Alcatel-Lucent 5620

SERVICE AWARE MANAGER

INTEGRATION 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

Preface **ix**

Prerequisites ix
5620 SAM documentation suite ix
Obtaining customer documentation xiii
On-product documentation xiii
Documentation and resources on the web xiii
Documentation conventions xiv
Procedures with options or substeps xiv
Measurement conventions xv
Important information xvi

Integration configuration

1 — 5620 SAM integration overview **1-1**

1.1 Introduction 1-2
1.2 Integration overview 1-2
Integration with other systems 1-2
Integration with Single Sign On 1-2
Integration with CFMA 1-2

2 — 5620 SAM integration with other systems **2-1**

2.1 5620 SAM integration overview 2-3
2.2 5620 SAM and 5650 CPAM integration 2-3
5650 CPAM deployment 2-3
5650 CPAM menus 2-4

2.3 Workflow for 5620 SAM and 5650 CPAM integration 2-5
2.4 5620 SAM and 5650 CPAM integration procedures 2-6
Procedure 2-1 To add the 5650 CPAM to a 5620 SAM system 2-6
2.5 5620 SAM and 5620 NM integration 2-7
Before you start 2-8
5620 SAM client GUI startup and navigation restrictions 2-8
2.6 Workflow for 5620 SAM and 5620 NM integration 2-9
2.7 5620 SAM and 5620 NM integration procedures 2-9
Procedure 2-2 To configure 5620 SAM and 5620 NM GUI integration 2-9
Procedure 2-3 To enable navigation from external systems on a 5620 SAM main server 2-12
Procedure 2-4 To start the 5620 NM GUI 2-13
Procedure 2-5 To navigate from the 5620 NM AS tool USM to the 5620 SAM client GUI 2-13
2.8 5620 SAM and 9959 NPO integration 2-14
9959 NPO redundancy 2-15
File transfer between the 5620 SAM and the 9959 NPO 2-15
East-West licensing for the 9959 NPO 2-15
2.9 5620 SAM and 9959 NPO integration procedures 2-16
Procedure 2-6 To discover the 9959 NPO as an EM system 2-16
Procedure 2-7 To unmanage and delete the 9959 NPO from the 5620 SAM network 2-18
2.10 5620 SAM and EM systems integration 2-18
2.11 5620 SAM and 5670 RAM integration 2-19
Procedure 2-8 To enable 5670 RAM support 2-19
2.12 5620 SAM and 9952 WPS integration 2-20
File transfer between the 5620 SAM and the 9952 WPS 2-20
Procedure 2-9 To view WebDAV activation status on a 5620 SAM main server 2-21
2.13 5620 SAM and 5780 DSC integration 2-21
2.14 5620 SAM and 5750 SSC integration 2-22
2.15 5620 SAM and 5520 AMS integration 2-23
2.16 Call trace data transfer to the 9958 WTA 2-24

3 — 5620 SAM integration with Single Sign On 3-1

3.1 SSO integration 3-2
3.2 SSO integration procedures 3-2
Procedure 3-1 To configure 5620 SAM and LSM portal integration 3-2
Procedure 3-2 To configure 5620 SAM integration with a system that uses the LSM portal 3-4
Procedure 3-3 To configure 5620 SAM and SANE portal integration 3-5
Procedure 3-4 To enable SSO between 5620 SAM and an identity provider using v1.1 SAML artifacts 3-9

4 — 5620 SAM integration with CFMA 4-1

4.1 CFMA integration overview 4-2
4.2 CFMA integration procedures 4-2
Procedure 4-1 Installing the SAM-CFMA adapter sar file 4-2
Procedure 4-2 Setting CFMA preferences 4-3
Procedure 4-3 Enabling 5620 SAM server communication 4-3

Integration configuration

1 — 5620 SAM integration overview

2 — 5620 SAM integration with other systems

3 — 5620 SAM integration with Single Sign On

4 — 5620 SAM integration with CFMA

1 — 5620 SAM integration overview

1.1 Introduction *1-2*

1.2 Integration overview *1-2*

1.1 Introduction

The *5620 SAM Integration Guide* describes several configurations that allow the 5620 SAM to integrate with other systems. Integration is achieved in a variety of ways depending on the components involved and a user's specific configuration. For example, a horizontal integration protocol is often used to provide east-west integration between products.

Visit the chapter pertaining to a specific solution to see how integration is accomplished in that scenario.

1.2 Integration overview

The *5620 SAM Integration Guide* contains information about integrating the 5620 SAM with systems that offer additional functionality. This includes both third-party, and Alcatel-Lucent systems. The 5620 SAM can also be integrated with systems that augment the behavior of previously-integrated systems, such as Single Sign On and CFMA.

Integration with other systems

A 5620 SAM system operates interactively with other systems to provide additional functionality and increased ease of use. Depending on the type of integration, the interface of one system can be used to perform functions on, or retrieve information from, the other system.

See chapter 2 for more information.

Integration with Single Sign On

Single Sign On (SSO) technology enables a user to access all resources within a given domain after having entered their credentials just one time.

See chapter 3 for more information.

Integration with CFMA

The SAM-CFMA adapter for CFMA translates 5620 SAM alarms into alarms for CFMA. Using CFMA as a fault manager, the adapter is used to aggregate 5620 SAM alarms within another NM.

The adapter connects to 5620 SAM using SAM-O and JMS. The adapter software can be found in the integration/samcfmadapter directory of the 5620 SAM installation DVD.

See chapter 4 for more information.

2 — 5620 SAM integration with other systems

2.1 5620 SAM integration overview *2-3*

2.2 5620 SAM and 5650 CPAM integration *2-3*

2.3 Workflow for 5620 SAM and 5650 CPAM integration *2-5*

2.4 5620 SAM and 5650 CPAM integration procedures *2-6*

2.5 5620 SAM and 5620 NM integration *2-7*

2.6 Workflow for 5620 SAM and 5620 NM integration *2-9*

2.7 5620 SAM and 5620 NM integration procedures *2-9*

2.8 5620 SAM and 9959 NPO integration *2-14*

2.9 5620 SAM and 9959 NPO integration procedures *2-16*

2.10 5620 SAM and EM systems integration *2-18*

2.11 5620 SAM and 5670 RAM integration *2-19*

2.12 5620 SAM and 9952 WPS integration *2-20*

2.13 5620 SAM and 5780 DSC integration *2-21*

2.14 5620 SAM and 5750 SSC integration *2-22*

2.15 5620 SAM and 5520 AMS integration ***2-23***

2.16 Call trace data transfer to the 9958 WTA ***2-24***

2.1 5620 SAM integration overview

You can integrate the 5620 SAM with a variety of other systems. Integration allows the 5620 SAM to provide a broader range of management functions from a single GUI. This chapter describes the configuration of different integration scenarios.

2.2 5620 SAM and 5650 CPAM integration

The 5650 CPAM provides real-time control-plane IGP and BGP topology capture, inspection, visualization, and troubleshooting. The 5650 CPAM can be integrated with the 5620 SAM, or installed as an independent system. Integration allows the 5650 CPAM to associate routing information with 5620 SAM network routes, service tunnels, LSPs, edge-to-edge service traffic paths, and OAM tests.

When the 5650 CPAM software is enabled on a 5620 SAM system, the 5650 CPAM functions are available from the 5620 SAM main menu. See the *5650 CPAM User Guide* for more information.

The 5650 CPAM provides a tight eastbound and westbound integration with the 5620 SAM. This integration allows for a real-time view of the network including routing topology and associated configurations whether performed on the GUI, OSS interface, or by CLI. The 5650 CPAM can leverage 5620 SAM redundancy and offer tight navigation between protocol maps and 5620 SAM-managed objects, such as protocol links. In addition, the 5620 SAM GUI supports the management of the 7701 CPAA platform.

When the 5650 CPAM and the 5620 SAM share the same database, the 5650 CPAM can access objects managed by 5620 SAM and display them on the 5650 CPAM topology views. Without integration with the 5620 SAM, the following functions are not available:

- service, LSP, multicast, and OAM highlights
- historical LSP active paths
- LDP and RSVP interface display on the MPLS view
- auto-OAM function that uses STM test policies for IP and LSP path monitors

The 5650 CPAM route controller, or server, communicates with GUI and OSS clients using the same API as the 5620 SAM. When the 5650 CPAM route controller is integrated with a 5620 SAM, the 5620 SAM and 5650 CPAM releases must be compatible. In addition, the 5650 CPAM route controller can run independently with one or multiple 5620 SAM servers.

5650 CPAM deployment

The 5650 CPAM system requirements are the same as the 5620 SAM main server requirements. The *5620 SAM Planning Guide* contains information such as platform specifications, scaling guidelines, and network requirements. The *5620 SAM | 5650 CPAM Installation and Upgrade Guide* contains deployment information such as the following:

- deployment considerations
- integration with the 5620 SAM during main server installation or upgrade

- independent installation and upgrade as a standalone or redundant system
- uninstallation

5650 CPAM integration with the 5620 SAM requires a license file in compressed format. Alcatel-Lucent generates a 5650 CPAM license file based on the system ID of the station that is to host the software. See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for information about how to obtain the system ID of a station.

Note 1 — The Alcatel-Lucent Software License Manager, or ASLM, accepts only the UUID of a station as the system ID.

Note 2 — The license files of 5620 SAM and 5650 CPAM servers that share a station must be generated using the same system ID.

You can specify the inclusion of an integrated 5650 CPAM server during a 5620 SAM main server installation or upgrade. See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for more information.

You can integrate the 5650 CPAM with an existing 5620 SAM main server by importing the 5650 CPAM license file to the main server configuration. The 5650 CPAM client GUI functions are not enabled until you restart the client. See Procedure 2-1 for more information.

5650 CPAM menus

The following 5650 CPAM menu items do not display, or are disabled, if the 5650 CPAM license is not enabled. See the *5650 CPAM User Guide* for more information.

Table 2-1 describes the 5650 CPAM menus.

Table 2-1 5650 CPAM menus

Menu item	Description
Tools→Route Analysis	Access all 5650 CPAM management menus
Tools→Route Analysis→IGP topology	View the IGP topology map
Tools→Route Analysis→OSPF topology	View the OSPF topology map
Tools→Route Analysis→OSPFv3 topology	View the OSPFv3 topology map
Tools→Route Analysis→ISIS topology	View the ISIS topology map
Tools→Route Analysis→MPLS topology	View the MPLS topology map
Tools→Route Analysis→Flat Maps	View the following flat topology maps: • IGP Topology • OSPF Topology • OSPFv3 Topology • ISIS Topology • MPLS Topology • Multicast Topology
Tools→Route Analysis→IGP Network Data	View IGP network data

(1 of 2)

Menu item	Description
Tools→Route Analysis→BGP Network Data	View BGP network data
Tools→Route Analysis→Historical Routing Events	View the following historical routing events: • IGP • BGP
Tools→Route Analysis→Historical Routing Events→BGP Partition Manager	Access the BGP Partition Manager form
Tools→Route Analysis→Prefix List	View a list of advertised prefixes
Tools→Route Analysis→Path and Prefix Monitoring	Monitor paths and prefixes
Tools→Route Analysis→Managed Routes	View managed routes
Tools→Route Analysis→Checkpoints	View or create checkpoints
Tools→Route Analysis→Admin Domains / CPAAs	View admin domains and CPAAs
Tools→Route Analysis→Alarm Configuration	View or configure alarm settings
Tools→Route Analysis→CPAM Audit Manager	Access the CPAM Audit Manager form
Tools→Route Analysis→Simulated Impact Analysis	Create or manage scenarios
Tools→Route Analysis→Historical Impact Analysis	Configure historical impact analysis
Tools→Route Analysis→Multicast Manager	Access the Multicast Manager form
Tools→Synchronization Manager	Access the Synchronization Manager form
Help→5650 CPAM License Information	View the 5650 CPAM license information

(2 of 2)

2.3 Workflow for 5620 SAM and 5650 CPAM integration

1. Determine the 5650 CPAM device quantity and module requirements. Contact your Alcatel-Lucent representative for assistance.
2. Obtain the system ID of the station that is to host the integrated 5620 SAM and 5650 CPAM systems. See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for more information.
3. Use the system ID to obtain a 5650 CPAM license from Alcatel-Lucent.
4. Perform one of the following:
   a. Add the 5650 CPAM to an existing 5620 SAM system. See Procedure 2-1 for more information.
   b. Specify the Inclusion of the 5650 CPAM during a 5620 SAM installation or upgrade. See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for more information.
5. Restart each 5620 SAM GUI client to enable the 5650 CPAM GUI menus and functions. See chapter *5620 SAM User Guide* for more information.
6. Perform the required 5650 CPAM functions using GUI and OSS clients, as required. See the *5650 CPAM User Guide* and *5620 SAM XML OSS Interface Developer Guide* for more information.

2.4 5620 SAM and 5650 CPAM integration procedures

The following procedure describes how to configure 5620 SAM and 5650 CPAM integration.

Procedure 2-1 To add the 5650 CPAM to a 5620 SAM system

Perform this procedure to enable the 5650 CPAM functions in an existing 5620 SAM system. After you perform this procedure, the 5620 SAM and 5650 CPAM systems are integrated.

Caution — The 5650 CPAM license file required in this procedure must be based on the system ID used to generate the 5620 SAM license file. See the *5620 SAM User Guide* for information about viewing and exporting the license information. See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for information about obtaining the system ID of a station.

Note 1 — In a redundant 5620 SAM system, you must perform this procedure on each main server station.

Note 2 — You can perform this procedure regardless of whether the 5620 SAM software on the main server is running.

Note 3 — After the integration, you must restart each GUI client to enable the 5650 CPAM menus and functions on the client.

1 Choose Help→5620 SAM License Information from the 5620 SAM main menu. The 5620 SAM License (Edit) form opens.

2 Record the Licensed System IDs values.

3 Close the 5620 SAM License (Edit) form.

4 Request a 5650 CPAM license file using the Licensed System IDs values recorded in step 2.

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

6 Open a console window.

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

8 Enter the following:

```
bash$ ./nmsserver.bash import_license license_file ↵
```

where *license_file* is the absolute file path of the 5650 CPAM license zip file from Alcatel-Lucent

The following prompt is displayed:

```
Detected a 5650 CPAM license key. Do you want to proceed?
(YES/no):
```

9 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 5650 CPAM license key...

Original license key file has been backed up to
/opt/5620sam/server/timestamp/CPAMLicense.zip

Done.
```

where *timestamp* is a directory name in the following format: yyyy.mm.dd-hh.mm.ss

The main server puts the updated license into effect and enables the 5650 CPAM. No further configuration is required.

10 Close the console window.

11 Verify the imported license information.

12 If a license parameter is incorrect, contact Alcatel-Lucent technical support for assistance.

2.5 5620 SAM and 5620 NM integration

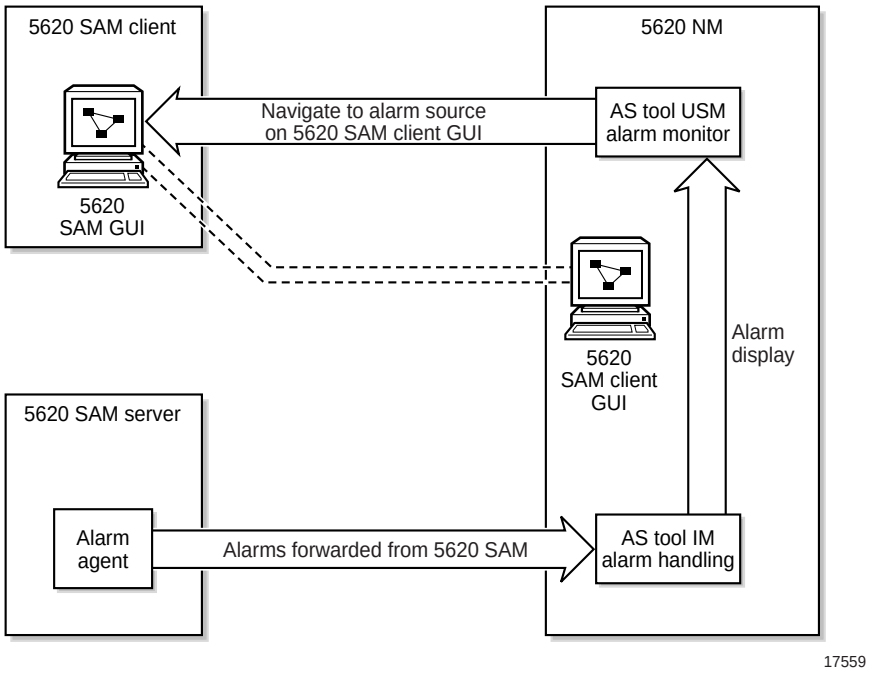
You can integrate the 5620 SAM and 5620 NM, which enables an operator to do the following.

- Navigate the 5620 SAM GUI using a 5620 NM client.
- Forward alarms from the 5620 SAM to the 5620 NM AS tool IM.
- Display 5620 SAM alarms graphically on the 5620 NM AS tool USM.
- Monitor services end-to-end using supported NM integration functions.

Note — Before you can integrate the 5620 SAM and 5620 NM, you must enable navigation from external systems during a 5620 SAM main server installation or upgrade, or enable it after an installation or upgrade using the 5620 SAM server configuration utility. See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for information about enabling navigation from external systems.

Figure 2-1 shows how navigation to the 5620 NM and 5620 NM AS tool for alarm management occurs.

Figure 2-1 Alarm navigation



Before you start

Consider the following before you attempt to integrate the 5620 SAM and 5620 NM:

- The *5620 NM Release Notice* lists the 5620 SAM releases that are compatible with various 5620 NM releases.
- The 5620 NM and 5620 SAM integration software is on the 5620 SAM software DVD-ROM.
- For 5620 SAM GUI navigation using a 5620 NM client, the 5620 SAM client must be installed on the same station that runs the 5620 NM client X-window access application.
- For alarm forwarding, the 5620 SAM and 5620 NM client software can be installed on the same or different stations.
- The platform for the 5620 NM software must meet the minimum requirements in the *5620 Network Manager Installation and Upgrade Guide*.
- You must configure the 5620 SAM to interwork with the 5620 NM software; for example, configure the 5620 SAM server to forward alarms and configure the 5620 SAM client to allow navigation from external systems.

5620 SAM client GUI startup and navigation restrictions

The following restrictions apply to 5620 SAM client GUI navigation using a 5620 NM client.

- When the client GUI is starting, 5620 NM navigation requests are blocked.
- A 5620 SAM client accepts navigation requests after the client GUI user logs in.

- Each navigation request is submitted only after a login timeout expires. This timeout helps to decrease the number of requests that are sent when a user submits and then immediately cancels a request.
- A 5620 SAM client delegate server acts as a single 5620 SAM client instance; you cannot configure a client delegate server to integrate with more than one 5620 NM client.
- The following navigation rules apply when multiple client GUIs are running.
  - A navigation request is cancelled when the client GUI is shut down.
  - All navigation requests are handled by the first registered client GUI.
  - If no client GUI is registered, a 5620 SAM server starts a new client GUI when it receives a navigation request.
  - If the currently registered 5620 SAM client GUI shuts down, another registered client GUI handles the navigation requests.

2.6 Workflow for 5620 SAM and 5620 NM integration

1. Ensure that the appropriate 5620 SAM integration software is installed and appropriately configured on the 5620 NM. See Procedure 2-2 for more information.
2. Configure the 5620 SAM client and server to support GUI navigation. See Procedure 2-3 for more information.
3. Start the 5620 SAM GUI. See the *5620 SAM User Guide* for more information.
4. Start the 5620 NM client GUI. See Procedure 2-4 for more information.
5. Perform the required network management function using the appropriate GUI, as described in section 2.5.

2.7 5620 SAM and 5620 NM integration procedures

The following procedures describe how to configure 5620 SAM and 5620 NM integration.

Procedure 2-2 To configure 5620 SAM and 5620 NM GUI integration

Perform this procedure to enable the use of a 5620 SAM client GUI through a 5620 NM client GUI.

1. Include the required 5620 SAM integration package in the 5620 NM installation. Consult the 5620 NM documentation for integration software installation and configuration information.
2. If required, configure the 5620 SAM server to forward alarms to the 5620 NM, as described in section 2.5.
3. If navigation from external systems is not currently enabled on each 5620 SAM main server, perform Procedure 2-3.

4 Install a 5620 SAM GUI client on a station that displays the 5620 NM client GUI. This is typically a station that runs an X-Window terminal emulator, but it can also be the 5620 NM database networkstation or the 5620 NM operator server networkstation, if a client GUI is locally displayed.

5 Perform one of the following on the station where the 5620 SAM client is installed.

a On a Solaris or RHEL station, open the *path*/nms-client.xml file with a plain-text editor

where *path* is the 5620 SAM client configuration directory, typically /opt/5620sam/client/nms/config

b On a Windows station, open the *path*/nms-client.xml file with a plain-text editor

where *path* is the 5620 SAM client configuration directory, typically C:\5620sam\client\nms\config

6 Perform the following steps to ensure that anti-aliasing is disabled.

i Search for the following XML tag that marks the beginning of the topologyMaps section:

```
<topologyMaps
```

ii Edit the antiAliasActive entry in the topologyMaps section to read “false” as shown below.

```
<topologyMaps
     iconReductionThreshold="40"
     labelHideThreshold="35"
        snapToGridInterval="25"
        antiAliasActive="false"
     />
```

7 Open a console window on the station.

8 Perform one of the following to run the navigator proxy script and start the client software.

a On a Solaris or RHEL station, perform the following steps.

i Enter the following at the CLI prompt:

```
# cd path
```

where *path* is the 5620 SAM client binary directory, typically /opt/5620sam/client/nms/bin

ii Enter the following:

./install_navigation_daemon.bash

iii Enter the following:

./nmsclient.bash

b On a Windows station, perform the following steps.

i Enter the following at the CLI prompt:

cd *path*

where *path* is the 5620 SAM client binary directory, typically C:\5620sam\client\nms\bin

ii Enter the following:

install_navigation_service.bat

iii Enter the following:

nmsclient.bat

The GUI client starts.

9 Use the 5620 SAM client GUI to create a 5620 NM user account that has a non-administrative privilege level with the appropriate scope of command role applied. See the *5620 SAM User Guide* for more information about configuring user accounts and how to apply a scope of command role.

10 Copy /opt/5620sam/server/nms/lib/common/generated/nms_common_core.jar from a 5620 SAM main server to the opt/netmgt/jnm/samjms/lib directory on the 5620 NM database networkstation.

11 Copy the following files from the /integration/5620NM/client/samadaptor directory on the 5620 SAM integration DVD-ROM to the /opt/netmgt/samadaptor/lib directory on the 5620 NM database networkstation:

- jbasiccomp.jar
- jnavapi.jar
- navrmi.jar
- samAdaptor.jar

12 Open the X-Window terminal emulator on the station that has the newly installed 5620 SAM client.

13 Log in to the 5620 NM operator server networkstation as a user with administrative privileges.

14 Open a console window on the 5620 NM operator server networkstation.

15 Start the 5620 NM client. The 5620 NM client GUI is displayed on the local station, and the 5620 SAM client GUI is available as a 5620 NM main menu item.

16 Use the 5620 SAM client account created in step 9 to perform the required interworking functions, as described in described in section 2.5, and the *5620 Network Manager User Guide*.

Procedure 2-3 To enable navigation from external systems on a 5620 SAM main server

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 Navigate to the DVD-ROM drive.

5 Perform one of the following

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.

6 Click on the Next button.

7 Accept the terms of the license agreement in the "Software License Agreement" panel.

8 Click on the Next button.

9 Choose Main Server Configuration in the "Choose Installation Type" panel.

10 Click on the Next button.

11 Click on the Next button in each subsequent panel until the "Navigation from External Systems" panel is displayed.

12 Select the "Enable Navigation from External Systems" parameter.

13 Configure the "TCP port for accepting GUI navigation requests" parameter.

14 Click on the Next button.

15 Click on the Next button in each subsequent panel until the "Installation Complete" panel is displayed.

16 Click on the Done button to close the server configuration utility.

17 Enter the following to switch to the samadmin user:

```
# su - samadmin ↵
```

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

19 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.

Procedure 2-4 To start the 5620 NM GUI

1 Log in to the 5620 SAM single-user client or client delegate station

2 Start the X-terminal software.

3 Use the X-terminal software to start the 5620 NM GUI on the station that has the 5620 NM Operator Position installed.

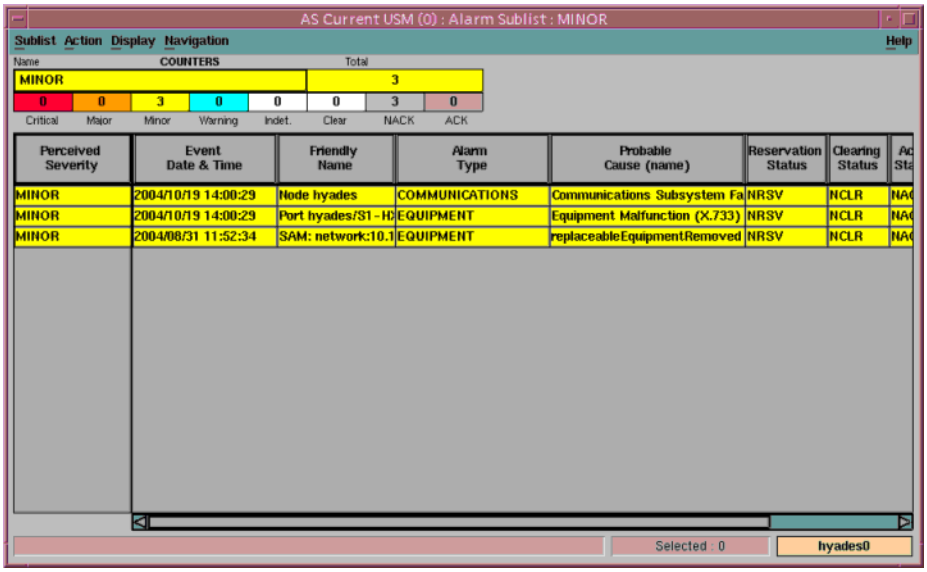
Procedure 2-5 To navigate from the 5620 NM AS tool USM to the 5620 SAM client GUI

See the *5620 SAM Troubleshooting Guide* for more information about troubleshooting using alarms.

1 Choose a counter summary window or alarm sublist from the AS tool USM.

2 Choose a sublist or an alarm in a sublist. 5620 SAM alarms are preceded by SAM in the Friendly Name field of the alarm sublist, as shown in Figure 2-2.

Figure 2-2 5620 SAM alarm in the AS tool USM



3 From the 5620 NM AS tool USM menu, choose Navigation→External Equipment→Show Equipment to navigate to the property form that lists the alarm on the 5620 SAM client GUI. The appropriate form is displayed. If the 5620 SAM client GUI is running, a new object properties form is displayed.

4 If the client GUI is not running, perform the following steps.

i Open the 5620 SAM client GUI.

ii View the object property form that is displayed on the 5620 NM client GUI.

5 After the alarm issue is resolved, clear the alarm using the 5620 SAM client GUI. Alarm status changes are shown in the 5620 NM AS tool USM.

2.8 5620 SAM and 9959 NPO integration

The 9959 NPO provides QoS information and cartographic tools for evaluating LTE RAN network performance and planning network expansion. When the 9959 NPO is discovered and by 5620 SAM, its QoS alerts be displayed as alarms in the 5620 SAM Alarm Window.

The 5620 SAM can manage the 9959 NPO as an EM system using the Horizontal Integration Protocol (HIP). When managed by the 5620 SAM, the 9959 NPO is displayed as an EM system in the equipment tree. Logical entities and 9959 NPO equipment are displayed as child objects of the parent EMS. See the *9959 Network Performance Optimizer (NPO) Administration User Guide* for information about 9959 NPO server configuration tasks that are required for integration with the 5620 SAM. See Procedure 2-6 for more information about discovering the 9959 NPO as a managed EM system. In the 5620 SAM GUI and documentation, the terms EMS and EM system are synonymous.

See the *5620 SAM LTE RAN User Guide* or the *5620 SAM LTE ePC User Guide* for information about viewing NPO alerts in the 5620 SAM GUI.

9959 NPO redundancy

The 5620 SAM supports 9959 NPO high availability through the management of redundant primary and secondary servers. In the event of a switchover, the new primary 9959 NPO server triggers a 5620 SAM resynchronization with both servers and the 5620 SAM updates the displayed alerts. The following behavior applies to 9959 NPO redundancy from a 5620 SAM perspective:

- The primary and secondary 9959 NPO servers must both be discovered as managed EMS. See Procedure 2-6.
- The secondary 9959 NPO server sends PMON alerts only. All QoS and real-time alert handling is done by the primary server.
- The 9959 NPO servers manage alert filtering between the primary and secondary to prevent alert duplication.
- The 9959 NPO servers manage all switchover triggering.
- The 5620 SAM periodically attempts to reconnect to an unreachable 9959 NPO server and triggers a resynchronization when the server is reachable.

See the *9959 Network Performance Optimizer (NPO) Administration User Guide* and related documentation for more information about managing 9959 NPO redundancy.

File transfer between the 5620 SAM and the 9959 NPO

The 9959 NPO retrieves files from 5620 SAM servers using the WebDAV protocol. You must enable WebDAV access during 5620 SAM server installation or reconfiguration, as this function is not enabled by default. See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for more information. See Procedure 2-9 for information about viewing the status of the WebDAV protocol for a 5620 SAM main server.

East-West licensing for the 9959 NPO

NEs, hardware, and objects managed by a 9959 NPO EMS in the 5620 SAM network consume East-West license tokens. An East-West license token is consumed by each of the following object types when managed by the 9959 NPO:

- MME pools
- standby 5620 SAM servers
- PLMNs
- 9959 NPO servers

Note — Managing PLMNs with the 9959 NPO can consume a large number of East-West license tokens. Provisioned license capacity must be able to accomodate the expected number of managed PLMNs, which can be viewed using the 9959 NPO Analysis Desktop.

2.9 5620 SAM and 9959 NPO integration procedures

Perform the procedures in this section to manage 9959 NPO integration with the 5620 SAM.

Procedure 2-6 To discover the 9959 NPO as an EM system

Note — You must specify a topology group other than the default Discovered NEs group when discovering an EM system. Step 1 of this procedure describes a basic process for creating a topology group. See the *5620 SAM User Guide* for more information about creating and populating topology groups.

1 If required, create a topology group for the EM system:

- **i** Choose Create→Equipment→Group from the 5620 SAM main menu. The Group (New Instance) (Create) form opens.
- **ii** Configure the parameters:
  - Name
  - Description
  - Background Image
- **iii** Click on the OK button. The form closes and the topology group is displayed in the navigation tree and topology map.

2 Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager (Edit) form opens with the Discovery Rules tab displayed.

3 Click on the Create button. The Create Discovery Rule form opens with the Specify General Attributes step displayed.

4 Click on the Select button for the Group Name, select a topology group other than Discovered NEs, and click on the OK button. The form is updated with the group name.

5 Click on the Next button until the Add EM Systems step is displayed.

6 Perform the following steps to complete the Add EM Systems step:

- **i** Click on the Create button. The EM System (Create) form opens with the General tab displayed.
- **ii** Configure the parameters:
  - Auto-Assign ID
  - ID
  - Element Manager System Name
  - Description
- **iii** Click on the Element Managers tab.
- **iv** Click on the Create button. The Element Manager (Create) form opens.

v Configure the parameters:

- Host Name
- Server IP Address
- Server Port Number
- User Name
- Password
- Confirm Password

Note — You cannot enter a hostname as the value of the Server IP Address parameter.

vi Click on the OK button. The Element Manager (Create) form closes and a dialog box opens.

vii Click on the OK button.

viii Click on the OK button. The EM System (Create) form closes and a dialog box opens.

ix Click on the OK button.

7 Click on the Finish button. The Create Discovery Rule form closes and a dialog box opens.

8 Click on the OK button.

9 Click on the Apply button in the Discovery Manager (Edit) form. A dialog box opens.

10 Click on the Yes button. The discovery rule is saved.

11 Activate the EMS discovery:

Note — The 5620 SAM does not discover an EM system until you set the Administrative State parameter of the EMS object to Up and save the changes in the Discovery Manager.

i In the Discovery Manager (Edit) form, click on the EM Systems tab.

ii Choose the EM system you created in step 6 and click on the Properties button. The EM System (Edit) form opens with the General tab displayed.

iii Set the Administrative State parameter to Up.

iv Click on the OK button. The EM System (Edit) form closes.

v Click on the Apply button in the Discovery Manager (Edit) form. A dialog box appears.

vi Click on the Yes button. The changes are saved and the 5620 SAM attempts to discover the EM system.

12 Close the Discovery Manager (Edit) form.

Procedure 2-7 To unmanage and delete the 9959 NPO from the 5620 SAM network

Warning 1 — Deleting an EMS results in a loss of management data and completely removes the EMS from the managed network. See the *5620 SAM User Guide* for more information.

Warning 2 — Deleting the 9959 NPO from the network clears all alarms raised by the 9959 NPO and all alarms raised by the 5620 SAM against the 9959 NPO.

1. Choose Administration→Discovery Manager from the 5620 SAM main menu. The Discovery Manager (Edit) form opens with the Discovery Rules tab displayed.
2. Click on the EM Systems tab.
3. Configure the filter criteria, if required, and click on the Search button.
4. Choose an EMS and click on the Properties button. The EM System (Edit) form opens with the General tab displayed.
5. Set the Administrative State parameter to Down.
6. Click on the OK button. The EM System (Edit) form closes.
7. Choose the administratively down EM system and click on the Delete button. A dialog box opens.
8. Click on the Yes button. The EM system is deleted.
9. Close the Discovery Manager (Edit) form.

2.10 5620 SAM and EM systems integration

The 5620 SAM can manage multiple element manager systems using the Horizontal Integration Protocol (HIP). The HIP allows EM systems to integrate with the 5620 SAM using a single jar file (the HIP library jar file). When integrated with the 5620 SAM, the EM system's inventory and alarm information are displayed in the 5620 SAM GUI. Any operations performed on the EM system's alarms using the 5620 SAM GUI are then sent to the EM system for processing, where they can be accepted or denied. The HIP also enables EM system alarms to be pushed directly onto 5620 SAM NEs. For more information about discovering EM systems, see the *5620 SAM User Guide*.

The HIP library jar file is provided with the 5620 SAM and must be installed in the project classpath. Two versions are delivered: one compiled with Java 1.6 and one compiled with Java 1.7. Only one of these may be used at a time. The HIP library jar file contains all required classes, a default logger, and two simulators. The EM system simulator can be used as an example for EM system development. The 5620 SAM simulator simulates a 5620 SAM connecting to an EM system and performing an initial resynchronization.

The user must create the HipServerImpl class, which will be dedicated to communication between the HIP server (located on the EM system server) and the HIP client (located on the 5620 SAM server), and the HipClientInterface callback. The HipServerImpl class will contain all the necessary facilities to connect via Cproto and to call HIP methods, as well as the HipClientInterface callback. All requests coming from the HIP client will arrive on the HipClientInterface callback.

Cproto is the protocol that is used to establish a session between the HIP server and the HIP client. It uses two seperate channels for events and requests. Cproto is based on TCP protocol and Java API NIO.

2.11 5620 SAM and 5670 RAM integration

The 5670 RAM server processes AA statistics. The 5620 SAM statistics collector - which can be an auxiliary 5620 SAM server - prepares the statistics files which are retrieved by the 5670 RAM. The 5620 SAM statistics collection intervalizes the statistics before they are retrieved by the 5670 RAM.

See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for more information about how to enable application assurance statistics collection on the 5620 SAM and how to install the 5670 RAM statistics adaptor component on the 5620 SAM.

See the *5620 SAM User Guide* for more information about application assurance and application assurance policies.

Procedure 2-8 To enable 5670 RAM support

Perform this procedure to enable the 5670 RAM functions on a 5620 SAM system. You require samadmin user privileges to perform this procedure.

1. Peform one of the following:
   a. If the 5620 SAM server is deployed in a standalone configuration, perform step 2 on the main server.
   b. If the 5620 SAM server is deployed in a redundant configuration, perform step 2 on the primary main server.
2. Log in to the main server station as the samadmin user.
3. Navigate to the server configuration directory, typically /opt/5620sam/server/nms/config.
4. Create a backup copy of the nms-server.xml file.
5. Open the nms-server.fml file using a plain-text editor.

Caution — Contact your Alcatel-Lucent techincal 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.

6. Locate the following section:

```
<ram5670

ramEnabled="false" />
```

7 Change “false” to “true”.

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

9 Open a console window.

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

11 Perform one of the following:

a If you are configuring a main server in a standalone deployment or the primary main server in a redundant deployment, enter the following at the prompt:

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

b If you are configuring the standby main server in a redundant deployment, enter the following at the prompt:

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

The main server restarts and puts the configuration change into effect.

12 Log out of the main server.

13 If the 5620 SAM server is deployed in a redundant configuration, perform steps 2 to 12 on the standby main server.

14 Close the open console windows.

2.12 5620 SAM and 9952 WPS integration

File transfer between the 5620 SAM and the 9952 WPS

The 9952 WPS transfers files to and from 5620 SAM servers using the WebDAV protocol. You must enable WebDAV access during 5620 SAM server installation or reconfiguration, as this function is not enabled by default. See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for more information. See Procedure 2-9 for information about viewing the status of the WebDAV protocol for a 5620 SAM main server.

You can set up the automatic transfer of CM XML files between the 5620 SAM and the 9952 WPS by enabling the server repository function of the 9952 WPS. Manual transfer via FTP is also supported. See the *9952 WPS User Guide* for more information about the server repository function.

Note — Alcatel-Lucent recommends enabling SSL on the 5620 SAM main server before using the server repository function of the 9952 WPS to import and export CM XML files. See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for information about configuring SSL.

Procedure 2-9 To view WebDAV activation status on a 5620 SAM main server

Perform this procedure to verify whether the WebDAV protocol for file transfers to the 9952 WPS and 9959 NPO is enabled.

1. Log in to a 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 command:

   ```
   bash$ ./nmsserver.bash -s nms_status ↵
   ```

5. Verify that the following status message is displayed:

   ```
   -- WebDAV Access to Activation Data Enabled
   ```

6. If the message is not displayed, enable WebDAV during a 5620 SAM server reconfiguration. See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for information about enabling the WedDAV protocol.
7. Close the console window.

2.13 5620 SAM and 5780 DSC integration

The 5780 DSC is treated as a device that is managed by the 5620 SAM, rather than an external system that requires integration with the 5620 SAM. The 5620 SAM allows you to view the properties for the equipment, instance, Diameter proxy agent, and policy charging rules for the 5780 DSC. The 5780 DSC is represented in the 5620 SAM equipment navigation tree. The instance, Diameter proxy agent, and policy charging rule properties are viewable using the Manage→Mobile Core→DSC Instances 5620 SAM main menu option.

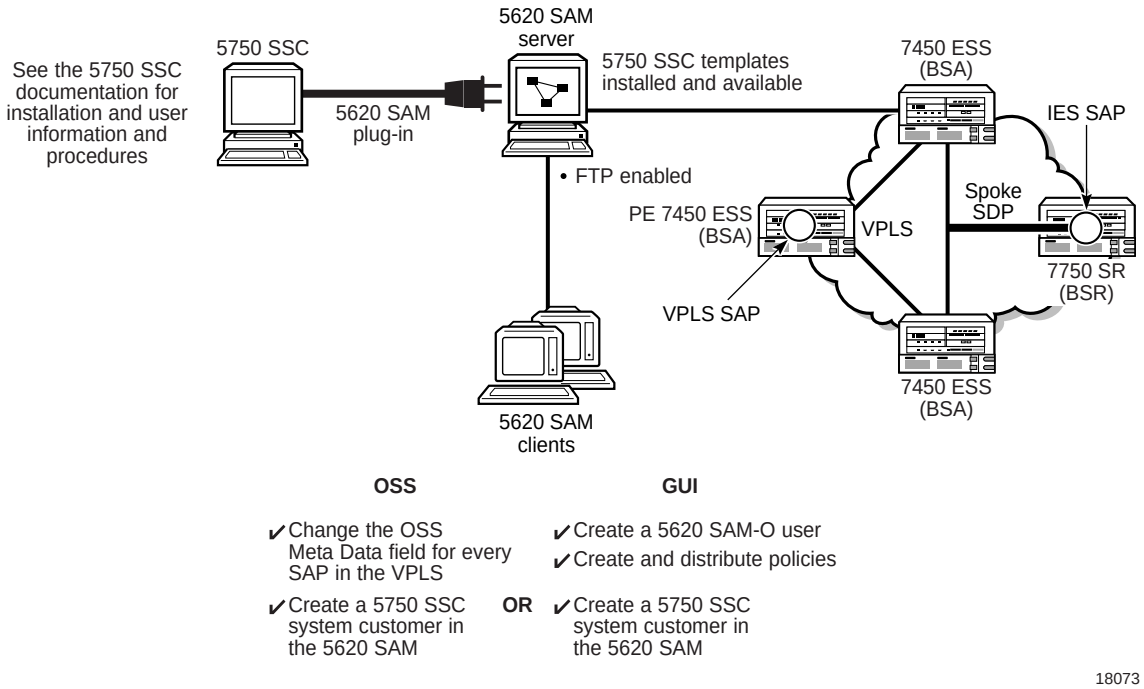
The *5620 SAM LTE ePC User Guide* describes 5780 DSC discovery and management using the 5620 SAM.

2.14 5620 SAM and 5750 SSC integration

The 5620 SAM can be configured to interoperate with the 5750 Subscriber Services Controller. The 5750 SSC provides centralized control of subscriber access services for triple play service delivery; for example, DHCP to identify subscribers and trigger service configuration.

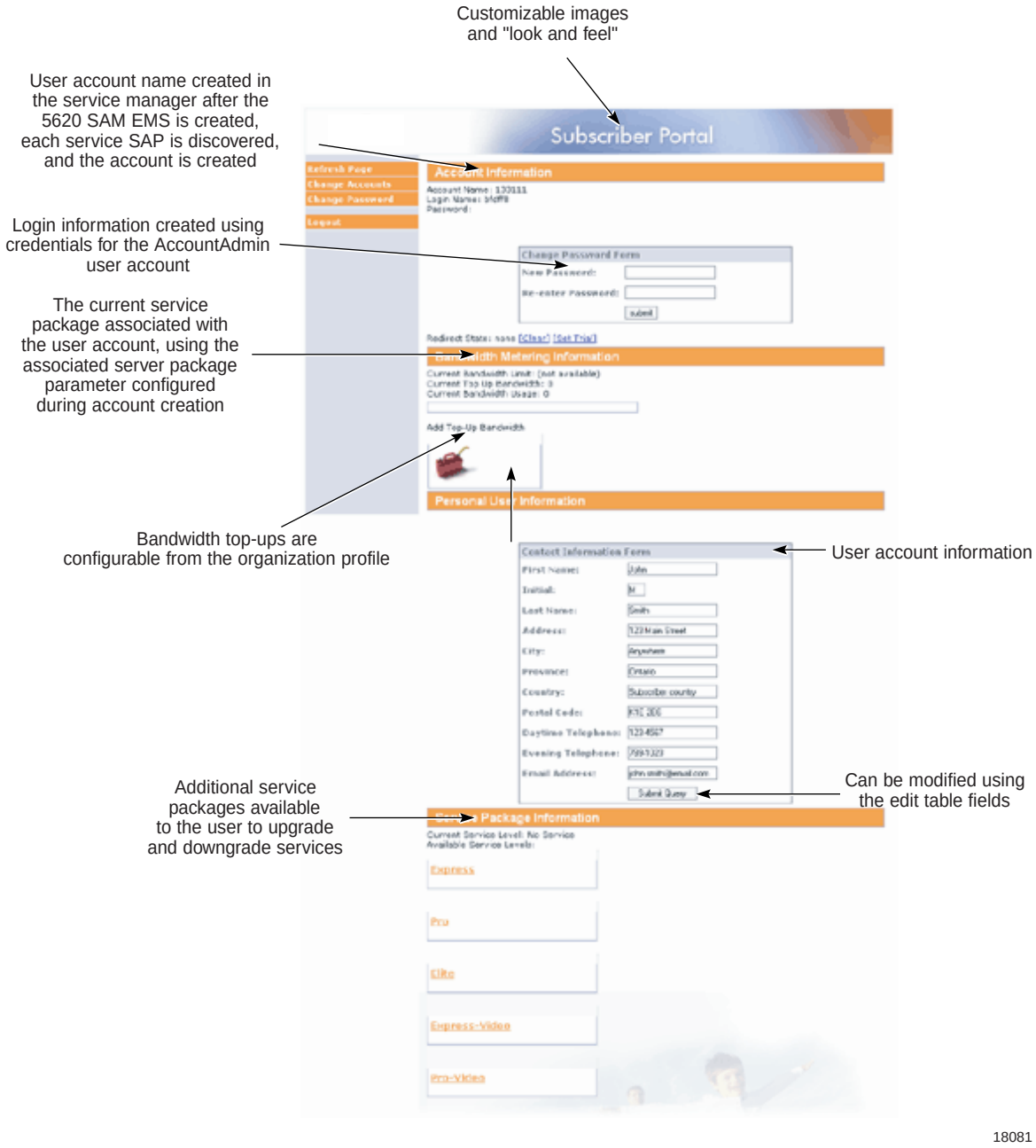
Figure 2-3 shows the integration requirements for the 5620 SAM and the 5750 SSC. See the 5750 SSC documentation suite for information about how to configure application interoperation.

Figure 2-3 5750 SSC and 5620 SAM integration



You use the 5750 SSC Service Manager to create and manage subscriber services, including user account information and QoS levels. The 5750 SSC user accounts represent the residential subscribers of triple play services. The information configured in the 5750 SSC Service Manager is used to build the subscriber web portal for user self-management. Figure 2-4 shows a subscriber web portal and how the component pieces are assembled from 5750 SSC subscriber management configurations.

Figure 2-4 Subscriber web portal



2.15 5620 SAM and 5520 AMS integration

A 5620 SAM client GUI can discover and monitor other element manager systems, including the 5520 AMS. When discovered as a managed EMS, the 5520 AMS can forward alarms raised against a 7705 SAR-M. These alarms are then correlated and shown against the corresponding network element within the 5620 SAM client GUI.

2.16 Call trace data transfer to the 9958 WTA

The 5620 SAM supports automatic and secure call trace data file transfer to the 9958 WTA over HTTPS via the WebDAV protocol. The transfer function uses the login credentials of a 5620 SAM user, and facilitates call trace file management by removing the need for manual transfers over SFTP. The following conditions must be true to use the call trace data file transfer function:

- SSL is enabled on all call trace auxiliary servers. See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for information about configuring SSL.
- A 5620 SAM user with read access to the calltrace.WebDAVSharedData permission is available. See the *5620 SAM System Administrator Guide* for more information about creating 5620 SAM users, configuring scope of command roles, and for lists of assignable permissions.

Note — Read access is the only required access type for the calltrace.WebDAVSharedData permission.

- Configuration for data collection from the 5620 SAM to the 9958 WTA using the login credentials of a 5620 SAM user is complete. See the *9958 Wireless Trace Analyzer Installation and User Guide for LTE and W-CDMA* for more information about configuring data collection.

3 — 5620 SAM integration with Single Sign On

3.1 SSO integration *3-2*

3.2 SSO integration procedures *3-2*

3.1 SSO integration

Single Sign On (SSO) technology enables a user to access all resources within a domain after having entered their credentials just one time. SSO uses centralized authentication servers to ensure that users do not need to enter their credentials repeatedly. Security is provided on all levels without the inconvenience of re-prompting users.

Note — Users who access the 5620 SAM client GUI through Internet Explorer must deselect the "Do not save encrypted pages to disk" Security option. This option is on the Advanced tab of the Internet Options form, which is accessible from the Tools menu.

You can use SSO to integrate the 5620 SAM and the following systems:

- SANE portal
- 1350 OMS
- OMC-RAN

3.2 SSO integration procedures

Use the following procedures to enable 5620 SAM SSO integration with other systems.

Procedure 3-1 To configure 5620 SAM and LSM portal integration

Perform this procedure to configure a 5620 SAM system for interworking with the LSM portal. The LSM portal is a component used for integration with the 1350 OMS. Ensure that the 5620 SAM Server is stopped before you begin. You require the following user privileges on each main server station to perform this procedure:

- root
- samadmin

The following steps assume that the 5620 SAM server is installed at /opt/5620sam/server. Modify paths accordingly if your 5620 SAM server is installed to a different location.

1 Deploy the csa_v2_proxy_spi.sar file.

```
/opt/5620sam/server/nms/jboss/server/default/deploy/csa_v2_proxy
_spi.sar

# cp -i
/opt/5620sam/server/nms/jboss/sso/csa/csa_v2_proxy_spi.sar
/opt/5620sam/server/nms/jboss/server/default/deploy/csa_v2_proxy
_spi.sar

# chown samadmin:sam
/opt/5620sam/server/nms/jboss/server/default/deploy/csa_v2_proxy
_spi.sar
```

2 Modify the following fields within /5620sam/sever/nms/config/sso/csa_proxy_config_service.xml:

   i Set the ipaddress parameter to the IP address of the LSM Portal. Contact your LSM Portal administrator to obtain.

   ii Set the port parameter to the port number of the LSM Portal. Contact your LSM Portal administrator to obtain.

3 Go to /opt/5620sam/server/nms/config/clientDeploy/nms-client.xml and add the following lines in the <integration> section:

```
lsmproperties="https://<pathToLsmApiProperties>"
applicationid="<applicationIdValue>"
```

Note 1 — <pathToLsmApiProperties> is the URL of the path to the LSM Portal LSM API properties file. Contact your LSM Portal administrator to obtain.

Note 2 — <applicationIdValue> is the value of the 5620 SAM target binding ID configured in the LSM Portal. Contact your LSM Portal administrator to obtain

4 When communication to the LSM Portal is SSL secured, perform the following steps to share the LSM Portal security certificates with the 5620 SAM server and its clients:

   i Obtain the public security certificate from the LSM Portal administrator.

   ii Import this certificate into the 5620 SAM server truststore found at /opt/5620sam/server/nms/config/ssl/trustStore/cacerts.trustStore.

   iii Go to /opt/5620sam/server/nms/bin/setenv.rc and set the SSL path parameter to the path of the 5620 SAM server truststore.

   iv Go to /opt/5620sam/server/nms/config/clientDeploy/setenv.bat and uncomment the following line:

```
rem  set
JVM_OPTIONS_SSL=-Djavax.net.ssl.trustStore=..\config\ssl\tru
stStore\cacerts.trustStore
```

   v Go to /opt/5620sam/server/nms/config/clientDeploy/setenv.rc and uncomment the following line:

```
#JVM_OPTIONS_SSL="-Djavax.net.ssl.trustStore=../config/ssl/t
rustStore/cacerts.trustStore"
```

   vi To deploy the changes, run the following command as the samadmin user:

```
bash$ /opt/5620sam/server/nms/bin/nmsdeploytool.bash deploy
```

5 Restart the 5620 SAM server.

Procedure 3-2 To configure 5620 SAM integration with a system that uses the LSM portal

Perform this procedure to configure a 5620 SAM system to allow navigation requests from an external system that uses the LSM portal.

Note — You must perform this procedure on each main server in the 5620 SAM system.

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

2 Open *path*/nms/config/sso/em_lsmproxy_config.xml using a plain-text editor.

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

3 Locate the following XML tag, which marks the beginning of the section that lists each external system, or target application, that connects to the 5620 SAM through the LSM portal, as shown in Code 3-1.

Code 3-1: Beginning of target applications section

```
<lsm-proxy-target-applications>
```

The section contains multiple target application entries in separate subsections. By default, each entry is populated with sample values, and the group of entries is surrounded by comment tags to disable them.

4 To configure a target application, edit the subsection directly below the leading comment tag, which is the first line in Code 3-2, to read as shown in Code 3-2.

Code 3-2: Target application subsection

```
<!--
    <target-application>
        <em-server>
            <servertype>serverType</servertype>
            <server-ip>serverIP</server-ip>
        </em-server>
        <jnlp-url>JNLP_URL</jnlp-url>
    </target-application>
```

where

serverType: is the application type, for example, OMC-RAN

serverIP is the public IPv4 address of the server application on the external system

JNLP_URL is the URL of the JNLP file required to run the client application; see the external system documentation for the file location

5 To enable the target application, move the leading comment tag line to the line directly below the closing tag of the target application subsection, as shown in Code 3-3.

Code 3-3: Enabled target application

```
    </target-application>
```

<! - -

6 Save and close the file.

Procedure 3-3 To configure 5620 SAM and SANE portal integration

Perform this procedure to configure a 5620 SAM system for interworking with the SANE portal. You require the following user privileges on each main server station to perform this procedure:

- root
- samadmin

Caution — If you are using this procedure to reconfigure one or more installed main servers, the following conditions apply:

- If the main servers do not currently have SSL enabled, you must prepare the 5620 SAM system for operation with SSL. See the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* for information about configuring SSL.
- The procedure requires that you stop and restart each main server, which causes a network management outage. Ensure that you perform this procedure only during a scheduled maintenance period.

In a redundant deployment, the sequence of events is the following:

- standby main server stopped
- standby main server reconfigured
- standby main server started
- primary main server stopped / server activity switch triggered
  This is the beginning of the network management outage.
- server activity switch completes
  This is the end of the network management outage.
- primary main server reconfigured
- primary main server started
- if required, manual activity switch performed to restore initial primary and standby main server roles

Note 1 — You can perform this procedure as part of a 5620 SAM main server installation or upgrade, or as a configuration activity on an installed main server.

Note 2 — You must perform this procedure on each main server In a redundant 5620 SAM deployment, in the following order:

- standby main server
- primary main server

1 Perform one of the following.

a If you are performing this procedure as part of a main server installation or upgrade, perform the initial installation or upgrade procedure steps in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* up to, but not including, the step that describes opening the 5620 SAM server installer.

b If you are performing this procedure to reconfigure one or more installed main servers, perform the following steps.

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

ii Open a console window.

iii Enter the following to change 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 main server software:

```
bash$ ./nmsserver.bash stop ↵
```

v Enter the following to display the 5620 SAM main server status:

```
bash$ ./nmsserver.bash appserver_status ↵
```

The command displays a status message.

vi The 5620 SAM main server is stopped when the command displays the following status message:

```
Application Server is stopped
```

If the command displays a different message, wait 5m and repeat step 1 b v. Do not proceed to the next step until the server is stopped.

vii Enter the following to switch to the root user:

```
bash$ su - ↵
```

viii Place the 5620 SAM software DVD-ROM in a DVD-ROM drive.

ix Navigate to the DVD-ROM drive.

2 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 -DconfigSANE=yes ↵

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 -DconfigSANE=yes ↵

where
R_r is the release identifier, in the form *MAJOR_minor*
revision is the revision identifier, such as R1, R3, or another descriptor

3 Accept the terms of the license agreement in the "Software License Agreement" panel.

4 Click on the Next button. The "Choose Installation Type" panel is displayed.

5 Perform one of the following.

a If you are performing this procedure as part of a main server installation or upgrade, select "Main Server Installation" in the "Choose Installation Type" panel.

b If you are performing this procedure to reconfigure an installed main server, select "Main Server Configuration" in the "Choose Installation Type" panel.

6 Click on the Next button.

7 Perform one of the following.

a If you are performing this procedure as part of a main server installation or upgrade, perform the subsequent installation or upgrade procedure steps described in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide* until the "SSL Configuration" panel is displayed.

b If you are performing this procedure to reconfigure an installed main server, click on the Next button in each subsequent panel until the "SSL Configuration" panel is displayed.

8 Select the "Enable Secure Communication" parameter.

Note — You must enable and configure SSL before you can enable or configure SANE SSO.

9 Configure the remaining parameters on the panel.

10 Click on the Next button. The "SANE SSO Configuration" panel is displayed.

11 Select the "Enable SANE SSO" parameter.

12 Configure the "Windows Client Installation Directory" parameter by specifying the 5620 SAM software installation directory used for Windows clients.

13 Configure the "Unix Client Installation Directory" parameter by specifying the 5620 SAM software installation directory used for Solaris clients.

14 Configure the "Enable Response Signature Validation" parameter.

15 Click on the Next button. The "SANE SSO Certificate Files Configuration" panel is displayed.

16 Click on the Add button to specify an SSO certificate file. A file browser opens.

17 Choose a certificate file and click on the OK button.

18 Repeat steps 16 and 17 to specify an additional certificate file, if required.

19 Click on the Next button.

20 Perform one of the following.

a If you are performing this procedure as part of a main server installation or upgrade, perform the subsequent installation or upgrade procedure steps described in the *5620 SAM | 5650 CPAM Installation and Upgrade Guide*.

b If you are performing this procedure to reconfigure an installed main server, perform the following steps.

i Click on the Next button in each subsequent panel until the "Installation Complete" panel is displayed.

ii Click on the Done button to close the server installer.

iii Enter the following to switch back to the samadmin user:

```
# exit ↵
```

iv Enter the following to start the 5620 SAM main server:

```
bash$ ./nmsserver.bash start ↵
```

The 5620 SAM main server restarts and puts the SANE SSO configuration into effect.

- If required, perform a manual server activity switch to restore the initial primary and standby main server roles.

Procedure 3-4 To enable SSO between 5620 SAM and an identity provider using v1.1 SAML artifacts

You require the following user privileges on each main server station to perform this procedure:

- root
- samadmin

1. Log in to the main server station as the samadmin user.
2. Open a console window.
3. Enter the following to add the metadata file:

```
# cd /opt/5620sam/server/nms/config/sso/metadata/1.1/ ↵

# cp -p idp_metadata.xml  idp_metadata.orig ↵

# vi idp_metadata.xml ↵
```

4. Configure the parameters as follows:

```
entityId = http://identity_provider_IP:8080/openam_954

singleSignOnServiceLocation.POST =
http://identity_provider_IP:8080/openam_954/SAMLPOSTProfileServl
et

singleSignOnServiceLocation.ARTIFACT =
http://identity_provider_IP:8080/openam_954/SAMLAwareServlet

artifactResolutionServiceLocation =
http://identity_provider_IP:8080/openam_954/SAMLSOAPReceiver

certificateFileLocation =

sourceID=EAJOXo5wCRwB9/30i3hUkkJIthE=
```

where
identity_provider_IP is the IP address of an identity provider using v1.1 SAML artifacts

Note — The values of the entityId and sourceID parameters will vary depending on the specific configuration of your identity provider.

5 Enter the following to configure the SAML.properties file:

 # vi /opt/5620sam/server/nms/jboss/server/default/deployAlcatel5620SRM/z_z_z/webSSO.war/WEB-INF/classes/config/SAML.properties ↵

6 Configure the parameters as follows:

```
com.alu.cnm.csa.saml.sp.signValidatorMarshaller = OPENSAML
```

4 — 5620 SAM integration with CFMA

4.1 CFMA integration overview *4-2*

4.2 CFMA integration procedures *4-2*

4.1 CFMA integration overview

The SAM-CFMA adapter for CFMA translates 5620 SAM alarms into alarms for CFMA. The adapter connects to 5620 SAM using SAM-O and JMS. The connection parameters will be specified in an XML configuration file that contains the required information to allow the 5620 SAM adapter to connect to SAM-O and JMS. The password provided in the XML file will be MD5 hashed. The adapter software can be found in the integration/samcfmadapter directory of the 5620 SAM installation DVD.

An installed SAM-CFMA adapter must be of the same release as the 5620 SAM server with which it is to interface, and these must be compatible with the CFMA version. The 5620 SAM server and the CFMA must also have their times synchronized to ensure that the JMS connection behaves properly and that the alarm timestamp matches on both systems. It is recommended that both systems synchronize their time against the same NTP server. Contact your Alcatel-Lucent support representative for more information.

The sam-cfma-adapter.sar file is an archive of files required to support the SAM-CFMA adapter. A CFMA system administrator must extract the contents of this file and deploy them to the correct CFMA directory. Contact your Alcatel-Lucent support representative for more information.

4.2 CFMA integration procedures

Use the following procedures to install the 5620 SAM adapter for CFMA.

Procedure 4-1 Installing the SAM-CFMA adapter sar file

The paths to the configurations provided in the following procedure are provided as an example only and may vary, depending on the CFMA installation and version. Consult the CFMA documentation for details.

1 Run the following command:

```
cd <JBOSS_dir>/alu_cnm_cfma_main/deploy
```

2 To create the SAM-CFMA adapter directory, run the following command:

```
mkdir sam-cfma-adapter.sar
```

3 To copy the sar file in the created directory, run the following commands:

```
cp <SAR_FILE_LOCATION>/sam-cfma-adapter.sar
<JBOSS_dir>/alu_cnm_cfma_main/deploy/sam-cfma-adapter.sar/

cd <JBOSS_dir>/alu_cnm_cfma_main/deploy/sam-cfma-adapter.sar/
```

4 To unzip the sar file, run the following command:

```
unzip sam-cfma-adapter.sar
```

5 To remove the unzipped sar file, run the following command:

```
rm sam-cfma-adapter.sar
```

Procedure 4-2 Setting CFMA preferences

The paths to the configurations provided in the following procedure are provided as an example only and may vary, depending on the CFMA installation and version. Consult the CFMA documentation for more information.

1 To set the EVENT_PROCESSING_WITH_DEVICETIME to true for the main and player servers, run the following commands:

```
cnm-preference-modify -c cfma -i main -d ../main/data/output
"/cfma/server/asset/main/com/alu/cnm/cfma/ngfm/server/fmcommon:E
VENT_PROCESSING_WITH_DEVICETIME:true"

cnm-preference-modify -c cfma -i main -d ../main/data/output
"/cfma/server/asset/player/com/alu/cnm/cfma/ngfm/server/fmcommon
:EVENT_PROCESSING_WITH_DEVICETIME:true"
```

2 To set the synchTimeout to 60, run the following command:

```
cnm-preference-modify -c cfma -i main -d ../main/data/output
"/cfma/server/asset/main/com/alu/cnm/cfma/ngfm/server/fmcollecto
r:synchTimeout:60"
```

Note — An initial discovery taking more than 60 minutes will require increasing the synchTimeout.

Procedure 4-3 Enabling 5620 SAM server communication

Included in the sam-cfma-adapter.sar file is the jboss-service.xml configuration file. Prior to deploying the SAM-CFMA adapter, the following parameters within the jboss-service.xml configuration file must be modified to allow communication with the 5620 SAM server.

1 Open the jboss-service.xml configuration file.

2 Set the ipAddressOne parameter to the IP address of the primary 5620 SAM server.

3 Set the httpPortOne parameter to the HTTP port of the primary 5620 SAM server used for OSS requests.

4 Set the jndiPortOne parameter to the JNDI port of the primary 5620 SAM erver.

5 Set the ipAddressTwo parameter to the IP address of the redundant 5620 SAM server.

6 Set the httpPortTwo parameter to the HTTP port of the redundant 5620 SAM server used for OSS requests.

7 Set the jndiPortTwo parameter to the JNDI port of the redundant 5620 SAM server.

8 Set the adapterType parameter to either 5620OMS or 5620XMS.

Note — This value is dependent on specific system integration.

9 Set the username parameter to the 5620 SAM user used for the OSS/JMS connections.

Note 1 — This user must be configured in the 5620 SAM server and must have have OSS privileges.

Note 2 — In 5620 SAM, this user should be bound to a Span Profile that contains spans defining all alarmable objects for which the CFMA user wishes to receive alarm events.

Note 3 — Do not specify a Span Profile containing blocked spans as this will cause the SAM-CFMA adapter to become out of sync with the 5620 SAM.

10 Set the password parameter to the MD5 hashed password required for the 5620 SAM username.

11 Set the spanIds to a comma separated list of numeric values corresponding to span numbers configured on the 5620 SAM Server.

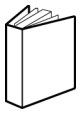
Note 1 — The span numbers specified here must match those belonging to the Span Profile of the 5620 SAM user specified in step 9.

Note 2 — Only alarms raised on objects belonging to the specified spanIds will be shown in CFMA.

Note 3 — Spans used by the SAM-CFMA adapter should not be modified after an interface is established between 5620 SAM and CFMA. Alarmed objects should not be added, removed, or moved from one span to another (i.e. move an NE from one group belonging to a spanId to another group belonging to a different spanId). Doing so will cause the CFMA alarm list to become out of sync with the 5620 SAM alarm list. If the CFMA alarms become out of sync with the 5620 SAM alarms, the 5620 SAM alarms can be synchronized from the CFMA GUI by performing Actions→Synchronize→Alarms and selecting the 5620SAM entry.

12 Restart the CFMA.

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

© 2014 Alcatel-Lucent. All rights reserved.

www.alcatel-lucent.com