontario. The application of the United Nations Convention on Contracts for the International Sale of Goods is hereby expressly excluded.

Preface

The Preface provides general information about the 5620 Service Aware Manager documentation suite, including this guide.

Prerequisites

Readers of the 5620 SAM documentation suite are assumed to be familiar with the following:

- 5620 SAM software structure and components
- 5620 SAM GUI operations and tools
- typical 5620 SAM management tasks and procedures
- device and network management concepts

5620 SAM documentation suite

The 5620 SAM documentation suite describes the 5620 SAM and the associated network management of its supported devices. Contact your Alcatel-Lucent support representative for information about specific network or facility considerations.

Table 1 lists the documents in the 5620 SAM customer documentation suite.

Table 1 5620 SAM customer documentation suite

Guide	Description
5620 SAM core documentation	

(1 of 5)

Guide	Description
5620 SAM Alarm Reference	The *5620 SAM Alarm Reference* provides a description of all alarms supported on the 5620 SAM, including LTE and optical alarms, the raising and clearing conditions of each alarm, and the remedial action to fix the problem. The reference is organized by network element type.
5620 SAM Chronos SyncWatch Integration Guide	The *5620 SAM Chronos SyncWatch Integration Guide* provides procedures to allow the 5620 SAM to integrate with the Chronos SyncWatch Probe and NetSMART server. The guide also provides general information about synchronization management in a 5620 SAM-managed network.
5620 SAM Glossary	The *5620 SAM Glossary* defines terms and acronyms used in all of the 5620 SAM documentation.
5620 SAM Integration Guide	The *5620 SAM Integration Guide* provides procedures to allow the 5620 SAM to integrate with other Alcatel-Lucent products and third-party products.
5620 SAM Network Element Compatibility Guide	The *5620 SAM Network Element Compatibility Guide* provides release-specific information about the compatibility of managed devices in 5620 SAM releases. This document is updated regularly; always consult the latest version on OLCS as described in Documentation and resources on the web.
5620 SAM Parameter Guide	The *5620 SAM Parameter Guide* provides: • parameter descriptions that include value ranges and default values • parameter options and option descriptions • parameter and option dependencies • parameter mappings to the 5620 SAM-O XML equivalent property names Parameters specific to LTE network elements are covered in the *5620 SAM LTE Parameter Reference*. Parameters specific to 1830 PSS network elements are covered in the *5620 SAM Optical Parameter Reference*. The 5620 SAM online help system includes a Parameter Search Tool that allows you to look up parameters or 5620 SAM and 5650 CPAM forms. See the *5620 SAM User Guide* for more information about using the Parameter Search Tool.
5620 SAM Planning Guide	The *5620 SAM Planning Guide* provides information about 5620 SAM scalability and recommended hardware configurations.
5620 SAM Release Description	The *5620 SAM Release Description* provides information about the new features associated with a 5620 SAM software release.
5620 SAM Release Notice	The *5620 SAM Release Notice* provides important information about the software release, including outstanding issues and restrictions. This document is not shipped with the on-product customer documentation and must be obtained from OLCS as described in Documentation and resources on the web.
5620 SAM Scripts and Templates Developer Guide	The *5620 SAM Scripts and Templates Developer Guide* provides information that allows users to develop, manage, and run CLI-based or XML-based scripts or templates. The guide is intended for developers, skilled administrators, and operators who are expected to be familiar with the following: • CLI scripting, XML, and the Velocity engine • basic scripting or programming • 5620 SAM functions
5620 SAM Statistics Management Guide	The *5620 SAM Statistics Management Guide* provides information about how to configure performance and accounting statistics collection and how to view counters using the 5620 SAM. Network examples are included.

(2 of 5)

Guide	Description
5620 SAM System Administrator Guide	The *5620 SAM System Administrator Guide* provides information about the tasks performed by a user with a 5620 SAM admin role, including: • 5620 SAM security management tasks such as setting up all required user accounts and user groups • advanced configuration tasks such as configuring, maintaining, and administering the 5620 SAM operational environment • routine maintenance tasks to maintain the 5620 SAM hardware and system integrity and efficiencies
5620 SAM System Architecture Guide	The *5620 SAM System Architecture Guide* is intended for technology officers, network planners, and system administrators to increase their knowledge of the 5620 SAM software structure and components. It describes the system structure, software components, and interfaces of the 5620 SAM. In addition, 5620 SAM fault tolerance, security, and network management capabilities are discussed from an architectural perspective.
5620 SAM Troubleshooting Guide	The *5620 SAM Troubleshooting Guide* provides task-based procedures and user documentation to: • help resolve issues in the managed and management networks • identify the root cause and plan corrective action for: • alarm conditions on a network object or customer service • problems on customer services with no associated alarms • list problem scenarios, possible solutions, and tools to help check: • network management LANs • network management platforms and operating systems • 5620 SAM client GUIs and client OSS applications • 5620 SAM servers • 5620 SAM databases
5620 SAM User Guide	The *5620 SAM User Guide* provides information about using the 5620 SAM to manage the service-aware IP/MPLS network, including GUI basics, service configuration, and policy management. The *5620 SAM User Guide* uses a task-based format that employs both high-level workflows and detailed procedures. 5620 SAM management information specific to LTE network elements is covered in the *5620 SAM LTE ePC User Guide* and *5620 SAM LTE RAN User Guide*. 5620 SAM management information specific to 1830 PSS network elements is covered in the *5620 SAM Optical User Guide*. 5620 SAM management information specific to 9500 MPR and 9500 MPRe devices is covered in the *5620 SAM MPR User Guide*.
5620 SAM | 5650 CPAM Installation and Upgrade Guide	The *5620 SAM | 5650 CPAM Installation and Upgrade Guide* provides OS considerations, configuration information, and procedures for the following: • installing, upgrading, and uninstalling 5620 SAM and 5650 CPAM software in standalone and redundant deployments • 5620 SAM system migration to a different system • conversion from a standalone to a redundant 5620 SAM system
5620 SAM MPR documentation	
5620 SAM MPR User Guide	The *5620 SAM MPR User Guide* describes how to discover, configure, and manage 9500 MPR and 9500 MPRe devices using the 5620 SAM. The guide is intended for network planners, administrators, and operators and is to be used in conjunction with other guides in the 5620 SAM documentation suite where management of 9500 MPR and 9500 MPRe devices does not differ from other network elements. Alcatel-Lucent recommends that you review the entire *5620 SAM MPR User Guide* before you attempt to use the 5620 SAM in your MPR network.
5620 SAM LTE documentation	
5620 SAM LTE Release Description	The *5620 SAM LTE Release Description* provides information about the LTE features associated with the release.

(3 of 5)

Guide	Description
5620 SAM LTE ePC User Guide	The *5620 SAM LTE ePC User Guide* describes how to discover, configure, and manage LTE ePC devices using the 5620 SAM. The guide is intended for LTE ePC network planners, administrators, and operators and is to be used in conjunction with other guides in the 5620 SAM documentation suite where management of ePC devices does not differ from other network elements. Alcatel-Lucent recommends that you review the entire *5620 SAM LTE ePC User Guide* before you attempt to use the 5620 SAM in your LTE network.
5620 SAM LTE OSS Interface Developer Guide	The *5620 SAM LTE OSS Interface Developer Guide* provides information about developing LTE OSS applications, including information about the 3GPP OSS interface components and architecture, understanding the 5620 SAM-O schema in the context of LTE, compliance with 3GPP standards, and typical operational scenarios.
5620 SAM LTE Parameter Reference	The *5620 SAM LTE Parameter Reference* provides a list of all LTE ePC and LTE RAN parameters supported in the 5620 SAM.
5620 SAM LTE RAN User Guide	The *5620 SAM LTE RAN User Guide* describes how to discover, configure, and manage the Evolved NodeB, or eNodeB, using the 5620 SAM. The guide is intended for LTE RAN network planners, administrators, and operators and is to be used in conjunction with other guides in the 5620 SAM documentation suite where management of RAN devices does not differ from other network elements. Alcatel-Lucent recommends that you review the entire *5620 SAM LTE RAN User Guide* before you attempt to use the 5620 SAM in your LTE network.
5620 SAM optical documentation	
5620 SAM Optical Parameter Reference	The *5620 SAM Optical Parameter Reference* provides a list of all optical device parameters supported in the 5620 SAM.
5620 SAM Optical User Guide	The *5620 SAM Optical User Guide* describes how to discover, configure, and manage optical devices using the 5620 SAM. The guide is intended for optical network planners, administrators, and operators and is to be used in conjunction with other guides in the 5620 SAM documentation suite where management of optical devices does not differ from other network elements. Alcatel-Lucent recommends that you review the entire *5620 SAM Optical User Guide* before you attempt to use the 5620 SAM in your optical network.
5620 SAM-O documentation	
5620 SAM XML OSS Interface Developer Guide	The *5620 SAM XML OSS Interface Developer Guide* provides information that allows you to: • use the 5620 SAM XML OSS interface to access network management information • learn about the information model associated with the managed network • develop OSS applications using the packaged methods, classes, data types, and objects necessary to manage 5620 SAM functions
5650 CPAM documentation	
5650 CPAM Release Description	The *5650 CPAM Release Description* provides information about the new features associated with a 5650 CPAM software release.
5650 CPAM Release Notice	The *5650 CPAM Release Notice* provides important information about the 5650 CPAM software release and corresponding 7701 CPAA software release, including outstanding issues and restrictions. This document is not shipped with the on-product documentation and must be obtained from OLCS as described in Documentation and resources on the web.
5650 CPAM User Guide	The *5650 CPAM User Guide* describes how to capture, inspect, visualize, and troubleshoot IGP and BGP topologies using the 5650 CPAM.
7701 CPAA Hardware Revision 2 Setup and Software Installation Instructions	The *7701 CPAA Hardware Revision 2 Setup and Software Installation Instructions* describes the hardware setup and software installation for the 7701 CPAA Hardware Revision 2, the route analyzer component of the 5650 CPAM.

(4 of 5)

Guide	Description
7701 CPAA Hardware Revision 1 Setup and Software Installation Instructions	The *7701 CPAA Hardware Revision 1 Setup and Software Installation Instructions* describes the hardware setup and software installation for the 7701 CPAA Hardware Revision 1, the route analyzer component of the 5650 CPAM.

(5 of 5)

Obtaining customer documentation

You can obtain 5620 SAM customer documentation:

- from the product
- on the web

On-product documentation

The 5620 SAM on-product customer documentation is delivered in HTML and PDF. Choose Help→User Documentation from the 5620 SAM client GUI to open the help system in a web browser. For best results, use Internet Explorer or Firefox.

The help system opens to the User Documentation Index, which provides a summary of and links to all 5620 SAM customer documents.

Click on the Using the help system tab on the User Documentation Index page to find usage tips for navigating and searching within the on-product customer documentation.

You can return to the User Documentation Index at any time by clicking on the Home icon, shown in Figure 1.

Figure 1 Home icon

Documentation and resources on the web

The 5620 SAM customer documentation is available for download in PDF format from the Alcatel-Lucent Customer Support Center: http://www.alcatel-lucent.com/myaccess. If you are a new user and require access to this service, please contact your Alcatel-Lucent support representative.

Release Notices and any other documents not delivered on-product are posted to this site.

5620 SAM product alerts

Product technical alerts are used to communicate important information to customers about released loads. You can view and subscribe to product alerts for the 5620 SAM from the Alcatel-Lucent Customer Support Center.

Working with PDFs

You can download PDFs of individual guides from the Alcatel-Lucent Customer Support Center, or you can choose to download a zip of all PDFs for a particular release.

You can use the Search function of Acrobat Reader (File→Search) to find a term in a PDF of any 5620 SAM document. To refine your search, use appropriate search options (for example, search for whole words only or enable case-sensitive searching). You can also search for a term in multiple PDFs at once, provided that they are located in the same directory. For more information, see the Help for Acrobat Reader.

Note — Users of Mozilla browsers may receive an error message when opening the PDF files in the 5620 SAM documentation suite. The offline storage and default cache values used by the browsers are the cause of the error message.

Alcatel-Lucent recommends changing the Mozilla Firefox offline storage or Mozilla 1.7 cache value to 100 Mbytes to eliminate the error message.

Documentation conventions

Table 2 lists the conventions that are used throughout the documentation.

Table 2 Documentation conventions

Convention	Description	Example
Key name	Press a keyboard key	Delete
Italics	Identifies a variable	*hostname*
Key+Key	Type the appropriate consecutive keystroke sequence	CTRL+G
Key–Key	Type the appropriate simultaneous keystroke sequence	CTRL–G
*	An asterisk is a wildcard character, which means “any character” in a search argument.	log_file*.txt
↵	Press the Return key	↵
—	An em dash indicates there is no information.	—
→	Indicates that a cascading submenu results from selecting a menu item	Policies→Alarm Policies

Procedures with options or substeps

When there are options in a procedure, they are identified by letters. When there are substeps in a procedure, they are identified by Roman numerals.

Example of options in a procedure

At step 1, you can choose option a or b. At step 2, you must do what the step indicates.

1 This step offers two options. You must choose one of the following.

- **a** This is one option.
- **b** This is another option.

2 You must perform this step.

Example of substeps in a procedure

At step 1, you must perform a series of substeps within a step. At step 2, you must do what the step indicates.

1 This step has a series of substeps that you must perform to complete the step. You must perform the following substeps.

- **i** This is the first substep.
- **ii** This is the second substep.
- **iii** This is the third substep.

2 You must perform this step.

Measurement conventions

Measurements in this document are expressed in metric units and follow the Système international d’unités (SI) standard for abbreviation of metric units. If imperial measurements are included, they appear in brackets following the metric unit.

Table 3 lists the measurement symbols used in this document.

Table 3 Bits and bytes conventions

Measurement	Symbol
bit	b
byte	byte
kilobits per second	kb/s

Important information

The following conventions are used to indicate important information:

Warning — Warning indicates that the described activity or situation may, or will, cause equipment damage or serious performance problems.

Caution — Caution indicates that the described activity or situation may, or will, cause service interruption.

Note — Notes provide information that is, or may be, of special interest.

Contents

5620 SAM System Administrator overview

5620 SAM Security management tasks

2 — 5620 SAM user security tasks 2-1

4 — TCP enhanced authentication 4-1

5620 SAM Advanced configuration tasks

5 — 5620 SAM component configuration 5-1

6 — 5620 SAM system redundancy 6-1

7 — 5620 SAM database management 7-1

8 — NE maintenance 8-1

5620 SAM routine maintenance tasks

Appendices

5620 SAM System Administrator overview

1 — 5620 SAM System Administrator Guide overview

1.1 *5620 SAM System Administrator Guide* overview

The *5620 SAM System Administrator Guide* describes the tasks that are typically performed by a user with an Administrator scope of command role. Information in this guide includes:

- 5620 SAM and UNIX security management tasks including:
  - planning and implementing the user security measures required to protect all 5620 SAM data, software, and hardware and monitor the system/network for any security threats.
  - setting up all required 5620 SAM user accounts and user groups with the required scope of command roles and span of control permissions and the ongoing monitoring and management of those accounts.
  - providing security support information for accessing and securing managed devices in your network.
  - configuration and management requirements for TCP enhanced authentication for NEs based on the MD5 encryption mechanism.
- advanced configuration tasks including:
  - configuring, maintaining, and administering the 5620 SAM operational environment including software licenses, system components, network functions, and system preferences.
  - performing the required tasks to establish and maintain 5620 SAM system redundancy; and as required, monitor/perform any maintenance activity switching or switchovers.
  - using the 5620 SAM database manager to view, configure, and monitor the 5620 SAM database.
  - performing NE maintenance for supported devices such as performing an on-demand or scheduled NE configuration backup.
- routine maintenance tasks to maintain hardware and system integrity and efficiencies including:
  - collecting baseline information to evaluate the activity and performance of the 5620 SAM and the various network components.
  - performing daily, weekly, monthly and supplemental routine maintenance on the 5620 SAM such as maintaining data backups and disaster recovery operations.

Note — This guide concentrates the majority of system administrator tasks into a single guide but some tasks are documented in other separate guides. See section 1.3 for a detailed listing of all system administrator tasks or information contained in this guide and other 5620 SAM customer documentation.

1.2 5620 SAM system administrator role

The Alcatel-Lucent 5620 SAM system administrator, in a typical network, would be the individual with a 5620 SAM administrative role given the responsibility for:

- performing the initial installation and setup of the 5620 SAM
- performing 5620 SAM startup and shutdown procedures
- planning and implementation of the user security measures required to protect all 5620 SAM data, software, and hardware

- setting up all required 5620 SAM user accounts with the required scope of command roles and span of control permissions and monitor the system/network for any security threats
- configuring, maintaining, and administering the 5620 SAM environment including computer hardware, system software/database, and any other advance configurations
- performing data backups and disaster recovery operations
- performing the required tasks to establish and maintain 5620 SAM system redundancy; and as required, monitor/perform any maintenance activity switching or switchovers
- monitoring the performance of the 5620 SAM to ensuring it operates and functions within set operational guidelines
- performing daily, weekly, monthly and supplementary routine maintenance on the 5620 SAM
- diagnosing any system-related alarm activity and solving unique problems identified by service and network operators
- diagnosing and troubleshooting platform, server/clients, database, services, and connectivity problems using the 5620 SAM diagnostic tools.
- performing the integration of the 5620 SAM with other Alcatel-Lucent products or third-party products

Suggested system administrator role prerequisites

As a minimum, the individual responsible for developing and performing 5620 SAM system administrator tasks need a good understanding of the following:

- UNIX including writing and executing scripts
- 5620 SAM architecture and the Alcatel-Lucent NMS portfolio
- 5620 SAM planning information and installation and upgrade procedures
- general security management concepts
- advanced configuration procedures
- routine and supplemental maintenance processes
- high-level troubleshooting workflows to help identify and isolate problems

1.3 5620 SAM system administrator task and information map

Table 1-1 provides a high-level navigation aid to help you locate specific system administrator tasks or information contained in this guide and other 5620 SAM customer documentation.

Table 1-1 5620 SAM system administrator task or information location

Task or information	Information location
Installation and upgrades	
Provides OS considerations, configuration information, and procedures for the following: • installing, upgrading, and uninstalling 5620 SAM and 5650 CPAM software in standalone and redundant deployments • 5620 SAM system migration to another system • conversion from a standalone to a redundant 5620 SAM system	*5620 SAM | 5650 CPAM Installation and Upgrade Guide (issued as a separate guide)*
Security management	
Provides information to help you access the requirements for user access to the 5620 SAM functional areas and configure and manage the following 5620 SAM user security functions and elements: • creating and managing user groups which 5620 SAM users are assigned to • creating and managing 5620 SAM user accounts • monitoring and managing active client sessions • configuring or managing 5620 SAM security functions • deleting 5620 SAM security elements that are no longer required	Chapter 2
Provides security support information for accessing managed devices, including the following: • create and manage users, profiles and passwords for access to NEs • configure RADIUS, TACACS+ or LDAP authentication to control access to the managed devices using 5620 SAM user accounts • configure device system security through CPM traffic filtering and management • configure DoS protection to protect NEs from high incoming packet rates that characterize DoS attacks	Chapter 3
Describes the configuration and management requirements for TCP enhanced authentication for NEs based on the MD5 encryption mechanism	Chapter 4
Provides a listing of the permissions, access levels, and descriptions of all pre-defined scope of command roles and profiles	Appendix A
Advanced configuration	
Describes how to perform miscellaneous configuration changes on the following 5620 SAM components: • 5620 SAM software and licences • System components • Network management functions • System preferences	Chapter 5
Describes how to perform the following redundancy tasks using the 5620 SAM GUI, or scripts on a 5620 SAM main server: • Check the 5620 SAM redundant server and database status. • Perform a manual activity switch from the primary to standby server. • Enable or disable automatic database realignment on the 5620 SAM primary servers. • Reinstantiate the former primary database as the standby database when an automatic or manual activity switch occurs and verify its status.	Chapter 6

(1 of 3)

Task or information	Information location
Describes how to use the 5620 SAM database manager to perform the following: • view the 5620 SAM database properties • configure statistics data retention criteria • manage database log storage • perform database backups and restores • schedule regular database backups • configure error monitoring for increased security • troubleshoot 5620 SAM database problems	Chapter 7
The 5620 SAM includes NE maintenance functionality for supported devices that allows a system administrator to: • define the 5620 SAM deployment and local device configuration-save conditions • perform an on-demand or scheduled NE configuration backup • restore a device configuration • perform an on-demand, ISSU, or scheduled a NE software upgrade • view the status of a deployment, backup, device configuration restore, device software upgrade, or accounting statistics retrieval operation in progress • troubleshoot a failed deployment, backup, or upgrade	Chapter 8
Routine maintenance	
Provides an overview of all 5620 SAM routine maintenance tasks and their suggested application.	Chapter 9
Provides a list of baseline information to collect for 5620 SAM applications to evaluate the performance of activity and performance of network components.	Chapter 10
Describes the daily, weekly, monthly, and as-required routine maintenance activities for 5620 SAM-managed networks and the 5620 SAM platform.	Chapter 11 Chapter 12 Chapter 13 Chapter 14
Troubleshooting	
Provides task-based procedures and user documentation to: • help resolve issues in the managed and management networks • identify the root cause and plan corrective action for: • alarm conditions on a network object or customer service • problems on customer services without associated alarms • list problem scenarios, possible solutions, and tools to help check: • network management LANs • network management platforms and operating systems • 5620 SAM client GUIs and client OSS applications • 5620 SAM servers • 5620 SAM databases	*5620 SAM Troubleshooting Guide (issued as a separate guide)*
Diagnosing alarms	
Provides a description of all alarms supported on the 5620 SAM, the raising and clearing conditions of each alarm, and the remedial action to fix the problem. Of interest to system administrators are alarms that require sysadmin access to solve such as database alarms or user authentication failure alarms.	*5620 SAM Alarm Reference (issued as a separate guide)*

(2 of 3)

Task or information	Information location
Integration tasks	
Provides the procedures to allow the 5620 SAM to be integrated with other Alcatel-Lucent products such the 5650 CPAM and 5780 DSC, and other third-party products.	*5620 SAM Integration Guide (issued as a separate guide)*

(3 of 3)

5620 SAM Security management tasks

2 — 5620 SAM user security tasks

2.1 5620 SAM user security overview

This chapter provides information to help you access the requirements for user access to the various 5620 SAM functional areas and develop a strategy for implementing user security to meet your operational requirements.

You can configure and manage the following 5620 SAM user security functions and elements:

- creating and managing user groups which 5620 SAM users are assigned too. User group creation also requires the following security elements to be defined:
  - Scope of command roles—contain the role that define the level of user control in 5620 SAM functional areas such as the read, create, update, and delete access permissions
  - Scope of command profiles—contain the appropriate scope of command role for the types of tasks to be performed
  - Span of control—is a list of the objects over which the user has control
  - Span of control profiles—contain the required spans allows user-group access to one or more 5620 SAM managed objects.
  - Span rules—instruct the 5620 SAM to add new services to other spans in addition to the Default Service span
- creating the various 5620 SAM user accounts and the configuration of global security parameters associated with the account such as specifying the expiry periods, the allowed number of login attempts, and any automated security e-mail notifications.
- managing 5620 SAM user accounts such as managing passwords, or listing, suspending, or reinstating users.
- managing 5620 SAM user group workspaces
- monitoring and managing active client sessions
- configuring or managing various 5620 SAM security functions such as RADIUS and TACACS+ authentication or monitoring OSS users.
- deleting 5620 SAM security elements that are no longer required such as inactive user accounts or user groups.
- configuring task monitoring parameters and monitoring the progress of operational tasks.
  - all write operations that are performed from the 5620 SAM GUI; for example, when you click on the Apply or OK buttons
  - all write operations that are performed using the OSSI
  - some read operations; for example, when you click on the Resync or Collect All buttons

Note — See Appendix A for a list of the permissions, access levels, and descriptions of all pre-defined scope of command roles and profiles.

See section 2.7 for a detailed listing of 5620 SAM user security tasks.

2.2 User account and group management

You can create 5620 SAM user accounts and user groups to:

- provide GUI or OSS access to the 5620 SAM functional areas that match specific operator requirements
- restrict access to functions or objects based on operator expertise or authority

Users have view access, read-write access, or no access to 5620 SAM objects and functions based on:

- the user group to which they belong
- the scope of command profile assigned to the user group.

The 5620 SAM user account that is called admin is created during 5620 SAM installation. The admin account is assigned the administrator scope of command role and a span of control profile that has Edit Access assigned to each default span. See “Scope of command” in this section for more information.

Caution — Because the 5620 SAM cannot obtain an authentication secret value from an NE, Alcatel-Lucent recommends that you use only the 5620 SAM to configure a shared authentication secret on an NE. If you configure a shared authentication secret on a managed NE using another interface, for example, a CLI, the 5620 SAM cannot synchronize the security policy with the NE.

Note — To restrict user access to top-level 5620 SAM functions such as 5620 SAM and NE security management, Alcatel-Lucent recommends the following:

- Assign the administrator scope of command role to a minimal number of 5620 SAM user accounts.
- Assign each 5620 SAM user to a user group that has the minimum privileges for performing the required tasks.

General 5620 SAM security management rules

The following general rules apply to 5620 SAM user and group security management:

- Only database space limits the number of accounts and groups that can be created.
- A user cannot belong to more than one user group.
- Only one session per user account can be open at the same time on a client station.
- A scope of command profile allows user-group access to one or more 5620 SAM functional areas.
- A span of control profile allows user-group access to one or more 5620 SAM managed objects.
- A user group is associated with only one scope of command profile that can contain multiple scope of command roles.
- A user group is associated with only one span of control profile that can contain multiple spans.

- The assigned user privileges determine the following for a GUI user:
  - the available 5620 SAM menu options
  - the parameters on object property forms that are configurable
- By default, a user group is assigned access to all 5620 SAM objects.
- A user acquires span of control access rights from the associated user group.
- When you modify a user group, and a user in the group has an open client session, client actions may fail for the user. To put the new user group permissions into effect, the user must close the current client session and open a new session.
- You can modify but not delete a span of control profile that is assigned to a group.

Password management

A 5620 SAM user password must observe the following constraints:

- It must be 8 to 100 characters.
- It must contain at least three of the following character types:
  - lowercase
  - uppercase
  - special
  - numeric
- It cannot be the user account name, in forward or reverse order.
- It cannot include more than three consecutive instances of the same character.
- It must change according to a configurable schedule, to prevent account lockout.
- It cannot be reused as a new password for the same user account.

Scope of command

A scope of command, which defines the actions that a user is allowed to perform, is a collection of configurable roles, which are sets of permissions. A scope of command profile contains one or more roles, and the profile is subsequently applied to a user group. Each user in the group acquires the access rights specified in the scope of command profile.

Scope of command roles

A scope of command role specifies the read, create, update, and delete access permissions for a 5620 SAM object type or package. You can create custom roles by assigning specific access permissions to different 5620 SAM functional areas. The functional areas are organized in packages, methods, and classes. See Appendix A for a list of all access permissions that can be assigned to a scope of command role.

Note 1 — When you enable the Create permission for a 5620 SAM package, method, or class, the Update permission is automatically enabled.

Note 2 — When you enable the Update permission for a 5620 SAM package, method, or class, the Create permission is not automatically enabled.

You can create an original scope of command role, or copy an existing role and modify the role permissions to create a role. The 5620 SAM has several predefined scope of command roles. See Appendix A for a list of the permissions, access levels, and descriptions of all pre-defined scope of command roles and profiles.

Note — When you create a scope of command role, you must enable create, update/execute, and delete access to allow the modification of a class or package.

Scope of command profiles

A scope of command profile contains one or more scope of command roles, and is assigned to a user group. Each user in the group acquires the permissions from the scope of command roles in the profile.

Span of control

The span of control for a user is a list of the objects over which the user has control, for example, a group of NEs or services. You can create an original span, or copy an existing span and modify the list of associated objects to create a new span. The objects that are in a span, or that can be added to a span, are called span objects.

The 5620 SAM has several pre-defined spans. Each new 5620 SAM object, for example, a discovered NE, is added to the corresponding pre-defined span. Table 2-1 lists the pre-defined 5620 SAM spans and the type of span objects in each.

Note — You cannot modify or delete a pre-defined span.

Table 2-1 pre-defined spans of control

Span	Included objects
Default Topology Group Span	Topology groups
Default Router Span	Managed NEs
Default Script Span	CLI and XML API scripts, service templates, tunnel templates, and auto-provision profiles
Default Test Suite Span	Test suites
Default Group Span	Ring groups and VLAN groups
Default Bulk Operation Span	Bulk operations
Default Service Span	Services
Default Customer Span	Customers

Spans are specified in span of control profiles that are associated with user groups. A user can create a 5620 SAM object only when the pre-defined span for the object type is in the span of control profile. For example, if you do not have the Default Group Span in your span of control profile, you cannot create a ring group.

NEs are added automatically to a span when the parent topology group, ring group, or VLAN group is in a span. An object that is automatically added to a span cannot be removed from the span, but an explicitly added object can be removed.

Note 1 — A user can view or configure a point-to-point connection only when each endpoint of the connection is in the user span of control. For example, when the endpoints of an LSP path are in different spans, you need view or configuration privileges in each span in order to view or configure the LSP path.

Note 2 — When you create a span, you can drag and drop NEs and topology groups into the span contents list.

Each user can control which objects the 5620 SAM displays in maps, lists, and navigation trees, based on the user span of control. The User Preferences form contains a parameter that globally specifies whether the Edit Access span objects of the user appear by default. Objects that are not in a View Access span of the user are not displayed, regardless of the user preference. See “To filter using span of control” in the *5620 SAM User Guide* for information about configuring the user span of control display preference.

In a list form, you can override the global display preference using the Span On parameter. The associated advanced filter form contains a selector for filtering the search results based on the span of control. See the *5620 SAM User Guide* for information about configuring span of control filters.

Span of control profiles

A span of control profile is a collection of one or more spans that is assigned to a user group. When you create a profile, each span in the profile is assigned one of the following access types:

- View Access—The user can view the span objects, unless the scope of command permissions deny read access.
- Edit Access—The user can modify the span objects, unless the scope of command permissions deny access.
- Blocked Edit—The user can view but not modify the span objects, regardless of the scope of command permissions.
- Blocked View—The user cannot view or modify the span objects, regardless of the scope of command permissions.

Blocked Edit and Blocked View spans restrict access to a subset of the objects in another span in the same profile. For example, when multiple span of control profiles each contain the Default Service Span, you can add a customer-specific Blocked View or Blocked Edit span to each profile so that the user group associated with a profile can view or configure only the services of specific customers.

A Blocked Edit or Blocked View span takes precedence over other spans. For example, when a user has an Edit Access span that contains all services and a Blocked View span that contains Customer A and Customer B, the user cannot view or configure the services that belong to Customer A and Customer B.

Caution — Alcatel-Lucent recommends that you consider the effects of combining customer, service, and NE spans in a span of control profile. For example, a user can modify a service only when the service, customer, and participating NEs are in one or more Edit Access spans of the user, and none of the objects is in a Blocked Edit or Blocked View span.

To ensure that span conflicts do not interfere with network troubleshooting, the 5620 SAM allows a user to execute tests on NEs and service sites that are not in an Edit Access span of the user. However, activities such as policy distribution, software upgrades, and statistics collection can be performed only by a user with Edit Access spans that contain the target objects.

Span rules

By default, the 5620 SAM automatically adds a new service to the Default Service span. Using an OSS or GUI client, you can create policies called span rules that add new services to other spans in addition to the Default Service span.

A span rule is associated with a format or range policy, and applies to the users and user groups that are specified in the format or range policy. You can associate multiple range policies with one user and service type, which enables the automatic addition of a new service to a specific span based on the service ID specified when the service is created.

When you create a span rule, you must specify one of the following to indicate which spans receive the services that the user creates:

- the Edit Access spans of each user associated with the format or range policy
- each span that is explicitly named in the rule

The span rules associated with a format or range policy take effect for new services only when the format or range policy is administratively enabled and has a valid configuration that includes at least one user or user group.

See section 2.4 for a sample span rule configuration and implementation.

2.3 User activity logging

The 5620 SAM logs each GUI and OSS user action, such as a system access attempt or the configuration of an object, in the 5620 SAM database. Table 2-2 lists the information in a user activity log record:

Table 2-2 User activity log record information

Field name	Description
Time	Time of activity

(1 of 2)

Field name	Description
Session Type	Type of session, which is GUI, JMS, or OSS
Session ID	Client session identifier
Session IP Address	Client IP address
Session Time	Client session start time
Server IP Address	IP address of 5620 SAM main server that reports the activity
Type	General activity type, which is Deployment, Operation, or Save
Sub Type	Specific activity type, which is Creation, Deletion, Modification, or name of the invoked method
Username	5620 SAM username
Site Name	Name of affected NE, if applicable
Site ID	IP address of affected NE, if applicable
Object Name	Name of affected object
Object ID	Fully qualified name of affected object
Object Type	Type of affected object
State	Activity status, which is Failure, Success, or Timeout
Request ID	Identifier assigned to the request, which is unique to a session
Additional Info	Information such as old and new parameter values after a modification
XML	5620 SAM object class descriptor, if applicable, and activity details in XML request format

(2 of 2)

To view general user activity log entries in the GUI, or retrieve the entries using the 5620 SAM-O, you need a 5620 SAM user account that has the Administrator or 5620 SAM Management and Operations scope of command role.

Note — Viewing or retrieving LI user activity entries requires the Lawful Intercept Management role, and is restricted to the entries of users in the same LI user group.

The logged activity types are the following:

- Operation—a request for the 5620 SAM
- Deployment—a change that is deployed to an NE
- Save—a change to a 5620 SAM database object

Each user activity creates an Operation log entry. If the activity results in an NE configuration change, a Deployment entry is logged. If the deployed information differs from the information that the 5620 SAM saves to the database, a Save entry is logged. If appropriate, a log entry contains the activity details in XML format.

Table 2-3 lists the user activity types and describes the associated sub types.

Table 2-3 User activity types

Type	Sub Type	sub type description
Deployment	Creation	NE object creation
	Deletion	NE object deletion
	Modification	NE object modification
Operation	*method*	Name of invoked method
Save	Creation	5620 SAM database object creation
	Deletion	5620 SAM database object deletion
	Modification	5620 SAM database object modification

The User Activity form displays a filterable list of the logged user activities, and a filterable list of the logged client and server session activities. Client session activities include connection, disconnection, and access violation. Server session activities include startup and shutdown. The properties form of a client connection log record lists the activities performed by the user during the client session.

The 5620 SAM GUI allows direct navigation between the following objects:

- activity record and the associated session record
- activity record and the activity target object
- object properties form and the associated user activity list form
- 5620 SAM Task Manager task and the associated user activity list form
- session record and the associated user activity list form

The User Activity form lists the recent user session and activity entries; older entries are purged according to configurable storage criteria. See Procedure 5-24 for information about configuring the user activity log retention criteria using the System Preferences form.

To archive user activity log entries before they are purged from the 5620 SAM database, an OSS client can use a time-based filter to retrieve entries from the sysact package using the find and findToFile methods. See the *5620 SAM-O XML Reference* for information about using the find and findToFile methods.

User activity logging is a valuable troubleshooting function. For example, if a port unexpectedly fails, you can quickly determine whether misconfiguration is the cause by doing one of the following:

- opening the port properties form and clicking on the User Activity button to view the recent user activity associated with the port
- opening the User Activity form, filtering the list by object type or name, and then verifying the associated user activities

Note — Script execution is logged, but the actions that a script performs are not.

See “Troubleshooting using the 5620 SAM user activity log” in the *5620 SAM Troubleshooting Guide* for more information.

The following conditions and restrictions apply to user activity logging.

- A Deployment activity typically does not have an associated Save activity for the following reasons:
    - A Deployment activity takes place only after a successful Save activity, so a Deployment implies a Save.
    - A Save activity typically contains the same information as the associated Deployment activity.
- When a high-level object such as an NE is deleted, one aggregate activity record is created, rather than multiple NE child object activity records.
- The XML text in a log entry is limited to 4000 characters. If an activity generates more than 4000 characters of XML text, the text is truncated, and the truncation is indicated on the log entry form.

Client session control

Each 5620 SAM GUI client, 5620 SAM-O JMS client, or XML API request creates a 5620 SAM client session. You can view a list of the active 5620 SAM client sessions on the Sessions tab of the 5620 SAM User Security - Security Management form. Using this form, an admin user, or a user with an assigned security span of control, can also terminate one or more 5620 SAM GUI client sessions. When a 5620 SAM GUI client session is terminated in this manner, each client application receives a warning message and the connection is closed by the 5620 SAM server after a short delay.

Messaging connections

A list of active 5620 SAM GUI connections and 5620 SAM-O JMS connections can be viewed on the Messaging Connections tab of the 5620 SAM User Security - Security Management form. Using this form, an admin user, or a user with an assigned security span of control, can terminate one or more connections. When a 5620 SAM-O client connection is terminated, a notification is sent to the 5620 SAM-O client, but the admin user must also remove the 5620 SAM-O JMS client connection so that the server stops storing JMS messages for the session.

Client delegate sessions

The threshold for the number of 5620 SAM client sessions allowed on a client delegate server is configurable using the 5620 SAM GUI. When a user tries to open a client session that exceeds the threshold, the client delegate server opens the session, displays a warning message to the user, and generates an alarm. The threshold-crossing function can help to balance the session load across multiple client delegate servers. You need the Update user permission on the Server package to configure the threshold. See Procedure 2-33 for more information.

2.4 Sample span rule configuration

This section describes the configuration of a policy that instructs the 5620 SAM to automatically add each service created for a specific customer to an Edit Access span associated with the creator of the service. Only the service administrator for the customer can create or edit the specific customer services. In contrast, a typical service user can only view the specific customer services. Table 2-4 describes the tasks to configure a span rule.

Table 2-4 Sample span rule configuration

Task	Description
1. Create a span that contains the existing customer services.	• Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. • Choose Create→Span on the Span of Control tab. • Specify a span name for the customer services. • Use the Contents tab to specify the customer X services.
2. Create a span of control profile for the service administrator.	• Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. • Choose Create→Profile on the Span of Control tab. • Add the Default Service Span as a View Access span to the span of control profile, which allows the user to create a service. • Add the customer services span as an Edit Access span to the span of control profile.
3. Create a range policy for each service type that the service administrator for the customer can create. In the sample, the services are IES and VPRN.	• Choose Administration→Format and Range from the 5620 SAM main menu. • Choose Create→Range Policy. • Specify IES Service as the Object Type. • Specify Service ID as the Property Name. • Configure a range. • Click on the Add button on the Users tab to assign the policy to the service administrator. • Choose Create→Range Policy. • Specify VPRN Service as the Object Type. • Specify Service ID as the Property Name. • Configure a range. • Click on the Add button on the Users tab to assign the policy to the service administrator.
4. Create a span rule that contains the customer span.	• Choose Administration→Span Rules from the 5620 SAM main menu. • Specify a name for the customer span rule. • Set the Created In parameter to All listed spans. • Add the customer span on the Spans tab.

After the span rule is created, the service administrator creates a new VPRN service for the customer. The 5620 SAM uses the VPRN range policy to automatically configure the service ID, and applies the associated customer span rule when the service is saved. As a result, the service is added to the customer span and to the Default Service Span. The service administrator has Edit Access to the customer span, and, therefore, can modify the service, as required.

2.5 Sample 5620 SAM user authentication configuration

Figure 2-1 shows an example of how 5620 SAM user and user group authentication is performed.

Note 1 — RADIUS and TACACS+ authentication servers support multiple users. If the 5620 SAM cannot reach the first authentication server, the 5620 SAM sequentially attempts the user authentication using the remaining authentication servers.

Note 2 — If user authentication fails against the first authentication server in a sequence (for example, because of wrong password), there is no attempt to authenticate the user against the next authentication server in the sequence.

Note 3 — The EMS server log and 5620 SAM session log record unsuccessful user authentication attempts for known and unknown users. A user that is not defined in the 5620 SAM but belongs to an external AAA server is an example of an unknown user.

Figure 2-1 Sample 5620 SAM user and user group authentication

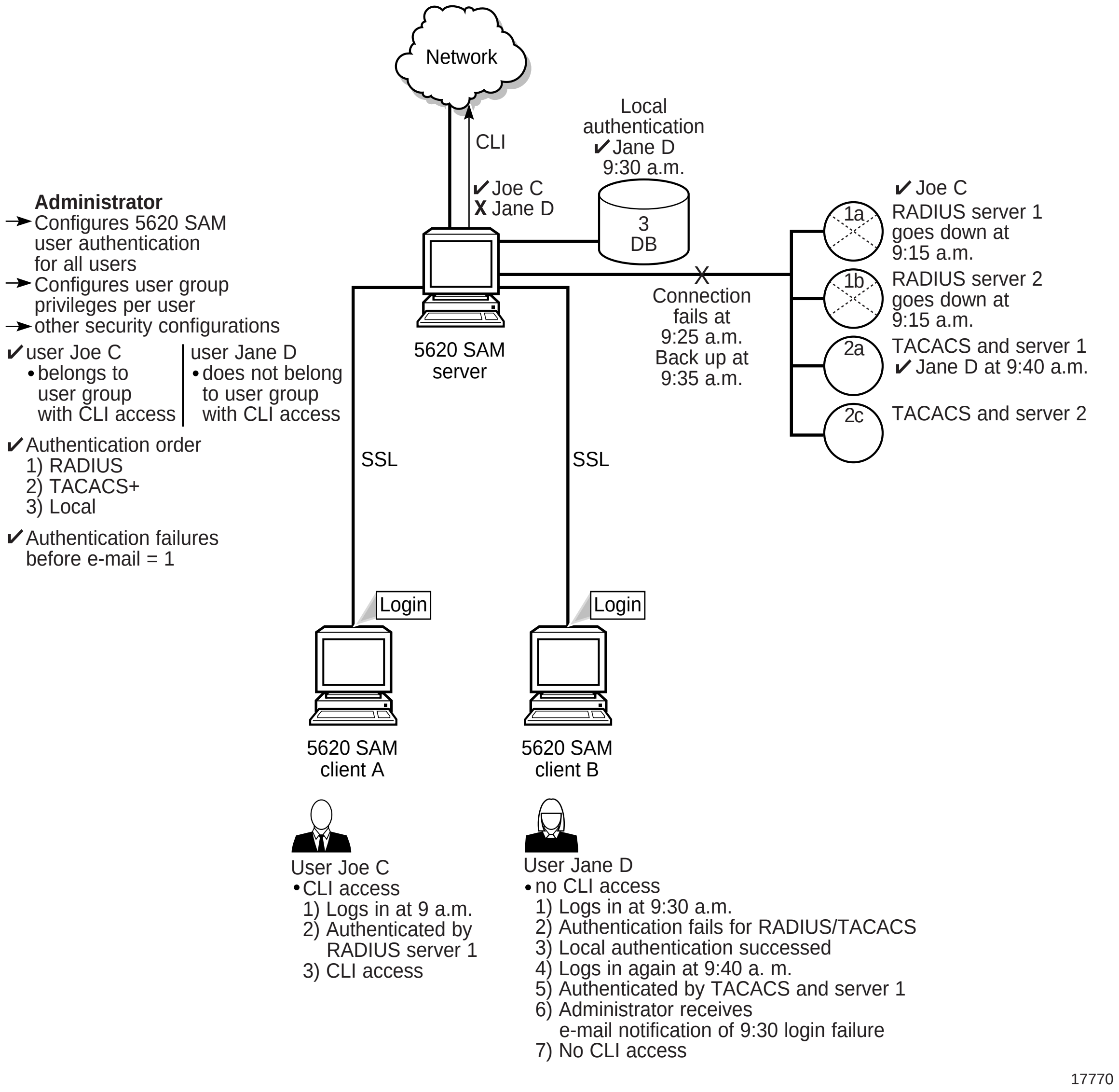

Network
CLI
✔Joe C
X Jane D
Local authentication
✔Jane D 9:30 a.m.
3 DB
Administrator
➛Configures 5620 SAM user authentication for all users
➛Configures user group privileges per user
➛other security configurations
✔user Joe C • belongs to user group with CLI access
user Jane D • does not belong to user group with CLI access
✔Authentication order 1) RADIUS 2) TACACS+ 3) Local
✔Authentication failures before e-mail = 1
5620 SAM server
Connection fails at 9:25 a.m. Back up at 9:35 a.m.
✔Joe C
1a
RADIUS server 1 goes down at 9:15 a.m.
1b
RADIUS server 2 goes down at 9:15 a.m.
2a
TACACS and server 1
✔ Jane D at 9:40 a.m.
2c
TACACS and server 2
SSL
SSL
Login
Login
5620 SAM client A
5620 SAM client B
User Joe C
•CLI access
1) Logs in at 9 a.m.
2) Authenticated by RADIUS server 1
3) CLI access
User Jane D
•no CLI access
1) Logs in at 9:30 a.m.
2) Authentication fails for RADIUS/TACACS
3) Local authentication successed
4) Logs in again at 9:40 a. m.
5) Authenticated by TACACS and server 1
6) Administrator receives e-mail notification of 9:30 login failure
7) No CLI access
17770

Table 2-5 lists the high-level tasks required to configure this sample.

Table 2-5 Sample 5620 SAM user authentication configuration

Task	Description
Pre-configurations	Ensure correct RADIUS or TACACS+ server configuration, according to your company requirements. PAP authentication is supported for RADIUS and TACACS+. The 5620 SAM server must be able to communicate with the authentication servers to validate users. All configuration tasks should be done with admin access. The 5620 SAM server IP address must be configured as the client of the RADIUS or TACACS+ server. The secret keys must match on the 5620 SAM server and the RADIUS or TACACS+ server.

(1 of 2)

Task	Description
1. Configure the remote authentication order for all users	Choose Administration→Security→5620 SAM RADIUS/TACACS+ User Authentication from the 5620 SAM main menu. Set the authentication order parameters to: • radius • tacplus • local Also specify the RADIUS and TACACS+ servers using the corresponding tabs on the same form.
2. Create scope of command profiles	Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. Create a CLI scope of command profile and assign the default CLI management role to the profile. Create at least one scope of command profile that does not allow CLI access by assigning the *default* scope of command role, which has no access permissions to CLI management.
3. Create and configure user groups	Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. Create a CLI user group and at least one user group that does not allow CLI access. Assign the scope of command profile with CLI management access to the CLI user group. Assign the scope of command profile without CLI management access to the user group without CLI access. Authorization is done using user groups, so each user must belong to a user group with a local account on the 5620 SAM server.
4. Create and configure user accounts	You can create local users on the 5620 SAM by performing the following steps, or define remote users using RADIUS and TACACS+. The local users are available when RADIUS or TACACS+ authentication is not available. Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. Create users. Assign the appropriate user group to each user: one with CLI access and one without CLI access.
5.Configure notification	Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. Configure the authentication failure action parameters, including the parameters that allow the e-mail account of the administrator to be notified after login failure.

(2 of 2)

Consider the following:

- The 5620 SAM server acts as a network access server. A network access server is considered a client of a RADIUS or TACACS+ server.
- The sequence of activity between the 5620 SAM server, which is the authentication client, and the RADIUS or TACACS+ server, which is the authentication server, is the following:
  - client requests authentication
  - server replies to authentication request
  - client requests logout and authentication stops
- When the remote authentication servers are down and local authentication is used, the user must log in using 5620 SAM credentials, as described in “Combined local and remote authentication”.

2.6 Remote authentication and authorization

The 5620 SAM uses a JAAS security framework to provide authentication and authorization services. When a user logs in to the 5620 SAM, the authentication method used depends on the 5620 SAM login module configuration. The 5620 SAM supports the following remote authentication login modules:

- RadiusJaasLoginModule
- TacacsPlusJaasLoginModule

The JAAS security framework integrates the login modules with the 5620 SAM. During startup, the 5620 SAM reads a file that contains the JAAS login module configuration. Depending on the VSA configuration in the file, one of the following authentication and authorization methods is available for remote users that do not have a 5620 SAM user account:

- The remote server authenticates the user and the 5620 SAM assigns a user group.
- The remote server authenticates the user and assigns a user group.

When the 5620 SAM assigns a user group to a remote user, a default external user group must be present in the 5620 SAM. User authentication succeeds when the remote authentication server validates the user password. User authorization succeeds and the user is provided with access rights when the default external user group is associated with the user. The 5620 SAM then creates a remote user account for the login session. In this scenario, when the default external user group is not specified, authorization fails and the user is denied access.

When the remote authentication server assigns a user group to a remote user, VSA support must be enabled in the JAAS login module configuration. In this scenario, a user group must be defined on the remote authentication server, and the remote server administrator must load the 5620 SAM RADIUS dictionary on the RADIUS server. The Sam-security-group-name VSA in the dictionary is used to configure a RADIUS remote user on the RADIUS server. The user group that is defined in the VSA must exist in the 5620 SAM. The remote authentication server administrator must specify the user group in the user configuration on the authentication server.

When the remote user logs in to the 5620 SAM, authentication succeeds when the remote authentication server validates the user password. Authorization succeeds and the user is provided with access rights when the user group defined on the remote server is sent to the 5620 SAM and validated. If the user group name matches a user group name in the 5620 SAM, the 5620 SAM creates a remote user account for the login session. Otherwise, authorization fails and user access is not granted.

See Procedure 2-35 for information about how to configure remote authentication and authorization for remote-only users.

In RADIUS, the authentication success message that is sent to the 5620 SAM contains the user group name. In TACACS+, authentication must succeed before an authorization message containing the user group name is sent to the 5620 SAM.

Successful remote authentication for an OSS user requires that the remote server and the 5620 SAM use the same password format. The OSS users can log in using a clear text password or an MD5-hashed password if the remote authentication server supports MD5-hashed password. See “Secure communication” in the *5620 SAM XML OSS Interface Developer Guide* for more information.

When a remote 5620 SAM GUI or OSS session terminates, the user account for the session does not get deleted. This allows remote authenticated users to keep details such as filters defined between sessions.

One-time password use

For increased security, a GUI user can provide an authentication token to a RADIUS or TACACS+ server that is validated only once. This is called one-time password use. You can enable one-time password use during 5620 SAM remote authentication policy configuration. See Procedure 2-34 for more information.

Note 1 — The one-time password function is not available to OSS clients.

Note 2 — To change the one-time password setting in a remote authentication policy, you require a scope of command that has Update/Execute access to the srmrmtauth package.

After a communication failure between a GUI client and a 5620 SAM main server when one-time password use is in effect, the GUI client is unable to obtain authentication using the cached credentials from the previous login attempt. When this occurs, the client prompts the GUI user to log in to the remote authentication server again, but does not automatically close the GUI, in order to preserve the current view until the user is ready to log in again.

Combined local and remote authentication

Many organizations already have existing TACACS+ or RADIUS authentication of users, based on long standing TACACS+ and RADIUS user accounts and passwords. You can incorporate new 5620 SAM user accounts for local 5620 SAM authentication with existing TACACS+ or RADIUS user accounts.

Consider the following:

- A system administrator can integrate the existing TACACS+ or RADIUS user accounts with 5620 SAM user accounts.
- You can create a 5620 SAM user name that exactly matches a TACACS+ or RADIUS user name.
- A 5620 SAM user name can be 1 to 80 characters in length, which is sufficient to match most remote authentication user names.

- 5620 SAM users who currently authenticate remotely can log in to the 5620 SAM using their RADIUS or TACACS+ passwords.
- 5620 SAM user authentication requires an account password that observes the 5620 SAM password constraints described in this chapter.

Note — When the samvsa parameter in the 5620 SAM JAAS configuration file is set to true, the 5620 SAM requires a user group from the remote server for authorization and the following conditions apply:

- If a 5620 SAM user account is associated with a local user group and configured to use remote authentication, the local user group is replaced by the remote user group.
- The user group sent by the remote server must exist in the 5620 SAM, otherwise, authentication fails.

The samvsa flag is set to false by default. See "Remote authentication and authorization" in this chapter and Procedure 2-35 for more information about configuring the 5620 SAM VSA.

For example, a user named jane has the following accounts:

- a remote RADIUS account called jane and the password accessforjane
- a local 5620 SAM account called jane and the password LetJane1In!

When jane is authenticated by RADIUS, she gains access to the 5620 SAM by typing in jane and accessforjane. If the RADIUS server is down, jane is authenticated locally by the 5620 SAM after typing jane and LetJane1In!.

2.7 Workflow to configure and manage 5620 SAM user security

1. Assess the requirements for user access to the different 5620 SAM functional areas and develop a strategy for implementing user security. See section 2.2 for more information.

2. Reserve a client GUI session for the admin user to ensure that the admin user can always log in. See Procedure 2-1 for more information.

3. Create scope of command roles or modify the default role to meet your operational requirements. See Procedure 2-2 for more information.

4. Create scope of command profiles that contain the appropriate scope of command roles for the types of tasks to be performed. See Procedure 2-3 for more information.

5. Create spans or modify the default span to meet your operational requirements. Add 5620 SAM managed objects to the spans. See Procedure 2-4 for more information.

6. Create span of control profiles that contain the required spans. See Procedure 2-5 for more information.

7 Create span rules, as required, to automatically assign new services to spans other than the Default Service Span. See Procedure 2-6 for more information.

8 Manage user groups, as required.

- Create or modify user groups and assign scope of command and span of control profiles to each group, as required. See Procedure 2-7 for more information.
- Add workspaces to user groups. See Procedure 2-8 for more information.
- Delete workspaces from user groups. See Procedure 2-9 for more information.

9 Create, modify, or copy user accounts for performing the tasks that are associated with each user group. See Procedures 2-11 and 2-12 for more information.

10 Configure global user account parameters, as required.

- user-account expiry periods, password criteria, and a GUI inactivity timeout; see Procedure 2-13 and 2-14 for more information
- minimum username length; see Procedure 2-15.
- allowed number of authentication attempts; see Procedure 2-16.
- suspended account actions; see Procedure 2-17.
- automated e-mail notification; see Procedure 2-18.

11 Configure global user activity log information, as required using the 5620 SAM system preference form. See Procedure 5-24 for more information.

12 Manage user accounts, as required.

- List inactive user accounts; see Procedure 2-19.
- Suspend or reinstate user accounts; see Procedures 2-20.
- Manage passwords.
  - As administrator, change the password of a specified 5620 SAM user account; see Procedure 2-21.
  - Force a specified 5620 SAM user to change the account password during the next login attempt; see Procedure 2-22.
  - Change the account password of the current user; see Procedure 2-23.
- Export user tab preferences; see Procedure 2-24.
- Assign user tab preferences; see Procedure 2-25.

13 Monitor and manage the active client sessions, as required.

- Broadcast a message to one or more 5620 SAM GUI users; see Procedure 2-26 for more information.
- List and optionally close GUI client sessions; see Procedure 2-27 for more information.
- List and optionally close OSS client sessions; see Procedure 2-28 for more information.
- View the 5620 SAM user activity logs to monitor GUI and OSS user activity. See Procedures 2-29 and 2-30 for more information.

14 As required, configure or manage the following 5620 SAM security functions to meet your operational requirements:

- Create a proprietary client GUI login screen. See Procedure 2-31 for more information.
- Change the maximum number of concurrent 5620 SAM admin user sessions. See Procedure 2-32 for more information.
- Limit the number of client sessions that the 5620 SAM accepts from one or more client delegate servers. See Procedure 2-33 for more information.
- Specify 5620 SAM RADIUS and TACACS+ authentication for 5620 SAM user accounts, as required. See Procedure 2-34.
- Configure authentication and authorization for remote users in which either the 5620 SAM or the remote authentication server associates the user with a user group. See Procedure 2-35 for more information.

15 As required, change the default parameter setting for the Task Manager to meet your operational requirements, see Procedure 2-36.

See “To monitor the 5620 SAM Task Manager” in the *5620 SAM User Guide* for more information on monitoring operational tasks.

16 As required, 5620 SAM delete security elements that are no longer required, such as the following:

- user accounts; see Procedure 2-37
- user groups; see Procedure 2-38
- user spans; see Procedure 2-39
- span of control profiles; see Procedure 2-40
- scope of command roles; see Procedure 2-41
- scope of command profiles; see Procedure 2-42

17 Export or import all workspaces and tab preferences, as required.

- Export all workspaces and tab preferences; see Procedure 2-43.
- Import all workspaces and tab preferences, import workspaces only, or import tabs only; see Procedure 2-44.

2.8 5620 SAM user security procedures

This section provides the procedures to create and manage 5620 SAM user security functions:

Procedure 2-1 To reserve an admin account login

You can reserve one client GUI session, from the maximum number of sessions allowed by the license key, for admin users only. This allows an administrator to manage the existing client GUI sessions.

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Configure the Reserve Administrator Login parameter.

3 Click on the OK button to save the changes and close the form. A dialog box appears.

4 Click on the Yes button.

5 Log in as required.

Procedure 2-2 To create a scope of command role

Perform this procedure to create a set of user permissions that define an operator role. You can apply one or more scope of command roles to a user group using a scope of command profile.

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Click on the Scope of Command tab.

3 Click on the Create button and choose Role. The Role (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Auto-Assign ID
- Role ID
- Role Name
- Description

5 Perform the following steps to configure the permissions for the scope of command role.

i Click on the Permissions tab. A list of the 5620 SAM packages, methods, and classes is displayed.

Note — When you enable the Create permission for a 5620 SAM package, method, or class, the Update/Execute permission is automatically enabled.

When you enable the Update/Execute permission for a 5620 SAM package, method, or class, the Create permission is not automatically enabled.

ii Select the required access permissions, which are displayed in the list column headings, for each package, class, or method that you need to assign to the scope of command role.

6 Click on the OK button. The Role (Create) form closes.

7 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 2-3 To create a scope of command profile

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Click on the Scope of Command tab.

3 Click on the Create button and choose Profile. The Scope of Command Profile (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Auto-Assign ID
- Profile ID
- Profile Name
- Description

5 Perform the following steps to assign one or more scope of command roles to the profile.

i Click on the Roles tab.

ii Click on the Add button. The Select Role - Role form opens.

iii Select one or more roles and click on the OK button. The Select Role - Role form closes and a dialog box appears.

iv Click on the OK button.

v Click on the OK button. The Scope of Command Profile (Create) form closes.

6 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 2-4 To create a span of control

Perform this procedure to specify a set of 5620 SAM objects in a span of control and the type of user access available for the objects. You can apply one or more spans to a user group using a span of control profile.

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Click on the Span of Control tab.

3 Click on the Create button and choose Span. The Span (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Auto-Assign ID
- Span ID
- Span Name
- Description

5 Click on the Contents tab.

6 Click on the Add button and choose an object type from the menu. The Select *(object_type)* list form opens.

7 Select one or more objects and click on the OK button. The Select *(objects)* list form closes and the objects are listed on the Span (Create) form. A dialog box appears.

8 Click on the OK button. The Span (Create) form closes.

9 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 2-5 To create a span of control profile

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2 Click on the Span of Control tab.

3 Click on the Create button and choose Profile. The Span of Control Profile (Create) form opens with the General tab displayed.

4 Configure the parameters:

- Auto-Assign ID
- Profile ID
- Profile Name
- Description

5 Perform the following steps to assign one or more spans to the profile.

i Click on the Spans tab. The pre-defined spans are listed.

ii Click on the Add button and choose an access type. The Select *access_type* Spans form opens.

iii Select one or more spans in the list and click on the OK button. The Select *access_type* Spans form closes, and a dialog box appears.

iv Click on the OK button. The spans are listed on the Span of Control Profile (Create) form with the type of access displayed in the Access Type column.

6 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 2-6 To create a span rule

Perform this procedure to create a span rule. A span rule is a policy that specifies to which span of control profiles, in addition to the Default Service Span, a newly created service is automatically assigned

1 Using an account with an assigned security scope of command role, choose Administration→Span Rules from the 5620 SAM main menu. The Span Rules form opens.

2 Click on the Create button. The Service Creation Span Rule (Create) form appears.

3 Configure the parameters:

- Auto-Assign ID
- Span Rule ID
- Name
- Created In

4 Perform the following steps to associate one or more spans with the rule.

i Click on the Spans tab.

ii Click on the Add button. The Select Span(s) form opens.

- **iii** Select one or more spans in the list.
- **iv** Click on the OK button. The Select Span(s) form closes and the selected spans are listed on the Service Creation Span Rule (Create) form.

5 Perform the following steps to associate one or more format or range policies with the rule.

- **i** Click on the Format and Range Policies tab.
- **ii** Click on the Add button. The Select Format or Range Policies form opens.
- **iii** Select one or more policies in the list.
- **iv** Click on the OK button. The Select Span(s) form closes and the selected policies are listed on the Service Creation Span Rule (Create) form.

6 Click on the OK button. The Service Creation Span Rule (Create) form closes.

Procedure 2-7 To create a 5620 SAM user group

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Click on the User Groups tab.

3 Perform one of the following:

- **a** Create a new group by clicking on the Create button. The User Group (Create) form opens with the General tab displayed.
- **b** Modify an existing group by performing the following steps.
  - **i** Set the filter criteria.
  - **ii** Click on the Search button. A list of groups is displayed.
  - **iii** Select a group in the list and click on the Properties button. The User Group (Edit) form opens with the General tab displayed.

4 Configure the parameters:

- User Group
- Description
- User Group State
- Apply Local Authentication Only
- Maximum User Sessions Allowed
- Account Expiry
- Password Expiry
- Override Global Timeout
- Client Timeout (minutes)

The Maximum User Sessions Allowed parameter is configurable when the Enable check box is selected.

5 If the user group is for OSS users or remote GUI users, configure the parameters in the Remote Users panel:

- Maximum GUI Sessions Allowed
- Maximum OSS Sessions Allowed
- OSS Request Priority
- OSS Request Timeout (seconds)

The Maximum GUI Sessions Allowed and Maximum OSS Sessions Allowed parameters are configurable when the Enable check box beside each is selected.

6 Perform the following steps to assign a scope of command profile to the user group.

i Click on the Select button in the Scope of Command panel. The Select Scope of Command Profile form opens.

ii Select a profile in the list and click on the OK button. The Select Scope of Command Profile form closes, and the User Group (Create) form displays the scope of command profile name.

7 Perform the following steps to assign a span of control profile to the user group.

i Click on the Select button in the Span of Control panel. The Select Span of Control Profile form opens.

ii Select a profile in the list and click on the OK button. The Select Span of Control Profile form closes, and the User Group (Create) form displays the span of control profile name.

8 If you are creating a new user account, perform the following steps.

i Click on the OK button. The User Group (Create) form closes.

ii Go to step 15.

9 Click on the Format and Range Policies tab.

10 Click on the Add button. The Select Format or Range Policies form opens.

11 Select one or more policies in the list and click on the OK button.

12 Click on the OK button. A dialog box appears.

Note — When you change the scope of command or span of control profiles of a group, the permissions of each user in the group are altered immediately when you click on the OK button.

13 Click on the Yes button. The User Group (Create) form closes.

14 If an active client GUI session is affected by the user group modification, restart the GUI client.

15 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 2-8 To add workspaces to a user group

1 Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Click on the User Groups tab.

3 Perform one of the following:

- **a** Create a group by clicking on the Create button. The User Group (Create) form opens with the General tab displayed. See Procedure 2-7.
- **b** Modify a group by performing the following steps. See Procedure 2-7.
    - **i** Set the filter criteria.
    - **ii** Click on the Search button. A list of groups is displayed.
    - **iii** Select a group from the list and click on the Properties button. The User Group (Edit) form opens with the General tab displayed.

4 Configure the Allow Mandatory Workspaces Only parameter in the Mandatory Workspaces panel:

- **a** Select the Allow Mandatory Workspaces Only check box.

Note 1 — The Add button on the User Preferences→Workspaces form will be disabled and the user cannot change the list of workspaces on their User Preferences form.

Note 2 — Any existing user-defined workspaces in the User Preferences form are deleted when the Allow Mandatory Workspaces Only check box is selected by the Administrator.

Note 3 — The user can change the order that the workspaces appear in the workspace selector and set any workspace as the default workspace.

- **b** Deselect the Allow Mandatory Workspaces Only check box.

Note 1 — The user can add additional workspaces to their workspace selector by clicking on the Add button in the User Preferences form. See "5620 SAM GUI custom workspace procedures" in the *5620 SAM User Guide* for more information.

Note 2 — The user can change the order that the workspaces appear in the workspace selector and set any workspace as the default workspace.

5 To add mandatory workspaces to a specific user group:

- **i** Click on the Add button. The Add Workspace form opens.
- **ii** Click on the Search button to display a list of workspaces.
- **iii** Choose a workspace from the list and click on the OK button. The workspace is displayed on the User Group (Edit) form.

Note — All mandatory workspaces that are added to the user group by the Administrator appear in the User Preferences→Workspaces form and in the workspace selector drop-down for each user in the user group and cannot be deleted.

6 Click on the Move Up or Move Down buttons to move the workspaces up or down. The workspace at the top of the list is the default workspace.

Note 1 — You need a minimum of one workspace in the User Group.

Note 2 — If the last user workspace is deleted, the users default workspace in the User Preferences form is replaced by the user group default workspace.

7 Click on the OK button. A dialog box appears.

8 Click on the Yes button. The User Group (Create) form closes.

9 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 2-9 To delete workspaces from a user group

1 Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2 Click on the User Groups tab.

3 Set the filter criteria and click on the Search button. A list of groups is displayed.

4 Select a group from the list and click on the Properties button. The User Group (Edit) form opens with the General tab displayed.

5 Choose a workspace in the Mandatory Workspaces panel.

6 Click on the Delete button to delete a workspace.

7 Click on the OK button. A dialog box appears.

8 Click on the Yes button. The User Group (Create) form closes.

Note 1 — You need a minimum of one workspace in the User Group.

Note 2 — If the last user workspace is deleted, the users default workspace in the User Preferences form is replaced by the user group default workspace.

Procedure 2-10 To add access permissions for web applications to a user group

Perform this procedure to add access permissions to the 5620 SAM web applications for a user group. The default admin user group has full access to the web applications.

1 Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Click on the User Groups tab.

3 Perform one of the following:

  a Create a group by clicking on the Create button. The User Group (Create) form opens with the General tab displayed. See Procedure 2-7.

  b Modify a group by performing the following steps. See Procedure 2-7.

    i Set the filter criteria.

    ii Click on the Search button. A list of groups is displayed.

    iii Select a group from the list and click on the Properties button. The User Group (Edit) form opens with the General tab displayed.

4 Enable the web applications for which you want to grant access to the user group.

Note — If you change the access permissions to a web application when a user in a user group is logged on to the web application, the changes are not effective until the user logs off and logs on again.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button. The User Group (Create) form closes.

7 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 2-11 To create a 5620 SAM user account

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2 Click on the Users tab

3 Perform one of the following:

- **a** Create a new user account by clicking on the Create button. The User (Create) form opens with the General tab displayed.
- **b** Modify an existing user account by performing the following steps.
    - **i** Set the filter criteria.
    - **ii** Click on the Search button. A list of user accounts is displayed.
    - **iii** Select an account in the list and click on the Properties button. The User (Edit) form opens with the General tab displayed.

4 Configure the general user parameters:

- User Name
- Description
- User State
- E-mail Address
- Password Change Required
- User Password
- Confirm Password

5 If required, test the validity of the user e-mail address by clicking on the Test E-mail button beside the E-mail Address parameter.

Note — Before you test the validity of the user e-mail address, ensure that the outgoing SMTP e-mail server and e-mail test message are configured. See Procedure 2-18 for information about configuring the outgoing e-mail server and test message.

6 Click on the Select button and use the list form that opens to choose a user group.

7 For a local GUI user, configure the Maximum Sessions Allowed parameter, which is configurable when the Enable check box beside the parameter is selected.

8 To configure an OSS user account, perform the following steps.

- **i** Configure the parameters in the OSS Session panel:
    - Maximum OSS Sessions Allowed
    - OSS Request Priority
    - OSS Request Timeout (seconds)
- **ii** To apply a GUI alarm filter to alarm information requests from the OSS user, click on the Select button in the OSS Session panel and use the list form that opens to choose an alarm filter.

9 Configure the parameters in the Client IP Address panel:

- Valid Client IP address
- Enable IP Address validation

10 If you are creating a new user account, perform the following steps.

i Click on the OK button. The User Group (Create) form closes.

ii Go to step 16.

11 Click on the Format and Range Policies tab.

12 Click on the Add button. The Select Format or Range Policies form opens.

13 Select one or more policies in the list and click on the OK button.

14 Click on the OK button. A dialog box appears.

15 Click on the Yes button. The User (Edit) form closes.

16 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 2-12 To copy a 5620 SAM user account

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2 Click on the Users tab.

3 Set the filter criteria and click on the Search button. A list of configured users opens.

4 Choose a user and click on the Properties button. The User *type_of_user*, Group *user_group* (Edit) form opens.

5 Click on the Copy button. A User (Create) form opens for the second user.

6 Configure the parameters, as required. You must change the User Name parameter and configure the User Password and Confirm Password parameters.

7 Click on the OK button to save the changes and close the form.

8 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 2-13 To configure expiry periods and a GUI inactivity timeout

You can configure global expiry periods for user accounts, passwords, and client GUI inactivity checks. You can configure per user group expiry periods for client GUI inactivity checks. You can enable a password history count.

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Configure the Password History Duration (days) and Password Reuse Cycle parameters.

3 Configure the global expiry period parameters:

- Account Expiry (days)
- Password Expiry (days)
- Client Timeout (minutes)
- Advance Password Expiry Notification (days)

If you set any of the parameters to 0, the corresponding expiry period check is disabled. To change the client inactivity check timeout for individual user groups, see Procedure 2-7.

4 Click on the OK button to save the changes and close the form. A dialog box appears.

5 Click on the Yes button.

When a user attempts to log in with an expired password, the user account is suspended. When a user updates their password, the password expiry period is reset, and the new password again expires when the Password Expiry (days) parameter value is reached.

Procedure 2-14 To configure the GUI inactivity timeout

A 5620 SAM user with an admin scope of command role can configure a GUI inactivity check that applies to all client GUIs, or to sets of users based on the associated user groups.

1 Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2 To change the GUI inactivity check for all 5620 SAM GUI users, perform the following steps.

i Configure the Client Timeout (minutes) parameter.

ii Click on the Apply button.

3 To change the GUI inactivity check for all users in a user group, perform the following steps.

  i Click on the User Groups tab. A list of user groups is displayed.

  ii Choose a user group from the list and click on the Properties button. The User Group *name* (Edit) form opens.

  iii Enable the Override Global Timeout parameter.

  iv Configure the Client Timeout (minutes) parameter.

  v Click on the OK button. A dialog box appears.

  vi Click on the Yes button. The User Group (Edit) form closes.

4 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 2-15 To configure the minimum allowable user name length

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 In the User Name panel, check the Enable box.

3 Configure the Minimum User Name Length Allowed parameter. Select a range between 5 to 40 characters, the minimum is 5 characters.

4 Click on the OK button to save the changes and close the form. A dialog box appears.

5 Click on the Yes button.

Procedure 2-16 To configure authentication failure actions

You can specify an authentication message or a lockout for a user account that exceeds the configured number of login authentication attempts. Only non–admin accounts can be locked out, as admin accounts always have access.

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Click on the E-mail tab.

3 Configure the authentication failure action parameters:

- Attempts before lockout
- Attempts before e-mail
- E-mail Subject
- E-mail text

If you set the Attempts before lockout parameter to 0, the lockout function is disabled.

4 Click on the OK button to save the changes and close the form. A dialog box appears.

5 Click on the Yes button.

Procedure 2-17 To configure suspended account actions

You can specify a suspended account message for a user account when you suspend the user account using the User State parameter.

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Click on the E-mail tab.

3 Configure the suspended account parameters:

- E-mail Subject
- E-mail text

4 Click on the OK button to save the changes and close the form. A dialog box appears.

5 Click on the Yes button.

Procedure 2-18 To configure automated e-mail notification

Perform this procedure to configure the 5620 SAM to automatically send e-mail messages to users and administrators; for example, when locking out a user account that exceeds the allowed number of authentication attempts.

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Click on the E-mail tab.

3 Configure the outgoing e-mail server SMTP parameters:

- Server
- E-mail User Name
- E-mail User Password
- E-mail Address

4 Configure the Test Message parameter.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button. The 5620 SAM User Security - Security Management (Edit) form closes.

Procedure 2-19 To list inactive user accounts

1 Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Click on the Users tab.

3 Click on the Inactive User Search button and perform one of the following.

a Choose ≥90 Days.

b Choose ≥180 Days.

c Specify another period; perform the following steps.

i Choose Custom User Inactivity Period. The Custom User Inactivity Period form opens.

ii Configure the User inactive greater than or equal to parameter.

iii Click on the OK button. The Custom User Inactivity Period form closes.

User accounts that have been inactive for a number of days that is greater than or equal to the specified value are listed on the 5620 SAM User Security - Security Management (Edit) form.

4 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 2-20 To suspend or reinstate a 5620 SAM user account

1 Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2 Click on the Users tab.

3 Specify a filter, if required, and click on the Search button.

4 Select a user account in the list.

5 Click on the Properties button. The User *type_of_user* (Edit) form opens.

6 Configure the User State parameter to suspend or reinstate the user account.

7 Click on the OK button. A dialog box appears.

8 Click on the Yes button. The User *type_of_user* (Edit) form closes.

9 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 2-21 To administratively change the password of a 5620 SAM user

The system administrator uses the Security Management form to maintain user accounts. The user can change their password in a separate form. If a user forgets their password, the system administrator can change the password and inform the user of the new password.

1 Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2 Click on the Users tab.

3 Specify a filter to create a filtered list of users and click on the Search button.

4 Choose a user from the user list.

5 Click on the Properties button. The User *type_of_user* (Edit) form opens.

6 Configure the User Password parameter and the Confirm Password parameter.

7 Click on the Apply button to save the changes.

8. Verify the action.
9. Close the form.

When a user attempts to log in with an expired password, the user account is suspended. When a user updates their password, the password expiry period is reset, and the new password again expires when the Password Expiry (days) parameter value is reached.

Procedure 2-22 To force a 5620 SAM user password change

Perform this procedure to force a specific 5620 SAM user to change the user password during the next login attempt.

Note — This change does not affect the current user session.

1. Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.
2. Click on the Users tab.
3. Specify a filter to create a filtered list of users and click on the Search button.
4. Choose a user from the user list.
5. Click on the Properties button. The User *type_of_user* (Edit) form opens.
6. Enable the Password Change Required check box to request a password change for the user.
7. Click on the Apply button to save the changes.
8. Verify the action.
9. Close the form.

The next time the user logs in to the 5620 SAM, the 5620 SAM prompts the user to change the password. After the user changes the password, the Password Change Required check box returns to the default of unchecked.

Procedure 2-23 To change the password of the current 5620 SAM user

Perform this procedure to change the password associated with the currently active 5620 SAM user account.

Note 1 — When a user attempts to log in with an expired password, the user account is suspended.

Note 2 — When a user updates a password, the password expiry period is reset.

1. Choose Administration→Security→Change Password from the 5620 SAM main menu. The Password Change form opens.
2. Verify that the Login Name matches your user account name.
3. Configure the parameters:
    - Old Password
    - New Password
    - Confirm Password
4. Click on the OK button. The Password Change form closes.

Procedure 2-24 To export user tab preferences

Perform this procedure to export tab preferences of single or multiple users to a specified directory. You can reuse these saved tab preferences by importing them into another 5620 SAM server.

1. Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.
2. Click on the Users tab.
3. Choose one or more users from the list.
4. Click on the Tab Preferences button and choose Export from the drop-down menu to export the selected user(s) tab preferences to a specified directory. The Export Directory window opens.
5. Specify the export directory in the Save In drop-down menu, or create a directory or folder, and click on the Save button. The selected user(s) tab preferences are exported to the specified directory.
6. Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 2-25 To assign tab preferences to users

Perform this procedure to assign exported single user tab preferences to all selected users in the 5620 SAM client.

1 Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Click on the Users tab.

3 Choose one or more users from the list.

4 Click on the Tab Preferences button and choose Assign from the drop-down menu to assign the tab preferences from the specified directory, to all the selected users. The Import Directory window opens.

5 In the Look In drop-down menu, navigate to the directory from which you need to assign a tab preference.

Note — Only a single users tab preferences can be in the specified directory or an error message appears.

6 Click on the Open button. A confirmation dialog box appears.

7 Click on the Yes button. The assigned tab preferences overwrite the tab preferences of the selected users.

All affected users who currently have a client session opened, other than the client session where the assign has been initiated, will receive a system-generated text message informing them that their tab preferences have been changed and they should restart their 5620 SAM client or risk losing the changes.

The user can click on the reply button to reply to the message.

8 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 2-26 To send a broadcast message to 5620 SAM GUI users

Perform this procedure to send a broadcast messages, for example, a maintenance notification, to some or all active GUI users.

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2 Click on the Sessions tab.

3 Specify a filter to create a filtered list of GUI client sessions and click on the Search button. A list of active client sessions is displayed.

4 Select the required client sessions in the list.

5 Click on the Text Message button. The Text Message form opens.

6 Enter a message in the Text Message form.

7 Click on the OK button. The 5620 SAM sends the text message to the selected clients.

8 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 2-27 To view and manage the active 5620 SAM client sessions

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2 Click on the Sessions tab.

3 Specify a filter to create a filtered list of GUI or 5620 SAM-O JMS client sessions and click on the Search button. The active client sessions are listed.

4 Review the following session information:

- associated user name
- ID
- user login time and date
- client IP address
- user group
- session type, which is 5620 SAM for a GUI client, or SAMOSS for an OSS client

5 If required, close a GUI client session; perform the following steps.

Note — Closing a 5620 SAM-O session has additional dependencies; see Procedure 2-28 for more information.

i Select a session in the list and click on the Close Session button.

ii Click on the Yes button. The client session closes.

6 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 2-28 To disconnect a 5620 SAM-O JMS client connection or remove a durable subscription

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.

2 Click on the Messaging Connections tab.

3 Specify a filter and click on the Search button. A list of active 5620 SAM-O client connections opens.

4 Select a connection in the list and perform one of the following:

- **a** Click on the Close Connection button to shut down the client connection.
- **b** Click on the Remove Connection button to shut down the client connection and remove the durable subscription.

A dialog box appears.

5 Click on the Yes button. The action is performed.

If you choose Close Connection, the connection is terminated, but the 5620 SAM server continues to store JMS messages for the session.

If you choose Remove Connection, the 5620 SAM server stops storing the JMS messages for the session.

Note — When you remove a durable subscription, the OSS client can still attempt to connect to the 5620 SAM-O. You can prevent an OSS client from attempting to connect by suspending the OSS user account. See Procedure 2-20 for more information.

6 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 2-29 To view the user activity log

Perform this procedure to view the user activity log entries associated with the following:

- a user
- a client session

Note 1 — Viewing user activity records other than LI activity records requires a user account with an assigned Administrator or 5620 SAM Management and Operations scope of command role.

Note 2 — Viewing LI user activity records requires a user account with an assigned Lawful Interception Management scope of command role. The scope is restricted to the records of users in the same LI user group.

1 Choose Administration→Security→User Activity from the 5620 SAM main menu. The 5620 SAM User Activity form opens with the Session tab displayed.

2 Perform one of the following:

a View the activities performed during a specific client session. Perform the following steps.

i Configure the filter criteria, if required, and click on the Search button. A list of session entries is displayed.

Note — Only client session entries with a State value of Connected contain activity entries.

ii Select the required session entry and click on the Properties button. The Session form opens with the General tab displayed.

iii Click on the Activity tab.

iv Configure the filter criteria, if required, and click on the Search button. A list of activity entries is displayed.

b View the activities of a specific user. Perform the following steps.

i Click on the Activity tab.

ii Specify the required username as the Username filter criterion and click on the Search button. A list of user-specific entries is displayed.

3 Select an entry in the list and click on the Properties button. The Activity form opens with the General tab displayed.

4 Review the general information, which matches the columnar information on the User Activity list form.

5 Depending on the activity Type and Sub Type, the Additional Info panel contains detailed activity information. If required, expand the panel to review the information. The following information is listed:

- **Type Operation, all Sub Types:**
  - left pane—object hierarchy in tree form; each object is selectable
  - right pane—properties and values of selected object in left pane

    The Actions property, which is highlighted in yellow for an object creation or modification activity, has values that represent the actions associated with the activity, such as create and modify.
- **Type Deployment or Save, Sub Type Modification:**
  - Property Name column—list of modified parameters
  - New Value column—the parameter value set during the activity
  - Old Value column—the previous parameter value

6 If required, expand the XML panel to display more information about the activity. The panel displays the following information:

- Full Class Name—the 5620 SAM class descriptor of the affected object type
- Additional Info—the activity details in the form of an XML request

Note — The displayed Additional Info text is limited to 4000 characters. If an activity generates more than 4000 characters of XML text, for example, access interface creation, the Additional Info panel of the log entry contains a “truncated” object, and the XML text contains a closing <truncated/> tag.

7 To navigate directly to the object of the activity, click on the View Object button. The object properties form opens.

Note — The View Object button is dimmed when there is no object associated with the activity, for example, a user login or logout operation.

8 Close the open forms, as required.

Procedure 2-30 To view the user activity associated with an object

Perform this procedure to navigate from the properties form of an object to a form that lists the recent user actions associated with the object.

1 Open the required object properties form.

2 Click on the User Activity button, or click on the More Actions button and choose User Activity. The Activity form opens.

Note — The User Activity function is available only for objects that exist in the 5620 SAM database. For example, the function is not available on the User Preferences form, because the settings on the form are saved in the client or client delegate file system.

3 Review the activity entries as described in Procedure 2-29.

4 Close the open forms, as required.

Procedure 2-31 To create a proprietary 5620 SAM login statement

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Configure the security statement parameters:

- Enabled
- Statement

3 Click on the OK button. A dialog box appears.

4 Click on the Yes button. The 5620 SAM User Security - Security Management (Edit) form closes.

The Statement parameter text is displayed on the login form during each subsequent client GUI login attempt.

Procedure 2-32 To change the maximum number of concurrent 5620 SAM admin user sessions

Perform this procedure to configure the maximum number of 5620 SAM admin user sessions that can be active concurrently.

1 Log in to the main server station as the samadmin user.

2 Navigate to the server configuration directory, typically /opt/5620sam/server/nms/config.

3 Create a backup copy of the nms-server.xml file.

4 Open the nms-server.xml file using a plain-text editor.

Caution — Contact your Alcatel-Lucent technical support representative before you attempt to modify the nms-server.xml file. Modifying the nms-server.xml file can have serious consequences that can include service disruption.

5 Locate the following XML tag:

```
<samsession
```

This section of the file contains the maximum number of admin sessions that can be configured.

```
max5620SAMAdminSessions="value"
```

where *value* is the max number of allowed admin user sessions.

6 Save and close the nms-server.xml file.

7 Open a console window.

8 Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin.

9 Enter the following at the prompt:

```
bash$ ./nmsserver.bash read_config ↵
```

The main server reads the nms-server.xml file and the number of sessions defined.

10 Log out of the main server.

11 Close the open console windows, as required.

Procedure 2-33 To configure the number of allowed client sessions for a client delegate server

Note — The 5620 SAM continues to accept new client sessions from a client delegate server after the allowed number of sessions is reached. The maximum number of sessions is to be used as a guide for balancing the client session load among multiple client delegate servers.

1 Using an account with Update permission on the Server package, choose Administration→System Information from the 5620 SAM main menu. The System Information form opens with the General tab displayed.

2 Click on the Client Delegate Servers tab.

3 Specify a filter and click on the Search button. A list of client delegate servers is displayed.

4 Select an entry in the list and click on the Properties button. The Client Delegate Server (Edit) form opens.

5 Configure the Maximum UI Sessions parameter.

6 Click on the OK button. The Client Delegate Server (Edit) form closes.

7 Closes the System Information form.

Procedure 2-34 To create RADIUS and TACACS+ authentication policies for 5620 SAM user accounts

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM RADIUS/TACACS+ User Authentication from the 5620 SAM main menu. The RemoteAuthenticationManager (Edit) form opens with the General tab displayed.

2 Configure the parameters:

- One Time Password
- Authentication Order 1
- Authentication Order 2
- Authentication Order 3

3 Click on the RADIUS tab to configure RADIUS authentication server parameters.

4 Click on the Create button. The SAM RADIUS Authentication Server (Create) form opens.

5 Configure the parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Description
- Address
- Port
- Retry Attempts
- Timeout (seconds)
- Secret Name

6 Click on the OK button to save the changes.

7 Verify the action.

8 Click on the TACACS tab to configure TACACS+ authentication server parameters.

9 Click on the Create button. The SAM TACACS+ Authentication Server (Create) form opens.

10 Configure the parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Description
- Address
- Timeout (seconds)
- Secret Name

11 Click on the OK button to save the changes.

12 Verify the action.

13 Click on the Faults tab to view alarms, as required.

14 Click on the OK button to save the changes and close the form.

Procedure 2-35 To configure remote authentication and authorization for remote-only users

Note 1 — Ensure that remote authentication is enabled. See Procedure 2-34 for information about creating RADIUS and TACACS+ authentication policies.

Note 2 — See "Remote authentication and authorization" in section 2.1 for information about remote authentication and authorization for remote-only users.

1 Perform one of the following:

a To configure remote authentication and authorization for remote-only users where the 5620 SAM provides the user group to which the user belongs, go to step 2.

Note — The samvsa flag must be set to false in the SamJaasLogin.config file. The default value is false. The SamJaasLogin.config file is located in the server installation configuration directory, typically C:\5620sam\client\nms\config or /opt/5620sam/server/nms/config.

b To configure remote authentication and authorization for remote-only users where the remote authentication server provides the user group to which the user belongs, go to step 3.

2 Specify the default external user group.

i Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

ii Configure the default external user group parameter: User Group.

iii Click on the Select button. The Select Group - TSecurityManager form opens.

iv Select a user group and click on the OK button. The Select Group - TSecurityManager form closes and the 5620 SAM User Security - Security Management (Edit) form refreshes with the selected user group.

Note — Do not select a user group that has the Apply Local Authentication Only parameter enabled. Doing so may cause subsequent login attempts to fail once the user is created locally in 5620 SAM.

v Click on the OK button. A dialog box appears.

vi Click on the Yes button. The 5620 SAM User Security - Security Management (Edit) form closes.

3 Modify the SamJaasLogin.config file.

> **Note —** Ensure that you create a backup of the SamJaasLogin.config file before you make any modifications to it.

i Log in to the 5620 SAM main server station as the samadmin user.

ii Navigate to the server configuration directory, typically /opt/5620sam/server/nms/config.

iii Open the SamJaasLogin.config file using a text editor.

iv If RADIUS authentication is enabled, find the RADIUSLogin section of the file and change the samvsa flag to true. Code 2-1 shows an example of the file text:

Code 2-1: RADIUS section of SamJaasLogin.config file

```
RADIUSLogin
{
  com.timetra.nms.server.jaas.provider.radius.auth.RadiusJaasLoginMo
dule REQUIRED
debug=false
  samvsa=true
;
};
```

If TACACS+ authentication is enabled, find the TACACSLogin section of the file and change the samvsa flag to true. Code 2-2 shows an example of the file text:

Code 2-2: TACACS+ section of SamJaasLogin.config file

```
TACACSLogin
{
  com.timetra.nms.server.jaas.provider.tacacs.auth.TacacsPlusJaasLog
inModule REQUIRED
debug=false
  samvsa=true
;
};
```

v Save the file.

vi Close the file.

vii Enter the following at the CLI prompt:

```
bash$ path/nms/bin/nmsserver.bash read_config ↵
```

where
path is the 5620 SAM server installation location, typically opt/5620sam/server

The 5620 SAM server puts the configuration changes into effect.

4 Define the user group VSA on the remote authentication server.

Note — Step 4 must be performed by the remote authentication server administrator.

Perform one of the following:

a If RADIUS authentication is enabled:

i Copy the example of the RADIUS dictionary below to the RADIUS dictionary file. Enter changes to the file based on your RADIUS configuration.

ii Configure the RADIUS user profile and add a previously defined 5620 SAM user group name to the Sam-security-group-name VSA. Code 2-3 shows an example of the RADIUS user group VSA:

Code 2-3: RADIUS user group VSA example

```
Sam-security-group-name="user_group_name_locally_defined_in_5620SAM"
```

The VSA configuration file contains information such as usernames, passwords, and the 5620 SAM user group name. The user authentication process returns the user group name in the Sam-security-group-name VSA of the access-accept message.

Code 2-4 shows an example of the RADIUS dictionary text:

Code 2-4: RADIUS dictionary text: example

```
###########################################################
#           Alcatel-Lucent 5620 SAM Server dictionary.    #
#  $ld: dictionary.alcatel.sam,v 1.1 2006/08/18 10:00:22$ #
############################################################
VENDOR          Alcatel-Lucent                      123
BEGIN-VENDOR                          Alcatel-Lucent
ATTRIBUTE       Sam-security-group-name      3      string
END-VENDOR                            Alcatel-Lucent
```

Note 1 — The user group must be a valid user group in the 5620 SAM.

Note 2 — The vendor ID must be 123.

b If TACACS+ authentication is enabled, define the 5620 SAM user group VSA in the user profile on the TACACS+ server. Code 2-5 shows an example of the TACACS+ user group VSA:

Code 2-5: TACACS+ user group VSA example

```
service=sam-app{
  sam-security-group="user_group_name_locally_defined_in_5620SAM"
```

}

Note — The user group must be a valid 5620 SAM user group.

Procedure 2-36 To change the 5620 SAM Task Manager default settings

Perform this procedure to change the default parameter setting for the Task Manager to meet your operational requirements. The Task Manager allows 5620 SAM operators to monitor the progress of operational tasks. Only 5620 SAM administrators can change task monitoring parameters.

Note — The Task Manager is operational with the default values.

1 Log in to the 5620 SAM main server station as the samadmin user.

2 Navigate to the server configuration directory, typically /opt/5620sam/server/nms/config.

3 Open the nms-server.xml file using a text editor.

Caution — Contact your Alcatel-Lucent technical support representative before you attempt to modify the nms-server.xml file. Modifying the nms-server.xml file can have serious consequences that can include service disruption.

4 Find and configure the parameters to fit your operational requirements.

- maxNumRetainedTasks
- numTasksToPurgeWhenFull
- successfulTasksPurgeInterval
- failedTasksPurgeInterval

5 Save and close the nms-server.xml file.

Note — If one or more of the parameters are changed from their default values, you must restart the 5620 SAM server for the changes to take effect.

6 Open a console window.

7 Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin.

8 Enter the following to restart the main server:

```
bash$ ./nmsserver.bash force_restart ↵
```

The main server restarts, and the configuration change takes effect.

9 As required, modify the nms-client.xml file on the 5620 SAM standby server station.

- **i** Navigate to the client configuration directory, typically /opt/5620sam/client/nms/config.
- **ii** Open the nms-client.xml file using a text editor.
- **iii** Configure the autoRefreshInterval parameter.
- **iv** Save and close the nms-server.xml file.
- **v** Repeat steps 6 to 8 to restart the 5620 SAM server for the changes to take effect.

10 Close the console windows, as required.

11 Close the form. See the *5620 SAM User Guide* to monitor the Task Manager.

Procedure 2-37 To delete a 5620 SAM user account

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Click on the Users tab.

3 Configure the filter criteria and click on the Search button. A list of user accounts is displayed.

4 Select an account in the list and click on the Delete button. A dialog box appears.

> **Note —** When a user account is associated with a scheduled task, you must decide whether to remove the schedules. If you do not need to remove the schedules, no schedules are removed. If you need to remove schedules, the schedules associated with the user account are removed if the schedule is not associated with a scheduled task. Schedules that are associated with a scheduled task are not removed.

5 Click on the Yes button. The 5620 SAM deletes the user account.

6 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 2-38 To delete a 5620 SAM user group

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Click on the User Groups tab.

3 Configure the filter criteria and click on the Search button. A list of user groups is displayed.

4 Select a group in the list and click on the Delete button. A dialog box appears.

Note — You cannot delete a user group that contains users.

5 Click on the Yes button. The 5620 SAM deletes the user group.

6 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 2-39 To delete a span of control

1 Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Click on the Span of Control tab.

3 Choose Span (Security) from the object drop-down menu and click on the Search button. A list of spans is displayed.

4 Select a span in the list and click on the Delete button. A dialog box appears.

Note — You cannot delete a default span, or a span in a span of control profile that is assigned to a user group that contains users.

5 Click on the Yes button. The 5620 SAM deletes the span of control.

6 Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 2-40 To delete a span of control profile

1. Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.
2. Click on the Span of Control tab.
3. Choose Profile (Security) from the object drop-down menu and click on the Search button. A list of span of control profiles is displayed.
4. Select a profile in the list and click on the Delete button. A dialog box appears.

Note — You cannot delete a span of control profile that is assigned to a user group that contains users.

5. Click on the Yes button. The 5620 SAM deletes the span of control profile.
6. Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 2-41 To delete a scope of command role

1. Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.
2. Click on the Scope of Command tab.
3. Choose Role (Security) from the object drop-down menu and click on the Search button. A list of scope of command roles is displayed.
4. Select a role in the list and click on the Delete button. A dialog box appears.

Note 1 — You cannot delete a pre-defined scope of command role.

Note 2 — You cannot delete a scope of command role that is assigned to a scope of command profile when the scope of command profile is assigned to a user group that contains users.

5. Click on the Yes button. The 5620 SAM deletes the scope of command role.
6. Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 2-42 To delete a scope of command profile

1. Using an account with an assigned security scope of command role, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.
2. Click on the Scope of Command tab.
3. Choose Profile (Security) from the object drop-down menu and click on the Search button. A list of scope of command profiles is displayed.
4. Select a profile in the list and click on the Delete button. A dialog box appears.

Note — You cannot delete a scope of command profile that is assigned to a user group that contains users.

5. Click on the Yes button. The 5620 SAM deletes the scope of command profile.
6. Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 2-43 To export all workspaces and tab preferences

Perform this procedure to export all workspaces and tab preferences from an existing 5620 SAM server to a specified directory.

1. Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.
2. Click on the Settings button and choose Export All from the drop-down menu. The Export Directory window opens.
3. Specify the export directory in the Save In drop-down menu, or create a directory or folder, and click on the Save button. All the workspaces and tab preferences are exported to the specified directory. If the directory exists, a dialog box appears.
4. Click on the Yes button to overwrite all the workspaces and tab preferences saved in the existing directory.
5. Close the 5620 SAM User Security - Security Management (Edit) form.

Procedure 2-44 To import workspaces and tab preferences

Perform this procedure to import workspaces and tab preferences, only workspaces, or only tab preferences, from a directory.

1 Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens with the General tab displayed.

2 Click on the Settings button and choose Import from the drop-down menu. The Import Directory window opens.

3 Click on the drop-down menu and choose one of the following:

- **a** Import All (default)—to import all the workspaces and tab preferences

  If this option is chosen, click on the Overwrite Existing Workspace(s) check box to allow overwriting of existing workspaces.

- **b** Import Workspaces Only—to import only workspaces from the specified directory

  If this option is chosen, click on the Overwrite Existing Workspace(s) check box to allow overwriting of existing workspaces.

- **c** Import Tabs Only—to import only tab preferences from the specified directory

4 Click on the Open button. A confirmation dialog box displays the number of workspaces and tab preferences that will be imported from the specified directory.

5 Click on the Yes button.

All users who have their tab preferences changed and currently have a client session opened, other than the client session where the import has been initiated, will receive a system-generated text message informing them that their tab preferences have been changed and they should restart their 5620 SAM client or risk losing the changes.

The user can click on the reply button to reply to the message.

All users who have their current workspace changed and currently have a client session opened, the workspace selector displays Workspace Out of Sync. Select the current workspace from the workspace selector drop-down menu to apply the modified settings.

6 Close the 5620 SAM User Security - Security Management (Edit) form.

3 — NE user and device security

3.1 NE user and device security overview

The 5620 SAM provides security support for accessing managed devices, including the following:

- create and manage users, profiles and passwords for access to NEs
- configure RADIUS, TACACS+ or LDAP authentication to control access to the managed devices using 5620 SAM user accounts
- configure device system security through CPM traffic filtering and management
- configure DoS protection to protect NEs from high incoming packet rates that characterize DoS attacks

User and group permissions on managed devices

The following general rules apply to managed device users and groups:

- The authentication settings on the device override any configured and distributed authentication settings on the 5620 SAM. For example, if you configure a user account with SHA authentication, and distribute the account to a device configured to use MD5 authentication, authentication is changed to MD5 for that account.
- The management access and CPM filters applied to the managed device must be manually distributed.
- The system administrator can limit the type of access per managed device, for example, allowing FTP access, but denying console, Telnet, and SNMP access.
- User profiles exist independently of users, and are not in effect until they are linked to a user.
- Create device user accounts as a backup to RADIUS, TACACS+, or LDAP authentication. If the RADIUS, TACACS+, or LDAP server fails, or there are user issues on the servers, the user account can be used to access the managed device.

Caution — The 5620 SAM cannot obtain a secret value from an NE during resynchronization. Alcatel-Lucent recommends that you use only the 5620 SAM to configure a shared authentication secret. Do not configure a shared authentication secret directly on a managed NE using another interface, for example, a CLI, or the 5620 SAM cannot synchronize the security policy with the NE.

RADIUS, TACACS+, or LDAP policies and permissions

RADIUS is an access server AAA protocol. The protocol provides a standardized method of exchanging information between a RADIUS client, which is located on the 7750 SR or 7950 XRS and managed by the 5620 SAM, and a RADIUS server, which is located externally from the 7750 SR or 7950 XRS and the 5620 SAM.

RADIUS functionality provides an extra layer of login security. The RADIUS client relays user account information to the RADIUS server. The server authenticates the user and returns user privilege information to the RADIUS client. This determines the level of access that the user has to the device. For example, the user may not be able to FTP information to or from the device.

TACACS+ and LDAP provides functionality that is similar to RADIUS.

Note — The 5620 SAM server checks for reachability to the TACACS+ server using UDP port 49 to prevent long timeout issues. However, all subsequent communication is over TCP port 49.

See the appropriate RADIUS, TACACS+, or LDAP documentation for information about installing, configuring, maintaining lists of users, and managing these authentication servers.

For TACACS+ users, you can specify the following in a user template that is read by the global TACACS+ policy:

- The type of permitted NE access, for example, console, FTP, or both
- A home directory
- A login script that runs when the user logs in

You can enable or disable the user template as required to suit your current global policy requirements.

User and user accounts when combined local and remote authentication is used

Many organizations already have existing TACACS+ or RADIUS authentication of users, based on long standing TACACS+ and RADIUS user accounts and passwords. You can incorporate new 5620 SAM client GUI user accounts for local authentication on the 5620 SAM server with existing TACACS+ or RADIUS system and users.

Consider the following:

- system administrators can use existing TACACS+, RADIUS, or LDAP user accounts
- you can create 5620 SAM client user accounts that match the exact TACACS+, RADIUS, or LDAP user account, for example, if the RADIUS user account is jane, you can create a 5620 SAM user jane
- the 5620 SAM user name can be 1 to 80 characters, flexible enough to match most remote authentication user accounts
- 5620 SAM users already authenticated remotely can log in to 5620 SAM using their RADIUS, TACACS+, or LDAP passwords
- for 5620 SAM users to be authenticated locally, their account passwords must meet 5620 SAM password requirements, described in this section

For example, for user Jane:

- RADIUS user name is jane and password is accessforjane
- 5620 SAM user name is jane and password is LetJane1In!

When Jane is authenticated by RADIUS, she can log in to the 5620 SAM client by typing in jane and accessforjane. If the RADIUS server was down, and she could not be authenticated remotely, to be authenticated locally Jane must log in to the 5620 SAM client by typing jane and LetJane1In!

CPM filters and traffic management

Device CPMs provide dedicated traffic management and queuing hardware for protecting the control plane. You can use CPM filters to specify which types of traffic to accept or deny, and to allocate and rate-limit the shaping queues for traffic directed to the CPMs.

Note 1 — The 7705 SAR does not support IPv6 CPM IP filters, queue filters, or MAC CPM IP filters.

Note 2 — There is no partial distribution of CPM IP filter policies to the 7705 SAR. When you distribute a CPM IP Filter policy to a specific 7705 SAR, every entry, property, and value within that policy must be supported by that 7705 SAR, or distribution of that policy is blocked to that 7705 SAR.

The 5620 SAM supports the following CPM traffic management functionality:

- traffic classification using CPM filters
    - Packets going to the CPM are first classified by the IOM into forwarding classes before recognition by the CPM hardware. You can use CPM filters to further classify the packets using L3/L4 information, for example, destination IP, DSCP value, and TCP SYN/ACK.
- queue allocation
    - Queues 1 — 8 are the default queues. They cannot be modified or deleted. Unclassified traffic is directed to the default queues.
    - Queues 9 — 32 are reserved for future use.
    - Queues 33 — 2000 are available for allocation.
    - Queues 2001 — 8000 are used for per-peer queuing.
- queue configuration
    - PIR
    - CIR
    - CBS
    - MBS

DoS protection

The 5620 SAM supports the use of DoS protection on network and access interfaces. To protect NEs from the high incoming packet rates that characterize DoS attacks, you can use the 5620 SAM to configure DoS protection for the following scenarios:

- the arrival of unprovisioned link-layer protocol packets that are received from CE devices in the core network
- the arrival of excessive subscriber control-plane packets on L2 or L3 access interfaces in aggregation networks
- the arrival of excessive Ethernet CFM frames on L2 and L3 access interfaces, SAPs, and SDP bindings, based on a combination of CFM OpCode and MEG-level values

DoS protection limits the number of packets that are received each second, and optionally logs a violation notification if a policy limit is exceeded. You can use the NE System Security form to view the violations for a specific NE.

DoS protection in the core network

DoS protection in the core network limits the number of link-layer protocol packets that each network interface on an NE accepts for protocols that are not enabled on the interface. The interface drops the excessive packets before they are queued or processed by the CPU.

You can configure global DoS protection on an NE using the NE System Security form. DoS protection controls the following for unprovisioned link-layer protocols:

- the packet arrival rate per source on each network interface
- the overall packet arrival rate per source on the NE
- whether an NE sends a notification trap if a policy limit is exceeded

An NE that supports DoS protection automatically applies default DoS protection parameters to each network and access interface. These defaults limit only the overall packet arrival rate and apply to all of the interfaces on the NE.

DoS protection policies in aggregation networks

In a subscriber aggregation network, an NE typically receives few control-plane packets from a specific subscriber. If one or more subscribers generate excessive control-plane traffic, DoS protection policies can help to ensure that NEs do not become overburdened by these unwanted packets.

You can configure DoS protection policies to control the following on network interfaces, VPLS L2 access interfaces, and IES and VPRN L3 access interfaces:

- the control-plane packet arrival rate per subscriber host
- the overall control-plane packet arrival rate for the interface
- whether an NE sends a notification trap if a policy limit is exceeded

An NE that supports DoS protection automatically assigns a default DoS protection policy to each network and access interface. This default policy limits only the overall packet arrival rate for the interface, and cannot be deleted or modified.

See Procedure 3-3 for information about creating or modifying a DoS protection policy and assigning the policy to one or more NEs. See the appropriate service chapter for information about applying DoS protection policies to interfaces.

DDoS protection

DDoS protection extends DoS protection functionality by controlling traffic destined for IOM or CPM CPUs on a per SAP, per protocol basis. A DDoS protection policy isolates protocols from each other and, at the same time, isolates subscribers so that attacks or misconfigurations only affect the source SAP or protocol.

Policers are used to enforce a traffic rate limiting function. Rate limiting is configurable in packets per second or kb/s. Configurable burst tolerance allows a few extra full handshake attempts, as required by some protocols.

When a policer determines that a packet is non-conformant, it either discards the packet, or marks it as low priority. Traffic marked as low priority is more likely to be discarded at a downstream queueing point if there is congestion for the protocol. Traffic marking is also useful for routing protocols, where an operator may need to offer all packets to the CPU, and only discard packets if the CPU cannot keep up. A policer can be mapped to one or more specific traffic protocols.

The following types of policer can be configured on a DDoS protection policy:

- Static policers instantiate enforcement policers on a SAP permanenly.
- Local monitoring policers instantiate enforcement policers on a SAP dynamically.

A DDoS protection policy can be applied to a capture SAP or to an MSAP (or a SAP that is dedicated to a single subscriber). A DDoS protection policy that is assigned to a capture SAP typically has higher traffic rate limiting values than a policy that is assigned to an MSAP.

A DDoS protection policy can be configured on the following objects in the 5620 SAM:

- base router network interface (except system and loopback interfaces)
- VPRN network interface (except loopback interfaces)
- VPRN L3 access interface
- VPRN group interface SAP
- IES L3 access interface
- IES group interface SAP
- VPLS L2 access interface
- I-VPLS I-L2 access interface
- MVPLS L2 access interface
- I-MVPLS I-L2 access interface
- VLL E-Pipe L2 access interface
- VLL I-Pipe L2 access interface

DDoS alarm handling

The alarm messages generated by DDoS protection policies are presented in a unique manner. Instead of a new alarm message being generated in the Alarm Window every time a DDoS alarm event occurs for a given object (for example, a SAP or access interface), a single alarm message is generated and updated periodically as new DDoS alarm events are generated by the object. If an Alarm Information window is opened for an alarm message, the Additional Text field displays the updated alarm information.

The operator can view dynamically updated alarm information, and avoid the generation of excessive numbers of individual DDoS alarm messages. The alarm sequence for static policers is depicted in Figure 3-1. The alarm sequence for local monitoring policers is depicted in Figure 3-2. The alarm sequence for dynamic policers is depicted in Figure 3-3. In all of these sequences, the alarm is cleared when it returns to a Conform state.

Figure 3-1 Static policer alarm message sequence

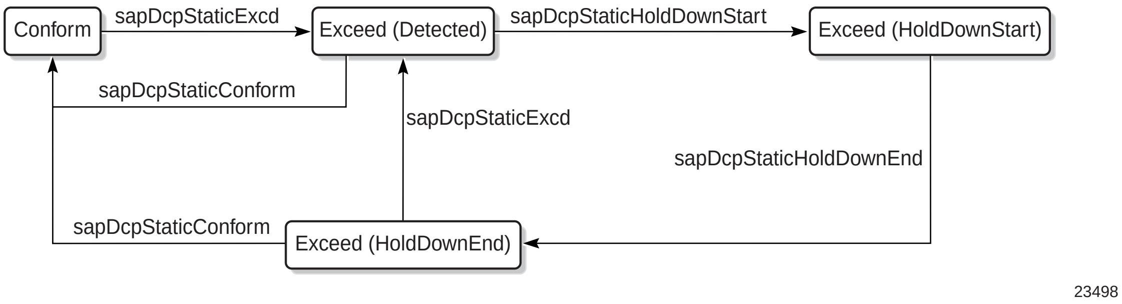


Figure 3-2 Local monitoring policer alarm message sequence

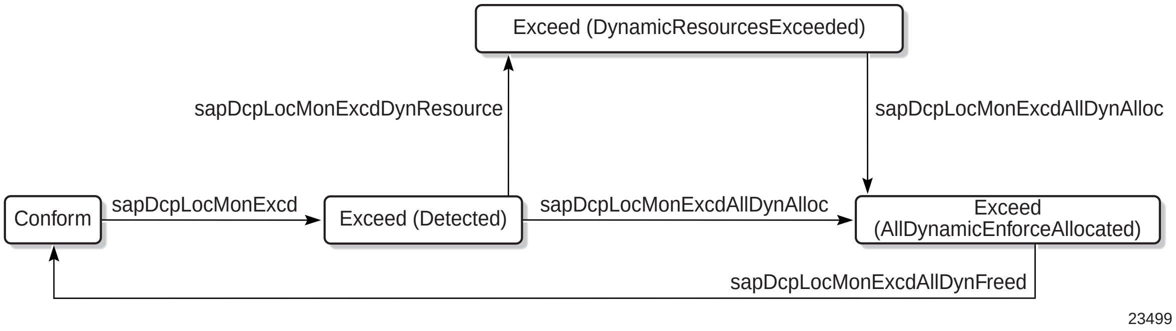
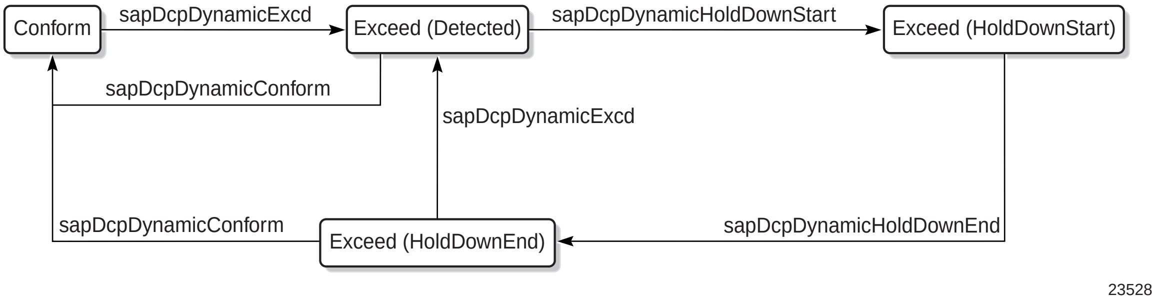

Exceed (DynamicResourcesExceeded)
sapDcpLocMonExcdDynResource
sapDcpLocMonExcdAllDynAlloc
Conform
sapDcpLocMonExcd
Exceed (Detected)
sapDcpLocMonExcdAllDynAlloc
Exceed (AllDynamicEnforceAllocated)
sapDcpLocMonExcdAllDynFreed
23499

Figure 3-3 Dynamic policer alarm message sequence



IP security

The 5620 SAM supports the IPsec MDA which provides IP security support including tunneling and encryption functions. See the 7750 SR security documentation for more information about configuring IP security.

Configuring a firewall on a 7705 SAR-H using the firewall manager

The 5620 SAM supports the firewall functionality on the 7705 SAR-H through a firewall manager. You can configure firewall functionality for every 7705 SAR-H node. Using the firewall manager, you can navigate to firewall policies, display statuses and states (faults), and configure firewalls as local configurations or distribute them to multiple nodes. The 5620 SAM supports configurations for every NE instance or as a policy. See Procedure 3-16 for more information.

Note — Procedure 3-16 is only applicable to the 7705 SAR-H, Release 5.0.

Configuring a firewall on a 7705 SAR-H management access or CPM interface

The 5620 SAM supports two interfaces to manage the 7705 SAR-H CTL traffic, for example, OSPF, BGP, RSVP-TE, LDP protocol, and SNMP configuration traffic, through the firewall. These management interfaces allow zone definition entries to be applied to the firewall. The two interfaces are:

- the NE management access firewall interface, which is the physical management Ethernet port on the main chassis. See Procedure 3-17.

  For the NE management access firewall interface via the management port, there is always only one set of zone rules applied to CTL traffic arriving on the interface. The management zone rules are applied if configured on ingress to the firewall. If the CTL packets pass, they are sent to the CPM without any further egress rules applied.
- the NE CPM firewall interface, which is the in-band management interface. See Procedure 3-18.

  For the NE CPM firewall management interface, CTL traffic that is intended for the CPM would have ingress and egress zone rules applied to the traffic. When CTL traffic ingresses the 7705 SAR-H on source interfaces (for example, SAP, spoke–SDP, or router interfaces) zone rules configured on those interfaces are applied on ingress to the firewall. If management zone rules are configured on the NE CPM firewall, those rules are applied to the packet on egress from the firewall before being processed by the CPM.

Note — Procedures 3-17 and 3-18 are only applicable to the 7705 SAR-H, Release 5.0.

3.2 Workflow to manage NE user and device security

This workflow describes the high-level steps to manage NE user and device security.

1. Specify the type of authentication keys used on the device; for example, SHA or MD5 as part of the device discovery. See “To commission a device for 5620 SAM management” in the *5620 SAM User Guide* for more information.
2. As required, manage user profiles and user accounts. See chapter 2 for more information:
    - modify profiles and users
    - delete profiles and users
    - change passwords as specified in the password policy
3. Create site management access filter policies for each device from the 5620 SAM; see Procedure 3-1.
4. Create filter policies for device CPM modules; see Procedure 3-2.
5. Create NE DoS protection policies, as required to control the amount of subscriber-based control-plane traffic that the NE interfaces receive; see Procedure 3-3.
6. Create NE DDoS protection policies, as required to isolate protocols from each other and, at the same time, isolate subscribers so that attacks or misconfigurations only affect the source SAP or protocol; see Procedure 3-4.
7. View NE DoS protection violations, as required; see Procedure 3-5.
8. Create site user profiles based on job classifications and the access needed to the managed devices; see Procedure 3-6.
9. Create individual site user accounts based on the configured profiles; see Procedure 3-7.
10. Specify password policies for access to managed devices and users; see Procedure 3-8.
11. Create RADIUS, TACACS+, or LDAP access or security policies for user authentication on the managed device; see Procedures 3-9, 3-10, or 3-11.
12. View or configure the system security settings on managed NEs; see Procedure 3-12.

13 As required, configure X.509 authentication or a PKI certificate authority profile on 7750 SR NE; see Procedure 3-13 or 3-14.

14 Configure an NE firewall on the 7705 SAR-H using the firewall manager; see Procedure 3-16.

15 Configure an NE management access firewall on the 7705 SAR-H using the firewall manager; see Procedure 3-17.

16 Configure an NE CPM firewall on the 7705 SAR-H using the firewall manager; see Procedure 3-18.

17 Perform the following NE system security tasks, as required:

- **a** Create subscriber authentication policies for DHCP sessions; see Procedure 3-19.
- **b** Modify the security policies; see Procedure 3-20.
- **c** Release and distribute security policies to the managed devices; see Procedure 3-21.
- **d** Delete security policies; see Procedure 3-22.
- **e** Unlock user accounts that are locked due to failed login attempts; see Procedure 3-23.
- **f** Clear the password history for a user on a managed object; see Procedure 3-25.
- **g** Perform CPMv2 certificate administration actions; see Procedure 3-15.
- **h** Clear collected statistics information on a CPM filter; see Procedure 3-24.

3.3 NE user and device security procedures

This section provides procedures to create and manage security on the managed devices.

Procedure 3-1 To create or modify a site management access filter policy for a managed device

A site management access filter performs the following functions:

- Restricts the type of management access allowed
- Specifies a strict underlying connection protocol usage and the accepted IP addresses and ports that can access to device

Note — You need an account with an assigned administrator scope of command role to the sitesec package, or scope of command role with write access permissions to the sitesec package, to perform this procedure

1 Choose Administration→Security→NE Management Access Filters from the 5620 SAM main menu. The NE Management Access Filter form opens.

2 Perform one of the following:

a Specify a filter to search for and modify an existing site management access filter. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The Site Management Access Filter (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description

4 Configure the following parameters on the IPv4, IPv6, and MAC panels, as required:

- Default Filter Action
- Administrative State

5 Click on the IPv4 Entries tab.

6 Perform one of the following.

a Click on the Create button to add a new site entry. The Site MAF Match Entry (Create) form opens.

b Choose an entry in the list and click on the Properties button to modify an existing entry. The Site MAF Match Entry (Edit) form opens.

7 Configure the parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Description
- Action
- Source IP
- Source IP Mask
- Source Port Type
- Source Port ID
- Destination Port
- Destination Port Mask
- Protocol
- Log
- Router

When you set the Action parameter to deny, you cannot distribute the policy to the managed device. Before setting the parameter to deny, set the parameter to permit, distribute the configuration to the managed devices, then reconfigure the parameter to deny.

8 Click on the OK button. The Site MAF Match Entry (Create) or Site MAF Match Entry (Edit) form closes.

9 Click on the IPv6 Entries tab.

10 Perform one of the following.

a Click on the Create button to add a new site entry. The Site IPv6 MAF Match Entry (Create) form opens.

b Choose an entry in the list and click on the Properties button to modify an existing entry. The Site IPv6 MAF Match Entry (Edit) form opens.

11 Configure the parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Description
- Action
- Source IP
- Source IP Mask
- Source Port Type
- Source Port ID
- Destination Port
- Destination Port Mask
- Next Header
- Log
- Flow Label
- Router

When you set the Action parameter to deny, you cannot distribute the policy to the managed device. Before setting the parameter to deny, set the parameter to permit, distribute the configuration to the managed devices, then reconfigure the parameter to deny.

12 Click on the OK button. The Site IPv6 MAF Match Entry (Create) or Site IPv6 MAF Match Entry (Edit) form closes.

13 Click on the MAC Entries tab.

14 Click on the Create button. The Site MAC MAF Match Entry (Create) form opens with the General tab displayed.

15 Configure the parameters:

- Entry ID
- Auto-Assign ID
- Displayed Name
- Description

16 Click on the Filter Properties tab.

17 Configure the parameters:

- Action
- Frame Type
- Source MAC
- Destination MAC
- Src Mask
- Dst Mask
- Dot1p
- Dot1p Mask
- CFM Opcode
- CFM Val 1
- CFM Val 2
- Service Id

18 Perform one of the following.

a If you set the Frame Type parameter to e802dot2LLC in step 17, configure the following parameters. Otherwise, go to step 19.

- DSAP
- DSAP Mask
- SSAP
- SSAP Mask

b If you set the Frame Type parameter to e802dot2SNAP in step 17, configure the following parameters. Otherwise, go to step 19.

- SNAP OUI
- SNAP PID

c If you set the Frame Type parameter to Ethernet II in step 17, configure the Ether Type parameter. Otherwise, go to step 19.

19 Click on the OK button to save the configuration and close the CFM MAC Filter Entry (Create) or CFM MAC Filter Entry (Edit) form.

20 Click on the OK button. A confirmation window appears.

21 Confirm the action.

22 Repeat for each site management access filter you need to create or modify.

Note 1 — If the policy is in draft mode, the Distribute button, or the Distribute option located under the More Actions button, is disabled and the policy cannot be distributed. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can choose which NEs to distribute the policy to.See Procedure 3-21 for more information about how to release a policy.

Note 2 — If the Source IP Address and other filter criteria are improperly set, you receive the following error message when you attempt to distribute the policy:

- Policy distribution failed due to the following incompatible node(s):,[x.x.x.x]
- Cannot set the Action to deny if the Source IP Address is 0.0.0.0 and no other filter criteria is set. The network element will become unreachable.

This indicates that the request is unprocessed.

While the NE allows you to perform this action using a CLI, the 5620 SAM does not. It is blocked because after the NE becomes unreachable, there is no way that 5620 SAM can re-establish the connection. You must then use a CLI on the NE to solve the issue and re-establish the connection.

You must distribute policies to specific devices, as described in Procedure 3-21.

Procedure 3-2 To create or modify a CPM filter policy for a managed device

A device CPM module provides traffic management and queuing hardware for protecting the control plane. The device provides dedicated 10 Gb/s hardware protection for the control planes. You can create CPM filters for the following traffic management functions:

- Drop traffic
- Accept traffic
- Allocate dedicated hardware shaping queues for traffic directed to the control processors

Note 1 — You need an account with an assigned administrator scope of command role to the sitesec package, or scope of command role with write access permissions to the sitesec package, to perform this procedure

Note 2 — The 7705 SAR does not support IPv6 CPM filters, Queue filters, or MAC CPM filters.

1 Choose Administration→Security→NE CPM Filter from the 5620 SAM main menu. The NE CPM Filter form opens.

2 Perform one of the following:.

a Specify a filter to search for and modify an existing site management access filter. Use the filters to search for and open an existing policy by choosing a policy in the filtered list and clicking on the Properties button.

b Click on the Create button. The CPM Filter (Create) form opens.

3 Click on the General tab.

4 Configure the parameters as required.

- Displayed Name
- Description
- Default Filter Action
- IP Administrative Status
- IPv6 Administrative Status
- MAC Administrative Status

Note — The 7705 SAR does not support IPv6 and MAC CPM filters.

5 Click on the IPv4 Entries tab.

6 Perform one of the following:

a Click on the Create button to add a new filter entry.

b Click on an entry in the list and click on the Properties button to modify an existing entry.

The CPM IP Filter Entry (Create) form opens with the General tab displayed.

7. Configure the parameters:

   - Entry ID
   - Auto-Assign ID
   - Displayed Name
   - Description

8. Click on the Filter Properties tab.

9. Configure the parameters:

   Note — The configurable parameters that are displayed depends on the choice you make for the Protocol parameter.

   - Action
   - Protocol
   - Queue ID
   - DSCP
   - Source IP
   - Source Mask
   - Source IP Prefix
   - Destination IP
   - Destination Mask
   - Destination IP Prefix
   - Routing Instance
   - Fragment
   - IP Option
   - IP Option Mask
   - Option Present
   - Multiple Option
   - ICMP Code
   - ICMP Type
   - Configuration Type
   - Source Port Operator
   - Source Port List
   - Destination Port Operator
   - Destination Port List
   - Port Operator
   - Port List
   - TCP Syn
   - TCP Ack

   The Queue ID parameter is configurable when the Action parameter is set to queue.

   The Source Port, Destination Port, and Port related parameters are configurable when the Protocol parameter value is TCP or UDP.

   If you select the Source and Destination option for the Configuration Type parameter, you can configure the Source and Destination ports separately, specifying either a Mask, Range, or Port List for each. If you select the Port option for the Configuration Type, then the Mask, Range, or Port List you specify will apply to both the source and destination.

10. Click on the OK button. The new CPM IP filter entry appears in the list.

11. Click on the IPv6 Entries tab.

12 Perform one of the following:

a Click on the Create button to add a new filter entry.

b Choose an entry in the list and click on the Properties button to modify an existing entry.

The CPM IPv6 Filter Entry (Create) form opens with the General tab displayed.

13 Configure the parameters:

- Entry ID
- Auto-Assign ID
- Displayed Name
- Description

14 Click on the Filter Properties tab.

15 Configure the parameters:

Note — The configurable parameters that are displayed depends on the choice you make for the Next Header parameter.

- Action
- Next Header
- Queue ID
- DSCP
- Source IP
- Source Mask
- Source IP Prefix
- Destination IP
- Destination Mask
- Destination IP Prefix
- Routing Instance
- Flow Label
- Hop-By-Hop Options
- Configuration Type
- Source Port Operator
- Source Port List
- Destination Port Operator
- Destination Port List
- Port Operator
- Port List
- TCP Syn
- TCP Ack

The Queue ID parameter is configurable when the Action parameter is set to queue.

The Source Port, Destination Port, and Port related parameters are configurable when the Protocol parameter value is TCP or UDP.

If you select the Source and Destination option for the Configuration Type parameter, you can configure the Source and Destination ports separately, specifying either a Mask, Range, or Port List for each. If you select the Port option for the Configuration Type, then the Mask, Range, or Port List you specify will apply to both the source and destination.

16 Click on the OK button. The new CPM IPv6 filter entry appears in the list.

17 Click on the MAC Entries tab.

18 Perform one of the following:

a Click on the Create button to add a new MAC entry. The CPM MAC Filter Entry (Create) form opens with the General tab displayed.

b Choose an entry from the list and click on the Properties button to modify an existing CPM MAC entry. The CPM MAC Filter Entry (Edit) form opens with the General tab displayed.

19 Configure the parameters:

- Entry ID
- Auto-Assign ID
- Displayed Name
- Description

20 Click on the Filter Properties tab.

21 Configure the parameters:

- Action
- Frame Type
- Source MAC
- Destination MAC
- Src Mask
- Dst Mask
- Dot1p
- Dot1p Mask
- CFM Opcode
- CFM Val 1
- CFM Val 2
- Service Id

22 Perform one of the following.

a If you set the Frame Type parameter to e802dot2LLC in step 21, configure the following parameters. Otherwise, go to step 24.

- DSAP
- DSAP Mask
- SSAP
- SSAP Mask

b If you set the Frame Type parameter to Ethernet II in step 21, configure the Ether Type parameter. Otherwise, go to step 24.

23 Click on the OK button to save the configuration and close the CFM MAC Filter Entry (Create) or CFM MAC Filter Entry (Edit) form.

24 Click on the Queues tab.

25 Perform one of the following:

a Click on the Create button to add a new CPM filter queue. The CPM Filter Queue (Create) form opens with the General tab displayed.

b Click on an entry in the list and click on the Properties button to modify an existing CPM filter queue.

26 Configure the parameters:

- ID
- Displayed Name
- Description

27 Click on the CIR/PIR tab.

28 Configure the parameters:

- CIR (kb/s)
- PIR (kb/s)
- MAX

Ensure that the CIR value is lower than the PIR value.

29 Click on the Burst Size tab.

30 Configure the parameters:

- Committed Burst Size (KB)
- Maximum Burst Size (KB)

The parameters are configurable when the Default check box above each is deselected.

Ensure that the Committed Burst Size (KB) parameter value is lower than the Maximum Burst Size (KB) parameter value.

31 Click on the OK button. A dialog box appears.

32 Click on the OK button. The CPM IP Filter (Create) form reappears.

33 Repeat for each CPM filter that you need to create or modify.

34 Click on the Apply button to save the changes.

You must distribute policies to specific devices, as described in Procedure 3-21.

Procedure 3-3 To configure an NE DoS protection policy

Perform this procedure to control the amount of subscriber-based control-plane traffic that NE interfaces receive.

Note — You need an account with an assigned administrator scope of command role to the sitesec package, or scope of command role with write access permissions to the sitesec package, to perform this procedure

1 Choose Administration→Security→NE DoS Protection from the 5620 SAM main menu. The NE DoS Protection form opens.

2 Perform one of the following.

a Create a policy.

i Click on the Create button. The NE DoS Protection (Create) form opens.

ii Configure the following parameters:

- Auto-Assign ID
- Policy ID

iii Click on the Apply button. The form displays additional buttons and the form name changes to NE DoS Protection (Edit).

b Modify an existing policy.

i Configure the filter criteria. A list of DoS protection policies is displayed.

ii Choose a policy in the list and click on the Properties button. The NE DoS Protection (Edit) form opens.

3 Configure the following parameters:

- Description
- Packet Rate Limit (pps)
- Overall Rate Limit (pps)
- Out Profile Rate (pps)
- Out Profile Rate Log Event
- Receive Notification
- Rate Limit DHCP Packets

4 Perform the following steps to configure CFM frame-rate limiting, if required.

i Click on the CFM Rate Limiting tab.

ii Click on the Create button. The CfmRateLimiting (Create) form opens.

iii Configure the parameters:

- Policy ID
- Description
- Packet Rate Limit (pps)
- Level Set

iv Click on the Add button in the Op Code Set panel. The Select Property form opens.

Note — You must specify at least one OpCode value.

v Choose one or more OpCodes in the list and click on the OK button. The OpCode entries are listed on the CfmRateLimiting (Create) form.

vi Click on the OK button. A dialog box appears.

vii Click on the OK button. The CfmRateLimiting (Create) form closes.

5 Distribute the policy to NEs, as required, as described in Procedure 3-21.

6 Click on the OK button. A dialog box appears.

7 Click on the Yes button. The NE DoS Protection (Edit) form closes.

Procedure 3-4 To configure an NE DDoS protection policy

1 Choose Administration→Security→NE DDoS Protection from the 5620 SAM main menu. The NE DDoS Protection form opens.

2 Perform one of the following:

a Create a DDoS protection policy.

i Click on the Create button and choose DDoS Protection Policy from the drop-down menu. The DDoS Protection Policy form opens.

ii Go to step 3.

b Modify a DDoS protection policy.

i Choose DDoS Protection Policy from the object drop-down menu.

ii Configure the filter criteria and click on the Search button. A list of DDoS protection policies appears.

iii Choose a DDoS protection policy and click on the Properties button. The DDoS Protection Policy (Edit) form opens.

3 Configure the parameters:

- Displayed Name
- Description

Note — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

4 Click on the Apply button. The DDoS Protection Policy form refreshes with additional tabs.

5 Configure static policers, if required.

i Click on the Static Policers tab.

ii Click on the Create button to create a static policer or choose a static policer in the list, and click Properties. The Static Policer form appears.

iii Configure the parameters:

- Displayed Name
- Description
- Log Events State
- Detection Time
- Rate Type

iv If the Rate Type parameter is set to Kbps, configure the Rate Limit (Kb/s) and Buffer Space (Bytes) parameters in the Kbps panel. You can specify a default value for these parameters by selecting the Default check box.

v If the Rate Type parameter is set to Packets, configure the Rate Limit (packets), Time Limit (seconds), and Initial Delay (packets) parameters in the Packets panel. You can specify a default value for the Rate Limit (packets) parameter by selecting the Default check box.

vi Configure the Exceed Action parameter. If you set this parameter to Discard or Low Priority, configure the Hold Down Duration (seconds) parameter.

vii Click on the OK button. The Static Policer form closes.

6 Configure local monitoring policers, if required.

i Click on the Local Monitoring Policer tab.

ii Click on the Create button to create a local monitoring policer, or choose a local monitoring policer in the list and click Properties. The Local Monitoring Policer form appears.

iii Configure the parameters:

- Displayed Name
- Description
- Log Events State
- Rate Type

iv If the Rate Type parameter is set to Kbps, configure the Rate Limit (Kb/s) and Buffer Space (Bytes) parameters in the Kbps panel. You can specify a default value for these parameters by selecting the Default check box.

v If the Rate Type parameter is set to Packets, configure the Rate Limit (packets), Time Limit (seconds), and Initial Delay (packets) parameters in the Packets panel. You can specify a default value for the Rate Limit (packets) parameter by selecting the Default check box.

vi Configure the Exceed Action parameter.

vii Click on the OK button. The Local Monitoring Policer form closes.

7 Configure protocol mappings for static policers and local monitoring policers, if required.

i Click on the Protocols tab.

ii Click on the Create button to create a protocol, or choose a protocol in the list and click Properties. The Protocols form appears.

iii Configure the parameters:

- Protocol
- Type
- Local Monitoring Bypass

iv Click on the Select button in the Enforcement panel and choose a policer from the Select Policer form.

Note — If the Type parameter is set to Static, you must choose a static policer. If the Type parameter is set to Dynamic, you must choose a local monitoring policer. However, if the Type parameter is set to Dynamic and the Local Monitoring Bypass parameter is enabled, you cannot specify a local monitoring policer.

v In the Dynamic Parameters panel, configure the parameters:

- Log Events State
- Detection Time
- Rate Type

vi If the Rate Type parameter is set to Kbps, configure the Rate Limit (Kb/s) and Buffer Space (Bytes) parameters in the Kbps panel. You can specify a default value for these parameters by selecting the Default check box.

vii If the Rate Type parameter is set to Packets, configure the Rate Limit (packets), Interval (seconds), and Initial Delay (packets) parameters in the Packets panel. You can specify a default value for the Rate Limit (packets) parameter by selecting the Default check box.

viii Configure the Exceed Action parameter. If you set this parameter to Discard or Low Priority, configure the Hold Down Duration (seconds) parameter.

ix Click on the OK button. The Protocols form closes.

8 Click on the OK button. The DDoS Protection Policy form closes.

9 Close the Residential Subscriber Policies form.

Procedure 3-5 To view NE DoS protection violations

1 Choose Administration→Security→NE System Security from the 5620 SAM main menu. The Select Site form opens.

2 Choose a managed device in the list and click on the OK button. The NE System Security (Edit) form opens with the General tab displayed.

3 Click on the NE DoS Protection tab.

4 Perform one of the following to view a specific violation type.

  a Click on the Per MAC Source Violations tab to view a list of the violations associated with subscriber hosts according to MAC address.

  b Click on the Per IP Source Violations tab to view a list of the violations associated with subscriber hosts according to IP address.

  c Click on the Link Specific Port Violations tab to view a list of the violations at the port level. The following kinds of violations are listed:

  - violations that exceed the Link Rate Limit (pps) parameter value specified for the NE
  - violations that exceed the Port Overall Rate Limit (pps) parameter value specified for the NE.

  d Click on the Network Interface Violations tab to view a list of the violations for network interfaces that exceed the Overall Rate Limit (pps) parameter value specified in an associated NE DoS protection policy.

  e Click on the SAP Violations tab to view a list of the violations for SAPs that exceed the Overall Rate Limit (pps) parameter value specified in an associated NE DoS protection policy.

5 Repeat step 4 as required to view another violation type.

6 Close the NE System Security (Edit) form.

Procedure 3-6 To create a user profile for managed device access

A site user profile specifies the commands or command groups that are permitted or denied on the managed device by the 5620 SAM.

Note — You need an account with an assigned administrator scope of command role to the sitesec package, or scope of command role with write access permissions to the sitesec package, to perform this procedure

1 Choose Administration→Security→NE User Profiles from the 5620 SAM main menu. The NE User Profiles form opens.

2 Click on the Create button. The Site User Profile (Create) form opens.

3 From the General tab, Configure the parameters:

- Displayed Name
- Description
- Default Profile Action
- LI Profile

Note — To configure the LI Profile parameter you need LI privileges. For more information about LI, see "Lawful Intercept overview" in the *5620 SAM User Guide*.

4 Click on the Apply button.

5 Click on the Entries tab.

6 Click on:

a The Create button to add a new site entry.

b An entry in the table and click on the Properties button to modify an existing entry.

The Site User Profile Match Entry (Create) form opens when you create a new entry.

7 Configure the parameters:

- ID
- Auto-Assign ID
- Displayed Name
- Description
- Action
- Match String

  Specify the Match String parameter. A match string is a CLI command prefix, which defines the scope of the user profile. For example, when you set the match string to "config" and specify a deny action, this user profile cannot use any CLI commands that begin with the word "config".

8 Click on the Apply button to save the changes. The site user profile match entry appears in the list form.

9 Verify the action.

10 Click on the OK button to close the form.

11 Repeat for each required site user profile.

You must distribute policies to specific devices, as described in Procedure 3-21.

Procedure 3-7 To configure a user account for access to a managed device

Perform this procedure to create a user account on a device for managed device access when the authentication servers are unavailable, or to specify the allowed types of device access, for example, Telnet, SNMPv3, FTP, or console.

Note — You need an account with an assigned administrator scope of command role to the sitesec package, or scope of command role with write access permissions to the sitesec package, to perform this procedure

1 Choose Administration→Security→NE User Configuration from the 5620 SAM main menu. The NE User Configuration form opens.

2 Click on the Create button. The NE User (Create) form opens with the General tab displayed.

3 Configure the parameters:

- User Name
- Additional ID
- Description
- Access
- Password
- Confirm Password
- Home Directory
- Restrict to Home
- Console Login Exec File
- Console Cannot Change Password
- Console New Password At Login

Note — For SNMP v2 managed NEs, you can create and update an SNMP user configuration policy when the Access parameter SNMP option is not selected.

4 When a user has console permission, you can configure the parameters on the Console Profiles tab.

i Click on the Console Profiles tab. The list of profiles numbered one through eight appears.

Each user can have up to eight profiles.

ii Click on the Select button beside Profile 1 and Profile 2 to 8 parameters. Profile 1 is automatically configured to use the system-generated default profile.

The Select Site User Profile form opens. Default profiles and the profiles created in Procedure 3-6 are listed.

iii Choose a profile from the list.

iv Click on the OK button. The profile name appears beside the profile number.

5 When a user has SNMPv3 permissions, you can configure the authentication parameters. Ensure that the SNMPv3 user and user group is created on the managed device. If MD5 or SHA authentication and DES privacy is used, ensure the keys have been created and associated with the managed device and the SNMPv3 user group.

i Click on the SNMP v3 tab.

ii Configure the parameters:

- Authentication Protocol
- Privacy Protocol
- New Authentication Password
- Confirm New Auth Password
- New Privacy Password
- Confirm New Privacy Password

6 To specify an RSA key for use by SFTP on a 7750 MG, perform the following steps.

Note — Only the 7750 MG supports RSA key configuration.

i Click on the RSA Key tab.

ii Click on the Create button. The RSA Key (Create) form opens.

iii Configure the parameters:

- Public Key Number
- Public Key Name

iv Click on the OK button. A dialog box appears.

v Click on the OK button. The RSA Key (Create) form closes.

7 Click on the OK button. A dialog box appears.

8 Click on the Yes button. The NE User (Create) form closes.

9 Close the NE User Configuration form.

Procedure 3-8 To create or modify a password policy

Perform this procedure to create a policy that specifies the rules to which a password must conform on one or more devices.

Note — You need an account with an assigned administrator scope of command role to the sitesec package, or scope of command role with write access permissions to the sitesec package, to perform this procedure

1 Choose Administration→Security→NE Password Policy from the 5620 SAM main menu. The NE Password Policy form opens.

2 Click on the Create button. The Site Password Policy (Create) form opens.

3 Configure the parameters:

- ID
- Auto-Assign ID
- Name
- Description
- Complexity
- Lockout Time (minutes)
- Password Never Expires
- Maximum Attempts
- Maximum Attempts Time (minutes)
- Days Before Expiration
- Minimum Length
- Health Check
- Health Check Interval
- Password History
- Authentication Order 1
- Authentication Order 2
- Authentication Order 3
- Exit On Reject
- Admin Password
- Dynamic Service Password
- Tacplus Map to Privilege Level

If the password can expire, specify the expiration parameter to indicate the number of days that the password can be active before the old password expires and a new password must be set.

Use the Maximum Attempts and Maximum Attempts Time (minutes) parameters to specify the number of attempts allowed within a specified time.

If the maximum number of password attempts in the specified time is exceeded, set how long the account is locked out using the Lockout Time (minutes) parameter.

4 Specify the types and order of password authentication to be used to verify the user account password using the Authentication Order 1 through 3 parameters. Set the order from the most preferred method of authentication to the least preferred method of authentication.

5 Configure the password complexity rules using the parameters in the Complexity Rules panel:

- Password Allow User Name
- Maximum Credits LowerCase
- Maximum Credits UpperCase
- Maximum Credits Special Character
- Maximum Credits Numeric
- Maximum Number Of Times Character Can Be Use Consecutively
- Minimum Number Of Distinct Kind of Characters
- Minimum Number Of LowerCase Characters
- Minimum Number Of UpperCase Characters
- Minimum Number Of Special Characters
- Minimum Number Of Numeric

6 Click on the OK button to save the changes.

You must distribute policies to specific devices, as described in Procedure 3-21.

Procedure 3-9 To create an NE RADIUS authentication policy

See the appropriate RADIUS documentation for more information about configuring RADIUS servers.

1 Choose Administration→Security→NE RADIUS Authentication from the 5620 SAM main menu. The NE RADIUS Authentication form opens.

2 Click on the Create button. The Site RADIUS Policy (Create) form opens.

3 Configure the parameters:

- Displayed Name
- Description
- Administrative State
- Enable Accounting
- Enable Authorization
- RADIUS Authorization Algorithm
- Retry Attempts
- Timeout (seconds)
- Authentication Port
- Source Address
- Accounting Port
- Enable User Template

Note — The Source Address parameter on the Site RADIUS Policy (Create) form is configurable but is not used. You must use the Source Address tab of the routing instance properties form for the device to specify the source address of the RADIUS server.

4 Click on the Servers tab to configure a connection to the RADIUS servers. You can configure up to five RADIUS servers.

i Click on the Create button. The Site RADIUS Server (Create) form opens.

ii Configure the parameters:

- ID
- Displayed Name
- Description
- Address
- Secret Name

iii Click on the OK button to save the changes.

5 Click on the Apply button to save the changes.

You must distribute policies to specific devices, as described in Procedure 3-21.

Ensure that the authentication order uses RADIUS first. See Procedure 3-8 for more information.

Procedure 3-10 To create an NE TACACS+ authentication policy

See the appropriate TACACS+ documentation for more information about configuring TACACS+ servers.

1 Choose Administration→Security→NE TACACS+ Authentication from the 5620 SAM main menu. The NE TACACS+ Authentication form opens.

2 Click on the Create button. The Site TACACS+ Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description
- Administrative State
- Enable Accounting
- Accounting Type
- Enable Authorization
- Use Privilege Map
- Use Interactive Authentication
- Timeout (seconds)
- Single Connection
- Source Address
- Enable User Template

The Use Privilege Map parameter only appears for configuration when Enable Authorization is set to true.

Note — The Source Address parameter on the Site TACACS+ Policy (Create) form is configurable but is not used. You must use the Source Address tab of the routing instance properties form for the device to specify the source address of the TACACS+ server.

4 Click on the Privilege Level Map tab.

5 Click on the Create button. The Privilege Level Map (Create) form opens.

6 Configure the Privilege Level parameter.

7 Perform one of the following:

  a Create a new User Profile. See Procedure 3-6.

  b Select an existing User Profile.

    i Click on the Select button to choose a User Profile. The Select User Profile form opens.

    ii Select an entry from the list and click OK. The Select User Profile form closes and the Privilege Level Map (Create) form displays the selected User Profile entry.

8 Click on the Servers tab to configure a connection to the TACACS+ servers. You can configure up to 5 TACACS+ servers.

  i Click on the Create button.

  The Site TACACS+ Server (Create) form opens.

  ii Configure the parameters:

  - ID
  - Displayed Name
  - Description
  - Address
  - Secret Name

  iii Click on the OK button to save the changes.

9 Click on the Apply button to save the changes.

You must distribute policies to specific devices, as described in Procedure 3-21.

Procedure 3-11 To create a RADIUS, TACACS+, or LDAP security policy on an OmniSwitch

1 Choose Administration→Security→NE AOS Security Authentication from the 5620 SAM main menu. The NE AOS Security Authentication form opens.

2 Click on the Create button. The Site AOS Security Policy (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description
- Protocol Name

Note 1 — Do not use a colon in the policy name because the 5620 SAM uses colons as separators for the object full name.

Note 2 — Ensure that the authentication order uses RADIUS first. See Procedure 3-8 for more information.

4 Perform one of the following:

a If you set the Protocol Name parameter to RADIUS, go to step 5.

b If you set the Protocol Name parameter to TACACS+, go to step 7.

c If you set the Protocol Name parameter to LDAP, go to step 9.

5 Configure the parameters:

- IP Address
- IP Address 2
- Time Out
- Retries
- Secret
- Authentication Port
- Account Port

6 Click on the Apply button to save the changes. Go to step 11.

7 Configure the parameters:

- IP Address
- IP Address 2
- Time Out
- Secret
- Port

8 Click on the Apply button to save the changes. Go to step 11.

9 Configure the parameters:

- IP Address
- IP Address 2
- Time Out
- Retries
- Password
- Port
- Domain Name
- Search Base
- Server Type
- SSL

10 Click on the Apply button to save the changes. Go to step 11.

11 Close the Site AOS Security Policy (Create) form.

12 You must distribute the security policies to specific devices, as described in Procedure 3-21.

Procedure 3-12 To view or configure the system security settings on managed NEs

Perform this procedure to view or configure the following system security settings on managed devices:

- view the device site ID and site name
- enabling or disabling FTP, Telnet, Telnet IPv6, or SSH servers
- allocating peer queuing for hardware CPM queues
- accessing and configuring RADIUS and TACACS+ user templates
- configuring global NE DoS protection parameters and viewing any violations
- configuring rate limits for VPRN network exceptions
- viewing the device deployment information
- viewing alarm information

1 Choose Administration→Security→NE System Security from the 5620 SAM main menu. The Select Site form opens.

2 Choose a managed device in the list and click on the OK button. The NE System Security (Edit) form opens with the General tab displayed. The device Site ID IP address and Site Name display.

Note — Items that appear on the device NE System Security (Edit) form are device-dependent. Not all configuration form tabs and parameters in this procedure apply to all devices.

3 Click on the Servers Configuration tab to configure the server parameters.

4 Configure the parameters:

- Servers Enabled
- SSH
- Graceful Shutdown
- Minimum TTL Value

Note — The 7705 SAR may become temporarily unreachable when enabling SSH and starting the SSH server on the device.

5 Click on the CPM Per-Peer-Queuing tab to ensure that the managed device allocates a separate CPM hardware queue for the peer, for example, a BGP or T-LDP peer.

6 Configure the CPM Per-Peer-Queuing parameter.

7 Click on the System User Template tab. The default System User radius_default and tacplus_default templates appear.

8 Choose the appropriate default template and click on the Properties button. The System User Template (Edit) form opens.

9 Configure the parameters:

- Access
- Home Directory
- Restricted to Home Directory
- Console Login Exec File

10 Choose one the following:

a If you intend to use the default Template Profile, go to step 21.

b If you intend to select the administrative Template Profile or create a new Template Profile, go to step 11.

11 Click on the Select button. The Select Template Profile - System User Template form opens. The form that displays is based on the type of the template profile previously selected.

12 Choose one the following:

a If you intend to use the administrative Template Profile, choose the administrative template and click on the OK button. Go to step 21.

b To create a new template profile, click on the Create button. The Site User Profile, Global Policy (Create) form opens with the General tab displayed.

13 Configure the parameters:

- Display Name
- Description
- Default Profile Action

14 Click the Entries tab.

15 Click on the Create button. The Site User Profile Match Entry, Global Policy (Create) form opens.

16 Configure the parameters:

- Displayed Name
- Description
- Action
- Match String

17 Click on the OK button. The Site User Profile Match Entry, Global Policy (Create) form closes.

18 Click on the OK button. The Site User Profile Global Policy (Create) form closes.

19 Click on the OK button. The Select Template Profile - System User Template form closes.

20 Click on the OK button. The System User Template (Edit) form closes.

21 Click on the NE DoS Protection tab to configure global DoS functionality for the NE. The Protection tab is displayed.

22 Configure the parameters:

- Link Rate Limit (pps)
- Port Overall Rate Limit (pps)
- Protection Administrative State
- Allow Sham Links
- Block PIM Tunneled
- Action low Priority
- IP Src Monitor DHCP

PIM in an MVPN on the egress DR does not switch traffic from the (*,G) to the (S,G) tree if protocol protection is enabled, and if PIM is not enabled on the ingress network interface. Enable the Block PIM Tunneled parameter to enable extraction and processing of PIM packets arriving at the 7450 ESS, 7750 SR, or 7950 XRS NE inside a tunnel (for instance, MPLS or GRE) on a network interface.

23 Click on the following tabs in the NE DoS Protection tab to view violations information, as required. See Procedure 3-5 for more information.

- Per Source Violations
- Link Specific Port Violations
- Network Interface Violations
- SAP Violations
- SDP Violations

24 Click on the VPRN Network Exceptions tab to configure rate limits for VPRN network exceptions.

25 Configure the parameters:

- Enable Network Exception
- Number of Replies Allowed
- Time (sec)
  After the Enable Network Exception parameter is enabled, the configuration form expands to display the Rate Limit Parameters panel.

26 Click on the Deployment tab to view device deployment information, as required.

27 Click on the Faults tab to view alarm information, as required.

28 Click on the OK button. A dialog box appears.

29 Click on the Yes button. The NE System Security (Edit) form closes.

You must distribute policies to specific devices, as described in Procedure 3-21.

Procedure 3-13 To configure X.509 authentication on 7750 SR NEs

X.509 is an ITU-T standard for a Public Key Infrastructure (PKI). It provides an infrastructure for Certificate Management. Use the procedure to enable a 7750 SR NE to establish IPsec tunnels between IPsec peers by using an X.509 certificate to authenticate each other during the initial exchange of IKEv2.

Perform the following to configure PKI Site Security.

1 Choose Administration→Security→NE PKI Authentication→Site Public Key Infrastructure from the 5620 SAM main menu. The Select Site form opens.

2 Choose a managed device in the list and click on the OK button. The Site Security Public Key Infrastructure (Edit) form opens with the General tab displayed.

3 Configure the parameters:

- Maximum Certificate Chain Depth
- Synchronization Certificate Mode
- Perform Certificate Synchronization

Administration Certificate script and CLI-based tasks

Note — The following tasks are available when you click the Admin Certificate button at the bottom of the Site Security Public Key Infrastructure (Edit) form. They allow you to perform various X.509 certificate operations for the selected site NE using 5620 SAM system scripts and CLI mediation. Execute the tasks as required.

4 Generate Keypair

This task generates RSA or DSA private key/public key pairs and store them in a local file in the NE's cf3:\system-pki\filename.

Configure the parameters as follows:

- Output File URL: Specify a local URL of the keyfile. This can be located on cf1:, cf2:, or Cf3. For example: cf3:/system-pki/filename
- Key Size: Specify the key size in bits. The choices include:
    - 512
    - 1024
    - 2048 (default)
- Key Type: Specify the type of the key.
    - rsa (default)
    - dsa

Click the Execute button to run the task.

5 Generate local certificate request

This task generates a PKCS#10 formatted certificate request by using a local existing key pair file.

Configure the parameters as follows:

- Input Keypair URL: Specify the local URL of the key file that is used to generate the certificate request. For example: cf3:/system-pki/filename
- Subject Distinguish Name: Specify a distinguishing name that is used as the subject in the certificate request, including:
    - C-Country
    - ST-State
    - O-Organization name
    - OU-Organization Unit name
    - CN-common name

      This parameter is formatted as a text string and can include any of the listed attributes. An attribute and its value are linked by an equals sign. A comma is used to separate different attributes. For example: C=US,ST=CA,O=ALU,CN=7750 SR12
- Domain Name: You can optionally specify a domain name string up to 255 characters in length as a dNSName in the Subject Alternative Name extension of the certificate request.
- IP Address: You can optionally specify an IPv4 address string as the ipAddress in the Subject Alternative Name extension of the certificate request.
- Output File URL: Specify a local CF card path and filename to save the certificate request. For example: cf3:/system-pki/filename
- Hash Algorithm

Click the Execute button to run the task.

6 Import File

This task converts an input file (key, certificate, or CRL) to a 7750 SR system format file.

Configure the parameters as follows:

- Input File Type: Specify the type of input file. The choices include:
    - cert
    - key
    - crl
- Input File URL: Specify a local URL for the keyfile. This URL can either be a local CF card URL file or an FP URL used to download the input file. For example: cf3:/system-pki/filename
- Output Filename: Specify the name of output file. The maximum string length is 95 characters.
- Input Format: Specify the format of the input file. The choices include:
    - pkcs12
    - pkcs7-der
    - pkcs7-pem
    - pem
    - der
- Password: Specify the password to decrypt the input file, if it is an encrypted PKCS#12 file. The maximum string length is 32 characters.

Click the Execute button to run the task.

7 Export File

This task converts an 7750 SR system format file (key, certificate, or CRL) to another format.

Configure the parameters as follows:

- Input File Type: Specify the type of input file. The choices include:
  - cert
  - key
  - crl
- Input Filename: Specify the name of input file. The maximum string length is 95 characters.
- Output File URL: Specify a local URL for the output file. For example: cf3:/system-pki/filename
- Output Format: Specify the format of the output file. The choices include:
  - pkcs12
  - pkcs7-der
  - pkcs7-pem
  - pem
  - der
- Password: Specify the password to decrypt the output file, if it is an encrypted PKCS#12 file. The maximum string length is 32 characters.
- Key File: Specify the corresponding key file when exporting a certificate to the PKCS12 format. The maximum string length is 95 characters.

Click the Execute button to run the task.

8 Display File

This task displays the content of an input file in plain text. If you are requesting key file content, only the Key Size and Key Type will be displayed.

Configure the parameters as follows:

- Input File Type: Specify the type of input file. The choices include:
  - cert
  - key
  - crl
- Input File URL: Specify a local URL for the input file. For example: cf3:/system-pki/filename
- Input Format: Specify the format of the input file. The choices include:
  - pkcs12
  - pkcs7-der
  - pkcs7-pem
  - pem
  - der
- Password: Specify the password to decrypt the input file, if it is an encrypted PKCS#12 file. The maximum string length is 95 characters.

Click the Execute button to run the task.

9 Reload File

This task reloads the specified file from compact flash disk.

Configure the parameters as follows:

- Input File Type: Specify the type of input file. The choices include:
    - cert
    - key
- Input File URL: Specify the name of the file to be reloaded. For example: cf3:/system-pki/filename

Click the Execute button to run the task. For example: cf3:/system-pki/filename

10 Click on the OK button when the script and CLI-based tasks that you needed to execute have been completed. A dialog box appears.

11 Click on the Yes button. The Site Security Public Key Infrastructure (Edit) form closes.

Procedure 3-14 To configure a PKI certificate authority profile

A Certificate Authority (CA) is a trusted third party whose job is to certify the authenticity of users. Authenticity is guaranteed by the CA digital signature created with the CA private key. You can verify a digital signature using the CA public key. Only the CA public key can decrypt the digital certificate.

Perform the following to create and distribute CA Profile policy.

1 Choose Administration→Security→NE PKI Authentication→PKI Certificate Authority Profiles from the 5620 SAM main menu. The PKI Certificate Authority Profiles form opens.

2 Click the Create button. The Certificate Authority Profile (Create) form opens with the General tab displayed.

3 Configure the parameters:

- Name
- Description
- CRL File
- Certificate File
- Administrative State
- Responder URL
- Service ID

4 Click on the CMPv2 tab.

5 Configure the parameters:

- HTTP Response Timeout
- Response Signing Certificate
- Accept Unprotected Error Messages
- Accept Unprotected PKI Configuration Messages
- Use Same Recipient Nonce
- Set Sender Field in CMPv2 Header
- CA Server URL
- Service ID

6 Perform the following to create CMP keys, as required.

Note — Keys that are created on an NE, for example when the NE is discovered or a Certificate Authority Profile is created using CLI, are not transmitted using SNMP, and appear in Certificate Authority Profile form as "N/A". Any N/A keys must be deleted before the profile can be distributed.

i Click on the Create button in the Key List panel. The CMP Key List (Create) form opens.

ii Configure the parameters:

- Reference Number
- Key Secret

iii Click on the OK button. The CMP Key List (Create) form closes and the new key appears in the Key List panel.

7 Click on the Apply button. The Policy Configuration panel is displayed in the General tab.

8 Click on the Distribute button to manually distribute the policy to the selected devices. If the Distribute button is not visible, click on the More Actions button and choose Distribute.

Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can choose which NEs to distribute the policy to. See Procedure 3-21 for more information about distributing security policies.

9 Close the Distribute - PKI Certificate Authority Profile form.

10 Close the Certificate Authority Profile (Edit) form.

Procedure 3-15 To perform CMPv2 actions

1 Choose Administration→Security→NE PKI Authentication→Site Public Key Infrastructure from the 5620 SAM main menu. The Select Site form opens.

2 Choose a managed device in the list and click on the OK button. The Site Security Public Key Infrastructure (Edit) form opens with the General tab displayed.

3 Click on the Admin Certificate button and choose Perform CMPv2 Actions. The Admin Certificate form opens.

4 Perform the following to select a certificate authority profile. For information about configuring certificate authority profiles, see Procedure 3-14.

  i Click on the Select button beside the CA Profile Name parameter. The Select CA Profile form opens.

  ii Configure the filters and click on the Search button. A list of certificate authority profiles appears.

  iii Select a profile and click on the OK button. The Select CA Profile form closes and the selected profile appears in the CA Profile Name parameter.

CMPv2 actions

5 Select the CMPv2 action you need to perform from the drop-down menu beside the Type parameter in the Action panel. Table 3-1 lists the available CMPv2 actions. You can view the status of the last CMPv2 action performed on this site in the Last Action Status panel.

Table 3-1 CMPv2 actions

Action	See step
Initial Registration	6
Certificate Request	9
Key Update	12
Poll	15
Clear Request	16
Abort Request	17

Initial Registration

6 Configure the parameters in the Action panel:

- Action Key
- Subject Domain
- Save As File

7 Perform one of the following:

  a To perform an initial registration using a password, configure the parameters in the Protection Algorithm - using Password panel:

  - Password
  - Reference Number

  b To perform an initial registration using a certificate, configure the parameters in the Protection Algorithm - using Certificate panel:

  - Certificate
  - Protection Key
  - Hash
  - Send Chain

8 Click on the Apply button to perform the action.

Certificate Request

9 Configure the parameters in the Action panel:

- Action Key
- Subject Domain
- Save As File
- New Key

10 Configure the parameters in the Protection Algorithm - using Certificate panel:

- Certificate
- Hash

11 Click on the Apply button to perform the action.

Key Update

12 Configure the parameters in the Action panel:

- Action Key
- Save As File
- New Key

13 Configure the parameters in the Protection Algorithm - using Certificate panel:

- Certificate
- Hash

14 Click on the Apply button to perform the action.

Poll

15 Click on the Apply button to send the poll request.

Clear Request

16 Click on the Apply button to send the clear request.

Abort Request

17 Click on the Apply button to send the abort request.

Procedure 3-16 To configure an NE firewall on the 7705 SAR-H

Note — The following firewall procedure is only applicable to the 7705 SAR-H, Release 5.0.

Perform the following procedure to configure a firewall using the firewall manager.

1 Choose Administration→Security→NE Firewall→Default NE Firewall from the 5620 SAM main menu. The Firewall - Default (Edit) form opens.

2 Click on the Search button to display a list of site IDs.

3 Choose a Site ID from the list and click on the Properties button.

4 The Firewall Site (Edit) form opens with the General tab displayed.

5 Configure the parameters:

- Key
- Discard Fragments
  - Enabled
  - Disabled (default)

6 Click on one of the following tabs to modify the firewall properties:

a Host Groups

b Service Groups

c Rule Sets

d Zones

e Statistics

7 In the Firewall Site on the navigation tree, choose one of the following to create a new policy on the site:

a Right-click on Zones and choose Create Zone.

b Right-click on Rule Sets and choose Create Rule Set.

c Right-click on Service Groups and choose Create Service Group.

d Right-click on Host Groups and choose Create Host Group.

8 In the Firewall Site on the navigation tree, choose one of the following to add a firewall policy on the site:

a To add a zone, right-click on Zones and choose Add.

b To add a rule set, right-click on Rule Sets and choose Add.

c To add a service group, right-click on Service Groups and choose Add.

d To add a host group, right-click on Host Groups and choose Add.

9 The Select Global Policies - Firewall Site - Default, Site form opens.

10 Click on the Search button to display a list of policies.

11 Choose a policy from the list and click on the OK button to add the policy to the existing site.

12 To delete a firewall policy right-click on one of the following and choose Delete:

a Zone

b Rule Set

c Service Group

d Host Group

Note 1 — Policies can be deleted in the following order:

- Zone
- Rule Set
- Host Group or Service Group

Note 2 — Host Group or Service Group policies cannot be deleted if rule sets are associated with them.

Note 3 — Rule set policies cannot be deleted if they are associated with zones.

Note 4 — Zone policies cannot be deleted if they are associated with SAP, SDP, MGMT, or CPM interfaces.

13 Click on the OK button to close the Firewall Site (Edit) form.

14 The Firewall - Default (Edit) form opens.

15 The Network Interfaces, SAPs and SDPs tabs display the firewall instances associated with the zone.

16 To add a firewall entry for the network interfaces, SAPs or SDPs:

i Choose a Site Id from the list.

ii Click on Add Firewall Entry.

iii The Firewall Interface Entry, Firewall SAP Entry, or the Firewall SDP Entry (Create) form opens.

iv Configure the following parameters:

- Auto-Assign ID (Entry Id is disabled if Auto-Assign ID is selected)
- Entry Id
- Zone ID
- Zone Name

v Click on the Select button, the Select Zone form opens.

vi Choose a zone from the list and click on the OK button.

vii Click on the OK button in the Firewall Interface Entry, Firewall SAP Entry, or the Firewall SDP Entry (Create) form.

viii The Firewall - Default (Edit) form opens.

17 To view the Firewall Properties from the Network Interfaces, SAPs and SDPs tabs, choose a Site Id and click on the Properties button.

18 Click on the OK button to close the Firewall - Default (Edit) form.

Procedure 3-17 To configure an NE management access firewall on the 7705 SAR-H

Caution — If the zone entry using the Management Access Firewall on the 7705 SAR-H is not properly configured, the essential communication channel between 5620 SAM and the NE could be terminated. It is advisable to check before turning up the Management Access Firewall that protocols such as UDP, ICMP, SSH, TFTP, FTP, TELNET, SCP, and NTP are not blocked.

Note 1 — The following firewall procedure is only applicable to the 7705 SAR-H, Release 5.0.

Note 2 — You cannot attach a zone containing a ruleset that has a firewall log with destination as syslog to the management access firewall.

Perform the following procedure to configure a firewall using the management access interface.

1 Choose Administration→Security→NE Firewall→NE Management Access Firewall from the 5620 SAM main menu. The NE Management Access Firewall form opens.

2 Perform one of the following:

a To create a firewall, click on the Create button. The Management Access Firewall (Create) form opens.

b To modify a firewall, click on the search button to display a list of firewall entries. Choose an entry from the filtered list and click on the Properties button. The Management Access Firewall (Edit) form opens with the General tab displayed.

3 Configure the following parameters:

- Displayed Name
- Description
- Administrative State
  - Enabled
  - Disabled (default)

4 Click on the Firewall Entries tab.

5 Click on the Create button. The Firewall Entry (Create) form opens.

6 Configure the following parameters:

- Auto-Assign ID (Entry Id is disabled if Auto-Assign ID is selected)
- Entry Id
- Zone ID
- Zone Name

7 Click on the Select button, the Select Zone form opens.

8 Choose a zone from the list and click on the OK button.

9 Select the IP Operator check box from the IP Address panel on the Firewall Entry (Create) form.

10 Choose one of the following from the IP Operator drop-down menu and enter the range, if required:

- EQUAL
- RANGE

11 Click on the OK button to close the form. The Management Access Firewall (Create) form opens.

12 Choose the newly created NE Management Access Firewall policy and click on the Properties button.

13 The Management Access Firewall form opens. The Configuration Mode parameter in the Policy Configuration panel is in the Draft state. Release the policy and distribute the policy as required.

i Click on the Switch Mode button. A confirmation dialog box opens.

ii Click on the Yes button to confirm the action. The Configuration Mode is changed to Released state.

14 When you release the global policy, the policy is also distributed to local definitions. See “To distribute a policy” in the *5620 SAM User Guide* for information.

Procedure 3-18 To configure an NE CPM firewall on the 7705 SAR-H

Note — The following firewall procedure is only applicable to the 7705 SAR-H, Release 5.0.

Perform the following procedure to configure a firewall using the CPM interface.

1. Choose Administration→Security→NE Firewall→NE CPM Firewall from the 5620 SAM main menu. The NE CPM Firewall form opens.
2. Perform one of the following:
   - **a** To create a firewall, click on the Create button. The NE CPM Firewall (Create) form opens.
   - **b** To modify a firewall, click on search to display a list of firewall entries. Choose an entry from the filtered list and click on the Properties button. The NE CPM Firewall (Edit) form opens with the General tab displayed.
3. Configure the following parameters:
   - Displayed Name
   - Description
   - Administrative State
     - Enabled
     - Disabled (default)
4. Click on the Firewall Entries tab.
5. Click on the Create button. The Firewall Entry (Create) form opens.
6. Configure the following parameters:
   - Auto-Assign ID (Entry Id is disabled if Auto-Assign ID is chosen)
   - Entry Id
   - Zone ID
   - Zone Name
7. Click on the Select button, the Select Zone form opens.
8. Choose a zone from the list and click on the OK button.
9. Select the IP Operator check box from the IP Address panel on the Firewall Entry (Create) form.
10. Choose one of the following from the IP Operator drop-down menu and enter the range, if required:
    - EQUAL
    - RANGE
11. Click on the OK button to close the form. The NE CPM Firewall (Create) form opens.
12. Choose the newly created NE CPM Firewall policy and click on the Properties button.

13 The NE CPM Firewall form opens. The Configuration Mode parameter in the Policy Configuration panel is in the Draft state. Release the policy and distribute the policy as required.

   i Click on the Switch Mode button. A confirmation dialog box opens.

   ii Click on the Yes button to confirm the action. The Configuration Mode is changed to Released state.

14 When you release the global policy, the policy is also distributed to local definitions. See “To distribute a policy” in the *5620 SAM User Guide* for information.

Procedure 3-19 To configure a subscriber authentication policy

The 5620 SAM provides security support for creating DHCP sessions on supporting devices. The 5620 SAM allows you to create a policy that uses RADIUS authentication to grant network access to a dynamic host. You can apply the policy to a VPLS or IES SAP, or to a VPRN or IES group interface. Authentication is not performed for statically provisioned hosts.

Perform this procedure to create a DHCP-based subscriber authentication policy that defines the parameters for dynamically created subscriber host sessions and authenticates the sessions. The 5620 SAM supports up to 32 subscriber authentication policies.

1 From the 5620 SAM main menu, choose Policies→AAA Policies→Subscriber Authentication. The Subscriber Authentication form opens.

2 Perform one of the following:

   a To create a subscriber authentication policy, click on the Create button. The Subscriber Authentication Policy (Create) form opens.

   b To modify a subscriber authentication policy, click on Search to display a list of subscriber authentication policy entries. Choose an entry from the list and click on the Properties button. The Subscriber Authentication Policy (Edit) form opens with the General tab displayed.

3 Configure the parameters:

- Displayed Name
- Description
- Re-Authenticate When DHCP Lease Expires
- Accept CoA
- RADIUS Attributes
- PPPoE Access Method
- Accounting Stop Message
- Password
- NAS Port Bit Specification
- Calling Station ID Type
- Port Type
- Port Type Value
- Port Prefix Type
- Port Prefix String
- Port Suffix Type

Note — The NAS Port Bit Specification parameter is configurable when the NAS Port option is enabled for the RADIUS Attributes parameter.

The Calling Station ID Type parameter is configurable when the Calling Station ID option is enabled for the RADIUS Attributes parameter.

The Port Type parameter is configurable when the NAS Port Type option is enabled for the RADIUS Attributes parameter.

The Port Type Value parameter is configurable when the NAS Port Type option is enabled for the RADIUS Attributes parameter, and the Port Type parameter is set to Config.

The Port Prefix Type, Port Prefix String, and Port Suffix Type parameters are configurable when the NAS Port ID option is enabled for the RADIUS Attributes parameter.

4 If you need to configure PAP/CHAP user name re-writing, configure the following parameters in the User Name panel:

- User Name Format
- User Name Operation
- Domain Name
- User Name Mac Format
- Show Format

Note — The Domain Name parameter is configurable when the User Name Operation parameter is set to Append, Replace, or Use As Default.

The User Name Mac Format and Show Format parameters are configurable when the User Name Format parameter is set to DHCP Client Vendor Options.

5 In the RADIUS Fallback panel, configure the following parameters:

- Fallback Action
- Local User DB Name

Note — The Local User DB Name parameter is configurable when the Fallback Action parameter is set to User DB.

6 In PPP User Name panel, configure the following parameters:

- User Name Operation
- Domain Name

Note — The Domain Name parameter is configurable when the User Name Operation parameter is set to Append, Replace, or Use As Default.

7 Configure RADIUS script policies, if required.

i Click on the Select button next to the Accept Script field and choose an accept script from the Select Script Policy form.

ii Click on the Select button next to the CoA Script field and choose a CoA script from the Select Script Policy form.

iii Click on the Select button next to the Request Script field and choose a request script from the Select Script Policy form.

8 Click on the Select button in the RADIUS Server Policy panel and choose a RADIUS server policy from the Select RADIUS Server Policy form.

9 Configure the RADIUS servers for the policy, if required. Otherwise, go to step 10.

i Click on the RADIUS Servers tab.

ii Configure the parameters:

- Retry Attempts
- Timeout (seconds)
- Access Algorithm
- Source Address
- Authentication Hold Down Time

iii Configure the Router Instance parameter. If you set the Router Instance parameter to VPRN, perform step iv. Otherwise, go to step v.

iv Configure a VPRN service as a virtual router instance for the RADIUS-based accounting policy. Click on the Select button in the VPRN ID panel and choose a VPRN site from the Select VPRN ID - Radius Accounting Policy list form.

v Click on the Create button. The RadiusEntry form opens.

vi Configure the parameters:

- Auto-Assign ID
- ID
- Description
- Server IP Address
- Port
- CoA Only
- RADIUS Authentication Requests Limit
- Secret Name

vii Click on the OK button. A dialog box appears.

viii Click on the OK button. The RadiusEntry form closes and the Subscriber Authentication Policy form refreshes with the RADIUS server information displayed in a list in the RADIUS Servers tab.

ix Repeat steps v to viii to add additional RADIUS servers, as required.

10 Click on the Apply button. The Subscriber Authentication Policy form refreshes with additional buttons and tabs.

11 Click on the Distribute button to manually distribute the policy to the selected devices. If the Distribute button is not visible, click on the More Actions button and choose Distribute.

See Procedure 3-21 for information about distributing security policies. Policies are also automatically distributed to devices when they are used by resources on the device.

Note — When the policy is in draft mode, the Distribute button, or the Distribute option under the More Actions button, is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution. Releasing the global policy displays the Distribute window, where you can choose which NEs to distribute the policy to. See Procedure 3-21 for more information.

12 Close the Subscriber Authentication Policy form. The Subscriber Authentication form refreshes with the policy information displayed in a list.

Procedure 3-20 To modify a security policy

Note 1 — Before you distribute policies to managed devices, ensure the management access filter Action parameter is not set to deny. Shut down the filter, distribute the policies, and then turn the filter back up.

Note 2 — If the policy is in draft mode, the Distribute button, or the Distribute option located under the More Actions button, is disabled and the policy cannot be distributed. You must first release the policy for distribution.

When you change the configuration mode of a management access filter or CPM IP filter to released, the policy is not distributed to existing local definitions. When all other policies are changed to released, the policy is distributed to existing local definitions

1 Choose the appropriate policy from one of the following.

- **a** The Administration→Security→*option* 5620 SAM main menu
- **b** The Policies→AAA Policies→*option* 5620 SAM main menu

The appropriate form opens.

2 Set the filter criteria, if applicable. You can filter or local or global policies by using the Policy Scope parameter. When you set the parameter to Local, you can search on a specific managed device by clicking on the Select button beside the Local Node IP Address parameter.

3 Click on the Search button. A policy list opens.

4 Specify whether to modify the global or the local instance of the policy.

- **a** Local policies have a check mark for the Local column.
- **b** Global policies do not have a check mark for the Local column.

5 Choose a policy from the list.

6 Click on the Properties button.

7 Configure the policy parameters, as required.

From either a local or global policy, you can click on the Local Definitions or Global Definitions tab to view the local instances of policies or the global policy used to define the local instance.

8 Save the changes and close the file. You must distribute global policies to the managed devices. You do not distribute modified local policies.

Procedure 3-21 To distribute a security policy

1 Create policies, as described in Procedures 3-1 to 3-19.

2 Choose the appropriate policy from one of the following.

- **a** The Administration→Security→*option* 5620 SAM main menu
- **b** The Policies→AAA Policies→*option* 5620 SAM main menu

The appropriate form opens.

3 Set the filter criteria, if applicable.

4 Click on the Search button. A policy list opens.

5 When:

- **a** A management access filter is configured to deny access to managed devices, ensure the following:
  - **i** List the applicable management access filters. A list of management access filters opens.
  - **ii** Shut down the management access filter.
  - **iii** Distribute the policies. Complete steps 6 to 14.
- **b** If no management access filter is configured, go to step 6.

6 Choose a policy from the list.

7 Click on the Properties button if you are distributing a CPM IP, NE DoS protection, or management access filter. The *Policy_Type*, Global (Edit) form opens.

8 When the policy is in Draft configuration mode, the Distribute button, or the Distribute option located under the More Actions button, is disabled and the policy cannot be distributed to the NEs. You must first release the policy for distribution by performing the following steps. Otherwise, go to step 9.

- **i** Click on the Switch Mode button beside the Configuration Mode parameter. A dialog box appears.
- **ii** Click on the Yes button. The configuration mode of the policy is changed to Released.

Warning — When you change the configuration mode of a management access filter or CPM IP filter to Released, the policy is not automatically distributed to existing local definitions. When all other policies are changed to released, use the Distribute window distribute the policy to the required NEs.

- **iii** View the local policy, if necessary, by clicking on the Local Definitions tab and double-clicking on the local policy in the list.
- **iv** Close the local policy form.

9 Click on the Distribute button. If the Distribute button is not visible, click on the More Actions button and choose Distribute. The Distribute form opens.

10 Choose a row or rows from the Available Objects list.

11 Click on the right arrow button. The chosen device or devices move to the Selected Objects panel on the right side of the form.

12 Click on the Distribute button. If the Distribute button is not visible, click on the More Actions button and choose Distribute. CPM IP and management access filters require that you confirm the policy distribution. The policy is distributed to the device or devices.

13 Close the Distribute form. The *Policy_Type*, Global (Edit) form reappears.

14 Configure the distribution mode of the local definitions by performing the following steps.

- **i** Click the Switch Distribution Mode button. If the Switch Distribution Mode button is not visible, click on the More Actions button and choose Switch Distribution Mode. The Distribution Mode - *Policy* form opens.
- **ii** Configure the Distribution Mode parameter. The existing local definitions that are configured with the selected distribution mode are listed.
- **iii** Choose one ore more rows from the Available Nodes with Local Policies list.
- **iv** Click on the right arrow button. The chosen device or devices move to the Selected Nodes with Local Policies panel on the right side of the form.
- **v** Depending on the distribution mode of the chosen device or devices, perform one of the following:
    - Click on the Sync With Global button.
    - Click on the Local Edit Only button.
- **vi** Close the Distribution Mode - *Policy* form. The *Policy_Type*, Global (Edit) form reappears.

15 Turn up the management access filter if you performed step 5 a ii. Otherwise, go to step 16.

16 Close the *Policy_Type*, Global (Edit) form.

17 Close the policy manager form.

Procedure 3-22 To delete a security policy

Note 1 — When you delete site management access filter policies in which the Action parameter is set to deny, ensure that you modify the policy to set the parameter to permit before it is deleted, otherwise, the 5620 SAM may be isolated.

Note 2 — You cannot remove a site management access filter if the filter administrative state is up and the default action of the filter is set to deny or deny host unreachable.

Note 3 — If you attempt to delete an OmniSwitch RADIUS or TACACS+ security policy that is applied to an authentication service, the 5620 SAM generates a deployment error. You must use the OmniSwitch CLI to delete the policy from the authentication service before you can delete the policy from the 5620 SAM.

1 Choose the appropriate policy from one of the following.

  a The Administration→Security→*option* 5620 SAM main menu

  b The Policies→AAA Policies→*option* 5620 SAM main menu

  The appropriate form opens.

2 Set the filter criteria, if applicable.

3 Click on the Search button. A policy list opens.

4 Choose a policy from the list.

5 Click on the Delete button.

6 Click on the Yes button. The policy is deleted.

Procedure 3-23 To manually unlock a user account

Use this procedure to manually unlock a user account that is locked due to too many failed login attempts.

1 From the 5620 SAM main menu, choose Administration→Security→NE User Configuration. The NE User Configuration form opens.

2 Configure the filters and click on the Search button. A list of user accounts appears.

3 Perform one of the following:

- **a** To unlock a 5620 SAM user, choose the user and click on the Unlock User button. The user account is unlocked.
- **b** To unlock the local definition of a user on an NE, perform the following:
    - **i** Choose a user account and click on the Properties button. The NE User form opens.
    - **ii** Click on the Local Definitions tab.
    - **iii** Configure the filters and click on the Search button. A list of NEs with local definitions for the user appears.
    - **iv** Choose an NE and click on the Unlock User button. The user account on the selected NE is unlocked.
    - **v** Close the NE User form.

4 Close the NE User Configuration form.

Procedure 3-24 To clear collected statistics on a CPM filter

Use this procedure to clear the IPv4, IPv6, MAC or Queue statistics collected on a local definition of a CPM filter.

1 From the 5620 SAM main menu, choose Administration→Security→NE CPM Filter. The CPM Filter form appears.

2 Configure the filters and click on the Search button. A list of CPM filters appears.

3 Choose a CPM filter and click on the Properties button. The CPM Filter (Edit) form appears.

4 Click on the Local Definitions tab.

5 Configure the filters and click on the Search button. A list of CPM filter local definitions appears.

6 Choose a local definition and click on the Properties button. The CPM Filter Local Policy form appears.

7 Click on the IPv4 Entries, IPv6 Entries, MAC Entries or Queues tab, depending on the type of statistic you need to clear.

8 Configure the filters and click on the Search button. A list of filter entries appears.

9 Perform one of the following:

- **a** To clear specific entries, choose the entries you need to clear and click on the Clear Statistics on Entry button.
- **b** To clear all entries, choose an entry and click on the Clear Statistics on All Entries button. This button is not available in the Queues tab.

10 To view the status of all clear requests, perform the following:

  i Click on the Clear Statistics Status tab.

  ii Configure the filters, and click on the Search button. A list of clear requests appears.

  iii Choose a clear request and click on the Properties button. The status of the clear request appears.

11 Close the CPM Filter Local Policy, CPM Filter (Edit) and CPM Filter forms.

Procedure 3-25 To clear the password history of a user on a managed device

1 Choose Administration→Security→NE User Configuration from the 5620 SAM main menu. The NE User Configuration form opens.

2 Configure the filters and click on the Search button. A list of configured users appears.

3 Select a user and click on the Properties button. The NE User (Edit) form opens.

4 Click on the Local Definitions tab. A list of sites with local definitions for the selected user appears.

5 Select one or more sites and click on the Clear Password History button. A dialog box appears.

6 Click on the Yes button to confirm the operation. The password history for the selected user at the specified sites is cleared.

7 Click on the OK button. The NE User (Edit) form closes.

Procedure 3-26 To manage OCSP cache entries on an NE

1 Choose Administration→Security→NE PKI Authentication→Site Public Key Infrastructure from the 5620 SAM main menu. The Select Site form opens.

2 Choose a managed device in the list and click on the OK button. The Site Security Public Key Infrastructure (Edit) form opens with the General tab displayed.

3 Click on the OCSP Cache Entries tab.

4 Configure the filters and click on the Search button. A list of OCSP cache entries for the site opens.

5 To clear cache entries, perform the following.

- **i** Click on the Admin Certificate button and choose Clear OCSP Cache. The Admin Certificate Clear OCSP Cache form opens.
- **ii** Enter the Entry ID number of the cache entry you need to clear in the Entry ID parameter. To clear all entries, leave the parameter blank.
- **iii** Click on the Execute button. The results of the clear operation appear in the results panel.
- **iv** Click on the Close button. The Admin Certificate Clear OCSP Cache form closes.

6 Click on the OK or Cancel button. The Site Security Public Key Infrastructure (Edit) form closes.

4 — TCP enhanced authentication

4.1 TCP enhanced authentication overview

This chapter describes the 5620 SAM support of TCP enhanced authentication for NEs based on the MD5 encryption mechanism described in RFC2385. 5620 SAM TCP enhanced authentication allows the use of powerful algorithms for authenticating routing messages.

The 5620 SAM uses a TCP extension to enhance BGP and LDP security. TCP enhanced authentication is used for applications that require secure administrative access at both ends of a TCP connection. TCP peers update authentication keys during the lifetime of a connection.

A 5620 SAM operator with administrative privileges can create, delete, modify, and distribute TCP enhanced authentication components, and can perform an audit of a local key chain to compare it with the associated global key chain or other local key chains. The 5620 SAM TCP enhanced authentication components are called keys and key chains.

Global key chains are created in draft mode. This allows operators to verify that the key chain is correctly configured before they distribute it to the network elements. When the key chain is approved for distribution, you can change the global key chain to released mode, which also distributes the key chain to existing local definitions. The 5620 SAM saves the latest released version of the global key chain.

Caution — Alcatel-Lucent recommends that you use only the 5620 SAM to create keys and key chains. Do not create a key or key chain directly on a managed NE using another interface, for example, a CLI. The 5620 SAM cannot obtain a TCP key secret value from an NE during resynchronization, so it cannot specify the key for use on another NE.

If a local NE key chain and the associated global 5620 SAM key chain differ after a resynchronization, the 5620 SAM generates an alarm.

TCP keys and key chains

A key is a data structure that is used to authenticate TCP segments. One or more keys can be associated with a TCP connection. Each key contains an identifier, a shared secret, an algorithm identifier, and information that specifies when the key is valid for authenticating the inbound and outbound segments.

A key chain is a list of up to 64 keys that is associated with a TCP connection. Each key within a key chain contains an identifier that is unique within the key chain. You can use the 5620 SAM to distribute a global key chain to multiple NEs and assign a key to multiple BGP or LDP instances.

The 5620 SAM treats global and local key chain management as it does policy management; depending on the distribution mode configuration of a local key chain, when you modify a global key chain using the 5620 SAM, all local instances can be updated to ensure that all instances of the key chain in the network are synchronized. See “Policies overview” in the *5620 SAM User Guide* for information about global and local policy instances, policy distribution and distribution modes, and local policy audits.

When the 5620 SAM attempts to synchronize the keys in a global key chain with the keys on an NE, the NE does not return the secret key value. After a key chain is deployed to an NE, the shared secret and the encryption algorithm cannot be modified. You can delete a key chain or key only when it is not in use by a protocol.

You can specify whether an NE uses a TCP key for sending packets, receiving packets, or both. Using keys that are configured for both, or send-receive, is general good practice because communication between NEs cannot be affected by assigning the wrong key type.

There are two classes of TCP keys:

- Active
- Eligible

Active keys

A key set contains one active key. An active key is a key that TCP uses to generate authentication information for outbound segments. You cannot delete the active key in a keychain.

Eligible keys

Each set of keys, called a key chain, contains zero or more eligible keys. An eligible key is a key that TCP uses to authenticate inbound segments.

4.2 Workflow to configure TCP enhanced authentication for NEs

1. Create a global key chain that contains at least one key. See Procedure 4-1 for more information.
2. Distribute the key chain to the NEs. See Procedure 4-2 for more information.
3. Verify the distribution of a global key chain to the NEs. See Procedure 4-3 for more information.
4. Assign the key chain to a routing protocol, such as BGP or LDP. See “Protocol configuration overview” in the *5620 SAM User Guide* for more information.
5. If required, identify the differences between a global and local policy or two local key chains. See Procedure 4-4 for more information.
6. As required, delete a key from a local or global TCP key chain or delete a local or global TCP key chain. See Procedure 4-5 or 4-6 for more information.

4.3 TCP enhanced authentication procedures

Use the following procedures to perform TCP enhanced authentication management functions.

Procedure 4-1 To configure a global TCP key chain

1 Choose Administration→Security→TCP KeyChains from the 5620 SAM main menu. The TCP KeyChains form opens.

2 Perform one of the following:

a To create a key chain, perform the following steps:

i Click on the Create button. The KeyChain (Create) form opens with the General tab displayed.

ii Configure the Displayed Name parameter.

Note — Do not use a colon in the policy name. The 5620 SAM uses colons as separators for the object full name.

b To configure an existing key chain, perform the following steps:

i If required, configure the filter criteria and click the Search button. A list of key chains appears.

ii Choose a key chain and click on the Properties button. The KeyChain (Edit) form opens with the General tab displayed.

Note — When you modify a key chain or key, the modified object is automatically distributed to the NEs that have a local instance of the key chain.

3 Configure the parameters:

- Description
- Send Option
- Receive Option
- Admin State

4 Click the KeyChain Key tab.

5 Perform one of the following:

a To create a key chain key, perform the following steps:

i Click the Create button. The KeyChain Key (Create) form opens.

ii Configure the parameters:

- Key ID
- Auto-Assign ID
- Secret Key Algorithm
- Key
- Key Direction

Caution — Alcatel recommends that you choose the Send-receive option for the Key Direction parameter to ensure bidirectional communication between NEs.

Note — The 5620 SAM generates a random default value for the Key parameter. For greater security, Alcatel-Lucent recommends that you accept this value rather than manually enter a value.

b To configure an existing key chain key, perform the following steps:

i If required, configure the filter criteria and click the Search button. A list of key chain keys appears.

ii Choose a key chain key and click on the Properties button. The KeyChain Key (Edit) form opens with the General tab displayed.

6 Configure the parameters:

- Admin State
- Begin Time
- End Time
- Tolerance (seconds)

The End Time parameter is configurable only if the Key Direction parameter is set to Receive.

7 Click on the OK button. A dialog box appears.

8 Click the OK button. The key is added to the keychain and displayed on the KeyChain (Edit) form.

9 Click the OK button. The KeyChain (Edit) form closes.

10 Close the TCP KeyChains form.

Procedure 4-2 To distribute global key chains to NEs

Perform the following procedure to distribute one or more global TCP key chains to one or more NEs. When you distribute a global key chain, local key chain using the Sync With Global distribution mode allow the NE to receive the key chain.

Note — Local key chains using the Local Edit Only distribution mode do not allow the NE to receive the distribution of a global key chain. You must ensure that the distribution mode for the local key chain is set to Sync With Global if you need the NE to receive the distribution of a global key chain.

1 Choose Administration→Security→TCP KeyChains from the 5620 SAM main menu. The TCP KeyChains form opens.

2 Configure the filter criteria and click on the Search button. A list of key chains is displayed.

3 Select one or more key chains in the list.

4 When the key chain is in draft configuration mode, the Distribute button, or the Distribute option located under the More Actions button, is disabled and the key chain cannot be distributed to the network elements. You must first release the key chain for distribution by performing the following steps. Releasing the global key chain also distributes the key chain to existing local definitions. Otherwise, go to step 5.

  i Click on the Properties button. The Key Chain (Edit) form opens.

  ii Click on the Switch Mode button beside the Configuration Mode parameter. A dialog box appears.

  iii Click on the Yes button. The configuration mode of the key chain is changed to Released.

Warning — When you switch the configuration mode of the global key chain to released, the key chain is distributed to existing local definitions.

  iv View the local key chain, if necessary, by clicking on the Local Definitions tab and double-clicking on the local key chain in the list.

  v Close the Key Chain (Edit) form. The TCP KeyChains form reappears.

5 Click on the Distribute button. If the Distribute button is not visible, click the More Actions button and choose Distribute. The Distribute - KeyChain form opens.

6 Select one or more NEs in the Available Nodes list.

7 Click on the right-arrow button. The selected NEs move to the Selected Nodes list.

8 Click on the Distribute button. If the Distribute button is not visible, click the More Actions button and choose Distribute. The 5620 SAM distributes the key chains to the NEs.

9 Close the Distribute - KeyChain form. The TCP KeyChains form reappears.

10 Configure the distribution mode of the local definitions by performing the following steps.

- **i** Click on the Switch Distribution Mode button. If the Switch Distribution Mode button is not visible, click on the More Actions button and choose Switch Distribution Mode. The Distribution Mode form opens.
- **ii** Choose Sync With Global, Local Edit Only, or All from the Distribution Mode parameter drop-down menu. The sites that are configured with the selected distribution mode are listed.
- **iii** Choose one ore more rows from the Available Nodes list.
- **iv** Click on the right arrow button. The chosen site or sites move to the Selected Nodes panel on the right side of the form.
- **v** Depending on the distribution mode of the chosen site or sites, perform one of the following:
  - Click on the Sync With Global button.
  - Click on the Local Edit Only button.
- **vi** Close the Distribution Mode form. The TCP KeyChains form reappears.

11 Close the TCP KeyChains form.

Procedure 4-3 To verify the distribution of a global key chain to NEs

Perform the following procedure to view a list of the NEs to which the 5620 SAM has successfully distributed a specific TCP key chain.

1 Choose Administration→Security→TCP KeyChains from the 5620 SAM main menu. The TCP KeyChains form opens.

2 Configure the filter criteria and click on the Search button. A list of key chains is displayed.

3 Select a key chain in the list.

4 Click on the Properties button. The KeyChain (Edit) form opens.

5 Click on the Local Definitions tab. The NEs that have a local instance of the key chain are displayed in a list.

6 View the list of NEs to confirm that the key chain is distributed to the required NEs.

7 Close the KeyChain (Edit) form.

8 Close the TCP KeyChains form.

Procedure 4-4 To identify differences between a global and local key chain policy or two local key chains

Note 1 — You can cancel the local audit at any time by clicking on the Local Audit Off button on the KeyChain (Edit) form.

Note 2 — The 5620 SAM does not identify differences between the Begin Time and End Time properties of key chains.

1 Choose Administration→Security→TCP KeyChains from the 5620 SAM main menu. The TCP KeyChains form opens.

2 Choose Local from the Policy scope drop-down menu.

3 Click on the Select button beside the Local Node IP Address parameter. The Select a Network Element form opens.

4 Choose a device from the list and click on the OK button. The Select a Network Element form closes and the TCP KeyChains form is updated with the network element IP address.

5 Click on the Search button. A list of local key chains is displayed.

6 Choose the local key chain that you need to compare with another key chain.

7 Click on the Properties button. The KeyChain (Edit) form opens.

8 Click on the Local Audit On button. The Local Audit form opens.

9 From the Policy scope drop-down menu:

- **a** Choose Global and go to step 10.
- **b** Choose Local and configure the Local Node IP Address parameter by using the Select button to choose a network element. The Select a Network Element form opens.
    - **i** Choose a network element and click on the OK button. The Select a Network Element form disappears, and the policy manager form reappears with a list of the local policies for the chosen network element in the bottom panel.
    - **ii** Go to step 10.

10 Click on the OK button. The Local Audit form closes.

11 View the differences between the key chains by clicking on the tabs that are highlighted with an arrow icon to indicate that differences exist on the forms. An arrow icon beside a property indicates that the property is modified. In lists, new entries are highlighted in pink and modified entries are highlighted in purple.

12 Close the local and global key chain (Edit) forms.

Procedure 4-5 To delete a key from a local or global TCP key chain

Perform the following procedure to permanently remove a key from a local or global TCP key chain.

Caution — Deleting a TCP key can be service-affecting. Ensure that you understand the implications of deleting the key before you proceed.

Note — You cannot delete a TCP key when the Admin State parameter for the key is set to In Service.

1 Choose Administration→Security→TCP KeyChains from the 5620 SAM main menu. The TCP KeyChains form opens.

2 Perform one of the following:

- **a** Delete a key from a global key chain.
    - **i** Select Global from the Policy scope drop-down menu.
    - **ii** Configure the filter criteria and click on the Search button. A list of global key chains is displayed on the form.
- **b** Delete a key from a local key chain.
    - **i** Select Local from the Policy scope drop-down menu.
    - **ii** Click on the Select button to choose an NE. The Select a Network Element form opens.
    - **iii** Select an NE in the list and click on the OK button. The NE IP address is displayed in the Local Node IP Address field.
    - **iv** Click on the Search button. A list of key chains on the NE is displayed.

3 Select a key chain in the list and click on the Properties button. The KeyChain (Edit) form opens with the General tab displayed.

4 Click the KeyChain Key tab. The key chain keys are listed.

5 Select a key in the list and click on the Delete button. A dialog box appears.

6 Click on the OK button. The 5620 SAM deletes the key and removes it from the list.

7 Click on the OK button. A dialog box appears.

8 Click on the OK button. The KeyChain (Edit) form closes.

9 Close the TCP KeyChains form.

Procedure 4-6 To delete a local or global TCP key chain

Perform the following procedure to permanently remove a local or global TCP key chain.

Caution — Deleting a TCP key chain can be service-affecting. Ensure that you understand the implications of deleting the key chain before you proceed.

Note — You cannot delete a TCP key chain when the Admin State parameter for the key chain is set to In Service.

1 Choose Administration→Security→TCP KeyChains from the 5620 SAM main menu. The TCP KeyChains form opens.

2 Perform one of the following:

- **a** Delete a global key chain.
    - **i** Select Global from the Policy scope drop-down menu.
    - **ii** Configure the filter criteria and click on the Search button. A list of global key chains is displayed on the form.
- **b** Delete a local key chain.
    - **i** Select Local from the Policy scope drop-down menu.
    - **ii** Click on the Select button to choose an NE. The Select a Network Element form opens.
    - **iii** Select an NE in the list and click on the OK button. The NE IP address is displayed in the Local Node IP Address field.
    - **iv** Click on the Search button. A list of key chains on the NE is displayed.

3 Select a key chain in the list and click on the Delete button. A dialog box appears.

4 Click on the OK button. A dialog box appears.

5 Click on the OK button. The 5620 SAM deletes the key chain and removes it from the list.

6 Close the TCP KeyChains form.

5620 SAM Advanced configuration tasks

5 — 5620 SAM component configuration

5.1 5620 SAM component configuration overview

The 5620 SAM may require a configuration change after it is installed to meet your specific operational requirements. The procedures in this chapter change the default system-wide behavior of 5620 SAM settings or functional preferences. The procedures in this chapter describe how to perform configuration changes on the following 5620 SAM components:

- 5620 SAM software and licenses
- System components
- Network management functions
- System preferences

Note 1 — You can also change the configuration of a 5620 SAM component such as a database, server, or client using the 5620 SAM installer utility. See “Automated 5620 SAM client installation, upgrade, and configuration updates” in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for more information.

Note 2 — You can use the 5620 SAM auto-client update function to reconfigure multiple 5620 SAM clients. See “Automated 5620 SAM client installation, upgrade, and configuration updates” in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for information about using auto-client update to perform a client update. See Procedure 5-8 for information about performing global auto-client updates.

5.2 Workflow to configure 5620 SAM components

1. As required, manage the 5620 SAM software and license configuration.
    - a View information about the installed 5620 SAM software release, license capacity, and installed 5620 SAM modules. See Procedure 5-1.
    - b Export 5620 SAM license information to a file. See Procedure 5-2.
    - c Update the 5620 SAM license. For a standalone deployment, see Procedure 5-3. For a redundant deployment, see Procedure 5-4.
    - d List the backup copy of 5620 SAM license files. See Procedure 5-5.
    - e Change the default 5620 SAM license expiry notification date. See Procedure 5-6.
    - f Distribute a license key to all 7705 SAR-H nodes. See Procedure 5-7.
2. As required, configure 5620 SAM system components.
    - a Modify the base configuration of each 5620 SAM GUI client that connects to the 5620 SAM. See Procedure 5-8.
    - b Display multiple server login options on a 5620 SAM client GUI to allow you to connect to an alternate 5620 SAM server. See Procedure 5-9.

  - **c** Customize the default file location of 5620 SAM client delegate server files such as the user-defined GUI preference, script results files, and client log files. See Procedure 5-10.
  - **d** Change the IP address or hostname of a 5620 SAM main server, auxiliary server, client delegate server, or database. See Procedure 5-11.
  - **e** Enable 5620 SAM database backup file synchronization. See Procedure 5-12.
  - **f** Modify the default time period of the statistics displayed by the 5620 SAM Statistics Manager search filters. By default, the 5620 SAM Statistics Manager limits search results to statistics records collected during the past hour. See Procedure 5-13.
  - **g** Modify the default time period of the statistics displayed on the Statistics tab on object properties forms. By default, the 5620 SAM displays the statistics records collected during the past hour on the Statistics tab on the object properties form.See Procedure 5-14.

3 As required, configure 5620 SAM network management functions.

  - **a** Configure the 5620 SAM to save device configuration backups as files in addition to saving them in the database. See Procedure 5-15.
  - **b** Configure the 5620 SAM to automatically remove the configuration backup files for a device when the device is unmanaged. See Procedure 5-16.
  - **c** Configure the service CAC functionality to enable the 5620 SAM to automatically bind PBB tunnels to services based on the available bandwidth. See Procedure 5-17.
  - **d** Enable alarm reporting to identify duplicate NE system IP addresses. See Procedure 5-18.
  - **e** Enable LSP on-demand resynchronization; the 5620 SAM scheduled resynchronization is then disabled for some LSP objects.See Procedure 5-19.
  - **f** Reload the debug configuration file after an NE restarts to ensure mirror services in a managed network resume operation after a reboot or a CPM activity switch. See Procedure 5-20.
  - **g** Create a default SNMPv2 OmniSwitch user on a 5620 SAM system. See Procedure 5-23.

4 As required, customize or change the 5620 SAM system preferences default values; see Procedure 5-24.

5.3 Software and license configuration procedures

The following procedures describe how to view and modify the 5620 SAM software and license configuration.

Procedure 5-1 To view the 5620 SAM release, license, and installed module information

Perform this procedure to display information about the installed 5620 SAM software release, license capacity, and installed 5620 SAM modules.

1 To view only the GUI client information, perform the following steps.

Note — The 5620 SAM release information is also displayed on the form described in step 2.

i Choose Help→About 5620 SAM/5650 CPAM from the 5620 SAM main menu. The About the 5620 SAM/5650 CPAM Client Application form opens. The form displays the client release and patch level, and displays a padlock icon if the client communication is SSL-encrypted.

ii Close the About the 5620 SAM/5650 CPAM Client Application form.

2 To view the 5620 SAM system information, perform the following steps.

i Choose Help→5620 SAM License Information from the 5620 SAM main menu. The 5620 SAM License (Edit) form opens with the General tab displayed.

ii Review the 5620 SAM application information, which includes the following:

- release, build, and patch levels
- customer name
- license creation date
- licensed system IDs
- application key type
- maximum supported operator client positions
- maximum supported supervision module client positions
- active main server OS type
- main server IPs and hostnames
- installed 5620 SAM modules and packages

iii Click on the Devices and Quantities Licensed tab.

iv Specify a filter, if required, and click on the Search button.

v Review the device equipment information, which includes the following:

- quantity licensed
- quantity consumed
- quantity remaining
- whether the licensed quantity is exceeded

Note — You can also display equipment license information for one NE or the entire network using the 5620 SAM Equipment Manager. See the “Inventory management” chapter of the *5620 SAM User Guide* for information.

vi To view the current alarms for an entry, select the entry and click on the Properties button. The SAM Product License (View) form opens.

Note — A highlighted entry is alarmed.

vii Close the SAM Product License (View) form.

viii Close the 5620 SAM License (Edit) form.

3 To verify the contents of a 5620 SAM license file, for example, if you are unsure which file contains a specific licensed MDA quantity, perform the following steps.

i Open the license zip file on a 5620 SAM main server using the unzip utility.

Caution — A 5620 SAM license file is digitally signed. Do not rename or modify the file that the zip file contains. Otherwise, the 5620 SAM rejects the license file.

ii View the contents of the contained file.

Note — A license file does not include an object that has a licensed quantity of zero.

iii Close the license file.

iv Close the file decompression utility.

Procedure 5-2 To export 5620 SAM license information to a file

Perform this procedure to export 5620 SAM license information to a file.

1 Choose Help→5620 SAM License Information from the 5620 SAM main menu. The 5620 SAM License (Edit) form opens.

2 Click on the Export License information to file button. A Save as form opens.

3 Use the form to specify a name, location, and format for the file that is to contain the license information.

4 Click on the Save button. The license information is saved in the specified file.

5 Close the 5620 SAM License (Edit) form.

Procedure 5-3 To update the 5620 SAM license in a standalone deployment

Perform this procedure to update the current 5620 SAM license in a standalone 5620 SAM system; for example, after the purchase of additional MDA capacity.

1 Log in to the main server station as the samadmin user.

2 Open a console window.

3 Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin.

4 Enter the following to import the license:

```
bash$ ./nmsserver.bash import_license license_file ↵
```

where *license_file* is the absolute file path of the 5620 SAM license zip file from Alcatel-Lucent

The following prompt is displayed:

```
Detected a 5620 SAM license key. Do you want to proceed? (YES/no):
```

5 Enter the following:

```
YES ↵
```

The main server reads the license file, copies the license file to a backup location, and displays the following status information:

```
Importing 5620 SAM license key...

Original license key file has been backed up to
/opt/5620sam/server/timestamp/SAMLicense.zip

Done.
```

where *timestamp* is a directory name in the following format: yyyy.mm.dd-hh.mm.ss

6 Close the console window.

Verify new license information

7 Perform Procedure 5-1 to verify the imported license information.

8 If a license parameter is incorrect, contact Alcatel-Lucent technical support for assistance.

Procedure 5-4 To update the 5620 SAM license in a redundant deployment

Perform this procedure to update the 5620 SAM license in a redundant deployment with a new license, for example, after you purchase additional MDA capacity.

Note 1 — The license files that you import to the primary and standby main servers must contain identical quantity, package, and module parameters.

To reduce the risk of importing mismatched licenses, Alcatel-Lucent recommends that you obtain one license file that contains the system IDs of both main servers, and then import the same file on each main server.

Note 2 — The primary and standby main server licenses must be synchronized to ensure correct 5620 SAM operation in the event of a main server activity switch. The main servers compare license values after a system reconfiguration. If a difference is detected, the 5620 SAM generates an alarm that clears when the licenses are resynchronized.

Update license on primary main server

1 Open a client GUI to monitor the 5620 SAM during the license update.

2 Log in to the primary main server station as the samadmin user.

3 Open a console window.

4 Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin.

5 Enter the following:

```
bash$ ./nmsserver.bash import_license license_file ↵
```

where *license_file* is the absolute file path of the 5620 SAM license zip file from Alcatel-Lucent

The following prompt is displayed:

```
Detected a 5620 SAM license key. Do you want to proceed? (YES/no):
```

6 Enter the following:

```
YES ↵
```

The primary main server reads the license file, copies the license file to a backup location, and displays the following status information:

```
Importing 5620 SAM license key...

Original license key file has been backed up to
/opt/5620sam/server/timestamp/SAMLicense.zip
```

```
Done.
```

where *timestamp* is a directory name in the following format: yyyy.mm.dd-hh.mm.ss

Note — Importing the new license on the primary main server creates a license mismatch with the standby main server. As a result, the 5620 SAM generates an alarm. The alarm clears automatically after you import the new license on the standby main server, as described later in the procedure.

7 Close the console window.

Update license on standby main server

8 Log in to the standby main server station as the samadmin user.

9 Open a console window.

10 Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin.

11 Enter the following:

```
bash$ ./nmsserver.bash import_license license_file ↵
```

where *license_file* is the absolute file path of the 5620 SAM license zip file from Alcatel-Lucent

The following prompt is displayed:

```
Detected a 5620 SAM license key. Do you want to proceed? (YES/no):
```

12 Enter the following:

YES ↵

The standby main server reads the license file, copies the license file to a backup location, and displays the following status information:

```
Importing 5620 SAM license key...

Original license key file has been backed up to
/opt/5620sam/server/timestamp/SAMLicense.zip

Done.
```

where *timestamp* is a directory name in the following format: yyyy.mm.dd-hh.mm.ss

13 Ensure that the license mismatch alarm clears automatically. If it does not, contact Alcatel-Lucent technical support for assistance.

Verify new license information

14 Perform Procedure 5-1 to verify the imported license information.

15 If a license parameter is incorrect, contact Alcatel-Lucent technical support for assistance.

Procedure 5-5 To list the backed-up 5620 SAM license files

When you import a new 5620 SAM license, the 5620 SAM creates a backup copy of the existing license files. Perform this procedure to list the backup copy of 5620 SAM license files.

1 Log in to the main server station as the samadmin user.

2 Open a console window.

3 Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin.

4 Enter the following:

```
bash$ ./nmsserver.bash import_license ↵
```

The command lists the files as shown below:

```
The following backed up license key files have been detected on
the system.

/opt/5620sam/server/timestamp1/SAMLicense.zip

/opt/5620sam/server/timestamp2/SAMLicense.zip

.

.

.
```

where *timestamp1* and *timestamp2* are directory names in the following format: yyyy.mm.dd-hh.mm.ss

5 Close the console window.

Procedure 5-6 To change the default 5620 SAM license expiry notification date

The 5620 SAM raises a daily warning alarm as the expiry date of the 5620 SAM license approaches. By default, the first alarm is raised seven days before the expiry date. Perform this procedure to change the default 5620 SAM license expiry notification date.

1 Log in to the main server station as the samadmin user.

2 Navigate to the server configuration directory, typically /opt/5620sam/server/nms/config.

3 Create a backup copy of the nms-server.xml file.

4 Open the nms-server.xml file using a plain-text editor.

Caution — Contact your Alcatel-Lucent technical support representative before you attempt to modify the nms-server.xml file. Modifying the nms-server.xml file can have serious consequences that can include service disruption.

5 Locate the following XML tag in the nms-server.xml file:

```
<license
timedLicenseExpiryCount="value"
```

where *value* is the number of days prior to timed license expiry.

6 Modify the value to the required number of days to be notified before expiry.

7 Save and close the nms-server.xml file.

8 Open a console window.

9 Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin.

10 Enter the following at the prompt:

```
bash$ ./nmsserver.bash read_config ↵
```

The main server reads the nms-server.xml file and the time period is updated.

Procedure 5-7 To distribute a license key to all 7705 SAR-H nodes

The following procedure is only applicable to the 7705 SAR-H, Release 5.0.

1 Choose Administration→Security→NE Firewall→Default NE Firewall from the 5620 SAM main menu. The Firewall - Default (Edit) form opens.

2 Choose one or more system IDs from the list and click on the Distribute Key button.

3 The Distribute License Key dialog box opens.

4 Enter the license key to be distributed.

Warning — Change is applied immediately when the OK button is clicked.

5 Click on the OK button to distribute the license key to all nodes.

6 The Firewall - Default (Edit) form opens.

7 Click on the OK button to close the form.

5.4 System components configuration procedures

The following procedures describe how to configure 5620 SAM system components.

Procedure 5-8 To modify the base configuration of all 5620 SAM clients

Perform this procedure to modify the base configuration of each 5620 SAM GUI client that connects to a specific 5620 SAM main server using the auto-client update utility.

Note 1 — You can exclude a specific 5620 SAM client from a global configuration change by using a command line option when you open the client GUI.

Note 2 — Do not use this procedure to configure SSL for 5620 SAM clients. Use the appropriate SSL configuration procedures in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* to configure SSL.

1 Log in to the 5620 SAM main server station as the samadmin user.

2 Modify the appropriate client configuration file in the *install_dir*/nms/config/clientDeploy directory with the configuration change. For example, update the nms-client.xml file with a new client log location.

where *install_dir* is the server installation location, typically /opt/5620sam/server

3 Open a console window.

4 Enter the following at the prompt to enable an update notification for clients that connect to the server and to prepare the client configuration files for download.

```
bash$ install_dir/bin/nmsdeploytool.bash deploy ↵
```

where *install_dir* is the server installation location, typically /opt/5620sam/server

5 Perform one of the following on each 5620 SAM single-user GUI client station and client delegate server station.

Note — When you perform this step on a client delegate server, you affect each GUI client that connects through the client delegate server.

a Update the client configuration by restarting the client GUI. The client automatically backs up the current configuration and applies the configuration change.

Note — On a client delegate server station, you must start the client software as the root user or the configuration update fails.

A Solaris client stores the backup of the current configuration in the *install_dir*/nms/configBackup directory

where *install_dir* is the client installation location, typically /opt/5620sam/client

A Windows client stores the backup of the current configuration in the *install_dir*\nms\configBackup directory

where *install_dir* is the client installation location, typically C:\5620sam\client

b Save the current client configuration when the client GUI starts by specifying a startup option that disables the auto-client update function. See “5620 SAM GUI opening and closing procedures” in the *5620 SAM User Guide* for information about 5620 SAM client startup options.

Note — Specifying a client startup option affects only the current GUI session. To ensure that the client configuration is not updated automatically during a subsequent session, you must open the session using the startup option that disables the auto-client update.

Procedure 5-9 To configure the display of multiple 5620 SAM systems as client GUI login options

Perform this procedure to configure a client GUI login form to list multiple 5620 SAM systems as options in a drop-down menu. By default, one 5620 SAM system is listed.

Note 1 — You cannot configure a client delegate server to display multiple server options on the client login form. If you need client connections to multiple 5620 SAM servers through a client delegate server, you must install one 5620 SAM client delegate software instance for each 5620 SAM server.

Note 2 — The 5620 SAM auto-client update function overrides the nms-client.xml configuration changes that are specified in this procedure. If the nms-client.xml file on a main server changes, it overwrites the local client copy the next time the client connects to the server, unless a client startup option is used to prevent it. For information about using client startup options, see “5620 SAM GUI opening and closing procedures” in the *5620 SAM User Guide*.

Alcatel-Lucent recommends that you use the 5620 SAM auto-client update function described in chapter 5 to modify the 5620 SAM client configuration.

1 Click on Application→Exit to close the 5620 SAM client GUI, if it is open. The client GUI closes.

2 Navigate to the client configuration directory, typically /opt/5620sam/client/nms/config on Solaris and C:\5620sam\client\nms\config on Windows.

3 Open the nms-client.xml file using a text editor.

4 Find the lines starting with <j2ee> and <systemMode>. By default, the IP address and port information of the standalone or redundant servers, as configured during installation, are displayed.

5 For each standalone main server or redundant main server pair you need displayed on the client GUI login form, perform the following:

i Copy the entire <j2ee> and <systemMode> sections of the file.

ii Paste the <j2ee> and <systemMode> sections after the previous section.

iii Modify the ejbServer IP address to the IP address or hostname of the server you need displayed during client GUI login.

iv Modify the nameOne (for standalone) or nameOne and nameTwo (for redundant) parameters to indicate the domain name and hostname of the server, for easier identification by operators. This name does not have to be the hostname of the server domain. In some cases, the name may be the same for the active and standby server in a redundant server domain. The name is not automatically derived from a host lookup.

Note — Common hostname restrictions apply to the nameOne and nameTwo fields. You cannot use the following special characters:

- !
- #
- $
- %
- &
- (
-)
- +

v Save the changes and close the file.

6 Log in to the client GUI. The new server options are displayed in the Server drop-down menu.

Procedure 5-10 To change the default user file locations on a client delegate server

Perform this procedure to configure the default location of one or more of the following on a 5620 SAM client delegate server:

- user preference files that contain the following information:
    - saved table layouts
    - preferences saved using Application→User Preferences
- script result files

1 Close each 5620 SAM GUI client that connects through the client delegate server by choosing Application→Exit from the 5620 SAM main menu.

2 Log in to the client delegate server station as the samadmin user.

3 Open a console window.

4 Navigate to the client configuration directory, typically /opt/5620sam/client/nms/config.

5 Open the nms-client.xml file using a plain-text editor.

6 To change the default GUI preferences and table layout file location, insert the following line directly above the </configuration> line at the end of the file:

```
<guiPreferences path="new_file_location" />
```

where *new_file_location* is the new default GUI table layout and GUI preferences location

Note — The specified location can be an absolute file path or a file path relative to *install_dir*/nms, where *install_dir* is the client installation location, typically /opt/5620sam/client.

7 To change the default script result file location, insert the following line directly above the </configuration> line at the end of the file:

```
<cache directoryName="new_file_location" />
```

where *new_file_location* is the new default script result file location

Note — The specified location can be an absolute file path or a file path relative to *install_dir*/nms, where *install_dir* is the client installation location, typically /opt/5620sam/client.

8 Save and close the nms-client.xml file. Subsequent 5620 SAM client sessions on the client delegate server use the new file location.

Procedure 5-11 To change the IP address or hostname of a 5620 SAM main server, auxiliary server, client delegate server, or database

Changing the IP address or hostname of one or more 5620 SAM components in a standalone or redundant system may be required, for example, when the management network topology changes.

Typically, an IP address or hostname change on a 5620 SAM component requires a series of component uninstallation and re-installation activities, depending on the scope of the change. The requirements of such an operation depend on the management network topology and other considerations, so must be co-ordinated and performed only under the guidance of Alcatel-Lucent technical support.

Caution — Changing an IP address or hostname in a 5620 SAM system is a complex operation that requires careful planning and organization, and depending on the type of change required, may involve a brief network management outage. Do not attempt to modify the network configuration of a 5620 SAM component without assistance from Alcatel-Lucent technical support.

1 Collect the following information:

- the current hostname of each main server, auxiliary server, client delegate server, and database in the 5620 SAM deployment
- the current IP address of each interface that is used by the main servers, auxiliary servers, client delegate servers, and databases
- configuration information for mechanisms in the management network that affect addressing, such as NAT
- the new IP addresses and hostnames that are to be assigned to the components

2 Contact Alcatel-Lucent technical support to schedule a maintenance period for the network configuration change.

Procedure 5-12 To enable 5620 SAM database backup file synchronization

Perform this procedure to enable the main servers in a redundant 5620 SAM deployment to synchronize the database backup file sets. After a database backup, if database backup file synchronization is enabled, the 5620 SAM automatically copies the new database backup file set to the other database station.

Note 1 — This procedure applies only to redundant 5620 SAM deployments.

Note 2 — You must perform this procedure first on the standby main server station, and then on the primary main server station.

Note 3 — Before you perform this procedure, you must ensure that there is sufficient network bandwidth between the database stations for a database copy operation. See the *5620 SAM Planning Guide* for information about the bandwidth requirements of database backup file synchronization.

1 Log in to the main server station as the root user.

2 Place the 5620 SAM software DVD-ROM in a DVD-ROM drive.

3 Open a console window.

4 Perform one of the following to open the 5620 SAM server installer.

- **a** On a RHEL station:
  - **i** Enter the following:

    ```
    # cd Linux ↵
    ```

  - **ii** Enter the following:

    ```
    # ./ServerInstall_RHEL_R_r_revision.bin ↵
    ```

    where
    R_r is the release identifier, in the form *MAJOR_minor*
    revision is the revision identifier, such as R1, R3, or another descriptor

- **b** On a Solaris station:
  - **i** Enter the following:

    ```
    # cd Solarisx86 ↵
    ```

  - **ii** Enter the following:

    ```
    # ./ServerInstall_SolarisX86_SAM_R_r_revision.bin ↵
    ```

    where
    R_r is the release identifier, in the form *MAJOR_minor*
    revision is the revision identifier, such as R1, R3, or another descriptor

The 5620 SAM server configuration utility opens, and displays the Introduction panel.

5 Click on the Next button.

6 Accept the terms of the license agreement in the “Software License Agreement” panel.

7 Click on the Next button.

8 Choose Main Server Configuration in the “Choose Installation Type” panel.

9 Click on the Next button.

10 Click on the Next button in each subsequent panel until the “Standby Database Configuration” panel is displayed.

11 Select the “Enable Database Backup File Synchronization” parameter.

12 Click on the Next button.

13 Click on the Next button in each subsequent panel until the “Installation Complete” panel is displayed.

14 Click on the Done button to close the server configuration utility.

15 Enter the following to switch to the samadmin user:

```
# su - samadmin ↵
```

16 Navigate to the 5620 SAM server binary directory, typically /opt/5620sam/server/nms/bin.

17 Enter the following at the prompt:

```
bash$ ./nmsserver.bash read_config ↵
```

The 5620 SAM main server puts the configuration changes into effect. The 5620 SAM automatically copies subsequent database backup file sets from the primary database station to the standby database station.

Procedure 5-13 To modify the default time period of statistics displayed by the Statistics Manager search filters

By default, the 5620 SAM Statistics Manager limits search results to statistics records collected during the past hour. Perform this procedure to modify the default time period of the statistics displayed by the 5620 SAM Statistics Manager search filters.

Caution — Changing the default time period for the 5620 SAM Statistics Manager search filters can affect the performance of the 5620 SAM.

1 Choose Application→Exit to close the 5620 SAM client GUI, if it is open. The 5620 SAM client GUI closes.

2 Navigate to the client configuration directory, typically /opt/5620sam/client/nms/config on Solaris and C:\5620sam\client\nms\config on Windows.

3 Open the nms-client.xml file using a text editor.

4 Locate the XML tag:

```
<statistics
```

5 Edit the following line to read:

```
browserDefaultHour="value"
```

where *value* is the default number of hours for the Past <number_of_hours> filter.

6 Save the changes and close the file.

7 Open a new 5620 SAM client and login. The new value is displayed on the Statistics Manager form.

Procedure 5-14 To modify the default time period of statistics displayed on object properties forms

By default, the 5620 SAM displays the statistics records collected during the past hour on the Statistics tab on object properties forms. Perform this procedure to modify the default time period of the statistics displayed on the Statistics tab on the object properties form.

Caution — Changing the default time period for the 5620 SAM Statistics Manager search filters can affect the performance of the 5620 SAM.

1. Choose Application→Exit to close the 5620 SAM client GUI, if it is open. The 5620 SAM client GUI closes.
2. Navigate to the client configuration directory, typically /opt/5620sam/client/nms/config on Solaris and C:\5620sam\client\nms\config on Windows.
3. Open the nms-client.xml file using a text editor.
4. Locate the XML tag:

   ```
   <statistics
   ```

5. Edit the following line to read:

   ```
   tabDefaultHour="value"
   ```

   where *value* is the default number of hours for the Past <number_of_hours> filter.
6. Save the changes and close the file.
7. Open a new 5620 SAM client and login. The new value is displayed on the Statistics tab of the object properties form.

5.5 Network management configuration procedures

The following procedures describe how to configure system-wide 5620 SAM network management functions.

Procedure 5-15 To configure the 5620 SAM to save device configuration backups on a file system

Perform this procedure to configure the 5620 SAM to save device configuration backups as files in addition to saving them in the database. By default, the 5620 SAM saves device configuration backups only in the 5620 SAM database.

Note — The samadmin user requires read and write permissions to each directory specified in this procedure.

1 Log in to the 5620 SAM main server station as the samadmin user.

2 Navigate to the 5620 SAM server configuration directory, typically /opt/5620sam/server/nms/config.

3 Create a backup copy of the nms-server.xml file.

4 Open the nms-server.xml file using a plain-text editor.

Caution — Contact your Alcatel-Lucent technical support representative before you attempt to modify the nms-server.xml file. Modifying the nms-server.xml file can have serious consequences that can include service disruption.

5 Locate the following XML tag, which marks the beginning of the section that you need to configure:

```
<device_typebackup
```

where *device_type* is one of the following:

Ran—for RAN devices such as the eNodeB

AosSr—for OmniSwitch devices

MPRSr—for 9500 MPR devices

sr—for all other devices, such as the 7450 ESS, 7710 SR, 7750 SR, and 7950 XRS

The same *device_type* identifier is used in the following steps.

6 To enable the storage of device backups on the main server file system, configure the following parameter by inserting the storage location between the quotation marks:

```
device_typeBackupDirectory="location"
```

where *location* is an absolute or relative file path

Note — A relative file path that you specify in this step is relative to the *installation_directory*/nms/bin directory on the 5620 SAM main server.

7. If required, configure the following parameters by changing the value between the quotation marks:

   Note — The default value for each parameter is shown in this step.

   ```
   diskUsageThreshold="80"

   maxNumberOfFiles="5000"

   purgeDiskUsageThreshold="95"

   saveLatestOnly="true"

   device_typeBackupSyncEnabled="false"

   device_typeBackupSyncInterval="30"
   ```

   The following are the parameter descriptions:

   - diskUsageThreshold—The percentage of disk usage above which the 5620 SAM raises a major alarm. When the disk usage falls below this value, the alarm clears. The range is 0 to 95; the default is 80. A value of 0 means that the disk usage is not monitored.
   - maxNumberOfFiles—The maximum number of backup files for this device type that are saved on the file system. When this value is exceeded, the 5620 SAM deletes the oldest backup files. The range is 0 to 100 000; the default is 5000. A value of 0 means that no limit is enforced.
   - purgeDiskUsageThreshold—The percentage of disk usage above which the 5620 SAM deletes the oldest backup files and raises a major alarm. The files are deleted until the disk usage falls below the percentage specified by diskUsageThreshold. A value of 0 means that no file deletion occurs and, accordingly, no alarm is raised. The range is 0 to 95; the default is 95.
   - saveLatestOnly—If set to true, specifies that only the latest device backup is saved. If set to false, specifies that device backups are saved according to the constraints specified by the diskUsageThreshold, maxNumberOfFiles, and purgeDiskUsageThreshold parameters.
   - *device_type*BackupSyncEnabled—If set to true, specifies that the 5620 SAM synchronizes the backup files between the primary and standby main servers.
   - *device_type*BackupSyncInterval—If *device_type*BackupSyncEnabled is set to true, specifies how often, in minutes, the 5620 SAM synchronizes the files.

8. To disable the storage of device backups on the main server file system, configure the following parameter by removing the storage location between the quotation marks, as shown in the following example:

   ```
   device_typeBackupDirectory=""
   ```

9. Perform steps 5 to 8 to configure the storage of device backups for another device type, if required.

10. Save and close the nms-server.xml file.

11. Open a console window.

12 Navigate to the 5620 SAM server binary directory, typically /opt/5620sam/server/nms/bin.

13 Enter the following at the prompt:

```
bash$ ./nmsserver.bash read_config ↵
```

The 5620 SAM main server reads the nms-server.xml file and puts the configuration changes into effect. Subsequent device configuration backups are saved to the path specified in the nms-server.xml file.

The 5620 SAM saves the device backup files in the following directory under the location specified in step 5:

samNodeBackup/*device_ID*/*timestamp*

where
device_ID is the unique identifier of a device
timestamp is the time of the backup

Procedure 5-16 To configure automatic device configuration backup file removal

Perform this procedure to configure the 5620 SAM to automatically remove the configuration backup files for a device when the device is unmanaged.

Caution — This procedure requires a restart of the 5620 SAM server, which is service-affecting.

Note — This procedure configures the removal of backup files only; device configuration backups in the database are retained.

1 Navigate to the 5620 SAM server configuration directory, typically /opt/5620sam/server/nms/config.

2 Create a backup copy of the nms-server.xml file.

3 Open the nms-server.xml file using a plain-text editor.

Caution — Contact your Alcatel-Lucent technical support representative before you attempt to modify the nms-server.xml file. Modifying the nms-server.xml file can have serious consequences that can include service disruption.

4 Search for the following XML tag:

```
</configuration>
```

5 Enter the following line above the </configuration> tag:

```
<nodeBackups removeBackupOnDelete="true"/>
```

6 Save and close the nms-server.xml file.

7 Open a console window.

8 Navigate to the 5620 SAM server binary directory, typically /opt/5620sam/server/nms/bin.

9 Enter the following at the console prompt to restart the 5620 SAM server:

```
bash$ ./nmsserver.bash force_restart ↵
```

Caution — Restarting a 5620 SAM server is service-affecting. Ensure that you perform this step only during a scheduled maintenance window.

10 The 5620 SAM main server restarts. The 5620 SAM deletes the configuration backup files of NEs that are subsequently unmanaged.

Procedure 5-17 To configure service CAC to automatically bind PBB tunnels

Perform this procedure to configure the service CAC functionality to enable the 5620 SAM to automatically bind PBB tunnels to services based on the available bandwidth.

Note 1 — This feature has limited availability. Contact your Alcatel-Lucent technical support representative for information about the availability of this feature.

Note 2 — You must perform this procedure on each main server in a 5620 SAM system.

1 Close each 5620 SAM client that connects to the main server through the client delegate server, by choosing Application→Exit from the 5620 SAM main menu.

2 Use an OS utility to change the IP address of the client delegate server station to the new value.

3 Log in to the main server station as the samadmin user.

4 Open a console window.

5 Navigate to the server configuration directory, typically /opt/5620sam/server/nms/config.

6 Open the nms-server.xml file using a plain-text editor.

Caution — Contact your Alcatel-Lucent technical support representative before you attempt to modify the nms-server.xml file. Modifying the nms-server.xml file can have serious consequences that can include service disruption.

7 Locate the following XML tag:

```
<require-CAC
```

The service CAC section should read as follows:

```
<require-CAC

        enabled="false"

        defaultBWThreshold="90"

        linkTunnelCacheMaxSize="1000"

        tunnelServiceCacheMaxSize="10000"

        serviceBWCacheMaxSize="50000"

    />
```

8 Change enabled="false" to enabled="true".

9 Save and close the nms-server.xml file.

10 Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin.

11 Enter the following at the prompt:

```
bash$ ./nmsserver.bash read_config ↵
```

The main server reads the nms-server.xml file and enables the server CAC features on the client delegate server.

Procedure 5-18 To enable alarm reporting to identify duplicate NE system IP addresses

Perform this procedure to enable the 5620 SAM to verify the uniqueness of NE system IP addresses. When verification is enabled, the 5620 SAM generates an alarm when an NE reports a system IP address that is in use by another NE.

1 Log in to the main server station as the samadmin user.

2 Open a console window.

3 Navigate to the server configuration directory, typically /opt/5620sam/server/nms/config.

4 Open the nms-server.xml file using a plain-text editor.

Caution — Contact your Alcatel-Lucent technical support representative before you attempt to modify the nms-server.xml file. Modifying the nms-server.xml file can have serious consequences that can include service disruption.

5 Locate the following tag that marks the beginning of the SNMP section:

```
<snmp
```

6 Add the following before the end of the SNMP section, ensuring that there is a space between the last character and the section end, which is marked by a /> tag:

```
verifyNodeIdentity=”1"
```

7 Save and close the nms-server.xml file.

8 Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin.

9 Enter the following at the prompt:

```
bash$ ./nmsserver.bash read_config ↵
```

The main server reads the nms-server.xml file and alarm reporting for duplicate NE system IP addresses is enabled.

Procedure 5-19 To enable LSP on-demand resynchronization

Perform this procedure to enable LSP on-demand resynchronization. The 5620 SAM scheduled resynchronization is then disabled for some LSP objects. See “LSP on-demand resynchronization” in the *5620 SAM User Guide* for information about which LSP objects do not support on-demand resynchronization.

Caution — Modify only the parameters specified in this procedure. Unauthorized modification of the nms-server.xml file can seriously affect network management and 5620 SAM performance.

1 Log in to the main server station as the samadmin user.

2 Navigate to the server configuration directory, typically /opt/5620sam/server/nms/config.

3 Create a backup copy of the nms-server.xml file.

4 Open the nms-server.xml file using a plain-text editor.

5 Locate the following line:

```
 <lspOnDemand overrideEnabled="false" />
```

6 Change "false" to "true".

7 Save and close the nms-server.xml file.

8 Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin.

9 Enter the following at the prompt:

```
bash$ ./nmsserver.bash read_config ↵
```

The main server reads the nms-server.xml file and LSP on-demand resynchronization is enabled.

Procedure 5-20 To enable debug configuration file reloading on an NE for mirror services

Perform this procedure to ensure that managed NEs reload the debug configuration file after an NE restarts. This ensures that the mirror services in the managed network resume operation after a reboot or a CPM activity switch on the NE that hosts the mirror service. By default, debug configuration file reloading is disabled.

Caution — This procedure requires a 5620 SAM main server restart, which is service-affecting.

1 Log in to the main server station as the samadmin user.

2 Open a console window.

3 Navigate to the server configuration directory, typically /opt/5620sam/server/nms/config.

4 Open the nms-server.xml file using a plain-text editor.

Caution — Contact your Alcatel-Lucent technical support representative before you attempt to modify the nms-server.xml file. Modifying the nms-server.xml file can have serious consequences that can include service disruption.

5 Locate the following XML tag:

```
<serviceMirror
```

6 Specify the NE location of the debug configuration file. For example:

```
 <serviceMirror
debugFilename=""
reloadDelay="10"
/>
```

where

reloadDelay specifies the time, in seconds, to wait before a reload request is sent

debugFilename specifies the location of the file on an NE, for example, cf3:/ServiceMirror.dbg

Note — The debugFilename value must be the debug configuration filename that is configured on the NEs that host mirror services.

7 Save and close the nms-server.xml file.

8 Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin.

9 Enter the following at the prompt to restart the main server:

```
bash$ ./nmsserver.bash force_restart ↵
```

Caution — Restarting a 5620 SAM main server is service-affecting. Ensure that you perform this step only during a scheduled maintenance window.

The main server restarts.

10 If required, create a device backup policy to ensure that device configurations are not lost in the event of an NE failure.

Procedure 5-21 To configure throttle rates for subscriber trap events

Perform this procedure to configure throttle rates for residential subscriber create and delete event traps on the 7750 SR. The throttle rate defines the number of events that can be received during a specified interval before the NE stops sending individual traps.

1 Choose Equipment from the network navigation tree view selector. The network navigation tree displays the Equipment view.

2 Right-click on the NE for which you want to configure trap event throttle rates and choose Properties from the contextual menu. The Network Element (Edit) form opens with the General tab displayed.

3 Click on the Event Throttling button. The ESM Event Throttle form opens.

4 Disable the Default check box.

5 Configure the parameters:

- Interval (seconds)
- Limit

6 Click on the Execute button. The Detailed Status/Error message field displays status information about the throttle rate change.

7 Close the ESM Event Throttle form.

8 Close the Network Element (Edit) form.

Procedure 5-22 To configure the windowing trap delayer option for subscriber table resyncs

Perform this procedure to configure the windowing trap delayer option, which provides an enhanced method to resync the subscriber table in the event of a trap drop from an NE.

Configurable hold-off options prevent subscriber table resyncs for a minimum specified duration after a trap drop is received from the NE, and until a specified time window has elapsed with no additional trap drops received from the NE. Additionally, a maximum hold-off time is specified to prevent excessive periods during which the 5620 SAM is out of sync with the NE. The windowing trap delayer configuration reduces the number of subscriber table resync events while providing a reasonable in-sync state with the NE.

The windowing trap delayer option is configured in nms-server.xml file. It only affects tmnxTrapDropped traps which are related to tmnxSubscriberCreated, tmnxSubscriberDeleted or tmnxSubscriberRenamed traps. When the windowing trap delayer option is disabled, tmnxTrapDropped traps are delayed using the default trap delayer function.

1 Log in to the main server station as the samadmin user.

2 Navigate to the server configuration directory, typically /opt/5620sam/server/nms/config.

3 Create a backup copy of the nms-server.xml file.

4 Open the nms-server.xml file using a text editor.

Caution — Contact your Alcatel-Lucent technical support representative before you attempt to modify the nms-server.xml file. Modifying the nms-server.xml file can have serious consequences that can include service disruption.

5 Locate the following XML tag:

```
<snmp
```

This section of the file contains the 5620 SAM SNMP information.

6 Add the following before the end of the SNMP section, ensuring that there is a space between the last character and the section end, which is marked by a /> tag:

```
    <windowingTrapDelayer enabled="true" checkInterval="10"
windowLength="30" maxHoldOff="60"/>

 /snmp>
```

where *windowingTrapDelayer enabled* (boolean) sets the windowing trap delayer option as enabled or disabled. The default is true.

checkInterval is the minimum interval after a trap drop is recieved, during which subscriber table resyncs are prevented. The range is 5 to 30 seconds. The default is 10 seconds.

windowLength is a sliding time interval after a trap drop is recieved, during which no additional trap drops can be recieved before subscriber table resyncs are allowed. The range is 5 to 60 seconds. The default is 30 seconds.

maxHoldOff is the absolute maximum hold-off time, after which subscriber table resyncs are allowed. The range is 5 to 1800 seconds. The default is 60 seconds.

The checkInterval value must be less than the windowLength value, which must be less than the maxHoldOff value.

7 Save and close the nms-server.xml file.

8 Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin.

9 Execute the following command at the prompt:

```
bash$ ./nmsserver.bash read_config ↵
```

The main server reads the nms-server.xml file and the window trap delayer function is enabled.

Procedure 5-23 To create a default SNMPv2 OmniSwitch user on a 5620 SAM system

Perform this procedure to create a default SNMPv2 OmniSwitch user on a 5620 SAM system.

Caution — Modify only the parameters specified in this procedure. Unauthorized modification of the nms-server.xml file can seriously affect network management and 5620 SAM performance.

1 Log in to the main server station as the samadmin user.

2 Navigate to the server configuration directory, typically /opt/5620sam/server/nms/config.

3 Create a backup copy of the nms-server.xml file.

4 Open the nms-server.xml file using a plain-text editor.

5 Locate the following XML tag:

```
<snmp
```

This section of the file contains the 5620 SAM SNMP information.

6 Add the following before the end of the SNMP section, ensuring that there is a space between the last character and the section end, which is marked by a /> tag:

```
snmpV2UserName=”user_name”
```

where *user_name* is a user name that is configured on the switch

The SNMP section should read as follows:

```
<snmp
            ip="server_IP_address"
            port="port_number"
            trapLogId="log_ID"
            snmpV2UserName="user_name" />
```

7 Save and close the nms-server.xml file.

8 Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin.

9 Execute the following command at the prompt:

```
bash$ ./nmsserver.bash read_config ↵
```

The main server reads the nms-server.xml file and the new SNMPv2 user name is enabled.

5.6 System preferences configuration procedures

The following procedures describe how to configure 5620 SAM system preferences that affects the system-wide behaviour of various global settings and functions.

Procedure 5-24 To configure 5620 SAM system preferences

Perform this procedure to customize or change the default value of 5620 SAM system preferences to meet your specific operational requirements.

Caution — Changing a system preference parameter value may adversely affect the 5620 SAM service or function. Do not change the parameter value from the default without contacting Alcatel-Lucent technical support.

Note — You need a user account with the Administrator scope of command role to perform this procedure.

1 Choose Administration→System preferences from the 5620 SAM main menu. The system preferences form opens with the services tab displayed.

Table 5-1 lists the settings and functions that can be configured using the system preferences form and the location of additional information if applicable. System preferences are listed by the functional tabs they appear on the system preferences form.

Table 5-1 System preference functions or settings

Function or setting	Additionally see
General tab	
To configure the system preferences for custom tab display on configuration forms.	*5620 SAM User Guide*
To configure the Save to File option to export CSV files using UTF-8 with BOM (byte order mark) encoding.	*5620 SAM User Guide*
Services tab	
To configure the system preferences of services associated with a customer such as specifying the default service priority or the automatic removal of empty services.	—
To perform a service size reduction associated with a customer by moving sites from one service to another.	*5620 SAM User Guide*
To configure the default system preferences for composite services such as specifying if they are auto discovered or if service alarms are aggregated for them.	—
TCA tab	
To configure the system preferences associated with TCA policies such as specifying the default TCA alarm severity or the maximum TCA alarm limit.	—
Statistic tab	
To configure the system preferences associated with exported statistics files on a 5620 SAM server such as the default log file retention time (applies to accounting and performance statistics) or log file rollover time (applies to performance statistics).	*5620 SAM Statistics Management Guide*
To configure the system preferences associated with exported statistics files on a 5620 SAM server to specify the default number of JMS client connection checks that are performed before the auto-deregistration of the registerLogToFile. This applies to accounting and performance statistics.	*5620 SAM XML OSS Interface Developer Guide*
Test Manager tab	
To configure the system preferences associated with the STM such as the default retention time for db test results and log file.	*5620 SAM User Guide*

(1 of 3)

Function or setting	Additionally see
User Activity tab	
To configure the system preferences associated with user activity such as how much user activity log information is stored in the 5620 SAM db before it purges information and the retention period.	—
OLC tab	
To configure the default OLC state when shutting down or turning up an object in the system preference form. You can also configure OLC scheduling. Additionally, the following applies to this system preference configuration: • If the Enable Automatic OLC State change parameter is enabled in the System Preferences form, a Shut Down action will set the object's state to Maintenance and a Turn Up action will set the object's state to In Service. This state change is also applied to any child objects. • The Enable Automatic OLC State change parameter applies only to objects which support the OLC state. It does not apply to routing objects.	—
Policies tab	
To enable access ingress and access egress policy names, and ACL IP, ACL IPv6, and ACL MAC policy filter names to be displayed on the policy configuration form.	*5620 SAM User Guide*
To enable a restriction in the distribution mode for certain types of local policies that will permit local editing only. Additionally, the following applies to this system preference configuration: • Policy types supported by this system preference include Access Ingress, Access Egress, Network QoS, ACL MAC, ACL IPv4, and ACL IPv6. • When creating any of these policies, if you set the Scope parameter to exclusive, the 5620 SAM will set the distribution mode to local edit. • The 5620 SAM will not allow policies with the Scope parameter set to exclusive to be assigned or used more than once. • If you attempt to set the Policy Distribution Mode to Sync With Global while the Scope attribute is configured as exclusive, an error message will be displayed.	*5620 SAM User Guide*
To enable a policy change made using CLI to switch the distribution mode for certain types of local policies to Local Edit Only, as opposed to the default Sync with Global mode.	*5620 SAM User Guide* *5620 SAM Parameter Guide*
To allow for the automatic distribution of a global policy to applicable NEs once the policy is released.	*5620 SAM User Guide*
To configure the maximum number of scheduled audit results stored for a local policy.	*5620 SAM User Guide*
To enable all zones resynchronized from the node as local edit only. If you disable the Discover Security Zone in Local Edit Only parameter, all zones resynchronized from the node are set to Sync With Global. • The Discover Security Zone in Local Edit Only parameter is only supported on the 7705 SAR-8 with CSMv2, 7705 SAR-8v2 with CSMv2, 7705 SAR-18, 7705 SAR-H, 7705 SAR-Hc, and 7705 SAR-Wx variants, Release 6.1 R1 or later.	*5620 SAM User Guide*
Custom NE Properties tab	

(2 of 3)

Function or setting	**Additionally see**
To configure custom property labels and values on an NE, for example, the location and site name that differs from the actual NE site name. These properties cannot be configured on the NE. Additionally, the following applies to this system preference configuration: • If custom property labels are not configured, the default labels are used. • NE custom properties support the extended character set including multi-byte characters. • Custom property labels and values are displayed in the following locations: • NE Properties form • NE List form	—

(3 of 3)

2 Configure the required parameters. See the *5620 SAM Parameter Guide* for a description of system preference parameters or use on-line parameter search tool.

3 As required, click on the appropriate tab to configure another system preference.

4 Click on the OK button. A dialog box appears.

5 Click on the Yes button. The System Preferences form closes.

6 — 5620 SAM system redundancy

6.1 5620 SAM system redundancy overview

5620 SAM system redundancy is initially configured during 5620 SAM installation. You use the 5620 SAM GUI, or scripts on a 5620 SAM main server, to perform the following redundancy functions:

- Check the 5620 SAM redundant server and database status.
- Perform a manual activity switch from the primary to the standby main server.
- Enable or disable automatic database realignment.
- Reinstantiate the former primary database as the standby database when an automatic or manual activity switch occurs and verify its status.

You can configure the following redundancy parameters to specify how a 5620 SAM system manages a loss of connection to the managed NEs; contact Alcatel-Lucent technical support for more information:

- the number of elapsed seconds that constitute a loss of connectivity
- how often a main server refreshes the list of managed NEs
- the minimum number of NEs that must respond to a connectivity check

6.2 5620 SAM system redundancy models

You can deploy a 5620 SAM system in a redundant configuration to provide greater fault tolerance by ensuring that there is no single point of software failure in the 5620 SAM management network. A redundant 5620 SAM deployment consists of the following components:

- primary and standby 5620 SAM main servers
- primary and standby 5620 SAM databases

Caution — For increased 5620 SAM system performance and fault tolerance, Alcatel-Lucent recommends that you deploy the primary server and database in the same geographical location and LAN.

The current state of a component defines the primary or standby role of the component. The primary main server actively manages the network and the primary database is open in read/write mode. When a standby component detects a primary component failure, it automatically changes roles from standby to primary. You can also change the role of a component using the 5620 SAM client GUI or a CLI script.

The 5620 SAM supports collocated and distributed system redundancy. A collocated system requires two stations that each host a main server and database. A distributed system requires four stations that each host a main server or database. Each main server and database is logically independent, regardless of the deployment type.

The primary and standby main servers communicate with the redundant databases and periodically verify server redundancy. If the standby server fails to reach the primary server within 60s, the standby server becomes a primary server. See section 6.4 for information about various 5620 SAM redundancy failure scenarios.

A 5620 SAM database uses the Oracle DataGuard function to maintain redundancy. During a redundant 5620 SAM installation or upgrade, the Oracle DataGuard synchronization level is set to real-time apply, which ensures that the primary and standby databases are synchronized.

Figure 6-1 shows a collocated redundant 5620 SAM deployment.

Figure 6-1 Collocated redundant 5620 SAM deployment

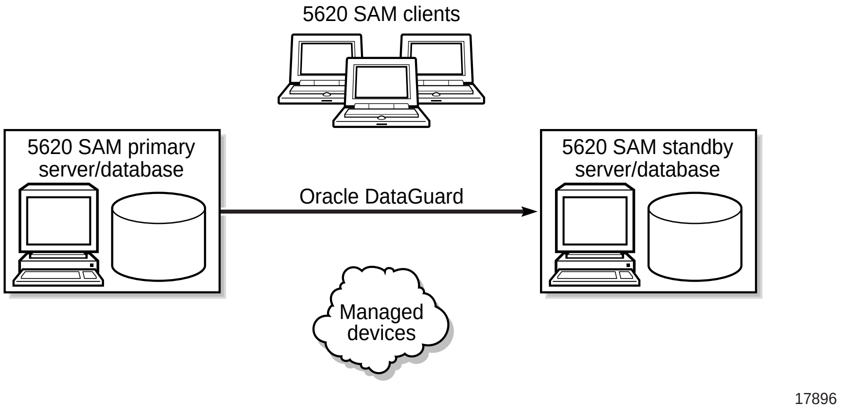
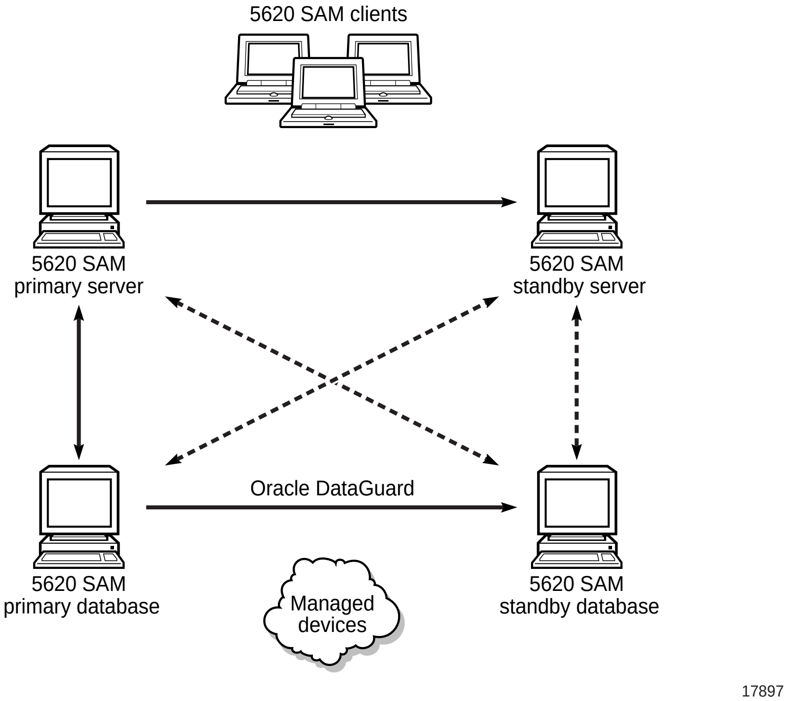

5620 SAM clients
5620 SAM primary server/database
Oracle DataGuard
5620 SAM standby server/database
Managed devices
17896

Figure 6-2 shows a distributed redundant 5620 SAM deployment.

Figure 6-2 Distributed redundant 5620 SAM deployment



A main server role change is called a server activity switch. An automatic database role change is called a failover; a manual database role change is called a switchover.

A typical redundant 5620 SAM deployment has a primary server and database in a geographically separate facility from the standby server and database facility. To ensure that the primary components are in the same LAN after an activity switch or failover, you can configure automatic database realignment during a main server installation or upgrade. See "Automatic database realignment" for more information.

The 5620 SAM GUI clients always communicate with the current primary server. After a server activity switch, the GUI clients automatically connect to the new primary server, which is the former standby server. The 5620 SAM OSS clients also communicate with the current primary server, but after a server activity switch, the OSS clients do not automatically connect to the new primary server.

The following general conditions apply to 5620 SAM system redundancy:

- The main servers and databases must each be redundant. For example, you cannot have redundant servers and a standalone database.
- The network that contains a redundant 5620 SAM system must meet the latency and bandwidth requirements described in the *5620 SAM Planning Guide*.

  Note — To provide hardware fault tolerance in addition to software redundancy, Alcatel-Lucent recommends using redundant physical links between the primary and standby servers and databases to ensure there is no single point of network or hardware failure.

- The server and database stations require the same OS version and patch level.
- The server stations require identical disk layouts and partitioning.
- The database stations require identical disk layouts and partitioning.
- The following users can perform manual server activity switches or database switchovers:
  - the samadmin user on a main server station
  - a client GUI user with update or execute permissions on the following classes:
    db.DatabaseManager.switchover
    db.DatabaseManager.reinstantiateStandby
  - a GUI client user with the admin scope of command role

Auxiliary server redundancy

5620 SAM auxiliary servers are optional servers that extend the network management processing engine by distributing server functions, for example, statistics collection, among multiple stations in a 5620 SAM domain. Each auxiliary server is installed on a separate station in a 5620 SAM server cluster. An auxiliary server communicates only with the primary main server and database. Main and auxiliary servers open sessions only on the primary database.

A 5620 SAM main server controls task scheduling and sends task requests to auxiliary servers. When a Preferred auxiliary server is unresponsive, the main server directs the requests to a Reserved auxiliary server. If a Preferred auxiliary server returns to service after a failure, the main server reverts to using the Preferred auxiliary server and stops using the Reserved auxiliary server. The Preferred or Reserved role of an auxiliary server is specified during a main server installation.

When an auxiliary server cannot connect to the primary main server or database, it re-initializes and continues trying to connect until it succeeds or, in the case of a database failover, until the main server directs it to the peer database.

An auxiliary server does not cause, perform, or initiate redundancy activities such as failovers; only a main server controls auxiliary server redundancy functions and decides which auxiliary servers to use after a failure.

After startup, an auxiliary server waits for initialization information from a main server. An auxiliary server restarts if it does not receive all required initialization information within five minutes.

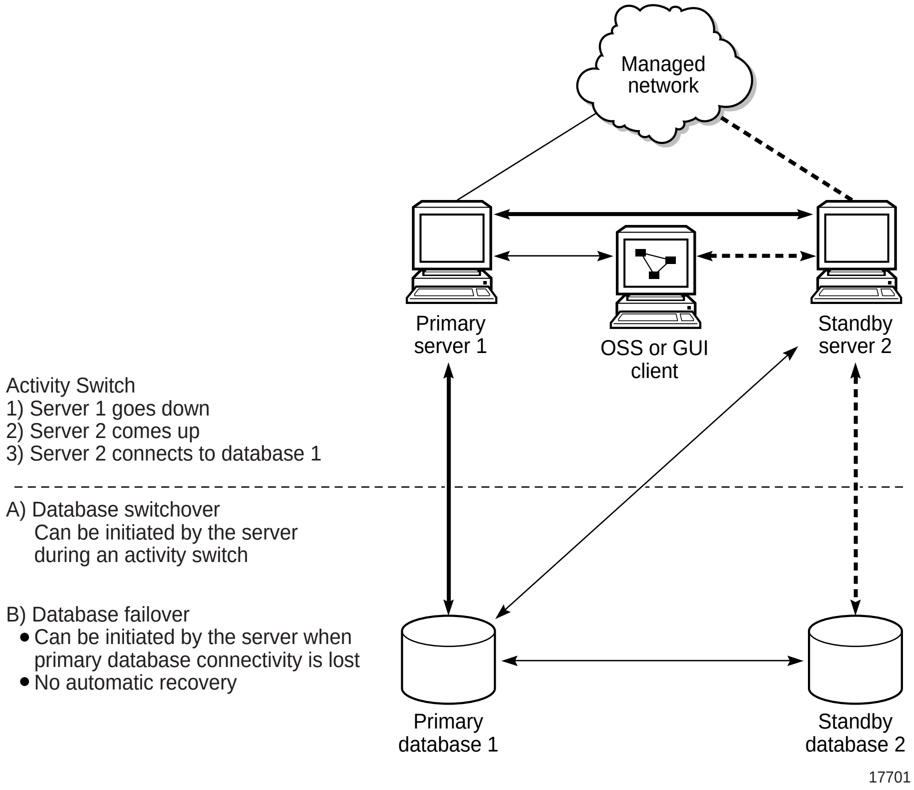
Note — 5620 SAM system performance may degrade when a main server loses contact with a number of auxiliary servers that exceeds the number of Preferred auxiliary servers in the server cluster.

When an auxiliary server fails to respond to a primary main server, the main server tries repeatedly to establish communication before it generates an alarm. The alarm clears when the two servers re-establish communication.

6.3 Redundancy functions

Figure 6-3 shows the 5620 SAM system redundancy role-change functions.

Figure 6-3 5620 SAM redundancy role-change functions

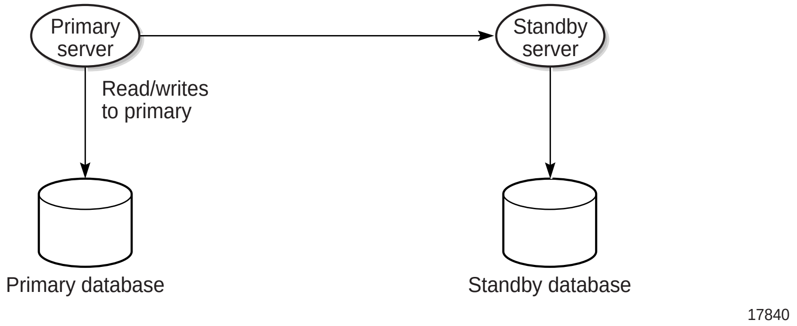


Server activity switches

The standby server initiates an automatic server activity switch when it cannot communicate with the primary server. A 5620 SAM administrator performs a manual server activity switch, which is typically a planned server maintenance or test operation. For security reasons, you cannot use a 5620 SAM GUI or OSS client to perform a server activity switch.

Figure 6-4 shows the server and database roles before an activity switch.

Figure 6-4 Server and database roles before server activity switch



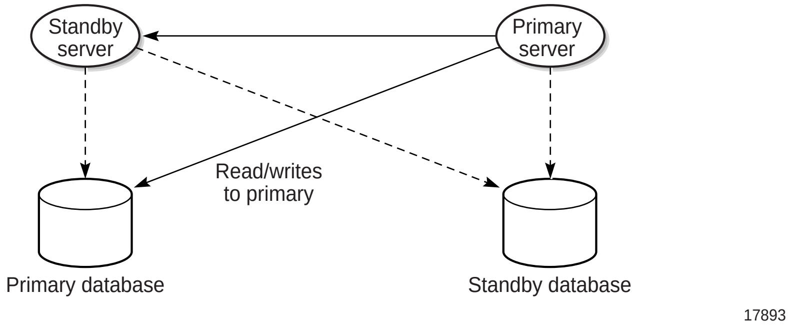
During a server activity switch, a main server does not process SNMP traps, attempt to synchronize NEs, or collect statistics. Auxiliary servers process outstanding requests during an activity switch, but do not communicate with a main server.

The following occurs during a server activity switch:

- The primary server raises alarms about the event.
- Each GUI client receives notification of the activity switch and displays a message about the server unavailability during the activity switch.

Figure 6-5 shows the server and database roles after a successful activity switch.

Figure 6-5 Server and database roles after server activity switch



The following occur after a server activity switch:

- If automatic database realignment is enabled, the new primary server performs a database switchover.
- The GUI clients communicate with the new primary server and display the current redundancy status.
- The OSS clients must connect to the new primary server.
- The new primary server establishes communication and synchronizes information with the 5620 SAM auxiliary servers.
- The auxiliary servers exchange information with the new primary server; no auxiliary servers exchange information with the former primary server.
- The Preferred or Reserved state of each auxiliary server changes, depending on the configuration of the new primary server.
- The new primary server attempts to redeploy the client requests that the former primary server did not complete before the activity switch.

Database switchovers

A 5620 SAM administrator directs a main server to initiate a database switchover. Figure 6-6 shows the main server and database roles before a database switchover.

Figure 6-6 Server and database roles before database switchover

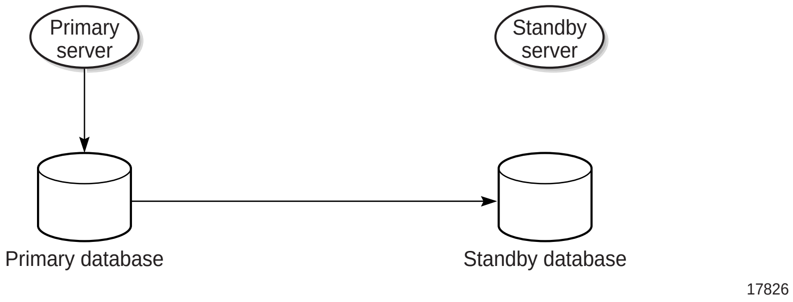
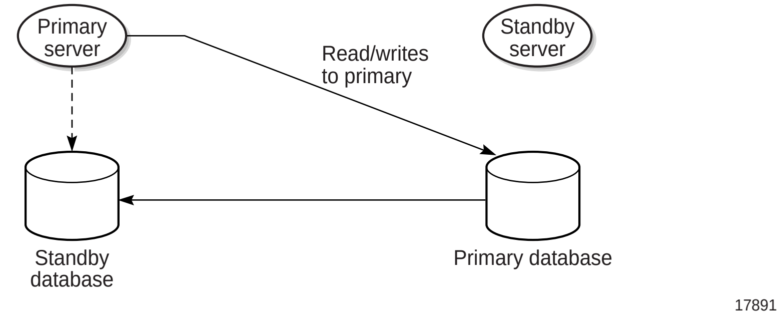


Figure 6-7 shows the server and database roles after a database switchover.

Figure 6-7 Server and database roles after database switchover



The following occurs after a successful database switchover:

- The primary server connects to the new primary database.
- Archive logging begins on the new primary database.
- The primary server directs each auxiliary server to use the new primary database.

When a database switchover fails, the primary and standby database roles do not change. No automatic database realignment occurs as a result of a switchover.

Database failovers

The 5620 SAM database failover function is enabled by default. A failover occurs when a main server cannot communicate with the primary database, but can communicate with the standby database and the managed NEs. When this happens, the main server directs the standby database to become the primary database.

A database failover occurs only if the following conditions are true.

- The standby database is configured, operational, and reachable.
- The main server can communicate with the managed NEs.

Figure 6-8 shows the server and database roles before a failover.

Figure 6-8 Server and database roles before database failover

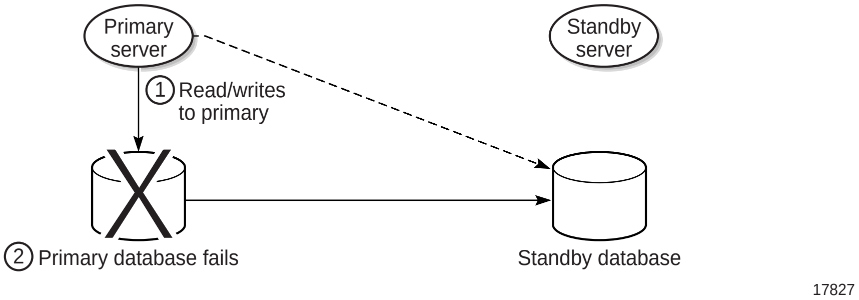
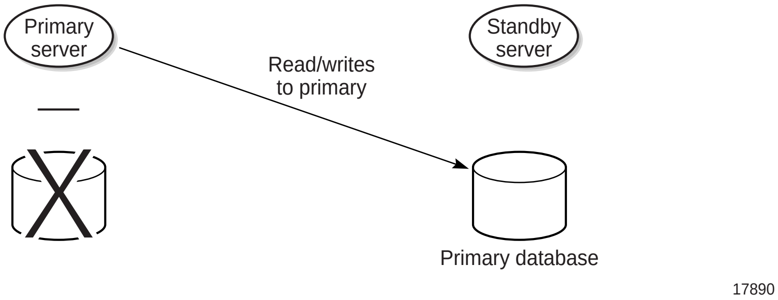


Figure 6-9 shows the server and database roles after a successful failover.

Figure 6-9 Server and database roles after database failover



When a database failover fails, the primary server tries again to communicate with the primary database. If the primary database remains unavailable, the primary server tries again to initiate a failover.

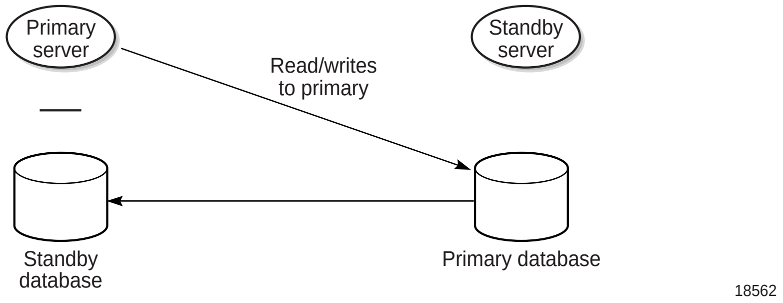
Note — After a successful failover, database redundancy is not available. See "Re-establishing database redundancy" in this section.

Re-establishing database redundancy

After a failover, the former primary database is no longer part of the redundant configuration. To re-establish database redundancy, you must reinstantiate the former primary database as the new standby database. You can do this only when the failed database station is restored to full operation and has a functional proxy port. See Procedures 6-8 and 6-9 for information about how to reinstantiate a database.

Figure 6-10 shows a former primary database serving as the new standby database.

Figure 6-10 Server and database roles after database reinstantiation



Automatic database reinstantiation

You can configure the 5620 SAM to automatically reinstantiate the former primary database as the new standby database. Automatic database reinstantiation occurs only in the event of a database failover. When the function is enabled, the 5620 SAM attempts an automatic reinstantiation every 60 minutes by default. You can enable automatic database reinstantiation during a 5620 SAM main server installation or upgrade. See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for information about enabling and configuring automatic database reinstantiation.

Automatic database realignment

In a redundant 5620 SAM system that is geographically dispersed, the primary server and database may be in separate LANs or WANs after an activity switch or failover. The network latency that this introduces can affect 5620 SAM system performance. Automatic database realignment is an optional mechanism that attempts to ensure that each main server uses the local database.

The database with which a main server tries to align itself is called the preferred database of the main server. An operator enables automatic database realignment and specifies the preferred database during 5620 SAM server installation, or during server configuration after installation.

Note — For automatic database alignment to work, you must enable it and specify a preferred database on each main server in a redundant 5620 SAM system.

When a primary server starts, it verifies that the primary database is the preferred database. If the primary database is not the preferred database, the server performs a database switchover to reverse the primary and standby database roles. If the switchover is successful, the main servers and databases in the 5620 SAM system are aligned. If the switchover fails, each database reverts to the former role, and the main server generates an alarm about the failed switchover.

When you perform a database switchover and automatic database realignment is enabled, the primary server does not attempt database realignment. A switchover is a manual operation that is considered to be a purposeful act.

Performing a server activity switch when automatic database realignment is enabled triggers a database switchover.

Redundancy function summary

Table 6-1 summarizes the 5620 SAM main server redundancy functions.

Table 6-1 5620 SAM server redundancy functions

Function	Notes
Automatic server activity switch An automatic activity switch occurs when the primary server cannot communicate with the standby server, and involves the following sequence of events. • The standby server cannot communicate with the primary server within 60 seconds, or the primary server cannot communicate with the managed network. • The standby server performs an activity switch to become the new primary server. The activity switch occurs only if the standby server can communicate with the managed network. • If automatic database realignment is enabled, the new primary server attempts a database switchover. • The new primary server connects to the primary database and manages the network. • The new primary server and the auxiliary servers synchronize the outstanding request information.	When the primary server detects a standby server communication failure, each GUI client receives notification of the failure. During an activity switch, each client GUI displays a main server status message. During an activity switch, a main server does not process SNMP traps from the network, and no NE resynchronizations occur. The auxiliary servers continue to process outstanding requests, and synchronize the request information with the new primary server after the activity switch. When the communication failure is resolved, each GUI client receives notification that redundancy is restored.
Manual server activity switch A manual activity switch is typically performed for maintenance or testing during a scheduled period of low activity, and involves the following sequence of events. • A 5620 SAM administrator initiates the activity switch on the primary server. • The standby server performs an activity switch to become the new primary server. • The new primary server connects to the primary database and manages the network. • The new primary server and the auxiliary servers synchronize the request information. • If automatic database realignment is enabled, the new primary server attempts a database switchover.	

Table 6-2 summarizes the 5620 SAM database redundancy functions.

Table 6-2 5620 SAM database redundancy functions

Function	Notes
Database switchover A database switchover is a manual operation that reverses the primary and standby database roles, for example, for primary database maintenance, or to realign database roles with database stations after a server activity switch. A switchover can occur only when the primary and standby databases are functioning correctly and can communicate with each other. A database switchover involves the following sequence of events. • A 5620 SAM administrator initiates the switchover on a primary or standby server. • The main server asks each auxiliary server to release all database connections. The switchover fails if all database connections are not released within 15 minutes. • The main server directs the standby database to become the primary database. • The main server fully synchronizes information with the new primary database. See Procedure 6-5 for information about performing a database switchover.	No automatic database realignment occurs after a database switchover.
Database failover A database failover is an automatic operation that changes the standby database into a primary database when the original primary database is unreachable, for example, because of a power disruption on the primary database station. A database failover involves the following sequence of events. • No main server can communicate with the primary database within a period that is 2 min by default. • The currently active main server directs the standby database to become the primary database. • If automatic database realignment is enabled and the primary server and database are not aligned, the primary server performs an activity switch. • The primary server directs each auxiliary server to connect to the new primary database. • The main server restarts after a failover.	When the primary server detects a communication failure with the primary or standby database, the GUI clients are informed that the database is not reachable. After the cause of the communication failure is resolved, the GUI clients are notified that the database is reachable. After a failover, you must reinstantiate the former primary database as the new standby database. Database redundancy is not restored until reinstantiation is complete. The 5620 SAM attempts to automatically reinstantiate the former primary database when automatic database reinstantiation is enabled.
Re-establishing database redundancy Re-establishing database redundancy after a database failure requires database reinstantiation to replicate the current primary database as the standby database. After a failover, the former primary database is not available for redundancy until an operator or the automatic database reinstantiation function reinstantiates it as the new standby database. See Procedures 6-8 and 6-9 for information about re-establishing database redundancy after a failover.	The following conditions must be met before you can re-establish database redundancy. • The failover completes successfully. • The station that contains the primary database is operational. • The former primary database proxy port is configured and in service.

6.4 Redundancy failure scenarios

The following describe the 5620 SAM actions in response to various types of redundancy failures.

- **Primary server loses contact with primary database**

  If the standby server can communicate with the primary database and the managed NEs, the primary server performs a server activity switch. No database failover occurs.

  If automatic database realignment is enabled, the new primary server performs a database switchover.
- **Primary server loses contact with managed NEs**

  If the standby server can communicate with the primary database and the managed NEs, the primary server performs a server activity switch.

  If automatic database realignment is enabled, the new primary server performs a database switchover.
- **Primary server loses contact with primary database and managed NEs**

  If the standby server can communicate with the primary database and the managed NEs, the primary server performs a server activity switch. No database failover occurs.

  If automatic database realignment is enabled, the new primary server performs a database switchover.
- **Primary server loses contact with primary database, managed NEs, and standby server**

  The standby server activates to become the new primary server, and if automatic database realignment is enabled, initiates a database switchover.
- **Both servers lose contact with primary database**

  The primary server initiates a database failover, and if automatic database realignment is enabled, also initiates a server activity switch.
- **Both servers lose contact, primary server and database can communicate**

  The primary server and database remain the primary server and database. The 5620 SAM raises an alarm about the server communication failure.
- **Both servers lose contact with managed NEs**

  If the primary and standby servers can each communicate with the preferred database, no server activity switch or database failover occurs. The 5620 SAM raises a reachability alarm against each NE in the network.
- **Both servers lose contact with primary database and managed NEs**

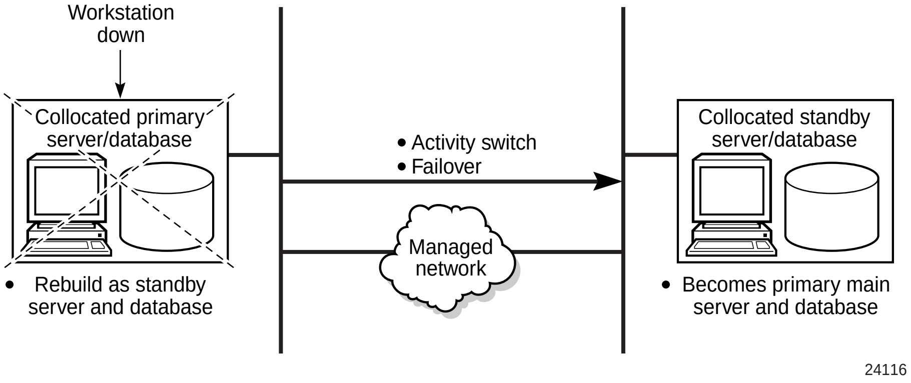
  If the primary and standby servers can communicate with each other, no server activity switch or database failover occurs. However, the 5620 SAM system is unavailable; manual intervention such as a database failover is required.
- **Both servers fail, primary database isolated, standby database operational**

  When both servers return to operation, the servers cannot connect to the primary database. Because the state of the standby database is unknown, no database failover occurs; manual intervention such as a database switchover is required.

Collocated system, primary station unreachable

Figure 6-11 shows a collocated system in which the station that hosts the primary server and database is unreachable.

Figure 6-11 Primary server and database station down, collocated system


Workstation down
Collocated primary server/database
Rebuild as standby server and database
• Activity switch
• Failover
Managed network
Collocated standby server/database
Becomes primary main server and database
24116

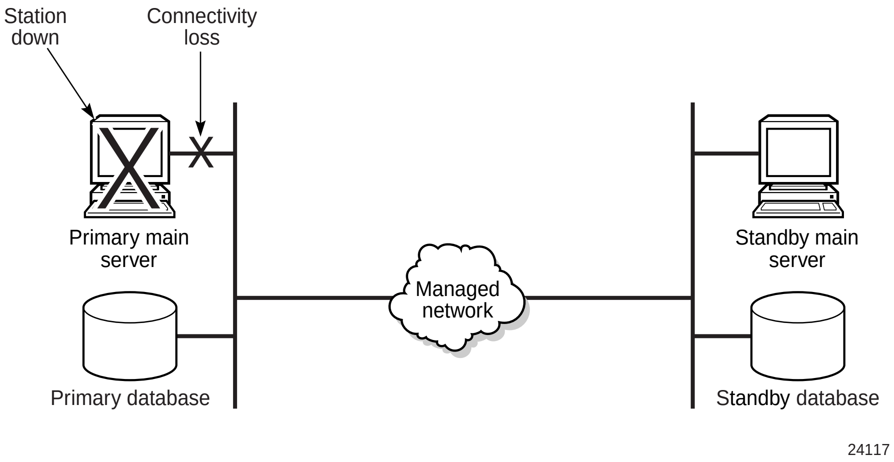
The following occur when the primary station becomes unresponsive:

- The standby server and database become the primary server and database.
- Redundancy is restored when the former primary station returns to service as the standby station.

Distributed system, primary server unreachable

Figure 6-12 shows a distributed system in which the primary server is unreachable.

Figure 6-12 Primary server unreachable, distributed system



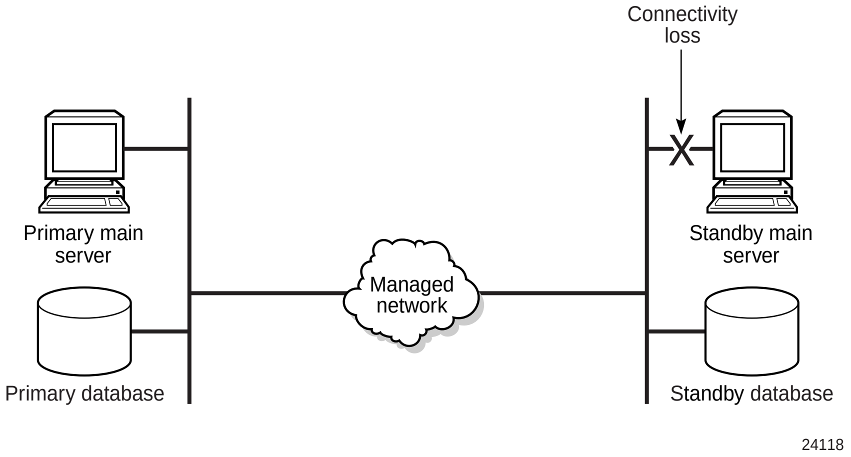
The following occur when the primary station becomes unresponsive:

- The standby server detects the connectivity loss and becomes the primary server.
- The new primary server raises alarms about the unavailability of the former standby server and about the activity switch.
- If automatic database realignment is enabled, the new primary server initiates a database switchover.
- When connectivity is restored, the former primary server assumes the standby server role.

Distributed system, standby server unreachable

Figure 6-13 shows a a distributed system in which the standby server is unreachable.

Figure 6-13 Standby server unreachable, distributed system



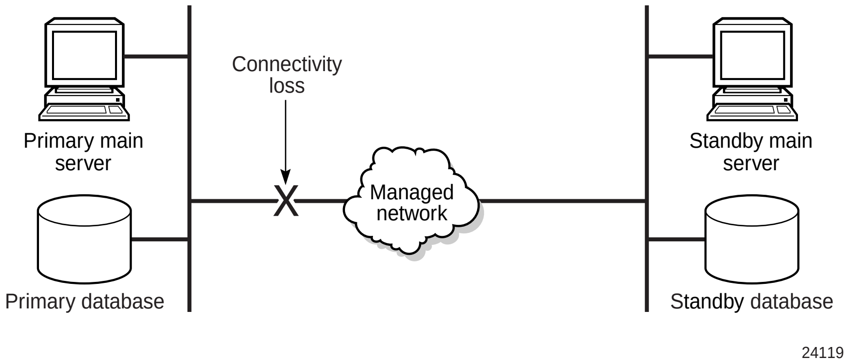
The following occur when the standby station becomes unresponsive:

- The standby server interprets the primary server unresponsiveness as a primary server failure, so attempts to assume the primary server role.
- The primary server generates an alarm to indicate that the standby server is down.
- When the reachability is restored, the standby server resumes the standby role and the alarm clears.

Distributed system, managed network unreachable by primary side

Figure 6-14 shows a managed network connection failure on the primary side of a distributed 5620 SAM system.

Figure 6-14 Network failure on primary side, distributed system



The following occur after the connectivity loss is detected:

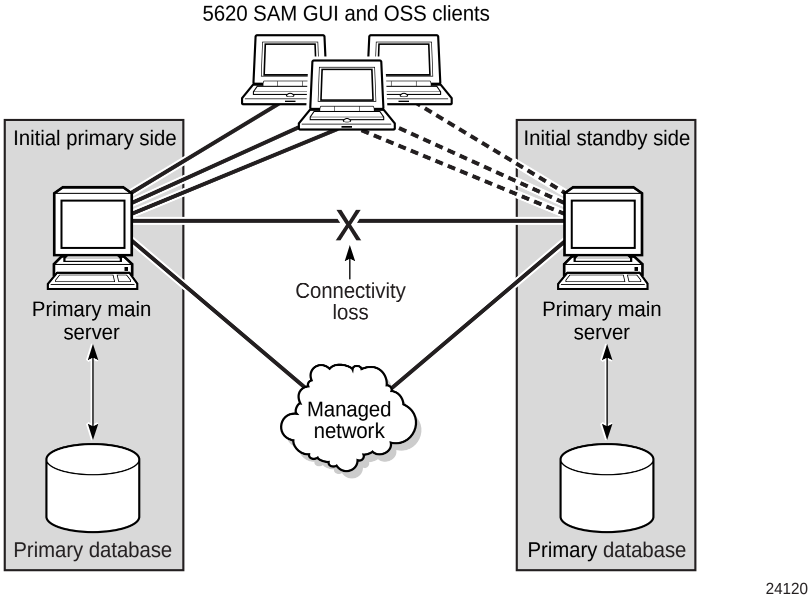
- The initial primary server continues to operate as a primary server.
- The initial primary server generates an alarm about the standby server unavailability, and a reachability alarm against each NE in the network.
- Each GUI client displays the standby server status as Down.
- The standby server becomes a primary server.

Note — You can eliminate a single point of hardware or network failure by using redundant interfaces and redundant physical network paths. See the *5620 SAM Planning Guide* for more information.

Split complex

A split complex is a scenario in which both servers in a collocated or distributed 5620 SAM system lose contact, but each server can communicate with the preferred database, as shown in Figure 6-15.

Figure 6-15 Split complex, collocated or distributed system



The following occur after the connectivity loss is detected:

- The initial primary server and database roles do not change; the initial primary server continues to manage the network. The client sessions are not interrupted.
- The primary server raises an alarm about the communication failure.
- The standby server and database switch roles to become a second primary server and database.
- New clients connect to the initial primary server; however, if a client explicitly tries to connect to the second primary server, a session is established.
- When the servers regain contact:
  - If the network disruption also isolates one server from the managed NEs, the other server and database remain the primary.
  - Otherwise, the server that has currently held the primary role for longer remains the primary, and the other server and database assume the standby role,

6.5 Workflow to perform 5620 SAM system redundancy functions

1 Configure redundancy during 5620 SAM component installation. See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide*.

2 As required, a perform manual activity switch and switchover.

  a For 5620 SAM main servers:

    i Verify the 5620 SAM system redundancy status. See Procedure 6-1.

    ii If required, verify the redundancy status of the 5620 SAM auxiliary server. See Procedure 6-2.

   iii Perform a manual activity switch on the primary server. See Procedure 6-3.

   iv Validate the updated redundancy status. See Procedure 6-1.

  b For 5620 SAM databases:

   i Verify the redundancy status of the 5620 SAM software. See Procedure 6-1.

   ii As required, perform a switchover. See Procedures 6-5 and 6-6.

   iii As required, configure automatic database realignment. See Procedure 6-7.

   iv Validate the updated redundancy status. See Procedure 6-1.

3 After a failover, re-establish redundancy between the standby and primary databases. See Procedures 6-8 and 6-9.

6.6 5620 SAM system redundancy procedures

Use the following procedures to perform redundancy tasks.

Procedure 6-1 To view the 5620 SAM system redundancy status

1 View the Standby Server, Primary DB and Standby DB status indicators in the 5620 SAM client GUI task bar. Each indicator should display Up.

2 Choose Administration→System Information. The System Information form opens with the General tab displayed.

3 View the general redundancy information:

- Domain Name—the 5620 SAM domain name specified at installation
- Redundancy Enabled—selected if redundancy is enabled
- Realignment Enabled—selected if automatic database realignment is enabled; displayed only if the 5620 SAM system is redundant
- Auto Standby Re-instantiation Enabled
- Realignment Status—Aligned or Not Aligned

4 View the following information in the Primary Server panel:

- Host Name—the host name of the primary or standalone main server
- Preferred DB—the preferred database of the main server
- Status—Unknown, Down, or Up

5 View the following information in the Primary Database Server panel:

- Instance Name—the name of the primary database instance, also called a SID
- IP Address—the IP address that each main or auxiliary server uses to reach the primary database
- Host Name—the host name of the primary database, or of the database in a standalone 5620 SAM system

6. If the 5620 SAM system is redundant, view the following information in the Standby Server panel:
    - Host Name—the host name of the standby main server
    - Status—Unknown, Down, or Up
7. If the 5620 SAM system is redundant, view the following information in the Standby Database Server panel:
    - Instance Name—the name of the standby database instance, also called a SID
    - IP Address—the IP address that each main or auxiliary server uses to reach the standby database
    - Host Name—the host name of the standby database
8. Click on the Properties button to display additional information about the primary or standby 5620 SAM main server. The Main Server properties form opens.
9. View the following general main-server information:
    - Host Name—the host name of the primary main server
    - Server Type—Main
    - Resource Managed—selected if the main server is included in 5620 SAM resource management
10. View the following information in the Client Communication panel:
    - Private IP Address—the IP address that the main server uses as the source address for communication with the 5620 SAM GUI and OSS clients through a NAT router
    - Public IP Address—the IP address that the 5620 SAM GUI and OSS clients use to reach the main server through a NAT router

Note 1 — The Private IP Address and Public IP Address display 0.0.0.0 when the 5620 SAM clients and the main server use host names, rather than IP addresses, for communication.

Note 2 — The Private IP Address and Public IP Address display the same IP address when NAT is not used between the main server and clients.

11. View the following information in the Redundant Server Communication panel:
    - Private IP Address—the IP address that the main server uses as the source address for communication with the standby main server through a NAT router
    - Public IP Address—the IP address that the standby main server uses to reach the primary main server through a NAT router
    - Peer Public IP Address—the IP address that the standby main server uses to reach the main server

Note — The Private IP Address and Public IP Address display the same IP address when NAT is not used between the primary and standby main servers.

12 View the following information in the Redundancy Database State panel:

- Switchover State—whether switchover in progress, and operational state
- Last Attempted Switchover Time—time of previous switchover attempt
- Failover State—whether failover in progress, and operational state
- Last Attempted Failover Time—time of previous failover attempt
- Standby Re-instantiation State—whether reinstantiation is in progress, and operational state
- Last Attempted Standby Re-instantiation Time—time of previous standby reinstantiation attempt
- Number of Archive Logs To be Applied—number of archive logs that remain to be applied on standby database
- Estimated Time to Apply Archive Logs (seconds)—system time estimate for application of archive logs on standby database

13 View the following information in the Auxiliary Server Communication panel:

- Private IP Address—the IP address that the main server uses as the source address for communication with the auxiliary servers through a NAT router
- Public IP Address—the IP address that the auxiliary servers use to reach the primary main server

Note — The Private IP Address and Public IP Address display the same IP address when NAT is not used between the main server and the auxiliary servers.

14 View the following information in the Main Server Communication panel:

- Server Public IP Address—the IP address that the auxiliary server uses to communicate with the main server

15 Close the Main Server properties form. The System Information form reappears.

16 Click on the Database button to view more detailed database information, if required. See chapter 7 for information about the 5620 SAM database.

17 Click on the Faults tab to view alarm information, if required.

18 Close the System Information form.

Procedure 6-2 To view the 5620 SAM auxiliary server status

1 Choose Administration→System Information. The System Information form opens.

2 Click on the Auxiliary Servers tab.

3 Review the list of auxiliary servers.

4 Select an auxiliary server in the list and click on the Properties button. The properties form for the auxiliary server opens.

5 Review the auxiliary server information, which includes the following:

- Host Name—the host name of the auxiliary server
- Port Number—identifies the port that the auxiliary server uses to communicate with each main server and database
- Auxiliary Server Type—Reserved or Preferred
- Server Status—Unknown, Down, Up or Unused
- Resource Managed—selected if the auxiliary server is included in 5620 SAM resource management
- Public IP address—the IP address that the main servers use to reach the auxiliary server

6 Perform one of the following:

a View the following main server information for a redundant 5620 SAM system:

- Server 1 Public IP address—the IP address that the auxiliary server uses to communicate with the primary or standby main server
- Server 2 Public IP address—the IP address that the auxiliary server uses to communicate with the primary or standby main server

b View the following main server information for a standalone 5620 SAM system:

- Server Public IP address—the IP address that the auxiliary server uses to communicate with the main server

7 Click on the Auxiliary Services tab.

8 Review the list of auxiliary services.

9 Review the information for each auxiliary service, which includes the following:

- Service Name—the type of service, for example, statistics collection
- Selected—indicates whether this auxiliary server is currently used by a main server to process requests
- IP Address—the IPv4 address that the managed NEs use to reach the auxiliary server
- IPv6 Address—the IPv6 address that the managed 9500 MPR NEs use to reach the auxiliary server
- Host Name—the host name of this auxiliary server
- Auxiliary Server Type—Reserved or Preferred

10 Close the Auxiliary Services form.

11 Click on the Faults tab to view alarm information, if required.

12 Close the System Information form.

Procedure 6-3 To perform a server activity switch

Perform this procedure to reverse the primary and standby roles of the main servers in a redundant 5620 SAM system. Consider the following before you perform a server activity switch.

- Each client GUI receives notification of a server activity switch.
- During a server activity switch, a main server does not process SNMP traps, attempt to synchronize NEs, or collect statistics.
- During a server activity switch, auxiliary servers process outstanding requests, but do not communicate with a main server.
- After a server activity switch, the new primary main server deploys outstanding configuration changes to NEs, establishes communication with the auxiliary servers, and synchronizes information with the auxiliary servers.
- A manual activity switch stops and starts the former primary main server. Server redundancy is unavailable until the former primary main server is fully initialized as the new standby main server.

1 Log in to the primary main server station as the samadmin user.

2 Open a console window.

3 Enter the following at the CLI prompt:

```
bash$ install_dir/nms/bin/nmsserver.bash force_restart ↵
```

where *install_dir* is the 5620 SAM server installation location, typically /opt/5620sam/server

The server activity switch begins. The primary main server restarts as the standby main server, and the former standby main server becomes the new primary main server.

4 Close the console window.

5 Clear alarms, as required. The activity switch alarms must be cleared manually.

6 Verify that the GUI and OSS clients can connect to the new primary main server.

Procedure 6-4 To configure 5620 SAM database switchover behavior

Perform this procedure on a redundant 5620 SAM system to specify how database switchovers are executed. A database switchover occurs immediately upon request unless a database query is in progress, in which case the 5620 SAM does the following:

- if session interruption is enabled, waits a specified period before forcing the switchover
- if session interruption is disabled, the switchover does not occur and the Switchover State is Failed

1 Choose Administration→Database from the 5620 SAM main menu. The Database Manager (Edit) form opens with the General tab displayed.

2 Configure the parameters:

- DB Session wait time (minutes)
- Interrupt Read sessions after time out
- Interrupt Write sessions after time out

3 Click on the OK button. A dialog box appears.

4 Click on the Yes button. The Database Manager (Edit) form closes.

Procedure 6-5 To perform a 5620 SAM database switchover using the 5620 SAM client GUI

Perform this procedure to use the 5620 SAM client GUI to switch the primary and standby database roles. Before you perform the procedure, ensure that you understand the following implications of a switchover.

- The primary and standby database roles are reversed.
- The primary main server connects to the new primary database.
- Archive logging begins on the new primary database.
- The primary main server directs each auxiliary server to connect to the new primary database.

Caution — The execution of a database switchover depends on how the database switchover behavior is configured. Alcatel-Lucent recommends you review Procedure 6-4 before you attempt to perform this procedure to verify the current database switchover configuration.

1 Log in to the client GUI as a 5620 SAM user with the admin scope of command role.

2 Choose Administration→System Information from the 5620 SAM main menu. The System Information form opens with the General tab displayed.

3 Click on the Switchover button. If the Switchover button is not visible, click on the More Actions button and choose Switchover. A dialog box appears.

> **Note —** The Switchover option is disabled when the correct switchover conditions are not in place, for example, when a switchover or failover is in progress.

4 Respond to the dialog-box prompt.

5 Click on the Yes button. The 5620 SAM server performs the database switchover.

6 Close the System Information form.

Procedure 6-6 To perform a 5620 SAM database switchover using a CLI script

Perform this procedure to use a CLI script to switch the primary and standby database roles. Before you perform the procedure, ensure that you understand the following implications of a switchover.

- The primary and standby database roles are reversed.
- The primary main server connects to the new primary database.
- Archive logging begins on the new primary database.
- The primary main server directs each auxiliary server to connect to the new primary database.

> **Caution —** The execution of a database switchover depends on how the database switchover behavior is configured. Alcatel-Lucent recommends you review Procedure 6-4 before you attempt to perform this procedure to verify the current database switchover configuration.

1 Log in to the primary main server station as the samadmin user.

2 Open a console window.

3 Enter the following at the CLI prompt:

```
bash$ install_dir/switchoverdb.bash username password ↵
```

where

install_dir is the 5620 SAM server installation location, typically /opt/5620sam/server

username and *password* are the login credentials for a 5620 SAM client account with the required privilege level and scope of command

The script displays the following confirmation message:

```
The standby database will become the new primary database,

and the old primary will become the new standby.

Do you want to proceed? (YES/no) :
```

4 Enter the following case-sensitive text at the prompt to start the switchover:

```
YES ↵
```

The 5620 SAM server initiates a database switchover. Progress is indicated by a rolling display of dots in the console window. The database switchover is complete when the CLI prompt reappears.

5 Close the console window when the database switchover is complete.

Procedure 6-7 To configure automatic database realignment

Perform this procedure to enable or disable automatic database realignment on the main servers.

Caution — This procedure requires a restart of a 5620 SAM main server, which is service-affecting. To avoid service interruption, schedule the reconfiguration to coincide with a maintenance window.

Note 1 — This procedure applies only to redundant 5620 SAM deployments.

Note 2 — You must perform this procedure first on the standby main server station, and then on the primary main server station.

1 Log in to the standby main server as the samadmin user.

2 Stop the main server software.

- i Navigate to the server binary directory. Enter the following at the prompt:

  ```
  bash$ cd install_dir/nms/bin ↵
  ```

  where *install_dir* is the server installation location, typically /opt/5620sam/server

- ii Enter the following at the prompt:

  ```
  bash$ ./nmsserver.bash stop ↵
  ```

- iii Enter the following at the prompt:

  ```
  bash$ ./nmsserver.bash appserver_status ↵
  ```

- iv The server application is stopped when the command in step 2 iii returns the following text string:

  ```
  Application Server is stopped
  ```

  If the command returns anything other than the above text string, wait five minutes and repeat step 2 iii. Do not proceed unless the console displays the above text.

3 Enter the following to switch to the root user:

```
bash$ su - ↵
```

4 Place the 5620 SAM software DVD-ROM in a DVD-ROM drive.

5 Navigate to the DVD_ROM drive.

6 Perform one of the following to open the 5620 SAM server installer.

a On a RHEL station:

i Enter the following:

```
# cd Linux ↵
```

ii Enter the following:

```
# ./ServerInstall_RHEL_R_r_revision.bin ↵
```

where
R_r is the release identifier, in the form *MAJOR_minor*
revision is the revision identifier, such as R1, R3, or another descriptor

b On a Solaris station:

i Enter the following:

```
# cd Solarisx86 ↵
```

ii Enter the following:

```
# ./ServerInstall_SolarisX86_SAM_R_r_revision.bin ↵
```

where
R_r is the release identifier, in the form *MAJOR_minor*
revision is the revision identifier, such as R1, R3, or another descriptor

The 5620 SAM server configuration utility opens, and displays the Introduction panel.

7 Click on the Next button.

8 Accept the terms of the license agreement in the “Software License Agreement” panel.

9 Click on the Next button.

10 Choose Main Server Configuration in the “Choose Installation Type” panel.

11 Click on the Next button.

12 Click on the Next button in each subsequent panel until the “Database Alignment” panel is displayed.

13 Configure the “Enable Database Alignment” parameter.

Note — You must configure this parameter the same way on the standby and primary main servers.

14 If you selected the “Enable Database Alignment” parameter in step 13, select a server to act as the preferred server.

15 Click on the Next button.

16 Click on the Next button in each subsequent panel until the “Installation Complete” panel is displayed.

17 Select the “Start the 5620 SAM Main Server” parameter.

18 Click on the Done button to close the server configuration utility.

19 Enter the following to switch back to the samadmin user:

```
# exit ↵
```

20 Verify the standby main server has started.

21 Log out of the standby main server.

22 Perform steps 1 to 21 on the primary main server.

Note — When you stop the primary main server, a switchover to the standby main server occurs.

23 If required, perform Procedure 6-3 to perform a server activity switch and revert the main servers to their original roles.

Procedure 6-8 To reinstantiate a redundant database using the 5620 SAM client GUI

Perform this procedure to re-establish redundancy after a database failover or similar maintenance activity. This procedure reinstantiates the former primary database as the new standby database.

When automatic database reinstantiation is enabled, a failed manual reinstantiation attempt does not affect the reinstantiation timer. If a manual reinstantiation is successful, the 5620 SAM does not attempt a subsequent reinstantiation.

Before you attempt to perform this procedure, the following conditions must be true:

- The primary database proxy and the standby database proxy are in contact with the primary 5620 SAM server.
- The database listener is operating.

1 Log in to the client GUI as a user with the 5620 SAM admin scope of command role.

2 Choose Administration→System Information from the 5620 SAM main menu. The System Information form opens with the General tab displayed.

3 Verify the database redundancy status matches the following:

- Failover State: Successful
- Switchover State: Not Attempted

4 Click on the Re-Instantiate Standby button. If the Re-Instantiate Standby button is not visible, click on the More Actions button and choose Re-Instantiate Standby. A dialog box appears.

5 Click on the Yes button to confirm. The database reinstantiation begins.

The client GUI status bar and the System Information form display the reinstantiation status. The Standby Re-instantiation State changes from In Progress to Success when reinstantiation is complete. The Last Attempted Standby Re-instantiation Time displays the start time of the current reinstantiation.

6 Close the System Information form when the reinstantiation is complete.

Procedure 6-9 To reinstantiate a redundant database using a CLI script

Perform this procedure to re-establish redundancy after a database failover or similar maintenance activity. This procedure reinstantiates the former primary database as the new standby database. Before you start, the following conditions must be true:

- The primary database proxy and the standby database proxy are in contact with the 5620 SAM server.
- The database listener is operating.

1 Log in to the primary main server station as the samadmin user.

2 Open a console window.

3 Navigate to the 5620 SAM server binary directory, typically /opt/5620sam/server/nms/bin.

4 Enter the following at the CLI prompt:

```
bash$ ./reinstantiatedb.bash -u username -p password ↵
```

where

username is the user name of a 5620 SAM client account with the required privilege level and scope of command

password is the password for the user account

The script displays the following confirmation message:

```
This action will rebuild the standby database.

Do you want to proceed? (YES/no) :
```

5 Enter the following case-sensitive text at the prompt to begin reinstantiation:

YES ↵

The 5620 SAM server begins to reinstantiate the former primary database as the standby database. Progress is indicated by a rolling display of dots in the console window. Database reinstantiation is complete when the CLI prompt reappears.

6 Close the console window when the reinstantiation is complete.

7 — 5620 SAM database management

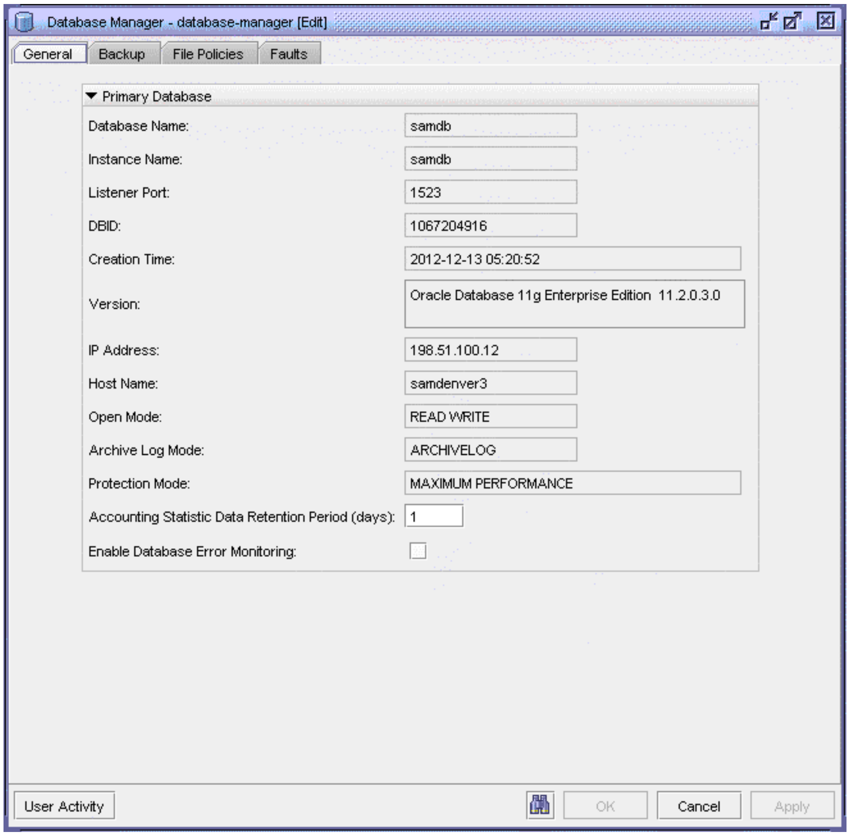
7.1 5620 SAM database management overview

The 5620 SAM uses an Oracle database to store information. You can use the 5620 SAM Database Manager to manage functions that include the following:

- database security
- statistics data retention
- database backups
- database log storage
- SQL error monitoring
- database troubleshooting

Figure 7-1 shows the General tab of the Database Manager form.

Figure 7-1 Database Manager form — General tab



Database Name: samdb
Instance Name: samdb
Listener Port: 1523
DBID: 1067204916
Creation Time: 2012-12-13 05:20:52
Version: Oracle Database 11g Enterprise Edition 11.2.0.3.0
IP Address: 198.51.100.12
Host Name: samdenver3
Open Mode: READ WRITE
Archive Log Mode: ARCHIVELOG
Protection Mode: MAXIMUM PERFORMANCE
Accounting Statistic Data Retention Period (days): 1
Enable Database Error Monitoring: ☐

A redundant 5620 SAM deployment has two databases that are synchronized in a primary/standby configuration to minimize data loss in the event of a failure.

In addition to the database protection of system redundancy, the 5620 SAM has protective mechanisms that raise alarms for the following:

- database disk and tablespace capacity problems
- redundancy events, misconfiguration, and failures
- database backup misconfiguration and failures
- archive log management actions and failures
- internal errors that may be a security risk, and size-constraint policy violations

7.2 Workflow to manage the 5620 SAM database

1. As a security precaution, configure the number of failed Oracle database user login attempts that the 5620 SAM allows before the user is locked out; see Procedure 7-1.
2. Configure how the 5620 SAM responds to Oracle database errors; see Procedure 7-3.
3. Configure the statistics data retention period for the 5620 SAM database according to your company policy; see Procedure 7-4.
4. Manage the 5620 SAM database disk usage by configuring policies to limit the maximum size of database log files, such as the alert, trace, listener, and audit logs; see Procedure 7-5.
5. Verify the synchronization of managed-device and 5620 SAM database information; see Procedure 11-3.
6. Back up the 5620 SAM database, as required, according to your company policies. Alcatel-Lucent recommends that you back up the 5620 SAM database daily. See Procedures 11-4 and 11-5.
7. If required, schedule a regular database backup that defines when an automated database backup occurs; see Procedure 7-6.
8. As required, monitor the 5620 SAM database; see Procedure 7-7.
9. Test the 5620 SAM database restore function to ensure that 5620 SAM database backups are viable in the event that a restore is required; see Procedure 12-3.
10. As required, restore the 5620 SAM database on a standalone or a redundant 5620 SAM system; see Procedures 14-7 and 14-8.
11. As required, troubleshoot 5620 SAM database problems such as corruption or failure issues, disk space problems, or performance issues. See the *5620 SAM Troubleshooting Guide*.

7.3 5620 SAM database management procedures

Use the following procedures to perform database management tasks.

Procedure 7-1 To set the allowed number of database login failures

Perform this procedure to configure the number of Oracle database user login failures that the 5620 SAM allows. When the configured number is reached, the 5620 SAM prevents subsequent login attempts by the user until the user account is unlocked.

See Procedure 7-2 for information about how to unlock the Oracle database user account.

Note 1 — In a redundant deployment, you must perform this procedure on the primary database station. After you perform the procedure, the primary database automatically copies the configuration change to the standby database.

Note 2 — The configuration changes that you make in this procedure are not affected by subsequent database upgrades.

1 Log in to the 5620 SAM database station as the Oracle management user.

2 Open a console window.

3 Enter the following:

```
bash$ path/install/config/samdb/SAMDb_security.sh ↵
```

where *path* is the 5620 SAM database installation location, typically /opt/5620sam/samdb

The following prompt is displayed:

```
Enter the password for the "sys" user (terminal echo is off):
```

4 Enter the Oracle SYS user password and press ↵.

The following prompt is displayed:

```
 Accept value? [y/n/q] (y):
```

5 Perform one of the following.

a Press ↵ to confirm that the supplied password is correct.

The following prompt is displayed:

```
Please select one of the following options:

   1) Setting failed login attempts

   2) Unlock database user

   0) Exit

  Please enter(1,2 or 0):
```

b Press n ↵ if you have incorrectly entered the password; return to step 4.

6 To specify the allowed number of login failures, perform the following steps.

i Enter 1 ↵.

The following prompt is displayed:

```
Please select one of the following options:

   1) Setting the number of failed login attempts

   2) Remove the number of failed login attempts setting (no
checking)
```

```
0) Exit

Please enter(1,2 or 0):
```

ii Enter 1 ↵.

The following prompt is displayed:

```
This value will be use for setting the number of failed login
attempts before locking the database user account.

Please enter value for number of failed login attempts(20 to
1000) (30):
```

iii Perform one of the following.

- Accept the default of 30. Press ↵.
- Specify a value between 20 and 1000, and then press ↵.

The following messages are displayed:

```
About to change the Oracle database user settings

Completed changing the Oracle database user settings
```

iv Go to step 8.

7 To remove the allowed number of failed login attempts, enter 2 ↵.

The following messages are displayed, and the 5620 SAM no longer locks the Oracle database user account after multiple login failures.

```
About to change the Oracle database user settings

Completed changing the Oracle database user settings
```

8 Close the console window.

Procedure 7-2 To unlock the Oracle database user account

Perform this procedure to allow Oracle database user login attempts after the user is locked out because of multiple login failures. See Procedure 7-1 for information about how to configure the number of allowed login failures for the Oracle database user.

1 Log in to the 5620 SAM database station as the Oracle management user.

2 Open a console window.

3 Enter the following:

```
bash$ path/install/config/samdb/SAMDb_security.sh ↵
```

where *path* is the 5620 SAM database installation location, typically /opt/5620sam/samdb

The following prompt is displayed:

```
Enter the password for the "sys" user (terminal echo is off):
```

4 Enter the Oracle SYS user password and press ↵.

The following prompt is displayed:

```
 Accept value? [y/n/q] (y):
```

5 Perform one of the following.

- **a** Press ↵ to confirm that the supplied password is correct.

  The following prompt is displayed:

  ```
  Please select one of the following options:
     1) Setting failed login attempts
     2) Unlock database user
     0) Exit
    Please enter(1,2 or 0):
  ```

- **b** Press n ↵ if you have incorrectly entered the password; return to step 4.

6 Enter 2 ↵.

The following messages are displayed, and the Oracle database user account is unlocked.

```
About to unlock the database user username
Completed unlocking the database user username
```

where *username* is the Oracle database username

7 Close the console window.

Procedure 7-3 To configure database error monitoring

Perform this procedure to configure how the 5620 SAM reacts to Oracle database errors. When database error monitoring is enabled, the 5620 SAM raises an alarm when the Oracle software reports an error, for example, an invalid SQL statement. The monitoring function provides information that may help with troubleshooting or the detection of security violations such as SQL injection attacks.

1 Choose Administration→Database from the 5620 SAM main menu. The Database Manager (Edit) form opens.

2 To enable database error monitoring, select the Enable Database Error Monitoring parameter.

3 To disable database error monitoring, deselect the Enable Database Error Monitoring parameter.

4 Click on the OK button. A dialog box appears.

5 Click on the Yes button. The Database Manager (Edit) form closes.

Procedure 7-4 To configure statistics data retention for the 5620 SAM database

1 Choose Administration→Database from the 5620 SAM main menu. The Database Manager (Edit) form opens.

2 Configure the Accounting Statistic Data Retention Period (Days) parameter.

Caution — Configuring the Accounting Statistic Data Retention Period (Days) parameter can affect 5620 SAM system performance. Consult an Alcatel-Lucent support representative before you configure the parameter.

3 Click on the OK button. A dialog box appears.

4 Click on the Yes button.

5 Close the Database Manager (Edit) form.

Procedure 7-5 To manage the database log files

You can use policies to manage the file size of stored alert, trace, listener, and audit log files. When the size and number of files are left unbounded, exceeding database disk space limits may become a problem. The default settings of the file policies reduce the number of log files that are kept.

Database log files are compressed and stored in the alert log directory (for trace, alert, and audit log files) or the listener directory for listener log files.

For historical or troubleshooting purposes, Alcatel-Lucent recommends that you archive the database log files.

1 Choose Administration→Database from the 5620 SAM main menu. The Database Manager (Edit) form opens.

2 Click on the File Policies tab.

3 Perform one of the following.

  a Create a new database file policy.

    i Click on the Database File Policies button. The Database File Policies form opens.

    ii Click on the Create button. The File Policy (Create) form opens.

iii Configure the parameters:

- ID
- Description
- Auto-Assign ID
- Purge Mode
- Max (Collective) Log Size
- Number of Archives

iv Click on the OK button. The File Policy (Create) form closes.

v Close the Database File Policies form.

b Modify an existing policy.

i Click on the Database File Policies button. The Database File Policies form opens.

ii If required, specify a filter and click on the Search button.

iii Select a policy from the list and click on the Properties button. The File Policy (Edit) form opens.

iv Configure the parameters:

- Description
- Purge Mode
- Max (Collective) Log Size
- Number of Archives

v Click on the OK button. The File Policy (Edit) form closes.

vi Close the Database File Policies form.

4 Associate the file policy with a database log type, if required.

i Click on the Select button beside one of the following:

- Alert Log File Policy
- Listener Logs File Policy
- Trace and Audit Logs File Policy

The Database File Policies - Database Manager (Edit) form opens.

ii Choose a policy from the list.

iii Click on the OK button. The Database File Policies - Database Manager (Edit) form closes and the policy identifier is displayed on the Database Manager (Edit) form.

5 Click on the OK button. A dialog box appears.

6 Click on the Yes button. The Database Manager (Edit) form closes.

Procedure 7-6 To schedule a database backup

Perform this procedure to create a schedule that defines when automated database backups occur. See the *5620 SAM Parameter Guide* for detailed parameter information.

Note — The 5620 SAM backs up the Oracle encryption wallet during a database backup, and restores the wallet during a database restore. In a redundant deployment, the 5620 SAM automatically replicates the encryption wallet from the primary to the standby database after the standby database reinstantiation.

1 Choose Administration→Database from the 5620 SAM menu. The Database Manager form opens.

2 Click on the Backup tab.

3 Configure the parameters in the Backup Schedule panel.

4 Configure the Scheduled Backup Directory parameter in the Backup Setting panel. The parameter value that you specify is the directory on the database station in which the 5620 SAM stores the database backup file sets. Each backup file set is stored in a subdirectory under this directory, and is named backupset*n*

where *n* is a sequential number; the lowest value is 1, and the highest value is the Number to Keep parameter value

Caution — Before the 5620 SAM performs a database backup, it deletes the contents of the specified backup directory. Ensure that the backup directory that you specify in this step does not contain files that you need to retain.

Note 1 — The Scheduled Backup Directory must be a directory on the local file system.

Note 2 — The Oracle management user requires read and write permissions on the Scheduled Backup Directory.

5 After each scheduled database backup occurs, move the new database backup to another station for safekeeping.

Procedure 7-7 To view the 5620 SAM database properties

Perform this procedure to view general information about the Oracle database that the 5620 SAM uses.

1 Choose Administration→Database from the 5620 SAM main menu. The Database Manager (Edit) form opens and displays information that includes the following:

- Database Name—created during 5620 SAM installation; the default is samdb
- Instance Name—created during 5620 SAM installation; the default is samdb
- Listener Port—the port on the server used for database communication
- DBID—the Oracle database ID, sometimes referred to as the SID
- Creation Time—the database creation time
- Version—the Oracle version identifier, for example, Oracle Database 11g Enterprise Edition 11.2.0.2.0
- IP Address—the IP address that the server uses as the destination address for communicating with the database
- Host Name—the host name of the database station
- Open Mode—specifies the type of database access, either READ or READ WRITE
- Archive Log Mode—specifies whether to archive the database log files; this is configured during database installation
- Protection Mode—the database protection mode, which is set by default during installation to MAXIMUM PERFORMANCE

2 View the information.

3 Close the Database Manager (Edit) form.

8 — NE maintenance

8.1 NE maintenance overview

The 5620 SAM includes NE maintenance functionality for supported devices that allows a system administrator to:

- define the 5620 SAM deployment and local device configuration-save conditions
- perform an on-demand or scheduled NE configuration backup
- restore a device configuration
- perform an on-demand, ISSU, or a scheduled NE software upgrade
- view the status of a deployment, backup, device configuration restore, device software upgrade, or accounting statistics retrieval operation in progress
- troubleshoot a failed deployment, backup, or upgrade

A 5620 SAM operator with an administrator or network element software management scope of command role can perform device configuration save, backup, or restore operations, and can create policies for scheduling backups and configuration saves.

A 5620 SAM operator can upgrade software or schedule a software upgrade on sites and routers that are within their span of control.

A 5620 SAM operator with the lawful intercept management scope of command role can back up and restore NE LI configurations. Backup data is saved only when the LI local save allowed parameter is enabled. See the *5620 SAM User Guide* for more information.

Managing NE deployments

When you use the 5620 SAM to apply an NE configuration change, for example, by clicking on the OK or Apply button after setting a service parameter, the 5620 SAM deploys the change to the NE according to the 5620 SAM deployment policy. The 5620 SAM deployment policy also specifies the conditions under which each managed NE performs a configuration save.

The information in a deployment policy includes the following:

- number and frequency of 5620 SAM deployment retries
- NE configuration save settings, such as the following:
    - save frequency
    - level of configuration detail to save
    - delay between consecutive saves

In a lab or testing environment, it is sometimes necessary to disable 5620 SAM deployment. See the *5620 SAM XML OSS Interface Developer Guide* for information about disabling 5620 SAM deployment.

Note — The Deployment tab on an object properties form lists the failed deployments and deployments that are in progress. In addition, a deployment icon is displayed on the configuration form beside the parameter associated with the failed or attempted deployment, beside the NE object in the navigation tree, in list tables, and in map info tables.

Managing NE backups and restores

A 5620 SAM backup policy specifies the conditions under which the 5620 SAM performs a device backup to ensure that the device configuration is not lost in the event of a failure. A default policy that is assigned to all managed NEs is in place after a 5620 SAM installation. You can create and configure multiple backup policies, and you can assign them to multiple NEs. You must unassign all NEs from a backup policy before you can delete the policy. The information in a backup policy includes the following:

- the frequency of backups
- the files that a backup collects
- the type of file compression that the 5620 SAM uses
- the age and number of backup files that the 5620 SAM retains

The 5620 SAM stores the backed-up device configuration files in the 5620 SAM database for ease of tracking and retrieval. You can perform an on-demand export of backup files from the database to a file system, and can import NE backups from a file system to the 5620 SAM database.

You can configure the 5620 SAM to save device configuration backup files to the main-server file system, in addition to the 5620 SAM database, by editing a main-server configuration file. The saved files are synchronized between the primary and standby main servers in a redundant 5620 SAM deployment.

You can configure the 5620 SAM to do the following:

- automatically save device backups to a file system in addition to the database
- automatically delete device backup files after the associated NE is unmanaged

See chapter 7 for more information.

When a device configuration requires replacement, for example, because it becomes corrupted, you can restore a previously backed-up configuration. Unless otherwise specified, the 5620 SAM restores the most recent device configuration backup. See Procedures 8-4 and 8-7 for more information.

Managing NE software upgrades

You can use the 5620 SAM to perform scheduled or on-demand NE software upgrades, including ISSUs. A software upgrade requires a software upgrade policy.

A software upgrade policy contains settings such as the device family, file transfer credentials, software image and backup locations, and the actions to perform; for example, image download, activation, or ISSU. Depending on the device family, the activation function supports the reboot and reboot upgrade options. See “Reboot and reboot upgrade” in this section for more information.

Using a software upgrade policy, a 5620 SAM operator can independently perform the image download and software activation tasks. For example, you can configure a policy to perform the time-consuming software image downloads only, and then schedule the image activation as a separate task. When the image downloads are performed in advance, the 5620 SAM can perform more activations in one maintenance period.

During a software upgrade, the 5620 SAM verifies that the new software is compatible with the device type and that the required files are present; otherwise, the upgrade is not attempted. You can use the 5620 SAM to roll back a software upgrade to the previous release in the event of an upgrade failure.

Caution — Ensure that you regularly remove from the 5620 SAM the device software images that are no longer required, for example, by deleting the images or by exporting to a file system. An accumulation of device software images can dramatically increase the length of database operations such as backup, restore, and reinstantiation.

Note — You cannot upgrade an NE to a chronologically older release. For example, you cannot upgrade from Release 10.0 R8 to 11.0 R1, because Release 11.0 R1 predates 10.0 R8. See the *5620 SAM Network Element Compatibility Guide* for information about the supported upgrade paths.

ISSUs

You can use the 5620 SAM to perform an in-service software upgrade, or ISSU, on a managed NE that has dual CPMs. An ISSU allows an NE to provide uninterrupted service during the upgrade process.

Caution — Before you attempt an ISSU, see the appropriate device release notice and the *5620 SAM Network Element Compatibility Guide* for information about the supported upgrade paths.

Note 1 — ISSUs are restricted to device maintenance releases only. See the device documentation for the supported ISSU release transitions.

Note 2 — The 7210 SAS-R does not support ISSUs.

A device software upgrade requires a CPM restart, which causes a temporary NE outage. When an NE has dual CPMs, however, one CPM can remain active while the other restarts using the upgraded software. The alternate CPM restarts mean that the NE remains fully in service during an upgrade. If the upgrade of a CPM fails, the CPM reports the failure and an alarm is raised.

Reboot and reboot upgrade

You can perform a manual or an automatic NE reboot during an on-demand software upgrade, and can configure an automatic reboot in a software upgrade policy. See Procedure 8-1 for information about configuring an automatic reboot in a software upgrade policy, or Procedure 8-22 for information about performing a manual reboot during an on-demand software upgrade.

The 5620 SAM supports the 7210 SAS and 7705 SAR reboot upgrade option, which upgrades the system firmware during a device reboot. You can manually perform a reboot upgrade on an NE, or configure an automatic reboot upgrade in a software upgrade policy. See Procedure 8-1 for information about configuring an automatic reboot upgrade, and Procedure 8-22 for information about performing a manual reboot upgrade during an on-demand software upgrade.

Managing NE configuration rollbacks

You can revert to a previous device configuration on a specified 7450 ESS, 7750 SR, or 7950 XRS. A configuration rollback minimizes the impact to services by avoiding a system reboot. 5620 SAM supports up to five simultaneous NE rollback revert and rescue operations.

The rollback function allows you to use a configuration temporarily and revert to a previous configuration, for example to:

- troubleshoot network problems on an NE
- configure trial sites
- set configurations for specific days such as weekdays or weekend days

For each NE, you create a rescue file, which is the master file for the NE configuration. In addition, you can create multiple checkpoint files for each NE at any time. You can also create checkpoint files manually, or you can automate the creation of the file using NE rollback policies. The checkpoint files provide a history of NE configuration changes. The rescue file and checkpoint files are saved locally or remotely to an FTP site or to a flash drive. You can change the NE configuration using either file at any time without having to reboot.

The 5620 SAM scheduling function supports NE configuration rollback, which allows you to automate NE configuration checkpoint file creation and NE configuration reversion. See the *5620 SAM User Guide* for scheduling information.

Comparing configuration files

A compare function allows you to display NE configuration changes between selected checkpoints, a selected checkpoint and the active configuration, a selected checkpoint and the rescue file, or the active configuration and the rescue file. This is useful for troubleshooting NE configurations.

When you choose one of the compare NE configuration rollback file options, the Checkpoint Compare window opens listing differences between the selected configuration files. The window title displays the names of the NE configuration files that are compared. For example, the title “Index 0 and rescue” indicates that the first NE configuration checkpoint file listed on the Checkpoint Files tab is compared with the NE configuration rescue file. Differences in the configuration files are noted as follows:

- The plus sign (+) indicates that the configuration is in the first NE configuration file listed in the window title but not in the second NE configuration file. In this case, the configuration is in the checkpoint file index 0.
- The minus sign (–) indicates that the configuration is in the second NE configuration listed file in the window title but not in the first NE configuration file. In this case, the configuration is in the rescue file.
- Configurations that are in both NE configuration files are not listed in the Checkpoint Compare window.

NE file system browsing

A 5620 SAM operator can browse the file system of a managed NE to list the contents of the compact flash devices. You can browse the file system of a 7210 SAS, 7450 ESS, 7705 SAR, 7710 SR, 7750 SR, 7950 XRS, or OmniSwitch using simple FTP or a CLI session using SSH. The 5620 SAM GUI is used to browse the different types of files.

Browsing an NE file system using the 5620 SAM is a convenient way to confirm that operations such as the following occur as planned by verifying the sizes and time stamps of local NE files:

- NE configuration saves
- NE software image transfers and upgrades
- NE configuration restores
- NE accounting-statistics collection

FTP file browsing on an NE requires FTP user-account access on the NE. SSH file browsing requires console user-account access and the configuration of SSH security on the NE. See the *5620 SAM User Guide* for information about enabling FTP or console access for an NE user account or configuring SSH on an NE.

Note — The 7705 SAR may become temporarily unreachable when enabling SSH and starting the SSH server on the device.

See Procedure 8-36 for information about browsing an NE file system using an FTP file browser. See Procedure 8-37 for information about browsing an NE file system using an SSH file browser.

Sample deployment policy configuration

The following example describes the configuration and operation of a 5620 SAM deployment policy. See Procedure 8-2 for deployment policy configuration information.

Example details

The example policy settings are the following:

- Auto Save Scheme—Every Nth Successful Deployment

  Initiate a device configuration save after the number of configuration changes specified by Auto Save Threshold.
- Auto Save Threshold—3

  Initiate a configuration save after every three successful deployments, if Auto Save Scheme is set to Every Nth Successful Deployment.
- Scheduled Save Scheme—None

  Do not perform a scheduled configuration save on any NE.
- Scheduled Save Interval—1 hour

  If scheduled saves are enabled, perform a save every hour.
- Save Details—disabled

  Save only non-default parameter values.

- Configuration Save Interval—30 seconds

  Delay consecutive configuration save requests for an NE that are less than 30 seconds apart.
- Interval Repeat Limit—5

  Wait up to five Configuration Save Interval periods before performing a configuration save.
- Retry Scheme—Retry Number Of Times

  Retry each deployment the number of times specified by Retry Interval.
- Retry Interval—5 minutes

  Wait five minutes before retrying a failed deployment.
- Retry Threshold—3

  Retry each failed deployment three times.

Sample backup/restore policy configuration

The following example describes a sample 5620 SAM backup/restore policy configuration and its operation using parameter values that are appropriate for most applications. The Backup Policy form contains the parameters listed in the example. See Procedure 8-3 for the configuration information.

Example details

The sample backup policy specifies that the 5620 SAM obtains the backup files by FTP from the device once every hour regardless of configuration activity, and after every 25 configuration changes. The policy also specifies that the 5620 SAM backs up the device configuration file and boot options file (BOF) only when a newer file is present, and uses gzip file compression. The 5620 SAM is to retain at most 30 backup versions, and purge versions that are more than 30 days old.

The backup policy parameters and their values are:

- Enable Backup—enabled
- Auto Reboot After Successful Restore—enabled
- Scheduled Backup Scheme—Every Scheduled Interval
- Scheduled Backup Interval—1 hour
- Scheduled Backup Sync Time — 00:00
- Scheduled Backup Threshold (operations)—5
- Auto Backup Scheme—Every Nth 5620 SAM Server Initiated Save
- Auto Backup Threshold (operations)—50
- CLI Config File Mode—New Version Only
- CLI Config Save Details—disabled
- CLI Debug Save Config File Mode—disabled
- Boot Option File Mode—New Version Only
- File Compression—GZIP
- Backup 7705 Radio Database—disabled
- Auto-Purge Scheme—By Age But Retain A Minimum Number Of Backups
- Number of Backups—30
- Maximum Backup Age (days)—30

Figure 8-1 5620 SAM backup process

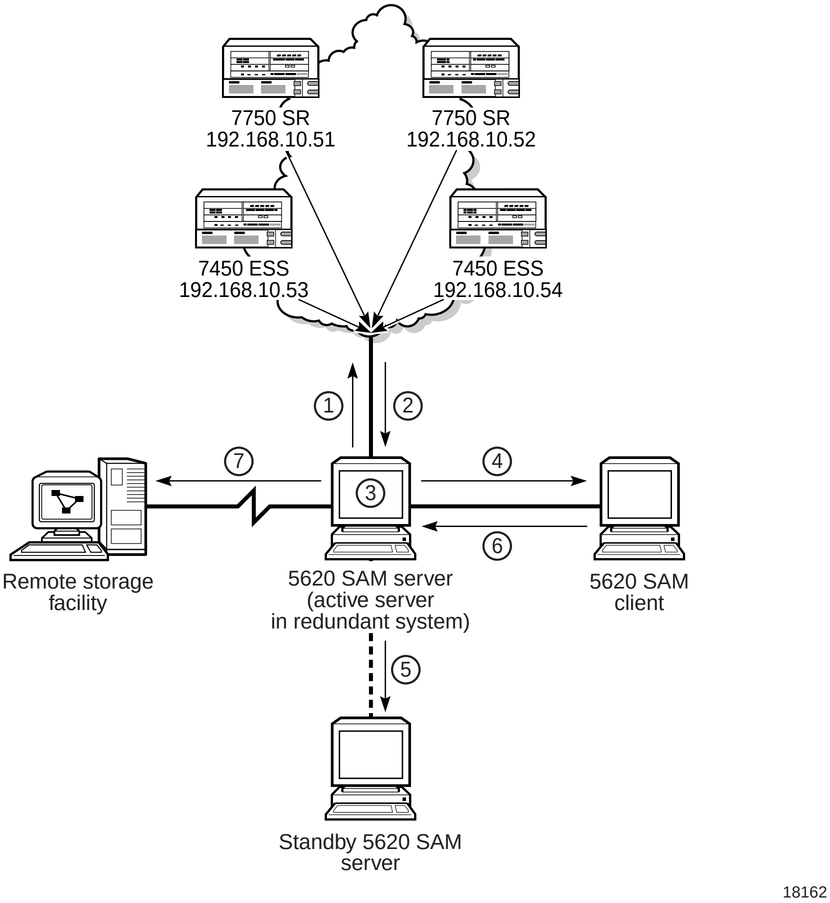


Figure 8-1 illustrates the activities of the 5620 SAM backup/restore process. The labels correspond to events in the following sequence:

1. At the interval specified—every hour in this example—the 5620 SAM issues an FTP or SCP request to all devices for a backup.
2. The devices use FTP or SCP to send the BOF and configuration files to the 5620 SAM server.
3. The 5620 SAM server stores the received files in the 5620 SAM database.
4. An operator using a 5620 SAM client uses the Backup/Restore Status tab of the Backup Policy form to view the backup status.
5. If the 5620 SAM system is a redundant configuration, the active server synchronizes the backed-up information with the standby server.
6. A 5620 SAM operator uses the Backup/Restore form to perform on-demand and scheduled device backups, restores, and configuration saves, as required.
7. A third-party application periodically sends a copy of the backup files from the 5620 SAM server to a remote storage facility for safekeeping.

8.2 Workflow to perform NE maintenance

1. For secure backups, restores and upgrades, verify that SSH2 is correctly configured on the device and that the 5620 SAM mediation policy for the device is configured for secure FTP or SCP.
2. Commission the managed devices using the CLI; see the *5620 SAM User Guide* for information.
3. Create a software upgrade policy to specify an on-demand, ISSU, or a scheduled device software image upgrade; see Procedure 8-1.
4. Configure the 5620 SAM deployment policy to specify how and when the 5620 SAM tries to send configuration changes from 5620 SAM clients to the managed devices. See Procedure 8-2 for more information.
5. Use the 5620 SAM to configure device backup or restore policies. A device backup policy specifies how often the 5620 SAM backs up the device configuration. See Procedure 8-3 for more information.
6. As required, perform on-demand NE configuration saves, imports, exports, backups, and restores of NE device files.

    a Perform an on-demand device backup, restore, or configuration save; see Procedure 8-4.

    b Import a device backup file; see Procedure 8-5.

    c Export a device backup file; see Procedure 8-6.

    d Restore a backed up device configuration; see Procedure 8-7.

    e Perform an OmniSwitch device backup; see Procedure 8-8.

    f Restore an OmniSwitch device configuration backup; see Procedure 8-9.

7. As required, configure NE rollback configuration to revert to a previous router configuration on a specified NE; see section 8.3.
8. As required, perform an on-demand software upgrade or ISSU.
    - For an 1830 PSS software upgrade, see the *5620 SAM Optical User Guide*.
    - For 7210 SAS, 7450 ESS, 7705 SAR, 7710 SR, 7750 SR, 7950 XRS, or OmniSwitch software upgrades, see section 8.4.
    - For a 9471 WMM software upgrade, see the *5620 SAM LTE ePC User Guide*.
    - For a 9500 MPR or 9500 MPRe software upgrade, see section 8.5.
    - For an eNodeB software upgrade, see the *5620 SAM LTE RAN User Guide*.

9 As required, schedule device software upgrades. Scheduled software upgrades are supported on the following NEs.

- 7210 SAS
- 7450 ESS
- 7705 SAR
- 7710 SR
- 7750 SR
- 7950 XRS
- 9500 MPR
- 9500 MPRe

i Create a 5620 SAM schedule. See Procedure 8-28 for more information. See the *5620 SAM User Guide* for information about creating 5620 SAM schedules.

ii Review the results and status of the scheduled upgrade and, as required, take the appropriate actions based on your company policies.

iii As required, manage scheduled software upgrades; see Procedure 8-29.

10 As required, activate a previously downloaded device software image on an NE. See Procedure 8-30 for more information. This is not supported on OmniSwitches.

11 As required, export a device software image from the 5620 SAM database to a file system; see Procedure 8-31.

12 View the status of various maintenance activities to confirm that ISSU or scheduled tasks occur as planned.

a Monitor software upgrade status of an NE; see Procedure 8-32.

b View the deployment, backup/restore, or software upgrade status of an NE; see Procedure 8-33.

c View the accounting statistics collection status of an NE; see Procedure 8-34.

d View the trap metrics information; see Procedure 8-35.

13 View the contents of NE file systems by opening an FTP or SSH file browser from the 5620 SAM client GUI, as required. See Procedure 8-36 and Procedure 8-37 for more information.

14 As required, troubleshoot failed configuration deployments using the 5620 SAM alarm window and the Deployment form. See Procedure 8-38 for more information.

8.3 Workflow to configure NE configuration rollback

1 Configure the storage location for the NE configuration rollback rescue file and checkpoint files; see Procedure 8-11.

2 Create the NE configuration rollback rescue file; see Procedure 8-12.

3 As required, perform one or both of the following:

a Create the NE configuration rollback checkpoint files manually; see Procedure 8-13.

b Configure scheduled checkpoint file creation; see Procedure 8-14.

4. As required, compare NE configuration rollback files with each other or with the current NE configuration file; see Procedure 8-15

5. As required, perform one or both of the following:

    a. Revert to a previous NE configuration manually; see Procedure 8-16.

    b. Configure scheduled reversion to an NE configuration rollback checkpoint file; see Procedure 8-17.

8.4 Workflow to perform a software upgrade on a 7210 SAS, 7450 ESS, 7705 SAR, 7710 SR, 7750 SR, 7950 XRS, or OmniSwitch

Caution 1 — Before you perform an ISSU, review the appropriate device release notice for more information about the device software releases that support the ISSU. The software upgrade information in the device documentation takes precedence over this procedure.

Caution 2 — Ensure that you regularly remove from the 5620 SAM device software images that are no longer required, for example, by deleting the images or by exporting to a file system. An accumulation of device software images can dramatically increase the length of database operations such as backup, restore, and reinstantiation.

1. Perform a preliminary check before you start the software upgrade.

    i. Manually verify the software image file checksums.

    ii. Verify that the device supports the new software.

    iii. Verify that there is sufficient space on the compact flash drive for the software image files.

    iv. For NEs with redundant CPMs, verify that the boot environments are synchronized by using the appropriate CLI command.

2. Download the software description file to a directory on a 5620 SAM client station.

3. Import the software description file; see Procedure 8-19.

4. Back up the device configuration. See Procedure 8-4 for 7210 SAS, 7450 ESS, 7710 SR, 7750 SR, or 7950 XRS backup information. See Procedure 8-8 for OmniSwitch backup information.

5. Perform an on-demand software upgrade or an ISSU to transfer the software image files to each NE that you need to upgrade. See Procedure 8-22 for 7210 SAS 7450 ESS, 7705 SAR, 7710 SR, 7750 SR, or 7950 XRS upgrade information. See Procedure 8-24 or Procedure 8-25 for OmniSwitch upgrade information.

6. Perform a software license upgrade to allow OS 6250SME and OS 6450 NEs to function in the Ethernet (Metro) role and support the OmniSwitch Ethernet (Metro) feature set; see Procedure 8-26.

7. After the upgrade, verify that the boot environment synchronization is successful.
8. If required, reboot the NE.
9. View the software upgrade status of the NE to verify whether the upgrade is successful. See Procedure 8-33 for more information.
10. Verify whether the transferred files and configurations are on the device by viewing the contents of the NE file systems through an FTP or SSH file browser, as required. See Procedures 8-36 and 8-37 for more information.
11. Remove obsolete software images from the device.
12. Resynchronize the NE using the 5620 SAM GUI. See the *5620 SAM User Guide* for more information.
13. As required, perform upgrade verification tests.

8.5 Workflow to perform a 9500 MPR or 9500 MPRe software upgrade

Caution — Ensure that you regularly remove from the 5620 SAM device software images that are no longer required, for example, by deleting the images or by exporting to a file system. An accumulation of device software images can dramatically increase the length of database operations such as backup, restore, and reinstantiation.

1. Create a 9500 MPR or 9500 MPRe software upgrade policy; see Procedure 8-1 for more information. Configure the FTP server details in the upgrade policy. The images are transferred to the specified FTP server; the 9500 MPR or 9500 MPRe device subsequently retrieves the image files from the FTP server.

Note — The software upgrade policy provides the 9500 MPR or 9500 MPRe device with information about the location of the new software image files.

2. Download the image package to the 5620 SAM client. Extract the package and ensure that the .DSC file is present in the same folder. When you click on the import button, the image transfer is initiated; see Procedure 8-19. The 5620 SAM copies and temporarily stores the image files. When you click on the Upgrade Sites button, the stored image files are transferred to the FTP server and retrieved by the 9500 MPR or 9500 MPRe.

Note — The software description files have a .DSC file extension. A software description file identifies the 9500 MPR or 9500 MPRe files that require an upgrade.

3 Perform a scheduled software upgrade or an on-demand software upgrade to transfer the software image files to each 9500 MPR and 9500 MPRe that you need to upgrade. See Procedure 8-27 for more information about performing an on-demand software upgrade. See Procedure 8-28 for more information about performing a scheduled software upgrade.

4 Activate the new software on each upgraded 9500 MPR or 9500 MPRe device.

8.6 NE maintenance procedures

Use the following procedures to perform NE maintenance operations.

Procedure 8-1 To create a software upgrade policy

Perform this procedure to create a policy that you can use to perform an on-demand device software upgrade, ISSU, or a scheduled device software upgrade.

Note — For information about device software downgrades, contact Alcatel-Lucent technical support.

1 Perform Procedure 8-19 to import the required device software image.

2 Ensure that the following conditions are present.

- An FTP account is configured and available on each device.
- The device configuration files are backed up, as described in Procedures 8-3 and 8-4.

3 Choose Administration→NE Maintenance→Software Upgrade from the 5620 SAM main menu. The Software Upgrade form opens.

4 Click on the Create button. The Software Upgrade Policy (Create) form opens.

5 Configure the Policy Type parameter.

6 Perform one of the following.

a If the Policy Type parameter is set to AOS Based Node, perform the following steps.

i Configure the parameters:

- Auto-Assign ID
- Policy ID
- Name
- Image Root Path
- Upgrade File Type
- Running Directory

ii Go to step 15.

b If the Policy Type parameter is set to MPR Node, go to step 13.

7 Configure the following parameters:

- Auto-Assign ID
- Policy ID
- Name
- CFlash Image Root Path
- CFlash Backup Root Path

Note 1 — You can open an FTP or SSH file browser from this form to determine the values to use for the CFlash Image Root Path and CFlash Backup Root Path parameters. Click on the FTP File Browser or SSH File Browser button, as required. If these buttons are not displayed, click on the More Actions button and choose FTP File Browser or SSH File Browser. See Procedures 8-36 and 8-37 for information about using the file browsers.

Note 2 — By default, compact flash cf3 is used to store image and backup files. Some devices do not have a cf3. Ensure that you specify a supported compact flash for the NE type when you configure the CFlash Image Root Path and CFlash Backup Root Path parameters.

8 Configure the Software Download and Software upgrade parameters to specify the actions that the 5620 SAM is to perform using the policy.

Note — If neither parameter is selected, the 5620 SAM performs no action based on the policy configuration.

9 If the Software Upgrade parameter is selected, perform one of the following to configure the Software Upgrade Options parameter.

a Select Activate and Reboot if you want the NE to reboot after the activation.

b To specify an out-of-service upgrade for a 7210 SAS or 7705 SAR that includes an NE reboot with firmware upgrade after the software activation, select Activate and Reboot with Firmware Upgrade.

Note — Depending on the device configuration, a 7210 SAS or 7705 SAR device determines whether a firmware upgrade is required, and may override the parameter setting.

c To specify an ISSU for a device with dual CPMs, select ISSU (In Service Software Upgrade).

Note — ISSUs are restricted to device maintenance releases only. See the device documentation for the supported ISSU release transitions.

10 Click on the Apply button.

11 If the Software Upgrade parameter is set to Activate and Reboot or Activate and Reboot with Firmware Upgrade, a dialog box appears; perform the following steps.

i Read the warning message.

ii To acknowledge that you understand the implications of the action, select the check box.

iii Click on the Yes button to proceed with the action.

12 Go to step 16.

13 Configure the parameters:

- Policy ID
- Name

14 Perform one of the following.

a Configure the FTP parameters:

- Transfer Protocol
- FTP User ID
- FTP Password
- FTP Server Port
- SFTP/FTP Server IP
- Root Directory
- Forced Download
- Auto-Activate After Successful File Transfer

b Configure the SFTP parameters:

- Transfer Protocol
- SFTP User ID
- SFTP Password
- SFTP Server Port
- Host Key Fingerprint
- SFTP/FTP Server IP
- Root Directory
- Forced Download
- Auto-Activate After Successful File Transfer

15 Click on the Apply button.

16 The Software Upgrade Policy (Create) form name changes to Software Upgrade Policy (Edit). Perform the following steps to assign the policy to one or more NEs.

i Click on the Software Upgrade Policy Assignment tab. The Software Upgrade Policy Filter (Edit) form opens.

ii Configure the filter parameters, if required. Click on the OK button.

iii Select one or more NEs in the Unassigned Sites list and click on the right-pointing arrow to move them to the Assigned Sites list.

iv Click on the OK button. A dialog box appears.

v Click on the Yes button. The policy is assigned to the NEs.

17 Close the Software Upgrade Policy (Edit) form. The new policy is listed on the Software Upgrade form.

18 Close the Software Upgrade form.

Procedure 8-2 To configure the 5620 SAM deployment policy

1 Choose Administration→NE Maintenance→Deployment from the 5620 SAM main menu. The Deployment form opens with the Incomplete Deployments tab displayed.

2 Click on the Deployment Policy tab.

3 Configure the parameters:

- Auto Save Scheme
- Auto Save Threshold
- Scheduled Save Scheme
- Scheduled Save Interval
- Save Details
- Configuration Save Interval
- Interval Repeat Limit
- Retry Scheme
- Retry Interval
- Retry Threshold

4 Click on the OK button. A dialog box appears.

5 Click on the Yes button. The Deployment form closes.

Procedure 8-3 To create a device backup policy

Perform this procedure to create a device backup policy and assign it to NEs. As a restore policy works implicitly with a backup, there is no explicit restore policy. The user must select the imported or pre-existing backup file and click on the Restore button.

Note — The default backup policy is assigned automatically to all 5620 SAM-managed NEs that do not currently have an assigned backup policy.

1 Choose Administration→NE Maintenance→Backup/Restore from the 5620 SAM main menu. The Backup/Restore form opens with the Backup/Restore Policy tab displayed.

2 Click on the Create button. The Backup Policy (Create) form opens.

3 Specify whether backup functionality is enabled.

  a Enable the Enable Backup parameter.

  b Disable the Enable Backup parameter. The remaining parameters on the form cannot be configured. Go to step 15.

4 Configure the following parameters:

- Policy ID
- Auto-Assign ID
- Name
- Policy Type

5 If you selected AOS Based Node policy type, go to step 7.

6 Specify whether to perform a reboot after the configuration is restored to the device by specifying the Auto-Reboot After Successful Restore parameter.

> **Caution —** When you use the 5620 SAM client GUI to restore a managed device configuration and you disable the Auto-Reboot After Successful Restore parameter, there is a risk that the bof.cfg file may be overwritten in the following situations:
>
> - when a user performs “bof save” using CLI on the managed device
> - If there is a gap between a restore and a reboot, perform a “show bof” to ensure that another user has not performed a “bof save”.
>
> For the 9500 MPR or 9500 MPRe, you must enable the Auto-Reboot After Successful Restore parameter in order for the restored database to be activated on the NE after the reboot. If the Auto-Reboot After Successful Restore parameter is not enabled, the restored database will not be activated on the NE after the reboot or when the NE is rebooted at a later date.

7 You can schedule backups based on a time interval or on the number of NE configurations performed from the 5620 SAM server. Configure the backup triggering parameters:

- Scheduled Backup Scheme
- Scheduled Backup Interval
- Scheduled Backup Sync Time
- Scheduled Backup Threshold (operations)
- Auto Backup Scheme
- Auto Backup Threshold (operations)

8 Perform one of the following:

- **a** If you selected SR Based Node policy type, go to step 9.
- **b** If you selected AOS Based Node policy type, go to step 11.
- **c** If you selected MPR Based Node policy type, go to step 13

Note 1 — See the *5620 SAM LTE RAN User Guide* for more information on creating a backup policy for an eNodeB.

Note 2 — See the *5620 SAM Optical User Guide* for more information on creating a backup policy for an 1830 PSS.

Note 3 — See the *5620 SAM LTE ePC User Guide* for more information on creating a backup policy for a 7750 MG.

9 Configure the Backup Settings parameters:

- CLI Config File Mode
- CLI Config Save Details
- CLI Debug Save Config File Mode
- Boot Option File Mode
- File Compression
- Backup 7705 Radio Database

Note 1 — In addition to enabling the CLI Debug Save Config File Mode parameter, you must specify the location of the debug configuration files in the 5620 SAM main server configuration. See chapter 5 for more information.

Note 2 — If the Backup 7705 Radio Database parameter is enabled, the 9500 MPT radio databases are backed up along with the configuration file, depending on the CLI Config File Mode setting. The backup of the 9500 MPT radio databases is only supported on the 7705 SAR-8 or 7705 SAR-18.

10 Go to step 14.

11 Configure the AOS Backup Settings parameters:

- Save Certified Directory
- Save Network Directory
- File Compression
- Command to Apply After Backup

Note — The 5620 SAM can only backup configuration files stored in the certified directory. If you need to backup configuration files in the working directory, you must ensure that the files in the certified and working directories are identical. See the *5620 SAM User Guide* to perform a Certify or Certify and Synchro command before you backup the OmniSwitch configuration files.

12 Go to step 14.

13 Configure the MPR Backup Settings parameters:

- Save Certified Directory
- File Compression

14 Configure the parameters in the Backup Purging panel. Backup purging parameters allow you to specify the number of backup files kept. These settings allow you to eliminate manual monitoring and deletion of backup files. The purge criteria can be the number of files, the age of the files, or both.

- Auto-Purge Scheme
- Number of Backups
- Maximum Backup Age (days)

15 Click on the OK button to save the backup policy. The Backup Policy (Create) form closes.

16 Assign the policy to NEs as required.

i Select the new policy in the list and click on the Properties button. The Backup Policy (Edit) form opens.

ii Click on the Backup/Restore Policy Assignment tab. The Backup Policy (Edit) Filter form opens.

iii Configure an advanced search, if required.

iv Click on the OK button. The Backup Policy (Edit) Filter form closes and the filtered NEs appear in the Unassigned Sites or Assigned Sites lists.

v Select one or more NEs in the Unassigned Sites list and click on the right-pointing arrow to move them to the Assigned Sites list.

vi Click on the OK button. The Backup Policy (Edit) form closes and a dialog box appears.

vii Click on the Yes button. The policy is assigned to the NEs.

17 The 5620 SAM creates the backup based on the specified schedule.

You can optionally perform the backup immediately. See Procedure 8-4 for more information.

18 Close the Backup/Restore form.

Procedure 8-4 To perform an on-demand device backup, restore, or configuration save

When you start an on-demand backup, you back up the device configuration based on the backup policy associated with the NE.

A device configuration restore operation uses the most recently backed-up device configuration file unless otherwise specified. See Procedure 8-7 for more information.

The following conditions must be present before you can perform a device configuration backup, restore, or configuration save:

- You have a 5620 SAM user account with an administrator or network element software management scope of command role or a scope of command role with write access to the mediation package. See chapter 2 for more information about scope of command roles.
- FTP or secure FTP is configured in the mediation policy for the NE. See the *5620 SAM User Guide* for more information.
- The BOF persist parameter is set on the 7210 SAS, 7450 ESS, 7710 SR, 7750 SR, or 7950 XRS. See the *5620 SAM User Guide* for information about device commissioning.

Depending on the operation type, the Backup State or Restore State column displays the current state of the operation. The possible values are:

- Not Attempted - the operation is unattempted
- Saving Config - the device configuration is being saved on the device
- Transferring Files - a file transfer is in progress
- Success - the operation is complete and successful
- Failure - the operation is complete but unsuccessful
- CPM Sync and Pending Reboot - the device configuration is restored and the device is synchronizing the CPMs before it reboots
- CPM Sync and Pending Reboot Standby - the 5620 SAM is waiting for the reboot of the standby CPM
- Standby Reboot and Pending Redundant Switch-over - the 5620 SAM is waiting for the switchover to the standby CPM

Note — During a backup, if a device is unresponsive to the 5620 SAM because SNMP on the device is disabled, the Backup State column entry for the device does not immediately display the correct value of Failed. This latency is caused by the inability of the 5620 SAM to communicate with the unresponsive device. In such a situation, the Backup State column displays the initial value of Saving Config until three 10-minute SNMP polling periods, or 30 minutes, have elapsed, after which the Backup State changes to Failed if SNMP remains disabled.

1. Choose Administration→NE Maintenance→Backup/Restore from the 5620 SAM main menu. The Backup/Restore form opens.

2. Click on the Backup/Restore Status tab. The managed devices are listed.

3. Select a device from the list and click on the Backup button, the Restore button, or the Save Config button, depending on the operation that you need to perform. A dialog box appears.

4. Click on the Yes button. The backup or restore operation starts, and the current backup or restore state for the device is indicated in the Backup State or Restore State column.

5 You can resynchronize an NE with the 5620 SAM database, if required, by clicking on the Resync button. See the *5620 SAM User Guide* for information about resynchronizing an NE.

6 Close the Backup/Restore form.

Procedure 8-5 To import a device backup to the 5620 SAM database

1 Choose Administration→NE Maintenance→Backup/Restore from the 5620 SAM main menu. The Backup/Restore form opens with the Backup/Restore Policy tab displayed.

2 Click on the Backup/Restore Status tab.

3 Select the NE in the list for which you are importing a backup and click on the Properties button. The NE Backup/Restore Status form opens.

4 Click on the Import button. If the Import button is not visible, click on the More Actions button and choose Import. A file navigator form opens.

5 Use the form to specify the directory that contains the device backup and click on the OK button.

If the directory contains a backup for this NE, the 5620 SAM imports the backup files into the 5620 SAM database and the import is successful. Otherwise, a dialog box appears if the directory does not contain a backup from this NE, and the import fails. Click on the OK button to close the dialog box.

6 Close the NE Backup/Restore Status form.

7 Close the Backup/Restore form.

Procedure 8-6 To export a device backup to a file

1 Choose Administration→NE Maintenance→Backup/Restore from the 5620 SAM main menu. The Backup/Restore form opens with the Backup/Restore Policy tab displayed.

2 Click on the Backup/Restore Status tab.

3 Select the NE in the list for which you are exporting a backup and click on the Properties button. The NE Backup/Restore Status form opens.

4 Click on the Backups tab. A list of backups for the NE is displayed.

5 Select a backup in the list and click on the Export button. A file navigator form opens.

6 Use the form to specify the directory that is to contain the exported device backup and click on the OK button. The NE configuration backup is saved to the specified directory.

7. Close the NE Backup/Restore Status form.
8. Close the Backup/Restore form.

Procedure 8-7 To restore a device configuration backup other than the most recent

You can choose to restore an older version of the device configuration to meet special network requirements.

Caution 1 — Older backups do not have the most recent network information. Restoring an older device configuration may be service-affecting.

Caution 2 — Ensure that you back up the current device configuration using Procedure 8-3 before you proceed.

1. Choose Administration→NE Maintenance→Backup/Restore from the 5620 SAM menu. The Backup/Restore form opens.
2. Click on the Backup/Restore Status tab. The managed devices are listed.
3. Double-click on a device from the list. The NE Backup/Restore Status form for the selected device opens.
4. Click on the Backups tab. A list of configuration backups for the selected device opens, ordered from the oldest to the most recent.
5. Select a backup in the list and click on the Restore button. A dialog box appears.
6. Click on the Yes button.
7. Click on the Resync button to ensure the latest network information is available, if required.
8. Close the Backup/Restore form.

Procedure 8-8 To perform a device backup on an OmniSwitch

1. Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.
2. Expand the OmniSwitch icon and right-click on an OmniSwitch shelf object in the equipment view and choose Properties from the contextual menu. The Shelf (Edit) form opens with the General tab displayed.
3. Click on the Software Control Module tab.

4 Set the Command to Apply parameter to Certified.

Note — You must perform a Resync to the NE to make sure the "/flash/working" and "/flash/certified" directories are the same even though the Certified Status field is shown as Certified.

5 Click on the Resync button. A dialog box appears. Click on the Yes button.

6 Click on the OK button to apply the changes. A dialog box appears. Click on the Yes button. The Shelf (Edit) form closes.

7 Choose Administration→NE Maintenance→Backup/Restore from the 5620 SAM menu. The BackupRestore form opens with the Backup/Restore Policy tab displayed. The default backup/restore policies are listed on the Backup/Restore Policy tab.

8 Perform one of the following:

- **a** To use the default AOS backup/restore policy for the backup without modifications, go to step 9.
- **b** To use the default AOS backup/restore policy for the backup with modifications, choose a policy and click on the Properties button. Modify the policy as required. Go to step 9.
- **c** To create a backup/restore policy, click on the Create button. See Procedure 8-1 for more information.

9 Click on the Backup/Restore Status tab. A list of NEs for which backups can be performed on and any previous backup information appears.

10 Choose the device that you need to back up and click on the Backup button. A dialog box appears.

11 Click on the Yes button. The backup runs and the success or failure of the backup is indicated in the Last Operation Details column.

12 If required, export a copy of the backup to a local drive by clicking on the Save Config button.

Procedure 8-9 To restore a configuration backup on an OmniSwitch

Note 1 — You can import the locally available backup file for the same NE to the 5620 SAM which can be restored. Ensure the backup policy remains the same as was in place during the backup procedure. This will prevent the 5620 SAM from generating an error while importing the file.

Note 2 — The restored backup configuration is stored on a working directory. Success indicates that the file is successfully transferred to the appropriate NEs. However, the file will not become active until the device(s) have been reloaded from the working directory.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Expand the OmniSwitch icon and right-click on an OmniSwitch shelf object in the equipment view and choose Properties from the contextual menu. The Shelf (Edit) form opens with the General tab displayed.

3 Click on the Software Control Module tab.

4 Set the Command to Apply parameter to Reload.

5 If required, configure the Delayed Activation Timer and Redundancy Time (seconds) parameters.

6 Configure the Image Files Directory parameter.

7 Click on the OK button. A dialog box appears. Click on the Yes button. The Shelf (Edit) form closes.

8 Choose Administration→NE Maintenance→Backup/Restore from the 5620 SAM main menu. The BackupRestore form opens with the Backup/Restore Policy tab displayed with a list of the default backup/restore policies.

9 Perform one of the following:

- **a** To use the default AOS backup/restore policy for the backup without modifications, go to step 10.
- **b** To use the default AOS backup/restore policy for the backup with modifications, choose a policy and click on the Properties button. Modify the policy as required. Go to step 10.
- **c** To create a backup/restore policy, click on the Create button. See Procedure 8-1 for more information.

10 Click on the Backup/Restore Status tab. A list of NEs for which restores can be performed on and any previous restore information appears.

11 Choose the device that you need to restore and click on the Restore button. A dialog box appears.

12 Click on the Yes button. The restore runs and the success or failure of the restore is indicated in the Last Operation Details column.

13 Verify that the Command to Apply parameter is set to Certified. See steps 1 to 4 of Procedure 8-8.

Procedure 8-10 To certify or synchronize OmniSwitch software

1 Choose Administration→NE Maintenance→OMNI Software Maintenance from the 5620 SAM main menu. The OMNI Software Maintenance form opens.

2 Configure the search filter criteria and click on the Search button. A list of OmniSwitch devices appear.

3 Perform one of the following:

  a Select one or more NEs from the list and click on the Certify button. Go to step 7.

  b Select one or more NEs from the list and click on the Certify and Synchronize button. Go to step 7.

  c Select one or more NEs from the list and click on the Flash Synchronization button. Go to step 7.

  d Select one or mode NEs from the list and click on the Properties button. The Software Control Module (Edit) form opens.

4 Configure the Command to Apply parameter.

5 If the Command to Apply parameter was set to Reload, configure the Delayed Activation Timer parameter.

6 Click on the OK button. The Software Control Module (Edit) form closes.

7 Close the OMNI Software Maintenance form.

Procedure 8-11 To configure an NE configuration rollback file storage location

Use this procedure to configure the storage location for the NE configuration rollback rescue file or checkpoint files. To configure NE configuration rollback file storage locations FTP must be configured on the device; see the *5620 SAM User Guide* for more information.

1 Choose Administration→NE Maintenance→NE Configuration Rollback from the 5620 SAM main menu. The NE Configuration Rollback form opens with the Rollback Policy tab displayed.

2 Click the NE Rollback tab. The NE Rollback list form opens.

3 Choose a device and click on the Properties button. The NE Rollback (Edit) form opens.

4 Perform one or both of the following:

a To configure the storage location for the NE configuration rollback rescue file, go to step 5.

b To configure the storage location for the NE configuration rollback checkpoint files, go to step 6.

5 To configure the rescue file storage location:

i In the Rescue File panel, configure the Rescue File Location Type parameter:

- If you specified FTP, in the Rescue File — Remote Location panel, configure the parameters:
    - FTP User ID
    - FTP User Password
    - FTP Server IP
    - File Path
- If you specified CFLASH, in the Rescue File — CFLASH panel, configure the parameters:
    - Compact Flash
    - File Path

ii Click on the Apply button. A dialog box appears.

iii Click on the Yes button.

6 To configure the checkpoint files storage location:

i In the Checkpoint File Storage panel, configure the parameters:

- Maximum # of Local Checkpoint Files
- Maximum # of Remote Checkpoint Files

ii Configure the Rollback Location Type parameter:

- If you specified FTP, in the Checkpoint File Storage — Remote Location panel, configure the parameters:
    - FTP User ID
    - FTP User Password
    - FTP Server IP
    - File Path
- If you specified CFLASH, in the Checkpoint File Storage — CFLASH panel, configure the parameters:
    - Compact Flash
    - File Path

iii Click on the Apply button. A dialog box appears.

iv Click on the Yes button. The Checkpoint Files tab lists the checkpoint files.

7. Close the NE Rollback (Edit) form.

8. Close the NE Configuration Rollback list form.

Procedure 8-12 To create the NE configuration rollback rescue file

The rollback rescue file storage location must be configured before you can create the NE configuration rollback rescue file; see Procedure 8-11.

1. Choose Administration→NE Maintenance→NE Configuration Rollback from the 5620 SAM main menu. The NE Configuration Rollback form opens with the Rollback Policy tab displayed.

2. Click the NE Rollback tab. The NE Rollback list form opens.

3. Choose a device from the list and click on the Properties button. The NE Rollback (Edit) form opens.

4. Click on the Create Rescue File button. A dialog box appears.

5. Click on the Yes button. The rescue file is saved to the specified file location. The Delete Rescue File, View Rescue File, and Revert to Rescue File buttons are enabled.

Note — If a rescue file exists, the Rescue File Exists parameter is enabled, and the dialog box prompts you to confirm that you need to overwrite the existing rescue file.

6. Close the NE Rollback (Edit) form.

7. Close the NE Configuration Rollback list form.

Procedure 8-13 To create NE configuration rollback checkpoint files

The checkpoint file storage location must be configured before you can create NE configuration rollback checkpoint files; see Procedure 8-11. You can also automate NE configuration rollback checkpoint file creation; see Procedure 8-14.

1. Choose Administration→NE Maintenance→NE Configuration Rollback from the 5620 SAM main menu. The NE Configuration Rollback form opens with the Rollback Policy tab displayed.

2. Click the NE Rollback tab. The NE Rollback list form opens.

3. Choose a device and click on the Properties button. The NE Rollback (Edit) form opens.

4. Click on the Checkpoint Files tab.

5 Click on the Create button. A dialog box appears.

6 Click on the Yes button. The Create Checkpoint form opens.

7 If required, add a comment to the checkpoint file. Click on the OK button. The comment dialog box closes.

8 Click on the OK button. The Create Checkpoint form opens and the checkpoint is added to the list form on Checkpoint Files tab.

9 If required, enable redundant rollback synchronization between the active and standby CPM.

> **Note —** You can enable redundant rollback synchronization only when the following conditions are met.
>
> - The rollback file location is CFLASH.
> - The device has a standby CPM.

i Click on the General tab.

ii Perform one of the following:

- To configure automated redundant rollback synchronization, select the Redundant Rollback Synchronization check box.
- To perform manual redundant rollback synchronization, click on the Rollback-Sync Now button.

10 Close the NE Rollback (Edit) form.

11 Close the NE Configuration Rollback list form.

Procedure 8-14 To configure scheduled checkpoint file creation

See the *5620 SAM User Guide* for more information about scheduling. You can also create NE configuration rollback checkpoint files manually; see Procedure 8-13.

1 Choose Administration→NE Maintenance→NE Configuration Rollback from the 5620 SAM main menu. The NE Configuration Rollback form opens with the Rollback Policy tab displayed.

2 Perform one of the following:

a Use the filters to search for and open a policy by choosing a policy and clicking on the Properties button. The Rollback Policy (Edit) form opens.

b Click on the Create button. The Rollback Policy (Create) form opens.

3 Configure the parameters:

- Policy ID
- Auto-Assign ID
- Policy Name
- Policy Description

4 Click on the Apply button. The Rollback Policy (Edit) form opens with the configured values.

5 In the Checkpoint File Creation panel, click on the Create button. The Checkpoint Create Scheduled Task (Create) form opens.

6 Configure the parameters:

- Scheduled Task Name
- Scheduled Task Description
- Checkpoint Comment
- Administrative State

7 Click on the Select button beside the ID parameter. The Select Schedule - Checkpoint Create Scheduled Task form opens.

8 Perform one of the following:

a Click on the Create button to create a schedule. The SAM Schedule (Create) form opens.

b Choose an existing schedule.

9 Click on the OK button. The Checkpoint Create Scheduled Task (Create) form refreshes with the schedule information.

10 Click on the OK button. The Checkpoint Create Scheduled Task (Create) form closes and the Rollback Policy (Edit) form refreshes with the schedule information.

11 Assign the NE rollback policy to NEs as required.

i Click on the NEs Assignment tab. The Rollback Policy (Edit) Filter form opens.

ii Configure an advanced search if required.

iii Click on the OK button. The Rollback Policy (Edit) Filter form closes and the filtered NEs appear in the Unassigned Sites or Assigned Sites lists.

iv Choose one or more NEs in the Unassigned Sites list and click on the right-pointing arrow to move the NEs to the Assigned Sites list.

Note — 5620 SAM supports up to five simultaneous NE rollback reverts/rescues.

- **v** Click on the OK button. A dialog box appears.
- **vi** Click on the Yes button. The Rollback Policy (Edit) form closes and the policy is assigned to the NEs.

12 Close the NE Configuration Rollback list form.

Procedure 8-15 To compare NE configuration rollback files

Use this procedure to compare NE configuration rollback files with each other or with the current NE configuration file.

1 Choose Administration→NE Maintenance→NE Configuration Rollback from the 5620 SAM main menu. The NE Configuration Rollback form opens with the Rollback Policy tab displayed.

2 Click the NE Rollback tab. The NE Rollback list form opens.

3 Choose a device and click on the Properties button. The NE Rollback (Edit) form displays.

4 Click on the Checkpoint Files tab. The Checkpoint File list form displays.

5 Perform one of the following:

- **a** To compare the NE configurations of two checkpoint files:
  - **i** Choose two checkpoint files.
  - **ii** Click on the Compare File button and choose Checkpoint Vs Checkpoint.
- **b** To compare the NE configurations of a checkpoint file and the active configuration:
  - **i** Choose a checkpoint file.
  - **ii** Click on the Compare File button and choose Checkpoint Vs Active-Configuration.
- **c** To compare the NE configurations of a checkpoint file and the rescue file:
  - **i** Choose a checkpoint file.
  - **ii** Click on the Compare File button and choose Checkpoint Vs Rescue.
- **d** To compare the NE configuration of the current configuration and the rescue file, click on the Compare File button and choose Active-Configuration Vs Rescue.

The Checkpoint Compare window opens listing differences between the selected configuration files; see “Comparing configuration files” in this chapter for more information.

6 Close the Checkpoint Compare window.

7 Close the NE Rollback (Edit) form.

8 Close the NE Configuration Rollback list form.

Procedure 8-16 To revert to a previous NE configuration

Use this procedure to revert to a previous NE configuration without rebooting the system. You can automate NE configuration reversion for NE configuration rollback checkpoint files; see Procedure 8-17.

1 Choose Administration→NE Maintenance→NE Configuration Rollback from the 5620 SAM main menu. The NE Configuration Rollback form opens with the Rollback Policy tab displayed.

2 Click the NE Rollback tab. The NE Rollback list form opens.

3 Choose a device and click on the Properties button. The NE Rollback (Edit) form opens.

4 Perform one of the following:

  a To revert to the NE configuration rollback rescue file, go to step 6.

  b To revert to the NE configuration rollback checkpoint files, go to step 7.

5 Click on the Revert to Rescue File button. A dialog box appears.

6 Click on the OK button. Go to step 10.

7 Click on the Checkpoint Files tab.

8 Choose a checkpoint file and click on the Revert Checkpoint File button. A dialog box appears.

9 Click on the OK button.

10 Close the NE Rollback (Edit) form.

11 Close the NE Configuration Rollback list form.

Procedure 8-17 To configure scheduled NE rollback configuration checkpoint reverts

Use this procedure if, for example, you need different NE configurations for weekdays versus weekends. See the *5620 SAM User Guide* for more information about scheduling. You can also revert to a previous NE configuration manually; see Procedure 8-16.

1. Choose Administration→NE Maintenance→NE Configuration Rollback from the 5620 SAM main menu. The NE Configuration Rollback form opens with the Rollback Policy tab displayed.
2. Click the NE Rollback tab. The NE Rollback list form opens.
3. Choose a device and click on the Properties button. The NE Rollback (Edit) form opens.
4. Click on the Checkpoint Files tab.
5. Choose a checkpoint file and click on the Schedule Revert button. The Checkpoint Revert Scheduled Task (Create) form opens.

Note — If a scheduled task exists, the Schedule Revert button is unavailable.

6. Configure the parameters:
   - Scheduled Task Name
   - Scheduled Task Description
   - Administrative State
7. Click on the Select button beside the ID parameter. A Select Schedule - Checkpoint Revert Scheduled Task form opens.
8. Perform one of the following:
   - **a** Click on the Create button to create a schedule. A Schedule (Create) form opens.
   - **b** Choose an existing schedule.
9. Click on the OK button. The Checkpoint Revert Scheduled Task (Create) form refreshes with the schedule information.
10. Click on the OK button. The Checkpoint Revert Scheduled Task (Create) form closes and the NE Rollback (Edit) form reappears.
11. Close the NE Rollback (Edit) form.
12. Close the NE Configuration Rollback list form.

Procedure 8-18 To view NE configuration files

Use this procedure to view NE configuration rollback rescue files and checkpoint files, or the current NE configuration file.

1 Choose Administration→NE Maintenance→NE Configuration Rollback from the 5620 SAM main menu. The NE Configuration Rollback form opens with the Rollback Policy tab displayed.

2 Click the NE Rollback tab. The NE Rollback list form opens.

3 Choose a device and click on the Properties button. The NE Rollback (Edit) form opens.

4 Perform one of the following:

- **a** To view to the NE configuration rollback rescue file, go to step 5.
- **b** To view the NE configuration rollback checkpoint files or the active configuration file, go to step 6.

5 Click on the View Rescue File button. The Rescue View window opens. Go to step 9.

6 Click on the Checkpoint Files tab.

7 Choose a checkpoint file and click on the View File button.

8 Choose an option from the drop-down menu. The *[option]* View window opens.

9 Close the *[option]* View window.

10 Close the NE Rollback (Edit) form.

11 Close the NE Configuration Rollback list form.

Procedure 8-19 To import device software image or description files to the 5620 SAM database

Perform this procedure to import a set of device software files or 9500 MPR/9500 MPRe software description files into the 5620 SAM database for use during device software upgrades.

1 Make the new device software files available to the 5620 SAM.

i If the device software files are compressed in an archive, for example, a TiMOS ZIP file, extract the files from the archive to an empty directory. The directory contents must have one of the following structures:

- flat—all files are in one directory, and there are no subdirectories
- tiered—the directory contains a boot loader file and a subdirectory contains the software image files; for example, if you are importing a set of 7750 SR files and you extract the files to /ExtractDir, the structure is the following:

  /ExtractDir/cflash contains boot.ldr

  /ExtractDir/cflash/*X.x.Rx* contains the following files:
  - both.tim
  - cpm.tim

where *X.x.Rx* is the software release identifier

When you import the software, you must specify the parent software directory, which in the example is the cflash directory.

Note 1 — The type of directory structure in a device software archive depends on the device type and release.

Note 2 — Release 8.0 and later 7450 ESS, 7710 SR, and 7750 SR devices use a common software image with a Product Name of Alcatel-SR/ESS-7XXX.

Note 3 — If you are importing a device software image for the 7705 SAR-8, 7705 SAR-8 CSMv2, or 7705 SAR-18, Release 6.0 R1 or later, the TiMOS ZIP file contains a pkgs directory with an MPT subdirectory.

ii Copy or move the files to a location that is accessible to the 5620 SAM.

Note 1 — Alcatel-Lucent recommends that all OmniSwitch software image files, including any optional and boot files, are available in the specified directory for importing to the 5620 SAM database.

Note 2 — 9500 MPR devices require only the software description (.DSC) files to be available for importing into the 5620 SAM database.

2 Choose Administration→NE Maintenance→Software Upgrade from the 5620 SAM main menu. The Software Upgrade form opens with the Software Upgrade Policy tab displayed.

3 Click on the Software Images tab.

4 Click on the appropriate tab for the type of NE that you need to upgrade.

5 Click on the Import button. The Open form opens.

6 Navigate to directory that contains the software image and click on the Open button.

Note — If the directory structure is tiered, you must navigate to the directory that contains the boot loader file. For the example in step 1, this directory is the cflash directory.

The 5620 SAM verifies the file set, imports the files to the 5620 SAM database, and displays an entry for the imported image in the list.

7 If the directory does not contain only the required files, a dialog box appears. Perform the following steps.

  i Click on the OK button.

  ii Copy or move files, as required, to ensure that the directory contains only the files required for the upgrade.

  iii Go to step 5.

8 Close the Software Upgrade form.

Procedure 8-20 To perform a soft reset of an IOM, IMM, or XCM

Use this procedure to perform a manual soft reset of one of the following:

- an IOM, IOM3, or IMM in a 7450 ESS or 7750 SR
- an FP3 line card in a Release 11.0 or later 7450 ESS or 7750 SR
- an XCM in a Release 11.0 R6 or later 7950 XRS

Note 1 — Soft reset is supported only under the following conditions:

- The IOM or XCM is operationally up.
- The IOM or XCM is supported.
- The MDAs or XMAs are Ethernet MDAs but not HSMDAs, and are provisioned.

Note 2 — MDAs that do not support soft reset are hard rebooted during the soft reset.

1 To select an IOM or XCM, choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Navigate to the card slot object. The path is Network→*NE*→Shelf→Card Slot *n*.

3 Right-click on the card slot icon and choose Soft Reset. A Warning form opens.

4 View the dependency information.

5 Select the I understand the implications of this action check box.

6 Click on the Yes button. The operational state of the IO card displays the soft reset status when the soft reset is in progress.

Procedure 8-21 To perform a hard reboot of an IOM or XCM

Use this procedure to perform a manual hard reboot of an IOM or XCM.

1 To select the IOM or XCM, choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Navigate to the card slot object. The path is Network→*NE*→Shelf→Card Slot *n*.

3 Right-click the card slot icon and choose Properties. The Card Slot (Edit) form opens with the General tab displayed.

4 Click on the IO Card tab.

5 Click on the Reboot button. If the Reboot button is not visible, click on the More Actions button and choose Reboot. The operational state of the IO card displays the hard reboot status when the hard reboot is in progress.

6 Close the Card Slot form.

Procedure 8-22 To perform an ISSU or on-demand software upgrade on a 7210 SAS, 7450 ESS, 7705 SAR, 7710 SR, 7750 SR, or 7950 XRS

Perform this procedure to upgrade the device software on one or more NEs. The following must be true before you attempt a device software upgrade.

- You have a 5620 SAM user account with an administrator or network element software management scope of command role or a scope of command role with write access to the mediation package. See chapter 2 for more information about scope of command roles.
- The FTP or secure FTP credentials are configured in the NE mediation policy. See the *5620 SAM User Guide* for more information.

Warning — A device may require a firmware upgrade before a software upgrade. To avoid a service outage, ensure that the device firmware version supports the software version. See the device software Release Notes for information about firmware and software version compatibility and the firmware upgrade procedure.

Caution 1 — Alcatel-Lucent recommends that you open a physical console session on the device that you need to upgrade. The console session allows you to monitor the upgrade and recover in the event of an upgrade failure.

Caution 2 — Read the software upgrade information in the device documentation before you perform a software upgrade.

Caution 3 — Before you attempt an ISSU, see the appropriate device release notice and the *5620 SAM Network Element Compatibility Guide* for information about the supported upgrade paths. See section 8.1 for general ISSU information.

Caution 4 — You cannot upgrade a device to a release that is chronologically older than the currently installed release. For example, you cannot upgrade from Release 10.0 R8 to 11.0 R1, because Release 11.0 R1 predates Release 10.0 R8. See the *5620 SAM Network Element Compatibility Guide* for information about the supported upgrade paths.

Note 1 — If you downgrade a device software image, you must unmanage and delete the device before you perform the downgrade, as described in the *5620 SAM User Guide*. Contact Alcatel-Lucent technical support for information about device downgrades.

Note 2 — If you attempt to upgrade a 7950 XRS, Release 11.0 R3 or earlier to Release 11.0 R4 or later, the 5620 SAM raises a NodeVersionMismatch alarm. You must manually unmanage and remanage the node after performing the upgrade. The same action is required if you attempt to downgrade a 7950 XRS, Release 11.0 R4 or later to Release 11.0 R3 or earlier.

Note 3 — The 5620 SAM does not support an upgrade of the 7705 SAR-H, Release 5.0 to Release 6.1. You must first unmanage the 7705 SAR-H using the 5620 SAM and then perform an upgrade using CLI. You can use the 5620 SAM to manage the NE after the upgrade.

Note 4 — If you are performing a major ISSU from a release prior to Release 10.0 R12, you must provide the correct username and password credentials for the CLI Communication Protocol in the mediation policy. This ensures that the support.tim file is copied from the active CPM to the standby CPM.

1 Perform the following steps.

  i Verify that the device supports the new software.

  ii Manually verify the software image file checksum.

  iii Verify that the device file system has space for the software image file.

  iv For NEs with redundant CPMs, verify that the boot environments are synchronized by using the appropriate CLI command.

  v Configure the appropriate software upgrade policy, as described in Procedure 8-1; assign the policy to the NEs that you need to upgrade.

2 Back up the device configuration. See Procedure 8-4.

3 Choose Administration→NE Maintenance→Software Upgrade from the 5620 SAM main menu. The Software Upgrade form opens.

4 Click on the Software Images tab.

5 Choose a software image in the list and click on the Import button. The Open window appears.

6 Navigate to the directory that contains the software image, select the image, and click on the Open button.

> **Note 1 —** The directory must contain only the files required for the upgrade.
>
> **Note 2 —** The 7450 ESS, 7710 SR, 7750 SR, and 7950 XRS use a common software image. The Product Name field displays Alcatel-SR/ESS-7XXX to indicate that the software image is common to multiple devices.
>
> **Note 3 —** If you are upgrading a 7705 SAR-8 or 7705 SAR-18, Release 6.0 R1 or later, there are two images; one image contains the boot.ldr and both.tim, and the second image contains the MWA files in the pkgs/MPT folder. If the image version is 6.0 and contains the MPT files, the MPT Image Software Version is displayed on the Software Image form. If the image folder does not contain MPT packages, the MPT Image Software Version shows N/A.

7 If the directory contains only the required files, the 5620 SAM imports the files to the 5620 SAM database, and an entry for the image is listed on the Software Upgrade form. Go to step 9. Otherwise, a dialog box appears.

8 Perform the following steps.

- **i** Click on the OK button.
- **ii** Move files out of the directory until the directory contains only the files required for the upgrade.
- **iii** Go to step 5.

9 Click on the Upgrade Sites button. A list of NEs is displayed. Only the devices that support the software image are listed.

10 Choose one or more NEs in the list.

11 Click on the OK button. The software upgrade begins.

12 Click on the Software Upgrade Status tab to view the upgrade progress.

13 If the Software Upgrade parameter in the software upgrade policy is not selected, you must activate the image on each NE and then reboot each NE. Perform the following steps.

> **Caution —** Rebooting an NE that is in service is service-affecting. Ensure that you perform the reboot only during a scheduled maintenance period.

Note 1 — Some device software upgrades, for example, ISSUs, do not require a reboot. See the device documentation for more information.

Note 2 — When you perform an ISSU, you can manually soft reset or hard reboot the IOMs or IMMs after the upgrade. A soft reset results in minimal downtime, but has restricted support. See Procedure 8-20 to perform a manual soft reset, or Procedure 8-21 to perform a manual hard reboot.

Note 3 — For 7710 SR MDAs, CMAs, and MCMs, the device performs the required resets automatically after an ISSU.

Note 4 — When the IOMs are not manually soft reset or hard rebooted, the device performs a soft reset, if supported, after two hours; otherwise, the device performs a hard reboot after two hours.

i Select the NEs that are to be upgraded.

ii Click on the Software Images tab. A list of software images on the selected NEs is displayed.

iii Select the required software image in the list and click on the Activate Image button. A dialog box appears.

iv Click on the Yes button. The software image is activated on each NEs.

v Click on the Software Images tab to monitor the activation progress.

vi Wait until the image activation completes.

vii Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

viii Navigate to the shelf object. The path is Network→*NE*→Shelf.

ix Right-click the shelf icon and choose Reboot or Reboot Upgrade. A dialog box appears.

Note — Only the 7210 SAS and 7705 SAR support the Reboot Upgrade option.

x Click on the Yes button. The NE reboots.

14 Verify the upgrade success, as described in Procedure 8-33.

15 Use the 5620 SAM FTP or SSH file browser to verify that the transferred files and configuration are on each upgraded NE. See Procedure 8-36 for information about using the FTP file browser. See Procedure 8-37 for information about using the SSH file browser.

16 Resynchronize each upgraded NE.

Procedure 8-23 To upgrade the ISA-AA MDA software

Perform this procedure to upgrade only the ISA-AA MDA software on an NE, for example, when the new software includes new AA protocol signatures.

Note 1 — You cannot use the procedure to upgrade between major releases; only minor-release ISA-AA upgrades within the same major release are supported.

Note 2 — An ISA-AA MDA software upgrade is an in-service upgrade that does not require an NE reboot. Although the Software Upgrade parameter in the associated software upgrade policy must be selected for the image activation and upgrade to occur, the Software Upgrade Options in the policy do not apply to an ISA-AA MDA software upgrade.

Note 3 — The 7450 ESS, 7750 MG, and 7750 SR support ISA-AA MDA upgrades.

The following must be true before you attempt an ISA-AA software upgrade.

- You have a 5620 SAM user account with an administrator or network element software management scope of command role or a scope of command role with write access to the mediation package. See chapter 2 for information about scope of command roles.
- The FTP or secure FTP credentials are configured in the NE mediation policy. See the *5620 SAM User Guide* for more information.

Caution 1 — Alcatel-Lucent recommends that you open a physical console session on the device that you need to upgrade. The console session allows you to monitor the upgrade and recover in the event of an upgrade failure.

Caution 2 — Before you attempt an ISA-AA MDA software upgrade, see the appropriate device release notice and the *5620 SAM Network Element Compatibility Guide* for information about the supported upgrade paths. See section 8.1 for general ISSU information.

1 Perform the following steps.

i Verify that the device supports the new ISA-AA software.

ii Extract the isa-aa.tim and md5sums.txt files from the Alcatel-Lucent software package to a directory that is reachable by the 5620 SAM. Ensure that there are no other files in the directory.

iii Manually verify the software image file checksum against the file checksum listed in the md5sums.txt file.

iv Verify that the device file system has space for the software image file.

v For NEs with redundant CPMs, verify that the boot environments are synchronized by using the appropriate CLI command.

vi Configure the appropriate software upgrade policy, as described in Procedure 8-1; apply the policy to the NEs that you need to upgrade.

2. Back up the device configuration. See Procedure 8-4.
3. Choose Administration→NE Maintenance→Software Upgrade from the 5620 SAM main menu. The Software Upgrade form opens.
4. Click on the Software Images tab.
5. Click on the Import button. The Open window appears.
6. Navigate to the directory that contains the software image, select the directory, and click on the Open button.

Note — The directory must contain only the isa-aa.tim and md5sums.txt files.

7. The 5620 SAM verifies the isa-aa.tim checksum and imports the file to the 5620 SAM database. An entry for the image is listed on the Software Upgrade form.
8. Select the required ISA-AA image.
9. Click on the Upgrade Sites button. A list of NEs is displayed. Only the devices that support the software image are listed.
10. Select one or more NEs in the list.
11. Click on the OK button. A dialog box appears.
12. Ensure that the conditions described in the dialog box are met, and then click on the Yes button. The software upgrade begins.
13. Click on the Software Upgrade Status tab to monitor the upgrade progress. The following Upgrade State value is displayed:

    - Transferring Image Files—The 5620 SAM imports the image file from the specified directory to the 5620 SAM database.

Note — Each upgrade stage also has one or more specific failure values.

If the Software Upgrade parameter in the software upgrade policy is selected, the 5620 SAM activates the new software image and displays the following sequence of Upgrade State values during the activation:

- Backing Up ISA-AA File—The 5620 SAM makes a backup copy of the isa-aa.tim file in the primary-image location specified by the BOF.
- Updating ISA-AA File—The new isa-aa.tim file is downloaded to the primary-image location specified by the BOF, and the appropriate ISA-AA upgrade command is issued on each NE.
- Pending ISA MDA Reboot—A reboot of the ISA-AA MDA is required.

14 If the Software Upgrade parameter in the software upgrade policy is deselected, you must activate the software image. Perform the following steps.

Note — Alternatively, you can select the required ISA-AA image on the Software Images tab and click on the Activate Image button.

i Edit the following software upgrade policy settings, as described in Procedure 8-1:

- Deselect the Software Download parameter.
- Select the Software Upgrade parameter.

ii Select the required software image and click on the Upgrade Sites button. The Select Sites form opens.

iii Use the form to select the required NEs, and then click on the OK button. A dialog box appears.

iv Ensure that the conditions described in the dialog box are met, and then click on the Yes button. The software image activation begins.

v Click on the Software Upgrade Status tab to monitor the activation progress. The Upgrade State displays the following sequence of values:

- Backing Up ISA-AA File—The 5620 SAM makes a backup copy of the isa-aa.tim file in the primary-image location specified by the BOF.
- Updating ISA-AA File—The new isa-aa.tim file is downloaded to the primary-image location specified by the BOF, and the appropriate ISA-AA upgrade command is issued on each NE.
- Pending ISA MDA Reboot—A reboot of the ISA-AA MDA is required.

15 Perform the following steps on each upgraded ISA-AA MDA to shut down and reboot the MDA.

i Choose Equipment from the network navigation tree view selector. The network navigation tree displays the Equipment view.

ii Navigate to the upgraded ISA-AA MDA. The path is Network→*NE*→Shelf→Card Slot *n*→Daughter Card Slot *n*.

iii Right-click on the Daughter Card Slot object and choose Shut Down from the contextual menu. A dialog box appears.

iv Click on the View Dependencies button. A dialog box displays the number of objects that shutting down the ISA-AA MDA may affect.

v Click on the OK button.

vi When you are certain that shutting down the MDA has no unintended effects, select the check box and click on the Yes button. The 5620 SAM shuts down the ISA-AA MDA.

vii Right-click on the Daughter Card Slot object and choose Reboot from the contextual menu. A dialog box appears.

viii Click on the View Dependencies button. A dialog box displays the number of objects that rebooting the ISA-AA MDA may affect.

ix Click on the OK button.

x When you are certain that rebooting the MDA has no unintended effects, select the check box and click on the Yes button. The 5620 SAM reboots the ISA-AA MDA.

xi After the MDA reboots, right-click on the Daughter Card Slot object and choose Turn Up from the contextual menu. A dialog box appears.

xii Click on the Yes button. The 5620 SAM turns up the ISA-AA MDA.

16 Click on the Software Upgrade Status tab.

17 View the Upgrade Status, which is one of the following:

- Success—The new image is successfully loaded on each ISA-AA MDA.
- Failed to upgrade ISA—The upgrade is a failure on at least one ISA-AA MDA.

18 If required, verify the upgrade as described in Procedure 8-33.

19 If required, use the 5620 SAM FTP or SSH file browser to verify that the transferred file and configuration are on each upgraded NE. See Procedure 8-36 for information about using the FTP file browser. See Procedure 8-37 for information about using the SSH file browser.

20 Update each ISA-AA policy, as required, to enable the new protocol signatures. See the *5620 SAM User Guide* for information about configuring AA policies.

Procedure 8-24 To perform an on-demand software upgrade or ISSU on an OmniSwitch

Perform this procedure to upgrade the device software on an OmniSwitch. You can perform an on-demand software upgrade on any supported OmniSwitch variant.

Note — ISSU is supported only on the OS 9700E, OS 9800E, and OS 10K.

See Procedure 8-25 for information about performing an ISSU on an OS 6400, OS 6850E, or OS 6855. You can perform the following types of software upgrades:

- Image file
- Boot files
- CPLD/FPGA files (OS 6250 and OS 6450, Release 6.6.3-453R01 and later only)

Warning — An OmniSwitch may require a firmware upgrade before a device software upgrade. To avoid a service outage, ensure that the device firmware version supports the software upgrade. See the device software Release Notes to obtain information about firmware and software version compatibility.

Caution — Alcatel-Lucent recommends that you establish a physical console session on the device that you need to upgrade. The console session allows you to monitor the upgrade and recover the device in the event of an upgrade failure.

The following conditions must be present before you can perform a device software upgrade on an OmniSwitch:

- You have a 5620 SAM user account with an administrator or network element software management scope of command role or a scope of command role with write access to the mediation package. See chapter 2 for more information about scope of command roles.
- FTP is configured in the mediation policy for the NE. See the *5620 SAM User Guide* for more information.

The operational restrictions and requirements for software upgrades on OmniSwitches are:

- Only OS 9700E, OS 9800E, and OS 10K CMM images can be upgraded.
- The following CMM images are ISSU capable:
  - For OS 9700E and OS 9800E NEs, Jbase.img, Jsecu.img, Jadvrout.img and Jos.img are supported.
  - For OS 10K NEs, Ros.img, Reni.img are supported.
- The OS 9700E, OS 9800E, and OS 10K NE platforms must be fully synchronized and certified.
- Target images must be loaded to the /flash/issu directory.
- Sufficient flash memory must be available for upgrade images.
- The CMM software build must be in the same major build tree branch, differing only in the build number (for example, 6.4.1.*.R01)
- OS 9700E and OS 9800E NEs running an ‘R##’ build, such as 6.4.1.123.R01 do not support ISSU patches. The NE must first be upgraded to an ‘S##’ build such as 6.4.1.123.S01. This does not apply to OS 10K NE platforms.

- The directory structure that stores the image and configuration files is divided into two parts:
  - The certified directory contains files that have been certified by an authorized user as the default files for the switch.
  - The working directory contains files that may or may not be modified from the certified directory. The working directory is a holding place for new files. Files in the working directory must be tested before you commit them to the certified directory.

Note 1 — To perform an ISSU, use the software upgrade window only.

Note 2 — The OS 6400, OS 6850E, OS 9700E, OS 9800E, and OS 10K support standard software upgrades in addition to ISSU. On an OmniSwitch, the introduction of new images requires a system reload which disrupts all data traffic during the reload process. Data traffic loss is limited to L3 base routing instance traffic; no loss of Layer 2 data traffic should occur.

1 Choose Administration→NE Maintenance→Software Upgrade from the 5620 SAM main menu. The Software Upgrade form opens.

2 Perform one of the following:

- **a** If you need to upgrade the image files or the image and boot files, go to step 3.
- **b** If you need to upgrade the boot files, go to step 18.
- **c** If you need to upgrade the FPGA files, go to step 32.

3 Choose the appropriate software upgrade policy.

Note — The 5620 SAM performs the upgrade according to the configuration in the software upgrade policy that is assigned to the NE.

4 Click on the Software Images tab.

5 Click on the AOS Software tab.

6 Choose a software image in the list.

7 Click on the Transfer to Sites button. A list of NEs opens. The list is filtered to display only the device type that is appropriate for the selected software image.

8 Choose one or more NEs in the list.

9 Click on the OK button. The selected software image file is uploaded to the working directory of the selected NEs.

10 Click on the Software Upgrade Status tab to view the status of the upgrade as it progresses. Wait until the files have been successfully transferred before going to step 11.

11 Click on the Reload working Sites button. A list of NEs opens.

12 Choose one or more NEs in the list.

13 Click on the OK button. The selected NEs reboots using the new software image that was uploaded to the working directory.

Caution — Rebooting an NE that is in service is service-affecting. Ensure that the reboot activity occurs during a maintenance window.

Note — Alcatel-Lucent recommends monitoring the switch to ensure that the reboot completes successfully.

14 Click on the Certify Sites button. A list of NEs opens.

Note — Only software that is thoroughly validated as viable and reliable software should be copied to the certified directory. After you copy the software to the certified directory, you cannot recover a previous version of the image or configuration files.

15 Choose one or more NEs in the list.

16 Click on the OK button. The software image stored in the NE working directory is copied to the certified directory. The working directory and the certified directory are synchronized so that the same files are in both directories.

17 Perform one of the following:

- **a** If you need to upgrade the boot files, go to step 26.
- **b** If you need to upgrade the FPGA files, go to step 34.
- **c** If you are only upgrading the image files, go to step 39.

18 Choose the appropriate software upgrade policy.

Note — The 5620 SAM performs the upgrade according to the configuration in the software upgrade policy that is assigned to the NE.

19 Click on the Software Images tab.

20 Click on the AOS Software tab.

21 Choose a software image in the list.

22 Click on the Transfer to Sites button. A list of NEs opens. The list is filtered to display only the device type that is appropriate for the selected software image.

23 Choose one or more NEs in the list.

24 Click on the OK button. The boot files are uploaded to the root directory of the selected NEs.

25 Click on the Software Upgrade Status tab to view the status of the upgrade as it progresses. Wait until the files have been successfully transferred before going to step 26.

26 Click on the Upgrade Boot files button. A list of NEs opens. The list is filtered to display only the device type that is appropriate for the selected files.

27 Choose one or more NEs in the list.

28 Click on the OK button. The boot files are upgraded on the selected NEs.

29 Click on the Software Upgrade Status tab to view the status of the upgrade as it progresses. Wait until the files have been successfully transferred before going to step 30.

30 Click on the Delete boot files button.

31 Perform one of the following:

  a If you need to upgrade the FPGA files, go to step 34.

  b If you do not need to upgrade the FPGA files, go to step 39.

32 Click on the Software Images tab.

33 Click on the AOS Software tab.

34 Choose a software image in the list.

35 Click on the Upgrade FPGA files button. A list of NEs opens. The list is filtered to display only the device type that is appropriate for the selected file type.

36 Choose one or more NEs in the list.

37 Click on the OK button. The selected FPGA files are uploaded to the root directory of the selected NEs.

38 Click on the Software Upgrade Status tab to view the status of the upgrade as it progresses. After the FPGA files are successfully transferred, the selected NEs are rebooted.

39 Verify the upgrade success, as described in Procedure 8-33.

40 Close the Software Upgrade form.

Procedure 8-25 To perform an ISSU on an OS 6400, OS 6850E, or OS 6855

This procedure is only applicable for OS 6400, OS 6850E, or OS 6855 NEs, Release 6.4.5 R02 or later, in stacked configuration. ISSU cannot be used to upgrade from one major release to another.

1 Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2 Expand the icon of the OmniSwitch to upgrade, right-click on an OmniSwitch shelf object in the equipment view, and choose Properties from the contextual menu. The Shelf (Edit) form opens with the General tab displayed

3 Click on the Software Control Module tab.

4 Click on the Resynch button. A dialog box appears. Click on the Yes button.

5 Ensure that one of the following is true:

- **a** The Certify Status is Need Certify and the Synchronization Status is Not Synchronized.
- **b** The Certify Status is Certified and the Synchronization Status is Synchronized.

6 Click on the OK button to apply the changes. A dialog box appears. Click on the Yes button. The Shelf (Edit) form closes.

7 Choose Administration→NE Maintenance→Software Upgrade from the 5620 SAM main menu. The Software Upgrade form opens.

8 Choose the ISSU software upgrade policy for an AOS Based Node.

> **Note —** For stacked NEs, the ISSU directory should be created automatically under /flash/issu. If the ISSU directory does not exist, it can be created by setting the File Transfer Type parameter to Secure on the NE being upgraded. See the "To configure NE mediation" procedure in the *5620 SAM User Guide* for more information.

9 Click on the Software Images tab.

10 Click on the AOS Software tab.

11 Choose a software image in the list.

> **Note 1 —** ISSU software images should not contain Kencrypt image files. If the ISSU software image contains a Kencrypt image file, it will transfer the image to the working directory and perform an on-demand software upgrade.
>
> **Note 2 —** For OS 6400, ISSU software images should not contain Gdiag image files. If the ISSU software image contains a Gdiag image file, it will transfer the image to the working directory and perform an on-demand software upgrade.

12. Click on the Transfer to Sites button. A list of NEs opens. The list is filtered to display only the device type that is appropriate for the selected software image.
13. Choose one or more NEs in the list.
14. Click on the OK button. A dialog box appears.
15. Click on the OK button. A dialog box appears.
16. Click on the Yes button. The boot files are uploaded to the root directory of the selected NEs.
17. Click on the Software Upgrade Status tab to view the status of the upgrade as it progresses. Once the files have been successfully transferred, continue to step 18.
18. Click on the Software Images tab.
19. Click on the Certify Sites button. A list of NEs opens.

Note — Only software that is thoroughly validated as viable and reliable software should be copied to the certified directory. After you copy the software to the certified directory, you cannot recover a previous version of the image or configuration files.

20. Choose one or more NEs in the list.
21. Click on the OK button. A dialog box appears.
22. Click on the Yes button. The software image stored in the NE working directory is copied to the certified directory. The working directory and the certified directory are synchronized so that the same files are in both directories.
23. Click on the Software Upgrade Status tab to view the status of the upgrade as it progresses. Once the sites have been successfully certified, continue to step 24.

Note — After the desired sites have been certified, the Command to Apply parameter should be set to Flash Synchro on each affected shelf. See the “To manage an OmniSwitch running configuration” procedure in the *5620 SAM User Guide* for more information.

24. Click on the Software Images tab.
25. Click on the Reload Sites button. A list of NEs opens.
26. Choose one or more NEs in the list.
27. Click on the OK button. A dialog box appears.
28. Click on the Yes button. The selected NEs reboot using the new software image that was uploaded to the working directory.

Caution — Rebooting an NE that is in service is service-affecting. Ensure that the reboot activity occurs during a maintenance window.

29 Click on the Software Upgrade Status tab to view the status of the upgrade as it progresses. Once the sites have been successfully rebooted, continue to step 30.

30 Close the Software Upgrade form.

Procedure 8-26 To upgrade OS 6250SME and OS 6450 NE software licenses for an Ethernet (Metro) role

Perform this software licence upgrade to allow OS 6250SME and OS 6450 NEs to perform in the Ethernet (Metro) role and support the OmniSwitch Ethernet (Metro) features such as ERP, SAA/OAM, stacking/IPM Enterprise VLANs, Dying Gasp, Link OAM, CPE Test-Head profiles, and group profiles. This procedure is not applicable OS 6250 Ethernet (Metro) nodes.

After you upgrade the OS 6250SME and OS 6450 NEs for an Ethernet (Metro) role, perform Procedure 8-24 to perform any future software license upgrades on these NEs.

Caution — This procedure is service-affecting because the OS 6250SME and OS 6450 NEs will reboot. Ensure that the license upgrade activity occurs during a maintenance window.

The following prerequisites are required before you can perform an upgrade:

- You need a new license key for each OS 6250 and OS 6450 OmniSwitch to be upgraded. Contact your Alcatel-Lucent sales representative if you need a new software license.
- You must copy the new license key to a text file and position the file in a folder in the node file system so the file can be imported into the 5620 SAM. Record the path to the folder where the license key text file is located.

1 Choose Administration→NE Maintenance→License Upgrade from the 5620 SAM main menu. The License Upgrade form opens with the License Upgrade Policy tab selected.

2 Optionally, click on the License Upgrade Status tab to confirm the software version and license policy that is currently applied to the NE being upgraded. Otherwise, go to step 3.

- **i** Choose an NE from the list and click on the Properties button. The License Upgrade Status - [Policy Name] [Router ID] [View] form appears.
- **ii** Confirm the software version that is installed and the license policy that is applied to the NE.
- **iii** Click on the Cancel button to close the form.
- **iv** Click on the License Upgrade Policy tab.

3 Perform one of the following:

- **a** To create a new AOS license policy, go to step 4.
- **b** To modify the default AOS default license policy, go to step 7.

4 Click on the Create button. The Licence Upgrade Policy [Create] form opens.

5 Configure the parameters:

- Policy ID
- Auto-Assign ID
- Name
- Root Path

6 Click on the OK button to save the changes and close the License Upgrade Policy [Create] form. The new AOS default license policy appears on the License Upgrade form. Go to step 10.

7 Choose the AOS default license policy on the License Upgrade form, and click on the Properties button. The License Upgrade Policy - AOS Default Policy [Edit] form opens.

8 As required, modify the Root Path parameter to specify the license text file location.

9 Click on the OK button to save the changes and close the License Upgrade Policy [Edit] form. The modified AOS Default License policy appears on the License Upgrade form.

10 Click on the Licenses tab on the License Upgrade form.

11 Click on the Import button. The Open form appears.

12 Locate the license key text file in the appropriate folder in the node file system and click on the Open button. The license_key.txt file appears on the Licenses tab on the License Upgrade form.

13 Optionally, review the license key information before the installation by double-clicking on the license_key.txt file. The License Info form appears. Click on the Cancel button to close the form and return to the Licence Upgrade form.

14 Choose a license to install and click on the Install License button. The Select Sites-Select Sites form appears.

15 Choose an NE to upgrade and click on the OK button. You can press CTRL to choose multiple NEs. A Warning message displays the consequences of upgrading the software.

16 Click on the Yes button to proceed.

17 Optionally, click on the License Upgrade Status tab on the License Upgrade form to confirm whether the upgrade on the NEs was successful. The status is displayed in the Upgrade State column.

18 Click on the Close button to close the License Upgrade form.

Procedure 8-27 To perform an on-demand software upgrade on a 9500 MPR or 9500 MPRe

Perform the following procedure to download 9500 MPR/9500 MPRe software to one or more 9500 MPR/9500 MPRe devices. After a successful software upgrade, activate the software on the 9500 MPR/9500 MPRe device. See the *5620 SAM User Guide* for more information.

The 9500 MPR/9500 MPRe software is stored in two banks on a compact flash card:

- The committed bank contains the software that is currently running.
- The standby bank contains downloaded software that has not been activated or software that was active before the current committed software.

Note — A 9500 MPR/9500 MPRe that has never been upgraded only displays the committed bank. The standby bank does not appear until new software is downloaded for the first time.

You need a 5620 SAM user account with an administrator or network element software management scope of command role or a scope of command role with write access to the mediation package before you can perform a 9500 MPR/9500 MPRe software download. See chapter 2 for more information about scope of command roles.

1 Choose Administration→NE Maintenance→Software Upgrade from the 5620 SAM main menu. The Software Upgrade form opens.

2 Choose the appropriate software upgrade policy.

Note — The 5620 SAM performs the upgrade according to the configuration in the software upgrade policy that is assigned to the NE.

3 Click on the Software Images tab.

4 Click on the MPR 9500 Software Images tab.

5 Choose a software image file in the list. The image descriptor file has a .DSC file extension and must be present on the client system. Other software files do not need to be present on the client system.

6 Click on the Upgrade Sites button. A list of NEs opens. The list is filtered to display only the device type that is appropriate for the selected software image.

7 Choose one or more NEs in the list.

8 Click on the OK button. The software upgrade starts.

9 Click on the Software Upgrade Status tab to view the status of the upgrade as it progresses. Verify that the files are successfully transferred.

Note — If the Auto-Activate After Successful File Transfer check box is enabled, the device activates the new software image after an upgrade operation successfully completes.

10 Close the Software Upgrade form.

Procedure 8-28 To schedule a software upgrade

Perform this procedure to schedule a device software upgrade on one or more managed NEs according to a software upgrade policy and a 5620 SAM schedule. See Procedure 8-1 for information about creating a software upgrade policy. See the *5620 SAM User Guide* for information about creating schedules.

Note — A new SAM scheduled task is shut down by default and must be turned up before it can be executed with one exception. Scheduled software upgrade tasks associated with all NE types are by default automatically enabled.

1 Perform Procedure 8-19 to import the required device software image.

2 Choose Administration→NE Maintenance→Software Upgrade from the 5620 SAM main menu. The Software Upgrade form opens with the Software Upgrade Policy tab displayed.

3 Select the required software upgrade policy.

Note — The 5620 SAM performs the upgrade according to the configuration in the software upgrade policy that is assigned to the NE.

4 Click on the Software Images tab.

5 Select a software image in the list and click on the Schedule Upgrades button. The Select Sites form opens.

6 Choose an NE in the list and click on the OK button. You can choose multiple NEs. The Select Schedule form opens.

Note 1 — If no schedules are listed, you can create one for the upgrade. You cannot proceed unless a schedule is available. See the *5620 SAM User Guide* for information about creating 5620 SAM schedules.

Note 2 — You cannot use a schedule in which the Ongoing parameter is enabled.

7 Select a schedule in the list and click on the OK button. See Procedure 8-29 and the *5620 SAM User Guide* for more information on how to create a schedule. A dialog box appears.

8 Click on the Yes button. The 5620 SAM schedules the upgrade.

9 Close the Software Upgrade form.

Procedure 8-29 To manage scheduled software upgrades

1 Choose Administration→NE Maintenance→Software Upgrade from the 5620 SAM main menu. The Software Upgrade form opens with the Software Upgrade Policy tab displayed.

2 Click on the Software Upgrade Status tab.

3 Click on the Scheduled Task button. The Scheduled Task form opens.

4 Configure the filter criteria and click on the Search button. A list of scheduled tasks is displayed.

5 Choose a scheduled software upgrade entry.

6 To view the scheduled task configuration, click on the Properties button. The Software Upgrade Scheduled Task form opens.

7 Administratively enable or disable the scheduled software upgrade, if required, by configuring the Administrative State parameter.

8 Click on the Properties button in the Schedule panel to view the schedule information, if required.

9 Click on the Properties button in the Task panel to view the 5620 SAM task information, if required.

10 Close the Software Upgrade Scheduled Task form. The Scheduled Task form reappears.

11 Click on the Task Action button and choose the appropriate option to turn up, shut down, or execute the task, if required.

12 Click on the Delete button to remove the scheduled task from the 5620 SAM, if required.

> **Note 1 —** You cannot delete a scheduled task that is operationally enabled. Click on the Task Action button and choose Shut Down from the menu to operationally disable the scheduled task before you delete it.
>
> **Note 2 —** The 5620 SAM does not delete a scheduled task after it runs; you must delete it manually. You cannot reuse a completed scheduled task.

13 Close the Scheduled Task form. The Software Upgrade form reappears.

14 Close the Software Upgrade form.

Procedure 8-30 To activate a device software image

Perform this procedure to activate a previously downloaded device software image on an NE. When the 5620 SAM activates an NE software image, it does the following:

- Updates the BOF with the new software image location
- Backs up the original boot.ldr at the location specified by the CFlash Backup Root Path parameter
- Replaces the currently active boot.ldr file with the new one
- Forces a “boot env synch” and a “config synch” on NEs that have redundant CPMs

> **Note 1 —** If the BOF update fails, then the original boot.ldr file is put in place to align with the BOF specification.
>
> **Note 2 —** The 5620 SAM ensures that the software image is present on the NE and valid for the device before it updates the BOF.

1 Choose Administration→NE Maintenance→Software Upgrade from the 5620 SAM main menu. The Software Upgrade form opens with the Software Upgrade Policy tab displayed.

2 Click on the Software Upgrade Status tab. A list of NEs is displayed.

3 Choose an NE in the list.

4 Click on the Software Images tab. A list of software images on the selected NE is displayed.

5 Select a software image in the list and click on the Activate button. A dialog box appears.

6 Click on the Yes button. The software image is activated.

7 Verify the activation success, as described in Procedure 8-33.

8 Close the Software Upgrade form.

Procedure 8-31 To export a device software image from the 5620 SAM database to a file system

1 Choose Administration→NE Maintenance→Software Upgrade from the 5620 SAM main menu. The Software Upgrade form opens with the Software Upgrade Policy tab displayed.

2 Click on the Software Images tab.

3 Perform one of the following:

  a To export SR device software images, go to step 4

  b To export OmniSwitch software images click on the AOS Software tab. Go to step 4.

4 Choose an image from the displayed list.

5 Click on the Export button. A file navigator form opens.

6 Use the form to specify the directory that is to contain the exported software image and click on the OK button. The software image is saved to files in the specified directory.

7 Close the Software Upgrade form.

Procedure 8-32 To monitor software upgrade status

1 Choose Administration→NE Maintenance→Software Upgrade from the 5620 SAM main menu. The Software Upgrade form opens.

2 Click on the Software Upgrade Status tab.

3 Configure the filter criteria, if required, and click on the Search button. A list of NEs is displayed.

4 Select an NE from the list and click on the Properties button. The Software Upgrade Status (View) form opens.

5 Click on the Software Upgrade tab to view information on the software upgrade.

6 Close the Software Upgrade Status (View) form.

7 Close the Software Upgrade form.

Procedure 8-33 To view the deployment, backup/restore, or software upgrade status of an NE

1 Perform one of the following:

  a Choose Administration→NE Maintenance→Deployment from the 5620 SAM main menu to view deployment status. The Deployment form opens with the Incomplete Deployments tab displayed.

    i Double-click on a deployment in the list. The deployment properties form opens.

    ii View the deployment status.

  b Choose Administration→NE Maintenance→Backup/Restore from the 5620 SAM main menu to view the backup or restore status. The Backup/Restore form opens with the Backup/Restore Policy tab displayed.

    i Click on the Backup/Restore Status tab. The Restore State column of the backup or restore is: Transferring Files, Pending, Reboot, CPM Sync and Reboot, Success, Not Attempted, Save Config, or Failure. The timestamp is also displayed.

    ii Double-click on a row in the list to display information about the backup or restore operation. You can click on the General, Backups, Configuration Saves, and Faults tabs.

Note — When you click on the Backups tab, the date and time in the Config File Version column corresponds to the date and time for the Last Boot Cfg Version on the NE.

  c Choose Administration→NE Maintenance→Software Upgrade to view the software upgrade status. The Software Upgrade form opens.

    i Click on the Software Upgrade Status tab. A list of NEs displayed.

    ii Double-click on an NE in the list to view information about the upgrade. The Software Upgrade Status form opens.

    iii Close the Software Upgrade Status form.

2 Close the form.

Procedure 8-34 To view the accounting statistics collection status of an NE

1 Choose Tools→Statistics→Accounting Retrieval Status from the 5620 SAM menu. The Accounting Retrieval Status form opens with a list of managed NEs displayed.

2 Select an NE in the list and click on the Properties button. The Accounting Retrieval Status (View) form opens.

3 View the statistics collection information for the NE.

4 Close the Accounting Retrieval Status (View) form.

5 Close the Accounting Retrieval Status form.

Procedure 8-35 To view the trap metrics information

1 Choose Tools→Statistics→Trap Metrics Information from the 5620 SAM main menu. The Trap Metrics Information form opens and lists the NEs that generated the most traps during the last collection interval. The collection interval is indicated by the Start Collection Period and End Collection Period values at the top of the form.

Note — The number of displayed NEs is limited by the metrics configuration in the nms-server.xml file.

2 Click on the Search button to refresh the trap metrics information. The list and collection interval values are updated.

3 Close the Trap Metrics Information form.

Procedure 8-36 To view an NE file system using an FTP file browser

Perform this procedure to browse and list the files on a managed NE. You need FTP user-account privileges on the NE for access to the NE file system. See the *5620 SAM User Guide* for information about enabling FTP access for an NE user account.

1 Initiate an FTP file browser session.

- **a** Use the 5620 SAM main menu.
  - **i** Choose Tools→Network Elements→NE Sessions→FTP File Browser. The FTP File Browser form opens.
  - **ii** Enter the IP address of the NE that you need to browse in the field at the top of the form.
  - **iii** Press Enter or click on the Connect button. The Enter the Username and Password form opens.

Note — When you use the 5620 SAM main menu to open a file-browser session, you are not restricted to the original NE; you can use the same form to connect to other NEs. This is useful when several NEs are to be browsed in succession.

b Use the Software Upgrade Policy form.

  i Choose Administration→NE Maintenance→Software Upgrade. The Software Upgrade form opens with the Software Policy tab displayed.

  ii Select a policy in the list and click on the Properties button. The Software Upgrade Policy (Edit) form opens.

  iii Click on the FTP File Browser button. If the FTP File Browser button is not visible, click on the More Actions button and choose FTP File Browser. The FTP File Browser form opens.

  iv Enter the IP address of the NE that you need to browse in the field at the top of the form.

  v Press Enter or click on the Connect button. The Enter the Username and Password form opens.

c Use the contextual menu for an NE.

  i Select an NE icon in the 5620 SAM network navigation tree or topology map.

  ii Right-click on the NE icon and choose NE Sessions→File Browser from the contextual menu. The FTP File Browser form opens, then displays the Enter the Username and Password form.

d Use the properties form of an NE.

  i Select an NE icon in the 5620 SAM network navigation tree or topology map.

  ii Right-click on the NE icon and choose Properties from the contextual menu. The Network Element (Edit) form opens.

  iii Click on the File Browser button. If the File Browser button is not visible, click on the More Actions button and choose File Browser. The FTP File Browser form opens, then displays the Enter the Username and Password form.

e Use the topology view of a service.

  i Choose one of the following from the 5620 SAM main menu:

- Manage→Service→Services
- Manage→Service→Composite Services
- Manage→Service→Mirror Services

  ii Configure the filter criteria.

  iii Choose a service from the list.

  iv Click on the Topology View button. A Topology View dialog box appears.

v Click on the Yes button. The Service Topology map opens.

vi Right-click on a managed device and choose NE Sessions→File Browser from the contextual menu. The FTP File Browser form opens to display the Enter the Username and Password form.

Note — You can open a file browser session on only one managed device at a time.

f Use the navigation tree of a service management form.

i Choose one of the following from the 5620 SAM main menu:

- Manage→Service→Services
- Manage→Service→Composite Services
- Manage→Service→Mirror Services

ii Configure the filter criteria.

iii Choose a service from the list.

iv Click on the Properties button.

v The *Service* (Edit) form opens.

where *Service* is the type of service selected

vi On the navigation tree, right-click on a service site and choose NE Sessions→File Browser from the contextual menu. The FTP File Browser form opens to display the Enter the Username and Password form.

Note — You can open a file browser session on only one service site at a time.

g Use the Sites tab of a service.

i Choose one of the following from the 5620 SAM main menu:

- Manage→Service→Services
- Manage→Service→Composite Services
- Manage→Service→Mirror Services

ii Configure the filter criteria.

iii Choose a service from the list.

iv Click on the Properties button.

v The *Service* (Edit) form opens.

where *Service* is the type of service selected

vi Click on the Sites tab.

vii Choose a site from the list.

viii Click on the NE Sessions button and choose File Browser from the contextual menu. The FTP File Browser form opens to display the Enter the Username and Password form.

Note — You can open a file browser session to only one service site at a time.

h Use the NE alarm contextual menu.

i Select an NE alarm in the 5620 SAM alarm window.

ii Right-click on the alarm and choose NE Sessions→File Browser. The FTP File Browser form opens, then displays the Enter the Username and Password form.

Note — When you use the 5620 SAM main menu or the Software Upgrade form to open a file-browser session, you are not restricted to the original NE; you can use the same form to connect to other NEs. This is useful when several NEs are to be browsed in succession.

2 Enter the user name and password of a user account with FTP access privileges on the NE and click on the OK button or press Enter. If the NE accepts the credentials, the form lists the contents of the NE.

<DIR> in the Type column indicates a directory. The file path to the current directory is displayed in the Path field.

Note — On an NE with redundant CPMs, the form lists the contents of the cf3 device on the active CPM.

You can browse the cf3 device on the standby CPM by specifying cf3-B:\ in the Path field.

3 If the login attempt fails with the supplied credentials, a dialog box appears. Click on the OK button to close the dialog box, check the credentials and repeat step 2.

4 Sort the list entries by a specific attribute, if required, by clicking on the column heading for the attribute. Clicking again on the column heading reverses the sort order.

5 Reorder the columns, if required, by clicking on a column heading and dragging the column to a new position.

6 Navigate the file system as required. Perform one of the following actions to open a directory and list the contents.

a Double-click on the directory row in the list.

b Select the directory row and press <CTRL>O.

c Type the path to the directory in the Path field and click on the Go button or press Enter.

7 If you opened the browser using the 5620 SAM main menu, you can browse another NE file system using the same form, if required.

- **i** Click on the Disconnect button to end the browsing session.
- **ii** Go to step 1 a ii.

8 Close the FTP File Browser form.

Procedure 8-37 To view an NE file system using an SSH file browser

Perform this procedure to browse and list the contents of a managed NE using a secure file browser. You need console and SSH user-account privileges on the NE for access to the NE file system, and an SSH server must be configured on the NE. See the *5620 SAM User Guide* for information about enabling console or SSH access for an NE user account or configuring an SSH server for an NE.

1 Initiate an SSH file browser session.

- **a** Use the 5620 SAM main menu.
  - **i** Choose Tools→Network Elements→NE Sessions→SSH File Browser. The SSH File Browser form opens.
  - **ii** Enter the IP address of the NE that you need to browse in the field at the top of the form.
  - **iii** Press Enter or click on the Connect button. The Enter the Username and Password form opens.
- **b** Use the Software Upgrade Policy form.
  - **i** Choose Administration→NE Maintenance→Software Upgrade. The Software Upgrade form opens with the Software Policy tab displayed.
  - **ii** Select a policy in the list and click on the Properties button. The Software Upgrade Policy (Edit) form opens.
  - **iii** Click on the SSH File Browser button. If the SSH File Browser button is not visible, click on the More Actions button and choose SSH File Browser. The SSH File Browser form opens.
  - **iv** Enter the IP address of the NE that you need to browse in the field at the top of the form.
  - **v** Press Enter or click on the Connect button. The Enter the Username and Password form opens.

c Use the contextual menu for an NE.

  i Select an NE icon in the 5620 SAM network navigation tree or topology map.

  ii Right-click on the NE icon and choose NE Sessions→File Browser from the contextual menu. The SSH File Browser form opens, then displays the Enter the Username and Password form.

d Use the properties form of an NE.

  i Select an NE icon in the 5620 SAM network navigation tree or topology map.

  ii Right-click on the NE icon and choose Properties from the contextual menu. The Network Element (Edit) form opens.

  iii Click on the File Browser button. If the File Browser button is not visible, click on the More Actions button and choose File Browser. The SSH File Browser form opens, then displays the Enter the Username and Password form.

e Use the NE alarm contextual menu.

  i Select an NE alarm in the 5620 SAM alarm window.

  ii Right-click on the alarm and choose NE Sessions→File Browser. The SSH File Browser form opens, then displays the Enter the Username and Password form.

Note — When you use the 5620 SAM main menu or the Software Upgrade form to open a file-browser session, you are not restricted to the original NE; you can use the same form to connect to other NEs. This is useful when several NEs are to be browsed in succession.

2 Enter the user name and password of a user account with FTP and SSH access privileges on the NE and click on the OK button or press Enter. If the NE accepts the credentials, the form lists the contents of the NE.

<DIR> in the Type column indicates a directory. The file path to the current directory is displayed in the Path field.

Note — On an NE with redundant CPMs, the form lists the contents of the cf3 device on the active CPM.

You can browse the cf3 device on the standby CPM by specifying cf3-B:\ in the Path field.

3 If the login attempt fails with the supplied credentials, a dialog box appears. Click on the OK button to close the dialog box, check the credentials and repeat step 2.

4 Sort the list entries by a specific attribute, if required, by clicking on the column heading for the attribute. Clicking again on the column heading reverses the sort order.

5 Reorder the columns, if required, by clicking on a column heading and dragging the column to a new position.

6 Navigate the file system as required. Perform one of the following actions to open a directory and list the contents.

- **a** Double-click on the directory row in the list.
- **b** Select the directory row and press <CTRL>O.
- **c** Type the path to the directory in the Path field and click on the Go button or press Enter.

7 If you opened the browser using the 5620 SAM main menu or from the Software Upgrade form, you can browse another NE file system using the same form, if required.

- **i** Click on the Disconnect button to end the browsing session.
- **ii** Go to step 1 a ii.

8 Close the SSH File Browser form.

Procedure 8-38 To troubleshoot a failed configuration deployment

The 5620 SAM continues to retry deployments after a failed or incomplete deployment attempt, based on the 5620 SAM deployment policy, as configured in Procedure 8-2. When there is a deployment error, a number of problems can occur, for example:

- The 5620 SAM database may lose synchronization with the device database.
- Configuration changes requested using the client GUI may clash with configuration changes, retries, and recovery applications developed by an OSS system using the 5620 SAM-O interface or by an operator using a CLI.

When a failed or incomplete deployment or a failed SNMP configuration request occurs, a Problems Encountered error display form appears automatically. This form displays error information about the failure(s).

Note 1 — The Request Id and Task Name fields appearing on the Problems Encountered error form can be used for troubleshooting using the Task Manager application.

Note 2 — The Problems Encountered error form can appear for non-deployment generated errors also.

For example, to view more information on a failed deployment, select a failed deployment entry, then click on the Properties button, or double-click on the failed deployment entry.

An error form opens which contains a View Affected Object button and a Details button.

Click on the Details button to view detailed diagnostic information about the failure(s).

Click on the View Affected Object button. A form displaying object properties opens. This form facilitates rapid navigation to the object which caused the failure for troubleshooting purposes.

Click on the Faults tab. Alarm information related to the failure(s) is displayed.

A failure error message is not generated when the alarm is cleared or the failure entry is deleted.

Note 1 — If a deployment failure is associated with more than one 5620 SAM GUI, the Problems Encountered form and related forms appear only on the GUI from which the deployment was issued.

Note 2 — The automatically generated Problems Encountered form and related forms, are an additional tool to the following troubleshooting procedure.

The Deployment form displays failed configuration deployments and allows you to view information about failed deployments. Using this form, you can clear the deployment, override the error to force the configuration to be downloaded to the device, or suspend or resume deployment retries to a device.

1 Choose Administration→NE Maintenance→Deployment from the 5620 SAM main menu. The Deployment form opens with the Incomplete Deployments tab displayed.

2 Review the deployment information. The State value indicates the cause of the deployment failure.

3 Select a deployment in the list and click on the Properties button. The properties form for the deployment opens. The objects that the deployment failed to modify are displayed in the Objects list.

4 Select an entry in the Objects list and click on the Properties button. The Object Change form that describes the attempted configuration change opens.

5 Select an entry in the Attributes list and click on the Properties button. The Attribute Change form opens and displays the following object attribute information for troubleshooting:

- the NE attribute that was to be modified
- the old, unmodified attribute value
- the new attribute value that the deployment failed to assign

6 Click on the Cancel button to close the Attribute Change form.

7 Click on the Cancel button to close the Object Change form.

8 Click on the Cancel button to close the deployment properties form.

9 Perform one of the following actions, depending on the result of the investigation into the failed deployment.

a Click on the Suspend Retries button to override the deployment policy setting and prevent further retries of the deployment. A dialog box appears; click on the Yes button.

b Click on the Resume Retries button to override a previous Suspend Retries action performed on the deployment. A dialog box appears; click on the Yes button.

c Click on the Clear button to clear the deployment. A dialog box appears; click on the Yes button. The deployment is cleared.

> **Note —** Clearing a failed deployment may result in a loss of data synchronization between the 5620 SAM database and the NE. Alcatel-Lucent recommends that you resynchronize the NE objects associated with a failed deployment after you clear a failed NE deployment.

d Click on the Force Submit button to force the 5620 SAM to immediately resend the deployment to the NE. A dialog box appears; click on the Yes button.

10 Click on the Refresh button to update the list of failed deployments.

11 Take the appropriate action described in this procedure to troubleshoot other failed deployments, as required.

12 Close the Deployment form.

5620 SAM routine maintenance tasks

9 — 5620 SAM routine maintenance overview

9.1 Routine maintenance overview

The 5620 SAM maintenance tasks and procedures are intended for NOC operations or other engineering operational staff that are responsible for developing and implementing maintenance procedures in 5620 SAM-managed IP/MPLS networks.

The 5620 SAM maintenance tasks and procedures are categorized by the frequency they are performed or on an as required basis. Alcatel-Lucent recommends the implementation of a regular maintenance schedule to help:

- prevent downtime caused by software, platform, or network failure
- your 5620 SAM applications operate at maximum performance

The appropriate maintenance frequency depends on the network conditions of the individual service provider or operation. Tailor the suggested maintenance actions and frequency to the unique needs of your network.

Table 9-1 lists where to find maintenance information.

Table 9-1 Maintenance information

For information about	See chapter
Performance maintenance baselines	10
Daily maintenance tasks	11
Weekly maintenance tasks	12
Monthly maintenance tasks	13
As required maintenance tasks	14

9.2 Routine maintenance guidelines

Use these guidelines as a basis for developing new or enhancing existing maintenance procedures and workflows that are used in the NOC. These guidelines do not provide a complete list of the features and functionality of the 5620 SAM. The guide includes a high-level view of maintenance actions based on frequency, suggests baseline measures to ensure performance tracking, and describes how to use 5620 SAM applications to check performance.

The staff responsible for developing or performing 5620 SAM maintenance tasks need a good understanding of:

- creating and interpreting 5620 SAM-O XML requests and responses
- executing 5620 SAM client GUI functions and operations
- the relationship of 5620 SAM software applications, log files, and the platforms on which the applications run

See the other documentation, as described in section 1.3, to supplement the development of individualized maintenance procedures for your network.

9.3 Obtaining technical assistance

Collect the information listed in Table 9-2 before you contact Alcatel-Lucent technical support. The list of Alcatel-Lucent support contacts is available at the following URL:

http://support.alcatel-lucent.com.

Table 9-2 Required technical-support Information

Information type	Description
Issue description	• recent 5620 SAM GUI or OSS operations • screen captures or text versions of error or information messages • actions performed in response to the issue
Platform and software specifications	• 5620 SAM software release ID • OS type, release, and patch level • hardware information such as the following: • CPU type • number of CPUs • disk sizes, partition layouts, and RAID configuration • amount of RAM
System and application logs	You can run the following script on a server station to collect the required log files for Alcatel-Lucent technical support: *install_directory*/nms/bin/getDebugFiles.bash See the *5620 SAM Troubleshooting Guide* for information about using the script.

9.4 Routine maintenance checklist

Table 9-3 is a checklist of the recommended 5620 SAM routine maintenance tasks.

Table 9-3 Recommended 5620 SAM preventive maintenance tasks

✓	Maintenance task	Purpose	See section
Daily maintenance tasks			
	Managing alarms	• Track and handle incoming alarms. • Log historical logs for record keeping.	11.1
	Verifying the synchronization of managed-device and 5620 SAM database information	Ensure consistency between the 5620 SAM database and managed device databases.	11.2
	Backing up the 5620 SAM database	Prevent the loss of network data.	11.3
	Collecting and storing 5620 SAM log and configuration files	Record historical system activities and current configuration settings.	11.4
	Backing up NMS domain platforms	Back up an entire platform to ensure that all data can be restored.	11.5
Weekly maintenance tasks			
	To check for performance monitoring statistics collection	Ensure that there is sufficient capacity to process and store network statistics.	12-1
	To gather port inventory data for a specific managed device	Collect inventory information for future baseline checks and post processing of equipment trends and use.	12-2
	To test a 5620 SAM database restore	Ensure that database backups are viable in the event that a restore is required.	12-3
	To check scheduled device backup status	Ensure that managed device configuration backups are stored and collected correctly if a restore is required.	12-4
	To reduce the number of Oracle audit logs	Ensure that the logs do not use excessive disk space.	12-5
Monthly maintenance tasks			
	Performing main server and database activity switches	Perform regular main server and database activity switches to ensure that 5620 SAM server and database redundancy functions correctly and responsively.	13.1
	Checking the 5620 SAM platform performance	Compare platform performance over time to check for degradation.	13.2
	Checking Windows client platform performance	Compare platform performance over time to check for degradation.	13.3
	Checking LAN TCP/IP connections between network-management domain elements	Test connectivity between the 5620 SAM platforms.	13.4
	Generating and storing a user account list	Keep up-to-date records of staff and their assigned user accounts.	13.5
	Verifying documentation and support contact list updates	Check for product updates and new load information.	13.6
	Setting the time and date	Keep network devices and the NMS domain on the same clock.	13.7

(1 of 2)

✓	**Maintenance task**	**Purpose**	**See section**
As required maintenance tasks			
	General 5620 SAM platform changes	You must uninstall and reinstall the 5620 SAM software after you make a change to the physical 5620 SAM server, database, or platform.	14.1
	Adding or removing RAM	When the amount of RAM on a 5620 SAM database station changes, you must reconfigure the Oracle System Global Area, or SGA.	14.2
	Relinking the Oracle executable files	Relink the Oracle program files after an OS upgrade or the application of an OS patch.	14.3
	Changing 5620 SAM database and Oracle user passwords	For greater security, Alcatel-Lucent recommends that you regularly change the 5620 SAM database user and Oracle SYS user passwords.	14.4
	Restoring a 5620 SAM database	Restore a 5620 SAM database using a previously created database backup.	14.5
	Clearing inactive residential subscriber instances from the 5620 SAM database	Periodically run a script to clear out the accumulation of inactive residential subscriber instance records from the 5620 SAM database	14.6
	Listing customer service information	Record customer service inventory information.	14.7
	Checking for duplicate service or resource names	Check for duplicate names to ensure naming conventions are followed.	14.8

(2 of 2)

10 — 5620 SAM maintenance base measures

10.1 Base measures overview

Maintenance base measures can be used by NOC operations or engineering staff that are responsible for maintenance issues to evaluate the activity and performance of network components, for example, client GUI response times when listing equipment.

The data from a series of base measures can be used, over time, to track performance trends. For example, if there are reports that client GUI response times for listing equipment degrades over time, you can use the base measures to determine how much performance has degraded. The procedures in this guide can help narrow the search for the cause of performance degradation.

You should:

- determine the types of base measures that should be implemented for your network
- record base measures data
- create and regularly perform the tasks necessary to gather and compare base measures over time

This chapter provides base measure information for:

- platform—to ensure system sizes are tracked
- performance and scalability—to categorize system limitations as a baseline against NMS response times
- inventory counts—to generate inventory lists for storage and post-processing
- reachability—to ensure that customer services are available

10.2 Base measures guidelines

Base measures can be affected by issues that are beyond the scope of this guide, including:

- network topology design
- NOC or operations area LAN design

The 5620 SAM service test manager (STM) provides the ability to group OAM diagnostic tests into test suites that you can run as scheduled tasks. You can customize a test suite to your network topology and execute the test suite to establish baseline performance information. You can retain the test suite, modify it to accommodate network topology changes, and execute the test suite to establish new base measures as required. Scheduled execution of the test suite and regular review of the results may reveal deviations from the baseline. See the *5620 SAM User Guide* for information about using the STM and creating scheduled tasks.

Platform base measures

You can use 5620 SAM base measures to:

- record the details of the platform configuration
- track network-specific growth to provide a delta for performance measures, for example, how long it takes to list 1000 ports on the current station compared to 10 000 ports on the same station, or on a smaller or larger station

You can use Table 10-1 to record 5620 SAM station specifications and capacities.

Table 10-1 Platform base data

Application	Platform information
Windows	
5620 SAM client GUI	RAM: CPU (quantity, type, speed): OS version, patch level: Disk space: Monitor: Graphics card:
Windows	
Additional 5620 SAM client GUI	RAM: CPU (quantity, type, speed): OS version, patch level: Disk space: Monitor: Graphics card:
Additional 5620 SAM client GUI	RAM: CPU (quantity, type, speed): OS version, patch level: Disk space: Monitor: Graphics card:
RHEL or Solaris	
5620 SAM main server 1	RAM: CPU (quantity, type, speed): OS version, patch level: Swap space: Disk slices:
5620 SAM database 1	RAM: CPU (quantity, type, speed): OS version, patch level: Swap space: Database disk file systems: Disk slice sizes:

(1 of 3)

Application	Platform information
5620 SAM main server 2	RAM: CPU (quantity, type, speed): OS version, patch level: Swap space: Disk slices:
5620 SAM database 2	RAM: CPU (quantity, type, speed): OS version, patch level: Swap space: Database disk file systems: Disk slice sizes:
5620 SAM preferred auxiliary server 1	RAM: CPU (quantity, type, speed): OS version, patch level: Swap space: Database disk file systems: Disk slice sizes:
5620 SAM preferred auxiliary server 2	RAM: CPU (quantity, type, speed): OS version, patch level: Swap space: Database disk file systems: Disk slice sizes:
5620 SAM reserved auxiliary server 1	RAM: CPU (quantity, type, speed): OS version, patch level: Swap space: Database disk file systems: Disk slice sizes:
5620 SAM reserved auxiliary server 2	RAM: CPU (quantity, type, speed): OS version, patch level: Swap space: Database disk file systems: Disk slice sizes:
5620 SAM client GUI	RAM: CPU (quantity, type, speed): OS version, patch level: Swap space: Disk slices: Monitor: Graphics card:

(2 of 3)

Application	Platform information
Additional 5620 SAM client GUI	RAM: CPU (quantity, type, speed): OS version, patch level: Swap space: Disk slices: Monitor: Graphics card:
Additional 5620 SAM client GUI	RAM: CPU (quantity, type, speed): OS version, patch level: Swap space: Disk slices: Monitor: Graphics card:

(3 of 3)

Inventory base measures

You can use inventory base measures to:

- create lists of network objects for future processing
- track network-specific growth to provide a delta for any performance measures, for example, how long it takes 5 versus 15 client GUIs to list 1000 ports

Use the following sequence to create inventory base measures, for example, for access ports. You can modify the sequence to create additional inventory base measures for other objects.

1. Determine the type of object data for which you need to create inventory records, for example, access ports.
2. List the ports of all managed network devices using the client GUI manage equipment window or create an XML OSS request to generate the list.
3. Format the inventory for future processing, based on your inventory processing applications.
4. Generate the inventory data, using the same listing and filtering criteria, on a weekly or monthly basis, as necessary to track changes to the network.

   When new devices are added to the network on a regular basis, increase the inventory frequency.
5. Use the generated list to record the current inventory of network objects and as a baseline measure of performance.

   For example, baseline the time required to generate a client GUI list of 1000 access ports.

   When an access port list is later generated, record the time required to generate the list using 2000 ports. Ideally, it takes twice as long to list twice as many ports; if the ratio of listing time to number of ports is highly nonlinear, there may be scalability issues that require investigation.

Performance and scalability base measures

You can use the following 5620 SAM performance and scalability base measures to:

- record the system limit numbers and compare to the measurement data collected in your network
- track network-specific growth to provide a delta for any performance measures on similarly-sized platforms, for example, how long it takes to discover 10 new devices versus 20 new devices
- quantify user perceptions of performance

Table 10-2 indicates some scalability base measures that can be used to baseline and record scalability data.

Table 10-2 Scalability base measures

Type of base measure	System limits	Expected response time	Network base measure response time	Additional information
Total devices managed	See the appropriate *5620 SAM Release Description* and *5620 SAM Planning Guide* for information about release-specific system limits.	The client GUI is operational *XX* seconds after launching.		The time to open icons in the Equipment navigation tree increases depending on the number of configured MDAs.
Total services		• XML OSS configuration of 300 VLL services in *X* min • XML OSS configuration of 100 VPLS services with 3 sites and one SAP in 5 min		The complexity of the service configuration affects response time. For example, adding additional SAPs to a VPLS increases provisioning time.
Outstanding alarms		The client GUI is able to retrieve and display *XX* 000 alarms in the dynamic alarm list during startup.		—
Client GUIs for each server		—		Open a configuration form using the client GUI in X amount of time. Measure X against a constant platform size over time
Device discovery		Discover one additional device with an IP address in the X.X.X.1 to 255 range in less than 1 min.		—

Performance base measures

For networks, commonly available tools such as ping, which measures round trip time using ICMP, can be used to determine quantities such as packet loss and round trip delay. See the ping command information in this guide, and the *5620 SAM Troubleshooting Guide*, for more information about performing the commands.

- Packet loss is defined as the fraction of packets sent from a measurement agent to a test point for which the measurement agent does not receive an acknowledgement from the test point. Acknowledgements that do not arrive within a pre-defined round trip delay at the measurement agent are considered lost.
- Round trip delay is defined as the interval between the time a measurement agent application sends a packet to a test point and the time it receives acknowledgement that the packet was received by the test point.

You can baseline the packet loss results and round trip delay times for specific NMS LAN and network scenarios. Record those results for future baselines against regularly run packet loss and round trip delay tests.

Reachability base measures

System reachability is important in business-critical applications. Service reachability components are:

- Can the customer reach the service? (reachability)
- If so, is the service available for customer use? (service availability)
- If not, how frequently and how long do service outages last? (service outage duration)

The types of measures and baselines necessary to ensure reachability and availability are network-dependent, and vary depending on the topology of the network, the networking technologies used to move data, and the types of equipment used.

Reachability

A test point is reachable from a testing measurement agent when the agent can send packets to the test point and receive a response from the test point that the packet was received. The ping test and the OAM diagnostics using the 5620 SAM or device CLI can test reachability. The results from these tests should be recorded for future baselining.

These tests can be performed when you troubleshoot a customer service, or when you perform SLA tests before you enable a customer service.

Service availability

The network between a measurement agent and a test point is considered available at a given time when the measured packet loss rate and the round trip delays are both below pre-defined thresholds. The threshold values are dependent on network topology. The ping test and the OAM diagnostics using the 5620 SAM or CLI to a device can test service availability. The results from these tests should be recorded for future baselining.

Service outage duration

The duration of an outage is defined as the difference between the time a service becomes unavailable and the time it is restored. Time between outages is defined as the difference between the start times of two consecutive outages. Troubleshooters that resolve customer problems, or the data generated to resolve SLAs, can provide the baseline metrics to measure outages, and the time between outages. Record the information for future baselining.

11 — Daily maintenance tasks

11.1 Managing alarms

In large 5620 SAM-managed networks where 5620 SAM applications are constantly interacting with a busy network in a non-stop management environment, many alarms are raised on the 5620 SAM. These alarms should be:

- tracked as they arrive
- historically logged for trend and performance analysis

You should review alarms on a daily basis to check the type and characteristics of the alarms, and to resolve the network problems caused by the alarms. You can create search filters to identify alarms for a specific site or service, and view up to six filtered alarm lists to monitor network wide issues. You can analyze the alarm history log to determine whether there are any chronic or prolonged failures, or trends. You should correct physical equipment failure alarms or network device alarms immediately.

Note — If your NOC is organized to feed alarm streams from multiple vendor equipment to a third-party application, you should verify that all alarms are correctly logged by the third-party application and then remove alarms from the 5620 SAM client GUI. You can use the Faults tab on most 5620 SAM client GUI forms to view correlated alarm information for specific objects. See the *5620 SAM User Guide* for more information.

Daily maintenance operations that are performed on NEs can cause a large number of alarms to be raised in the 5620 SAM. The OLC state of an object shows whether the object is in service or in maintenance mode. You can filter alarms generated for objects with a particular OLC state. See Section 14.9.

Procedure 11-1 To list all incoming alarms

The dynamic alarm list allows you to monitor all incoming network and network management domain alarms.

1 Ensure that the Alarm Table tab in the Alarm Window at the bottom of the 5620 SAM client GUI is selected.

2 Right-click on an alarm entry row.

The contextual alarm menu appears.

3 Handle the alarms according to your company alarm policies.

For example, to acknowledge an alarm and then delete the alarm:

i Choose Acknowledge Alarm(s) from the contextual menu.

The Alarm Acknowledgement form appears.

ii Modify the Severity and Urgency parameters, as required.

iii In the Acknowledgement Text parameter, enter data about the alarm, according to your company alarm policies.

- **iv** Click on the OK button.
- **v** Confirm the action.

  The Ack column in the alarm row indicates that the alarm is acknowledged.
- **vi** Right-click on the alarm entry row.

  The contextual alarm menu appears.
- **vii** Choose Delete Alarm(s) from the contextual menu to delete the alarm.

Caution — You cannot recover a deleted alarm unless you store alarms in the alarm history log. Perform Procedure 11-2 to store the alarm in the history log.

- **viii** Confirm the action. The alarm is deleted.

Procedure 11-2 To store alarms in an alarm history log and view alarm history logs

1. Choose Administration→Alarm Settings from the 5620 SAM main menu. The Alarm Settings form appears with the General tab displayed.
2. Click on the Alarm History DB Behavior panel.
3. Set the alarm history behavior:
   - **i** Ensure that the Administrative State parameter is set to Up to enable alarm history logging.
   - **ii** Select the Log on Change check box to specify whether to log an alarm when one of its properties changes, for example, to log an alarm when the alarm is acknowledged.
   - **iii** Select the Log on Deletion check box to specify whether to log an alarm when it is deleted.

Note — Alcatel-Lucent recommends that you select the Log on Deletion option to ensure that there are logged records of all deleted alarms saved as historical alarm records.

4. Delete the alarms according to your alarm handling policies.

The deleted alarms are logged to the alarm history logs. To view logged alarm history records:

i Choose Tools→Historical Alarms from the 5620 SAM main menu. The Alarm History filter form opens.

ii If required, configure the filter criteria to limit the range of historical alarms displayed.

iii Click on the Search button. The historical alarms appear based on the filtering criteria.

Note — When you sort more than 50 000 outstanding or logged alarms, GUI performance is affected. Use filters to limit the number of alarms that are listed.

5 Review the alarm history log data for trends and other fault management purposes. Transfer the data from the 5620 SAM platform for post-processing, as required.

11.2 Verifying the synchronization of managed-device and 5620 SAM database information

Monitor device synchronization to confirm that the 5620 SAM database information is maintaining synchronization with the device database information.

Procedure 11-3 To verify 5620 SAM database information

1 Check for deployment failures. Deployment failures indicate that communication with a managed device is failing or has failed.

i Choose Administration→NE Maintenance→Deployment from the 5620 SAM main menu. The Deployment form opens with the Incomplete Deployments tab displayed.

ii Click on the Search button to display the latest information.

When no failed deployments are listed, deployment problems are not causing a synchronization issue.

iii If deployments are listed, view the state of a deployment in the State column. The possible deployment states include:

- Cancelled
- Deployed
- Failed (Configuration). Failure occurred because the configuration could not be applied to the specified objects.
- Failed (Internal Error). Failure occurred due to general error conditions. The state is intended for all other possible errors.
- Failed (Partial). Failure occurred at deployment and some of the configuration may have been sent to the network.
- Failed (Resource Unavailable). Failure occurred because one of the resources required to apply the configuration is not in the 5620 SAM database.
- Not Deployed
- Pending
- Postponed

iv Identify the source of the deployment problem. For example, for a Failed configuration state, ensure the configuration was performed correctly on the client GUI.

2 If you determine that there is a deployment problem and the problem is unrelated to the 5620 SAM or device configuration, use your company IT policies to check the LAN for connectivity and transmission problems, such as collisions and CRC errors.

11.3 Backing up the 5620 SAM database

Alcatel-Lucent recommends that you back up the database to prevent the loss of network data in the event of a failure. You should perform a backup every day, and after you make major changes to the network.

You can use the 5620 SAM client GUI to perform an immediate backup or you can use a CLI script to perform the backup. You can also schedule a regular database backup. See Procedure 7-6 for more information.

Because a database backup is a resource-intensive and time-consuming process, Alcatel-Lucent recommends that database backups occur only during times of low activity to minimize the impact on processing requests from XML OSS clients and client GUIs

Procedure 11-4 To back up the 5620 SAM database using the client GUI

Caution — Ensure that there is sufficient hard disk space to store the database backup. Alcatel-Lucent recommends that a separate database backup directory is created to store backup files. This backup directory should be at least five times larger than the expected database backup size. Contact your Alcatel-Lucent support representative or see the *5620 SAM Planning Guide* for more information.

Alcatel-Lucent recommends that you regularly back up the 5620 SAM database. A database backup provides a snapshot of the database that you can use to restore the network data. The reasons for performing a database backup include the following:

- To move a database from one station to another
- To recover from hardware or software errors
- To set aside a clean copy of the database before performing a system upgrade
- As a preventive measure before making major changes to the network

Note — During a database backup, the performance of database-related operations on the GUI or the OSS interface may be affected. Alcatel-Lucent recommends performing a database backup only during a period of low 5620 SAM activity.

1 The database must be in ARCHIVELOG mode to perform a backup. Perform Procedure 7-6 and ensure that Archive Log Mode is set to ARCHIVELOG.

2 Click on the Backup tab.

3 Perform one of the following.

a Configure a scheduled full or partial database backup. A full backup backs up the entire 5620 SAM database whereas a partial backup contains no accounting statistics data.

i Configure the parameters:

Note — Ensure that the Scheduled Backup Directory location is not tampered with and has more than enough space to contain the number of database backups specified by the Number to Keep parameter.

ii Select the Schedule Enabled parameter.

b Perform an unscheduled full database backup. A full backup backs up the entire 5620 SAM database.

i Configure the Manual Backup Directory parameter.

Note — Ensure that the Manual Backup Directory location is not tampered with and has more than enough space to contain the database backup

ii Click on the Full Backup button. A dialog box appears.

iii Click on the Yes button. The full backup starts. The Backup State shown on the form changes to In Progress.

c Perform an unscheduled partial database backup. A partial backup contains no accounting statistics data.

i Configure the Manual Backup Directory parameter.

Note — Ensure that the Manual Backup Directory location is not tampered with and has more than enough space to contain the database backup

ii Click on the Partial Backup button. A dialog box appears.

iii Click on the Yes button. The partial backup starts. The Backup State shown on the form changes to In Progress.

4 Configure the Enable Backup File Compression parameter.

5 View the information in the Backup Status panel, if required. This information includes the following:

- Scheduled Backup—whether a backup schedule is configured
- Backup State—the state of the current or previous backup operation; the Backup State is dynamically updated during a backup operation
- Next Scheduled Backup Time—the next scheduled backup time
- Last Successful Backup Time—when the previous successful backup completed
- Last Successful Backup Type—the type of previous successful backup completed
- Last Attempted Backup Time—when the previous attempted backup took place
- Last Attempted Backup Type—the type of backup that was last attempted
- Directory of the Last Successful Backup—the storage location of the previous successful backup

6 Close the Database Manager (Edit) form.

Note — After backing up and restoring a database, you must perform a full resynchronization of the network to discover the recent managed device information changes.

Procedure 11-5 To back up the 5620 SAM database using a CLI script

Caution — Ensure that there is sufficient hard disk space to store the database backup. Alcatel-Lucent recommends that a separate database backup directory is created to store backup files. This backup directory should be at least five times larger than the expected database backup size. Contact your Alcatel-Lucent support representative or see the *5620 SAM Planning Guide* for more information.

Alcatel-Lucent recommends that you regularly back up the 5620 SAM database. A database backup provides a snapshot of the database that you can use to restore the network data. The reasons for performing a database backup include the following:

- To move a database from one station to another
- To recover from hardware or software errors
- To set aside a clean copy of the database before performing a system upgrade
- As a preventive measure before making major changes to the network

Note — During a database backup, the performance of database-related operations on the GUI or the OSS interface may be affected. Alcatel-Lucent recommends performing a database backup only during a period of low 5620 SAM activity.

1 Log in as the Oracle management user on the database station. In a redundant 5620 SAM system, this is the station that holds the primary database.

2 Open a console window.

3 Enter the following at the console prompt to begin the database backup:

```
path/install/config/samdb/SAMbackup.sh backup_directory ↵
```

where

path is the 5620 SAM database installation location, typically /opt/5620sam/samdb

backup_directory is the directory that is to contain the database backup

Caution — When you back up a 5620 SAM database, you must specify a backup directory path that does not include the 5620 SAM database installation directory, or data loss may occur. The typical 5620 SAM database installation location is /opt/5620sam/samdb.

The database backup begins. A database backup can take several hours to complete.

4 Close the console window when the database backup is complete.

11.4 Collecting and storing 5620 SAM log and configuration files

When a 5620 SAM system runs for long periods with significant activity, the number of generated log files can consume a large amount of disk space. You must ensure that the contents of the 5620 SAM log directories are backed up on a regular basis to maintain a system activity record and to save disk space. Alcatel-Lucent also recommends that you back up the 5620 SAM configuration files.

Note — You must contact your Alcatel-Lucent technical support representative to modify the 5620 SAM log storage parameters.

Procedure 11-6 To back up the 5620 SAM log and configuration files

Perform this procedure to save a copy of the 5620 SAM installation log and configuration files for later analysis in the event of a failure.

Note — During a system restart, 5620 SAM log files are backed up to directories that are named using a timestamp. A component that runs for a long time can generate multiple log files. Before you restart a 5620 SAM component, ensure that there is sufficient disk space to store the backed-up log files.

1 Collect the installation log files from the /tmp directory on a RHEL or Solaris station, or from the C:\5620sam directory on a Windows client station. The installation log files are named 5620_SAM_*application_type*_stderr.txt and 5620_SAM_*application_type*_stdout.txt.

where *application_type* indicates the 5620 SAM component type, for example, dbconfig or Server_Install

2 Collect the following 5620 SAM database, server, JMS server, and client system and log files, as required.

- **i** Collect the database dbconfig.properties file, which contains database configuration setting information, from the *installation_directory*/config directory on each database station.
- **ii** Collect the nms-server.xml file, which contains server configuration setting information, from the *installation_directory*/nms/config directory on each main server station.
- **iii** Collect the log files from the *installation_directory*/nms/log directory. There may be many log files in this directory, depending on how long the 5620 SAM software is running.

  When a 5620 SAM log file reaches a predetermined size, the 5620 SAM closes, compresses, and renames the file by including a sequence number and a timestamp. The following is an example of the filename format:

  EmsServer.#.*timestamp*.log

  where

# is a sequence number; the sequence begins at 0

timestamp is the time of closure, in the following format:
YYYY-MM-DD_hh-mm-ss

iv Collect the nms-auxserver.xml file, which contains server configuration settings, from the *installation_directory*/nms/config directory on each auxiliary server.

v Collect the *installation_directory*/nms/config/nms-client.xml file from each client station. This file contains the client configuration settings. Rename each file to indicate the client GUI station from which it is copied.

3 Transfer the log files to a secure location that is not in the network management domain.

11.5 Backing up NMS domain platforms

Alcatel-Lucent recommends that you should backup all NMS domain platforms running the 5620 SAM application software on a daily basis.

Use your company IT maintenance policies to create backups of all directories on each network management station. These backups can be used to restore an entire platform after a hardware or OS failure.

12 — Weekly maintenance tasks

12.1 Verifying performance statistics collection

Use the performance monitoring statistic log records to determine whether performance statistics are collected within the scheduled interval using the client GUI.

Procedure 12-1 To check for performance monitoring statistics collection

1 Choose Tools→Statistics Browser from the 5620 SAM main menu. The Browse Statistics form opens.

2 Set the Statistics Type parameter to Statistics Record to retrieve a list of historical data for the type of logged statistics.

3 Choose a type of statistics to collect from the Select Object Type... drop-down menu. For example, to check interface statistics for managed devices, choose Interface Additional Stats (Physical Equipment).

4 Perform one of the following:

- **a** To collect statistics for the past hour, click on the Search button. Go to step 6.
- **b** To collect statistics based on a set of user-defined criteria, choose No Filter from the Object Type filter drop-down menu.

5 Configure the filter criteria and click on the Search button.

Note — You must specify a filter to limit the number of log records to less than 15 000; otherwise, a problem encountered form appears.

6 Review the data for the selected statistic.

- **i** Click on the Monitored Object or Monitored Object Name headings to sort the historical statistics records by type of object.
- **ii** Review the Time Captured heading for one or more objects.

  Verify that the time captured intervals match the intervals set for the object or the statistic logging class, as specified in the *5620 SAM User Guide*.

  If the time captured intervals are not sufficient, there will be gaps in the historical record.

7 If there are gaps in the historical record, check the mediation policy to ensure that:

- polling is enabled and administratively up
- the polling interval for a specific MIB or MIB entry is sufficient for collecting the required statistics

Note — Each row that represents a log record shows the Suspect column. When a check mark is present for an interval, there may have been a problem with collection during that interval.

8 Record the data for the selected device and type of statistics. Use this data as a base measurement to verify that statistics data was collected correctly over the scheduled interval.

12.2 Gathering inventory data for device base performance checks

You can collect device hardware inventory information to:

- create a list of managed devices objects, for example, access ports that are available as SAPs
- save the lists for future processing and inventory uses
- compare the current and historical lists for status change trends, usage, and other post-processing applications
- record the time required to gather inventory data as a base measure for future performance checks

See the inventory chapter in the *5620 SAM User Guide* for more information about generating specific types of inventory reports.

Procedure 12-2 To gather port inventory data for a specific managed device

For most inventory lists you can:

- generate an inventory of the listed data
- reorganize the information from most important to least important
- remove columns of data
- sort rows in ascending or descending order

1 Choose Manage→Equipment→Equipment from the 5620 SAM main menu. The Manage Equipment form opens.

2 Choose a Network Element (Network) from the object drop-down menu and click on the Search button. The list form displays the results of the inventory search.

3 Choose an NE from the list and click on the Properties button. The Network Element (Edit) form opens.

4 Click on the Inventory tab and choose Port (Physical Equipment) from the object drop-down menu. The list form displays the results of the inventory search for the selected device.

5 Generate a list based on the inventory collection or comparison that you plan to make. For example, to compare weekly lists of access ports, generate a filter to list only access ports.

6 Record the amount of time required to generate the inventory list for future base measure comparisons.

7 Show or hide columns of access port information as required. For example, to hide Administrative State information:

- **i** Right-click on the Site ID heading. The contextual list menu appears.
- **ii** Deselect the Administrative State check box. The Administrative State column of data is removed from the access port list.

8 Save the list of access ports.

- **i** Right-click on a column heading to display the contextual list menu.
- **ii** Choose Save To File from the contextual list menu. The Save form opens.
- **iii** Enter a filename; for example, access_device123_*dateoflistgeneration*.
- **iv** Click on the Files of Type button to specify the file type.
- **v** Browse to choose a location in which to save the file.
- **vi** Click on the Save button. The file is saved to the specified location with the appropriate file extension.

9 You can save the table preferences for future use.

- **i** Right-click on a column heading to display the contextual list menu.
- **ii** Choose Save Table Preferences from the contextual menu. A dialog box appears.
- **iii** Click on the Yes button.

  The table preferences for the list form and user are saved. For example, when you choose another device, and click on the Ports tab and the Physical Ports tab, the Administrative State heading is not displayed. However, when you click on the SONET Channels tab, the Administrative State heading appears.

10 Move the file to another station, as required, for inventory analysis or post-processing.

12.3 Testing 5620 SAM database restores

When you create daily 5620 SAM database backups, the 5620 SAM backups should be tested to ensure that they can be used to restore the 5620 SAM database in the case of a catastrophic failure.

Caution 1 — Do not perform the database restore test in the NMS domain. Ensure that there is no IP connectivity to any live network devices.

Caution 2 — This procedure does not cover managed device database backups. See the *5620 SAM User Guide* for more information about managed device database backups and restores.

Procedure 12-3 To test a 5620 SAM database restore

Caution — Performing any database modifications using the Oracle database or tablespace tools can cause irreparable harm to the database and your network management data. Performing such modifications can void your Alcatel-Lucent warranty and support agreements. Contact your Alcatel-Lucent technical support representative to help you troubleshoot your database.

1 Generate comparison points for the 5620 SAM database, for example, the number of managed devices and cards, by creating an inventory of information, as described in the *5620 SAM User Guide*. This information is used to compare against the restored database information in a test environment to check the validity of the database backup.

2 Ensure that a recent database backup, such as from as scheduled backup operation, is available. Perform a 5620 SAM database backup, if required, as described in Procedure 11-4.

3 Shut down:

- any currently running 5620 SAM applications on the station on which the database restore test is to occur
- other 5620 SAM applications in the domain where the restore is to occur

4 FTP the database backup to the test station.

Caution — The station must not have IP connectivity to the managed devices in the network.

5 Ensure that the test database station has the same system configuration as the actual database station, for example, partitioning, OS version and OS patch level.

6 As the oracle management user, open the 5620 SAM database installer from the appropriate directory on the product DVD.

a On a RHEL station:

i Enter the following:

```
# cd Linux ↵
```

ii Enter the following:

```
# ./DBConfig_RHEL_R_r_revision.bin ↵
```

where
R_r is the release identifier, in the form *MAJOR_minor*
revision is the revision identifier, such as R1, R3, or another descriptor

b On a Solaris station:

i Enter the following:

```
# cd Solarisx86 ↵
```

ii Enter the following:

```
# ./DBConfig_SolarisX86_SAM_R_r_revision.bin ↵
```

where
R_r is the release identifier, in the form *MAJOR_minor*
revision is the revision identifier, such as R1, R3, or another descriptor

The 5620 SAM database configuration utility opens.

7 Follow the prompts, as specified in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide*. Specify a restore of the database from a backup version.

8 Enter the following database restore information, which is available when you choose Administration→Database from the 5620 SAM client GUI main menu:

- database name; for example, samdb
- DBID, the unique numerical identifier of the database
- database instance name; for example, samdb1 or samdb2

9 Specify the directory in which the recently backed-up database is located.

10 Specify whether to create a copy of the backup database. When the backup database is restored, Oracle modifies the backup and it cannot be reused. Create a copy if you need an additional database backup.

11 Specify any additional parameters, as described in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide*.

12 Review the comparison points of the restored backup database with the actual database, as generated in step 1. When the databases are the same, the backup and restore operation is successful.

12.4 Checking scheduled device backups

When the 5620 SAM performs a device configuration backup, the 5620 SAM FTPs the following files from the NE:

- bof.cfg
- primary-config file specified in bof.cfg
- index file, which is the primary-config file with an .ndx extension

Before you schedule a backup, you must:

- have a 5620 SAM user account with an assigned admin scope of command role or a scope of command role with write access to the mediation package.
- have a user account with FTP access on the managed device
- ensure the BOF persist parameter is set by typing the command: <show bof>. The parameter should be set to <persist on>.

Procedure 12-4 To check scheduled device backup status

1 Choose Administration→NE Maintenance→Backup/Restore from the 5620 SAM main menu. The Backup/Restore form opens with the Backup/Restore Policy tab displayed.

2 Click on the Backup/Restore Status tab. The managed devices are listed and backup and restore status information is displayed.

3 Select the device and click on the Properties button. The NE Backup/Restore Status form opens with the General tab displayed.

4 View the information in the Backup Status panel. A Backup State other than Successful may indicate a communication problem or a backup policy configuration error.

5 Ensure that the device configuration file and the associated index file are saved on the device and available for backup. Click on the Configuration Saves tab, and ensure that the Config Save State indicator reads Success.

See the appropriate device operating-system documentation for more information.

6 Click on the Backups tab to view a list of backup operations that are currently in progress. A backup operation disappears from the list after it completes.

7 Click on the Faults tab to view additional troubleshooting information.

8 Close the NE Backup/Restore Status form.The Backup/Restore form is displayed.

9 Use the information obtained from the NE Backup/Restore Status form to check the backup policy configuration, if required. Click on the Backup/Restore Policy tab.

10 Select the backup policy for the device and click on the Properties button. The Backup Policy (Edit) form opens with the General tab displayed.

11 Ensure that the policy is assigned to the device.

   i Click on the Backup/Restore Policy Assignment tab. The Backup Policy - Filter form opens.

   ii Configure the policy filter criteria.

   iii Click on the OK button. The Backup Policy - Filter form closes.

   iv Move the device to the Assigned Sites list if it is not there by selecting the site from the Unassigned Sites list and clicking on the right-arrow button.

   v Click on the Apply button to save changes, as required.

12 Click on the General tab.

13 Select the Enable Backup check box.

14 Modify the other parameters, if required.

15 Click on the OK button to save the changes and close the form.

12.5 Oracle audit log management

As part of the Oracle security functions, audit log files are automatically created to track database session creation activities. These files are not removed automatically by the 5620 SAM. You must monitor the directory that contains the audit log files to ensure that the files do not consume excessive disk space.

Procedure 12-5 To reduce the number of Oracle audit logs

1 Log in to the 5620 SAM database station as the Oracle management user.

2 Navigate to the *Oracle_base_directory*/rdbms/audit directory

where *Oracle_base_directory* is the directory in which the Oracle software is installed, typically /opt/5620sam/oracle11r2

3 Archive and delete the files, as required. If the number of audit files increases quickly, you may need to perform this procedure more frequently.

13 — Monthly maintenance tasks

13.1 Performing main server and database activity switches

In a redundant 5620 SAM deployment, performing regular main server and database activity switches is important for the following reasons:

- to ensure that 5620 SAM server and database redundancy functions correctly and responsively
- to identify problems that may interfere with a 5620 SAM upgrade

Note — Alcatel-Lucent strongly recommends that you perform a main server activity switch and a database activity switch monthly, or at least quarterly, if a monthly test is not possible. See Chapter 6 for information about performing a server or database activity switch. Contact your Alcatel-Lucent technical-support representative for further assistance.

13.2 Checking the 5620 SAM platform performance

Use the following procedure to test system performance and record base measures. You can compare platform performance monthly to:

- collect base measure information related to platform performance
- ensure that there is no degradation in performance

If the platform performance degrades, collect the necessary logs and performance data measures and contact your Alcatel-Lucent support representative. See the *5620 SAM Troubleshooting Guide* for information about 5620 SAM log collection.

Procedure 13-1 To check the 5620 SAM platform performance

Use UNIX utilities to review process and CPU usage data.

1 Open a command window.

2 Run a command on the client GUI, server, and database stations to check CPU usage for processes:

i Type one of the following:

- On a Solaris station:

  ```
  prstat ↵
  ```

- On a RHEL station:

  ```
  top ↵
  ```

Depending on your system configuration, approximately the top 20 processes are displayed.

ii Review the output.

The top 5620 SAM process listed under the CPU column should be the Java process. However, the Java process should not consume the majority of CPU cycles, compared to previous base measures. Some Oracle processes may also take CPU time, depending on the database load.

iii Record the data for future base measure comparison of station performance.

iv Press CTRL-C to stop the command.

3 If the station OS is Solaris, go to step 5.

4 Use the mpstat command to review the activities performed by the CPU.

i Enter the following:

```
# mpstat time ↵
```

where *time* is the interval, in seconds, between CPU polls; a value between 10 and 60 is recommended

ii Review the command output. Code 13-1 is an example of RHEL mpstat output; Table 13-1 describes each output field.

Code 13-1: RHEL mpstat output example

```
CPU    %usr   %nice    %sys %iowait    %irq    %soft  %steal %guest   %idle
all    0.25    0.00    0.17    0.00    0.00    0.00    0.00    0.00   99.58
```

Table 13-1 RHEL mpstat field descriptions

Heading	Description (events per second unless noted)
CPU	Processor number; the keyword all indicates that statistics are calculated as averages among all processors
%usr	Percentage of CPU utilization at the user application level
%nice	Percentage of CPU utilization at the user level with nice priority
%sys	Percentage of CPU utilization at the system level; does not include time spent servicing hardware and software interrupts
%iowait	Percentage of CPU idle time during which the system had an outstanding disk I/O request
%irq	Percentage of CPU time spent servicing hardware interrupts
%soft	Percentage of CPU time spent servicing software interrupts
%steal	Percentage of time spent in involuntary wait by the virtual CPU or CPUs during hypervisor servicing of another virtual processor
%guest	Percentage of CPU time spent running a virtual processor
%idle	Percentage of CPU idle time without an outstanding disk I/O request

iii Record the data for future base measure comparisons of station performance.

Look for differences in the output of the data for similar loads on each station. Such differences indicate performance degradation.

iv Press CTRL-C to stop the command.

5 Use the mpstat command to review the activities performed by the CPU.

i Enter the following:

```
# mpstat time ↵
```

where *time* is the interval, in seconds, between CPU polls; a value between 10 and 60 is recommended

ii Review the command output. Code 13-2 is an example of Solaris mpstat output; Table 13-2 describes each output field.

Code 13-2: Solaris mpstat output example

```
CPU minf mjf xcal  intr  ithr  csw  icsw migr smtx  srw  syscl usr sys  wt idl
 0    5   0    0   258   55    87    1    0    0    0   196    5   15   0  80
```

Table 13-2 Solaris mpstat field descriptions

Heading	Description (events per second unless noted)
CPU	Processor identification
minf	Minor faults
mjf	Major faults
xcal	Interprocessor cross-calls
intr	Interrupts
ithr	Interrupts as threads (not counting clock interrupts)
csw	Context switches
icsw	Involuntary context switches
migr	Thread migrations to another processor
smtx	Spins on mutexes (lock not acquired on first try)
srw	Spins on readers/writer locks (lock not acquired on first try)
syscl	System calls
usr	Percent user time
sys	Percent system time
wt	Percent wait time
idl	Percent idle time

iii Record the data for future base measure comparisons of station performance.

Look for differences in the output of the data for similar loads on each station. Such differences indicate performance degradation.

iv Press CTRL-C to stop the command.

6 If the station OS is Solaris, go to step 8.

7 Use the iostat command to collect disk read and write data for determining whether there is a disk bottleneck.

i Type:

```
iostat -x time ↵
```

where *time* is the time period, in seconds, during which you need to collect data. Alcatel-Lucent recommends that you start with 2 s

ii Review the command output. Code 13-3 is an example of RHEL iostat output; Table 13-3 describes each output field.

Code 13-3: RHEL iostat output example

```
Device:            tps   Blk_read/s   Blk_wrtn/s   Blk_read   Blk_wrtn
sdb               0.01         0.04         6.63      11573    1810153
sda               2.94        58.78       261.56   16040031   71372946
```

Table 13-3 RHEL iostat field description

Heading	Description
device	Name of the device
tps	Transfers per second
Blk_read/s	Block reads per second
Blk_wrtn/s	Block writes per second
Blk_read	Total blocks read
Blk_wrtn	Total blocks written

iii Record the data for future comparison of platform performance. Look for differences in the output of the data for similar loads on each station, which indicate performance degradation.

iv Press CTRL-C to stop the iostat command.

8 Use the iostat command to collect disk read and write data for determining whether there is a disk bottleneck.

i Type:

```
iostat -x time ↵
```

where *time* is the time period, in seconds, during which you need to collect data. Alcatel-Lucent recommends that you start with 2 s

ii Review the command output. Code 13-4 is an example of Solaris mpstat output; Table 13-4 describes each output field.

Code 13-4: Solaris iostat output example

```
                          extended device statistics
device   r/s  w/s    Kr/s   Kw/s   wait actv  svc_t  %w  %b
sd1      0.1  0.2    0.9    3.3    0.0  0.0   34.3   0   0
sd3      0.1  0.5    1.1    3.7    0.0  0.0   73.1   0   90
```

Table 13-4 Solaris iostat field description

Heading	Description
device	Name of the device
r/s	Reads per second
w/s	Writes per second
Kr/s	Reads per second (kb/s)
Kw/s	Writes per second (kb/s)
wait	Average number of transactions waiting for service (queue length)
actv	Average number of transactions actively being serviced (removed from the queue but not yet complete)
svc_t	Average service time in ms
%w	Percentage of time there are transactions waiting for service (non-empty queue)
%b	Percentage of time the disk is busy (transactions in progress)

iii The %b and svc_t columns are the key fields determining whether a disk bottleneck exists. When the svc_t is between 30 and 50 ms, and the %b is greater than 20% busy, there is a minor disk loading problem. If the svc_t exceeds 50 ms, the disk is considered I/O-bound, and a disk bottleneck exists.

In the sample output, the sd3 disk had 90% disk activity in the %b column. Because disk sd3 is busier than disk sd1, disk performance may be enhanced by moving data from disk sd3 to disk sd1.

iv Record the data for future comparison of platform performance. Look for differences in the output of the data for similar loads on each station, which indicate performance degradation.

v Press CTRL-C to stop the iostat command.

9 Use the netstat command to check for network interface performance issues.

i Type:

`netstat -i` ***`time`*** ↵

where *time* is the time period, in seconds, over which you need to collect data. Alcatel-Lucent recommends that you start with 5 s.

ii Review the netstat output.

13.3 Checking Windows client platform performance

You can compare Windows client station performance monthly to:

- collect base measure information related to platform performance
- ensure that there is no degradation in performance

Procedure 13-2 To check Windows client station performance

1 Open a command window on the client station.

2 Enter the following at the command prompt:

```
ping station_name ↵
```

where *station_name* is the IP address or hostname, if DNS is used, of the main server to which you need to test connectivity

3 Review the ping output for round-trip delays or lost packets. Resolve any connectivity issues that cause delays or dropped packets. Store ping round-trip delay or lost-packet data as a performance base measure for the station. You can use the data for future performance comparisons.

4 Choose Start→Run from the Windows menu bar. The Run form opens.

5 Enter the following in the Open field:

```
taskmgr ↵
```

The Windows Task Manager form opens. It provides details about the programs and processes that run on the station. If you are connected to a LAN, you can also view the network status and check network performance. Depending on the NOC work environment and shared computer usage policy, you can also view additional information about other users.

6 Check performance using the appropriate Task Manager tab.

a Click the Processes tab. A list of processes appears.

Organize the processes according to CPU usage. The name of each 5620 SAM process begins with 5620SAM. The CPU usage percentage for each 5620 SAM process should fall within your IT specifications or the established performance base measures.

b Click on the Performance tab. The CPU and page file usage charts appear.

The memory and page-file usage percentages should fall within your IT specifications or the established performance base measures.

c Click on the Networking tab. The Local Area Connection chart appears.

Network utilization greater than 10 or 20 percent may indicate collisions or other LAN problems that could affect performance in the network management domain.

7 Choose File→Exit Task Manager to close the form.

8 Open an MS-DOS command window.

9 Type:

```
tracert station_name ↵
```

where *station_name* is the IP address or hostname of the main server to which you need to test connectivity

The tracert command provides details about network connectivity.

10 Review the tracert data, including:

- number of hops required to reach the main server
- average time between hops

Record the data for future base measure comparison. For example, when the number of hops between a client GUI and main server increases over time, traffic takes longer to travel between them, which can degrade performance.

11 Check regularly for advisories related to the OS. If updates or patches are required, contact your IT department or your Alcatel-Lucent support representative for information about potential effects on the 5620 SAM software.

13.4 Checking LAN TCP/IP connections between network-management domain elements

Use the ping and traceroute functions each month to check LAN TCP/IP connectivity between elements in the network-management domain, such as the 5620 SAM client, main server, auxiliary server, and database platforms. Contact your IT department if there appears to be a communication problem between elements.

Procedure 13-3 To check network management connections

1 Open a console window on the station.

2 Ping the hostname of another station in the network management domain by entering one of the following:

a On a RHEL or Windows station:

```
ping station_name ↵
```

where *station_name* is the IP address or hostname of the other station

b On a Solaris station:

```
ping -s station_name ↵
```

where *station_name* is the IP address or hostname of the other station

3 Review the output. The following is an example of ping output:

```
PING station_name: 56 data bytes
```

```
64 bytes from station_name (station_IP_address): icmp_seq=0,
time=1. ms

64 bytes from station_name (station_IP_address): icmp_seq=1,
time=0. ms

64 bytes from station_name (station_IP_address): icmp_seq=2,
time=0. ms

----station_name PING Statistics----

3 packets transmitted, 3 packets received, 0% packet loss

round-trip (ms) min/avg/max = 0/0/1
```

LAN congestion may be a problem if packets are received out of order, are dropped, or take too long to complete the round trip.

4 Store the output for future base measure comparison.

Compare the output over time to ensure that changes in the data are not caused by deteriorating LAN conditions.

5 Check the routing information.

i Open a console window on the station.

ii Enter one of the following traceroute commands to determine the path taken to a destination by an ICMP echo request message:

- traceroute ↵ on a RHEL or Solaris station
- tracert ↵ on a Windows station

The list of near-side interfaces in the path between a source host and a destination device is displayed. The near-side interfaces are the interfaces closest to the source host.

6 Store the output as a record for future base measure comparisons. Compare routes over time to ensure that there is optimal connectivity.

7 To check the routing tables for the platform:

i Open a console window on the station.

ii To view the active routes for the platform, type:

```
netstat -rn ↵
```

The following information is displayed:

- network destination and gateway IP addresses
- gateway used to reach the network destination
- IP address of the interface on which communication occurs
- metric value of the route

8 Store the output as a record for future base measure comparison. Compare routes over time to ensure that there is optimal connectivity.

13.5 Generating and storing a user account list

System administrators should keep a record of 5620 SAM users to:

- associate staff names with user accounts
- provide account information to TAC or Support staff as required for support to log in
- review user account privileges

Procedure 13-4 To generate and store user account data

1 As admin user, choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The User Security -- Security Management (Edit) form opens.

2 Click on the Users tab.

3 Click on the Search button without setting any filtering. The complete list of user accounts appears.

4 Organize the list of users. For example, to organize the list by the type of group that the user belongs to, click on the User Group column heading. The user accounts are listed alphabetically by user group.

5 Save the list of user accounts.

- **i** Right-click on the user name list heading and choose Save To File from the contextual menu. The Save form opens.
- **ii** Enter a name for the user account list, for example, NOCabc_useraccounts_*yearmonthday*.
- **iii** Click on the Files of Type pull-down menu to specify the file type.
- **iv** Browse to choose a location in which to save the file.
- **v** Click on the Save button. The file is saved to the selected location in the specified format with the appropriate extension.

6 Move the account list to a secure location. Store the latest version of the list and keep existing versions of the list for historical purposes.

13.6 Verifying documentation and support contact list updates

Use the http://www.alcatel-lucent.com/support website as the source for 5620 SAM technical information and updates to:

- check for changes to TAC, Support, and Call Centre information
- find additional product updates, updated user documentation, and documentation generated for specific situations, such as Network Application Notes, Technical Notes, Product Change Notifications, and Field Notices

You should also regularly check your 5620 SAM platform vendor websites for information about OS patches, updates, and other software and hardware issues.

Procedure 13-5 To check for documentation and support updates

Note — You need a Support Documentation Service account to view customer documentation. Contact your Alcatel-Lucent account representative for more information.

1 Log in to https://www.alcatel-lucent.com/support.

2 Enter your login user name and password when prompted.

3 Click on the Support Documentation Service link.

4 Narrow the documentation search to 5620 SAM.

- **i** Set the Select a product category field to Network Management.

  The Select a product field list is updated.

- **ii** Set the Select a product field to 5620 SAM.

- **iii** Set the Select a type field to the type of information you are looking for, for example:

  - All types to view all applicable documentation for the product
  - Installation for a list of installation guides, sorted by date and release
  - Product Manual for list of guides, such as the *5620 SAM User Guide*, sorted by date and release
  - Release Description for a list of release descriptions that describe release information, such as feature overviews, supported platforms, and scalability considerations
  - Release Notice for a list of release notices that describe load information, such as outstanding and closed problem lists, and restrictions to functionality

5 Click on the Search button. The list of documents appears.

Note — You can also use the enhanced search feature to search for 5620 SAM updates between specified dates. Alternately, you can configure your user profile on the Alcatel-Lucent home page to automatically notify you of new 5620 SAM user information.

6 Download the documents.

7 Check for TAC, Call Center, or Support updates:

- **i** Click on the Support link.

- **ii** Click on the Global Support link.

- **iii** Click on the Carrier/Service Provider link.

iv Click on the link to the global technical support organization that supports your organization.

v Check the contact information for your regional Customer Service or Call Center.

13.7 Setting the time and date

You can use a variety of time synchronization and network time protocol tools, depending on network design needs, including:

- ntpd, xntpd, or rdate, for network management domain devices
- the clock function on Windows a station
- SNTP, for devices in the managed network

Alcatel-Lucent recommends that you keep time synchronous between network devices, for example, timing between routers. See the appropriate OS documentation or man pages for more information about using time and date synchronization protocols.

Note 1 — Timing between the 5620 SAM servers and clients must be synchronized.

Note 2 — Alcatel-Lucent only supports changing the time or date forward on 5620 SAM servers, databases, or clients.

14 — As required maintenance tasks

14.1 General 5620 SAM platform changes

After you make a change to the physical 5620 SAM server, database, or platform, such as increasing or decreasing the amount of RAM, adding or removing a CPU, or installing another NIC type, you must uninstall and reinstall the 5620 SAM software.

Caution — To prevent a network management outage, Alcatel-Lucent recommends that you contact 5620 SAM technical support before you modify the platform of a 5620 SAM component.

14.2 Adding or removing RAM

After you change the amount of RAM on a 5620 SAM station, you must do the following before you restart the 5620 SAM component on the station:

- database station—reconfigure the Oracle System Global Area, or SGA; see Procedure 14-1
- main server station—run the 5620 SAM server installer using the “Main Server Configuration” option; see Procedure 14-2
- auxiliary server station—run the 5620 SAM server installer using the “Auxiliary Server Configuration” option; see Procedure 14-3

Caution — The procedures in this section are to be performed only during a scheduled maintenance period, when the 5620 SAM system is shut down for the RAM upgrade.

Procedure 14-1 To reconfigure a 5620 SAM database after a RAM upgrade

Perform this procedure after a change in the amount of RAM on a 5620 SAM database station.

Note — You require root user privileges on the database station to perform this procedure.

1 Log in as the root user on the database station.

2 Open a console window.

3 Enter the following to stop the 5620 SAM database application:

```
# /etc/rc3.d/S95db5620sam stop ↵
```

Do not proceed until the command returns the following text string:

```
Done
```

4 Enter the following to run the Oracle SGA reconfiguration script:

```
# /opt/5620sam/db_name/install/config/db_name/SGA_reconfig.sh ↵
```

where *db_name* is the name of the 5620 SAM database, typically samdb

5 When the script execution is complete, enter the following to reboot the database station:

```
# init 6 ↵
```

The database station reboots.

Procedure 14-2 To reconfigure a 5620 SAM main server after a RAM upgrade

Perform this procedure to adjust the main server configuration after a RAM upgrade on the main server station.

Note — You require root and samadmin user privileges on the main server station to perform this procedure.

1 Log in as the samadmin user on the main server station.

2 Open a console window.

3 Perform the following steps to stop the main server, if it is running.

- **i** Enter the following to navigate to the server binary directory:

  ```
  bash$ cd path/nms/bin ↵
  ```

  where *path* is the main server installation location, typically /opt/5620sam/server

- **ii** Enter the following to stop the main server application:

  ```
  bash$ ./nmsserver.bash stop ↵
  ```

- **iii** Enter the following to display the main server status:

  ```
  bash$ ./nmsserver.bash appserver_status ↵
  ```

  The command displays a status message.

- **iv** The main server is stopped when the command displays the following status message:

  ```
  Application Server is stopped
  ```

  If the command displays another message, repeat step 3 iii. Do not proceed to the next step until the server is stopped.

4 Enter the following command to switch to the root user:

```
bash$ su -
```

5 Place the 5620 SAM software DVD-ROM in a DVD-ROM drive.

6 Open a console window.

7 Navigate to the DVD-ROM drive.

8 Perform one of the following to open the 5620 SAM server installer.

a On a RHEL station:

i Enter the following:

```
# cd Linux ↵
```

ii Enter the following:

```
# ./ServerInstall_RHEL_R_r_revision.bin ↵
```

where
R_r is the release identifier, in the form *MAJOR_minor*
revision is the revision identifier, such as R1, R3, or another descriptor

b On a Solaris station:

i Enter the following:

```
# cd Solarisx86 ↵
```

ii Enter the following:

```
# ./ServerInstall_SolarisX86_SAM_R_r_revision.bin ↵
```

where
R_r is the release identifier, in the form *MAJOR_minor*
revision is the revision identifier, such as R1, R3, or another descriptor

The 5620 SAM server installer opens, and displays the Introduction panel.

9 Click on the Next button. The Software License Agreement panel is displayed.

10 Select “I accept the terms of the License Agreement” and click on the Next button. The Choose Installation Type panel is displayed.

11 Select Main Server Configuration.

12 Click on the Next button.

13 Click on the Next button in each subsequent panel until the XML Output Directory panel is displayed.

14 Click on the Install button. The installer reconfigures the 5620 SAM server, and then displays the Installing the Server as a Unix Daemon panel.

15 Click on the Next button. The Installation Complete panel is displayed.

16 Click on the Done button. The installer closes.

17 Close the console window.

Procedure 14-3 To reconfigure a 5620 SAM auxiliary server after a RAM upgrade

Perform this procedure to adjust the auxiliary server configuration after a RAM upgrade on the auxiliary server station.

Note — You require root and samadmin user privileges on the auxiliary server station to perform this procedure.

1 Log in as the samadmin user on the auxiliary server station.

2 Open a console window.

3 Perform the following steps to stop the auxiliary server, if it is running.

   i Enter the following to navigate to the server binary directory:

```
bash$ cd path/nms/bin ↵
```

   where *path* is the auxiliary server installation location, typically /opt/5620sam/auxserver

   ii Enter the following to stop the auxiliary server application:

```
bash$ ./auxnmsserver.bash stop ↵
```

   iii Enter the following to display the auxiliary server status:

```
bash$ ./auxnmsserver.bash appserver_status ↵
```

   The command displays a status message.

   iv The auxiliary server is stopped when the command displays the following status message:

```
Auxiliary Server is stopped
```

   If the command displays another message, repeat step 3 iii. Do not proceed to the next step until the server is stopped.

4 Enter the following command to switch to the root user:

```
bash$ su -
```

5 Place the 5620 SAM software DVD-ROM in a DVD-ROM drive.

6 Open a console window.

7 Navigate to the DVD-ROM drive.

8 Perform one of the following to open the 5620 SAM server installer.

- **a** On a RHEL station:
  - **i** Enter the following:

    ```
    # cd Linux ↵
    ```

  - **ii** Enter the following:

    ```
    # ./ServerInstall_RHEL_R_r_revision.bin ↵
    ```

    where
    R_r is the release identifier, in the form *MAJOR_minor*
    revision is the revision identifier, such as R1, R3, or another descriptor

- **b** On a Solaris station:
  - **i** Enter the following:

    ```
    # cd Solarisx86 ↵
    ```

  - **ii** Enter the following:

    ```
    # ./ServerInstall_SolarisX86_SAM_R_r_revision.bin ↵
    ```

    where
    R_r is the release identifier, in the form *MAJOR_minor*
    revision is the revision identifier, such as R1, R3, or another descriptor

The 5620 SAM server installer opens, and displays the Introduction panel.

9 Click on the Next button. The Software License Agreement panel is displayed.

10 Select “I accept the terms of the License Agreement” and click on the Next button. The Choose Installation Type panel is displayed.

11 Select Auxiliary Server Configuration.

12 Click on the Next button.

13 Click on the Next button in each subsequent panel until the XML Output Directory panel is displayed.

14 Click on the Install button. The installer reconfigures the 5620 SAM server, and then displays the Installing the Server as a Unix Daemon panel.

15 Click on the Next button. The Installation Complete panel is displayed.

16 Click on the Done button. The installer closes.

17 Close the console window.

14.3 Relinking the Oracle executable files

You must relink the Oracle executable files on a 5620 SAM database station after you apply an OS patch, or after an OS upgrade.

Note 1 — You need Oracle management user privileges on the database station to perform this procedure.

Note 2 — This procedure requires a reboot of the 5620 SAM database station.

Procedure 14-4 To relink the Oracle executable files

1. Log in to the database station as the Oracle management user.
2. Open a console window.
3. Enter the following to run the relinking script:

```
bash$ /opt/5620sam/database_name/install/config/database_name/relinkOracle.sh ↵
```

where *database_name* is the name of the 5620 SAM database, for example, samdb on a standalone database station

The script relinks the Oracle executable files.

4. When the script execution is complete, reboot the database station.

14.4 Changing 5620 SAM database and Oracle user passwords

For greater security, Alcatel-Lucent recommends that you regularly change the 5620 SAM database user and Oracle SYS user passwords. You can optionally change other Oracle-user accounts passwords, if required. Procedure 14-5 describes how to change a password in a standalone system. Procedure 14-6 describes how to change a password in a redundant system.

Procedure 14-5 To change the Oracle SYS or database user password in a standalone 5620 SAM system

Perform this procedure to change the password of a user associated with the database or Oracle functions in a standalone 5620 SAM system.

Caution — The procedure requires a restart of the 5620 SAM main server, which is service-affecting. Alcatel-Lucent strongly recommends that you perform this procedure only during a scheduled maintenance period.

Note 1 — Before you perform the procedure, you must ensure that each 5620 SAM main server, auxiliary server, and database is running and operational.

Note 2 — You can use the procedure to change only one user password at a time. To change multiple user passwords, you must perform the procedure multiple times.

Note 3 — When you change a password on one station, the 5620 SAM automatically updates the password on all other 5620 SAM stations.

1 Log in to the main server station as the samadmin user.

2 Open a console window.

3 Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin.

4 Enter the following:

```
bash$ ./nmsserver.bash passwd ↵
```

The script prompts you for the current SYS user password.

5 Enter the password. The script validates the password, and then displays a list of user names like the following:

```
SAM Database Users:

 - sys

 - database_user_name (installation default is samuser)

Other Database Users:

- sqltxplain

- appqossys

- outln

- dip

- system


- exit
```

6 Enter a user name. The script prompts you for a password.

7 Enter the new password, which must:

- Be between 4 and 30 characters long
- Contain at least three of the following:
  - lower-case alphabetic character
  - upper-case alphabetic character
  - numeric character
  - special character, which is one of the following:
    # $ _
- Not contain four or more of the same character type in sequence
- Not be the same as the user name or the reverse user name
- Not contain a space character
- Differ by at least four characters from the current password

If the password is valid, the script prompts you to retype the password.

8 Enter the new password again. The script displays the following message:

```
WARNING: Changing passwords may cause instability to the 5620 SAM
server as well as the Oracle proxy on the database server.

Do you want to proceed (yes/no)?:
```

9 Enter yes ↵. The script displays status messages and then exits. If the status indicates a password change failure, contact Alcatel-Lucent technical support.

10 Record the password in a secure location.

11 Perform one of the following.

a If you are changing the SYS user password, perform the following steps.

i Log in to the database station as the root user.

ii Enter the following to stop the database proxy:

```
# /etc/rc3.d/S965620SAMOracleProxyWrapper stop ↵
```

Do not proceed until the command returns the following:

```
Done
```

iii Enter the following to start the database proxy:

```
# /etc/rc3.d/S965620SAMOracleProxyWrapper start ↵
```

Do not proceed until the command returns the following:

```
Done
```

iv Log out of the database station.

b If you are changing the database user password, perform the following steps.

i Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin.

ii Enter the following to restart the main server:

```
bash$ ./nmsserver.bash force_restart ↵
```

iii Enter the following to display the server status:

```
bash$ ./nmsserver.bash -s nms_status ↵
```

The command returns server status information.

If the main server is not completely started, the first line of status information is the following:

```
Main Server is not ready...
```

The main server is completely started when the command returns the following:

```
 -- SAM Server is UP
```

12 Close the console window.

Procedure 14-6 To change the Oracle SYS or database user password in a redundant 5620 SAM system

Perform this procedure to change the password of a user associated with the database or Oracle functions in a redundant 5620 SAM system.

Caution — The procedure requires a restart of each 5620 SAM main server, which is service-affecting. Alcatel-Lucent strongly recommends that you perform this procedure only during a scheduled maintenance period.

Note 1 — Before you perform the procedure, you must ensure that each 5620 SAM main server, auxiliary server, and database is running and operational.

Note 2 — You can use the procedure to change only one user password at a time. To change multiple user passwords, you must perform the procedure multiple times.

Note 3 — When you change a password on one station, the 5620 SAM automatically updates the password on all other 5620 SAM stations.

1 Log in to the primary main server station as the samadmin user.

2 Open a console window.

3 If you are changing the SYS user or 5620 SAM database user password, perform the following steps.

- **i** Navigate to the server configuration directory, typically /opt/5620sam/server/nms/config.

- **ii** Open the nms-server.xml file using a plain-text editor such as vi.

Caution — Contact Alcatel-Lucent technical support before you attempt to modify the nms-server.xml file. Modifying the nms-server.xml file can have serious consequences that can include service disruption.

- **iii** Locate the following parameter entry:

  ```
  dbAutoFailOver=
  ```

- **iv** Record the parameter value.

- **v** Edit the entry to read:

  ```
  dbAutoFailOver="no"
  ```

- **vi** Save and close the nms-server.xml file.

4 Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin.

5 Enter the following:

```
bash$ ./nmsserver.bash passwd ↵
```

The script prompts you for the current SYS user password.

6 Enter the password. The script validates the password, and then displays a list of user names like the following

```
SAM Database Users:

 - sys

 - database_user_name (installation default is samuser)

Other Database Users:
```

```
- sqltxplain

- appqossys

- outln

- dip

- system


- exit
```

7 Enter a user name. The script prompts you for a password.

8 Enter the new password, which must:

- Be between 4 and 30 characters long
- Contain at least three of the following:
  - lower-case alphabetic character
  - upper-case alphabetic character
  - numeric character
  - special character, which is one of the following:
    # $ _
- Not contain four or more of the same character type in sequence
- Not be the same as the user name or the reverse user name
- Not contain a space character
- Differ by at least four characters from the current password

If the password is valid, the script prompts you to retype the password.

9 Enter the new password again. The script displays the following message:

```
WARNING: Changing passwords may cause instability to the 5620 SAM
server as well as the Oracle proxy on the database server.

Do you want to proceed (yes/no)?:
```

10 Enter yes ↵. The script displays status messages and then exits. If the status indicates a password change failure, contact Alcatel-Lucent technical support.

11 Record the password in a secure location.

12 If you are changing a password other than the SYS or database user password, go to step 16.

13 If you are changing the SYS user password, perform the following steps on each database station.

i Log in to the database station as the root user.

ii Enter the following to stop the database proxy:

```
# /etc/rc3.d/S965620SAMOracleProxyWrapper stop ↵
```

Do not proceed until the command returns the following:

```
Done
```

iii Enter the following to start the database proxy:

```
# /etc/rc3.d/S965620SAMOracleProxyWrapper start ↵
```

Do not proceed until the command returns the following:

```
Done
```

iv Log out of the database station.

14 If you are changing the database user password, perform the following steps.

i Log in to the standby main server station as the samadmin user.

ii Navigate to the server binary directory, typically /opt/5620sam/server/nms/bin.

iii Enter the following to stop the main server:

```
bash$ ./nmsserver.bash stop ↵
```

The standby main server stops.

iv Enter the following to display the server status:

```
bash$ ./nmsserver.bash appserver_status ↵
```

The server application is stopped when the command returns the following:

```
Application Server is stopped
```

Caution — If the command returns a different message, wait five minutes and repeat the step. Do not proceed until the server application is stopped.

v On the primary main server station, enter the following:

```
bash$ ./nmsserver.bash force_restart ↵
```

The primary main server restarts.

vi Enter the following to display the server status:

```
bash$ ./nmsserver.bash -s nms_status ↵
```

The command returns server status information.

If the main server is not completely started, the first line of status information is the following:

```
Main Server is not ready...
```

The main server is completely started when the command returns the following:

```
 -- Primary Server is UP
```

Caution — If the command output indicates that the server is not completely started, wait five minutes and then repeat the step. Do not proceed to the next step until the server is completely started.

vii Close the console window on the primary main server.

viii Log out of the primary main server.

ix On the standby main server, enter the following to start the main server:

```
bash$ ./nmsserver.bash start ↵
```

The standby main server starts.

x Enter the following to check the server status:

```
bash$ ./nmsserver.bash -s nms_status ↵
```

The command returns server status information. The main server is completely started when the command returns the following line of output:

```
 -- Standby Server is UP
```

Caution — If the command output indicates that the server is not completely started, wait five minutes and then repeat the step. Do not proceed to the next step until the server is completely started.

15 If the dbAutoFailOver value recorded in step 3 is yes, perform the following steps.

i Navigate to the server configuration directory, typically /opt/5620sam/server/nms/config.

ii Open the nms-server.xml file using a plain-text editor such as vi.

Caution — Contact Alcatel-Lucent technical support before you attempt to modify the nms-server.xml file. Modifying the nms-server.xml file can have serious consequences that can include service disruption.

iii Locate the following parameter entry:

```
dbAutoFailOver=
```

iv Edit the entry to read:

```
dbAutoFailOver="yes"
```

v Save and close the nms-server.xml file.

vi Navigate to the server binary directory, typically `/opt/5620sam/server/nms/bin`.

vii Enter the following:

```
bash$ ./nmsserver.bash read_config ↵
```

The primary main server puts the configuration change into effect.

16 Close the console window.

17 Log out of the primary main server station.

14.5 Restoring a 5620 SAM database

You can restore a 5620 SAM database using a backup copy.

Note 1 — The station to which you restore a 5620 SAM database needs the same OS as the station from which the backup is obtained, or the restore fails.

Note 2 — Before you perform a database restore operation, you must shut down the databases and main servers in the 5620 SAM system. Contact Alcatel-Lucent technical support before you attempt to perform a database restore.

In a redundant 5620 SAM system, you must perform one or both of the following to regain database function and redundancy, depending on the type of failure.

- Restore the primary database.
- Reinstantiate the standby database.

Both operations are required after a primary database failure. After a standby database failure, no restore operation is required, but you must reinstantiate the primary database on the standby database station to restore redundancy. You can use the 5620 SAM client GUI or a CLI script to reinstantiate a database.

Note 1 — In a redundant 5620 SAM system, you can restore a database backup only on a primary database station. To restore a database backup on a station other than the primary station, you must do the following on the station before you attempt the restore:

- Uninstall the 5620 SAM database, if it is installed.
- Install a primary database on the station.

Note 2 — In a redundant 5620 SAM system, you can reinstantiate a database only on a standby database station. To reinstantiate a database on a station other than the standby station, you must do the following on the station before you attempt the reinstantiation:

- Uninstall the 5620 SAM database, if it is installed.
- Install a standby database on the station.

See Procedure 14-7 for information about restoring a standalone 5620 SAM database. See Procedure 14-8 for information about restoring a redundant 5620 SAM database. See Procedure 14-9 for information about reinstantiating a primary 5620 SAM database on a standby database station.

Procedure 14-7 To restore the database in a standalone 5620 SAM system

Perform this procedure to restore a standalone 5620 SAM database using a backup copy of the database. You need the following to perform this procedure:

- a database backup file set from the same 5620 SAM release
- the 5620 SAM database installation utility used to create the database during the most recent installation or upgrade
- the database name, database instance name, and the user names and passwords specified during database creation
- the user name and password of a 5620 SAM client account that has the admin scope of command role
- the original file path of the database backup
- root user privileges on the main server and database stations
- samadmin user privileges on the main server station
- Oracle management user privileges on the main server and database stations

1 If the database backup file set is on the database station, copy the file set to another station for safekeeping.

2 Perform the following steps to stop the 5620 SAM main server.

i Log in to the main server station as the samadmin user.

ii Open a console window.

iii Enter the following to navigate to the server binary directory:

```
bash$ cd path/nms/bin ↵
```

where *path* is the 5620 SAM server installation location, typically /opt/5620sam/server

iv Enter the following to stop the 5620 SAM server software:

```
bash$ ./nmsserver.bash stop ↵
```

v Enter the following to display the 5620 SAM server status:

```
bash$ ./nmsserver.bash appserver_status ↵
```

The command displays a status message.

vi The 5620 SAM server is stopped when the command displays the following status message:

```
Application Server is stopped
```

If the command displays another message, wait five minutes and repeat step 2 v. Do not proceed to the next step until the server is stopped.

3 Perform the following steps to disable the 5620 SAM main server startup daemon.

- **i** Enter the following to switch to the root user:

```
# su - ↵
```

- **ii** Enter the following:

```
# cd /etc/init.d ↵
```

- **iii** Enter the following:

```
# mv 5620SAMServerWrapper inactive.5620SAMServerWrapper ↵
```

4 Perform the following steps to stop the 5620 SAM database.

- **i** Log in to the database station as the root user.
- **ii** Enter the following:

```
# cd /etc/rc3.d ↵
```

- **iii** Enter the following to stop the Oracle proxy daemon:

```
# ./S965620SAMOracleProxyWrapper stop ↵
```

- **iv** Enter the following to stop the 5620 SAM database daemon:

```
# ./S95db5620sam stop ↵
```

Do not proceed until the command displays the following text string:

```
Done
```

5 Perform the “To uninstall the 5620 SAM database software” procedure in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide*.

Note 1 — Ensure that the Uninstall Oracle Software parameter in the Uninstall Oracle Software panel is not selected. The Oracle software is required for the restored database.

Note 2 — Do not perform the final step that describes removing files.

6 Log in to the database station as the root user.

7 Remove any files that remain in the *install_directory*/tablespace and *install_directory*/archivelog directories

where *install_directory* is the database installation directory, typically /opt/5620sam/samdb

8 Verify that the database backup file set is in the original backup directory on the database station. If it is not, copy the backup file set saved in step 1 to the original backup directory.

Note — The path to the backup file set must be the same as the initial path to the file set after backup creation.

9 Place the 5620 SAM software DVD-ROM in a DVD-ROM drive on the database station.

10 Open a console window.

11 Navigate to the DVD-ROM drive.

12 Perform one of the following to navigate to the appropriate directory.

- **a** On a RHEL station, enter the following:

  ```
  # cd Linux ↵
  ```

- **b** On a Solaris station, enter the following:

  ```
  # cd Solarisx86 ↵
  ```

13 Enter the following:

```
# ./OracleSw_PreInstall.sh ↵
```

Note — The default values displayed by the script are shown as [*default*]. To accept a default value, press ↵.

If you specify a value other than the default, you must record the value for use when the OracleSw_PreInstall.sh script is run during a software upgrade, or when the Oracle management user information is required by Alcatel-Lucent technical support.

14 The following prompt is displayed:

```
Please select between the following option:

1) NEW INSTALL OR DB RESTORE OF 5620 SAM

2) UPGRADE OF 5620 SAM

3) EXIT

Please enter(1,2 or 3):
```

Enter 1 ↵.

If you are restoring the database on a RHEL station, the following messages are displayed:

```
For Oracle, pre-install will create or reuse user->oracle,
group->dba with homedir->/opt/5620sam/oracle11r2.

Creating dba group ...

Group addition done for dba

Oracle user [oracle] new home directory will be
[/opt/5620sam/oracle11r2].

Checking or Creating the Oracle user home directory
/opt/5620sam/oracle11r2...

Checking user oracle...
```

```
Adding oracle...

Changing ownership of the directory /opt/5620sam/oracle11r2 to
oracle:dba.

About to unlock the UNIX user [oracle]

Unlocking password for user oracle.

passwd: Success

Unlocking the UNIX user [oracle] completed
```

15 If you are restoring the database on a RHEL station, go to step 20.

16 The script generates INFO messages as it validates the OS installation, and then displays the following prompt:

```
Enter the Oracle dba group name [default]:
```

17 Enter the Oracle dba group name and press ↵.

Note — To reduce the complexity of subsequent software upgrades and technical support activities, Alcatel-Lucent recommends that you accept the default for this parameter.

The following messages are displayed:

```
Creating dba group if it does not exist ...

done
```

The following prompt is displayed:

```
Enter the Oracle user name [default]:
```

18 Enter a username for the Oracle management user and press ↵. The following prompt is displayed:

```
Enter the Oracle user [username] home directory [default]:
```

19 Enter the full path of the Oracle management user home directory and press ↵. The following messages are displayed:

```
Checking or Creating the Oracle user home directory home_dir...

Checking user username...

Adding username...

Changing ownership of the directory home_dir to
username:user_group.

Oracle Corporation     SunOS 5.10     Generic Patch   January 2005

About to unlock the UNIX user [username]

passwd: password information changed for username
```

```
Unlocking the UNIX user [username] completed
```

Note — If the script generates a "failed to create group" message, ensure that NIS is disabled and re-run the pre-installation script. Contact Alcatel-Lucent technical support for more information.

20 The following prompt is displayed:

```
Do you want to change the password for the user username?
[Yes/No]:
```

Type No ↵.

21 The following prompt is displayed:

```
Specify whether a 5620 SAM server will be installed on this
workstation.

The database memory requirements will be adjusted to account for
the additional load.

Will the database co-exist with a 5620 SAM server on this
workstation [Yes/No]:
```

22 Enter Yes or No, as required, and press ↵.

On a RHEL station, the following messages are displayed as the script execution completes:

```
INFO: About to set kernel parameters in /etc/sysctl.conf...

INFO: Completed setting kernel parameters in /etc/sysctl.conf...

INFO: About to change the current values of the kernel parameters

INFO: Completed changing the current values of the kernel
parameters

INFO: About to set ulimit parameters in
/etc/security/limits.conf...

INFO: Completed setting ulimit parameters in
/etc/security/limits.conf...

INFO: Completed running Oracle Pre-Install Tasks
```

On a Solaris station, the following messages are displayed as the script execution completes:

```
Creating Oracle11R2 user_attr ...

Kernel parameters for user_attr Facility modified in
/etc/user_attr.

The original /etc/user_attr file has been backed up as
/etc/user_attr.bkp.nnnnn

Setting kernel parameters in /etc/system...Done.
```

```
About to update the boot archive

Update the boot archive completed
```

23 Enter the following to switch to the Oracle management user:

```
# su - Oracle_management_user_name ↵
```

where *Oracle_management_user_name* is the name of the UNIX account with Oracle management privileges, typically oracle

24 Perform one of the following to open the 5620 SAM database installation utility.

a On a RHEL station:

- **i** Enter the following:

  ```
  # cd Linux ↵
  ```

- **ii** Enter the following:

  ```
  # ./DBConfig_RHEL_R_r_revision.bin ↵
  ```

  where
  R_r is the release identifier, in the form *MAJOR_minor*
  revision is the revision identifier, such as R1, R3, or another descriptor

b On a Solaris station:

- **i** Enter the following:

  ```
  # cd Solarisx86 ↵
  ```

- **ii** Enter the following:

  ```
  # ./DBConfig_SolarisX86_SAM_R_r_revision.bin ↵
  ```

  where
  R_r is the release identifier, in the form *MAJOR_minor*
  revision is the revision identifier, such as R1, R3, or another descriptor

The 5620 SAM database installation utility opens with the Introduction panel displayed.

25 Perform the following steps.

i Click on the Next button. The Software License Agreement panel is displayed.

ii Select the “I accept the terms of the License Agreement” option.

iii Click on the Next button. The Choose Installation Type panel is displayed.

iv Select the “Restore a Database” option.

v Click on the Next button. The Install Oracle Software panel is displayed.

vi Select the “Do not install Oracle Software” option.

vii Click on the Install button. The installer prepares to restore the database, and then displays the Locate the Backup Directory panel.

viii Click on the Choose button and use the file browser form that opens to specify the directory that contains the backup file set.

Note — You must specify the original database backup directory verified in step 8.

ix Click on the Next button. The General Database Restore Info panel is displayed.

x Configure the parameters in each successive panel until the Database Restore panel is displayed. Use the values recorded during the most recent database installation or upgrade, and click on the Next button in each panel to continue.

xi Click on the Start Process button. The database restore process begins.

Note — A database restore takes considerable time, depending on the database size.

xii When the Installation Complete panel is displayed, open a separate console window and run the script specified in the panel.

xiii When the script execution is complete, click on the Done button to close the installation utility. The database begins to initialize.

26 Perform the following steps to enable the 5620 SAM main server startup daemon.

i Log in to the main server station as the root user.

ii Open a console window.

iii Enter the following:

```
# cd /etc/init.d ↵
```

iv Enter the following:

```
# mv inactive.5620SAMServerWrapper 5620SAMServerWrapper ↵
```

27 Perform the following steps to start the 5620 SAM main server.

i Log in to the main server station as the samadmin user.

ii Enter the following to navigate to the server binary directory:

```
bash$ cd path/nms/bin ↵
```

where *path* is the 5620 SAM server installation location, typically /opt/5620sam/server

iii Enter the following to start the 5620 SAM server software:

```
bash$ ./nmsserver.bash start ↵
```

28 Close the open console windows on each station.

Procedure 14-8 To restore the primary database in a redundant 5620 SAM system

Perform this procedure to restore a database using a database backup created on the same station in a redundant 5620 SAM system. The station is called the primary database station in this procedure.

To regain database redundancy when the database restore is complete, you must reinstantiate the restored primary database on the standby database station. See Procedure 14-9 for information.

You require the following to perform this procedure:

- a database backup file set from the same 5620 SAM release
- the 5620 SAM database installation utility used to create the database during the most recent installation or upgrade
- the database name, database instance names, and the user names and passwords specified during database creation
- the user name and password of a 5620 SAM client account that has the admin scope of command role
- the original file path of the database backup
- root user privileges on the main server and database stations
- samadmin user privileges on the main server stations
- Oracle management user privileges on the main server and database stations

1 If the database backup file set is on the primary database station, copy the file set to another station for safekeeping.

2 Perform the following steps to stop the standby 5620 SAM main server.

i Log in to the standby main server station as the samadmin user.

ii Open a console window.

iii Enter the following to navigate to the server binary directory:

```
bash$ cd path/nms/bin ↵
```

where *path* is the 5620 SAM server installation location, typically /opt/5620sam/server

iv Enter the following to stop the 5620 SAM server software:

```
bash$ ./nmsserver.bash stop ↵
```

v Enter the following to display the 5620 SAM server status:

```
bash$ ./nmsserver.bash appserver_status ↵
```

The command displays a status message.

vi The 5620 SAM server is stopped when the command displays the following status message:

```
Application Server is stopped
```

If the command displays another message, wait five minutes and repeat step 2 v. Do not proceed to the next step until the server is stopped.

3 Perform the following steps to disable the standby 5620 SAM main server startup daemon.

i Enter the following to switch to the root user:

```
# su - ↵
```

ii Enter the following:

```
# cd /etc/init.d ↵
```

iii Enter the following:

```
# mv 5620SAMServerWrapper inactive.5620SAMServerWrapper ↵
```

4 Perform the following steps to stop the standby 5620 SAM database.

i Log in to the standby database station as the root user.

ii Enter the following:

```
# cd /etc/rc3.d ↵
```

iii Enter the following to stop the Oracle proxy daemon:

```
# ./S965620SAMOracleProxyWrapper stop ↵
```

iv Enter the following to stop the 5620 SAM database daemon:

```
# ./S95db5620sam stop ↵
```

Do not proceed until the command displays the following text string:

```
Done
```

5 Perform the following steps to stop the primary 5620 SAM main server.

- **i** Log in to the primary main server station as the samadmin user.
- **ii** Open a console window.
- **iii** Enter the following to navigate to the server binary directory:

```
bash$ cd path/nms/bin ↵
```

  where *path* is the 5620 SAM server installation location, typically /opt/5620sam/server

- **iv** Enter the following to stop the 5620 SAM server software:

```
bash$ ./nmsserver.bash stop ↵
```

- **v** Enter the following to display the 5620 SAM server status:

```
bash$ ./nmsserver.bash appserver_status ↵
```

  The command displays a status message.

- **vi** The 5620 SAM server is stopped when the command displays the following status message:

```
Application Server is stopped
```

  If the command displays another message, wait five minutes and repeat step 2 v. Do not proceed to the next step until the server is stopped.

6 Perform the following steps to disable the primary 5620 SAM main server startup daemon.

- **i** Enter the following to switch to the root user:

```
# su - ↵
```

- **ii** Enter the following:

```
# cd /etc/init.d ↵
```

- **iii** Enter the following:

```
# mv 5620SAMServerWrapper inactive.5620SAMServerWrapper ↵
```

7 Perform the following steps to stop the primary 5620 SAM database.

- **i** Log in to the primary database station as the root user.
- **ii** Enter the following:

```
# cd /etc/rc3.d ↵
```

- **iii** Enter the following to stop the Oracle proxy daemon:

```
# ./S965620SAMOracleProxyWrapper stop ↵
```

- **iv** Enter the following to stop the 5620 SAM database daemon:

```
# ./S95db5620sam stop ↵
```

Do not proceed until the command displays the following text string:

```
Done
```

8 Perform the “To uninstall the 5620 SAM database software” procedure in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide*.

Note 1 — Ensure that the Uninstall Oracle Software parameter on the Uninstall Oracle Software panel is not selected. The Oracle software is required for the restored database.

Note 2 — Do not perform the final step that describes removing files.

9 Log in to the primary database station as the root user.

10 Remove any files that remain in the *install_directory*/tablespace and *install_directory*/archivelog directories

where *install_directory* is the database installation directory, typically /opt/5620sam/samdb

11 Verify that the database backup file set is in the original backup directory on the primary database station. If it is not, copy the backup file set saved in step 1 to the original backup directory.

Note — The path to the backup file set must be the same as the initial path to the file set after backup creation.

12 Open a console window.

13 Navigate to the DVD-ROM drive.

14 Perform one of the following to navigate to the appropriate directory.

a On a RHEL station, enter the following:

```
# cd Linux ↵
```

b On a Solaris station, enter the following:

```
# cd Solarisx86 ↵
```

15 Enter the following:

```
# ./OracleSw_PreInstall.sh ↵
```

Note — The default values displayed by the script are shown as [*default*]. To accept a default value, press ↵.

If you specify a value other than the default, you must record the value for use when the OracleSw_PreInstall.sh script is run during a software upgrade, or when the Oracle management user information is required by Alcatel-Lucent technical support.

16 The following prompt is displayed:

```
Please select between the following option:

1) NEW INSTALL OR DB RESTORE OF 5620 SAM

2) UPGRADE OF 5620 SAM

3) EXIT

Please enter(1,2 or 3):
```

Enter 1 ↵.

If you are restoring the database on a RHEL station, the following messages are displayed:

```
For Oracle, pre-install will create or reuse user->oracle,
group->dba with homedir->/opt/5620sam/oracle11r2.

Creating dba group ...

Group addition done for dba

Oracle user [oracle] new home directory will be
[/opt/5620sam/oracle11r2].

Checking or Creating the Oracle user home directory
/opt/5620sam/oracle11r2...

Checking user oracle...

Adding oracle...

Changing ownership of the directory /opt/5620sam/oracle11r2 to
oracle:dba.

About to unlock the UNIX user [oracle]

Unlocking password for user oracle.

passwd: Success

Unlocking the UNIX user [oracle] completed
```

17 If you are restoring the database on a RHEL station, go to step 20.

18 The script generates INFO messages as it validates the OS installation, and then displays the following prompt:

```
Enter the Oracle dba group name [default]:
```

19 Enter the Oracle dba group name and press ↵.

Note — To reduce the complexity of subsequent software upgrades and technical support activities, Alcatel-Lucent recommends that you accept the default for this parameter.

The following messages are displayed:

```
Creating dba group if it does not exist ...
```

```
done
```

The following prompt is displayed:

```
Enter the Oracle user name [default]:
```

20 Enter a username for the Oracle management user and press ↵. The following prompt is displayed:

```
Enter the Oracle user [username] home directory [default]:
```

21 Enter the full path of the Oracle management user home directory and press ↵. The following messages are displayed:

```
Checking or Creating the Oracle user home directory home_dir...

Checking user username...

Adding username...

Changing ownership of the directory home_dir to
username:user_group.

Oracle Corporation     SunOS 5.10     Generic Patch   January 2005

About to unlock the UNIX user [username]

passwd: password information changed for username

Unlocking the UNIX user [username] completed
```

Note — If the script generates a “failed to create group” message, ensure that NIS is disabled and re-run the pre-installation script. Contact Alcatel-Lucent technical support for more information.

22 The following prompt is displayed:

```
Do you want to change the password for the user username?
[Yes/No]:
```

Type No ↵. The following prompt is displayed:

23 The following prompt is displayed:

```
Specify whether a 5620 SAM server will be installed on this
workstation.

The database memory requirements will be adjusted to account for
the additional load.

Will the database co-exist with a 5620 SAM server on this
workstation [Yes/No]:
```

24 Enter Yes or No, as required, and press ↵.

On a RHEL station, the following messages are displayed as the script execution completes:

```
INFO: About to set kernel parameters in /etc/sysctl.conf...
```

```
INFO: Completed setting kernel parameters in /etc/sysctl.conf...

INFO: About to change the current values of the kernel parameters

INFO: Completed changing the current values of the kernel
parameters

INFO: About to set ulimit parameters in
/etc/security/limits.conf...

INFO: Completed setting ulimit parameters in
/etc/security/limits.conf...

INFO: Completed running Oracle Pre-Install Tasks
```

On a Solaris station, the following messages are displayed as the script execution completes:

```
Creating Oracle11R2 user_attr ...

Kernel parameters for user_attr Facility modified in
/etc/user_attr.

The original /etc/user_attr file has been backed up as
/etc/user_attr.bkp.nnnnn

Setting kernel parameters in /etc/system...Done.

About to update the boot archive

Update the boot archive completed
```

25 Enter the following to switch to the Oracle management user:

```
# su - Oracle_management_user_name ↵
```

where *Oracle_management_user_name* is the name of the UNIX account with Oracle management privileges, typically oracle

26 Perform one of the following to open the 5620 SAM database installation utility.

a On a RHEL station:

i Enter the following:

```
# cd Linux ↵
```

ii Enter the following:

```
# ./DBConfig_RHEL_R_r_revision.bin ↵
```

where
R_r is the release identifier, in the form *MAJOR_minor*
revision is the revision identifier, such as R1, R3, or another descriptor

b On a Solaris station:

i Enter the following:

```
# cd Solarisx86 ↵
```

ii Enter the following:

```
# ./DBConfig_SolarisX86_SAM_R_r_revision.bin ↵
```

where
R_r is the release identifier, in the form *MAJOR_minor*
revision is the revision identifier, such as R1, R3, or another descriptor

The 5620 SAM database installation utility opens with the Introduction panel displayed.

27 Perform the following steps.

i Click on the Next button. The Software License Agreement panel is displayed.

ii Select the “I accept the terms of the License Agreement” option.

iii Click on the Next button. The Choose Installation Type panel is displayed.

iv Select the “Restore a Database” option.

v Click on the Next button. The Install Oracle Software panel is displayed.

vi Select the “Do not install Oracle Software” option.

vii Click on the Install button. The installer prepares to restore the database, and then displays the Locate the Backup Directory panel.

viii Click on the Choose button and use the file browser form that opens to specify the directory that contains the backup file set.

Note — You must specify the original database backup directory verified in step 11.

ix Click on the Next button. The General Database Restore Info panel is displayed.

x Configure the parameters in each successive panel until the Database Restore panel is displayed. Use the values recorded during the most recent database installation or upgrade, and click on the Next button in each panel to continue.

xi Click on the Start Process button. The database restore process begins.

Note — A database restore takes considerable time, depending on the database size.

xii When the Installation Complete panel is displayed, open a separate console window and run the script specified in the panel.

xiii When the script execution is complete, click on the Done button to close the installation utility. The database begins to initialize.

28 Perform the following steps to enable the primary 5620 SAM main server startup daemon.

i Log in to the primary main server station as the root user.

ii Open a console window.

iii Enter the following:

```
# cd /etc/init.d ↵
```

iv Enter the following:

```
# mv inactive.5620SAMServerWrapper 5620SAMServerWrapper ↵
```

29 Perform the following steps to start the primary 5620 SAM main server.

i Enter the following to switch to the samadmin user:

```
# su - samadmin ↵
```

ii Enter the following to navigate to the server binary directory:

```
bash$ cd path/nms/bin ↵
```

where *path* is the 5620 SAM server installation location, typically /opt/5620sam/server

iii Enter the following to start the 5620 SAM server:

```
bash$ ./nmsserver.bash start ↵
```

iv Enter the following to check the server status:

```
bash$ ./nmsserver.bash -s nms_status ↵
```

The command returns server status information.

If the main server is not completely started, the first line of status information is the following:

```
Main Server is not ready...
```

The 5620 SAM server is completely started when the command returns the following line of output:

```
 -- Primary Server is UP
```

v If the command output indicates that the server is not completely started, wait five minutes and then repeat step 29 iv.

Note — Do not proceed to the next step until the server is completely started.

30 Perform the following steps to start the standby 5620 SAM database.

i Log in to the standby database station as the root user.

ii Enter the following:

```
# cd /etc/rc3.d ↵
```

iii Enter the following to start the 5620 SAM database daemon:

```
# ./S95db5620sam start ↵
```

Do not proceed until the command displays the following text string:

```
Done
```

iv Enter the following to start the Oracle proxy daemon:

```
# ./S965620SAMOracleProxyWrapper start ↵
```

31 Perform the following steps to enable the standby 5620 SAM main server startup daemon.

i Log in to the standby main server station as the root user.

ii Open a console window.

iii Enter the following:

```
# cd /etc/init.d ↵
```

iv Enter the following:

```
# mv inactive.5620SAMServerWrapper 5620SAMServerWrapper ↵
```

32 Perform the following steps to start the standby 5620 SAM main server.

i Log in to the standby main server station as the samadmin user.

ii Enter the following to navigate to the server binary directory:

```
bash$ cd path/nms/bin ↵
```

where *path* is the 5620 SAM server installation location, typically /opt/5620sam/server

iii Enter the following to start the 5620 SAM server:

```
bash$ ./nmsserver.bash start ↵
```

To restore database redundancy, you must reinstantiate the primary database on the standby database station. See Procedure 14-9 for information.

Procedure 14-9 To reinstantiate a 5620 SAM database

Perform this procedure to reinstantiate a restored primary database on a standby database station in a redundant 5620 SAM system.

1 Perform one of the following.

a Use a 5620 SAM client GUI. Perform the following steps.

Note — The 5620 SAM client GUI displays a progress indicator during the reinstantiation, unlike a CLI-based reinstantiation.

i Log in to the GUI client as a user with the 5620 SAM admin scope of command role.

ii Choose Administration→System Information from the 5620 SAM main menu. The System Information form opens with the General tab displayed.

iii Click on the Re-Instantiate Standby button. A dialog box appears.

Note — The Re-Instantiate Standby button may not display depending on your scope of command. See the *5620 SAM User Guide* for more information about scope of command.

iv Click on the Yes button. The database reinstantiation begins.

The client GUI status bar and the System Information form display the reinstantiation status. The Standby Re-instantiation State changes from In Progress to Success when reinstantiation is complete. The Last Attempted Standby Re-instantiation Time displays the start time of the current reinstantiation.

v Close the System Information form when the reinstantiation is complete.

b Use a CLI script. Perform the following steps.

Note — The CLI script does not display a progress indicator during the reinstantiation.

i Log in to the primary main server station as the samadmin user.

ii Open a console window.

iii Navigate to the 5620 SAM server binary directory, typically /opt/5620sam/server/nms/bin.

iv Enter the following:

```
./reinstantiatedb.bash -u username -p password ↵
```

where
username is the user name of a 5620 SAM client account that has the admin scope of command role
password is the password for the user account

The script displays the following confirmation message:

```
This action will rebuild the standby database.

Do you want to proceed? (YES/no) :
```

v Enter the following case-sensitive text to begin the reinstantiation:

YES ↵

The 5620 SAM server begins to reinstantiate the database on the standby database station. Progress is indicated by a rolling display of dots in the console window. Database reinstantiation is complete when the CLI prompt is again displayed.

vi Close the console window when the reinstantiation is complete.

2 Open a 5620 SAM GUI client to verify that the 5620 SAM servers and databases are functional. The server and database status are displayed in the status bar at the bottom of the GUI.

14.6 Clearing inactive residential subscriber instances from the 5620 SAM database

Alcatel-Lucent recommends that you periodically remove the inactive residential subscriber instance records from the 5620 SAM database. A residential subscriber instance becomes inactive when the associated subscriber is deleted from an NE. The inactive instances accumulate rapidly, for example, in a Wi-Fi offload deployment.

Note — Before you execute the script, Alcatel-Lucent recommends that you disable the GUI client timeout so that you can use the client GUI to monitor the script execution. Otherwise, if the execution takes longer then the GUI client timeout, you can monitor the script execution using the 5620 SAM user activity log.

Procedure 14-10 To delete the inactive residential subscriber instances

Perform this procedure to configure and execute a script that removes the inactive residential subscriber instance records from the 5620 SAM database.

1 Disable the GUI client timeout. Perform the following steps.

- **i** Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.
- **ii** Record the Client Timeout (minutes) parameter value for use later in the procedure.
- **iii** Set the Client Timeout (minutes) parameter to 0, which specifies no timeout. This ensures that the 5620 SAM GUI client session does not close because of user inactivity while the script execution is in progress.
- **iv** Click on the OK button. A dialog box appears.
- **v** Click on the Yes button. The 5620 SAM User Security - Security Management (Edit) form closes.

2 Choose Tools→Scripts from the 5620 SAM main menu. The Scripts form opens.

3 Choose Script Bundle (Scripting) from the object drop-down menu and click on the Search button. A list of script bundles is displayed.

4 If a subscriber instance deletion script bundle is listed, go to step 6.

5 Perform the following steps to create a script bundle using an example.

- **i** Click on the Browse Examples button. The Browse Examples of Scripts form opens.
- **ii** Navigate to the required bundle example. The path is Script Bundle Examples→Miscellaneous→Remove Inactive Residential Subscriber Instances Bundle.

- **iii** Select the bundle example and click on the Create Bundle button. The Script Bundle (Create) form opens.
- **iv** Configure the Name parameter.
- **v** Click on the OK button. The Script Bundle (Create) form closes.
- **vi** Close the Browse Examples of Scripts form. The new script bundle is listed on the Scripts form.

6 Select the script bundle and click on the Properties button. The Script Bundle (Edit) form opens.

7 Select Remove Residential Subscriber CTL and click on the Execute Script button. The Execute Script form opens.

8 Configure the parameter on the form to specify the number of days of inactivity that qualify a residential subscriber instance for deletion.

Note — If the 5620 SAM forwards statistics or billing information to the 5670 RAM, ensure that the parameter value is greater than the billing period in days to ensure that no inactive subscriber instances are deleted before the billing occurs.

9 Click on the Execute button. The script execution begins.

While the script runs, a new item with an hourglass symbol is displayed in the navigation panel on the left side of the form. When the script execution is complete, the symbol changes to a green check mark.

10 Close the Execute Script form.

11 Close the Script Bundle (Edit) form.

12 Close the Scripts form.

13 Restore the GUI client timeout. Perform the following steps.

- **i** Choose Administration→Security→5620 SAM User Security from the 5620 SAM main menu. The 5620 SAM User Security - Security Management (Edit) form opens.
- **ii** Configure the Client Timeout (minutes) parameter using the value recorded in step 1.
- **iii** Click on the OK button. A dialog box appears.
- **iv** Click on the Yes button. The 5620 SAM User Security - Security Management (Edit) form closes.

14.7 Listing customer service information

Record customer service information to:

- document which devices and interfaces are used to handle customer traffic
- provide raw data for post-processing customer trends and customer information

Procedure 14-11 To list service information

1 Choose Manage→Service→Services from the 5620 SAM main menu. The Manage Services form opens.

2 Specify a filter to narrow the services listed. You can filter based on service ID or other criteria.

3 Click on the Search button. The filtered list of services is displayed.

4 Save the list of customer services.

- **i** Order the columns of service data as required. For example, you can click on the Service Name heading to sort the services by name.
- **ii** Right-click on the Service Name heading and choose Save To File from the contextual menu. The Save form opens.
- **iii** Enter a filename for the customer services; for example:

  ABCindustries_services_*yearmonthday*
- **iv** Click on the Files of Type drop-down menu to specify the file type.
- **v** Browse to choose a location in which to save the file.
- **vi** Click on the Save button. The file is saved to the specified location with the appropriate file extension.

5 You can record other details about the services. For example, you can list Layer 2 access interface information for the customer's VPLS or VLL services.

- **i** Choose Manage→Service→Services→Create from the 5620 SAM main menu. The Manage Service form opens.
- **ii** Click on the Create button and choose VPLS or VLL. The VPLS Service (Create) form or VLL form opens.
- **iii** Order the columns of Layer 2 access interface data as required. For example, you can click on the Service Name heading to sort the Layer 2 access interface data based on the service name.
- **iv** Right-click on the Service Name heading and choose Save To File from the contextual menu. The Save form opens.
- **v** Enter a filename for the customer service Layer 2 interface list; for example:

  ABCindustries_services_l2interfacesused_*yearmonthday*

   - **vi** Click on the Files of Type drop-down menu to specify the file type.
   - **vii** Browse to choose a location in which to save the file.
   - **viii** Click on the Save button. The file is saved to the specified location with the appropriate file extension.

6 Save the customer service data lists for post-processing on another station.

14.8 Checking for duplicate service or resource names

Alcatel-Lucent recommends that you develop standardized naming conventions before you configure network objects, in order to:

- facilitate identifying the object type
- ensure that data passed to a northbound OSS interface or southbound in a data file for processing is named consistently throughout the management domain

It is good practice to include information such as the following when creating or configuring an object using the object properties form:

- the object type; for example, VPRN
- a customer association to the object; for example, site 1.1.1.1 for XYZ Industries
- source and destination endpoint identifiers; for example, the devices at each end of an LSP
- ports and IP addresses used

You can check for duplicate names to ensure that naming conventions are followed and to help prevent confusion when you deal with customers or operations staff. Procedure 14-12 uses ports as the objects to check for duplicate names.

Procedure 14-12 To check for duplicate port descriptions

Perform this procedure to check for duplicate object descriptions on all managed devices. This procedure uses ports as the object type. but you can also check logical entity names; for example, service or policy names. This procedure assumes that the Description parameter uniquely identifies each port.

1 Choose Manage→Equipment from the 5620 SAM main menu. The Manage Equipment form appears.

2 Generate a list of all ports:

   - **i** Choose Port (Physical Equipment) from the object drop-down menu.
   - **ii** Configure the filter for the Administrative State column to display devices that are administratively up.
   - **iii** Click on the Search button.

3 Click on the Description heading to list ports alphabetically by description.

4 Scan the list for duplicate names.

Note — By default, ports are assigned a description based on the card type when the Description parameter is not configured.

5 If you find a duplicate description, you can modify the description based on your naming conventions.

- **i** Click on the port row with the duplicate description.
- **ii** Click on the Properties button. The port configuration form opens.
- **iii** Modify the Description parameter to uniquely describe the port.
- **iv** Click on the OK button and confirm the action.
  - The port configuration form is saved.
  - The Description name on the Browse Equipment form is updated.
  - The cursor remains on the port row, even if the row moves up or down the list.
  - The port list refreshes with the modified description.

6 Click on the Close button.

14.9 Configuring the OLC state of equipment or services

Daily maintenance operations that are performed on NEs can cause a large number of alarms to be raised in the 5620 SAM. You can configure the OLC state on an object or service to specify whether the object is in maintenance or in-service mode to filter alarms in the alarm window.

Note — Alarms are generated for objects and services regardless of the Current OLC State parameter setting. The parameter setting is not sent to the network objects or services.

You can set the OLC state for the following objects and services:

- network elements
- power supply trays
- card slots
- daughter cards
- ports
- LAGs
- composite services
- services
- sites
- SAPs (L2 access interfaces and L3 access interfaces)

Caution — Changing the OLC state on an object also changes the OLC state on all of its child objects. The operation may take several minutes to complete, depending on the number of objects affected.

Note — An NE shelf inherits the OLC state of the NE, and is read-only.

In addition, you can specify on properties forms that the 5620 SAM reverts the OLC state to the in-service or maintenance mode after a specified time, depending on the current OLC state of the object or service. In addition, you can specify in NE discovery rules that the current OLC state reverts after the resynchronization is complete.You can specify that the 5620 SAM raises an informational alarm about the object OLC state reverting to the opposite state.

Setting the OLC state

The default value of the OLC state for NEs can be specified in the discovery rules. See the *5620 SAM User Guide* for more information about configuring the default OLC state for discovered network elements.

The OLC state default value of a child object is inherited from the parent object or service. The default value of the OLC state for composite services and services can be specified using the nms-server.xml file.

Caution — Unauthorized modification of the nms-server.xml file can seriously affect network management and 5620 SAM performance. Contact your Alcatel-Lucent representative for information about file modification.

When the OLC state of an NE is set to the maintenance mode, all child objects such as access interfaces, card slots, daughter cards, and ports are set to maintenance mode. The sites on the NE are set to the maintenance mode.

When the OLC state of a composite service or service is set to the maintenance mode, the following related objects are changed:

- sites on which the services reside
- access interfaces (SAPs, L2 and L3 access interfaces)
- SDP Bindings (mesh, mirror and spoke bindings)

When the OLC state of a composite service or services is changed to in service, access interfaces and sites may not change to in service if they belong to equipment objects that are set to maintenance.

The OLC state of the parent object must be in service to change the OLC state of the child object. You can change the OLC state of the parent object regardless of the OLC state of the child object. However, when a child object has more than one parent object and the OLC state of one parent is set to maintenance, the child object is set to maintenance. The OLC state for a child object cannot be changed if one of the parent OLC states is set to maintenance.

You can configure the default OLC state for objects that become administratively down from the OLC tab on the System Preferences form. See Procedure 5-24.

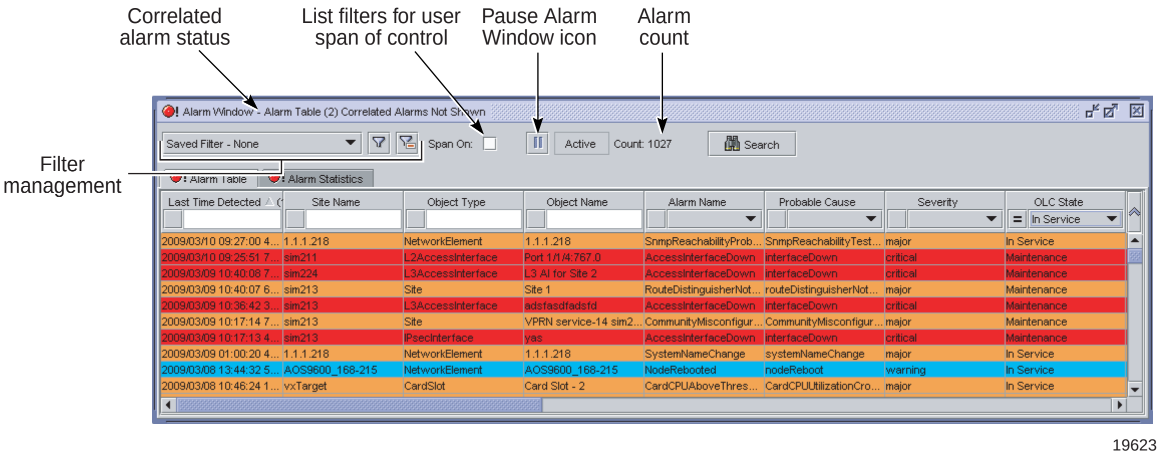
See the *5620 SAM User Guide* for information about how to configure the OLC state for network objects, equipment objects, services, and sites.

You must add the OLC state property to manually created service templates, as described in Procedure 14-18.

Procedure 14-13 To view the OLC state of all network alarms using the dynamic alarm list

The dynamic alarm list alarm window allows you to monitor incoming faults from the devices and 5620 SAM software. This feature is most useful when monitoring the network. Figure 14-1 shows the dynamic alarm list alarm window.

Figure 14-1 Dynamic alarm list alarm window - Alarm Table



Last Time Detected	Site Name	Object Type	Object Name	Alarm Name	Probable Cause	Severity	OLC State
							= In Service
2009/03/10 09:27:00 4...	1.1.1.218	NetworkElement	1.1.1.218	SnmpReachabilityProb...	SnmpReachabilityTest...	major	In Service
2009/03/10 09:25:51 7...	sim211	L2AccessInterface	Port 1/1/4:767.0	AccessInterfaceDown	interfaceDown	critical	Maintenance
2009/03/09 10:40:08 7...	sim224	L3AccessInterface	L3 AI for Site 2	AccessInterfaceDown	interfaceDown	critical	Maintenance
2009/03/09 10:40:07 6...	sim213	Site	Site 1	RouteDistinguisherNot...	routeDistinguisherNot...	major	Maintenance
2009/03/09 10:36:42 3...	sim213	L3AccessInterface	adsfasdfadsfd	AccessInterfaceDown	interfaceDown	critical	Maintenance
2009/03/09 10:17:14 7...	sim213	Site	VPRN service-14 sim2...	CommunityMisconfigur...	CommunityMisconfigur...	major	Maintenance
2009/03/09 10:17:13 4...	sim213	IPsecInterface	yas	AccessInterfaceDown	interfaceDown	critical	Maintenance
2009/03/09 01:00:20 4...	1.1.1.218	NetworkElement	1.1.1.218	SystemNameChange	systemNameChange	major	In Service
2009/03/08 13:44:32 5...	AOS9600_168-215	NetworkElement	AOS9600_168-215	NodeRebooted	nodeReboot	warning	In Service
2009/03/08 10:46:24 1...	vxTarget	CardSlot	Card Slot - 2	CardCPUAboveThres...	CardCPUUtilizationCro...	major	In Service

1 Click on the filter icon in the alarm window. A filter form opens.

Note — You can open and view up to six alarm windows. This is useful when you need to view multiple filtered incoming network alarms.

2 Choose Assigned OLC State from the Attribute drop-down menu.

3 Configure the filter form to search for alarms. See the *5620 SAM User Guide* for more information about creating search filters.

4 Assign the OLC State to the alarm. See Procedure 14-17 for more information.

5 Manage the alarms according to your fault management policies. See the *5620 SAM Troubleshooting Guide* for information about troubleshooting using alarm information guidelines.

Procedure 14-14 To view the OLC state of network equipment or a service

1 Choose Administration→OLC from the 5620 SAM main menu. The OLC form appears with the OLC tab displayed.

2 Choose a type of service or object from the object drop-down menu:

- Access Interface (Service Management) to view a list of access interfaces
- Network Element (Network) to view a list of NEs
- Card Slot (Physical Equipment) to view a list of cards
- Daughter Card Slot (Physical Equipment) to view a list of daughter cards
- Physical Port (Physical Equipment) to view a list of ports
- LAG (LAG) to view a list of LAG ports
- Composite Service (Service Management) to view a list of composite services
- Service (Service Management) to view a list of services
- Site (Service Management) to view a list of sites
- SDP Binding (Service Tunnel Management) to view a list of SDP bindings
- Optical Transport Service (Optical Management) to view a list of optical transport services
- Optical Site (Optical Management) to view a list of optical sites
- ISA-AA Group (ISA) to view a list of ISA-AA groups
- ISA-Tunnel Group (ISA) to view a list of ISA-tunnel groups
- ISA-WLAN GW Group (WLAN Gateway) to view a list of ISA-WLAN GW groups
- ISA-LNS Group (ISA) to view a list of ISA-LNS groups
- ISA-NAT Group (Network Address Translation) to view a list of ISA-NAT groups
- ISA-Video Group (ISA) to view a list of ISA-video groups
- BGP Site (Routing Management: BGP)
- Peer Group (Routing Management: BGP)
- Peer (Routing Management: BGP)
- Power Supply Tray (Physical Equipment)
- SFM Slot (Physical Equipment)

3 Configure the filter criteria and click on the Search button. The form displays a list of objects based on the search criteria.

Procedure 14-15 To view the scheduling of OLC state changes of network equipment or a service

1 Choose Administration→OLC from the 5620 SAM main menu. The OLC form opens with the OLC tab displayed.

2 Click on the Schedules tab. A list of scheduled OLC state changes appears.

3 Configure the filter criteria, if required.

4 View the following information:

- object ID and name
- current OLC state
- OLC state to which the object reverts at the scheduled time
- time when the OLC state reverts

5 To open the object properties form, select an entry and click on the Properties button.

Procedure 14-16 To change the OLC state of equipment or a service

Caution — Changing the OLC state can affect 5620 SAM performance and can take several minutes to complete. Changing the OLC state of a parent object changes the OLC state of the child objects.

1 Choose Administration→OLC from the 5620 SAM main menu. The OLC form appears with the OLC tab displayed.

2 Choose a type of service or object from the object drop-down menu:

- Access Interface (Service Management) to view a list of access interfaces
- Network Element (Network) to view a list of NEs
- Card Slot (Physical Equipment) to view a list of cards
- Daughter Card Slot (Physical Equipment) to view a list of daughter cards
- Physical Port (Physical Equipment) to view a list of ports
- LAG (LAG) to view a list of LAG ports
- Composite Service (Service Management) to view a list of composite services
- Service (Service Management) to view a list of services
- Site (Service Management) to view a list of sites
- SDP Binding (Service Tunnel Management) to view a list of SDP bindings
- Optical Transport Service (Optical Management) to view a list of optical transport services
- Optical Site (Optical Management) to view a list of optical sites
- ISA-AA Group (ISA) to view a list of ISA-AA groups
- ISA-Tunnel Group (ISA) to view a list of ISA-tunnel groups
- ISA-WLAN GW Group (WLAN Gateway) to view a list of ISA-WLAN GW groups
- ISA-LNS Group (ISA) to view a list of ISA-LNS groups
- ISA-NAT Group (Network Address Translation) to view a list of ISA-NAT groups
- ISA-Video Group (ISA) to view a list of ISA-video groups
- BGP Site (Routing Management: BGP)
- Peer Group (Routing Management: BGP)
- Peer (Routing Management: BGP)
- Power Supply Tray (Physical Equipment)
- SFM Slot (Physical Equipment)

3 Configure the filter criteria, as required.

4 Click on the Search button. A list of objects or services appears based on the filter criteria.

5 Select an entry from the list. You can select multiple objects.

6. Click on the OLC State button, and choose Maintenance or In Service from the drop-down menu. The OLC state of the object changes in the filtered list panel.

> **Note —** You can configure the Revert OLC State parameter on the properties form for the object. The Revert OLC State parameter allows you to specify that the object automatically reverts to either the In Service mode or the Maintenance mode after a selected time, depending on the current OLC state of the object.
>
> You can also configure the OLC state of a service or network object by configuring the OLC State parameter on the General tab of the object properties form.

7. Close the OLC form.

Procedure 14-17 To change the OLC state from the alarm window

1. Click on the Alarm Table tab in the alarm window. The dynamic list of incoming network alarms appears.
2. If required, click on the filter icon to create a filtered list of alarms. See the *5620 SAM User Guide* for more information about creating search filters.
3. Select an alarm from the list. You can select multiple alarms.
4. Right-click on the alarm and choose Assign OLC State from the drop-down menu. The OLC State Assignment form opens.
5. Choose Maintenance or In service from the Assigned OLC State drop-down menu.
6. Click on the OK button. A dialog box appears.
7. Click on the Yes button. The OLC State Assignment form closes.

Procedure 14-18 To add the OLC state to a template using the GUI builder

Some service objects have an OLC state property. You cannot configure the OLC state property during the configuration of the service object. For 5620 SAM-created service templates, the OLC state property is automatically added to the template. For manually created service templates, the OLC state property is not added to the template. Perform the following procedure to add the OLC state property to a manually created template.

1. Open the GUI builder. See the *5620 SAM Scripts and Templates Developer Guide*.
2. Create a combo box component and enter olcState for the Name combo box component attribute. See the *5620 SAM Scripts and Templates Developer Guide*.

3 Enter the value “maintenance” for the List combo box component attribute.

4 Enter the value “inService” for the List combo box component attribute.

5 Enter the value “maintenance” or “inService” for the Default combo box component attribute.

6 Save and close the GUI builder and Script editor windows.

Appendices

A. Scope of command roles and permissions

A.1 Predefined scope of command profiles and roles

This appendix describes the predefined 5620 SAM scope of command profiles and roles, and the access permissions for each predefined role. Predefined scope of command profiles and roles cannot be deleted.

Table A-1 provides a summary of the command profiles, roles, and permissions information contained in this appendix.

Table A-1 Summary of command profiles, roles, and permission information

Table	Description	See
Predefined scope of command profiles	Lists the predefined scope of command profiles, the assigned roles for each profile, and a description for each profile.	Table A-2
Predefined scope of command roles	Lists the 5620 SAM predefined scope of command roles and provides a description of the user security access provided for each role.	Table A-3
Permissions assigned to 5620 SAM scope of command roles	Lists the permissions that can be assigned to a 5620 SAM scope of command role and a description of the permission.	Table A-4
Summary of 5620 SAM scope of command roles	Lists each of the 5620 SAM default scope of command roles and provides a link to a table for each of the roles where the access permission are defined.	Table A-5

Predefined scope of command profiles

Table A-2 lists the predefined scope of command profiles, the assigned roles for each profile, and a description for each profile.

Table A-2 Predefined scope of command profiles

Profile name	Assigned roles	Description
admin	Administrator	Default administrative scope of command profile with access to all menus accessible from the 5620 SAM GUI with the exception of LI menu functions. This profile also has no OSSI access.

Predefined scope of command roles

Table A-3 lists the 5620 SAM predefined scope of command roles and a description of the access provided for each role.

Table A-3 Predefined scope of command roles

Role	**Access provided**
Base Read-only	Read-only to all objects except for the objects in the SAM Security and Mirror Service Management roles.
Administrator	GUI access, but no OSSI access, to all objects. Create, modify, delete, import, and export public workspaces. View private or public workspaces in the Manage Workspaces list.
User Management	5620 SAM user and group management. Create, modify, delete, import, and export public workspaces. View private or public workspaces in the Manage Workspaces list.
SAM Management and Operations	Database functions such as backup, restore, reinstantiation, and switchover. Alarm administration such as acknowledgement, clearing, and setting severity-change thresholds. General NE management functions such as discovery, deployment, mediation, polling, statistics management, and security management that includes modifying spans. Create, modify, delete, import, and export public workspaces. View private or public workspaces in the Manage Workspaces list.
Network Element Equipment Management	Physical equipment configuration and management.
Service Management	Service, service component, and service template management functions, excluding mirror-service management.
Old Service Template Management	Management of service templates deprecated; see Template Script Management in this table.
Subscriber Management	Customer and residential subscriber management.
QoS/ACL Policy Management	General QoS and ACL policy management, Ethernet service and time of day suite policy management.
Policy Management (except QoS/ACL)	Management of policies other than those in the QoS/ACL Policy Management role.
Routing Management	Routing protocol, L2 forwarding, and bandwidth management.
Tunnel Management	Service tunnel and underlying transport management.
SAM Management and Operations	Database management (Backups, Reinstantiation, and Switchovers), Alarm acknowledgement, Alarm clearing, and Severity Change Thresholds, Router administration (Scheduling, Backup Policies, Upgrade Policies, Deployment Policies, and Management Ping Policies), NE Security, LPS, and Mediation Policies, SNMP Poller/Stats Polices, Event Notification Policies, MIB Policies, SNMP Performance Statistics, SAM Performance Statistics, Statistics Plotter, Usage and Activity Records, and Span configuration.
Network Element Software Management	NE software management functions.
Fault Management	Functions such as alarm management and remote network monitoring.
Service Test Management	STM functions such as creating, running and scheduling OAM tests.
Script Management	XML API and CLI script management, excluding execution.
Script Execution	XML API and CLI script execution.
Mirror Service Management	Creation and management of mirror services and mirror-service components using the GUI.
OSS Management	Use of the OSSI.

(1 of 2)

Role	Access provided
Telnet/SSH Management	Telnet or SSH access to NEs from the GUI.
CPAM Management	Route Analysis of ISIS Topology, OSPF Topology, MPLS Topology, IP Path monitoring, LSP Monitoring, Checkpoints, and Impact Analysis Scenarios for CPAM management.
CPAM OSS PCA	Route Analysis of ISIS Topology, OSPF Topology, and MPLS Topology for CPAM routing.
CPAM Topology Simulator	Route Analysis of ISIS Topology, OSPF Topology, and MPLS Topology for CPAM Topology Simulator.
Root Cause Analysis (RCA) Object Verification	RCA functions.
Lawful Interception Management	LI configuration for mirror services, mediation policies, and NE security.
Template Script Management	Service and tunnel template script management.
Service Template Script Execution	Service template script execution.
Tunnel Template Script Execution	Tunnel template script execution.
Application Assurance (AA) Management	AA policy management.
Format and Range Policy Management	Format and range policy management, service-creation span rules.
Work Order Activation	The ability to perform CM work order activation.
Configuration Snapshot Export	The ability to perform export CM configuration snapshots.
Create and Delete Access	The ability to create and/or delete eNodeB objects via 5620 SAM-O.
Configuration Management which causes node reset	The ability to configure objects which causes a full or partial reset of the node.
EPC Operator	Read and write permission on all Evolved Packet Core classes.
eNodeB NEM Operator	The ability to launch the 9400 NEM (parameter configuration tool for the eNodeB) from the 5620 SAM client GUI.
Statistics Plotter Profile Management	Management of all Statistics Plotter profiles.
Admin Neto Launch	The ability to open the NEtO with the administration profile.
Viewer Neto Launch	The ability to open the NEtO with the viewer profile.
Default Neto Launch	The ability to open the NEtO with the null profile.
Ageout Constraint Policy Management	The ability to configure Ageout Constraint Policies.

(2 of 2)

A.2 Permissions assigned to 5620 SAM scope of command roles

Table A-4 lists the permissions that can be assigned to a 5620 SAM scope of command role and a description of the permissions.

Table A-4 Permissions assigned to 5620 SAM scope of command roles

Package.Class.Method/Property	Description
aaa	AAA - Configurations for authentication, authorization, and accounting.

(1 of 25)

Package.Class.Method/Property	Description
aaa.RadiusProxyInterface	RADIUS Proxy Interface - Access to Radius Proxy Interface configuration.
aaa.RadiusProxyServer	RADIUS Proxy Server - Access to Radius Proxy Server configuration.
aaa.RadiusServer	RADIUS Server - Access to Radius Server configuration.
aapolicy	Application Assurance - AA policies, configuration, protocol, group, filter, and profiles.
accessuplink	Access Uplink - Configuration of 7210 Access Uplink Specifics for physical ports and LAG interfaces.
accounting	Accounting Policy - Statistics Accounting Policies.
aclfilter	ACL Filter Policy - MAC, IP, and IPv6 ACL Filters.
aclfilterli	ACL Filter LI - All configurations for mirroring of packets matching entries of Lawful intercept ACL filters to mirror destinations.
activation	Activation - Used to define, manage, and deploy work orders used in activation.
activation.Session	Activation Session - Used to manage activation sessions and activate work orders.
activation.Snapshot	Snapshot - Used to manage CM configuration snapshots.
activation.SnapshotEntity	Snapshot Entity - Used to manage snapshot entities.
activation.WebDAVSharedData	Activation. Web DAVShared Data - Ability to restrict access to CM data (CM work orders and configuration snapshots) via the WebDAV protocol.
activation.WorkOrder	Work Order - Used to manage work orders.
aengr	Access Egress Policy - Access Egress QoS Policies.
ageoutcstr	Ageout Constraint - Configurations related to Ageout Constraint.
aingr	Access Ingress Policy - Access Ingress QoS Policies.
ancp	ANCP - Access Node Control Protocol (ANCP) policy and configuration.
ancp.AncpLoopback	ANCP Loopback - Access to ANCP Loopback tests, ANCP Loopback test definitions, and ANCP Loopback deployed tests.
antispoof	Anti-Spoofing - Anti-Spoofing for L2/L3 Access Interfaces and Filter configuration.
aosqos	AoS QoS - Quality of Service for Application over Signaling (AoS QoS) Policy and conditions, AoS QoS configuration for Physical Port and Layer 2 Bridge.
aosredundancy	Aos-Redundancy - AOS Multichassis.
aossas	AOS SAS - OAM tests specific to AOS nodes.
aossas.CPETestGroupHead	CPE SLA Test Group - Access to CPE SLA tests, CPE SLA test definitions, and CPE SLA deployed tests.
aossas.CPETestHead	CPE SLA Test - Access to CPE SLA tests, CPE SLA test definitions, and CPE SLA deployed tests.
apipe	APipe - All contained objects are listed. Package access is not currently used.
apipe.Apipe	Apipe Service - Access to VLL ATM Pipe (Apipe) Service objects themselves.

(2 of 25)

Package.Class.Method/Property	**Description**
apipe.Site	Apipe Site - Access to Apipe Sites.
aps	APS - Automatic Protection Switching (APS) Groups.
arp	ARP - ARP host and configurations on service interfaces.
atm	ATM - ATM configuration for Service interfaces and routers, ATM Connections, ILMI Link, and other ATM related objects.
atm.AtmPing	ATM Ping - Access to ATM Ping tests, ATM Ping test definitions, and ATM Ping deployed tests.
atmpolicy	ATM QoS Policy - ATM Traffic Descriptor Policy.
audit	Resource Audit - Ability to execute audits and view audit results.
autoconfig	Automatic Configuration - Auto-Config Source and Target Node Profiles.
autoconfig.AutoConfigScriptManager.method_configure	Automatic Configuration - method_configure - Ability to create/modify/delete an auto-config script.
autoconfig.AutoConfigScriptManager.method_copyContents	Automatic Configuration - method_copyContents - Ability to copy the contents of one auto-config script to new one.
bfd	BFD - Bi-Directional Forwarding Detection (BFD) can be configured on rtr.NetworkInterface, ies.L3AccessInterface, vprn.L3AccessInterface and vprn.NetworkInterface.
bgp	Routing Management: BGP - Border Gateway Protocol (BGP) configuration for routers, policies, peers, groups, MD5, and Confederations.
bgp.Site	BGP Site - Access to a BGP protocol site on a router.
bulk	Bulk Operations - Not currently used.
bulk.BulkChange	Bulk Change - The abilty to create, modify, and/or delete bulk changes.
bulk.BulkManager.method_execute	Bulk Operations Manager - method_execute - The ability to execute bulk operations.
bulk.BulkManager.method_generateBatches	Bulk Operations Manager - method_generateBatches - The ability to generate batches for bulk operations.
bundle	Bundle - Bundle configuration for T1/E1 Multilink Group and channel members, APS, Multichassis and Service interfaces.
cac	CAC - CAC configuration for Physical Links, Physical Port and other CAC related objects.
calltrace.WebDAVSharedData	Calltrace. Web DAVShared Data - Ability to restrict access to call traces via the WebDAV protocol.
ccag	CCAG - Cross-Connect Aggregation Group (CCAG) MDA card and forwarding path configuration.
cflowd	Cflowd - CFLOWD Objects.
cflowd.NeCflowd	Cflowd Configuration - Ability to configure cflowd params for SR.
cflowd.NeCollector	Cflowd Collector Configuration - Ability to configure collector for cflowd params for SR.
clear	Clear - Clear application commands and requests.
cli	CLI - Ability to connect to open NE sessions from SAM.
cli.SSH	Cli. SSH - Ability to open an SSH Telnet session to the node from SAM.

(3 of 25)

Package.Class.Method/Property	**Description**
cli.Telnet	Cli. Telnet - Ability to open a Telnet session to the node from SAM.
connprof	Connection Profile - Connection Profile configuration.
cpipe	CPipe - Access to this package is for configuring CES Interface Specifics for Cpipe specific SAPs.
cpipe.Cpipe	Cpipe Service - Access to VLL Circuit Emulation Pipe (Cpipe) Service objects themselves.
cpipe.Site	Cpipe Site - Access to Cpipe Sites.
crdtctrl	Credit Control - Credit Control configuration.
customproperties	Custom Properties - Custom properties configuration.
db	Database - Configuration for Size constraint policies and Database file policies.
db.AuxiliaryDatabase.method_reinstantiationDatabase	Auxiliary Database - method_reinstantiationDatabase - Ability to perform a auxiliary database reinstantiation.
db.AuxiliaryDatabase.method_snapshotDatabase	Auxiliary Database - method_snapshotDatabase - Ability to perform a auxiliary database snapshot.
db.DatabaseManager.method_backup	Database Manager - method_backup - Ability to perform a database backup.
db.DatabaseManager.method_reinstantiateStandby	Database Manager - method_reinstantiateStandby - Ability to re-instantiate the standby database.
db.DatabaseManager.method_snapshotAllDatabases	Database Manager - method_snapshotAllDatabases - Ability to perform a auxiliary database snapshot.
db.DatabaseManager.method_switchover	Database Manager - method_switchover - Ability to perform a database switchover.
dctr	Data Center - Data Center information and configurations.
dhcp	DHCP - Dynamic Host Configuration Protocol (DHCP) Server for rtr.VirtualRouter and vprn.Site.
diameter	Diameter - Access to this package is for configuring Diameter related configurations, e.g. Diameter Policy.
dns	Domain Name System - Domain Name System.
dynsvc	Dynamic Services - Dynamic Services Configuration.
epipe	EPipe - Access to this package is for configuring CES Interface Specifics and FR Interface Specifics for Epipe specific SAPs.
epipe.Epipe	Epipe Service - Access to VLL Ethernet Pipe (Epipe) Service objects themselves.
epipe.PbbMacName	PBB MAC Name - Ability to configure the MAC Name Address for a Network Element.
epipe.Site	Epipe Site - Access to Epipe Sites.
equipment	Physical Equipment - General equipment configuration.
equipment.PortPolicy	Port Policy - Access to Port Policy for 7750 nodes.
equipment.Shelf.method_rebootUpgrade	Shelf - method_rebootUpgrade - Ability to perform node reboot upgrade.
ethernetequipment	Ethernet Equipment - Ethernet Equipment configuration.

(4 of 25)

Package.Class.Method/Property	Description
ethernetoam	Ethernet OAM - Maintenance Domains and Maintenance Entity Groups, autogeneration of the MEPs on each SAP or Binding in a Service.
ethernetoam.CcmTest	CFM Continuity Check - Access to Continuity Check tests, Continuity Check test definitions, and Continuity Check deployed tests.
ethernetoam.CcTest	Global Maintenance Entity Group - Access to Continuity Check tests, Continuity Check test definitions, and Continuity Check deployed tests.
ethernetoam.CfmDmmBin	CFM DMM Session Bin - Access to CFM DMM Test Session, CFM DMM Test Session definitions.
ethernetoam.CfmDmmSession	CFM DMM Test Session - Access to CFM DMM Test Session, CFM DMM Test Session definitions.
ethernetoam.CfmEthTest	CFM Eth Test - Access to CFM EthTests, CFM EthTest definitions, and CFM EthTest deployed tests.
ethernetoam.CfmLinkTrace	CFM Link Trace - Access to Link Trace tests, Link Trace test definitions, and Link Trace deployed tests.
ethernetoam.CfmLMTest	CFM LM Test - Access to CFM LM tests, CFM LM test definitions, and CFM LM deployed tests.
ethernetoam.CfmLoopback	CFM Loopback - Access to CFM Loopback tests, CFM Loopback test definitions, and CFM Loopback deployed tests.
ethernetoam.CfmOneWayDelayTest	CFM One Way Delay Test - Access to CFM One Way Delay tests, CFM One Way Delay test definitions, and CFM One Way Delay deployed tests.
ethernetoam.CfmOneWaySlm	CFM One Way SLM Test - Access to CFM One Way SLM tests, CFM One Way SLM test definitions, and CFM One Way SLM deployed tests.
ethernetoam.CfmSingleEndedLossTest	CFM Single Ended Loss Test - Access to CFM Single Ended Loss tests, CFM Single Ended Loss test definitions, and CFM Single Ended Loss deployed tests.
ethernetoam.CfmSlmSession	CFM SLM Test Session - Access to CFM SLM Test Session, CFM SLM Test Session definitions.
ethernetoam.CfmTwoWayDelayTest	CFM Two Way Delay Test - Access to CFM Two Way Delay tests, CFM Two Way Delay test definitions, and CFM Two Way Delay deployed tests.
ethernetoam.CfmTwoWaySlm	CFM Two Way SLM Test - Access to CFM Two Way SLM tests, CFM Two Way SLM test definitions, and CFM Two Way SLM deployed tests.
ethernetoam.EthSession	Ethernet Test Session - Access to Ethernet Test Session, Ethernet Test Session definitions.
ethernetservice	Ethernet Service Policy - SAP Profile and UNI Profile policies.
ethernettunnel	Ethernet Tunnel - Ethernet Tunnel configuration.
ethring	Ethernet Ring - Ethernet Ring Configuration.
fabricqos	Fabric QoS Policies - Fabric Profile QoS policy.
file	File Policy - File creation on the NE for events and accounting.
filter	Filter - Public search filters.
filterprefixlist	Filter Policy - Filter PrefixList and PortList Policies.

(5 of 25)

Package.Class.Method/Property	Description
firewall	Firewall - All Firewall configurations.
fm	Fault Management - Alarm policies, Severity change thresholds, Alarms, Notes, and History.
fm.AlarmHistoryDatabase.method_purge	Alarm History Database - method_purge - Ability to purge the alarm history database.
fm.FaultManager	Fault Manager - Access to assign OLC state, alter severity, clear, acknowledge, and remove faults.
fm.FaultManager.method_editNote	Fault Manager - method_editNote - Ability to edit an alarm note.
fm.GlobalPolicy	Global Alarm Behavior - Access to configure the global alarm behavior.
fm.SpecificPolicy	Specific Alarm Policy - Access to configure specific alarm policies.
fpipe	FPipe - All contained objects are listed. Package access is not currently used.
fpipe.Fpipe	Fpipe Service - Access to Frame Relay Pipe (Fpipe) Service objects themselves.
fpipe.Site	Fpipe Site - Access to Fpipe Sites.
fr	Frame Relay - Frame Relay configuration for Service interfaces and routers.
generic	Generic - Generic configuration for SAM objects, deployment, and administrative state changes for DHCP and Multichassis objects, Maintenance Association End Points (MEP), and SRRP instances.
generic.GenericObject.method_collectData	Generic Object - method_collectData - Ability to collect and plot real-time statistics.
genericlog	Log Viewer - Display logs in Log Viewer.
genericne	Generic NE - Generic NE Interface and Profile configuration.
gsmp	GSMP - General Switch Management Protocol (GSMP) configuration for VPLS, MVPLS and VPRN routing instances.
hip	Horizontal Integration Protocol - Access to HIP managed Element Managers and subtending nodes.
hip.EMServer	Element Manager - Access to HIP managed Element Managers.
hip.EMSystem	EM System - Access to HIP managed EM Systems.
hpipe	HPipe - All contained objects are listed. Package access is not currently used.
hpipe.Hpipe	Hpipe Service - Access to HPipe (Hpipe) Service objects themselves.
hpipe.Site	Hpipe Site - Access to Hpipe Sites.
icmp	ICMP - Internet Control Message Protocol (ICMP) and Domain Name System (DNS) test results.
icmp.DnsPing	DNS Ping - Access to DNS Ping tests, DNS Ping test definitions, and DNS Ping deployed tests.
icmp.IcmpPing	ICMP Ping - Access to ICMP Ping tests, ICMP Ping test definitions, and ICMP Ping deployed tests.
icmp.IcmpTrace	ICMP Trace - Access to ICMP Trace tests, ICMP Trace test definitions, and ICMP Trace deployed tests.

(6 of 25)

Package.Class.Method/Property	Description
ies	IES - Access to this package is for configuring Group Interfaces, SAPs, MSAPs, IGMP Host Tracking on Sites and SAPs, and FR Interface Specifics for IES specific SAPs.
ies.AaInterface	IES AA Interface - Access to IES AA Interfaces.
ies.Ies	IES Service - Access to Internet Enhanced Service (IES) Service objects themselves.
ies.L3AccessInterface	IES L3 Access Interface - Access to IES L3 Access Interfaces.
ies.Site	IES Site - Access to IES Sites.
ies.SubscriberInterface	IES Subscriber Interface - Access to IES Subscriber Interfaces.
igh	IGH - Interface-Group-Handlers.
igmp	IGMP - Internet Group Management Protocol (IGMP) configuration for Service interfaces and routers.
igmp.Site	IGMP Site - Access to IGMP Sites.
impact.FullReset	Impact. Full Reset - Ability to configure objects which will result in a full reset of the node. Currently applies to 9412 node.
impact.PartialReset	Impact. Partial Reset - Ability to configure objects which will result in a partial reset of impacted SW/HW unit. Currently applies to 9412 node.
ipfix	IPFIX - IPFIX Policy.
ipipe	IPipe - Access to this package is for configuring IPCP on L2 Access Interfaces and FR Interface Specifics for Ipipe specific SAPs.
ipipe.Ipipe	Ipipe Service - Access to IP Interworking Pipe (Ipipe) Service objects themselves.
ipipe.L2AccessInterface	L2 Access Interface - Access to IPipe L2 Access Interfaces.
ipipe.Site	Ipipe Site - Access to Ipipe Sites.
ipsec	IP Security - IKE Policy and IPsec Transform.
isa	ISA - ISA-IPsec, ISA-MG, and ISA-AA configuration on a MDA card for IP Security, LTE, and Application Assurance.
isa.MgGroupMember	ISA-MG Group Member - Configuration of ISA-MG Group Member.
isa.MgIsaGroup	ISA-MG Group - Configuration of ISA-MG Group.
isis	Routing Management: ISIS - IS-IS configuration for Service interfaces and routers, Area, Adjacency, Neighbors, Policies and other IS-IS related objects.
l2fib	L2 FIB - Layer 2 Forwarding Information Base (FIB) configuration for Multicast and Non-Multicast.
l2fwd	L2 Forwarding - All Layer 2 Forwarding configuration for Service interfaces and routers, ciruits, ports, Spanning Tree, Registration, FIB, Mac Protection, IGMP Snooping, etc.
l2tp	L2TP - L2TP configuration for Service interfaces and routers, Groups, Tunnels, PeersRPs, and other L2TP related objects.
l3fwd	L3 Forwarding - All Layer 3 Forwarding configuration for Service interfaces and routers, Import and Export policies, Dot1p and DSCP for VPRNs.
lag	LAG - Link Aggregation Group (LAG) configuration for Service interfaces and routers.

(7 of 25)

Package.Class.Method/Property	Description
layer2	Layer 2 - All Layer 2 configuration: Bridges, Transparent LAN Service (TLS), and VLAN interfaces.
ldp	Routing Management: LDP - Label Distribution Protocol (LDP) configuration for Service interfaces and routers, Session, MD5 Key, Equal-Cost Multipath Routing (EMCP), Forwarding Equivalency Class (FEC), Policies, and Peers.
lldp	LLDP - Link Layer Discovery Protocol (LLDP) configuration on equipment.PhysicalPort.
localuserdb	Local User DB - DHCP or PPPoE configuration for Local User Databases on a router.
log	Statistics - Parent package for all statistics classes.
log.LogToFileManager.property_jmsRetries	Log To File Manager - property_jmsRetries - LogToFile preferences can only be modified by a user with an administrator role.
log.LogToFileManager.property_retention	Log To File Manager - property_retention - LogToFile preferences can only be modified by a user with an administrator role.
log.LogToFileManager.property_rollover	Log To File Manager - property_rollover - LogToFile preferences can only be modified by a user with an administrator role.
lps	LPS - Learned Port Security (LPS) configuration for layer2.Bridge and MAC Entries for ports.
lte	LTE - All LTE configurations and status.
lte.ApnPolicyRuleBase	Policy Rule Base - Configuration of Policy Rule Base.
lte.CallTraceDirectory	Call Trace Directory - Configuration of Call Trace Directory.
lte.DccaProfile	DCCA Profile - Configuration of DCCA Profile.
lte.DiameterPeerListEntry	Diameter Peer List Entry - Configuration of Diameter Peer List Entry.
lte.DiameterPeerProfile	Diameter Peer Profile - Configuration of Diameter Peer Profile.
lte.DiameterProfile	Diameter Profile - Configuration of Diameter Profile.
lte.DiscoveryLog	Drill Down Log - Creation of Drill Down Log.
lte.DupRadiusAccServerGroup	Duplicate Accounting RADIUS Server Group - Configuration of Serving Gateway APN.
lte.ENBEquipment.method_launchNEM	ENB Equipment - method_launchNEM - Ability to launch NEM.
lte.EPSPathDiscoveredLinkComponent	EPS Path Discovery Link Component - Configuration of EPS Path Discovery Link Component.
lte.EPSPathDiscoveryHint	EPS Path Drill Down Hint - Configuration of EPS Path Drill Down Hint.
lte.EPSPathDiscoveryProfile	Path Drill Down Profile - Configuration of Path Drill Down Profile.
lte.EPSPathInterfaceComponent	EPS Path Interface Component - Configuration of EPS Path Interface Component.
lte.EPSPathLinkComponent	EPS Path Link Component - Configuration of EPS Path Link Component.
lte.EPSPathSapComponent	EPS SAP Component - Configuration of EPS SAP Component.
lte.EPSPathSegment	EPS Path Segment - Configuration of EPS Path Segment.
lte.EPSPathServiceComponent	EPS Path Service Component - Configuration of EPS Path Service Component.

(8 of 25)

Package.Class.Method/Property	**Description**
lte.EPSPathSiteComponent	EPS Path Site Component - Configuration of EPS Path Site Component.
lte.GtpPrimaryServerListEntry	GTP Primary Server List Entry - Configuration of GTP Primary Server List Entry.
lte.GtpPrimeServerGroupProfile	GTP Prime Server Group Profile - Configuration of GTP Prime Server Group Profile.
lte.GtpProfile	GTP Profile - Configuration of GTP Profile.
lte.IpPool	IP Address Pool - Configuration of IP Address Pool.
lte.IpPoolBinding	IP Address Pool Binding - Configuration of IP Address Pool Binding.
lte.IpPoolEntry	IP Address Pool Entry - Configuration of IP Address Pool Entry.
lte.LTEEquipment.method_launchQoSAnalyzer	Lte. LTEEquipment - method_launchQoSAnalyzer - Ability to launch LTE QoS Analyzer.
lte.MobileNodeRegion	Mobile Node Region/Public Land Mobile Network (PLMN) - Configuration of Mobile Node Region.
lte.PdnApn	PDN APN - Configuration of PDN APN.
lte.PDNGateway	PDN Gateway - Configuration of PDN Gateway.
lte.PdnGxReferencePoint	PDN Gx Reference Point - Configuration of Pdn Gx Reference Point.
lte.PdnRfReferencePoint	PDN Rf Reference Point - Configuration of PGW Rf Reference Point.
lte.PdnS5ReferencePoint	PDN S5 Reference Point - Configuration of PGW S5 Reference Point.
lte.PdnS8ReferencePoint	PDN S8 Reference Point - Configuration of PGW S8 Reference Point.
lte.PdnSignalling	PGW Signalling - Configuration of PGW Signalling.
lte.PgwChargingProfile	PGW Charging Profile - Configuration of PGW Charging Profile.
lte.PlmnListPolicy	PLMN List Profile - Configuration of PLMN List Profile.
lte.PlmnListPolicyGroup	PLMN List Group - Configuration of PLMN List Group.
lte.QciPolicy	QCI Policy - Configuration of QCI Policy.
lte.QciPolicyEntry	QCI Policy Entry - Configuration of QCI Policy Entry.
lte.S11ReferencePoint	S11 Reference Point - Configuration of S11 Reference Point.
lte.S1uReferencePoint	S1-u Reference Point - Configuration of S1u Reference Point.
lte.ServingGateway	Serving Gateway - Configuration of Serving Gateway.
lte.SgwApn	Serving Gateway APN - Configuration of Serving Gateway APN.
lte.SgwChargingProfile	SGW Charging Profile - Configuration of SGW Charging Profile.
lte.SgwRfReferencePoint	SGW Rf Reference Point - Configuration of SGW Rf Reference Point.
lte.SgwS5ReferencePoint	SGW S5 Reference Point - Configuration of SGW S5 Reference Point.
lte.SgwS8ReferencePoint	SGW S8 Reference Point - Configuration of SGW S8 Reference Point.
lte.SgwSignalling	Serving Gateway Signalling - Configuration of Serving Gateway Signalling.
lte.SubscAndEquipmentTraces	Subsc And Equipment Traces - Configuration of Call Traces.
lte.TrustedPeerListEntry	Trusted Peers - Configuration of Trusted Peer List Entries.

(9 of 25)

Package.Class.Method/Property	Description
lte.TrustedPeerListEntryUnlisted	Unlisted Peer - Configuration of Unlisted Trusted Peer List Entries.
lte.TrustedPeerListPolicy	Trusted Peer List Policy - Configuration of Trusted Peer List Policy.
lteanr	LTE - Access to LTE ANR profiles.
lteggsn	LTE - All LTE configurations and status.
lteggsn.CdrAvpOptionProfile	CDR AVP Option Profile - Configuration of CDR AVP Option Profile.
lteggsn.DccaRatingGroup	DCCA Rating Group - Configuration of Dcca Rating Group.
lteggsn.GnReferencePoint	Gn Reference Point - Configuration of Gn Reference Point.
lteggsn.GpReferencePoint	Gp Reference Point - Configuration of Gp Reference Point.
lteggsn.GyAvpOptionProfile	Gy AVP Option Profile - Configuration of Gy AVP Option Profile.
lteggsn.PdnGyReferencePoint	Gy Reference Point - Configuration of Gy Reference Point.
lteggsn.PgwGaReferencePoint	PGW Ga Reference Point - Configuration of PGW Ga Reference Point.
lteggsn.SgwGaReferencePoint	SGW Ga Reference Point - Configuration of SGW Ga Reference Point.
ltegw	LTE - All LTE configurations and status.
ltegw.ApnListPolicy	APN List Profile - Configuration of APN List Profile.
ltegw.ApnListPolicyGroup	APN List Group - Configuration of APN List Group.
ltegw.DiameterPeerRedirHostEntry	Diameter Peer Redirect Host Entry - Configuration of Diameter Peer Redirect Host Entry.
ltegw.DiameterPeerSupportedHost	Diameter Peer Support Supported Host - Configuration of Diameter Peer Support Host Entry.
ltegw.PcscfGroupProfile	P-CSCF Group Profile - Configuration of P-CSCF Group Profile.
ltegw.PcscfPeerEntry	P-CSCF Peer Entry - Configuration of P-CSCF Peer Entry.
ltegw.PcscfResolvedPeerIPEntry	P-CSCF Resolved Peer Ip Entry - Configuration of P-CSCF Peer Entry.
ltegw.SCTPProfile	SCTP Profile - Configuration of SCTP Profile.
ltegw.UMTSQoSPolicy	UMTS QoS Policy - Configuration of UMTS QoS Policy.
lteli	LTE LI - All LTE LI configurations and status.
lteli.DFPeer	LTE LI Delivery Function Peer - Configuration of LTE LI Delivery Function Peer.
lteli.DFPeerCardGroup	LTE LI Delivery Function Peer Card Group Status - Display of LTE LI Delivery Function Peer Card Status.
lteli.InterceptionTarget	LTE LI Interception Target - Configuration of LTE LI Interception Target.
lteli.LILteCfg	LTE LI Pre Configuration - Contains system Lawful Intercept Configuration for MG.
ltemme	LTE - All LTE MME configurations.
ltemme.MmeInstance.method_abortMmeLoadBalance	WMM Instance - method_abortMmeLoadBalance - Ability to abort MME load balancing operation.
ltemme.MmeInstance.method_interMmeLoadBalance	WMM Instance - method_interMmeLoadBalance - Ability to perform inter MME load balancing operation.

(10 of 25)

Package.Class.Method/Property	Description
ltemme.MmeInstance.method_intraMmeLoadBalance	WMM Instance - method_intraMmeLoadBalance - Ability to perform intra MME load balancing operation.
ltemme.MmeInstance.method_lockMmeAggregateService	WMM Instance - method_lockMmeAggregateService - Ability to lock the MME aggregate service.
ltemme.MmeInstance.method_unlockMmeAggregateService	WMM Instance - method_unlockMmeAggregateService - Ability to unlock the MME aggregate service.
lteperf	LTE Performance Management - All LTE configurations : SGW, PGW, eNodeB.
ltepmip	LTE - All LTE configurations and status.
ltepmip.Pmipv6Profile	PMIPv6 Profile - Configuration of PMIPv6 Profile.
ltepmip.S2aReferencePoint	S2a Reference Point - Configuration of S2a Reference Point.
ltepmip.S2bReferencePoint	S2b Reference Point - Configuration of S2b Reference Point.
ltepmip.S6bAvpOptionProfile	S6b AVP Option Profile - Configuration of S6b AVP Option Profile.
ltepmip.S6bReferencePoint	S6b Reference Point - Configuration of S6b Reference Point.
ltepolicyoptions	LTE - All LTE configurations and status.
ltepolicyoptions.AsoOptions	ASO Options Profile - Configuration of ASO Options Profile.
ltepolicyoptions.ChargingRuleUnit	Charging Rule Unit Profile - Configuration of ChargingRuleUnit Profile.
ltepolicyoptions.DhcpServerGroupProfile	DHCP Server Group Profile - Configuration of DHCP Server Group Profile.
ltepolicyoptions.DhcpSGPeerEntry	DHCP Peer Entry - Configuration of DHCP Peer Entry.
ltepolicyoptions.GxAvpOptionProfile	Gx AVP Option Profile - Configuration of Gx AVP Option Profile.
ltepolicyoptions.PolicyRule	Policy Rule Profile - Configuration of PolicyRule Profile.
ltepolicyoptions.PolicyRuleBase	Policy Rule Base Profile - Configuration of PolicyRuleBase Profile.
ltepolicyoptions.PolicyRuleBaseEntry	Base Policy Entry - Configuration of PolicyRuleBase Profile.
ltepolicyoptions.PolicyRuleUnit	Policy Rule Unit Profile - Configuration of PolicyRuleUnit Profile.
ltepolicyoptions.PolRuleUnitFlwDescription	Policy Rule Unit Flow Description Entry - Configuration of Flow Description Entry.
ltepolicyoptions.ServiceClassIndicator	Service Class Indicator - Configuration of ServiceClassIndicator Profile.
ltepolicyoptions.TrafficRedirectProfile	Traffic Redirect Profile - Configuration of Traffic Redirect Profile.
ltepolicyoptions.TrafficRedirectTarget	Traffic Redirect Target Entry - Configuration of Traffic Redirect Target Entry.
ltepool	LTE POOL - All LTE POOL configurations.
ltepool.MmeInstanceBinding	MME Instance Binding - Ability to configure associations between an MME Instance and an MME Pool.
ltepool.TaBinding	Tracking Area Binding - Ability to configure associations between a Tracking Area and an MME Pool.
lteradius	LTE - All LTE configurations and status.
lteradius.RadiusGroupProfile	RADIUS Group Profile - Configuration of Radius Group Profile.
lteradius.RadiusPeerProfile	RADIUS Peer Profile - Configuration of RADIUS Peer Profile.
lteradius.RadiusProfile	RADIUS Profile - Configuration of RADIUS Profile.

(11 of 25)

Package.Class.Method/Property	Description
ltes1mme	LTES1MME - All LTE S1MME Configurations and Monitoring Status.
ltesecurity	LTE Security - All LTE configurations : SGW, PGW, Bearers, and more.
lteservice	LTE - All LTE configurations and status.
ltesgsn	LTE - All LTE configurations and status.
ltesgsn.SgwS12ReferencePoint	S12 Reference Point - Configuration of S12 Reference Point.
ltesgsn.SgwS4ReferencePoint	S4 Reference Point - Configuration of S4 Reference Point.
ltethreshold	LTE - All LTE configurations and status.
lteuserstats	LTE - All LTE configurations and status.
lteuserstats.UserStatsQuery	User Stat Query - Configuration of User Stats Queries.
lteuserstats.UserStatsQueryOutputSnapshot	User Query Output Snapshot - Configuration of User Stats Query Snapshots.
lteuserstats.UserStatsUserPgw	PGW User Data - Configuration of User Stats User Output.
lteuserstats.UserStatsUserSgw	SGW User Data - Configuration of User Stats User Output.
mediation	Router Admin: Policies - Router administration: Backup Policies, Upgrade Policies and Software images, Deployment Policies, and Management Ping Policies.
mirror	Mirror - All configurations for Service Mirroring.
mirror.Endpoint	Endpoint - Access to MIRROR Endpoints.
mirror.Mirror	Mirror Service - Access to Mirror Service objects themselves.
mirror.Site	Mirror Site - Access to Mirror Sites.
mld	MLD - Multicast Listener Discovery Protocol (MLD) configuration for a Service interfaces and routers.
mmepolicy	WMM Policies - Management of policies associated with 9471 WMM.
mmepolicy.MMEEmergencyNumListPolicy	WMM Emergency Number List - Configuration of Emergency Number List.
mmepolicy.MMEGTPProfile	WMM GTP Profile - Configuration of GTP Profile.
mmepolicy.MMESCTPProfile	WMM SCTP Profile - Configuration of SCTP Profile.
mmepolicy.WMMPfmJobEntry	WMM Performance Measurement Job Entry - Configuration of Performance Measurement Job Entry.
mmepolicy.WMMPfmJobMts	WMM Performance Measurement Job Measurements - Configuration of Performance Measurement Job Measurements.
mmepolicy.WMMPfmJobSched	WMM Performance Measurement Job Schedules - Configuration of Performance Measurement Job Measurements.
mmepolicy.WMMPfmMeasGroupName	WMM Performance Measurement Group Name - Configuration of Performance Measurement Group Name.
mmepolicy.WMMPfmMeasGroups	WMM Performance Measurement Groups - Configuration of Performance Measurement Groups.
monitor	Monitor - Subscriber Host monitoring and SAP monitoring.
monpath	Monitored Path - IP path monitoring and LSP monitoring.

(12 of 25)

Package.Class.Method/Property	Description
mpls	Path/Routing Management: MPLS - Multiprotocol Label Switching (MPLS) configuration on a rtr.VirtualRouter, LSPs, Segments, Hops, Tunnels, CrossConnects, and other MPLS related objects.
mpls.LdpTreeTrace	LDP Tree Trace - Access to LDP Tree Trace tests, LDP Tree Trace test definitions, and LDP Tree Trace deployed tests.
mpls.LspPing	LSP Ping - Access to LSP Ping tests, LSP Ping test definitions, and LSP Ping deployed tests.
mpls.LspTrace	LSP Trace - Access to LSP Trace tests, LSP Trace test definitions, and LSP Trace deployed tests.
mpls.P2MPLspPing	P2MP LSP Ping - Access to P2MP LSP Ping tests, P2MP LSP Ping test definitions, and P2MP LSP Ping deployed tests.
mpls.P2MPLspTrace	P2MP LSP Trace - Access to P2MP LSP Trace tests, P2MP LSP Trace test definitions, and P2MP LSP Trace deployed tests.
mplstp	MPLS TP - MPLS TP Configuration for Sites.
mpr	9500 MPR - 9500 Microwave Packet Radio (MPR) VLAN Paths and Hops.
mpr.Al2AccessInterface	9500 MPR Apipe L2 Access Interface - Access to L2AccessInterface objects.
mpr.Apipe	9500 MPR Apipe Service - Access to vll ATM Pipe (Apipe) Service objects themselves.
mpr.Asite	9500 MPR Apipe Site - Access to the service instance objects.
mpr.Cpipe	9500 MPR Cpipe Service - Access to VLL Circuit Emulation Pipe (Cpipe) Service objects themselves.
mpr.El2AccessInterface	9500 MPR Epipe L2 Access Interface - Access to L2AccessInterface objects.
mpr.Epipe	9500 MPR Epipe Service - Access to VLL Ethernet Pipe Service objects themselves.
mpr.Esite	9500 MPR Epipe Site - Access to the service instance objects.
mpr.L2AccessInterface	9500 MPR Cpipe L2 Access Interface - Access to L2AccessInterface objects.
mpr.Site	9500 MPR Cpipe Site - Access to the service instance objects.
msappolicy	MSAP Policy - MSAP policy configuration.
msdp	MSDP - Multicast Source Discovery Protocol (MSDP) configuration for a rtr.VirtualRouter, MD5 Key, Peers, Policies and Source.
multicast	Multicast - Multicast Connection Admission Control (CAC) Policies and Bandwidth Policies.
multicast.CustomerVlanTag	Customer Vlan Tag - Configuration of Customer VLAN Tags for a Multicast VLAN.
multicast.MfibPing	MFIB Ping - Access to MFIB Ping tests, MFIB Ping test definitions, and MFIB Ping deployed tests.
multicast.Mrinfo	Mrinfo - Access to Mrinfo tests, Mrinfo test definitions, and Mrinfo deployed tests.
multicast.Mtrace	Mtrace - Access to Mtrace tests, Mtrace test definitions, and Mtrace deployed tests.
multicastmgr	CPAM: Multicast - All CPAM Multicast related objects: PIM Domain, VPLS Domain, Groups, and Sources.

(13 of 25)

Package.Class.Method/Property	Description
multichassis	Multi-Chassis - Multi-Chassis configuration for a router; LAGs, Rings, Syncs, Peers, VLAN Ranges, IPsecs.
mvpls	MVPLS - All contained objects are listed. Package access is not currently used.
mvpls.BL2AccessInterface	MVPLS B-L2 Access Interface - Access to MVPLS B-L2 Access Interfaces.
mvpls.BSite	MVPLS B-Site - Access to MVPLS B-Sites.
mvpls.EvpnSite	MVPLS EVPN-Site - Access to MVPLS EVPN-Sites on a MVPLS Service.
mvpls.IL2AccessInterface	MVPLS I-L2 Access Interface - Access to MVPLS I-L2 Access Interfaces.
mvpls.ISite	MVPLS I-Site - Access to MVPLS I-Sites.
mvpls.L2AccessInterface	MVPLS L2 Access Interface - Access to MVPLS L2 Access Interfaces (except I and B).
mvpls.Mvpls	MVPLS Service - Access to Management Virtual Private LAN Service (MVPLS) Service objects themselves.
mvpls.Site	MVPLS Site - Access to MVPLS Sites (except I and B).
mvrp	MVRP - MVRP global configuration and for Interfaces(Ports and LAG's).
mwa	Microwave Aware - Access to MW (Microwave) Link and MW Link Members configuration for Service interfaces and routers.
nat	Network Address Translation - NAT Policy.
nat.LsnSubSession	LSN Subscriber Session - Access to NAT Package.
nat.PcpServer	Port Control Protocol Server - Access to Port Control Protocol Server configuration.
nat.PcpServerInterface	Port Control Protocol Server Interface - Access to Port Control Protocol Interface configuration.
neaudit	NE Audit Management - Ability to manage NE Audits.
nelicense	NeLicense - Apply License on the node.
netca	NE Threshold Crossing Alerts - Manage NE Threshold Crossing Alert profiles.
netw	Network - Network objects: groups and links.
netw.AdvertisedNode	Advertised Node - Control of Discovered Nodes.
netw.NeLimitHolder	NE Limit Holder - Access to NE Limit configuration.
netw.NetworkElement	Network Element - Access to Network Elements.
netw.NetworkElement.method_executeCli	Network Element - method_executeCli - Execute a single raw CLI command on this Network Element.
netw.NetworkElement.method_executeMultiCli	Network Element - method_executeMultiCli - Execute Multiple CLI commands on this Network Element.
netw.NetworkElement.method_GUICrossLaunch	Network Element - method_GUICrossLaunch - The ability to launch LTE web-browser based tools.
netw.NetworkElement.method_NetoAdminProfileBasedLaunch	Network Element - method_NetoAdminProfileBasedLaunch - The ability to launch Neto with Admin profile.
netw.NetworkElement.method_NetoViewerProfileBasedLaunch	Network Element - method_NetoViewerProfileBasedLaunch - The ability to launch Neto with Viewer profile.

(14 of 25)

Package.Class.Method/Property	**Description**
netw.NetworkElement.property_elementManagerCmd	Network Element - property_elementManagerCmd - Ability to update the 'Alternate Element Manager' command for a GNE.
netw.NodeDiscoveryControl	Node Discovery Control - Control of Discovered Nodes.
netw.Topology	Discovery Manager - Access to the Discovery Manager.
netw.Topology.method_move	Discovery Manager - method_move - Ability to move a node or group on the SAM Client GUI maps.
netw.UplinkBofConfiguration	Uplink Bof Configuration - Ability to configure the Uplink BOF for a 7210 node.
netw.UplinkRouteConfiguration	Uplink Route Configuration - Ability to configure the Uplink Routes for a 7210 node.
niegr	Network Ingress/Egress Policy - Network Policies.
nodelog	Node Log Policy - Filter Log and Sys Log Target Policies.
nqueue	Network Queue Policy - Network Queue QoS Policies.
ntp	Network Time Protocol - Network Time Protocol.
ntp.NTPBroadcast	NTP Broadcast - Ability to configure broadcast for ntp params.
ntp.NTPMulticast	NTP Multicast - Ability to configure multicast for ntp params.
olc	Object Life Cycle.
olc.OLCSchedulerManager.property_autosetMaintenanceOLCStateOnAdminDown	OLC Scheduler Manager - property_autosetMaintenanceOLCStateOnAdminDown - Service preferences can only be modified by a user with an administrator role.
olc.OLCSchedulerManager.property_createAlarmNotification	OLC Scheduler Manager - property_createAlarmNotification - OLC preferences can only be modified by a user with an administrator role.
olc.OLCSchedulerManager.property_leadTimeForNotification	OLC Scheduler Manager - property_leadTimeForNotification - OLC preferences can only be modified by a user with an administrator role.
openflow	OpenFlow - OpenFlow configuration and status on a router.
optical	Optical Management - Optical NE Specific Information.
optical.MultipointServicePath	Multipoint Service Path - Access for all Multi Point Service Paths.
optical.MultipointTransportService	Multipoint Transport Service - Access for all optical services.
optical.TransportService	Optical Transport Service - Access for all optical services.
opticalacl	Optical Access Control Lists - ACL Management.
opticalequipment	Optical Management - Optical NE Specific Configuration.
opticsperf	Optics Specifics - All 1830 PSS configurations.
ospf	Routing Management: OSPF - OSPF configuration for Service interfaces and routers, Area, Adjacency, MD5 Key, Virtual Links Neighbors, LSAs, Policies and other OSPF related objects.
ospf.Site	OSPF Site - Access to OSPF Sites.
oss	OSS - Ability to connect to the SAM Server through the OSS interface.
oth	Optical Transport Hierarchy - OTH Management.

(15 of 25)

Package.Class.Method/Property	**Description**
pae802_1x	PAE 802.1x - Port Access Entity (PAE) configuration for a router and physical port; RADIUS Server Policy.
pbbvlan	PBBVLAN - Access to this package is for configuring SPB-BVLAN Service, Site, SAPs, MeshSDPs and site stats.
pbbvlan.Site	SPB Site - Access to SPB Services.
pbbvlan.VlanPBBEdge	SPB Service - Access to SPB Services.
pim	PIM - PIM configuration for Service interfaces and routers, MDT Threshold, Policies, Neighbors, Groups, RPs, Multicast CAC Level and LAG Port Down events, and other PIM related objects.
pim.Site	PIM Site - Access to PIM Sites.
policing	Policing Policy - Policer Control.
policy	Policy - Parent package for all policies; Policy Audits.
policy.PolicyDefinition.method_setConfigurationModeToReleased	Policy Definition - method_setConfigurationModeToReleased - Ability set Configuration Mode to Released and distribute the global policy to the local definitions network-wide.
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	Policy Definition - method_setDistributionModeToLocalEditOnly - Ability set Configuration Mode to Local Edit Only for local policies and ignore changes to the global policy.
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	Policy Definition - method_setDistributionModeToSyncWithGlobal - Ability set Configuration Mode to Sync with Global and synchronize local policies with the most recent released global policy.
policy.PolicySyncGroupManager	Policy Sync Group Manager - Ability to configure and control policy sync group.
port.RestrictModeConfigModify	Port. Restrict Mode Config Modify - Ability to restrict Port Mode modification for Ports with dependencies.
portscheduler	Port Scheduler Policy - Port Scheduler and HSMDA Scheduler Policies.
ppp	PPP - Point-to-Point Protocol (PPP) configuration on a router.
pppoe	PPP Policy and Session - Point-to-Point Protocol over Ethernet over ATM (PPPoE/PPPoEoA/PPPoA) Policies and Sessions.
propertyrules	Property Rules - Range and Format Value Policies.
ptp	Precision Timing Protocol - Access to this package is for configuring Precision Timing Protocol.
qgroup	Queue Group Policy - Queue Group Policies.
qosprofile	Multilink QoS Profile - Multilink PPP QoS Profiles and Multilink Frame Relay QoS Profiles.
radioequipment	Radio Equipment - Radio Equipment configuration.
radiusaccounting	Radius Accounting - Radius Accounting Policy.
ranlicense	NE License Management - Ability to manage NE licenses.
ranradiom	eNodeB Router Admin: radio measurement - eNodeB Router administration: radio measurement.
rca	RCA - Root Cause Analysis (RCA) for verification applications (OSPF Area,ISIS Area,BGP AS,...).
rca.RcaManager.method_fixProblem	Rca Manager - method_fixProblem - Ability to fix a problem on an object.

(16 of 25)

Package.Class.Method/Property	Description
rca.RcaManager.method_preFixProblem	Rca Manager - method_preFixProblem - Ability to determine if a problem can be fixed, and the fix impact.
resiliency	HSDPA Resiliency - HSDPA Resiliency for services.
resources	SAM Resources - SAM Resource Pools as configured in the nms-server.xml file.
ressubscr	Residential Subscriber - All Residential Subscriber configuation including Connectivity Verifications (SHCV), SAPs, Packages, Hosts, QoS, and other related objects.
ressubscr.BgpPeeringPolicy	BGP Peering Policy - Access to BGP Peering Policies.
ressubscr.HostTrackingPolicy	Host Tracking Policy - Access to Host Tracking Policies.
ressubscr.IgmpPolicy	IGMP Policy - Access to IGMP Policies.
ressubscr.MldPolicy	MLD Policy - Access to MLD Policies.
ressubscr.ResidentialSubscriberManager.property_hostTrkSubscrRtrvTimeOut	Residential Subscriber Manager - property_hostTrkSubscrRtrvTimeOut - Service preferences can only be modified by a user with an administrator role.
ressubscr.ResidentialSubscriberManager.property_resSubscrInstRtrvMax	Residential Subscriber Manager - property_resSubscrInstRtrvMax - Service preferences can only be modified by a user with an administrator role.
ressubscr.ResidentialSubscriberManager.property_retrieveManagedRoutes	Residential Subscriber Manager - property_retrieveManagedRoutes - Service preferences can only be modified by a user with an administrator role.
ressubscr.ResidentialSubscriberManager.property_subscriberHostRtrvTimeOut	Residential Subscriber Manager - property_subscriberHostRtrvTimeOut - Service preferences can only be modified by a user with an administrator role.
ressubscr.SubMcastCacPolicy	Subscriber Multicast CAC Policy - Access to Subscriber Multicast CAC Policies.
rip	Routing Management: RIP - Routing Information Protocol (RIP) configuration for Service interfaces and routers, Authentication Key, Groups, Export and Import Policies.
rip.Site	RIP Site - Access to RIP Sites.
rmd	Remote Managed Device - Remote Managed Device Management.
rmon	Remote Network Monitoring - Remote Network Monitoring Alarm and Event Policies.
rollback	Rollback - All scheduled tasks; Cron Actions, OSS Commands, CLI Scripts and Schedules.
rp	Routing Policy - Policy Statements, Prefix Lists, Communities, Damping, and AS Paths.
rsvp	Routing Management: RSVP - RSVP configuration for a rtr.VirtualRouter, Authentication Keys, and Neighbors.
rtr	Routing Management: General - General rtr.VirtualRouter configurations including Neighbor Discovery, DHCP Relays, Interfaces, Peers, Address Ranges and ARP, Routes and Router Advertisement.
rules	Rules - Rule Repository and Sets of rules that may get invoked when a rule engine is fired.
sas	Assurance - Parent package for all tests; Service Test Manager.

(17 of 25)

Package.Class.Method/Property	**Description**
sas.TestManager.property_sasNumberOfHours	Service Test Manager - property_sasNumberOfHours - These preferences can only be modified by a user with an administrator role.
sas.TestManager.property_sasRetention	Service Test Manager - property_sasRetention - LogToFile preferences can only be modified by a user with an administrator role.
sas.TestManager.property_sasRollover	Service Test Manager - property_sasRollover - LogToFile preferences can only be modified by a user with an administrator role.
sasqos	7210 and 1830 QoS - QoS Policies for 7210 and 1830 nodes.
sasqos.QosPool	QoS Pool - Access to QoS Pools for 7210 nodes.
schedule	Schedule - All scheduled tasks; Cron Actions, OSS Commands, CLI Scripts and Schedules.
script	Scripting - Script Management and execution of Service and Tunnel Template, OSS, and CLI scripts.
script.AbstractScript.method_configureTarget	Script - method_configureTarget - Ability to configure targets and instances.
script.AbstractScript.method_configureTargets	Script - method_configureTargets - Ability to configure targets and instances.
script.Bundle	Script Bundle - Ability to configure script bundles.
script.ControlScript	Control Script - Ability to configure control scripts.
script.ControlScriptVersion	Control Script Version - Ability to configure Control script versions.
script.HandlerBinding	Handler Script Binding - Ability to configure associations between scripts and control scripts.
script.InvokerBinding	Invoker Script Binding - Ability to configure associations between scripts and control scripts.
script.LargeTextTargetParameter	Large Text Target Parameter - Ability to configure target/instance large text parameters.
script.Result	Result - Ability to create script results.
script.Script	CLI Script - Ability to configure CLI scripts.
script.Script.method_createTargetScript	CLI Script - method_createTargetScript - Ability to configure targets.
script.Script.method_createTargetScripts	CLI Script - method_createTargetScripts - Ability to configure targets.
script.ScriptManager	Script Manager - Ability to configure and control scripts and script operations.
script.ScriptManager.method_configure	Script Manager - method_configure - Ability to configure scripts.
script.ScriptManager.method_copyContents	Script Manager - method_copyContents - Ability to copy scripts.
script.ScriptManager.method_exportBundle	Script Manager - method_exportBundle - Ability to export bundle.
script.ScriptManager.method_importBundle	Script Manager - method_importBundle - Ability to import bundle.
script.ScriptManager.method_importBundleSimulation	Script Manager - method_importBundleSimulation - Ability to import bundle.
script.ScriptScheduledTask	Script Scheduled Task - Ability to schedule a script.
script.TargetParameter	Target Parameter - Ability to configure target/instance parameters.

(18 of 25)

Package.Class.Method/Property	Description
script.TargetParameterItem	Target Parameter Item - Ability to configure target/instance parameter items.
script.TargetParameterList	Target Parameter List - Ability to configure target/instance parameter lists.
script.TargetScript	Target Script - Ability to configure targets and instances.
script.TemplateBinding	Template Binding - Ability to configure associations between templates.
script.Version	Version - Ability to configure CLI script versions.
script.XmlApiConfigTemplate	Template - Ability to configure XML API templates.
script.XmlApiConfigTemplate.method_execute	Template - method_execute - Ability to create an object from a template.
script.XmlApiConfigTemplate.method_executeMulti	Template - method_executeMulti - Ability to create an object from a template.
script.XmlApiConfigTemplate.method_executeScript	Template - method_executeScript - Ability to create an object from a template.
script.XmlApiConfigTemplate.method_serviceTemplateExecute	Template - method_serviceTemplateExecute - Ability to execute a service template.
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	Template - method_tunnelTemplateExecute - Ability to execute a tunnel template.
script.XmlApiScript	XMLAPI Script - Ability to configure XML API scripts.
script.XmlApiVersion	XMLAPI Version - Ability to configure XML API script versions.
security	Security - SAM User security including Sessions, TCP KeyChains, and SSH2 Known Host Keys.
security.CpamLicense	CPAM License - Read-only view of the 5650 CPAM License.
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	CPAM License - method_clearRouterLimitExceedDueToMultiAdditions - Ability to clear the isRouterLimitExceedDueToMultiAdditions flag on the license.
security.CpamLicenseScenario	CPAM License Scenario - Read-only view of the 5650 CPAM Imapct Analysis Application License.
security.MediationPolicy	Mediation Policy - Access to Mediation Policies. Used in conjunction with snmp.PollerManager.
security.MessagingConnection	Messaging Connection - Ability to view messaging connections.
security.RoleBasedAccess	Security. Role Based Access - Ability to restrict online object creation and deletion to a specific role. Currently applies to 9412 node.
security.ScopeOfCommandProfile	Profile - Access to Scope of Command Profile configuration.
security.ScopeOfCommandRole	Role - Access to Scope of Command Role configuration.
security.Span	Span - Access to Span configuration. Used in conjunction with security.SpanObjectBinding.
security.SpanObjectBinding	Span Objects - Access to Span object configuration. Used in conjunction with security.Span.
security.SpanOfControlProfile	Profile - Access to Span of Control Profile configuration.
security.User	User - Access to User object configuration and password changes.
security.UserGroup	User Group - Access to UserGroup configuration.

(19 of 25)

Package.Class.Method/Property	**Description**
securitypolicy	Security Policy - All Security configurations including security policy,profile,zone,NAT.
selfconfig	Self Config - Ability to configure self config objects.
server	SAM Server - SAM Servers (JMS, Main, Auxilary Server, Auxiliary Database) as configured in the nms-server.xml file.
service	Service Management - Parent package for all services; Composite Services and Connectors and Access Policy Queue Override Policies.
service.AarpInterface	AARP Interface - Access to AARP Interface configuration between AARP.
service.CpePing	CPE Ping - Access to CPE Ping tests, CPE Ping test definitions, and CPE Ping deployed tests.
service.GneAccessInterface	GNE Service Interface - Access to GNE Service Interfaces.
service.GneSite	GNE Site - Access to GNE Sites.
service.MacPing	MAC Ping - Access to MAC Ping tests, MAC Ping test definitions, and MAC Ping deployed tests.
service.MacPopulate	MAC Populate - Access to MAC Populate tests, MAC Populate test definitions, and MAC Populate deployed tests.
service.MacPurge	MAC Purge - Access to MAC Purge tests, MAC Purge test definitions, and MAC Purge deployed tests.
service.MacTrace	MAC Trace - Access to MAC Trace tests, MAC Trace test definitions, and MAC Trace deployed tests.
service.RedundantInterface	Redundant Interface - Access to Redundant Interface configuration between SRRP instances.
service.Service.method_create	Service - method_create - Ability to create a service via the SAM Client GUI.
service.Service.method_highPriorityServiceDelete	Service - method_highPriorityServiceDelete - Ability to delete high priority Service.
service.Service.property_svcPriority	Service - property_svcPriority - Service priority can only be modified by a user with an administrator role.
service.ServiceManager.property_alarmAggregationCompositeService	Service Manager - property_alarmAggregationCompositeService - Service preferences can only be modified by a user with an administrator role.
service.ServiceManager.property_alarmAggregationSdp	Service Manager - property_alarmAggregationSdp - Service preferences can only be modified by a user with an administrator role.
service.ServiceManager.property_autoDiscoverCompositeSvc	Service Manager - property_autoDiscoverCompositeSvc - Service preferences can only be modified by a user with an administrator role.
service.ServiceManager.property_enableCac	Service Manager - property_enableCac - Service preferences can only be modified by a user with an administrator role.
service.ServiceManager.property_maxNumberOfMoveSites	Service Manager - property_maxNumberOfMoveSites - Service preferences can only be modified by a user with an administrator role.
service.ServiceManager.property_multiSegmentTunnelSelection	Service Manager - property_multiSegmentTunnelSelection - Service preferences can only be modified by a user with an administrator role.

(20 of 25)

Package.Class.Method/Property	Description
service.ServiceManager.property_propagateServiceNameToSites	Service Manager - property_propagateServiceNameToSites - Service preferences can only be modified by a user with an administrator role.
service.ServiceManager.property_removeEmptyService	Service Manager - property_removeEmptyService - Service preferences can only be modified by a user with an administrator role.
service.ServiceManager.property_supVprnSnmpCommunityStringMsg	Service Manager - property_supVprnSnmpCommunityStringMsg - Service preferences can only be modified by a user with an administrator role.
service.ServiceManager.property_svcPriority	Service Manager - property_svcPriority - Service priority can only be modified by a user with an administrator role.
service.ServiceMemberAuditPolicyEntry	Service Membership Audit Policy Entry - Access to Service Member Audit Policy Entry to configure service membership RCA audit behavior.
service.SitePing	Service Site Ping - Access to Service Site Ping tests, Service Site Ping test definitions, and Service Site Ping deployed tests.
service.TemplateService.method_constructServiceTemplate	Service Template - method_constructServiceTemplate - Ability to construct a Template from a Service.
service.TemplateService.method_constructTemplatedService	Service Template - method_constructTemplatedService - Ability to construct a Service from a Template.
service.Y1564TestHeadBiDirectional	Y1564 Bi-Directional Test - Access to Y1564 Bi-Directional tests, Y1564 Bi-Directional test definitions, and Y1564 Bi-Directional deployed tests.
shg	Split Horizon Group - Split Horizon Groups for VPLS services.
simulator	CPAM: Simulator - Parent package for all CPAM simulated objects; Scenarios, Sessions, Change and Action events.
simulator.SimSession	Session - Access to simulation sessions for 5650 CPAM Impact Analysis.
sitesec	NE Security - All Network Element security configuration including NE System Security, RADIUS, TACACS+ and AOS Authentication, Site Management Access and CPM Filters, DoS Protection, Password Policy, Users and Profiles.
sitesec.LocalUser	NE User - Access to NE Site User configuration.
sitesec.UserProfile	Site User Profile - Access to NE Site User Profile configuration.
sitesec.UserPublicKey	RSA Key - Public keys(SSHv2) configuration for the system users.
slaprofile	SLA Profile - SLA Profiles for QoS Policies.
slope	Slope Policy - WRED Slope, HSMDA WRED Slope, HSMDA Pool, and Named Buffer Pool Policies.
slope.QosPool	QoS Pool - Access to QoS Pools for 7450, 7750, and 7710 nodes.
snmp	SNMP - SNMP Poller Policies, Event Notification Policies, Statistics Poller Policies.
snmp.EventNotificationPolicy	Event Notification Policy - Access to Event Notification Policies.
snmp.PollerManager	Mediation - Access to Mediation Policies. Used in conjunction with security.MediationPolicy.
snmp.PollerManager.method_resync	Mediation - method_resync - Ability to resync a Network Element. Requires 'update' access on netw.NetworkElement.
sonet	SONET Sync - SONET Synchronization for Shelf and Processor Cards.

(21 of 25)

Package.Class.Method/Property	Description
sonetequipment	SONET Equipment - SONET Equipment configuration.
spanrules	Span Rules - Span Rules for service creation.
spb	SPB - Access to this package is for configuring SPB site and site stats.
spb.AccessInterface	Access Interface - Access to SPB Interface of VPLS B-L2 Access Interfaces on a BVPLS Service.
spb.NetworkInterface	Network Interface - Access to SPB Network Interfaces.
spb.SpokeSdpBindingInterface	Spoke SDP Binding Interface - Access to SPB Interface of VPLS Spoke-SDP on a BVPLS Service.
squeue	Shared Queue Policy - Shared Queue Policies.
srmrmtauth	SAM Remote Authentication - Remote Authentication for SAM configuration of RADIUS and TACACS+ authentication servers.
srpythonmgmt	Python Management - Python Management.
srrp	SRRP - Subscriber Routed Redundancy Protocol (SRRP) configuration for IES and VPRN services.
statistics	SAM Performance Statistics - SAM Performance Statistics (Memory, Alarm Rate, Snmp Traps, and Node Resyncs).
statsplot	Statistics Plotter - Statistics Plotter.
subscr	Subscriber Management - Customers configuration.
subscr.Site	Subscriber Site - Access to Subscriber Sites.
subscrauth	Subscriber Authentication - Subscriber Authentication Policy using RADIUS for DHCP sessions.
subscrexpmap	Subscriber Explicit Map - Subscriber Explict Map Entry.
subscrident	Subscriber Identification - Subscriber Identification Policy.
subscrprofile	Subscriber Profile - Subscriber Profile, SLA Entries, Access Policy Queue Overrides and Scheduler Policy Entry Overrides.
sup	Supervision - SAM Supervision (Dashboard).
svq	Aggregation Scheduler - Service and Subscriber Aggregation Scheduler, Ingress and Egress Aggregation Scheduler Overrides.
svr	Service Routing - All contained objects are listed. Package access is not currently used.
svt	Service Tunnel Management - All Service Tunnel configruations including Clouds, Service Distribution Path (SDP) Bindings and Pseudo Wires.
svt.BvlanTunnel	SPB BVLAN Tunnel (SDP) - Access to vlan Tunnel (SDP) configuration.
svt.L2TPv3Tunnel	L2TPv3 Tunnel (SDP) - Access to l2tpV3 Tunnel (SDP) configuration.
svt.MeshSdpBinding	Mesh SDP Binding - Access to Mesh SDP Binding configuration.
svt.MirrorSdpBinding	Mirror SDP Binding - Access to Mirror SDP Binding configuration.
svt.MtuPing	MTU Ping - Access to MTU Ping tests, MTU Ping test definitions, and MTU Ping deployed tests.
svt.SpokeSdpBinding	Spoke SDP Binding - Access to Spoke SDP Binding configuration.
svt.Tunnel	Tunnel - Access to Tunnel (or SDP object) configuration.

(22 of 25)

Package.Class.Method/Property	Description
svt.TunnelPing	Tunnel Ping - Access to Tunnel Ping tests, Tunnel Ping test definitions, and Tunnel Ping deployed tests.
svt.VccvPing	VCCV Ping - Access to VCCV Ping tests, VCCV Ping test definitions, and VCCV Ping deployed tests.
svt.VccvTrace	VCCV Trace - Access to VCCV Trace tests, VCCV Trace test definitions, and VCCV Trace deployed tests.
svt.VlanPBBEdgeMeshSdpBinding	PBB VLAN Mesh SDP Binding - Access to PBB VLAN Mesh SDP Binding configuration.
sw	Router Admin: Software - Router administration: Backup Files, Card Software, Upgrade schedules, and Accounting Statistics Retrieval.
sw.BackupRestoreManager.method_backup	Backup/Restore Status - method_backup - Ability to perform a Network Element backup.
sw.BackupRestoreManager.method_restore	Backup/Restore Status - method_restore - Ability to perform a Network Element restore.
swran	eNodeB Router Admin: Software - eNodeB Router administration: Upgrade schedules.
sysact	User Activity - User Activity.
taskmgmt	Task Management - Monitor the tasks being executed in the server.
tca	TCA Policy - Parent package for all TCA classes.
tca.TCAManager.property_maxTCAAlarmLimit	TCAManager - property_maxTCAAlarmLimit - TCA preferences can only be modified by a user with an administrator role.
tca.TCAManager.property_maxTCAAlarmResetInterval	TCAManager - property_maxTCAAlarmResetInterval - TCA preferences can only be modified by a user with an administrator role.
tdmequipment	TDM Equipment - TDM Equipment configuration.
template	Service Template - Deprecated 6.0: use XML API based configuration templates (see class script.XmlApiConfigTemplate).
tod	TOD - Time Of Day Range Policy.
todsuite	TOD Suite - Time Of Day Suite Policy for Egress and Ingress Entries.
topology	CPAM: Topology - All CPAM topology configurations including BGP, IS-IS, OSPF, CPAA, Links, Routers, Areas, Subnets, Checkpoints, and Route Alarms.
topologysim	CPAM: Simulated Topology - CPAM simulated IGP topology including Links, Routers, Areas, Subnets, and IP Paths.
trapmapper	Trap to Alarm Mapper - Trap to Alarm Mapper.
tunnelmgmt	Tunnel Management - All Tunnel related objects including Hubs, Spokes, Meshes, Chains, Rings, Two Neighbor, Class Forwarding and Rule-based Groups.
udprelay	UDP Relay - UDP Relay configuration and services for layer2.Bridge, DHCP Snooping for VLANs and Ports.
udptunnel	UDP Tunnel - Access to UDP Tunnel.
user	User Preference - SAM Client GUI preferences for Info Tables.
vlan	VLAN - Access to this package is for configuring TLS, MVR, Super VLAN, Customer VLAN, SAP and MSAP, Network Interfaces (Uplink Ports) and VLAN configuration for a MST Instance.

(23 of 25)

Package.Class.Method/Property	**Description**
vlan.EthernetService	VLAN Ethernet Service - Access to VLAN Ethernet Services.
vlan.L2AccessInterface	VLAN Access Interface - Access to VLAN Access Interfaces.
vlan.Site	VLAN Site - Access to VLAN Sites.
vlan.Vlan	VLAN Service - Access to Virtual LAN (VLAN) Service objects themselves.
vll	VLL - All contained objects are listed. Package access is not currently used.
vll.Endpoint	Endpoint - Access to VLL Endpoints.
vll.L2AccessInterface	L2 Access Interface - Access to VLL L2 Access Interfaces (except Ipipe).
vpls	VPLS - Access to this package is for configuring MLD Snooping, PIM Snooping, DHCP Relay, Multicast CAC Level and LAG Port Down events, and discovered VLAN Elements.
vpls.BL2AccessInterface	VPLS B-L2 Access Interface - Access to VPLS B-L2 Access Interfaces on a VPLS Service.
vpls.BSite	VPLS B-Site - Access to VPLS B-Sites on a VPLS Service.
vpls.Endpoint	VPLS Endpoint - Access to VPLS Endpoints on a VPLS Service.
vpls.EvpnSite	VPLS eVPN-Site - Access to VPLS eVPN-Sites on a VPLS Service.
vpls.IL2AccessInterface	VPLS I-L2 Access Interface - Access to VPLS I-L2 Access Interfaces on a VPLS Service.
vpls.ISite	VPLS I-Site - Access to VPLS I-Sites on a VPLS Service.
vpls.L2AccessInterface	VPLS L2 Access Interface - Access to VPLS L2 Access Interfaces (except I and B) on a VPLS Service.
vpls.L2ManagementInterface	VPLS L2 Management Interface - Access to VPLS L2 Management Interfaces on a VPLS Service.
vpls.Site	VPLS Site - Access to VPLS Sites (except I and B) on a VPLS Service.
vpls.Vpls	VPLS Service - Access to Virtual Private LAN Service (VPLS) Service objects themselves.
vprn	VPRN - Access to this package is for configuring VPRN Router Instance Sites, SNMP Community, IPsec Interfaces, Group Interfaces, SAPs, MSAPs, IGMP Host Tracking on Sites and SAPs, and FR Interface Specifics for VPRN specific SAPs.
vprn.AaInterface	VPRN AA Interface - Access to VPRN AA Interfaces.
vprn.DVRSSite	VPRN dVRS Site - Access to dVRS VPRN Sites on a VPRN service.
vprn.IPMirrorInterface	IP Mirror Interface - Access to VPRN IP Mirror Interfaces.
vprn.L3AccessInterface	VPRN L3 Access Interface - Access to VPRN L3 Access Interfaces.
vprn.Site	VPRN Site - Access to VPRN Sites.
vprn.SubscriberInterface	VPRN Subscriber Interface - Access to VPRN Subscriber Interfaces.
vprn.Vprn	VPRN Service - Access to Virtual Private Routed Network (VPRN) Service objects themselves.
vprn.VprnPing	VPRN Ping - Access to VPRN Ping tests, VPRN Ping test definitions, and VPRN Ping deployed tests.
vprn.VprnTrace	VPRN Trace - Access to VPRN Trace tests, VPRN Trace test definitions, and VPRN Trace deployed tests.

(24 of 25)

Package.Class.Method/Property	Description
vrrp	VRRP - Virtual Router Redundancy Protocol (VRRP) configuration on rtr.NetworkInterface, IES and VPRN access interfaces, Authentication Keys, Priority Control Policies and Events.
vs	Scheduler Policy - Scheduler Policies.
webclient	WebClient - Access to the WebClient.
webclient.WebClientManager	Web Client Manager - Ability to control Web Clients.
wlangw	WLAN Gateway - WiFi Offload.
workspace	Workspace - Ability to view workspaces, and Create/Edit/Delete private workspaces.
workspace.WorkspaceManager.method_publicControl	Workspace Manager - method_publicControl - Ability to create/edit/delete public workspaces.
wpp	WPP - Web Portal Protocol.
wpp.Site	WPP Site - Access to WPP Sites.

(25 of 25)

A.3 Permissions of predefined scope of command roles

This section describes the permissions of each default scope of command role. Each permission can have the following access levels to an object package, class, method or property:

- Read-only—provides read access to an object class without the ability to create or delete objects.
- Read/write—provides full access to an object class that includes read, create, update/execute, and delete access.
- Read/update/execute—provides read and update/execute access to an object package or property, but does not provide delete access.
- Update/execute—provides update/execute access on class methods, and is typically combined with read access on the parent object package.
- No access.

Note — This appendix does not list permissions with read-only access. Permissions that are not listed for a predefined scope of command role have an access level of read-only.

Table A-5 lists each of the 5620 SAM default scope of command roles and provides a link to a table for each of the roles where the access permissions are defined.

Table A-5 Summary of 5620 SAM scope of command roles

Role	Link
Base Read-only	Table A-6
Administrator	Table A-7

(1 of 3)

Role	Link
User Management	Table A-8
Network Element Equipment Manager	Table A-9
Service Management	Table A-10
Subscriber Management	Table A-11
QoS/ACL Policy Management	Table A-12
Policy Management (except QoS/ACL)	Table A-13
Routing Management	Table A-14
Tunnel Management	Table A-15
SAM Management and Operations	Table A-16
Network Element Software Management	Table A-17
Fault Management	Table A-18
Service Test Management	Table A-19
Script Management	Table A-20
Script Execution	Table A-21
Mirror Service Management	Table A-22
OSS Management	Table A-23
Telnet/SSH Management	Table A-24
CPAM Management	Table A-25
CPAM OSS PCA	Table A-26
CPAM Topology Simulator	Table A-27
Root Cause Analysis (RCA) Object Verification	Table A-28
Lawful Intercept Management	Table A-29
Template Script Management	Table A-30
Service Template Script Execution	Table A-31
Tunnel Template Script Execution	Table A-32
Application Assurance (AA) Management	Table A-33
Format and Range Policy Management	Table A-34
Work Order Activation	Table A-35
Configuration Snapshot Export	Table A-36
Create and Delete Access	Table A-37
Configuration Management which causes node reset	Table A-38
EPC Operator	Table A-39
eNodeB NEM Operator	Table A-40
Statistics Profile Plotter Management	Table A-41
Admin Neto Launch	Table A-42
Viewer Neto Launch	Table A-43
Default Neto Launch	Table A-44

(2 of 3)

Role	Link
Ageout Constraint Policy Management	Table A-45

(3 of 3)

Table A-6 Base Read-only

Package.Class.Method/Property	Access
aclfilterli	No access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
calltrace.WebDAVSharedData	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.AuxiliaryDatabase.method_reinstantiationDatabase	No access
db.AuxiliaryDatabase.method_snapshotDatabase	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_snapshotAllDatabases	No access
db.DatabaseManager.method_switchover	No access
equipment.Shelf.method_rebootUpgrade	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
lte.ENBEquipment.method_launchNEM	No access
lte.LTEEquipment.method_launchQoSAnalyzer	No access
lteli.DFPeer	No access
lteli.DFPeerCardGroup	No access
lteli.InterceptionTarget	No access
lteli.LILteCfg	No access

(1 of 3)

Package.Class.Method/Property	**Access**
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
ltepolicyoptions	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
netw.AdvertisedNode	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_NetoAdminProfileBasedLaunch	No access
netw.NetworkElement.method_NetoViewerProfileBasedLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access

(2 of 3)

Package.Class.Method/Property	Access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
sysact	No access
user	Read/write
vprn.IPMirrorInterface	No access
webclient	No access
webclient.WebClientManager	Read/write
workspace	Read/write
workspace.WorkspaceManager.method_publicControl	No access

(3 of 3)

Table A-7 Administrator

Package.Class.Method/Property	Access
aaa	Read/write
aaa.RadiusProxyInterface	Read/write
aaa.RadiusProxyServer	Read/write
aaa.RadiusServer	Read/write
aapolicy	Read/write
accessuplink	Read/write
accounting	Read/write

(1 of 18)

Package.Class.Method/Property	Access
aclfilter	Read/write
aclfilterli	No access
activation	Read/write
activation.Session	Read/write
activation.Snapshot	Read/write
activation.SnapshotEntity	Read/write
activation.WebDAVSharedData	Read/write
activation.WorkOrder	Read/write
aengr	Read/write
ageoutcstr	Read/write
aingr	Read/write
ancp	Read/write
ancp.AncpLoopback	Read/write
antispoof	Read/write
aosqos	Read/write
aosredundancy	Read/write
aossas	Read/write
aossas.CPETestGroupHead	Read/write
aossas.CPETestHead	Read/write
apipe	Read/write
apipe.Apipe	Read/write
apipe.Site	Read/write
aps	Read/write
arp	Read/write
atm	Read/write
atm.AtmPing	Read/write
atmpolicy	Read/write
audit	Read/write
autoconfig	Read/write
autoconfig.AutoConfigScriptManager.method_configure	Update/execute
autoconfig.AutoConfigScriptManager.method_copyContents	Update/execute
bfd	Read/write
bgp	Read/write
bgp.Site	Read/write
bulk	Read/write
bulk.BulkChange	Read/write
bulk.BulkManager.method_execute	Update/execute

(2 of 18)

Package.Class.Method/Property	**Access**
bulk.BulkManager.method_generateBatches	Update/execute
bundle	Read/write
cac	Read/write
ccag	Read/write
cflowd	Read/write
cflowd.NeCflowd	Read/write
cflowd.NeCollector	Read/write
clear	Read/write
cli	Read/write
cli.SSH	Read/write
cli.Telnet	Read/write
connprof	Read/write
cpipe	Read/write
cpipe.Cpipe	Read/write
cpipe.Site	Read/write
crdtctrl	Read/write
customproperties	Read/write
db	Read/write
db.AuxiliaryDatabase.method_reinstantiationDatabase	Update/execute
db.AuxiliaryDatabase.method_snapshotDatabase	Update/execute
db.DatabaseManager.method_backup	Update/execute
db.DatabaseManager.method_reinstantiateStandby	Update/execute
db.DatabaseManager.method_snapshotAllDatabases	Update/execute
db.DatabaseManager.method_switchover	Update/execute
dctr	Read/write
dhcp	Read/write
diameter	Read/write
dns	Read/write
dynsvc	Read/write
epipe	Read/write
epipe.Epipe	Read/write
epipe.PbbMacName	Read/write
epipe.Site	Read/write
equipment	Read/write
equipment.PortPolicy	Read/write
equipment.Shelf.method_rebootUpgrade	Update/execute
ethernetequipment	Read/write

(3 of 18)

Package.Class.Method/Property	Access
ethernetoam	Read/write
ethernetoam.CcTest	Read/write
ethernetoam.CcmTest	Read/write
ethernetoam.CfmDmmBin	Read/write
ethernetoam.CfmDmmSession	Read/write
ethernetoam.CfmEthTest	Read/write
ethernetoam.CfmLMTest	Read/write
ethernetoam.CfmLinkTrace	Read/write
ethernetoam.CfmLoopback	Read/write
ethernetoam.CfmOneWayDelayTest	Read/write
ethernetoam.CfmOneWaySlm	Read/write
ethernetoam.CfmSingleEndedLossTest	Read/write
ethernetoam.CfmSlmSession	Read/write
ethernetoam.CfmTwoWayDelayTest	Read/write
ethernetoam.CfmTwoWaySlm	Read/write
ethernetoam.EthSession	Read/write
ethernetservice	Read/write
ethernettunnel	Read/write
ethring	Read/write
fabricqos	Read/write
file	Read/write
filter	Read/write
filterprefixlist	Read/write
firewall	Read/write
fm	Read/write
fm.AlarmHistoryDatabase.method_purge	Update/execute
fm.FaultManager	Read/write
fm.FaultManager.method_editNote	Update/execute
fm.GlobalPolicy	Read/write
fm.SpecificPolicy	Read/write
fpipe	Read/write
fpipe.Fpipe	Read/write
fpipe.Site	Read/write
fr	Read/write
generic	Read/write
generic.GenericObject.method_collectData	Update/execute
genericlog	Read/write

(4 of 18)

Package.Class.Method/Property	**Access**
genericne	Read/write
gsmp	Read/write
hip.EMServer	Read/write
hip.EMSystem	Read/write
hpipe	No access
hpipe.Hpipe	Read/write
hpipe.Site	Read/write
icmp.DnsPing	Read/write
icmp.IcmpPing	Read/write
icmp.IcmpTrace	Read/write
ies	Read/write
ies.AaInterface	Read/write
ies.Ies	Read/write
ies.L3AccessInterface	Read/write
ies.Site	Read/write
ies.SubscriberInterface	Read/write
igh	Read/write
igmp	Read/write
igmp.Site	Read/write
impact.FullReset	Read/write
impact.PartialReset	Read/write
ipfix	Read/write
ipipe	Read/write
ipipe.Ipipe	Read/write
ipipe.L2AccessInterface	Read/write
ipipe.Site	Read/write
ipsec	Read/write
isa	Read/write
isa.MgGroupMember	Read/write
isa.MgIsaGroup	Read/write
isis	Read/write
l2fib	Read/write
l2fwd	Read/write
l2tp	Read/write
l3fwd	Read/write
lag	Read/write
layer2	Read/write

(5 of 18)

Package.Class.Method/Property	**Access**
ldp	Read/write
lldp	Read/write
localuserdb	Read/write
log	Read/write
log.LogToFileManager.property_jmsRetries	Read/update/execute
log.LogToFileManager.property_retention	Read/update/execute
log.LogToFileManager.property_rollover	Read/update/execute
lps	Read/write
lte	Read/write
lte.ApnPolicyRuleBase	Read/write
lte.CallTraceDirectory	Read/write
lte.DccaProfile	Read/write
lte.DiameterPeerListEntry	Read/write
lte.DiameterPeerProfile	Read/write
lte.DiameterProfile	Read/write
lte.DiscoveryLog	Read/write
lte.DupRadiusAccServerGroup	Read/write
lte.ENBEquipment.method_launchNEM	Update/execute
lte.EPSPathDiscoveredLinkComponent	Read/write
lte.EPSPathDiscoveryHint	Read/write
lte.EPSPathDiscoveryProfile	Read/write
lte.EPSPathInterfaceComponent	Read/write
lte.EPSPathLinkComponent	Read/write
lte.EPSPathSapComponent	Read/write
lte.EPSPathSegment	Read/write
lte.EPSPathServiceComponent	Read/write
lte.EPSPathSiteComponent	Read/write
lte.GtpPrimaryServerListEntry	Read/write
lte.GtpPrimeServerGroupProfile	Read/write
lte.GtpProfile	Read/write
lte.IpPool	Read/write
lte.IpPoolBinding	Read/write
lte.IpPoolEntry	Read/write
lte.LTEEquipment.method_launchQoSAnalyzer	Update/execute
lte.MobileNodeRegion	Read/write
lte.PDNGateway	Read/write
lte.PdnApn	Read/write

(6 of 18)

Package.Class.Method/Property	**Access**
lte.PdnGxReferencePoint	Read/write
lte.PdnRfReferencePoint	Read/write
lte.PdnS5ReferencePoint	Read/write
lte.PdnS8ReferencePoint	Read/write
lte.PdnSignalling	Read/write
lte.PgwChargingProfile	Read/write
lte.PlmnListPolicy	Read/write
lte.PlmnListPolicyGroup	Read/write
lte.QciPolicy	Read/write
lte.QciPolicyEntry	Read/write
lte.S11ReferencePoint	Read/write
lte.S1uReferencePoint	Read/write
lte.ServingGateway	Read/write
lte.SgwApn	Read/write
lte.SgwChargingProfile	Read/write
lte.SgwRfReferencePoint	Read/write
lte.SgwS5ReferencePoint	Read/write
lte.SgwS8ReferencePoint	Read/write
lte.SgwSignalling	Read/write
lte.SubscAndEquipmentTraces	Read/write
lte.TrustedPeerListEntry	Read/write
lte.TrustedPeerListEntryUnlisted	Read/write
lte.TrustedPeerListPolicy	Read/write
lteanr	Read/write
lteggsn	Read/write
lteggsn.CdrAvpOptionProfile	Read/write
lteggsn.DccaRatingGroup	Read/write
lteggsn.GnReferencePoint	Read/write
lteggsn.GpReferencePoint	Read/write
lteggsn.GyAvpOptionProfile	Read/write
lteggsn.PdnGyReferencePoint	Read/write
lteggsn.PgwGaReferencePoint	Read/write
lteggsn.SgwGaReferencePoint	Read/write
ltegw	Read/write
ltegw.ApnListPolicy	Read/write
ltegw.ApnListPolicyGroup	Read/write
ltegw.DiameterPeerRedirHostEntry	Read/write

(7 of 18)

Package.Class.Method/Property	**Access**
ltegw.DiameterPeerSupportedHost	Read/write
ltegw.PcscfGroupProfile	Read/write
ltegw.PcscfPeerEntry	Read/write
ltegw.PcscfResolvedPeerIPEntry	Read/write
ltegw.SCTPProfile	Read/write
ltegw.UMTSQoSPolicy	Read/write
ltemme	Read/write
ltemme.MmeInstance.method_abortMmeLoadBalance	Update/execute
ltemme.MmeInstance.method_interMmeLoadBalance	Update/execute
ltemme.MmeInstance.method_intraMmeLoadBalance	Update/execute
ltemme.MmeInstance.method_lockMmeAggregateService	Update/execute
ltemme.MmeInstance.method_unlockMmeAggregateService	Update/execute
lteperf	Read/write
ltepmip	Read/write
ltepmip.Pmipv6Profile	Read/write
ltepmip.S2aReferencePoint	Read/write
ltepmip.S2bReferencePoint	Read/write
ltepmip.S6bAvpOptionProfile	Read/write
ltepmip.S6bReferencePoint	Read/write
ltepolicyoptions	No access
ltepolicyoptions.AsoOptions	Read/write
ltepolicyoptions.ChargingRuleUnit	Read/write
ltepolicyoptions.DhcpSGPeerEntry	Read/write
ltepolicyoptions.DhcpServerGroupProfile	Read/write
ltepolicyoptions.GxAvpOptionProfile	Read/write
ltepolicyoptions.PolRuleUnitFlwDescription	Read/write
ltepolicyoptions.PolicyRule	Read/write
ltepolicyoptions.PolicyRuleBase	Read/write
ltepolicyoptions.PolicyRuleBaseEntry	Read/write
ltepolicyoptions.PolicyRuleUnit	Read/write
ltepolicyoptions.ServiceClassIndicator	Read/write
ltepolicyoptions.TrafficRedirectProfile	Read/write
ltepolicyoptions.TrafficRedirectTarget	Read/write
ltepool	Read/write
ltepool.MmeInstanceBinding	Read/write
ltepool.TaBinding	Read/write
lteradius	Read/write

(8 of 18)

Package.Class.Method/Property	**Access**
lteradius.RadiusGroupProfile	Read/write
lteradius.RadiusPeerProfile	Read/write
lteradius.RadiusProfile	Read/write
ltes1mme	Read/write
ltesecurity	Read/write
lteservice	Read/write
ltesgsn	Read/write
ltesgsn.SgwS12ReferencePoint	Read/write
ltesgsn.SgwS4ReferencePoint	Read/write
ltethreshold	Read/write
lteuserstats	Read/write
lteuserstats.UserStatsQuery	Read/write
lteuserstats.UserStatsQueryOutputSnapshot	Read/write
lteuserstats.UserStatsUserPgw	Read/write
lteuserstats.UserStatsUserSgw	Read/write
mediation	Read/write
mirror	Read/write
mirror.Endpoint	Read/write
mirror.Mirror	Read/write
mirror.Site	Read/write
mld	Read/write
mmepolicy	No access
mmepolicy.MMEEmergencyNumListPolicy	Read/write
mmepolicy.MMEGTPProfile	Read/write
mmepolicy.MMESCTPProfile	Read/write
mmepolicy.WMMPfmJobEntry	Read/write
mmepolicy.WMMPfmJobMts	Read/write
mmepolicy.WMMPfmJobSched	Read/write
mmepolicy.WMMPfmMeasGroupName	Read/write
mmepolicy.WMMPfmMeasGroups	Read/write
monitor	Read/write
monpath	Read/write
mpls	Read/write
mpls.LdpTreeTrace	Read/write
mpls.LspPing	Read/write
mpls.LspTrace	Read/write
mpls.P2MPLspPing	Read/write

(9 of 18)

Package.Class.Method/Property	Access
mpls.P2MPLspTrace	Read/write
mplstp	Read/write
mpr	Read/write
mpr.Al2AccessInterface	Read/write
mpr.Apipe	Read/write
mpr.Asite	Read/write
mpr.Cpipe	Read/write
mpr.El2AccessInterface	Read/write
mpr.Epipe	Read/write
mpr.Esite	Read/write
mpr.L2AccessInterface	Read/write
mpr.Site	Read/write
msappolicy	Read/write
msdp	Read/write
multicast	Read/write
multicast.CustomerVlanTag	Read/write
multicast.MfibPing	Read/write
multicast.Mrinfo	Read/write
multicast.Mtrace	Read/write
multicastmgr	Read/write
multichassis	Read/write
mvpls	Read/write
mvpls.BL2AccessInterface	Read/write
mvpls.BSite	Read/write
mvpls.EvpnSite	Read/write
mvpls.IL2AccessInterface	Read/write
mvpls.ISite	Read/write
mvpls.L2AccessInterface	Read/write
mvpls.Mvpls	Read/write
mvpls.Site	Read/write
mvrp	Read/write
mwa	Read/write
nat	Read/write
nat.LsnSubSession	Read/write
nat.PcpServer	Read/write
nat.PcpServerInterface	Read/write
neaudit	Read/write

(10 of 18)

Package.Class.Method/Property	Access
nelicense	Read/write
netca	Read/write
netw	Read/write
netw.AdvertisedNode	Read/write
netw.NeLimitHolder	Read/write
netw.NetworkElement	Read/write
netw.NetworkElement.method_GUICrossLaunch	Update/execute
netw.NetworkElement.method_NetoAdminProfileBasedLaunch	Update/execute
netw.NetworkElement.method_NetoViewerProfileBasedLaunch	Update/execute
netw.NetworkElement.method_executeCli	Update/execute
netw.NetworkElement.method_executeMultiCli	Update/execute
netw.NetworkElement.property_elementManagerCmd	Read/update/execute
netw.NodeDiscoveryControl	Read/write
netw.Topology	Read/write
netw.Topology.method_move	Update/execute
netw.UplinkBofConfiguration	Read/write
netw.UplinkRouteConfiguration	Read/write
niegr	Read/write
nodelog	Read/write
nqueue	Read/write
ntp	Read/write
ntp.NTPBroadcast	Read/write
ntp.NTPMulticast	Read/write
olc	Read/write
olc.OLCSchedulerManager.property_autosetMaintenanceOLCStateOnAdminDown	Read/update/execute
olc.OLCSchedulerManager.property_createAlarmNotification	Read/update/execute
olc.OLCSchedulerManager.property_leadTimeForNotification	Read/update/execute
openflow	Read/write
optical	Read/write
optical.MultipointServicePath	Read/write
optical.MultipointTransportService	Read/write
optical.TransportService	Read/write
opticalacl	Read/write
opticalequipment	Read/write
opticsperf	Read/write
ospf	Read/write
ospf.Site	Read/write

(11 of 18)

Package.Class.Method/Property	**Access**
oss	No access
oth	Read/write
pae802_1x	Read/write
pbbvlan	Read/write
pbbvlan.Site	Read/write
pbbvlan.VlanPBBEdge	Read/write
pim	Read/write
pim.Site	Read/write
policing	Read/write
policy	Read/write
policy.PolicyDefinition.method_setConfigurationModeToReleased	Update/execute
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	Update/execute
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	Update/execute
policy.PolicySyncGroupManager	Read/write
portscheduler	Read/write
ppp	Read/write
pppoe	Read/write
propertyrules	Read/write
ptp	Read/write
qgroup	Read/write
qosprofile	Read/write
radioequipment	Read/write
radiusaccounting	Read/write
ranlicense	Read/write
ranradiom	Read/write
rca	Read/write
rca.RcaManager.method_fixProblem	Update/execute
rca.RcaManager.method_preFixProblem	Update/execute
resiliency	Read/write
resources	Read/write
ressubscr	Read/write
ressubscr.BgpPeeringPolicy	Read/write
ressubscr.HostTrackingPolicy	Read/write
ressubscr.IgmpPolicy	Read/write
ressubscr.MldPolicy	Read/write
ressubscr.ResidentialSubscriberManager.property_hostTrkSubscrRtrvTimeOut	Read/update/execute
ressubscr.ResidentialSubscriberManager.property_resSubscrInstRtrvMax	Read/update/execute

(12 of 18)

Package.Class.Method/Property	Access
ressubscr.ResidentialSubscriberManager.property_retrieveManagedRoutes	Read/update/execute
ressubscr.ResidentialSubscriberManager.property_subscriberHostRtrvTimeOut	Read/update/execute
ressubscr.SubMcastCacPolicy	Read/write
rip	Read/write
rip.Site	Read/write
rmd	Read/write
rmon	Read/write
rollback	Read/write
rp	Read/write
rsvp	Read/write
rtr	Read/write
rules	Read/write
sas	Read/write
sas.TestManager.property_sasNumberOfHours	Read/update/execute
sas.TestManager.property_sasRetention	Read/update/execute
sas.TestManager.property_sasRollover	Read/update/execute
sasqos	Read/write
sasqos.QosPool	Read/write
schedule	Read/write
script	Read/write
script.AbstractScript.method_configureTarget	Update/execute
script.AbstractScript.method_configureTargets	Update/execute
script.Bundle	Read/write
script.ControlScript	Read/write
script.ControlScriptVersion	Read/write
script.HandlerBinding	Read/write
script.InvokerBinding	Read/write
script.LargeTextTargetParameter	Read/write
script.Result	Read/write
script.Script	Read/write
script.Script.method_createTargetScript	Update/execute
script.Script.method_createTargetScripts	Update/execute
script.ScriptManager	Read/write
script.ScriptManager.method_configure	Update/execute
script.ScriptManager.method_copyContents	Update/execute
script.ScriptManager.method_exportBundle	Update/execute
script.ScriptManager.method_importBundle	Update/execute

(13 of 18)

Package.Class.Method/Property	Access
script.ScriptManager.method_importBundleSimulation	Update/execute
script.ScriptScheduledTask	Read/write
script.TargetParameter	Read/write
script.TargetParameterItem	Read/write
script.TargetParameterList	Read/write
script.TargetScript	Read/write
script.TemplateBinding	Read/write
script.Version	Read/write
script.XmlApiConfigTemplate	Read/write
script.XmlApiConfigTemplate.method_execute	Update/execute
script.XmlApiConfigTemplate.method_executeMulti	Update/execute
script.XmlApiConfigTemplate.method_executeScript	Update/execute
script.XmlApiConfigTemplate.method_serviceTemplateExecute	Update/execute
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	Update/execute
script.XmlApiScript	Read/write
script.XmlApiVersion	Read/write
security	Read/write
security.CpamLicense	Read/write
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	Update/execute
security.CpamLicenseScenario	Read/write
security.MediationPolicy	Read/write
security.MessagingConnection	Read/write
security.RoleBasedAccess	Read/write
security.ScopeOfCommandProfile	Read/write
security.ScopeOfCommandRole	Read/write
security.Span	Read/write
security.SpanObjectBinding	Read/write
security.SpanOfControlProfile	Read/write
security.User	Read/write
security.UserGroup	Read/write
securitypolicy	Read/write
selfconfig	Read/write
server	Read/write
service	Read/write
service.AarpInterface	Read/write
service.CpePing	Read/write
service.GneAccessInterface	Read/write

(14 of 18)

Package.Class.Method/Property	**Access**
service.GneSite	Read/write
service.MacPing	Read/write
service.MacPopulate	Read/write
service.MacPurge	Read/write
service.MacTrace	Read/write
service.RedundantInterface	Read/write
service.Service.method_create	Update/execute
service.Service.method_highPriorityServiceDelete	Update/execute
service.Service.property_svcPriority	Read/update/execute
service.ServiceManager.property_alarmAggregationCompositeService	Read/update/execute
service.ServiceManager.property_alarmAggregationSdp	Read/update/execute
service.ServiceManager.property_autoDiscoverCompositeSvc	Read/update/execute
service.ServiceManager.property_enableCac	Read/update/execute
service.ServiceManager.property_maxNumberOfMoveSites	Read/update/execute
service.ServiceManager.property_multiSegmentTunnelSelection	Read/update/execute
service.ServiceManager.property_propagateServiceNameToSites	Read/update/execute
service.ServiceManager.property_removeEmptyService	Read/update/execute
service.ServiceManager.property_supVprnSnmpCommunityStringMsg	Read/update/execute
service.ServiceManager.property_svcPriority	Read/update/execute
service.ServiceMemberAuditPolicyEntry	Read/write
service.SitePing	Read/write
service.TemplateService.method_constructServiceTemplate	Update/execute
service.TemplateService.method_constructTemplatedService	Update/execute
service.Y1564TestHeadBiDirectional	Read/write
shg	Read/write
simulator	Read/write
simulator.SimSession	Read/write
sitesec	Read/write
sitesec.LocalUser	Read/write
sitesec.UserProfile	Read/write
sitesec.UserPublicKey	Read/write
slaprofile	Read/write
slope	Read/write
slope.QosPool	Read/write
snmp	Read/write
snmp.EventNotificationPolicy	Read/write
snmp.PollerManager	Read/write

(15 of 18)

Package.Class.Method/Property	**Access**
snmp.PollerManager.method_resync	Update/execute
sonet	Read/write
sonetequipment	Read/write
spanrules	Read/write
spb	Read/write
spb.AccessInterface	Read/write
spb.NetworkInterface	Read/write
spb.SpokeSdpBindingInterface	Read/write
squeue	Read/write
srmrmtauth	Read/write
srpythonmgmt	Read/write
srrp	Read/write
statistics	Read/write
statsplot	Read/write
subscr	Read/write
subscr.Site	Read/write
subscrauth	Read/write
subscrexpmap	Read/write
subscrident	Read/write
subscrprofile	Read/write
sup	Read/write
svq	Read/write
svr	Read/write
svt	Read/write
svt.BvlanTunnel	Read/write
svt.L2TPv3Tunnel	Read/write
svt.MeshSdpBinding	Read/write
svt.MirrorSdpBinding	Read/write
svt.MtuPing	Read/write
svt.SpokeSdpBinding	Read/write
svt.Tunnel	Read/write
svt.TunnelPing	Read/write
svt.VccvPing	Read/write
svt.VccvTrace	Read/write
svt.VlanPBBEdgeMeshSdpBinding	Read/write
sw	Read/write
sw.BackupRestoreManager.method_backup	Update/execute

(16 of 18)

Package.Class.Method/Property	**Access**
sw.BackupRestoreManager.method_restore	Update/execute
swran	Read/write
sysact	Read/write
tca	Read/write
tca.TCAManager.property_maxTCAAlarmLimit	Read/update/execute
tca.TCAManager.property_maxTCAAlarmResetInterval	Read/update/execute
tdmequipment	Read/write
template	Read/write
tod	Read/write
todsuite	Read/write
topology	Read/write
topologysim	Read/write
trapmapper	Read/write
tunnelmgmt	Read/write
udprelay	Read/write
udptunnel	Read/write
user	Read/write
vlan	Read/write
vlan.EthernetService	Read/write
vlan.L2AccessInterface	Read/write
vlan.Site	Read/write
vlan.Vlan	Read/write
vll	Read/write
vll.Endpoint	Read/write
vll.L2AccessInterface	Read/write
vpls	Read/write
vpls.BL2AccessInterface	Read/write
vpls.BSite	Read/write
vpls.Endpoint	Read/write
vpls.EvpnSite	Read/write
vpls.IL2AccessInterface	Read/write
vpls.ISite	Read/write
vpls.L2AccessInterface	Read/write
vpls.L2ManagementInterface	Read/write
vpls.Site	Read/write
vpls.Vpls	Read/write
vprn	Read/write

(17 of 18)

Package.Class.Method/Property	Access
vprn.AaInterface	Read/write
vprn.DVRSSite	Read/write
vprn.IPMirrorInterface	Read/write
vprn.L3AccessInterface	Read/write
vprn.Site	Read/write
vprn.SubscriberInterface	Read/write
vprn.Vprn	Read/write
vprn.VprnPing	Read/write
vprn.VprnTrace	Read/write
vrrp	Read/write
vs	Read/write
webclient	No access
webclient.WebClientManager	Read/write
wlangw	Read/write
workspace	Read/write
workspace.WorkspaceManager.method_publicControl	Update/execute
wpp	Read/write
wpp.Site	Read/write

(18 of 18)

Table A-8 User management

Package.Class.Method/Property	Access
aclfilterli	No access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
calltrace.WebDAVSharedData	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.AuxiliaryDatabase.method_reinstantiationDatabase	No access
db.AuxiliaryDatabase.method_snapshotDatabase	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access

(1 of 4)

Package.Class.Method/Property	Access
db.DatabaseManager.method_snapshotAllDatabases	No access
db.DatabaseManager.method_switchover	No access
equipment.Shelf.method_rebootUpgrade	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
lte.ENBEquipment.method_launchNEM	No access
lte.LTEEquipment.method_launchQoSAnalyzer	No access
lteli.DFPeer	No access
lteli.DFPeerCardGroup	No access
lteli.InterceptionTarget	No access
lteli.LILteCfg	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
ltepolicyoptions	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
netw.AdvertisedNode	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_NetoAdminProfileBasedLaunch	No access
netw.NetworkElement.method_NetoViewerProfileBasedLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access

(2 of 4)

Package.Class.Method/Property	Access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security	Read/write
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	Read/write
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
sysact	No access
user	Read/write

(3 of 4)

Package.Class.Method/Property	Access
vprn.IPMirrorInterface	No access
webclient	No access
webclient.WebClientManager	Read/write
workspace	Read/write
workspace.WorkspaceManager.method_publicControl	Update/execute

(4 of 4)

Table A-9 Network Element Equipment Manager

Package.Class.Method/Property	Access
aapolicy	Read/write
accessuplink	Read/write
aclfilterli	No access
activation.WebDAVSharedData	No access
aosredundancy	Read/write
aps	Read/write
atm	Read/write
audit	Read/write
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
bundle	Read/write
cac	Read/write
calltrace.WebDAVSharedData	No access
ccag	Read/write
cflowd	Read/write
cflowd.NeCflowd	Read/write
cflowd.NeCollector	Read/write
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.AuxiliaryDatabase.method_reinstantiationDatabase	No access
db.AuxiliaryDatabase.method_snapshotDatabase	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_snapshotAllDatabases	No access

(1 of 5)

Package.Class.Method/Property	**Access**
db.DatabaseManager.method_switchover	No access
dns	Read/write
equipment	Read/write
equipment.PortPolicy	Read/write
equipment.Shelf.method_rebootUpgrade	No access
ethernetequipment	Read/write
filter	Read/write
fm	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	Update/execute
fr	Read/write
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
igh	Read/write
impact.FullReset	No access
impact.PartialReset	No access
ipsec	Read/write
isa	Read/write
isa.MgGroupMember	Read/write
isa.MgIsaGroup	Read/write
l2fib	Read/write
lag	Read/write
lldp	Read/write
lte	Read/write
lte.ENBEquipment.method_launchNEM	No access
lte.LTEEquipment.method_launchQoSAnalyzer	No access
lte.SubscAndEquipmentTraces	Read/write
lteanr	Read/write
lteli.DFPeer	No access
lteli.DFPeerCardGroup	No access
lteli.InterceptionTarget	No access
lteli.LILteCfg	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access

(2 of 5)

Package.Class.Method/Property	**Access**
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
lteperf	Read/write
ltepolicyoptions	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
mpr	Read/write
multichassis	Read/write
mwa	Read/write
nat	Read/write
neaudit	Read/write
netw	Read/write
netw.AdvertisedNode	Read/write
netw.NetworkElement	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_NetoAdminProfileBasedLaunch	No access
netw.NetworkElement.method_NetoViewerProfileBasedLaunch	No access
netw.NetworkElement.method_executeCli	Update/execute
netw.NetworkElement.method_executeMultiCli	Update/execute
netw.Topology	Read/write
netw.Topology.method_move	Update/execute
netw.UplinkBofConfiguration	Read/write
netw.UplinkRouteConfiguration	Read/write
ntp	Read/write
ntp.NTPBroadcast	Read/write
ntp.NTPMulticast	Read/write
optical	Read/write
opticalequipment	Read/write
oss	No access
oth	Read/write
pae802_1x	Read/write
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
ppp	Read/write
ptp	Read/write

(3 of 5)

Package.Class.Method/Property	Access
radioequipment	Read/write
ranlicense	Read/write
ranradiom	Read/write
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
rmd	Read/write
sasqos.QosPool	Read/write
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
selfconfig	Read/write
service	Read/write
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
slope.QosPool	Read/write

(4 of 5)

Package.Class.Method/Property	**Access**
snmp.PollerManager.method_resync	Update/execute
sonet	Read/write
sonetequipment	Read/write
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
sysact	No access
tdmequipment	Read/write
user	Read/write
vprn.IPMirrorInterface	No access
webclient	No access
webclient.WebClientManager	Read/write
wlangw	Read/write
workspace	Read/write
workspace.WorkspaceManager.method_publicControl	No access

(5 of 5)

Table A-10 Service Management

Package.Class.Method/Property	**Access**
aaa.RadiusProxyServer	Read/write
aaa.RadiusServer	Read/write
aclfilterli	No access
activation.WebDAVSharedData	No access
ancp	Read/write
antispoof	Read/write
apipe	Read/write
apipe.Apipe	Read/write
apipe.Site	Read/write
arp	Read/write
atm	Read/write
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bfd	Read/write
bgp.Site	Read/write
bulk.BulkManager.method_execute	No access

(1 of 7)

Package.Class.Method/Property	Access
bulk.BulkManager.method_generateBatches	No access
cac	Read/write
calltrace.WebDAVSharedData	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
cpipe	Read/write
cpipe.Cpipe	Read/write
cpipe.Site	Read/write
db.AuxiliaryDatabase.method_reinstantiationDatabase	No access
db.AuxiliaryDatabase.method_snapshotDatabase	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_snapshotAllDatabases	No access
db.DatabaseManager.method_switchover	No access
dhcp	Read/write
epipe	Read/write
epipe.Epipe	Read/write
epipe.PbbMacName	Read/write
epipe.Site	Read/write
equipment.Shelf.method_rebootUpgrade	No access
ethernettunnel	Read/write
ethring	Read/write
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
fpipe	Read/write
fpipe.Fpipe	Read/write
fpipe.Site	Read/write
generic	Read/write
generic.GenericObject.method_collectData	No access
gsmp	Read/write
hpipe	No access
hpipe.Hpipe	Read/write
hpipe.Site	Read/write
ies	Read/write
ies.AaInterface	Read/write

(2 of 7)

Package.Class.Method/Property	**Access**
ies.Ies	Read/write
ies.L3AccessInterface	Read/write
ies.Site	Read/write
ies.SubscriberInterface	Read/write
igmp	Read/write
igmp.Site	Read/write
impact.FullReset	No access
impact.PartialReset	No access
ipipe	Read/write
ipipe.Ipipe	Read/write
ipipe.L2AccessInterface	Read/write
ipipe.Site	Read/write
ipsec	Read/write
isis	Read/write
l2fib	Read/write
l2fwd	Read/write
l2tp	Read/write
l3fwd	Read/write
layer2	Read/write
lte.ENBEquipment.method_launchNEM	No access
lte.LTEEquipment.method_launchQoSAnalyzer	No access
lteli.DFPeer	No access
lteli.DFPeerCardGroup	No access
lteli.InterceptionTarget	No access
lteli.LILteCfg	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
ltepolicyoptions	No access
mirror	No access
mirror.Endpoint	Read/write
mirror.Mirror	No access
mirror.Site	No access
mld	Read/write
mmepolicy	No access

(3 of 7)

Package.Class.Method/Property	**Access**
mpr	Read/write
mpr.Al2AccessInterface	Read/write
mpr.Apipe	Read/write
mpr.Asite	Read/write
mpr.Cpipe	Read/write
mpr.El2AccessInterface	Read/write
mpr.Epipe	Read/write
mpr.Esite	Read/write
mpr.L2AccessInterface	Read/write
mpr.Site	Read/write
mvpls	Read/write
mvpls.BL2AccessInterface	Read/write
mvpls.BSite	Read/write
mvpls.EvpnSite	Read/write
mvpls.IL2AccessInterface	Read/write
mvpls.ISite	Read/write
mvpls.L2AccessInterface	Read/write
mvpls.Mvpls	Read/write
mvpls.Site	Read/write
nat.PcpServer	Read/write
netw.AdvertisedNode	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_NetoAdminProfileBasedLaunch	No access
netw.NetworkElement.method_NetoViewerProfileBasedLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
optical	Read/write
optical.MultipointServicePath	Read/write
optical.MultipointTransportService	Read/write
optical.TransportService	Read/write
ospf	Read/write
ospf.Site	Read/write
oss	No access
oth	Read/write
pbbvlan	Read/write
pbbvlan.Site	Read/write

(4 of 7)

Package.Class.Method/Property	**Access**
pbbvlan.VlanPBBEdge	Read/write
pim	Read/write
pim.Site	Read/write
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
ressubscr	Read/write
rip	Read/write
rip.Site	Read/write
rtr	Read/write
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service	Read/write
service.AarpInterface	Read/write

(5 of 7)

Package.Class.Method/Property	Access
service.GneAccessInterface	Read/write
service.GneSite	Read/write
service.RedundantInterface	Read/write
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	Update/execute
service.TemplateService.method_constructTemplatedService	No access
shg	Read/write
snmp.PollerManager.method_resync	No access
spb	Read/write
spb.AccessInterface	Read/write
spb.NetworkInterface	Read/write
spb.SpokeSdpBindingInterface	Read/write
srmrmtauth	No access
srrp	Read/write
svt	Read/write
svt.MeshSdpBinding	Read/write
svt.MirrorSdpBinding	No access
svt.SpokeSdpBinding	Read/write
svt.VlanPBBEdgeMeshSdpBinding	Read/write
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
sysact	No access
template	Read/write
user	Read/write
vlan	Read/write
vlan.EthernetService	Read/write
vlan.L2AccessInterface	Read/write
vlan.Site	Read/write
vlan.Vlan	Read/write
vll	Read/write
vll.Endpoint	Read/write
vll.L2AccessInterface	Read/write
vpls	Read/write
vpls.BL2AccessInterface	Read/write
vpls.BSite	Read/write
vpls.Endpoint	Read/write

(6 of 7)

Package.Class.Method/Property	**Access**
vpls.IL2AccessInterface	Read/write
vpls.ISite	Read/write
vpls.L2AccessInterface	Read/write
vpls.L2ManagementInterface	Read/write
vpls.Site	Read/write
vpls.Vpls	Read/write
vprn	Read/write
vprn.AaInterface	Read/write
vprn.IPMirrorInterface	No access
vprn.L3AccessInterface	Read/write
vprn.Site	Read/write
vprn.SubscriberInterface	Read/write
vprn.Vprn	Read/write
vrrp	Read/write
webclient	No access
webclient.WebClientManager	Read/write
wlangw	Read/write
workspace	Read/write
workspace.WorkspaceManager.method_publicControl	No access
wpp	Read/write
wpp.Site	Read/write

(7 of 7)

Table A-11 Subscriber Management

Package.Class.Method/Property	**Access**
aaa	Read/write
aaa.RadiusProxyInterface	Read/write
aaa.RadiusProxyServer	Read/write
aaa.RadiusServer	Read/write
aclfilterli	No access
activation.WebDAVSharedData	No access
ancp	Read/write
arp	Read/write
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access

(1 of 5)

Package.Class.Method/Property	**Access**
bulk.BulkManager.method_generateBatches	No access
calltrace.WebDAVSharedData	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
connprof	Read/write
crdtctrl	Read/write
db.AuxiliaryDatabase.method_reinstantiationDatabase	No access
db.AuxiliaryDatabase.method_snapshotDatabase	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_snapshotAllDatabases	No access
db.DatabaseManager.method_switchover	No access
diameter	Read/write
equipment.Shelf.method_rebootUpgrade	No access
filter	Read/write
fm	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	Update/execute
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
igmp	Read/write
impact.FullReset	No access
impact.PartialReset	No access
l2tp	Read/write
localuserdb	Read/write
lte.ENBEquipment.method_launchNEM	No access
lte.LTEEquipment.method_launchQoSAnalyzer	No access
lteli.DFPeer	No access
lteli.DFPeerCardGroup	No access
lteli.InterceptionTarget	No access
lteli.LILteCfg	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access

(2 of 5)

Package.Class.Method/Property	**Access**
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
ltepolicyoptions	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mld	Read/write
mmepolicy	No access
monitor	Read/write
msappolicy	Read/write
nat.PcpServer	Read/write
nat.PcpServerInterface	Read/write
netw.AdvertisedNode	Read/write
netw.NeLimitHolder	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_NetoAdminProfileBasedLaunch	No access
netw.NetworkElement.method_NetoViewerProfileBasedLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
oss	No access
policy	Read/write
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
policy.PolicySyncGroupManager	Read/write
pppoe	Read/write
radiusaccounting	Read/write
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
ressubscr	Read/write
ressubscr.BgpPeeringPolicy	Read/write
ressubscr.HostTrackingPolicy	Read/write
ressubscr.IgmpPolicy	Read/write
ressubscr.MldPolicy	Read/write
ressubscr.SubMcastCacPolicy	Read/write
schedule	Read/write

(3 of 5)

Package.Class.Method/Property	Access
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
sitesec	Read/write
slaprofile	Read/write
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
srpythonmgmt	Read/write
subscr	Read/write
subscr.Site	Read/write
subscrauth	Read/write
subscrexpmap	Read/write
subscrident	Read/write
subscrprofile	Read/write

(4 of 5)

Package.Class.Method/Property	**Access**
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
sysact	No access
user	Read/write
vprn.IPMirrorInterface	No access
webclient	No access
webclient.WebClientManager	Read/write
wlangw	Read/write
workspace	Read/write
workspace.WorkspaceManager.method_publicControl	No access

(5 of 5)

Table A-12 QoS/ACL Policy Management

Package.Class.Method/Property	**Access**
aclfilter	Read/write
aclfilterli	No access
activation.WebDAVSharedData	No access
aengr	Read/write
aingr	Read/write
aosqos	Read/write
aossas	Read/write
atmpolicy	Read/write
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
calltrace.WebDAVSharedData	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.AuxiliaryDatabase.method_reinstantiationDatabase	No access
db.AuxiliaryDatabase.method_snapshotDatabase	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_snapshotAllDatabases	No access

(1 of 4)

Package.Class.Method/Property	Access
db.DatabaseManager.method_switchover	No access
equipment	Read/write
equipment.Shelf.method_rebootUpgrade	No access
ethernetservice	Read/write
fabricqos	Read/write
filter	Read/write
filterprefixlist	Read/write
fm	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	Update/execute
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
layer2	Read/write
lte	Read/update/execute
lte.DiameterProfile	Read/write
lte.ENBEquipment.method_launchNEM	No access
lte.LTEEquipment.method_launchQoSAnalyzer	No access
lte.TrustedPeerListPolicy	Read/write
lteli.DFPeer	No access
lteli.DFPeerCardGroup	No access
lteli.InterceptionTarget	No access
lteli.LILteCfg	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
ltepmip.S6bAvpOptionProfile	Read/write
ltepolicyoptions	No access
lteradius.RadiusProfile	Read/write
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access

(2 of 4)

Package.Class.Method/Property	Access
mpr	Read/write
netw.AdvertisedNode	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_NetoAdminProfileBasedLaunch	No access
netw.NetworkElement.method_NetoViewerProfileBasedLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
niegr	Read/write
nqueue	Read/write
oss	No access
policing	Read/write
policy	Read/write
policy.PolicyDefinition.method_setConfigurationModeToReleased	Update/execute
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	Update/execute
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	Update/execute
policy.PolicySyncGroupManager	Read/write
portscheduler	Read/write
qgroup	Read/write
qosprofile	Read/write
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
ressubscr	Read/write
sasqos	Read/write
schedule	Read/write
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access

(3 of 4)

Package.Class.Method/Property	**Access**
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service	Read/write
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
slope	Read/write
snmp.PollerManager.method_resync	No access
squeue	Read/write
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
sysact	No access
todsuite	Read/write
user	Read/write
vprn.IPMirrorInterface	No access
vs	Read/write
webclient	No access
webclient.WebClientManager	Read/write
workspace	Read/write
workspace.WorkspaceManager.method_publicControl	No access

(4 of 4)

Table A-13 Policy Management (except QoS/ACL)

Package.Class.Method/Property	**Access**
aaa	Read/write
aapolicy	Read/write
accounting	Read/write
aclfilterli	No access
activation.WebDAVSharedData	No access
ancp	Read/write
aossas	Read/write
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
calltrace.WebDAVSharedData	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
connprof	Read/write
crdtctrl	Read/write
db.AuxiliaryDatabase.method_reinstantiationDatabase	No access
db.AuxiliaryDatabase.method_snapshotDatabase	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_snapshotAllDatabases	No access
db.DatabaseManager.method_switchover	No access
diameter	Read/write
dynsvc	Read/write
equipment.PortPolicy	Read/write
equipment.Shelf.method_rebootUpgrade	No access
ethernetoam	Read/write
file	Read/write
filter	Read/write
fm	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	Update/execute
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
igmp	Read/write

(1 of 6)

Package.Class.Method/Property	**Access**
impact.FullReset	No access
impact.PartialReset	No access
l2fwd	Read/write
lte	Read/update/execute
lte.DccaProfile	Read/write
lte.DiameterPeerListEntry	Read/write
lte.DiameterPeerProfile	Read/write
lte.ENBEquipment.method_launchNEM	No access
lte.GtpPrimaryServerListEntry	Read/write
lte.GtpPrimeServerGroupProfile	Read/write
lte.GtpProfile	Read/write
lte.LTEEquipment.method_launchQoSAnalyzer	No access
lte.PgwChargingProfile	Read/write
lte.PlmnListPolicy	Read/write
lte.PlmnListPolicyGroup	Read/write
lte.QciPolicy	Read/write
lte.QciPolicyEntry	Read/write
lte.SgwChargingProfile	Read/write
lte.TrustedPeerListEntry	Read/write
lte.TrustedPeerListEntryUnlisted	Read/write
lteggsn.CdrAvpOptionProfile	Read/write
lteggsn.DccaRatingGroup	Read/write
lteggsn.GyAvpOptionProfile	Read/write
ltegw.ApnListPolicy	Read/write
ltegw.ApnListPolicyGroup	Read/write
ltegw.DiameterPeerRedirHostEntry	Read/write
ltegw.DiameterPeerSupportedHost	Read/write
ltegw.PcscfGroupProfile	Read/write
ltegw.PcscfPeerEntry	Read/write
ltegw.PcscfResolvedPeerIPEntry	Read/write
ltegw.SCTPProfile	Read/write
ltegw.UMTSQoSPolicy	Read/write
lteli.DFPeer	No access
lteli.DFPeerCardGroup	No access
lteli.InterceptionTarget	No access
lteli.LILteCfg	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access

(2 of 6)

Package.Class.Method/Property	Access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
ltepmip.Pmipv6Profile	Read/write
ltepolicyoptions	No access
ltepolicyoptions.AsoOptions	Read/write
ltepolicyoptions.ChargingRuleUnit	Read/write
ltepolicyoptions.DhcpSGPeerEntry	Read/write
ltepolicyoptions.DhcpServerGroupProfile	Read/write
ltepolicyoptions.GxAvpOptionProfile	Read/write
ltepolicyoptions.PolRuleUnitFlwDescription	Read/write
ltepolicyoptions.PolicyRule	Read/write
ltepolicyoptions.PolicyRuleBase	Read/write
ltepolicyoptions.PolicyRuleBaseEntry	Read/write
ltepolicyoptions.PolicyRuleUnit	Read/write
ltepolicyoptions.ServiceClassIndicator	Read/write
ltepolicyoptions.TrafficRedirectProfile	Read/write
ltepolicyoptions.TrafficRedirectTarget	Read/write
lteradius.RadiusGroupProfile	Read/write
lteradius.RadiusPeerProfile	Read/write
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
mmepolicy.MMEEmergencyNumListPolicy	Read/write
mmepolicy.MMEGTPProfile	Read/write
mmepolicy.MMESCTPProfile	Read/write
mmepolicy.WMMPfmJobEntry	Read/write
mmepolicy.WMMPfmJobMts	Read/write
mmepolicy.WMMPfmJobSched	Read/write
mmepolicy.WMMPfmMeasGroupName	Read/write
mmepolicy.WMMPfmMeasGroups	Read/write
mplstp	Read/write
mpr	Read/write
msappolicy	Read/write
multicast	Read/write

(3 of 6)

Package.Class.Method/Property	Access
netca	Read/write
netw.AdvertisedNode	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_NetoAdminProfileBasedLaunch	No access
netw.NetworkElement.method_NetoViewerProfileBasedLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
nodelog	Read/write
optical	Read/write
oss	No access
pae802_1x	Read/write
policy	Read/write
policy.PolicyDefinition.method_setConfigurationModeToReleased	Update/execute
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	Update/execute
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	Update/execute
policy.PolicySyncGroupManager	Read/write
pppoe	Read/write
radiusaccounting	Read/write
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
ressubscr	Read/write
ressubscr.BgpPeeringPolicy	Read/write
ressubscr.HostTrackingPolicy	Read/write
ressubscr.IgmpPolicy	Read/write
ressubscr.MldPolicy	Read/write
ressubscr.SubMcastCacPolicy	Read/write
rp	Read/write
sas	Read/write
schedule	Read/write
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access

(4 of 6)

Package.Class.Method/Property	**Access**
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
sitesec	Read/write
slaprofile	Read/write
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
srpythonmgmt	Read/write
subscrauth	Read/write
subscrexpmap	Read/write
subscrident	Read/write
subscrprofile	Read/write
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
sysact	No access
tod	Read/write
todsuite	Read/write
user	Read/write
vprn.IPMirrorInterface	No access

(5 of 6)

Package.Class.Method/Property	Access
vrrp	Read/write
vs	Read/write
webclient	No access
webclient.WebClientManager	Read/write
wlangw	Read/write
workspace	Read/write
workspace.WorkspaceManager.method_publicControl	No access

(6 of 6)

Table A-14 Routing Management

Package.Class.Method/Property	Access
aclfilterli	No access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bfd	Read/write
bgp	Read/write
bgp.Site	Read/write
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
calltrace.WebDAVSharedData	No access
cflowd.NeCflowd	Read/write
cflowd.NeCollector	Read/write
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.AuxiliaryDatabase.method_reinstantiationDatabase	No access
db.AuxiliaryDatabase.method_snapshotDatabase	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_snapshotAllDatabases	No access
db.DatabaseManager.method_switchover	No access
dhcp	Read/write
equipment.Shelf.method_rebootUpgrade	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access

(1 of 6)

Package.Class.Method/Property	**Access**
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
igmp	Read/write
igmp.Site	Read/write
impact.FullReset	No access
impact.PartialReset	No access
isis	Read/write
l2fib	Read/write
l2tp	Read/write
l3fwd	Read/write
lag	Read/write
layer2	Read/write
ldp	Read/write
lte	Read/write
lte.ApnPolicyRuleBase	Read/write
lte.DiscoveryLog	Read/write
lte.DupRadiusAccServerGroup	Read/write
lte.ENBEquipment.method_launchNEM	No access
lte.EPSPathDiscoveredLinkComponent	Read/write
lte.EPSPathInterfaceComponent	Read/write
lte.EPSPathLinkComponent	Read/write
lte.EPSPathSapComponent	Read/write
lte.EPSPathServiceComponent	Read/write
lte.EPSPathSiteComponent	Read/write
lte.IpPool	Read/write
lte.IpPoolBinding	Read/write
lte.IpPoolEntry	Read/write
lte.LTEEquipment.method_launchQoSAnalyzer	No access
lte.PDNGateway	Read/write
lte.PdnApn	Read/write
lte.PdnGxReferencePoint	Read/write
lte.PdnRfReferencePoint	Read/write
lte.PdnS5ReferencePoint	Read/write
lte.PdnS8ReferencePoint	Read/write
lte.PdnSignalling	Read/write

(2 of 6)

Package.Class.Method/Property	**Access**
lte.S11ReferencePoint	Read/write
lte.S1uReferencePoint	Read/write
lte.ServingGateway	Read/write
lte.SgwApn	Read/write
lte.SgwRfReferencePoint	Read/write
lte.SgwS5ReferencePoint	Read/write
lte.SgwS8ReferencePoint	Read/write
lte.SgwSignalling	Read/write
lteggsn	Read/write
lteggsn.GnReferencePoint	Read/write
lteggsn.GpReferencePoint	Read/write
lteggsn.PdnGyReferencePoint	Read/write
lteggsn.PgwGaReferencePoint	Read/write
lteggsn.SgwGaReferencePoint	Read/write
ltegw	Read/write
lteli.DFPeer	No access
lteli.DFPeerCardGroup	No access
lteli.InterceptionTarget	No access
lteli.LILteCfg	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
ltepmip	Read/write
ltepmip.S2aReferencePoint	Read/write
ltepmip.S2bReferencePoint	Read/write
ltepmip.S6bReferencePoint	Read/write
ltepolicyoptions	No access
lteradius	Read/write
ltesgsn.SgwS12ReferencePoint	Read/write
ltesgsn.SgwS4ReferencePoint	Read/write
ltethreshold	Read/write
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mld	Read/write

(3 of 6)

Package.Class.Method/Property	Access
mmepolicy	No access
mpls	Read/write
mplstp	Read/write
mpr	Read/write
msdp	Read/write
multicast	Read/write
mwa	Read/write
netw	Read/write
netw.AdvertisedNode	Read/write
netw.NetworkElement	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_NetoAdminProfileBasedLaunch	No access
netw.NetworkElement.method_NetoViewerProfileBasedLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology	Read/write
netw.Topology.method_move	Update/execute
netw.UplinkBofConfiguration	Read/write
netw.UplinkRouteConfiguration	Read/write
optical	Read/write
ospf	Read/write
ospf.Site	Read/write
oss	No access
oth	Read/write
pim	Read/write
pim.Site	Read/write
policy	Read/write
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
rip	Read/write
rip.Site	Read/write
rp	Read/write
rsvp	Read/write

(4 of 6)

Package.Class.Method/Property	**Access**
rtr	Read/write
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
sysact	No access
udprelay	Read/write
user	Read/write
vpls	Read/write
vprn.IPMirrorInterface	No access

(5 of 6)

Package.Class.Method/Property	Access
vrrp	Read/write
webclient	No access
webclient.WebClientManager	Read/write
workspace	Read/write
workspace.WorkspaceManager.method_publicControl	No access
wpp.Site	Read/write

(6 of 6)

Table A-15 Tunnel Management

Package.Class.Method/Property	Access
aclfilterli	No access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
calltrace.WebDAVSharedData	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.AuxiliaryDatabase.method_reinstantiationDatabase	No access
db.AuxiliaryDatabase.method_snapshotDatabase	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_snapshotAllDatabases	No access
db.DatabaseManager.method_switchover	No access
equipment.Shelf.method_rebootUpgrade	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
ipsec	Read/write

(1 of 4)

Package.Class.Method/Property	**Access**
ldp	Read/write
lte.ENBEquipment.method_launchNEM	No access
lte.LTEEquipment.method_launchQoSAnalyzer	No access
lteanr	Read/write
lteli.DFPeer	No access
lteli.DFPeerCardGroup	No access
lteli.InterceptionTarget	No access
lteli.LILteCfg	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
lteperf	Read/write
ltepolicyoptions	No access
ltesecurity	Read/write
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
mpls	Read/write
mplstp	Read/write
mpr	Read/write
netw.AdvertisedNode	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_NetoAdminProfileBasedLaunch	No access
netw.NetworkElement.method_NetoViewerProfileBasedLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology	Read/write
netw.Topology.method_move	Update/execute
opticsperf	Read/write
oss	No access
policy	Read/write
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access

(2 of 4)

Package.Class.Method/Property	Access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
rsvp	Read/write
rtr	Read/write
rules	Read/write
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	Update/execute
script.XmlApiConfigTemplate.method_executeMulti	Update/execute
script.XmlApiConfigTemplate.method_executeScript	Update/execute
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	Update/execute
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt	Read/write
svt.L2TPv3Tunnel	Read/write
svt.MirrorSdpBinding	No access

(3 of 4)

Package.Class.Method/Property	**Access**
svt.Tunnel	Read/write
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
sysact	No access
tunnelmgmt	Read/write
user	Read/write
vprn.IPMirrorInterface	No access
webclient	No access
webclient.WebClientManager	Read/write
workspace	Read/write
workspace.WorkspaceManager.method_publicControl	No access

(4 of 4)

Table A-16 SAM Management and Operations

Package.Class.Method/Property	**Access**
aaa	Read/write
aclfilterli	No access
activation.WebDAVSharedData	No access
ageoutcstr	Read/write
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
calltrace.WebDAVSharedData	No access
cflowd.NeCflowd	Read/write
cflowd.NeCollector	Read/write
cli	No access
cli.SSH	No access
cli.Telnet	No access
db	Read/write
db.AuxiliaryDatabase.method_reinstantiationDatabase	Update/execute
db.AuxiliaryDatabase.method_snapshotDatabase	Update/execute
db.DatabaseManager.method_backup	Update/execute
db.DatabaseManager.method_reinstantiateStandby	Update/execute
db.DatabaseManager.method_snapshotAllDatabases	Update/execute
db.DatabaseManager.method_switchover	Update/execute

(1 of 5)

Package.Class.Method/Property	**Access**
dctr	Read/write
equipment.Shelf.method_rebootUpgrade	No access
filter	Read/write
firewall	Read/write
fm	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	Update/execute
generic	Read/write
generic.GenericObject.method_collectData	Update/execute
genericlog	Read/write
hip.EMServer	Read/write
hip.EMSystem	Read/write
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
ipfix	Read/write
log	Read/write
lps	Read/write
lte	Read/write
lte.ENBEquipment.method_launchNEM	No access
lte.EPSPathDiscoveryHint	Read/write
lte.EPSPathDiscoveryProfile	Read/write
lte.EPSPathSegment	Read/write
lte.LTEEquipment.method_launchQoSAnalyzer	No access
lte.MobileNodeRegion	Read/write
lteanr	Read/write
lteggsn	Read/write
ltegw	Read/write
lteli.DFPeer	No access
lteli.DFPeerCardGroup	No access
lteli.InterceptionTarget	No access
lteli.LILteCfg	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access

(2 of 5)

Package.Class.Method/Property	Access
lteperf	Read/write
ltepmip	Read/write
ltepolicyoptions	No access
lteradius	Read/write
ltesecurity	Read/write
lteservice	Read/write
ltesgsn	Read/write
lteuserstats	Read/write
lteuserstats.UserStatsQuery	Read/write
lteuserstats.UserStatsQueryOutputSnapshot	Read/write
lteuserstats.UserStatsUserPgw	Read/write
lteuserstats.UserStatsUserSgw	Read/write
mediation	Read/write
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
mpls	Read/write
multicast	Read/write
nat	Read/write
neaudit	Read/write
netw	Read/write
netw.AdvertisedNode	Read/write
netw.NetworkElement	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_NetoAdminProfileBasedLaunch	No access
netw.NetworkElement.method_NetoViewerProfileBasedLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.NodeDiscoveryControl	Read/write
netw.Topology	Read/write
netw.Topology.method_move	Update/execute
netw.UplinkBofConfiguration	Read/write
netw.UplinkRouteConfiguration	Read/write
opticalacl	Read/write
opticsperf	Read/write
oss	No access

(3 of 5)

Package.Class.Method/Property	Access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
ranlicense	Read/write
ranradiom	Read/write
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
schedule	Read/write
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security	Read/update/execute
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	Read/write
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.Span	Read/write
security.SpanObjectBinding	Read/write
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
securitypolicy	Read/write
selfconfig	Read/write
server	Read/write

(4 of 5)

Package.Class.Method/Property	**Access**
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
sitesec	Read/write
sitesec.LocalUser	Read/write
sitesec.UserProfile	Read/write
sitesec.UserPublicKey	Read/write
snmp	Read/write
snmp.PollerManager	Read/write
snmp.PollerManager.method_resync	Update/execute
spanrules	Read/write
srmrmtauth	No access
statistics	Read/write
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
sysact	Read/write
tca	Read/write
user	Read/write
vprn.IPMirrorInterface	No access
webclient	No access
webclient.WebClientManager	Read/write
workspace	Read/write
workspace.WorkspaceManager.method_publicControl	Update/execute

(5 of 5)

Table A-17 Network Element Software Management

Package.Class.Method/Property	**Access**
aclfilterli	No access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
calltrace.WebDAVSharedData	No access

(1 of 4)

Package.Class.Method/Property	Access
cflowd.NeCflowd	Read/write
cflowd.NeCollector	Read/write
cli	Read/write
cli.SSH	No access
cli.Telnet	No access
db.AuxiliaryDatabase.method_reinstantiationDatabase	No access
db.AuxiliaryDatabase.method_snapshotDatabase	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_snapshotAllDatabases	No access
db.DatabaseManager.method_switchover	No access
equipment	Read/write
equipment.Shelf.method_rebootUpgrade	Update/execute
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
lte	Read/write
lte.ENBEquipment.method_launchNEM	No access
lte.LTEEquipment.method_launchQoSAnalyzer	No access
lteli.DFPeer	No access
lteli.DFPeerCardGroup	No access
lteli.InterceptionTarget	No access
lteli.LILteCfg	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
ltepolicyoptions	No access
mediation	Read/write
mirror	No access
mirror.Mirror	No access

(2 of 4)

Package.Class.Method/Property	**Access**
mirror.Site	No access
mmepolicy	No access
nelicense	Read/write
netw	Read/write
netw.AdvertisedNode	Read/write
netw.NetworkElement	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_NetoAdminProfileBasedLaunch	No access
netw.NetworkElement.method_NetoViewerProfileBasedLaunch	No access
netw.NetworkElement.method_executeCli	Update/execute
netw.NetworkElement.method_executeMultiCli	Update/execute
netw.Topology.method_move	No access
netw.UplinkBofConfiguration	Read/write
netw.UplinkRouteConfiguration	Read/write
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
rollback	Read/write
schedule	Read/write
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access

(3 of 4)

Package.Class.Method/Property	**Access**
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	Update/execute
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw	Read/write
sw.BackupRestoreManager.method_backup	Update/execute
sw.BackupRestoreManager.method_restore	Update/execute
swran	Read/write
sysact	No access
user	Read/write
vprn.IPMirrorInterface	No access
webclient	No access
webclient.WebClientManager	Read/write
workspace	Read/write
workspace.WorkspaceManager.method_publicControl	No access

(4 of 4)

Table A-18 Fault Management

Package.Class.Method/Property	**Access**
aclfilterli	No access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access

(1 of 4)

Package.Class.Method/Property	**Access**
calltrace.WebDAVSharedData	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.AuxiliaryDatabase.method_reinstantiationDatabase	No access
db.AuxiliaryDatabase.method_snapshotDatabase	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_snapshotAllDatabases	No access
db.DatabaseManager.method_switchover	No access
equipment.Shelf.method_rebootUpgrade	No access
filter	Read/write
fm	Read/write
fm.AlarmHistoryDatabase.method_purge	Update/execute
fm.FaultManager	Read/write
fm.FaultManager.method_editNote	Update/execute
fm.GlobalPolicy	Read/write
fm.SpecificPolicy	Read/write
generic	Read/write
generic.GenericObject.method_collectData	Update/execute
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
lte.ENBEquipment.method_launchNEM	No access
lte.LTEEquipment.method_launchQoSAnalyzer	No access
lteli.DFPeer	No access
lteli.DFPeerCardGroup	No access
lteli.InterceptionTarget	No access
lteli.LILteCfg	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
ltepolicyoptions	No access
mirror	No access
mirror.Mirror	No access

(2 of 4)

Package.Class.Method/Property	Access
mirror.Site	No access
mmepolicy	No access
netw.AdvertisedNode	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_NetoAdminProfileBasedLaunch	No access
netw.NetworkElement.method_NetoViewerProfileBasedLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
olc	Read/write
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
rmon	Read/write
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access

(3 of 4)

Package.Class.Method/Property	**Access**
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
sysact	No access
user	Read/write
vprn.IPMirrorInterface	No access
webclient	No access
webclient.WebClientManager	Read/write
workspace	Read/write
workspace.WorkspaceManager.method_publicControl	No access

(4 of 4)

Table A-19 Service Test Management

Package.Class.Method/Property	**Access**
aclfilterli	No access
activation.WebDAVSharedData	No access
ancp.AncpLoopback	Read/write
aosqos	Read/write
aossas	Read/write
aossas.CPETestGroupHead	Read/write
aossas.CPETestHead	Read/write
atm.AtmPing	Read/write
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
calltrace.WebDAVSharedData	No access

(1 of 5)

Package.Class.Method/Property	**Access**
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.AuxiliaryDatabase.method_reinstantiationDatabase	No access
db.AuxiliaryDatabase.method_snapshotDatabase	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_snapshotAllDatabases	No access
db.DatabaseManager.method_switchover	No access
equipment.Shelf.method_rebootUpgrade	No access
ethernetequipment	Read/write
ethernetoam	Read/write
ethernetoam.CcTest	Read/write
ethernetoam.CcmTest	Read/write
ethernetoam.CfmDmmBin	Read/write
ethernetoam.CfmDmmSession	Read/write
ethernetoam.CfmEthTest	Read/write
ethernetoam.CfmLMTest	Read/write
ethernetoam.CfmLinkTrace	Read/write
ethernetoam.CfmLoopback	Read/write
ethernetoam.CfmOneWayDelayTest	Read/write
ethernetoam.CfmOneWaySlm	Read/write
ethernetoam.CfmSingleEndedLossTest	Read/write
ethernetoam.CfmSlmSession	Read/write
ethernetoam.CfmTwoWayDelayTest	Read/write
ethernetoam.CfmTwoWaySlm	Read/write
ethernetoam.EthSession	Read/write
ethernettunnel	Read/write
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
icmp.DnsPing	Read/write
icmp.IcmpPing	Read/write
icmp.IcmpTrace	Read/write

(2 of 5)

Package.Class.Method/Property	Access
impact.FullReset	No access
impact.PartialReset	No access
ldp	Read/write
lte.ENBEquipment.method_launchNEM	No access
lte.LTEEquipment.method_launchQoSAnalyzer	No access
lteli.DFPeer	No access
lteli.DFPeerCardGroup	No access
lteli.InterceptionTarget	No access
lteli.LILteCfg	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
ltepolicyoptions	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
mpls	Read/write
mpls.LdpTreeTrace	Read/write
mpls.LspPing	Read/write
mpls.LspTrace	Read/write
mpls.P2MPLspPing	Read/write
mpls.P2MPLspTrace	Read/write
multicast.MfibPing	Read/write
multicast.Mrinfo	Read/write
multicast.Mtrace	Read/write
netw.AdvertisedNode	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_NetoAdminProfileBasedLaunch	No access
netw.NetworkElement.method_NetoViewerProfileBasedLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access

(3 of 5)

Package.Class.Method/Property	Access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
sas	Read/write
schedule	Read/write
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.CpePing	Read/write
service.MacPing	Read/write
service.MacPopulate	Read/write
service.MacPurge	Read/write
service.MacTrace	Read/write
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.SitePing	Read/write

(4 of 5)

Package.Class.Method/Property	Access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
service.Y1564TestHeadBiDirectional	Read/write
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
svt.MtuPing	Read/write
svt.TunnelPing	Read/write
svt.VccvPing	Read/write
svt.VccvTrace	Read/write
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
sysact	No access
user	Read/write
vprn.IPMirrorInterface	No access
vprn.VprnPing	Read/write
vprn.VprnTrace	Read/write
webclient	No access
webclient.WebClientManager	Read/write
workspace	Read/write
workspace.WorkspaceManager.method_publicControl	No access

(5 of 5)

Table A-20 Script Management

Package.Class.Method/Property	Access
aclfilterli	No access
activation.WebDAVSharedData	No access
autoconfig	Read/write
autoconfig.AutoConfigScriptManager.method_configure	Update/execute
autoconfig.AutoConfigScriptManager.method_copyContents	Update/execute
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
calltrace.WebDAVSharedData	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access

(1 of 4)

Package.Class.Method/Property	**Access**
db.AuxiliaryDatabase.method_reinstantiationDatabase	No access
db.AuxiliaryDatabase.method_snapshotDatabase	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_snapshotAllDatabases	No access
db.DatabaseManager.method_switchover	No access
equipment.Shelf.method_rebootUpgrade	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
lte.ENBEquipment.method_launchNEM	No access
lte.LTEEquipment.method_launchQoSAnalyzer	No access
lteli.DFPeer	No access
lteli.DFPeerCardGroup	No access
lteli.InterceptionTarget	No access
lteli.LILteCfg	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
ltepolicyoptions	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
netw.AdvertisedNode	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_NetoAdminProfileBasedLaunch	No access
netw.NetworkElement.method_NetoViewerProfileBasedLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access

(2 of 4)

Package.Class.Method/Property	Access
netw.Topology.method_move	No access
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
schedule	Read/write
script	Read/write
script.AbstractScript.method_configureTarget	Update/execute
script.AbstractScript.method_configureTargets	Update/execute
script.Bundle	Read/write
script.ControlScript	Read/write
script.ControlScriptVersion	Read/write
script.HandlerBinding	Read/write
script.InvokerBinding	Read/write
script.LargeTextTargetParameter	Read/write
script.Result	Read/write
script.Script	Read/write
script.Script.method_createTargetScript	Update/execute
script.Script.method_createTargetScripts	Update/execute
script.ScriptManager	Read/write
script.ScriptManager.method_configure	Update/execute
script.ScriptManager.method_copyContents	Update/execute
script.ScriptManager.method_exportBundle	Update/execute
script.ScriptManager.method_importBundle	Update/execute
script.ScriptManager.method_importBundleSimulation	Update/execute
script.ScriptScheduledTask	Read/write
script.TargetParameter	Read/write
script.TargetParameterItem	Read/write
script.TargetParameterList	Read/write
script.TargetScript	Read/write
script.Version	Read/write
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access

(3 of 4)

Package.Class.Method/Property	Access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
script.XmlApiScript	Read/write
script.XmlApiVersion	Read/write
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
sysact	No access
user	Read/write
vprn.IPMirrorInterface	No access
webclient	No access
webclient.WebClientManager	Read/write
workspace	Read/write
workspace.WorkspaceManager.method_publicControl	No access

(4 of 4)

Table A-21 Script Execution

Package.Class.Method/Property	Access
aclfilterli	No access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access

(1 of 4)

Package.Class.Method/Property	Access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
calltrace.WebDAVSharedData	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.AuxiliaryDatabase.method_reinstantiationDatabase	No access
db.AuxiliaryDatabase.method_snapshotDatabase	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_snapshotAllDatabases	No access
db.DatabaseManager.method_switchover	No access
equipment.Shelf.method_rebootUpgrade	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
lte.ENBEquipment.method_launchNEM	No access
lte.LTEEquipment.method_launchQoSAnalyzer	No access
lteli.DFPeer	No access
lteli.DFPeerCardGroup	No access
lteli.InterceptionTarget	No access
lteli.LILteCfg	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
ltepolicyoptions	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access

(2 of 4)

Package.Class.Method/Property	Access
netw.AdvertisedNode	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_NetoAdminProfileBasedLaunch	No access
netw.NetworkElement.method_NetoViewerProfileBasedLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
schedule	Read/write
script	Read/write
script.AbstractScript.method_configureTarget	Update/execute
script.AbstractScript.method_configureTargets	Update/execute
script.LargeTextTargetParameter	Read/write
script.Result	Read/write
script.Script.method_createTargetScript	Update/execute
script.Script.method_createTargetScripts	Update/execute
script.ScriptManager	Read/write
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.ScriptScheduledTask	Read/write
script.TargetParameter	Read/write
script.TargetParameterItem	Read/write
script.TargetParameterList	Read/write
script.TargetScript	Read/write
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access

(3 of 4)

Package.Class.Method/Property	Access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
sysact	No access
user	Read/write
vprn.IPMirrorInterface	No access
webclient	No access
webclient.WebClientManager	Read/write
workspace	Read/write
workspace.WorkspaceManager.method_publicControl	No access

(4 of 4)

Table A-22 Mirror Service Management

Package.Class.Method/Property	Access
aclfilterli	No access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
calltrace.WebDAVSharedData	No access

(1 of 4)

Package.Class.Method/Property	Access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.AuxiliaryDatabase.method_reinstantiationDatabase	No access
db.AuxiliaryDatabase.method_snapshotDatabase	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_snapshotAllDatabases	No access
db.DatabaseManager.method_switchover	No access
equipment.Shelf.method_rebootUpgrade	No access
ethernetequipment	Read/write
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
lte.ENBEquipment.method_launchNEM	No access
lte.LTEEquipment.method_launchQoSAnalyzer	No access
lteli.DFPeer	No access
lteli.DFPeerCardGroup	No access
lteli.InterceptionTarget	No access
lteli.LILteCfg	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
ltepolicyoptions	No access
mirror	Read/write
mirror.Mirror	Read/write
mirror.Site	Read/write
mmepolicy	No access
mpls	Read/write
mpr	Read/write

(2 of 4)

Package.Class.Method/Property	**Access**
netw.AdvertisedNode	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_NetoAdminProfileBasedLaunch	No access
netw.NetworkElement.method_NetoViewerProfileBasedLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
oss	No access
policy	Read/write
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
policy.PolicySyncGroupManager	Read/write
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
sas	Read/write
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access

(3 of 4)

Package.Class.Method/Property	Access
security.User	No access
security.UserGroup	No access
service	Read/write
service.GneAccessInterface	Read/write
service.GneSite	Read/write
service.Service.method_create	Update/execute
service.Service.method_highPriorityServiceDelete	Update/execute
service.SitePing	Read/write
service.TemplateService.method_constructServiceTemplate	Update/execute
service.TemplateService.method_constructTemplatedService	Update/execute
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
subscr.Site	Read/write
svt	Read/write
svt.MirrorSdpBinding	Read/write
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
sysact	No access
template	Read/write
user	Read/write
vprn.IPMirrorInterface	Read/write
webclient	No access
webclient.WebClientManager	Read/write
workspace	Read/write
workspace.WorkspaceManager.method_publicControl	No access

(4 of 4)

Table A-23 OSS Management

Package.Class.Method/Property	Access
aclfilterli	No access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
calltrace.WebDAVSharedData	No access

(1 of 4)

Package.Class.Method/Property	Access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.AuxiliaryDatabase.method_reinstantiationDatabase	No access
db.AuxiliaryDatabase.method_snapshotDatabase	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_snapshotAllDatabases	No access
db.DatabaseManager.method_switchover	No access
equipment.Shelf.method_rebootUpgrade	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
lte.ENBEquipment.method_launchNEM	No access
lte.LTEEquipment.method_launchQoSAnalyzer	No access
lteli.DFPeer	No access
lteli.DFPeerCardGroup	No access
lteli.InterceptionTarget	No access
lteli.LILteCfg	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
ltepolicyoptions	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
netw.AdvertisedNode	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_NetoAdminProfileBasedLaunch	No access

(2 of 4)

Package.Class.Method/Property	Access
netw.NetworkElement.method_NetoViewerProfileBasedLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
oss	Read/write
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
schedule	Read/write
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access

(3 of 4)

Package.Class.Method/Property	Access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
sysact	No access
user	Read/write
vprn.IPMirrorInterface	No access
webclient	No access
webclient.WebClientManager	Read/write
workspace	Read/write
workspace.WorkspaceManager.method_publicControl	No access

(4 of 4)

Table A-24 Telnet/SSH Management

Package.Class.Method/Property	Access
aclfilterli	No access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
calltrace.WebDAVSharedData	No access
cli	Read/write
cli.SSH	Read/write
cli.Telnet	Read/write
db.AuxiliaryDatabase.method_reinstantiationDatabase	No access
db.AuxiliaryDatabase.method_snapshotDatabase	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_snapshotAllDatabases	No access
db.DatabaseManager.method_switchover	No access
equipment.Shelf.method_rebootUpgrade	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access

(1 of 3)

Package.Class.Method/Property	Access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
lte.ENBEquipment.method_launchNEM	No access
lte.LTEEquipment.method_launchQoSAnalyzer	No access
lteli.DFPeer	No access
lteli.DFPeerCardGroup	No access
lteli.InterceptionTarget	No access
lteli.LILteCfg	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
ltepolicyoptions	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
netw.AdvertisedNode	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_NetoAdminProfileBasedLaunch	No access
netw.NetworkElement.method_NetoViewerProfileBasedLaunch	No access
netw.NetworkElement.method_executeCli	Update/execute
netw.NetworkElement.method_executeMultiCli	Update/execute
netw.Topology.method_move	No access
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
script.AbstractScript.method_configureTarget	No access

(2 of 3)

Package.Class.Method/Property	**Access**
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
sysact	No access
user	Read/write
vprn.IPMirrorInterface	No access
webclient	No access
webclient.WebClientManager	Read/write
workspace	Read/write
workspace.WorkspaceManager.method_publicControl	No access

(3 of 3)

Table A-25 CPAM Management

Package.Class.Method/Property	Access
aclfilterli	No access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
calltrace.WebDAVSharedData	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.AuxiliaryDatabase.method_reinstantiationDatabase	No access
db.AuxiliaryDatabase.method_snapshotDatabase	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_snapshotAllDatabases	No access
db.DatabaseManager.method_switchover	No access
equipment.Shelf.method_rebootUpgrade	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
lte.ENBEquipment.method_launchNEM	No access
lte.LTEEquipment.method_launchQoSAnalyzer	No access
lteli.DFPeer	No access
lteli.DFPeerCardGroup	No access
lteli.InterceptionTarget	No access
lteli.LILteCfg	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
ltepolicyoptions	No access

(1 of 3)

Package.Class.Method/Property	Access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
netw.AdvertisedNode	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_NetoAdminProfileBasedLaunch	No access
netw.NetworkElement.method_NetoViewerProfileBasedLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	Update/execute
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	Update/execute
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access

(2 of 3)

Package.Class.Method/Property	Access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
sysact	No access
topology	Read/write
user	Read/write
vprn.IPMirrorInterface	No access
webclient	No access
webclient.WebClientManager	Read/write
workspace	Read/write
workspace.WorkspaceManager.method_publicControl	No access

(3 of 3)

Table A-26 CPAM OSS PCA

Package.Class.Method/Property	Access
aclfilterli	No access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
calltrace.WebDAVSharedData	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.AuxiliaryDatabase.method_reinstantiationDatabase	No access
db.AuxiliaryDatabase.method_snapshotDatabase	No access

(1 of 4)

Package.Class.Method/Property	**Access**
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_snapshotAllDatabases	No access
db.DatabaseManager.method_switchover	No access
equipment.Shelf.method_rebootUpgrade	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
lte.ENBEquipment.method_launchNEM	No access
lte.LTEEquipment.method_launchQoSAnalyzer	No access
lteli.DFPeer	No access
lteli.DFPeerCardGroup	No access
lteli.InterceptionTarget	No access
lteli.LILteCfg	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
ltepolicyoptions	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
netw.AdvertisedNode	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_NetoAdminProfileBasedLaunch	No access
netw.NetworkElement.method_NetoViewerProfileBasedLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
oss	No access

(2 of 4)

Package.Class.Method/Property	Access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access

(3 of 4)

Package.Class.Method/Property	Access
sysact	No access
topology	Read/write
user	Read/write
vprn.IPMirrorInterface	No access
webclient	No access
webclient.WebClientManager	Read/write
workspace	Read/write
workspace.WorkspaceManager.method_publicControl	No access

(4 of 4)

Table A-27 CPAM Topology Simulator

Package.Class.Method/Property	Access
aclfilterli	No access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
calltrace.WebDAVSharedData	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.AuxiliaryDatabase.method_reinstantiationDatabase	No access
db.AuxiliaryDatabase.method_snapshotDatabase	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_snapshotAllDatabases	No access
db.DatabaseManager.method_switchover	No access
equipment.Shelf.method_rebootUpgrade	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access

(1 of 3)

Package.Class.Method/Property	**Access**
impact.PartialReset	No access
lte.ENBEquipment.method_launchNEM	No access
lte.LTEEquipment.method_launchQoSAnalyzer	No access
lteli.DFPeer	No access
lteli.DFPeerCardGroup	No access
lteli.InterceptionTarget	No access
lteli.LILteCfg	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
ltepolicyoptions	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
netw.AdvertisedNode	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_NetoAdminProfileBasedLaunch	No access
netw.NetworkElement.method_NetoViewerProfileBasedLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access

(2 of 3)

Package.Class.Method/Property	**Access**
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
simulator	Read/write
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
sysact	No access
topologysim	Read/write
user	Read/write
vprn.IPMirrorInterface	No access
webclient	No access
webclient.WebClientManager	Read/write
workspace	Read/write
workspace.WorkspaceManager.method_publicControl	No access

(3 of 3)

Table A-28 Root Cause Analysis (RCA) Object Verification

Package.Class.Method/Property	**Access**
aclfilterli	No access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
calltrace.WebDAVSharedData	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.AuxiliaryDatabase.method_reinstantiationDatabase	No access
db.AuxiliaryDatabase.method_snapshotDatabase	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_snapshotAllDatabases	No access
db.DatabaseManager.method_switchover	No access
equipment.Shelf.method_rebootUpgrade	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
lte.ENBEquipment.method_launchNEM	No access
lte.LTEEquipment.method_launchQoSAnalyzer	No access
lteli.DFPeer	No access
lteli.DFPeerCardGroup	No access
lteli.InterceptionTarget	No access
lteli.LILteCfg	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
ltepolicyoptions	No access

(1 of 3)

Package.Class.Method/Property	**Access**
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
netw.AdvertisedNode	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_NetoAdminProfileBasedLaunch	No access
netw.NetworkElement.method_NetoViewerProfileBasedLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca	Read/write
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access

(2 of 3)

Package.Class.Method/Property	Access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.ServiceMemberAuditPolicyEntry	Read/write
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
sysact	No access
user	Read/write
vprn.IPMirrorInterface	No access
webclient	No access
webclient.WebClientManager	Read/write
workspace	Read/write
workspace.WorkspaceManager.method_publicControl	No access

(3 of 3)

Table A-29 Lawful Intercept Management

Package.Class.Method/Property	Access
aclfilterli	Read/write
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
calltrace.WebDAVSharedData	No access
cflowd.NeCflowd	Read/write
cflowd.NeCollector	Read/write
cli	No access
cli.SSH	No access

(1 of 4)

Package.Class.Method/Property	Access
cli.Telnet	No access
db.AuxiliaryDatabase.method_reinstantiationDatabase	No access
db.AuxiliaryDatabase.method_snapshotDatabase	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_snapshotAllDatabases	No access
db.DatabaseManager.method_switchover	No access
equipment.Shelf.method_rebootUpgrade	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
lte	Read/write
lte.ENBEquipment.method_launchNEM	No access
lte.LTEEquipment.method_launchQoSAnalyzer	No access
lteli.DFPeer	Read/write
lteli.DFPeerCardGroup	Read/write
lteli.InterceptionTarget	Read/write
lteli.LILteCfg	Read/write
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
ltepolicyoptions	No access
mirror.Mirror	Read/write
mirror.Site	Read/write
mirrorli	Read/write
mmepolicy	No access
netw	Read/write
netw.AdvertisedNode	Read/write
netw.NetworkElement	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access

(2 of 4)

Package.Class.Method/Property	**Access**
netw.NetworkElement.method_NetoAdminProfileBasedLaunch	No access
netw.NetworkElement.method_NetoViewerProfileBasedLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.NodeDiscoveryControl	Read/write
netw.Topology	Read/write
netw.Topology.method_move	No access
netw.UplinkBofConfiguration	Read/write
netw.UplinkRouteConfiguration	Read/write
oss	No access
policy	Read/write
policy.PolicyDefinition.method_setConfigurationModeToReleased	Update/execute
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	Update/execute
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	Update/execute
policy.PolicySyncGroupManager	Read/write
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access

(3 of 4)

Package.Class.Method/Property	Access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
sitesec.LocalUser	Read/write
sitesec.UserProfile	Read/write
sitesec.UserPublicKey	Read/write
snmp.PollerManager	Read/write
snmp.PollerManager.method_resync	Update/execute
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
sysact	Read/write
user	Read/write
vprn.IPMirrorInterface	No access
webclient	No access
webclient.WebClientManager	Read/write
workspace	Read/write
workspace.WorkspaceManager.method_publicControl	No access

(4 of 4)

Table A-30 Template Script Management

Package.Class.Method/Property	Access
aclfilterli	No access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
calltrace.WebDAVSharedData	No access
cli	No access
cli.SSH	No access

(1 of 4)

Package.Class.Method/Property	Access
cli.Telnet	No access
db.AuxiliaryDatabase.method_reinstantiationDatabase	No access
db.AuxiliaryDatabase.method_snapshotDatabase	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_snapshotAllDatabases	No access
db.DatabaseManager.method_switchover	No access
equipment.Shelf.method_rebootUpgrade	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
lte.ENBEquipment.method_launchNEM	No access
lte.LTEEquipment.method_launchQoSAnalyzer	No access
lteli.DFPeer	No access
lteli.DFPeerCardGroup	No access
lteli.InterceptionTarget	No access
lteli.LILteCfg	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
ltepolicyoptions	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
netw.AdvertisedNode	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_NetoAdminProfileBasedLaunch	No access
netw.NetworkElement.method_NetoViewerProfileBasedLaunch	No access
netw.NetworkElement.method_executeCli	No access

(2 of 4)

Package.Class.Method/Property	**Access**
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
script	Read/write
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Bundle	Read/write
script.ControlScriptVersion	Read/write
script.HandlerBinding	Read/write
script.InvokerBinding	Read/write
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	Update/execute
script.ScriptManager.method_importBundle	Update/execute
script.ScriptManager.method_importBundleSimulation	Update/execute
script.TemplateBinding	Read/write
script.XmlApiConfigTemplate	Read/write
script.XmlApiConfigTemplate.method_execute	Update/execute
script.XmlApiConfigTemplate.method_executeMulti	Update/execute
script.XmlApiConfigTemplate.method_executeScript	Update/execute
script.XmlApiConfigTemplate.method_serviceTemplateExecute	Update/execute
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	Update/execute
script.XmlApiVersion	Read/write
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access

(3 of 4)

Package.Class.Method/Property	Access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
sysact	No access
user	Read/write
vprn.IPMirrorInterface	No access
webclient	No access
webclient.WebClientManager	Read/write
workspace	Read/write
workspace.WorkspaceManager.method_publicControl	No access

(4 of 4)

Table A-31 Service Template Script Execution

Package.Class.Method/Property	Access
aclfilterli	No access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
calltrace.WebDAVSharedData	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.AuxiliaryDatabase.method_reinstantiationDatabase	No access
db.AuxiliaryDatabase.method_snapshotDatabase	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access

(1 of 4)

Package.Class.Method/Property	**Access**
db.DatabaseManager.method_snapshotAllDatabases	No access
db.DatabaseManager.method_switchover	No access
equipment.Shelf.method_rebootUpgrade	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
lte.ENBEquipment.method_launchNEM	No access
lte.LTEEquipment.method_launchQoSAnalyzer	No access
lteli.DFPeer	No access
lteli.DFPeerCardGroup	No access
lteli.InterceptionTarget	No access
lteli.LILteCfg	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
ltepolicyoptions	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
netw.AdvertisedNode	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_NetoAdminProfileBasedLaunch	No access
netw.NetworkElement.method_NetoViewerProfileBasedLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access

(2 of 4)

Package.Class.Method/Property	**Access**
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	Update/execute
script.XmlApiConfigTemplate.method_executeMulti	Update/execute
script.XmlApiConfigTemplate.method_executeScript	Update/execute
script.XmlApiConfigTemplate.method_serviceTemplateExecute	Update/execute
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
sysact	No access
user	Read/write

(3 of 4)

Package.Class.Method/Property	Access
vprn.IPMirrorInterface	No access
webclient	No access
webclient.WebClientManager	Read/write
workspace	Read/write
workspace.WorkspaceManager.method_publicControl	No access

(4 of 4)

Table A-32 Tunnel Template Script Execution

Package.Class.Method/Property	Access
aclfilterli	No access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
calltrace.WebDAVSharedData	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.AuxiliaryDatabase.method_reinstantiationDatabase	No access
db.AuxiliaryDatabase.method_snapshotDatabase	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_snapshotAllDatabases	No access
db.DatabaseManager.method_switchover	No access
equipment.Shelf.method_rebootUpgrade	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
lte.ENBEquipment.method_launchNEM	No access
lte.LTEEquipment.method_launchQoSAnalyzer	No access

(1 of 3)

Package.Class.Method/Property	Access
lteli.DFPeer	No access
lteli.DFPeerCardGroup	No access
lteli.InterceptionTarget	No access
lteli.LILteCfg	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
ltepolicyoptions	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
netw.AdvertisedNode	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_NetoAdminProfileBasedLaunch	No access
netw.NetworkElement.method_NetoViewerProfileBasedLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access

(2 of 3)

Package.Class.Method/Property	Access
script.XmlApiConfigTemplate.method_execute	Update/execute
script.XmlApiConfigTemplate.method_executeMulti	Update/execute
script.XmlApiConfigTemplate.method_executeScript	Update/execute
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	Update/execute
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
sysact	No access
user	Read/write
vprn.IPMirrorInterface	No access
webclient	No access
webclient.WebClientManager	Read/write
workspace	Read/write
workspace.WorkspaceManager.method_publicControl	No access

(3 of 3)

Table A-33 Application Assurance (AA) Management

Package.Class.Method/Property	Access
aapolicy	Read/write
accounting	Read/write
aclfilterli	No access

(1 of 4)

Package.Class.Method/Property	**Access**
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
calltrace.WebDAVSharedData	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.AuxiliaryDatabase.method_reinstantiationDatabase	No access
db.AuxiliaryDatabase.method_snapshotDatabase	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_snapshotAllDatabases	No access
db.DatabaseManager.method_switchover	No access
equipment.Shelf.method_rebootUpgrade	No access
file	Read/write
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
lte.ENBEquipment.method_launchNEM	No access
lte.LTEEquipment.method_launchQoSAnalyzer	No access
lteli.DFPeer	No access
lteli.DFPeerCardGroup	No access
lteli.InterceptionTarget	No access
lteli.LILteCfg	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
ltepolicyoptions	No access

(2 of 4)

Package.Class.Method/Property	Access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
netw.AdvertisedNode	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_NetoAdminProfileBasedLaunch	No access
netw.NetworkElement.method_NetoViewerProfileBasedLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
oss	No access
policy	Read/write
policy.PolicyDefinition.method_setConfigurationModeToReleased	Update/execute
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	Update/execute
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	Update/execute
policy.PolicySyncGroupManager	Read/write
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
schedule	Read/write
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access

(3 of 4)

Package.Class.Method/Property	Access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
sysact	No access
user	Read/write
vprn.IPMirrorInterface	No access
webclient	No access
webclient.WebClientManager	Read/write
workspace	Read/write
workspace.WorkspaceManager.method_publicControl	No access

(4 of 4)

Table A-34 Format and Range Policy Management

Package.Class.Method/Property	Access
aclfilterli	No access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
calltrace.WebDAVSharedData	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access

(1 of 4)

Package.Class.Method/Property	**Access**
db.AuxiliaryDatabase.method_reinstantiationDatabase	No access
db.AuxiliaryDatabase.method_snapshotDatabase	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_snapshotAllDatabases	No access
db.DatabaseManager.method_switchover	No access
equipment.Shelf.method_rebootUpgrade	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
lte.ENBEquipment.method_launchNEM	No access
lte.LTEEquipment.method_launchQoSAnalyzer	No access
lteli.DFPeer	No access
lteli.DFPeerCardGroup	No access
lteli.InterceptionTarget	No access
lteli.LILteCfg	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
ltepolicyoptions	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
netw.AdvertisedNode	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_NetoAdminProfileBasedLaunch	No access
netw.NetworkElement.method_NetoViewerProfileBasedLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access

(2 of 4)

Package.Class.Method/Property	Access
netw.Topology.method_move	No access
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
propertyrules	Read/write
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
spanrules	Read/write

(3 of 4)

Package.Class.Method/Property	**Access**
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
sysact	No access
user	Read/write
vprn.IPMirrorInterface	No access
webclient	No access
webclient.WebClientManager	Read/write
workspace	Read/write
workspace.WorkspaceManager.method_publicControl	No access

(4 of 4)

Table A-35 Work Order Activation

Package.Class.Method/Property	**Access**
aclfilterli	No access
activation	Read/write
activation.Session	Read/write
activation.WebDAVSharedData	Read/write
activation.WorkOrder	Read/write
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
calltrace.WebDAVSharedData	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.AuxiliaryDatabase.method_reinstantiationDatabase	No access
db.AuxiliaryDatabase.method_snapshotDatabase	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_snapshotAllDatabases	No access
db.DatabaseManager.method_switchover	No access
equipment.Shelf.method_rebootUpgrade	No access
filter	Read/write

(1 of 4)

Package.Class.Method/Property	**Access**
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
fr	Read/write
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
ies	Read/write
impact.FullReset	Read/write
impact.PartialReset	Read/write
lte	Read/update/execute
lte.ENBEquipment.method_launchNEM	No access
lte.LTEEquipment.method_launchQoSAnalyzer	No access
lte.SubscAndEquipmentTraces	Read/write
lteli.DFPeer	No access
lteli.DFPeerCardGroup	No access
lteli.InterceptionTarget	No access
lteli.LILteCfg	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
ltepolicyoptions	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
netw.AdvertisedNode	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_NetoAdminProfileBasedLaunch	No access
netw.NetworkElement.method_NetoViewerProfileBasedLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access

(2 of 4)

Package.Class.Method/Property	**Access**
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
ppp	Read/write
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	Read/write
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
sysact	No access

(3 of 4)

Package.Class.Method/Property	Access
user	Read/write
vprn.IPMirrorInterface	No access
webclient	No access
webclient.WebClientManager	Read/write
workspace	Read/write
workspace.WorkspaceManager.method_publicControl	No access

(4 of 4)

Table A-36 Configuration Snapshot Export

Package.Class.Method/Property	Access
aclfilterli	No access
activation.Snapshot	Read/write
activation.SnapshotEntity	Read/write
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
calltrace.WebDAVSharedData	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.AuxiliaryDatabase.method_reinstantiationDatabase	No access
db.AuxiliaryDatabase.method_snapshotDatabase	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_snapshotAllDatabases	No access
db.DatabaseManager.method_switchover	No access
equipment.Shelf.method_rebootUpgrade	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access

(1 of 3)

Package.Class.Method/Property	Access
lte.ENBEquipment.method_launchNEM	No access
lte.LTEEquipment.method_launchQoSAnalyzer	No access
lteli.DFPeer	No access
lteli.DFPeerCardGroup	No access
lteli.InterceptionTarget	No access
lteli.LILteCfg	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
ltepolicyoptions	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
netw.AdvertisedNode	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_NetoAdminProfileBasedLaunch	No access
netw.NetworkElement.method_NetoViewerProfileBasedLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access

(2 of 3)

Package.Class.Method/Property	Access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
sysact	No access
user	Read/write
vprn.IPMirrorInterface	No access
webclient	No access
webclient.WebClientManager	Read/write
workspace	Read/write
workspace.WorkspaceManager.method_publicControl	No access

(3 of 3)

Table A-37 Create and Delete Access

Package.Class.Method/Property	Access
aclfilterli	No access

(1 of 4)

Package.Class.Method/Property	**Access**
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
calltrace.WebDAVSharedData	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.AuxiliaryDatabase.method_reinstantiationDatabase	No access
db.AuxiliaryDatabase.method_snapshotDatabase	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_snapshotAllDatabases	No access
db.DatabaseManager.method_switchover	No access
equipment.Shelf.method_rebootUpgrade	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
lte.ENBEquipment.method_launchNEM	No access
lte.LTEEquipment.method_launchQoSAnalyzer	No access
lteli.DFPeer	No access
lteli.DFPeerCardGroup	No access
lteli.InterceptionTarget	No access
lteli.LILteCfg	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
ltepolicyoptions	No access
mirror	No access

(2 of 4)

Package.Class.Method/Property	Access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
netw.AdvertisedNode	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_NetoAdminProfileBasedLaunch	No access
netw.NetworkElement.method_NetoViewerProfileBasedLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	Read/write
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access

(3 of 4)

Package.Class.Method/Property	**Access**
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
sysact	No access
user	Read/write
vprn.IPMirrorInterface	No access
webclient	No access
webclient.WebClientManager	Read/write
workspace	Read/write
workspace.WorkspaceManager.method_publicControl	No access

(4 of 4)

Table A-38 Configuration Management which causes node reset

Package.Class.Method/Property	**Access**
aclfilterli	No access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
calltrace.WebDAVSharedData	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.AuxiliaryDatabase.method_reinstantiationDatabase	No access
db.AuxiliaryDatabase.method_snapshotDatabase	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access

(1 of 4)

Package.Class.Method/Property	Access
db.DatabaseManager.method_snapshotAllDatabases	No access
db.DatabaseManager.method_switchover	No access
equipment.Shelf.method_rebootUpgrade	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	Read/write
impact.PartialReset	Read/write
lte.ENBEquipment.method_launchNEM	No access
lte.LTEEquipment.method_launchQoSAnalyzer	No access
lteli.DFPeer	No access
lteli.DFPeerCardGroup	No access
lteli.InterceptionTarget	No access
lteli.LILteCfg	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
ltepolicyoptions	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
netw.AdvertisedNode	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_NetoAdminProfileBasedLaunch	No access
netw.NetworkElement.method_NetoViewerProfileBasedLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access

(2 of 4)

Package.Class.Method/Property	**Access**
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
sysact	No access
user	Read/write

(3 of 4)

Package.Class.Method/Property	Access
vprn.IPMirrorInterface	No access
webclient	No access
webclient.WebClientManager	Read/write
workspace	Read/write
workspace.WorkspaceManager.method_publicControl	No access

(4 of 4)

Table A-39 EPC Operator

Package.Class.Method/Property	Access
aclfilterli	No access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
calltrace.WebDAVSharedData	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.AuxiliaryDatabase.method_reinstantiationDatabase	No access
db.AuxiliaryDatabase.method_snapshotDatabase	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_snapshotAllDatabases	No access
db.DatabaseManager.method_switchover	No access
equipment.Shelf.method_rebootUpgrade	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
isa.MgGroupMember	Read/write
isa.MgIsaGroup	Read/write

(1 of 6)

Package.Class.Method/Property	**Access**
lte	Read/write
lte.ApnPolicyRuleBase	Read/write
lte.DccaProfile	Read/write
lte.DiameterPeerListEntry	Read/write
lte.DiameterPeerProfile	Read/write
lte.DiameterProfile	Read/write
lte.DiscoveryLog	Read/write
lte.DupRadiusAccServerGroup	Read/write
lte.ENBEquipment.method_launchNEM	No access
lte.EPSPathDiscoveredLinkComponent	Read/write
lte.EPSPathDiscoveryHint	Read/write
lte.EPSPathDiscoveryProfile	Read/write
lte.EPSPathInterfaceComponent	Read/write
lte.EPSPathLinkComponent	Read/write
lte.EPSPathSapComponent	Read/write
lte.EPSPathSegment	Read/write
lte.EPSPathServiceComponent	Read/write
lte.EPSPathSiteComponent	Read/write
lte.GtpPrimaryServerListEntry	Read/write
lte.GtpPrimeServerGroupProfile	Read/write
lte.GtpProfile	Read/write
lte.IpPool	Read/write
lte.IpPoolBinding	Read/write
lte.IpPoolEntry	Read/write
lte.LTEEquipment.method_launchQoSAnalyzer	No access
lte.MobileNodeRegion	Read/write
lte.PDNGateway	Read/write
lte.PdnApn	Read/write
lte.PdnGxReferencePoint	Read/write
lte.PdnRfReferencePoint	Read/write
lte.PdnS5ReferencePoint	Read/write
lte.PdnS8ReferencePoint	Read/write
lte.PdnSignalling	Read/write
lte.PgwChargingProfile	Read/write
lte.PlmnListPolicy	Read/write
lte.PlmnListPolicyGroup	Read/write
lte.QciPolicy	Read/write

(2 of 6)

Package.Class.Method/Property	**Access**
lte.QciPolicyEntry	Read/write
lte.S11ReferencePoint	Read/write
lte.S1uReferencePoint	Read/write
lte.ServingGateway	Read/write
lte.SgwApn	Read/write
lte.SgwChargingProfile	Read/write
lte.SgwRfReferencePoint	Read/write
lte.SgwS5ReferencePoint	Read/write
lte.SgwS8ReferencePoint	Read/write
lte.SgwSignalling	Read/write
lte.TrustedPeerListEntry	Read/write
lte.TrustedPeerListEntryUnlisted	Read/write
lte.TrustedPeerListPolicy	Read/write
lteggsn	Read/write
lteggsn.CdrAvpOptionProfile	Read/write
lteggsn.DccaRatingGroup	Read/write
lteggsn.GnReferencePoint	Read/write
lteggsn.GpReferencePoint	Read/write
lteggsn.GyAvpOptionProfile	Read/write
lteggsn.PdnGyReferencePoint	Read/write
lteggsn.PgwGaReferencePoint	Read/write
lteggsn.SgwGaReferencePoint	Read/write
ltegw	Read/write
ltegw.ApnListPolicy	Read/write
ltegw.ApnListPolicyGroup	Read/write
ltegw.DiameterPeerRedirHostEntry	Read/write
ltegw.DiameterPeerSupportedHost	Read/write
ltegw.PcscfGroupProfile	Read/write
ltegw.PcscfPeerEntry	Read/write
ltegw.PcscfResolvedPeerIPEntry	Read/write
ltegw.SCTPProfile	Read/write
ltegw.UMTSQoSPolicy	Read/write
lteli.DFPeer	No access
lteli.DFPeerCardGroup	No access
lteli.InterceptionTarget	No access
lteli.LILteCfg	No access
ltemme	Read/write

(3 of 6)

Package.Class.Method/Property	Access
ltemme.MmeInstance.method_abortMmeLoadBalance	Update/execute
ltemme.MmeInstance.method_interMmeLoadBalance	Update/execute
ltemme.MmeInstance.method_intraMmeLoadBalance	Update/execute
ltemme.MmeInstance.method_lockMmeAggregateService	Update/execute
ltemme.MmeInstance.method_unlockMmeAggregateService	Update/execute
ltepmip	Read/write
ltepmip.S2aReferencePoint	Read/write
ltepmip.S2bReferencePoint	Read/write
ltepmip.S6bAvpOptionProfile	Read/write
ltepmip.S6bReferencePoint	Read/write
ltepolicyoptions	No access
ltepolicyoptions.AsoOptions	Read/write
ltepolicyoptions.ChargingRuleUnit	Read/write
ltepolicyoptions.DhcpSGPeerEntry	Read/write
ltepolicyoptions.DhcpServerGroupProfile	Read/write
ltepolicyoptions.GxAvpOptionProfile	Read/write
ltepolicyoptions.PolRuleUnitFlwDescription	Read/write
ltepolicyoptions.PolicyRule	Read/write
ltepolicyoptions.PolicyRuleBase	Read/write
ltepolicyoptions.PolicyRuleBaseEntry	Read/write
ltepolicyoptions.PolicyRuleUnit	Read/write
ltepolicyoptions.ServiceClassIndicator	Read/write
ltepolicyoptions.TrafficRedirectProfile	Read/write
ltepolicyoptions.TrafficRedirectTarget	Read/write
ltepool	Read/write
ltepool.MmeInstanceBinding	Read/write
ltepool.TaBinding	Read/write
lteradius.RadiusGroupProfile	Read/write
lteradius.RadiusPeerProfile	Read/write
lteradius.RadiusProfile	Read/write
ltesgsn.SgwS12ReferencePoint	Read/write
ltesgsn.SgwS4ReferencePoint	Read/write
ltethreshold	Read/write
lteuserstats.UserStatsQuery	Read/write
lteuserstats.UserStatsQueryOutputSnapshot	Read/write
lteuserstats.UserStatsUserPgw	Read/write
lteuserstats.UserStatsUserSgw	Read/write

(4 of 6)

Package.Class.Method/Property	**Access**
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
mmepolicy.MMEEmergencyNumListPolicy	Read/write
mmepolicy.MMEGTPProfile	Read/write
mmepolicy.MMESCTPProfile	Read/write
mmepolicy.WMMPfmJobEntry	Read/write
mmepolicy.WMMPfmJobMts	Read/write
mmepolicy.WMMPfmJobSched	Read/write
mmepolicy.WMMPfmMeasGroupName	Read/write
mmepolicy.WMMPfmMeasGroups	Read/write
netw.AdvertisedNode	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_NetoAdminProfileBasedLaunch	No access
netw.NetworkElement.method_NetoViewerProfileBasedLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
oss	No access
policy	Read/write
policy.PolicyDefinition.method_setConfigurationModeToReleased	Update/execute
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	Update/execute
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	Update/execute
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access

(5 of 6)

Package.Class.Method/Property	Access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
sysact	No access
user	Read/write
vprn.IPMirrorInterface	No access
webclient	No access
webclient.WebClientManager	Read/write
workspace	Read/write
workspace.WorkspaceManager.method_publicControl	No access

(6 of 6)

Table A-40 eNodeB NEM Operator

Package.Class.Method/Property	Access
aclfilterli	No access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access

(1 of 4)

Package.Class.Method/Property	**Access**
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
calltrace.WebDAVSharedData	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.AuxiliaryDatabase.method_reinstantiationDatabase	No access
db.AuxiliaryDatabase.method_snapshotDatabase	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_snapshotAllDatabases	No access
db.DatabaseManager.method_switchover	No access
equipment.Shelf.method_rebootUpgrade	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
lte.ENBEquipment.method_launchNEM	Update/execute
lte.LTEEquipment.method_launchQoSAnalyzer	No access
lteli.DFPeer	No access
lteli.DFPeerCardGroup	No access
lteli.InterceptionTarget	No access
lteli.LILteCfg	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
ltepolicyoptions	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access

(2 of 4)

Package.Class.Method/Property	**Access**
netw.AdvertisedNode	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_NetoAdminProfileBasedLaunch	No access
netw.NetworkElement.method_NetoViewerProfileBasedLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access

(3 of 4)

Package.Class.Method/Property	Access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
sysact	No access
udptunnel	Read/write
user	Read/write
vprn.IPMirrorInterface	No access
webclient	No access
webclient.WebClientManager	Read/write
workspace	Read/write
workspace.WorkspaceManager.method_publicControl	No access

(4 of 4)

Table A-41 Statistics Plotter Profile Management

Package.Class.Method/Property	Access
aclfilterli	No access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
calltrace.WebDAVSharedData	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.AuxiliaryDatabase.method_reinstantiationDatabase	No access
db.AuxiliaryDatabase.method_snapshotDatabase	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_snapshotAllDatabases	No access
db.DatabaseManager.method_switchover	No access
equipment.Shelf.method_rebootUpgrade	No access

(1 of 4)

Package.Class.Method/Property	**Access**
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
lte.ENBEquipment.method_launchNEM	No access
lte.LTEEquipment.method_launchQoSAnalyzer	No access
lteli.DFPeer	No access
lteli.DFPeerCardGroup	No access
lteli.InterceptionTarget	No access
lteli.LILteCfg	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
ltepolicyoptions	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
netw.AdvertisedNode	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_NetoAdminProfileBasedLaunch	No access
netw.NetworkElement.method_NetoViewerProfileBasedLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access

(2 of 4)

Package.Class.Method/Property	Access
resources	No access
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
statsplot	Read/write
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
sysact	No access
user	Read/write
vprn.IPMirrorInterface	No access
webclient	No access

(3 of 4)

Package.Class.Method/Property	Access
webclient.WebClientManager	Read/write
workspace	Read/write
workspace.WorkspaceManager.method_publicControl	No access

(4 of 4)

Table A-42 Admin Neto Launch

Package.Class.Method/Property	Access
aclfilterli	No access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
calltrace.WebDAVSharedData	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.AuxiliaryDatabase.method_reinstantiationDatabase	No access
db.AuxiliaryDatabase.method_snapshotDatabase	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_snapshotAllDatabases	No access
db.DatabaseManager.method_switchover	No access
equipment.Shelf.method_rebootUpgrade	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
lte.ENBEquipment.method_launchNEM	No access
lte.LTEEquipment.method_launchQoSAnalyzer	No access
lteli.DFPeer	No access
lteli.DFPeerCardGroup	No access

(1 of 3)

Package.Class.Method/Property	**Access**
lteli.InterceptionTarget	No access
lteli.LILteCfg	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
ltepolicyoptions	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
netw.AdvertisedNode	Read/write
netw.NetworkElement.method_GUICrossLaunch	Update/execute
netw.NetworkElement.method_NetoAdminProfileBasedLaunch	Update/execute
netw.NetworkElement.method_NetoViewerProfileBasedLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access

(2 of 3)

Package.Class.Method/Property	**Access**
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
sysact	No access
user	Read/write
vprn.IPMirrorInterface	No access
webclient	No access
webclient.WebClientManager	Read/write
workspace	Read/write
workspace.WorkspaceManager.method_publicControl	No access

(3 of 3)

Table A-43 Viewer Neto Launch

Package.Class.Method/Property	**Access**
aclfilterli	No access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access

(1 of 4)

Package.Class.Method/Property	**Access**
bulk.BulkManager.method_generateBatches	No access
calltrace.WebDAVSharedData	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.AuxiliaryDatabase.method_reinstantiationDatabase	No access
db.AuxiliaryDatabase.method_snapshotDatabase	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_snapshotAllDatabases	No access
db.DatabaseManager.method_switchover	No access
equipment.Shelf.method_rebootUpgrade	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
lte.ENBEquipment.method_launchNEM	No access
lte.LTEEquipment.method_launchQoSAnalyzer	No access
lteli.DFPeer	No access
lteli.DFPeerCardGroup	No access
lteli.InterceptionTarget	No access
lteli.LILteCfg	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
ltepolicyoptions	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
netw.AdvertisedNode	Read/write

(2 of 4)

Package.Class.Method/Property	**Access**
netw.NetworkElement.method_GUICrossLaunch	Update/execute
netw.NetworkElement.method_NetoAdminProfileBasedLaunch	No access
netw.NetworkElement.method_NetoViewerProfileBasedLaunch	Update/execute
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access

(3 of 4)

Package.Class.Method/Property	Access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
sysact	No access
user	Read/write
vprn.IPMirrorInterface	No access
webclient	No access
webclient.WebClientManager	Read/write
workspace	Read/write
workspace.WorkspaceManager.method_publicControl	No access

(4 of 4)

Table A-44 Default Neto Launch

Package.Class.Method/Property	Access
aclfilterli	No access
activation.WebDAVSharedData	No access
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
calltrace.WebDAVSharedData	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.AuxiliaryDatabase.method_reinstantiationDatabase	No access
db.AuxiliaryDatabase.method_snapshotDatabase	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_snapshotAllDatabases	No access
db.DatabaseManager.method_switchover	No access
equipment.Shelf.method_rebootUpgrade	No access
filter	Read/write

(1 of 4)

Package.Class.Method/Property	**Access**
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
lte.ENBEquipment.method_launchNEM	No access
lte.LTEEquipment.method_launchQoSAnalyzer	No access
lteli.DFPeer	No access
lteli.DFPeerCardGroup	No access
lteli.InterceptionTarget	No access
lteli.LILteCfg	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
ltepolicyoptions	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
netw.AdvertisedNode	Read/write
netw.NetworkElement.method_GUICrossLaunch	Update/execute
netw.NetworkElement.method_NetoAdminProfileBasedLaunch	No access
netw.NetworkElement.method_NetoViewerProfileBasedLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access

(2 of 4)

Package.Class.Method/Property	**Access**
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
sysact	No access
user	Read/write
vprn.IPMirrorInterface	No access
webclient	No access
webclient.WebClientManager	Read/write
workspace	Read/write

(3 of 4)

Package.Class.Method/Property	Access
workspace.WorkspaceManager.method_publicControl	No access

(4 of 4)

Table A-45 Ageout Constraint Policy Management

Package.Class.Method/Property	Access
aclfilterli	No access
activation.WebDAVSharedData	No access
ageoutcstr	Read/write
autoconfig.AutoConfigScriptManager.method_configure	No access
autoconfig.AutoConfigScriptManager.method_copyContents	No access
bulk.BulkManager.method_execute	No access
bulk.BulkManager.method_generateBatches	No access
calltrace.WebDAVSharedData	No access
cli	No access
cli.SSH	No access
cli.Telnet	No access
db.AuxiliaryDatabase.method_reinstantiationDatabase	No access
db.AuxiliaryDatabase.method_snapshotDatabase	No access
db.DatabaseManager.method_backup	No access
db.DatabaseManager.method_reinstantiateStandby	No access
db.DatabaseManager.method_snapshotAllDatabases	No access
db.DatabaseManager.method_switchover	No access
equipment.Shelf.method_rebootUpgrade	No access
filter	Read/write
fm.AlarmHistoryDatabase.method_purge	No access
fm.FaultManager.method_editNote	No access
generic	Read/write
generic.GenericObject.method_collectData	No access
hpipe	No access
impact.FullReset	No access
impact.PartialReset	No access
lte.ENBEquipment.method_launchNEM	No access
lte.LTEEquipment.method_launchQoSAnalyzer	No access
lteli.DFPeer	No access
lteli.DFPeerCardGroup	No access
lteli.InterceptionTarget	No access

(1 of 3)

Package.Class.Method/Property	**Access**
lteli.LILteCfg	No access
ltemme.MmeInstance.method_abortMmeLoadBalance	No access
ltemme.MmeInstance.method_interMmeLoadBalance	No access
ltemme.MmeInstance.method_intraMmeLoadBalance	No access
ltemme.MmeInstance.method_lockMmeAggregateService	No access
ltemme.MmeInstance.method_unlockMmeAggregateService	No access
ltepolicyoptions	No access
mirror	No access
mirror.Mirror	No access
mirror.Site	No access
mmepolicy	No access
netw.AdvertisedNode	Read/write
netw.NetworkElement.method_GUICrossLaunch	No access
netw.NetworkElement.method_NetoAdminProfileBasedLaunch	No access
netw.NetworkElement.method_NetoViewerProfileBasedLaunch	No access
netw.NetworkElement.method_executeCli	No access
netw.NetworkElement.method_executeMultiCli	No access
netw.Topology.method_move	No access
oss	No access
policy.PolicyDefinition.method_setConfigurationModeToReleased	No access
policy.PolicyDefinition.method_setDistributionModeToLocalEditOnly	No access
policy.PolicyDefinition.method_setDistributionModeToSyncWithGlobal	No access
rca.RcaManager.method_fixProblem	No access
rca.RcaManager.method_preFixProblem	No access
resources	No access
script.AbstractScript.method_configureTarget	No access
script.AbstractScript.method_configureTargets	No access
script.Script.method_createTargetScript	No access
script.Script.method_createTargetScripts	No access
script.ScriptManager.method_configure	No access
script.ScriptManager.method_copyContents	No access
script.ScriptManager.method_exportBundle	No access
script.ScriptManager.method_importBundle	No access
script.ScriptManager.method_importBundleSimulation	No access
script.XmlApiConfigTemplate.method_execute	No access
script.XmlApiConfigTemplate.method_executeMulti	No access
script.XmlApiConfigTemplate.method_executeScript	No access

(2 of 3)

Package.Class.Method/Property	**Access**
script.XmlApiConfigTemplate.method_serviceTemplateExecute	No access
script.XmlApiConfigTemplate.method_tunnelTemplateExecute	No access
security.CpamLicense.method_clearRouterLimitExceedDueToMultiAdditions	No access
security.MediationPolicy	No access
security.RoleBasedAccess	No access
security.ScopeOfCommandProfile	No access
security.ScopeOfCommandRole	No access
security.SpanOfControlProfile	No access
security.User	No access
security.UserGroup	No access
service.Service.method_create	No access
service.Service.method_highPriorityServiceDelete	No access
service.TemplateService.method_constructServiceTemplate	No access
service.TemplateService.method_constructTemplatedService	No access
snmp.PollerManager.method_resync	No access
srmrmtauth	No access
svt.MirrorSdpBinding	No access
sw.BackupRestoreManager.method_backup	No access
sw.BackupRestoreManager.method_restore	No access
sysact	No access
user	Read/write
vprn.IPMirrorInterface	No access
webclient	No access
webclient.WebClientManager	Read/write
workspace	Read/write
workspace.WorkspaceManager.method_publicControl	No access

(3 of 3)

Release 12.0 R2 | May 2014 | 3HE 08861 AAAB TQZZA Edition 01

Customer documentation and product support

Customer documentation

http://www.alcatel-lucent.com/myaccess

Product manuals and documentation updates are available at alcatel-lucent.com. If you are a new user and require access to this service, please contact your Alcatel-Lucent sales representative.

Technical Support

http://support.alcatel-lucent.com

Documentation feedback

documentation.feedback@alcatel-lucent.com

Release 12.0 R2 | May 2014 | 3HE 08861 AAAB TQZZA Edition 01

Alcatel·Lucent

© 2014 Alcatel-Lucent. All rights reserved.

www.alcatel-lucent.com