



Unified Communications Management Common Services Fundamentals Avaya Communication Server 1000

Release 7.5
NN43001-116
Issue 05.21
February 2013

All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

"Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on its hardware and Software ("Product(s)"). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: <http://support.avaya.com>. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTP://SUPPORT.AVAYA.COM/LICENSEINFO](http://support.avaya.com/licenseinfo) ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at <http://support.avaya.com/LicenseInfo> under the link "Heritage Nortel Products". For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software that may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya's website at: <http://support.avaya.com/Copyright>. You agree to the Third Party Terms for any such Third Party Components.

Note to Service Provider

The Product may use Third Party Components that have Third Party Terms that do not allow hosting and may need to be independently licensed for such purpose.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: <http://support.avaya.com>. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third

parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and "Linux" is a registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: <http://support.avaya.com>.

Contact Avaya Support

See the Avaya Support website: <http://support.avaya.com> for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: <http://support.avaya.com>, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: New in this release	11
Navigation	11
Features	11
UCM migration to System Manager	11
Other changes	11
Revision History	12
Chapter 2: Customer service	15
Navigation	15
Getting technical documentation	15
Getting product training	15
Getting help from a distributor or reseller	15
Getting technical support from the Avaya Web site	16
Chapter 3: Introduction	17
Navigation	17
Chapter 4: UCM overview	19
Navigation	19
Introduction	19
Avaya Communication Server 1000 task flow	21
UCM navigation tree	23
UCM basics	24
Network	26
Elements	27
CS 1000 Services	27
Corporate Directory	28
IPsec	28
Numbering Groups	28
Patches	29
SNMP Profiles	29
Secure FTP token	29
Software Deployment	30
Subscriber Manager	30
User Services	31
Security	31
Tools	31
Logs	32
Data	34
Applications and services	35
UCM client capacity	36
Benefits and features	37
Central authentication	38
Security domain	38
Certificate management	40
Server types	42
Primary security server	42

Backup security server.....	42
Member server.....	43
Domain Name System.....	44
Disaster Recovery.....	44
High Availability configuration.....	44
Chapter 5: Security Services overview.....	47
Navigation.....	47
Authentication.....	47
Identity management.....	48
Accounts.....	48
Local account.....	48
Built-in account.....	49
External account.....	50
Central logon.....	50
Security policies.....	50
Password aging policy enforcement.....	51
The password strength policy enforcement.....	52
Password history policy enforcement.....	52
Password lockout policy enforcement.....	52
Inactive session termination policy.....	53
Logon warning banner.....	53
Access control policies.....	53
Roles and permissions.....	54
Built-in roles.....	55
Custom roles.....	58
Inheritance of UCM role-based permissions for Element type of CS 1000.....	59
Permission templates.....	59
Role mapping and permission evaluation.....	59
Chapter 6: Security server configuration.....	61
Navigation.....	61
Prerequisites.....	61
Security Server configuration.....	62
Configuring the primary security server.....	62
Configuring a backup security server.....	64
Configuring a member server.....	65
Decommission a Backup Security Server.....	67
Security configuration changes.....	67
Making changes on a member server.....	67
Configuration failure.....	68
Demoting a primary and backup server.....	68
Resetting an Administrator password.....	68
Chapter 7: Logon and logoff options in UCM.....	71
Navigation.....	71
Logon modes in UCM.....	71
Central logon mode.....	71
Logging on to UCM in Central logon mode for the first time.....	72
Logging on using the FQDN in central logon mode.....	72

Network logon mode.....	72
Logging on to UCM in Network logon mode for the first time.....	72
Logging on using the IP address in network logon mode.....	73
Switching from network logon mode to central logon mode.....	74
Disabling digital certificate pop-up.....	74
SSO using FQDN without DNS infrastructure.....	75
Logoff options.....	75
Chapter 8: UCM Network configuration.....	77
Navigation.....	77
Elements.....	77
Manage elements using the edit navigation tree.....	77
Adding a group.....	78
Adding elements.....	79
Editing an element.....	80
Editing a group.....	81
Removing items using the Edit Navigation Tree.....	82
Assigning an element alias.....	83
Removing an element alias.....	83
Manage elements using table view.....	84
Starting a managed element.....	84
Adding a Hyperlink.....	85
Adding a CallPilot Messaging element.....	87
Edit Element properties.....	88
Editing the properties of a hyperlink element.....	88
Editing the properties for a CS 1000 element.....	89
Editing the properties of a Linux base element.....	91
Editing the properties of a Network Routing Service element.....	92
Editing the properties of a CallPilot Messaging element.....	92
Deleting selected elements.....	93
Prerequisites.....	93
CS 1000 Services.....	94
IPsec.....	94
Patches.....	94
SNMP Profiles.....	95
Secure FTP token.....	95
Software Deployment.....	95
Deployment targets.....	96
Chapter 9: UCM User Services configuration.....	97
Navigation.....	97
Administrative Users.....	97
Reviewing existing users.....	97
Adding a new local or external user.....	98
Editing user role mapping.....	100
Configure the properties of a local user.....	102
Editing the password and full name for a local user account.....	102
Disabling a user account.....	103
Enabling a user account.....	103

Deleting a user account.....	104
External Authentication.....	104
Authentication scheme policy.....	105
Editing the authentication scheme.....	105
Provision the authentication servers.....	106
Provisioning the LDAP Server.....	107
Provisioning the Radius Server.....	108
Provisioning the Kerberos Server.....	109
Password.....	109
Reviewing the status of a local account password.....	109
Changing a local account password.....	110
Chapter 10: UCM Security configuration.....	113
Navigation.....	113
Roles.....	113
Reviewing existing roles.....	114
Adding a custom role.....	114
Using templates for permission mapping.....	119
Assign or edit role mapping.....	120
Selecting users.....	120
Copying user assignment.....	121
Editing a role description.....	122
Deleting custom roles.....	123
Policies.....	123
Reviewing security policies.....	123
Editing password policies.....	124
Editing Session Properties.....	127
Security Settings.....	128
Editing the login warning banner.....	128
Editing the Single Sign-on Cookie Domain.....	129
Certificates.....	130
Viewing the details of a certificate endpoint.....	130
Updating the CRL.....	131
Downloading Private Certificate Authority Details.....	132
Revoking a certificate.....	132
Downloading the Certificate Revocation List (CRL) Details.....	133
Adding a CallPilot certificate.....	133
Active Sessions.....	134
Viewing active sessions.....	135
Terminating Single Sign-On sessions.....	135
Chapter 11: UCM Tools configuration.....	137
Navigation.....	137
Logs.....	137
Enabling OAM and Security logs for consolidation.....	137
Viewing log types with the network administrator role.....	138
Configuring or editing the configuration of logs for forwarding to third-party OSS.....	139
Viewing audit logs by date.....	141
Viewing Audit logs using the search functionality.....	141

Exporting the log file as a CSV file.....	142
Data.....	142
Appendix A: Migration to System Manager.....	143
Navigation.....	143
Migration option 1.....	144
Migration task flow (option 1).....	146
Premigration requirements.....	150
Migrating CS 1000 systems already upgraded to Release 7.5.....	150
Post migration requirements.....	152
Migration option 2.....	153
Migration task flow (option 2).....	154
Configuring UCM to appear on System Manager.....	158
System Elements migration task flow.....	159
Registering CS 1000 UCM Linux members to System Manager.....	160
Registering VxWorks servers to SMGR.....	161
Registering CS 1000 Primary security server and co-resident applications to System Manager.....	162
Software deployment.....	162
Linux Base system upgrade.....	163
Adding a software load from the client machine.....	164
User management.....	164
Manually redefining deployment distributions and server groupings.....	164
Additional information.....	165
VxWorks systems and devices.....	165
Co-resident Call Server and Signaling Server systems.....	167
Add or remove elements from the UCM security domain.....	167
Appendix B: Certificate authorities.....	171
Navigation.....	172
TLS certificate authorities on Session Manager and Primary UCM.....	172
TLS certificate authorities task flow.....	173
Adding a UCM primary certificate authority on Session Manager.....	173
System Manager certificate authorities on the UCM primary server.....	175
Adding a TLS certificate authority on Session Manager with UCM on System Manager.....	176
TLS certificate authorities for One-X Communicator.....	179
Adding a UCM primary certificate authority for the One-X Communicator.....	180
Adding a One-X Communicator root CA to UCM.....	180
Adding a certificate for SIP TLS.....	181
Index.....	183

Chapter 1: New in this release

The following sections detail what is new in this document for Avaya Communication Server 1000 Release 7.5.

Navigation

[Features](#) on page 11

Features

See the following sections for information about feature changes:

UCM migration to System Manager

For Communication Server 1000 Release 7.5, Avaya Aura® System Manager 6.2 is available for managing systems with Avaya Aura® Session Manager or Avaya Aura® Presence Services. The functionality of UCM is now available in System Manager. In networks that do not use Avaya Aura® Session Manager or Avaya Aura® Presence Services, you can continue to use UCM without migrating to System Manager for Communication Server 1000 Release 7.5.

Note:

- On systems where System Manager is available, the term UCM in the documentation refers to UCM in System Manager.
- On systems where System Manager is not available, the term UCM in the documentation remains unchanged.

For more information, see [Migration to System Manager](#) on page 143.

Other changes

See the following section for information about changes that are not feature-related.

Revision History

February 2013	Standard 05.21. This document is up-issued to support Avaya Communication Server 1000 Release 7.5.
February 2013	Standard 05.20. This document is up-issued to support Avaya Communication Server 1000 Release 7.5. The date format has been changed in the procedure Viewing audit logs by date on page 141.
January 2013	Standard 05.19. This documented is up-issued for System Manager 6.2.
January 2013	Standard 05.18. This documented is up-issued to reflect changes in technical content in the section Backup security server on page 42.
February 2012	Standard 05.17. This document is up-issued to include new information in the section Registering VxWorks servers to SMGR on page 161.
December 2011	Standard 05.16. This document is up-issued to include updates to the Assign or edit role mapping section.
October 2011	Standard 05.15. This document is published to support Avaya Communication Server 1000 Release 7.5. Fixes to migration content.
August 2011	Standard 05.13 and 05.14. This documented is up-issued to support Avaya Communication Server 1000 Release 7.5. Added migration requirements to Appendix A: Migration to System Manager.
August 2011	Standard 05.12. This document is up-issued to support Avaya Communication Server 1000 Release 7.5. Changes were made to the Migration to System Manager appendix. Option 2 was added.
June 2011	Standard 05.11. This document is up-issued to include updates to the Overview section. A statement is added describing browser requirements.
June 2011	Standard 05.10. This document is up-issued to support Avaya Communication Server 1000 Release 7.5 to reflect changes in technical content for registering VxWorks servers to SMGR, added procedures for TLS certificates, updated the procedures for Adding a custom role, and added a note for two instances of RBAC for System Manager 6.1.
January 2011	Standard 05.09. This document is published to support Avaya Communication Server 1000 Release 7.5 to reflect changes in technical content for uploading the CS 1000 Linux Base image to SMGR from a client machine.
January 2011	Standard 05.08. This document is published to support Avaya Communication Server 1000 Release 7.5. Fixes to migration content.
November 2010	Standard 05.07. This document is published to support Avaya Communication Server 1000 Release 7.5.

November 2010	Standard 05.01 to 05.06. These documents were issued to support Avaya Communication Server 1000 Release 7.5
June 2010	Standard 04.01. This document is up-issued for Avaya Communication Server Release 7.0.
August 2009	Standard 03.07. This document is up-issued for Communication Server Release 6.0. More clarity was added to the procedures about changing the FQDN of a member server.
July 2009	Standard 03.06. This document is up-issued for Communication Server Release 6.0.
July 2009	Standard 03.05. This document is up-issued for Communication Server Release 6.0.
June 2009	Standard 03.04. This document is up-issued for Communication Server Release 6.0.
June 2009	Standard 03.03. This document is up-issued for Communication Server Release 6.0.
May 2009	Standard 03.02. This document is up-issued for Communication Server Release 6.0.
May 2009	Standard 03.01. This document is up-issued for Communication Server Release 6.0.
July 2008	Standard 02.11. This document is up-issued to reflect changes in Security management.
February 2008	Standard 02.10. This document is up-issued to reflect changes in technical content.
February 2008	Standard 02.09. This document is up-issued to reflect changes in technical content.
January 2008	Standard 02.08. This document is up-issued to reflect changes in technical content.
December 2007	Standard 02.07. This document is up-issued to reflect changes in technical content.
December 2007	Standard 02.06. This document is up-issued to reflect changes in technical content.
December 2007	Standard 02.05. This document is up-issued to support Communication Server 1000 Release 5.5.
October 2007	Standard 01.05. This document is up-issued to reflect changes in technical content. Reference to Telephony Local Area Network (TLAN) in the Introduction chapter corrected.
September 2007	Standard 01.04. This document is up-issued to reflect changes in content. Addition to Elements chapter as per CR Q01739494.

New in this release

- | | |
|-----------|---|
| July 2007 | <p>Standard 01.03. This document is up-issued to reflect changes in content.</p> <ul style="list-style-type: none">• Addition to Security management chapter as per CR Q01688518.• Addition to Enterprise Common Manager overview chapter as per CR Q01662496.• Addition to Enterprise Common Manager overview chapter as per CR Q01688543. |
| June 2007 | <p>Standard 01.02. This document is up-issued to reflect changes in content:</p> <ul style="list-style-type: none">• Addition to Security chapter as per CR Q01639381-01. |

Chapter 2: Customer service

Visit the Avaya Web site to access the complete range of services and support that Avaya provides. Go to www.avaya.com or go to one of the pages listed in the following sections.

Navigation

- [Getting technical documentation](#) on page 15
- [Getting product training](#) on page 15
- [Getting help from a distributor or reseller](#) on page 15
- [Getting technical support from the Avaya Web site](#) on page 16

Getting technical documentation

To download and print selected technical publications and release notes directly from the Internet, go to www.avaya.com/support.

Getting product training

Ongoing product training is available. For more information or to register, go to www.avaya.com/support. From this Web site, locate the Training link on the left-hand navigation pane.

Getting help from a distributor or reseller

If you purchased a service contract for your Avaya product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

Getting technical support from the Avaya Web site

The easiest and most effective way to get technical support for Avaya products is from the Avaya Technical Support Web site at www.avaya.com/support.

Chapter 3: Introduction

This document contains information about the components, features, and benefits of the Unified Communications Management (UCM) Common Services. It describes UCM security management, including the various user account and identity configuration options and security policies for password thresholds. The document describes authorizations and permissions for built-in and custom role permission assignments that provide access control to the Common Services.

This document also provides information for the following tasks:

- how to review and configure local account password policies
- how to manage and configure elements within UCM
- how to manage and configure users, roles, and permissions within UCM
- how to upgrade the primary or backup security service and member server
- how to configure system account passwords and Telephony Local Area Network (TLAN) and Embedded Local Area Network (ELAN) network interface IP addresses for the various server types within UCM

Navigation

- [UCM overview](#) on page 19
- [Security Services overview](#) on page 47
- [Security server configuration](#) on page 61
- [Logon and logoff options in UCM](#) on page 71
- [UCM Network configuration](#) on page 77
- [UCM User Services configuration](#) on page 97
- [UCM Security configuration](#) on page 113
- [UCM Tools configuration](#) on page 137

Chapter 4: UCM overview

This chapter provides an overview of Unified Communications Management (UCM) Common Services and the required components.

Navigation

- [Introduction](#) on page 19
- [UCM navigation tree](#) on page 23
- [Applications and services](#) on page 35
- [UCM client capacity](#) on page 36
- [Benefits and features](#) on page 37
- [Central authentication](#) on page 38
- [Security domain](#) on page 38
- [Certificate management](#) on page 40
- [Server types](#) on page 42
- [High Availability configuration](#) on page 44

Introduction

The UCM solution provides an intuitive, common interface to manage and run managed elements. UCM is a container that stores several system management elements in a single repository. You have access to all network system management elements under the Unified Communications Management solution. You need to sign in only once to access the elements. A single sign-on eliminates the need for you to reauthenticate when a system management application starts.

UCM Security Services simplifies security control for managed elements and system management applications. UCM Security services manage secure access to Web applications and provide authentication and authorization with a single unified Common Service. UCM secures the delivery of essential identity and application information.

With UCM Common Services, administrators can control which users have access to specific managed elements. They can assign users to roles and map the permissions to those roles

to control which operations a user can perform on an assigned managed element. Users can access only assigned elements and perform only the tasks specific to their assigned role and permissions for an element.

With UCM Common Services, the integration of managed elements within a single container provides users with centralized security, user access control, simplified management tasks, improved workflow efficiency, convenience, and time-saving advantages.

UCM Deployment Manager provides two methods for software deployment:

- centralized software deployment (recommended)
- local software deployment

UCM Common Services supports Microsoft Internet Explorer 6.0, 7.0, and 8.0. Other versions and browsers are not tested or supported.

Note:

The PC used for web browser access to UCM must be connected to the TLAN (except for networks in the Managed Services configuration).

Linux Platform Base and Applications can run on the following hardware platforms:

- CP PM card
- CP DC card
- CP MG card
- COTS Servers
 - IBM x306m
 - HP DL320 G4
 - IBM x3350
 - Dell R300

Important:

To connect a terminal to the IBM X3350, you require a 9-pin female to 9-pin female null modem cable, part number NTRX26NPE6.

Note:

For web browser access to UCM, the address must be entered in IPv4 format. IPv6 is not supported.

You require only one primary security server for each secured domain. A network supports only one backup security server. Replication is unidirectional from the primary to the backup. You can perform all administrative changes, for example, security configuration and identity management, on the primary security server.

Avaya Communication Server 1000 task flow

This section provides a high-level task flow for the installation or upgrade of an Avaya Communication Server 1000 system. The task flow indicates a recommended sequence of events to perform when you configure a system and provides the technical document number that contains the detailed procedures required for the task.

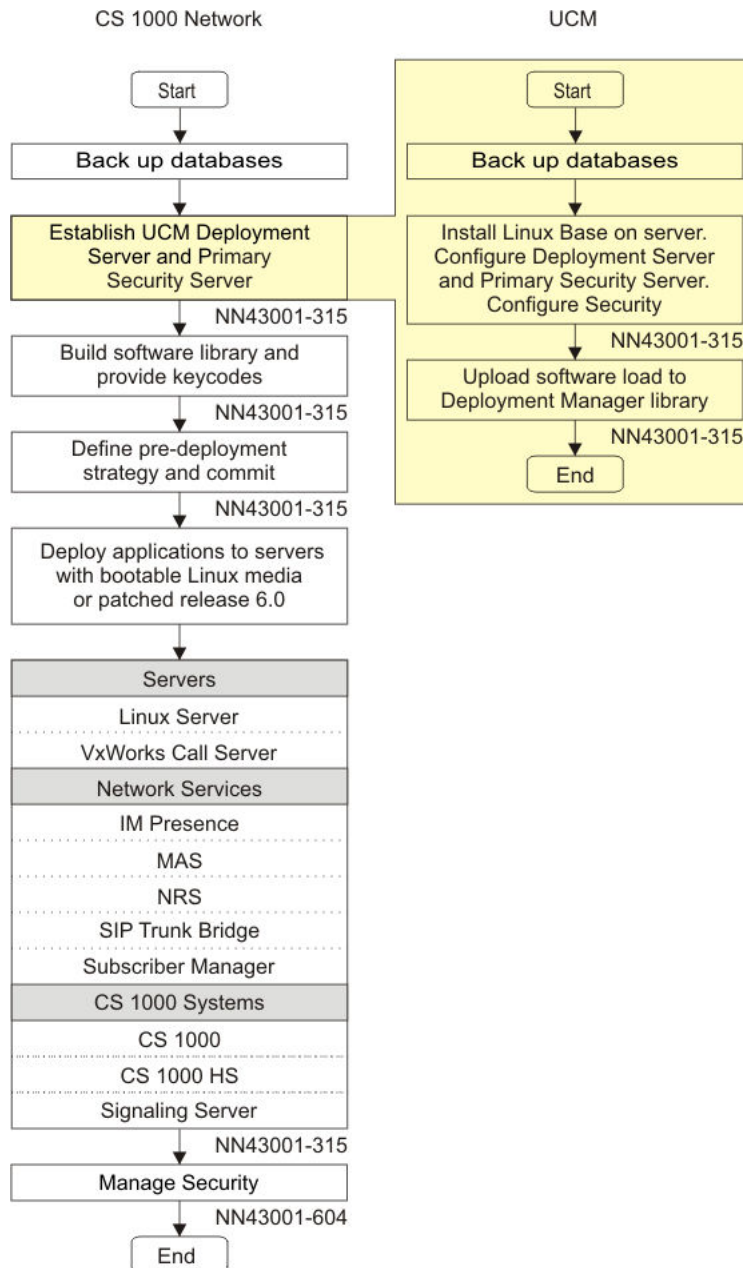


Figure 1: CS 1000 task flow

For more information, see the following technical documents.

- *Avaya Linux Platform Base and Applications Installation and Commissioning, NN43001-315*
- *Avaya Network Routing Service Fundamentals, NN43001-130*
- *Avaya Communication Server 1000M and Meridian 1 Large System Upgrades Overview, NN43021-458*
- *Avaya Communication Server 1000E Software Upgrades, NN43041-458*

- *Avaya Signaling Server IP Line Applications Fundamentals, NN43001-125*
- *Avaya Branch Office Installation and Commissioning, NN43001-314*
- *Avaya SIP Line Fundamentals, NN43001-508*
- *Avaya Security Management Fundamentals, NN43001-604*

UCM navigation tree

The UCM navigation tree is on the left side of the Web page. The root level branches are as follows:

- Network: Network-level objects, network navigation, and device management
- User Services: User-related objects and identity management
- Security: UCM Security Services objects and security policy management
- Tools: Logging services

The following figure depicts the UCM main navigation page.

Avaya Unified Communications Management

Host Name: bwfox1ssl.cnda.avaya.com Software Version: 02.20.0003.00(3778) User Name design

Elements

New elements are registered into the security framework, or may be added as sir its management service. You can optionally filter the list by entering a search term

Search Reset

Add Edit Delete

Element Name	Element Type	Release	
1 <input type="checkbox"/> EM on bwfox1ssl	CS1000	7.5	
2 <input type="checkbox"/> EM on bwhtssipsunvSSL	CS1000	7.0	
3 <input type="checkbox"/> bwhtssipsunvssl.cnda.nortel.com (member)	Linux Base	7.0	
4 <input type="checkbox"/> bwfox1ssl.cnda.nortel.com (primary)	Linux Base	7.5	
5 <input type="checkbox"/> 135.20.225.72	Media Gateway Controller	7.0	
6 <input type="checkbox"/> 135.20.225.70	Media Gateway Controller	7.0	135.20.225.70 element.
7 <input type="checkbox"/> 47.20.225.70	Media Gateway Controller	7.0	47.20.225.70 New element.
8 <input type="checkbox"/> NRS on kwei	Network Routing Service	6.0	47.11.65.9 New element.

Copyright 2002-2010 Avaya Inc. All rights reserved.

Launches Patching Manager

Launches SNMP Profile Manager

Launches Deployment Manager

Launches Subscriber Manager

Launches Element Manager

Launchers Base Manager

Launches NRS Manager

Figure 2: UCM main navigation page

UCM basics

Two methods are available to use the UCM Common Services interface: table view and tree view.

- The table view is the default view. From the table view, you can add, edit, or delete elements. For more information, see [Table view](#) on page 24 .
- The tree view is a hierarchical view. From the tree view, you can create groups of elements according to your business needs. For example, an administrator can create a group in the tree for elements that are part of a specific CS 1000 node. You can nest groups. For more information about using the tree view, see [Tree view](#) on page 24.

Use the following icons on the UCM main navigation page to change your view. To update the list, click the refresh icon.

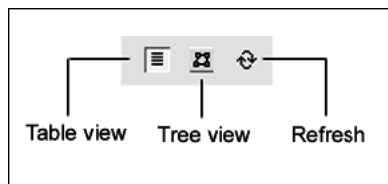


Figure 3: Element icons

Table view

Table view is the default view on the Elements page. You see a list of UCM Common Services elements that are based on your role permissions. A network administrator can see all elements. From the table view, you can add, edit, or delete elements.

Secured elements in Security Services may be subject to authentication because single sign-on is not available for elements outside UCM Security Services. You can search and filter elements from the Elements page. Search for a managed element by Element Name, Element Type, Release, or Address.

Tree view

The Network group is the root level of the tree view. To navigate, click an element name and the Web browser is redirected to the management application of that element. If the element is a secured element in Security Services, no sign-on is required. If the element is a third-party element (such as a Hyperlink element), the administrator is subject to administrator authentication, as single sign-on is not available. In some instances, groups appear as links in the tree, and this indicates that an element is associated with the group. For example, a group representing a node can be associated with the node master element. Click the group name to navigate to the associated element. When the tree appears in navigation mode, only

the elements that the administrator is authorized to access appear. The tree expands to the second level by default.

The System Groups contains two member groups: All Elements and System Types. The All Elements group contains all the elements visible in the list view sorted alphabetically by element name. The System Types group contains groups of elements by system type, such as CS 1000 or Hyperlink. Elements in each folder are sorted alphabetically by element name. Click an element in a system group to navigate to the management application running on that element.

Central launch point and common User Interface

The UCM security domain provides a central launch point for installed managed elements and hyperlinks. You can access a managed element when you log on to UCM Common Services or through a direct Web link.

On the Elements Web page, you can access an element by performing one of the following tasks:

- Click an element item

The selected element starts in the current browser window and replaces the UCM Common Services or element interface.

- Right-click the element to open the element in a new browser window.
- Select an element from the Favorites list in the browser window.

The selected element starts in the current window and replaces the UCM Common Services or element interface.

To add an element to your Favorites list, right-click the element and select Add to Favorites.

UCM Common Services is a common User Interface that remains consistent between other element applications. UCM Common Services displays the items, specific to the selected element, in the left navigation pane. For example, if a user selects NRS Manager from the element list, the NRS Manager replaces the UCM Common Services interface in the browser window and the NRS Manager navigation items appear in the left navigation pane.

Click Common Manager from the navigation pane to return to UCM Common Services.

Button bar

The most frequently used commands are available in the top right-pane of the Edit Navigation tree. Frequently used commands are Add Group, Remove, Edit, and Undo. These commands are also available from the shortcut menu when you right-click an element or group.

Important:

Buttons appear dimmed if you do not select the appropriate number of elements for a command.

Undo feature

Use the Undo button in the button bar to cancel the last modification to the tree. You can undo up to 10 changes. If you saved the changes to the Edit Navigation tree, you cannot undo the changes.

Cut, Copy, and Paste commands

You can use cut, copy, and paste to move items in the tree or to copy groups.

- For a single item, right-click the item and select Copy from the shortcut menu.
- For multiple items, hold the Ctrl key and left-click the items to copy or move. Right-click on the selection and select Copy from the shortcut menu.
- For a range of items, left-click the first and last items. All the elements between and including the first and last item are selected. Right-click the selection and choose Copy from the shortcut menu.

Paste the selected items by right-clicking the destination group and choosing Paste from the shortcut menu.

The items in the copy buffer are added to the bottom of the destination group.

Important:

The target of a paste operation must be a group.

You can paste items in the copy buffer multiple times until the copy buffer is over written by another copy operation.

Items that are cut but not pasted into the tree are removed from the tree.

Network

The Network section contains the following items:

- [Elements](#) on page 77
- [CS 1000 Services](#) on page 94

- [Software Deployment](#) on page 30
- [Subscriber Manager](#) on page 30

Elements

The Elements page is the default Web page that opens when UCM Common Services starts. The Elements section contains links to the managed elements (application plug-ins and bookmarks). From this Web page users can add a new element or edit or delete an existing element. You can also access base manager by clicking on an element.

Users can add, edit, or delete elements within Security Services.

The following is a list of the supported element types:

- Linux base
- CS 1000
- Network Routing Service Manager (NRSM)
- Media Gateway Controller (MGC)
- MC32
- Media Application Server (MAS)
- Hyperlink
- CallPilot (Available only when Subscriber Manager is deployed.)

When you click on the CallPilot element, you are redirected to the CallPilot logon page that was configured for the selected element. Use your CallPilot logon credentials to log on.

Important:

Users see only the elements that are enabled based on the assigned role permissions.

CS 1000 Services

This section contains the following items:

- [IPsec](#) on page 28
- [Patches](#) on page 29
- [SNMP Profiles](#) on page 29
- [Secure FTP token](#) on page 29

Corporate Directory

The Communication Server 1000 Corporate Directory allows M3900 digital telephones and IP Phones to display and access a corporate-wide telephone directory. UCM Common Services provides a Corporate Directory application that generates the corporate directory file and uploads it to CS 1000 systems.

For more information Corporate Directory, see *Signaling Server IP Line Applications Fundamentals*, NN43001-125.

IPsec

IP security (IPsec) is centrally managed from the UCM Primary Security server using the IPsec for Intra System Signaling Security (ISSS) management interface. ISSS employs IPsec to provide security services, including confidentiality, authentication, and anti-replay, to application layer protocols.

From the ISSS interface on the Primary UCM server, you can administer several aspects of IP security, such as configuring a domain-wide security policy, adding and removing IPsec targets, enabling or disabling IPsec for network elements, and scheduling IPsec synchronization and activation.

Changes to the security policy are securely distributed to the network elements by the UCM transfer mechanism and activated according to a schedule defined by the administrator. Automatically scheduled distribution and activation allows changes to IPsec configurations without individually reconfiguring each element in the UCM security domain.

The ISSS management interface lists all Avaya Communication Server 1000 and Communication Server 1000 HS systems available on the UCM domain. ISSS can be enabled only on those UCM targets which belong to a CS 1000 system or CS 1000 HS system. ISSS parameters (PSK & level) are specified as a Security policy that can be applied to one or more Communication Server 1000 systems or a Communication Server 1000 High Scalability (HS) systems. ISSS operations like Synchronization and Activation can be performed on one or more CS 1000 systems simultaneously.

For procedures relating to ISSS, see *Avaya Security Management Fundamentals*, NN43001-604.

Numbering Groups

A numbering group represents common numbering planning attributes which are shared by a group of subscriber telephony accounts. Each telephony account can belong to only one numbering group. If a telephony account does not belong to a specified numbering group, it is classified as a member of the default numbering group category. A member of the default

numbering group category only uses a private numbering plan (private CDP and UDP dialing). The Numbering Group application is installed in UCM Common Services at the Network level under CS 1000 Services.

For more information about Numbering Groups, see *Signaling Server IP Line Applications Fundamentals*, NN43001-125.

Patches

Use Avaya Patching Manager by logging on to UCM from the primary security server to remotely deploy patches from a central location to other Linux servers on the same security domain. From the Avaya CS 1000 server, click Patches. A central patching library is maintained and patches can be uploaded and centrally deployed on all Linux elements in the security domain.

You can install patches locally. Local Patching is accessible from the Base Manager of each Linux Element. Access Patching Manager by logging on to the primary security server and clicking an element or by logging on locally to the element.

Accounts must have Patch Administrator permissions assigned for access to Patching Manager. Local logon users have full permissions to use the local Patching Manager. For more information about Patching Manager, see *Avaya Patching Fundamentals*, NN43001-407.

SNMP Profiles

Use the Simple Network Management Protocol (SNMP) Profile Manager to perform configuration at the network level for CS 1000 and stand-alone UCM elements such as a stand-alone primary security server and stand-alone NRS. You can configure using the following:

- **SNMP Profile:** Configure SNMP profiles in UCM such as adding or deleting.
- **SNMP Distribution:** Assign and send SNMP profiles to Elements configured in UCM.

To send SNMP traps, you must configure SNMP parameters such as the SNMP trap destination. You can centrally configure the SNMP parameters including the SNMP trap destination in profiles by using SNMP Profile Manager. SNMP profiles are then assigned and propagated to all devices in the UCM security domain. You must configure SNMP for the Linux element; otherwise, no information is available about where to send SNMP traps. For more information about configuring SNMP Profiles, see *Avaya Communication Server 1000 Fault Management — SNMP*, NN43001-719.

Secure FTP token

From the CS 1000 Services, click Secure FTP Token. The Secure FTP Token Management page appears on which you can view the date of the most recent generated token, refresh the status of the current token, and regenerate a new token for distribution throughout the network.

You can search and filter for secure FTP token endpoints by typing in the endpoint address or token transfer status from the Secure FTP Token Management page. For more information about Secure FTP Token, see *Avaya Security Management Fundamentals*, NN43001-604.

Software Deployment

Use Deployment Manager on the Primary security server for an end-to-end installation and configuration of Linux Base and applications. Deployment Manager provides a simplified and unified solution that enables network installation of Linux Base on target servers. The Primary security server is the Deployment Server.

On the UCM navigation pane click Network, Software Deployment. The Deployment Manager Web page appears on which you can select the following:

- Deployment View
- Software Loads
- Backups
- 6.0 Deployment Targets

You can deploy software locally before the server joins the security domain; however, Avaya recommends that you use the central deployment method.

For more information about Software Deployment, see *Avaya Linux Platform Base and Applications Installation and Commissioning*, NN43001-315.

Subscriber Manager

In the Network branch of the UCM navigation tree, click Subscriber Manager. Subscriber Manager centrally manages subscribers and subscriber accounts from the primary security server and provides a central location from which to manage subscriber information for enterprise services. With Subscriber Manager, users can easily manage subscribers and subscriber accounts (phone services) within a network.

Prior to the UCM Subscriber Manager, subscribers and accounts were managed by individual element managers or element management systems. Subscriber Manager eliminates the need to configure and manage separate subscriber management applications for specific products in a management system.

For more information about Subscriber Manager and how to configure subscribers and subscriber accounts (phone services), see *Avaya Subscriber Manager Fundamentals*, NN43001-120.

User Services

In the User Services branch of the UCM navigation tree, you can select the following items:

- **Administrative Users:** You can view administrative users, add a new administrative user, or disable or delete an existing administrative user.
- **External Authentication:** The External Identity Repositories Web page contains a summary page for authentication scheme and authentication servers. In the Authentication Servers page you can configure an LDAP server, RADIUS (Remote Authentication Dial-in User Service) server, or a Kerberos server. For more information about configuring these servers, see [Provision the authentication servers](#) on page 106.
- **Password:** View the status for a password or to change the password.

Security

In the Security branch of the UCM navigation tree, you can select the following items:

- **Roles:** View user role assignments or to add or delete a role name. Users can also view the element permissions and description assigned to a role.
- **Policies:** Configure the authentication scheme and authentication servers, establish password policies, and edit security settings.
- **Certificates:** Configure the information for certificate configuration status.
- **Active Sessions:** Display all users who are currently logged on and the session time for each user.

For more information about Security configuration, see [Navigation](#) on page 113.

Tools

In the Tools branch of the UCM navigation tree, select the following items:

- [Logs](#) on page 32
- [Data1](#) on page 34

Logs

In the Tools branch of the UCM navigation tree, click Logs. The Logs Web page appears.

From the central UCM primary security server, use the log viewer tool to view Security and Operation, Administration, and Maintenance (OAM)-related audit logs.

Log on as network administrator to perform the following functions:

- Filter the log based on the query string and event types.
- View the log for a specific date.
- Configure the remote SYSLOG server to forward audit logs in real time to the third-party Operational Support System (OSS) SYSLOG server for monitoring and analyzing.
- Export the log as a comma-separated value (CSV) file.

Important:

You must log on as a network administrator to view the Logs link.

No restrictions exist to the number of users that can simultaneously access the Log Viewer tool when they log on with the network administrator role. Log files must be less than 5 megabytes (MB) to view using the Log Viewer tool. If the log file size exceeds 5 MB, a link is available to export and download the file.

Log storage

Operation, Administration, and Maintenance (OAM) and application logs are stored on the Linux server where they are generated. For optimal access control and to maintain an audit trail of all system administrator activities and security-related events, the OAM logs from the backup and member servers are forwarded to the UCM primary security server as the central storage location. OAM logs are provided for the CS 1000 management applications running on a Linux platform to record security, operational, configuration, and maintenance events. Application logs are stored locally on a Linux server and are not forwarded to the primary security server for consolidation.

The oam.log and security.log files are created daily on the primary security server with the date appended to the log file name. The logs are stored in /var/log/nortel/OAM. You must restart the syslog service at the CLI level when you manually modify the syslog files. To restart the syslog service, log on as a root user and run the command `/sbin/service rsyslog restart`.

During the Linux base installation, 10 percent of the total hard disk space is allocated for the storage partition and cannot be changed. Log files for all Avaya applications can be found in /var/log/nortel. You can access these log files by logging on as a root user at the CLI level. The Linux base alarm script monitors the partitions. If storage capacity is reached, a Linux console message appears.

Use the Log Viewer Tool to view the application and OAM logs. You can display the log for the last 30 days, sort by field, or filter and export the log as a comma-separated value (CSV) file.

Important:

The log files are stored on the primary security server and have a 30-day rotation.

Log configuration :

The following table shows the logs files stored in the /var/log/nortel/OAM folder of the UCM primary security server.

Table 1: UCM primary security server log files

Log file type	Description
OAM logs are stored in two files based on the type of logging event:	
Audit logs: oam.log	<p>Storage location of all OAM administration events that occur from the CS 1000 management applications running on a Linux platform:</p> <ul style="list-style-type: none"> • Operational events—captures the query for status and enabling or disabling resources. • Configuration events—captures all the feature or functional provisioning and modifications. • Maintenance events—captures all the upgrades, backups, restores and patching.
Security logs: security.log	<p>Storage location of all security related events:</p> <ul style="list-style-type: none"> • security policy changes • Linux CLI messages—captures logon and logoff attempts. • logon success and failures • certificate changes • user account creation and illegal (failed) login events • Any OAM security event where network administrator privilege (or flag) is enabled or required.
Application logs are generated using the Syslog framework at a Linux operating system level. View Application logs stored on a local system by using the Log Viewer tool from the base manager.	
Application logs	<p>These applications include the following:</p> <ul style="list-style-type: none"> • LTPS • SIP Line Gateway • SIP Signaling Gateway • NRS Routing bundle (NCS, H323, and SIP Redirect Server) • Management bundle • Linux Base log

Log file type	Description
	<ul style="list-style-type: none"> • CP PM Co-resident Signaling Server • Any other Avaya-specific application log

Forwarding logs to third-party OSS

The consolidated OAM audit logs from the primary security server can be forwarded in real time to external third-party Operation Support System (OSS) Syslog servers for monitoring and analyzing. You must configure the third-party OSS syslog server before audit log forwarding can occur. The following is the list of values assigned to each severity level.

- Emergency: 0
- Alert: 1
- Critical: 2
- Error: 3
- Warning: 4
- Notice: 5
- Information: 6
- Debug: 7

Severity is listed in order of lowest priority. All messages with the selected priority and the priorities below it are forwarded, for example, if you select Alert, this forwards Alert and Emergency messages.

For more information about configuring, see [Configuring or editing the configuration of logs for forwarding to third-party OSS](#) on page 139.

Important:

Only OAM logs from the primary server can be configured for forwarding. Application logs based on syslog format cannot be forwarded using this feature. Once the configuration is saved, the forwarding of the OAM audit logs occurs.

Archived files

The archived files for both oam.log and security.log are in a compressed format. The naming convention for the archived files is xxx.log-YYYYMMDD.gz.

Data

Use the reload data tool to synchronize the server after the backup server has been restored or upgraded. For more information, see [Data](#) on page 142.

Caution:

The reload data tool deletes data. Use with caution.

Applications and services

The following table identifies the applications deployable within the UCM Common Services.

Table 2: UCM Applications

Services and applications	Description and document reference
UCM Patching Manager	The Patching Manager centrally deploys patches from the primary security server to other Linux servers in the same security domain. For more information, see Patches on page 29 and <i>Avaya Patching Fundamentals</i> , NN43001-407.
UCM Deployment Manager	The Deployment Manager on the Primary security server (Deployment Server) provides an end-to-end installation and configuration of Linux base and applications on a Server. Deployment Manager also provides backup services of Linux elements. For more information, see <i>Avaya Linux Platform Base and Applications Installation and Commissioning</i> , NN43001-315.
IPsec Manager	The IPsec Manager centrally configures security services, including confidentiality, authentication, and anti-replay, to application layer protocols from the primary security server. IPsec settings are configured for all elements in the security domain. For more information, see <i>Avaya Security Management Fundamentals</i> , NN43001-604.
CS 1000 Element Manager	See <i>Avaya Element Manager System Reference — Administration</i> , NN43001-632.
Network Routing Service Manager	The NRS Manager runs on the same element as NRS. NRS Manager centrally configures, provisions, and maintains the NRS from the primary security server to other Linux servers in the same security domain. For more information, see <i>Avaya Network Routing Service Fundamentals</i> , NN43001-130.
Base Manager	The Base Manager, a Web-based interface, is used for low level configuration of all Linux elements. For more information, see <i>Avaya Linux Platform Base and Applications Installation and Commissioning</i> , NN43001-315.
Subscriber Manager	The Subscriber Manager centrally manages subscribers and subscriber accounts from the primary security server. For more information, see <i>Avaya Subscriber Manager Fundamentals</i> , NN43001-120.
SNMP Profile Manager	The SNMP Profile Manager centrally configures SNMP parameters for all elements from the primary security server to other Linux servers in the same security domain. For more information, see

Services and applications	Description and document reference
	<i>Avaya Communication Server 1000 Fault Management — SNMP, NN43001-719.</i>
Secure FTP Token	The Secure FTP Token on the UCM Backup security server refreshes the status of the current token or regenerates a new token for distribution throughout the network. For more information, see <i>Avaya Security Management Fundamentals, NN43001-604.</i>
Media Application Server	The Media Application Server (MAS) provides media services, such as IP Ad Hoc Conference, IP Music, IP Tone, IP RAN, and IP Attendant, to Communication Server 1000 systems. For more information, see <i>Avaya Signaling Server IP Line Applications Fundamentals, NN43001-125</i> or refer to the MAS documentation.

The following table identifies the services that are intrinsic to the UCM Common Services management framework.

Table 3: Services

Services	Description and document reference
UCM Security Service	Security Service is the primary interface for system-wide security configuration and administration and provides centralized authentication for users, systems, and devices by operating as a RADIUS server, providing authentication for RADIUS clients based on defined roles and policies. For more information, see Security Services overview on page 47 and <i>Avaya Security Management Fundamentals, NN43001-604.</i>
UCM Web Service	Web Service provides a common navigation hierarchy for installed management applications. With Web Services, you can develop new applications and customize scripts. For more information, see <i>Avaya Web Services API Applications, NN43001-640.</i>
UCM Logging Service	The Logging Service securely maintains a central audit trail of all system administrator Operation, Administration, and Maintenance (OAM) activities and security-related events. From the primary security server, you can use the log viewer tool to view Security and OAM-related audit logs. For more information, see <i>Avaya System Management Reference, NN43001-600.</i>

UCM client capacity

The following table lists the maximum number of UCMs, elements, and administrators supported for UCM client management systems.

Table 4: UCM client capacity

UCM, element, and administrator thresholds	Maximum capacity
The maximum number of elements supported in one UCM	5000
The maximum number of Linux members elements	1000
The maximum number of Vxworks Elements (MC/MGC/CS)	1000
The maximum number of concurrent active administrators supported within an UCM network	40
The maximum number of groups supported in UCM	100
The maximum number of administrators configured on one UCM	500
The maximum number of administrators connected simultaneously on one UCM	10 Important: Although 10 administrators can connect simultaneously, not all users can access the same elements within a system at the same time.
The maximum number of administrators connected simultaneously on the same element in a system with one or more UCMs	5

For information about installing Linux and the UCM applications, see *Avaya Linux Platform Base and Applications Installation and Commissioning, NN43001-315*.

You can increase the number of elements by adding supplementary UCM servers. Regardless of the number of UCM servers installed, all elements within the same security domain appear in each UCM navigation tree.

Benefits and features

UCM Common Services is a generic system management software infrastructure that provides the following benefits and features:

- central launch point for management facilities that oversee multiple network elements to manage the entire network
- common User Interface look and feel across all supported management facilities

- Web service interface where third-party developers can create applications to access UCM
- registry of the managed elements that start the management applications
- security that provides Authentication, Authorization, and Auditing (AAA) for plug-in Web applications (elements) that reside within UCM Common Services
- central security policy administration and enforcement
- private certificate authority and X.509 certificate management
- Single Sign-On (SSO) and external Lightweight Directory Access Protocol (LDAP) and Remote Authentication Dial-in User Service (RADIUS) authentication
- Role Based Access Control (RBAC) and Instance Level Access Control (ILAC)
- central point to manage users, passwords, and system access

Central authentication

The UCM Common Services provides a central GUI-based interface for individual account administration for the Avaya Communication Server 1000 network. This authentication feature implements a RADIUS client that authenticates with the external UCM security server for all VxWorks software platforms that the current Avaya Communication Server 1000 supports.

When a user attempts to gain access to any VxWorks system in the Communication Server 1000 network, they are prompted for a user name and password. The user name and password are encrypted and transferred to the centralized UCM security server by the RADIUS verification protocol. The UCM operates as a RADIUS server providing authentication for RADIUS clients. If the user name is defined in the UCM database, the user access is granted to the system with the privileges assigned to them as defined in the UCM database. Each VxWorks system and UCM database has a series of pre defined roles and groups.

Security domain

A UCM security domain is defined by the UCM primary security server. The UCM security domain comprises the UCM primary security server, the UCM backup security server, and associated member servers that contain UCM Common Services and management applications. Each primary and backup security server must co-reside with an instance of the LDAP server. Replication is unidirectional, from the LDAP primary to the backup. The primary security service or backup security service is not installed on a member server.

The primary security server must be the first server deployed in the security domain. The security domain can have 0 or 1 backup servers and additional servers are member servers, as shown in the following figure.

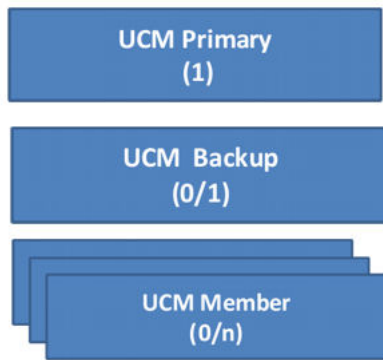


Figure 4: Security domain

The primary security server is trusted by all servers in the security domain and is based on Secure Shell (SSH) public key authentication. All servers in the security domain use the primary security server for authentication, authorization, and audit log storage. The `joinSecDomain` command, used to join the UCM security domain, uses the SSH client to communicate with the UCM primary security server but does not provide shell-level access. A VxWorks device joins UCM security domain by using the `joinSecDomain` command and a mutually trusted SSH tunnel is established with the UCM primary security server. VxWorks devices also send information such as a RADIUS secret over the channel to UCM which provides a unique secret with UCM for securing RADIUS communication. Shell level access to users is not provided. Support for Unsecured remote access methods such as `rlogin` and `Telnet` is available on the Avaya CS 1000 but you can disable them. For more information, see *Avaya Security Management Fundamentals, NN43001-604*.

When replication initializes between the backup security server and the primary security server, the backup security server is in standby mode with the primary security server. When the primary security server is offline, servers in the security domain switch automatically to the backup security server for authentication and authorization.

A management system can have one or more UCM servers that are part of the same security domain. The security domain provides central authentication, authorization, and auditing for secure navigation between managed elements. All elements appear in a single navigation tree within the same security domain and run independently of UCM Common Services. UCM Common Services provides the features and capabilities for all installed elements.

When a user logs on to UCM Common Services, the Elements Web page displays a list of installed elements. Reauthentication to access a different element within UCM is not necessary.

Certificate management

UCM uses certificate management: the X.509 certificate for Web Secure Sockets Layer (SSL) for secure communication between a Web browser and a Web server. The following built-in certificates types are available:

- Web interface using Secure Sockets Layer (Web SSL)
- Session Initiation Protocol signaling using Transport Layer Security (SIP TLS)
- Datagram Transport Layer Security (DTLS)

An Administrator can revoke certificates that were previously issued.

Within the UCM security domain, only one private Certificate Authority (CA) is used for Avaya CS 1000 to sign internally generated certificates. For certificate management, a private CA is configured only on the primary security server during installation. You cannot change the private CA.

Important:

A private CA is always available on the primary security server. A user can choose to install the private CA to set up the trust on their system.

When the SIP TLS certificates, signed by the private CA, are distributed to the Network Routing Service or SIP Gateway, the private CA is automatically added to the trusted CA list of the Network Routing Service or SIP Gateway. Therefore, if all the Network Routing Service and SIP Gateway elements use certificates signed by the private CA, mutual authentication for SIP TLS is configured automatically between them. Similarly, you can install a certificate signed by the private CA on the server for Web SSL, as shown in [Figure 5: Certificates for SIP TLS and for Web SSL](#) on page 41.

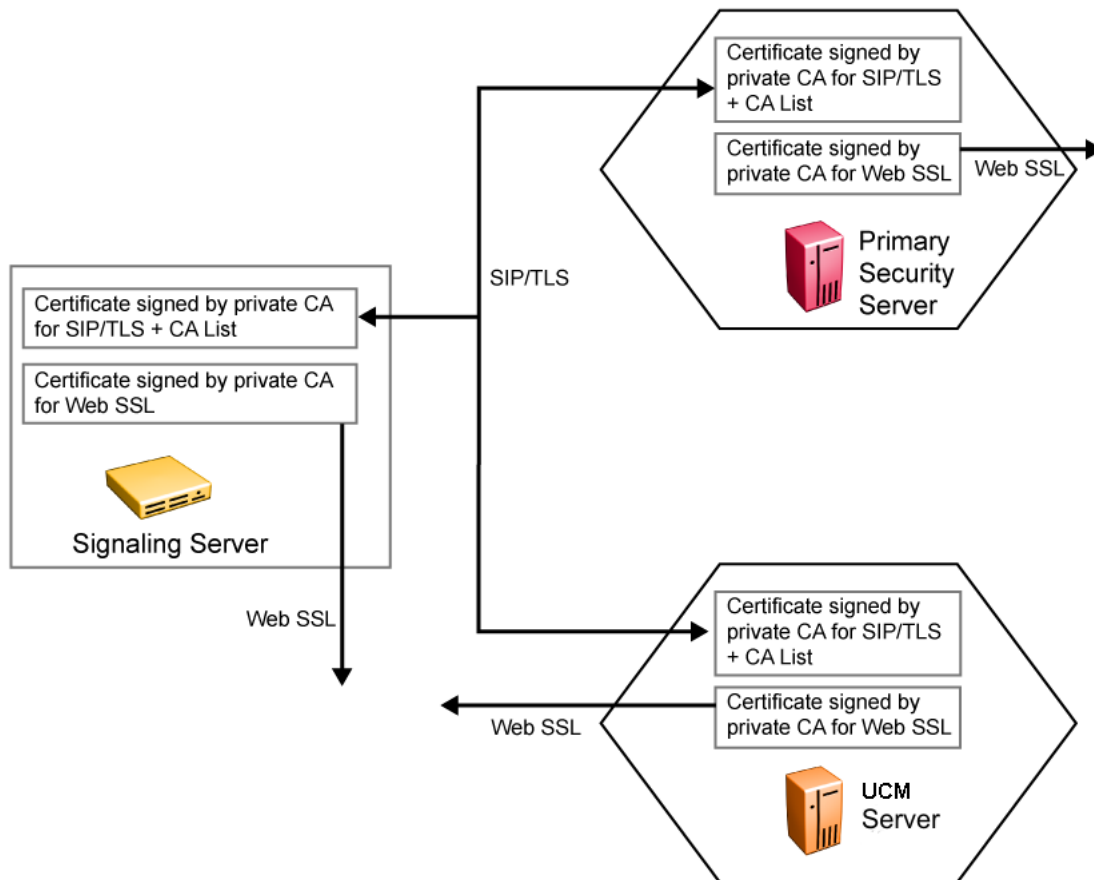


Figure 5: Certificates for SIP TLS and for Web SSL

Important:

You must configure certificate management through the primary security server Web interface. You cannot manage certificates in Web interfaces on other Linux servers.

Configuration for Secure Shell Trust of CA: SSH is used for the certificate management communication between SIP Proxy Servers (SPS). All SPS servers in the same security domain trust the primary security server where the private CA resides. The Rivest, Shamir, and Adleman (RSA) public key of the primary security server is entered into the authorized key lists of all the servers.

Web SSL: A Web SSL certificate for UCM is installed when you install the application. The network administrator must configure the Web SSL certificate through the Certificates link of UCM on the primary security server.

For more information about certificate management, see *Avaya Security Management Fundamentals*, NN43001-604.

Server types

This section describes the UCM security server roles. For more information about the configuration options, see [Security server configuration](#) on page 61.

Primary security server

Only one primary security server is required on a network. This server stores all administrator identities, authorization data, and security configuration data. The server contacts and queries all authentication, authorization, and logging. Administrators use the primary security server for navigation to UCM Common Services, network navigation, and the launch pad for network applications such as Subscriber Manager. A primary and backup security server can be demoted to a member server. For more information, see [Demoting a primary and backup server](#) on page 68.

The primary security server provides the following roles:

- Private certificate authority: only the primary security server can issue certificates for new member servers. The certificate management console access is only from the primary security server.
- Write access to all security-related data: configuration of all options in UCM Common Services can occur only on the primary server.

Backup security server

The role of the backup server is to manage authentication and authorization requests when the primary server cannot be contacted. The backup server is optional; only one backup security server can be on a network. You can start the backup server by accessing `http://<FQDN of backup>`.

Deploying an application (for example, SS or NRS) on a backup server puts that application in a non-dedicated mode.

The following figure shows the items that are available from the navigation pane. The elements table is shown but you cannot modify it.

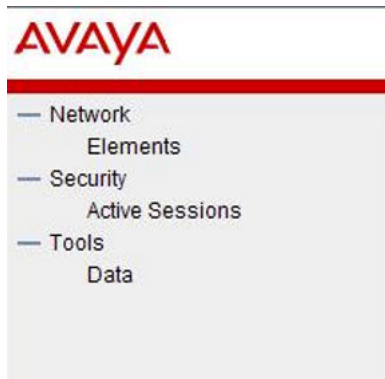


Figure 6: Backup server navigation pane

The backup security server provides the following roles when the primary server is unavailable:

- All authentication and authorization requests are managed.
- All certificates continue to function.
- Audit logs are recorded when the backup server handles authentication. No log synchronization occurs between the primary and backup. Avaya recommends that you manually transfer the OAM log files from the local servers to the primary security server and append them to the OAM file for that day.

Important:

You cannot use the backup security server to configure changes such as adding new administrators. The UCM Web pages and network navigation are available for viewing but the Certificate Management pages are not available for viewing or changing. The backup security server cannot be promoted to a primary security server. The backup server always maintains real-time synchronization with the primary server. A backup security repository is part of the backup server installation. This repository is read-only.

Member server

The member server is part of a secured network and is not a primary or backup security server. A member sends all security requests to the primary security server. No access is available to UCM Common Services and LDAP server is not running on it. For emergency situations, you can use a local logon page.

When an administrator types the URL of the member server, the member first verifies that the primary server is running. If the primary is running, then the user is forwarded to the primary server. If the primary is down then the user is forwarded to the backup. If the backup is also down, then the user goes to the local logon page of the member server.

If you try to access an application running on a member server, the member server attempts to use the first security server that responds, for example, a primary or backup server. The first primary or backup server to respond is the one closest to the member server. This approach is intended to load balance the security servers. Therefore, for a RADIUS server on the security

domain, the radius server must have records for both the primary and backup security servers with the same shared secret.

No session failover occurs on the member server. If an administrator is logged on to the primary server and it becomes unavailable, the administrator must log on to the backup server.

Important:

You must create two records in the external RADIUS server with the same shared secret for both the primary security server and backup security server IP address.

Domain Name System

During the Linux base installation, you are prompted to configure the Domain Name System (DNS) server IP address. Users can also manually configure the DNS after installing the Linux base. The DNS server IP address is stored in `/etc/resolv.conf`.

For more information about configuring the DNS server, see *Avaya Linux Platform Base and Applications Installation and Commissioning, NN43001-315*.

Disaster Recovery

A file backup and restore option supports the disaster recovery mechanism for the Linux Base and Avaya applications including UCM. For information about prerequisites and procedures for Avaya Linux system disaster recovery on a COTS or CP PM server, see *Avaya Linux Platform Base and Applications Installation and Commissioning, NN43001-315*.

High Availability configuration

High Availability (HA) provides continuous availability and reliability in case the active server fails or abnormally terminates. High availability is achieved by replicating the security repository, configuring a backup server, and replicating the admin users and policies data for redundancy.

In normal operation, an agent is installed on a member server. The agent talks to the security services on the primary security server. When the member server registers with the primary server, the member server receives a list of backup security servers.

The private Certificate Authority (CA) runs only on the primary security server. The CA is not a point of failure as it is not required to be online during normal operation. The CA is required only to sign Certificate Signing Requests (CSR). When the primary security server is down,

certificates between member servers remain valid and trusted because they each maintain a trusted CA list.

Important:


If the primary server must be rebuilt due to new hardware, the IP address and the Fully Qualified Domain Name (FQDN) of the new hardware must be the same as what was previously used.

- The primary security server hosts the private CA that signs a Certificate Signing Request (CSR) from other servers. If the IP or FQDN does not stay the same, then future CSRs signed by the new primary security server cause trust problems with older certificates on other servers.
- The agents on member servers have the FQDN of the primary security server. If the IP or FQDN cannot be reused and rebuilding the admin users, roles, and policies does not occur, then new CSRs must be issued and signed by the new CA and all member servers and backups must be manually updated with the location of the primary security server. Server types are not interchangeable. For example, member servers cannot change to a primary or backup security server.

The following table shows the HA failover scenarios for the primary and backup security servers and member server.

Table 5: Failover scenarios

Primary security server	Backup security server	Member server	Failover scenario
offline	online	online	<p>The member server checks the availability of the primary and backup security server. If the primary fails to reply, the member server switches to the backup security server. Failover can be triggered by failure of the security services, security repository, the network, or any other cause of the member failing to get a heartbeat.</p> <p>Updates to users and policy changes are not allowed on the backup security server. Updates to operational information such as time of last logon and number of logon attempts continues, but changes to this data revert to the previous values when the primary security server is restored.</p> <p>After the primary security server becomes available and the member server status is detected, the member server then switches back to the primary security server without administrator intervention. No manual process triggers failover or fallback.</p> <p>The audit trail logs are maintained independently on all security and member servers when the primary is down. When the primary server becomes available,</p>

Primary security server	Backup security server	Member server	Failover scenario
			the logs must be manually sent to the primary security server and appended to the OAM file for that day. For disaster recovery purposes, the backup data store copies everything from the primary data store. The backup data store synchronizes with the primary data store. For more information about how to reload from the UCM primary, see Data on page 142.
offline continued	online continued	online continued	<p>Important:</p> <p>Avaya strongly recommends that you do not run in the failover state for extended periods of time as logs can be lost on the backup and member servers if you exceed the storage limits.</p> <p>Admin user and policy configuration changes are not allowed when the primary security server is not available.</p> <p> Caution:</p> <p>Changes to the backup server are not supported if the primary server is operational but is unreachable due to a network problem. Do not make changes to the backup server under these conditions.</p>
offline	offline	online	When a member server switches to the backup server and the backup server fails or when the member cannot reach either the primary or backup server, the member is taken to the local logon page of the member server. The administrator can log on and perform emergency configuration in the local logon page.
online	offline	online	Everything works as usual; however, if the Primary server goes offline, the system is not accessible because the backup server is not working.

Chapter 5: Security Services overview

The Unified Communications Management (UCM) Security services enables element and service management applications to access a common application security infrastructure. Security manages secure access to Web applications and provides security for Web interfaces and Web utilities.

The UCM security domain provides the central point for Authentication, Authorization, and Auditing (AAA); open, standards-based authentication; and policy-based authorization with a single unified common service.

Access to various security features that enable administrators to configure user and security rights within the application server are provided. Network administrators can create custom roles or use the built-in roles. Permissions can map to roles for each user. For more information, see [Built-in roles](#) on page 55 and [Custom roles](#) on page 58.

Important:

The pages are view only, unless you permission to perform operations such as editing and deleting.

The authorization process, also known as access control, determines and enforces assigned privileges for an authenticated user.

Navigation

- [Authentication](#) on page 47
- [Security policies](#) on page 50
- [Access control policies](#) on page 53

Authentication

Authentication verifies the user logon identity. The user authentication is based on an assigned password.

Identity management

With identity management, network administrators can create, read, update, or delete user accounts.

Each user in a company has a unique digital identity. However, the unique identity can have various user accounts for different managed elements.

The UCM Security Services supports the following account types:

- local account
- built-in account
- external account

Accounts

Use the following information for UCM Security.

Local account

The UCM Security maintains the data entry and password for a local user account; which is stored in persistent storage.

The following table lists the status types for a local user account.

Table 6: Types of status for local user accounts

Status Type	Description
Enabled	An account with enabled status can log on to UCM according to the roles and permissions assigned.
Disabled	An account with disabled status cannot log on to UCM.

Built-in account

UCM Security has one built-in account that is used by network administrators to log on to UCM Common Services after installation. The built-in account is assigned to built-in roles.

The following table describes the supported built-in accounts.

Table 7: Supported built-in accounts

Built-in account	Default password	Preassigned built-in roles	Description
admin	No default password. The password is created during configuration.	NetworkAdministrator	Use this account as the default account to log on to the UCM Common Services after a new installation. You use this account to create individual user accounts. See the Attention box below for important information regarding security best practise for the admin account.
admin2	No default password. The password is created during the Linux base installation.	none	Use this account when the administrator password is forgotten, the admin account is locked out, or to access EM when the primary security server is down.

Important:

With the built-in admin account, administrators can add, delete, and edit managed elements. Administrators can control the users who have direct access to specific managed elements. Administrators can assign users to roles and map the permissions to those roles to control which operations a user can perform on an assigned managed element. Users can access only assigned elements and perform only the tasks specific to their assigned role and permissions for an element.

Avaya recommends as a security best practise that administrators create new accounts and assign roles to those accounts for access to the managed elements based on your security policy requirements. The admin account should be disabled after these new accounts are created. For more information about role assignment, see [Table 10: Built-in roles](#) on page 55.

External account

When an administrator is authenticated with external authentication with either Lightweight Directory Access Protocol (LDAP) or Remote Authentication Dial-in User Service (RADIUS), Kerberos server, the external administrator account is added to UCM.

Administrators can configure only one RADIUS or LDAP external authentication authority.

An external user has a shadow entry inside the persistent repository of the UCM Security Services. Security Services uses the shadow entry to assign roles to the external user.

Important:

The network administrator role is not available for external LDAP users.

The password for an external account is stored in external authentication authorities. Users cannot initialize or change passwords for external users by using UCM Common Services.

Central logon

Central logon authenticates all applications in a single security domain. Central logon removes the need to manage multiple passwords on separate management applications within an Avaya Communication Server 1000 system.

Central logon is different from Single Sign-On (SSO). Central logon requires administrators to provide a logon name and password for each application. However, administrators use the same logon name and password for all applications inside the same security domain.

In a Communication Server 1000 system, central logon refers to the command line interface (CLI) access for Linux hosts.

Security policies

With the UCM Security, you can configure password and authentication settings.

Password aging policy enforcement

The password aging policy has the following time-based password thresholds that the network administrator can configure as the number of days:

- Minimum password age
- password expiration warning
- password expiration

The following table describes what occurs when a user logs on to UCM Common Services when the password aging policy thresholds expire.

Table 8: Password aging policy thresholds

Password threshold	What occurs when a threshold has expired
Minimum password age	You cannot change the password until the minimum password age has been reached. For example, you cannot change the password for three days after the last change was made.
Password expiration warning	You receive a password expiration warning when the password is about to expire and before the password expires.
Password expiration period	You are forced to change the password after the threshold for the password expires and before the threshold to disable the account. The password is locked until it is reset by the network administrator. For example, if your password expiration period is configured to 90 days and the expiration warning is 15 days, you start receiving password expiration warnings 15 days prior to the password expiring. After the password expires, you have three opportunities to logon and change the password before the account is disabled. There is no time limit associated with the three logon opportunities. If you do not change the password during the three additional logon opportunities, the account is disabled on the fourth logon attempt and the network administrator must reset the user account password.

Warning:

The password expiration warning message does not appear on the CLI of VxWorks Call Servers. You cannot change the password from a VxWorks server if the password has expired. If the password expires, you see an invalid logon message when attempting to log in to the VxWorks Call Server. At this point, the account is locked and the network administrator must reset the user account password.

The password strength policy enforcement

Passwords must contain a combination of alphanumeric and special characters as defined by the network administrator. The password strength policy enforces the following constraints.

- Passwords must have a total character length between 6 to 25. Default is eight.
- Passwords are not required to have a minimum character type; however, the default is one lower- and upper case character, one numeric character, and one special character, such as an exclamation mark (!). The sum cannot exceed the minimum total length.

After the password strength policy is enabled, the following passwords standards must be met.

- Password must not have a character repeated more than twice consecutively.
- Passwords must not be your User ID, in forward or reverse order.

If a password does not contain the required parameters for password requirements, the system rejects the password.

Important:

The password strength policy can be disabled.

Password history policy enforcement

The password history policy verifies that a password is new. The previous blocked passwords can range from 1 to 99. The default is six.

Password lockout policy enforcement

The lockout policy provides a limit for the number of attempts to access UCM Common Services. The user is locked out of UCM Common Services when the specified number of logon attempts is reached. By default, the user is locked out for two minutes after five failed attempts if the consecutive attempts occur within a ten minute period.

You can change the password policies from the Password Policy Web page, as shown in [Figure 40: Password Policy Web page](#) on page 125.

Inactive session termination policy

By default, the system suspends a user session after 30 minutes of inactivity. A user must log on to UCM Common Services again when this occurs. Session properties can be managed, as shown in [Editing Session Properties](#) on page 127.

Logon warning banner

UCM Common Services provides the text for the logon warning banner that a network administrator can change, as shown in [Editing the login warning banner](#) on page 128.

Access control policies

The authorization process, also known as access control, determines and enforces assigned privileges for an authenticated user of UCM Common Services and the managed elements.

Authorization supports both Role Based Access Control (RBAC) and Instance Level Access Control (ILAC).

RBAC controls which users have access to protected resources based on user roles. Access rights are grouped by role name, and access to a managed element is restricted to users who are assigned the role name.

ILAC controls which users can perform an operation on a specific instance of a managed element, such as NRS Manager or Element Manager, based on the roles of the user and the permissions of the element granted to the roles. ILAC determines if the request is allowed or denied.

The UCM Security Services uses the instance and RBAC data model. RBAC identifies the following administrative elements:

- users
- roles
- permissions
- operations
- managed elements

With RBAC, a network administrator can add custom roles to map to specific elements, for example a single CS 1000 element, and then customize permissions for that element.

With RBAC, administrators can customize user role assignments for each user within UCM. They can also map permissions to roles so that assigned users can perform only specific configurations on an element.

The UCM Security Services implements RBAC with Access Control Lists (ACL). An ACL entry specifies which set of predefined actions a user with a certain role can perform on a managed element. For example, the role of Patcher can be granted administration access to All elements of type: Patching Manager.

The following table describes the features supported in the UCM Security Services access control service.

Table 9: Features supported in UCM Security

Feature	Description
Centralized access control policy administration and review	You provision, modify, and review user role and role permission assignments from a central point.
Centralized access control decision point	At run time, RBAC denies or allows the current user to apply certain operations to a managed element from a central point.
Distributed access control policy enforcement	Implemented on each network element. Supports various systems with different access control enforcement policies for each type of system.
Multiple access control enforcement modules	You can access only Web pages you are authorized to see. If you try to access an unauthorized site, you receive an HTTP 403 Access Denied Error. Also, if an unauthorized user tries to directly access the business logic layer, for example, through a Web service client, an Access Denied Exception message is sent to the user.

Important:

Roles in CS 1000 are independent of UCM roles. You must separately configure roles for CS 1000 management systems.

Roles and permissions

In the Security branch of the UCM navigation tree, click Roles. On the Roles Web page, users are given permissions to perform tasks. This section describes the two type of roles that UCM Security Services supports—built-in and custom roles.

Built-in roles

UCM built-in roles cannot be deleted and the element and permission mappings cannot be changed by the network administrator. Built-in roles provide authorization to users whose roles are authorized for all the elements of type: x, where x is the type of elements provided for that role. Users who do not require this level of authorization can use custom roles. For more information about custom roles, see [Custom roles](#) on page 58.

The built-in roles that can be assigned to users are MemberRegistrar, NetworkAdministrator, Patcher, CS1000_Admin1, CS1000_Admin2, CS1000_CLI_REGISTRAR and CS1000_PDT2, as shown in the following table. Within these roles, you have access to various elements and from there you can choose specific permission mappings.

The following is a list of the built-in role permission assignments for UCM Security Services.

Table 10: Built-in roles

Built-in role types	Description
NetworkAdministrator	<p>NetworkAdministrator role provides full privileges on the system. With this role, you have emergency account access to any system including situations when the primary server is down.</p> <p>Use the NetworkAdministrator role where the administrative users are authorized for all roles on all UCM elements with all permissions. Otherwise, it is best practice for the administrator to create separate administrative roles for managing UCM elements and services other than UCM security policies, roles, and users. The NetworkAdministrator role should be used for managing only UCM security.</p> <p>You have access to the following elements:</p> <ul style="list-style-type: none"> • All elements of type: CS1000 • All elements of type: Deployment Manager • All elements of type: Hyperlink • All elements of type: IPSec Manager • All elements of type: Linux Base • All elements of type: Network Routing Service • All elements of type: Patching Manager • All elements of type: Secure FTP Token Manager • All elements of type: Snmp Manager • All elements of type: Subscriber Manager

Built-in role types	Description
	<p>The following hidden permissions are granted to the NetworkAdministrator role and cannot be copied to another role:</p> <ul style="list-style-type: none"> • PERM_QuantumSecurityAdmin: Permission to perform UCM Security Administration operations • PERM_PkiAdmin: Permission to perform PKI administration operations • PERM_AddElement: Permission to add new element instances • PERM_DeleteElement: Permission to delete element instances • PERM_EditElement: Permission to modify existing element instances
MemberRegistrar	<p>The MemberRegistrar role provides limited access. With this role, you can register new members to the primary server.</p> <p>You have access to the following elements:</p> <ul style="list-style-type: none"> • All elements of type: IPSec Manager • All elements of type: LinuxBase <p>The following hidden permissions are granted to the MemberRegistrar role and cannot be copied to another role:</p> <p>PERM_PkiAdmin: Permission to perform PKI administration operations.</p>
Patcher	<p>The Patcher role provides access to software maintenance functions such as patching and maintenance.</p> <p>You have access to the following elements:</p> <ul style="list-style-type: none"> • All elements of type: Linux Base • All elements of type: Patching Manager
CS1000_Admin1	<p>The CS1000_Admin1 role provides unrestricted OAM access to most administrative functions (except security and account administration) and provisioning for all customers on all call servers and related elements. The role also includes basic diagnostic (PDT1) privileges and access to UCM network-level services for deployment, patching, and SNMP management for CS 1000 systems. Use the CS1000_Admin1 role where the administrative users are authorized for all roles on all UCM elements with all permissions.</p> <p>You have access to the following elements:</p>

Built-in role types	Description
	<ul style="list-style-type: none"> • All elements of type: CS1000 • All elements of type: Deployment Manager • All elements of type: Linux Base • All elements of type: Patching Manager • All elements of type: Snmp Manager <p>As this role gives permissions to All elements of type: Linux Base, this role is not recommended to users who only require authorization to manage CS 1000 systems. The administrator must create a custom role for these users. For more information, see Custom roles on page 58.</p>
CS1000_Admin2	<p>The CS1000_Admin2 role provides unrestricted OAM access including security and account administration, and provisioning for all customers on all call server elements. The role also includes basic diagnostic (PDT1) privileges and access to UCM network-level services for deployment, patching, SNMP, IPsec and SFTP management for CS 1000 systems.</p> <p>You have access to the following elements:</p> <ul style="list-style-type: none"> • All elements of type: CS1000 • All elements of type: Deployment Manager • All elements of type: IPSec Manager • All elements of type: Linux Base • All elements of type: Patching Manager • All elements of type: Secure FTP Token Manager • All elements of type: Snmp Manager <p>As this role gives permissions to All elements of type: Linux Base, this role is not recommended to users who only require authorization to manage CS 1000 systems. The administrator must create a custom role for these users. For more information, see Custom roles on page 58.</p>
CS1000_PDT2	<p>The CS1000_PDT2 role provides full diagnostic and operating system access to all call servers. It restricts access to administrative functions and customer provisioning data unless combined with another role. You have access to the following elements:</p> <ul style="list-style-type: none"> • All elements of type: CS1000
CS1000_CLI_REGISTRAR	<p>The CS 1000 Command Line Registrar role provides permission to register and unregister individual CS 1000 elements, such as Call Server, MGC, and Media Card, using the local device OAM CLI.</p>

Built-in role types	Description
	<p>The role has a single permission value to allow or deny a user to register or unregister an element. You have access to the following elements:</p> <ul style="list-style-type: none"> • All elements of type: CS1000 • All elements of type: Linux Base <p>Users assigned to this role do not have CS 1000 security or Network level security privileges. This role is intended specifically for installation and repair technicians.</p>

Custom roles

On the Roles Web page, a network administrator can create a custom role to map to specific elements and specify custom permissions for that element. Security policy best practices for managing UCM administrative users suggests that the network administrator create custom roles for any users whose roles are not authorized on one or more individual elements of any UCM element type.

For larger CS 1000 systems and for larger enterprise networks of CS 1000 systems of any size, security policy best practice suggests using UCM custom roles for the purposes of limiting administrative user permissions only to the UCM elements on which they are authorized to perform OAM or diagnostic tasks and procedures.

Users whose roles are limited to managing only CS 1000 systems or CS 1000 systems located in a given enterprise site or region, custom roles must be created that map to the individual Linux base elements that have been deployed and configured as Signaling Server elements of the CS 1000 systems they are managing. These users must not have built-in roles with permissions of All elements of type: Linux Base.

Assigned users can perform only specific tasks on an element. For example, a custom role that has been created for a single element can only perform specific tasks on that element. There is a specific permissions set that defines what this role allows you to do on that element.

With custom roles, you can create a role to map to specific elements and specify custom permissions for that element. This ensures that assigned users can perform only specific tasks on an element. For example, a role that has been created for User A with permissions to an individual element can only perform specific tasks that are defined from the permission set for that role.

You can also define roles that apply to how elements and element types are hierarchically arranged under user-defined groups. When you create a permission mapping against a selected group, that group is taken into account when determining user permissions. For example, if you create a permission mapping for the custom role Technician against the element type LinuxBase and apply it to Group A, users assigned to the Technician role can

only perform tasks on elements of type LinuxBase, if they are assigned directly to Group A or to any sub-groups contained within Group A.

For more information about creating custom roles, see [Adding a custom role](#) on page 114.

Inheritance of UCM role-based permissions for Element type of CS 1000

A UCM element of type CS 1000 represents an instance of CS 1000 Element Manager which has been configured to manage a single Avaya CS 1000 system and all of its system elements, for example, Call Server, Signaling Servers, SIP Line Gateways, Media Gateway Controllers, Voice Gateway Media Cards, and any other CS 1000 system-level servers or devices.

UCM role-based permissions for CLI access are inherited from the parent CS 1000 type of element for all children Call Server, Media Gateway Controller, and Voice Gateway Media Card system elements.

UCM role-based permissions for Linux Base Manager and Linux CLI are not inherited for Linux base elements that have been deployed and configured to run CS 1000 Signaling Server applications or CS 1000 Element Manager. Therefore, custom roles for users who are authorized to manage only CS 1000 systems must be mapped to permissions on individual Linux base elements that are deployed and configured as CS 1000 system elements.

Permission templates

The built-in permission templates list contains a listing of UCM built-in roles that are applicable to the UCM type of element whose permission mapping is being edited.

For elements of type CS1000, there is an additional template corresponding to a blank set of permissions for a CS 1000 administrative account "with specified OAM privileges". This UCM template corresponds to the previous CS 1000 system-level OAM account with "limited access to overlays password" (LAPW).

You can customize the permission templates when adding a new role. For more information, see [Adding a custom role](#) on page 114.

Role mapping and permission evaluation

When adding a custom role, a permission mapping is created against a selected group and evaluated against that group. Permissions are evaluated using the most privileged algorithm.

For example, a permission mapping is created for the custom role Technician against the LinuxBase element type and applied against the group named Belleville. The Technician role now has permissions for the element of type LinuxBase because the Belleville group (including any sub-group of the Belleville group) is associated with the LinuxBase element type. However, if you are assigned directly to the LinuxBase element type without being assigned to a particular group, for example, within the Belleville group hierarchy, this overrides any group specific permission mappings for the LinuxBase element type and you then have access to all LinuxBase element types.

Chapter 6: Security server configuration

This chapter describes security server configuration and administrator password reset.

Navigation

- [Security Server configuration](#) on page 62
- [Security configuration changes](#) on page 67
- [Resetting an Administrator password](#) on page 68

Prerequisites

- Ensure Linux base operating system is installed and default Avaya account is configured.
- Ensure the DNS server is configured.
- A local user account must be created before it can be validated.

For more information, see *Avaya Linux Platform Base and Applications Installation and Commissioning*, NN43001-315.

Important:

Avaya strongly recommends that you do not change the FQDN and host name of the primary and backup security servers after security configuration has been completed. You can change the FQDN of the member security server. For information about changing the configuration on an already configured member server, see [Making changes on a member server](#) on page 67.

In Base Manager, on the **Edit Network Identify** page, the Host name and Domain fields in the Fully Qualified Domain Name (FQDN) section cannot be changed as these fields are dimmed.

Security Server configuration

The following procedures describe security configuration of the primary security server, backup security server, and member server. Access UCM by typing `https://<FQDN>`, where <FQDN> is the Fully Qualified Domain Name. If the server is not configured, the local logon page appears. Log on using the default Avaya account using the password that you specified during the Linux base installation. For more information, see [Table 7: Supported built-in accounts](#) on page 49.

Configuring the primary security server

You must configure the primary security server on a stand-alone system to provide basic security features such as user administration including password changes from the Web EM, the ability to configure authorization levels, and the enforcement of security policies.

1. In the Web browser Address bar, type **`https://<FQDN>`** of the Primary Security Server and press **Enter**.
2. On the Security Configuration page, select **Full security configuration**.
3. Click **Security Configuration**.

The FQDN validation page appears.

4. Confirm the IP address and FQDN is correct, and click **Next**.

Important:

If using a DNS server, the DNS server must be configured before proceeding.

The Select server type page appears.

5. Select **Primary security server**, and click **Next**.

The Enter server information page appears.

Important:

When using the admin account to change user account passwords, the user is forced to change their password upon logging on for the first time. During admin account creation, the NetworkAdministrator privilege is provided by default.

6. In the **Administrator password** field for the built-in Admin account, type the new password. The password must contain a minimum of eight characters with.
 - at least one number from 0 to 9
 - one special character such as an exclamation mark (!)

- one upper- and one lowercase character

Allowed characters in the password are a-zA-Z0-9{ }|()<>./,=[]^~ _@!\$%&-+":?`\'

7. In the **Confirm Administrator password** field, type the new password.

8. Click **Next**.

The Enter certificate information page appears.

9. Configure the following values:

Friendly name: Type a string that would be used to identify the certificate, for example, UCM Primary Security Server.

Bit Length: Type a value that represents the number of bits used for encryption. Values can be 512, 1024, and 2048. More CPU is required for processing as the bit value increases.

Organization: Your company name.

Organization unit: A division within your company.

Common name: FQDN of the server. The default is a combination of Windows environment variables Computername and Userdnsdomain. Ensure this field matches the hostname of the system the certificate is on.

Country/Region: Select a country from the list.

State/Province: A State/Province where the primary server is located.

City/Locality: A City/Locality where the primary server is located.

10. Click **Finish**.

The Security server configuration progress page appears.

11. Click **Restart** to restart the Web server and for the security configuration changes to take effect.

The Restarting the server Web page appears.

Important:

Restarting the Web server affects all applications. Packaged and custom applications are offline during the restart. Close the browser window during the restart process. The user can log on with the recently configured Administrator password after the Web server restarts.

Configuring a backup security server

The backup security server is an optional server that can be configured to be used for authentication and authorization when the primary security server is unavailable. Use the following procedure to configure the backup security server.

1. In the Web browser address bar, type **https://<FQDN>** of the Backup security server and press **Enter**.
2. On the Security Configuration page, select **Full security configuration**.
3. Click **Security Configuration**

The FQDN validation page appears

4. Click **Next**.

The Select server type page appears.

5. Select Backup security server and click **Next**.

The Enter server information page appears.

6. Confirm the FQDN of the Primary security server is correct, and click **Next**.

Important:

If using a DNS server, the DNS server must be configured before proceeding.

The Verify primary security server fingerprint page appears.

7. Verify the FQDN and fingerprint of the primary security server. If it is valid, type a Primary Security server user ID with the NetworkAdministrator role and password, and click **Next**.

Important:

The primary security server must be configured and running. The Primary Security server user ID is any administrator account that has NetworkAdministrator role assigned.

8. The Enter certificate information window appears.
9. The following values are populated from the Primary security server. You can accept the selected options or change them.

Friendly name: A string that would be used to identify the certificate, for example, UCM Backup Security Server.

Bit Length: A value that represents the number of bits used for encryption. Values can be 512, 1024, and 2048. More CPU is required for processing as the bit value increases.

Organization: Your company name.

Organization unit: A division within your company.

Common name: FQDN of the server. The default is a combination of Windows environment variables Computername and Userdnsdomain. Ensure this field matches the hostname of the system the certificate is on.

Country/Region: A Country/Region where the primary server is located.

State/Province: A State/Province where the primary server is located.

City/Locality: A City/Locality where the primary server is located.

10. Click **Finish**.

The Security server configuration progress page appears.

11. Click **Restart** to restart the Web server for the security configuration changes to take effect.

Important:

Restarting the Web server affects all applications. Packaged and custom applications are offline during the restart. Close the browser window during the restart. You can log on with the recently configured Administrator password after the Web server restarts.

Configuring a member server

Configure the member security server.

1. In the Web browser Address bar, type **https://<FQDN>** of the Member security server and press **Enter**.
2. On the Security Configuration page, select **Full security configuration**.
3. Click **Security Configuration**.

The FQDN validation page appears to confirm that the information is correct.

4. Select **Yes**, and click **Next**.

The FQDN validation page refreshes.

5. Select **No**, and click **Next**.
6. Select **Member server**, and click **Next**.

The Enter Server Information page appears.

7. Type the FQDN or IP address of the Primary security server, and click **Next**.

Important:

The primary security server must be configured and running.

The Verify the primary security server fingerprint page appears.

8. Type a Primary Security server user ID with the network administrator role and password, and click **Next**.

Important:

The primary security server must be configured and running. The Primary Security server User ID is any administrator account that has the NetworkAdministrator role assigned.

The Enter certification information window appears.

9. The following values are populated from the Primary security server. You can accept the selected options or change them.

Friendly name: A string that would be used to identify the certificate, for example, UCM Backup Security Server.

Bit Length: A value that represents the number of bits used for encryption. Values can be 512, 1024, and 2048. More CPU is required for processing as the bit value increases.

Organization: Your company name.

Organization unit: A division within your company.

Common name: FQDN of the server. The default is a combination of Windows environment variables Computername and Userdnsdomain. Ensure this field matches the hostname of the system the certificate is on.

Country/Region: A Country/Region where the primary server is located.

State/Province: A State/Province where the primary server is located.

City/Locality: A City/Locality where the primary server is located.

10. Click **Finish**.

The Security server configuration progress window appears.

11. Click **Restart** to restart the Web server for the security configuration changes to take effect.

Important:

Restarting the Web server affects all applications. Packaged and custom applications are offline during the restart. Close the browser window during the restart. You can log on with the recently configured Administrator password after the Web server restarts.

For information about changing the configuration of a member server, see [Making changes on a member server](#) on page 67.

Decommission a Backup Security Server

Before you reinstall a Backup Security Server that had previously been joined to a Primary Security Server, you must first delete the Backup Security Server element from the list of elements on the Primary Security Server. For information about deleting elements, see [Deleting selected elements](#) on page 93.

Security configuration changes

You can make configuration changes to the member server. The following procedure describes the steps to change the Fully Qualified Domain Name (FQDN), change the certificate information, point to a different primary server, and demote a primary and backup server.

Important:

Certificates are managed from the security server at the network level. You must restart the Web server after you save the changes.

Making changes on a member server

Important:

The primary and backup server cannot be reconfigured. You cannot promote a member server to a primary server. A fresh installation is required if you want to change a member server to a primary server.

1. Go to the local logon page of an already configured member server.
2. Select **Full security configuration**, and click **Security Configuration**.
The FQDN validation page appears.
3. Select **Yes**, and click **Next**.
The FQDN validation page refreshes to confirm that the information is correct.
4. Select **No**, and click **Next**.
5. Select **Member server**, and click **Next**.
6. Type the FQDN or IP address of the Primary security server, and click **Next**.
7. Continue to follow step [8](#) on page 66 to step [11](#) on page 66 in [Configuring a member server](#) on page 65.

Configuration failure

Failed configuration attempts are identified in the Status field. Click **Try again** to clear the previous configuration attempt and to begin a new configuration attempt. The new configuration attempt begins at the Primary security server from the Security Configuration Server Information page. Partial configurations are not supported.

Demoting a primary and backup server

The UCM primary and backup security server can be demoted to a member server in a new domain. The security domain of the demoted primary server is no longer valid so the existing backup server must also be demoted to a member server in the new domain. The security configuration of any existing member servers must be reconfigured to a primary server in another domain, see [Security configuration changes](#) on page 67.

Prerequisites

You must be logged on locally to the primary security server as Administrator.

Procedure

1. From the Security Configuration page, click **Demote Security Server**, and click **Security Configuration**.
The FQDN validation page appears.
2. Select **No**, and click **Next**.
The FQDN validation page refreshes allowing you to make changes.
3. Select IP address of the Primary or backup server from the list, and click **Next**.
The Select server type page appears.
4. Select **Member server**, and click **Next**.
5. Continue to follow step [7](#) on page 65 to step [11](#) on page 66 in [Configuring a member server](#) on page 65.

Resetting an Administrator password

If the Administrator password is forgotten or the account is locked out, the password can be reset from the user interface. Use the following procedures for logging on to the local logon page with an emergency account.

1. In the Web browser Address bar, type `https://<FQDN>/local-login` of the Primary Security Server and press **Enter**.
2. Log on using the default emergency account or Avaya account. For more information, see [Built-in account](#) on page 49.

The Security Configuration page appears.

3. In the Web browser Address bar, type `https://<FQDN>/passwordReset` of the Primary Security Server and press **Enter**.
4. In the User ID field, type the User ID for the password you want to reset.
5. In the New password field, type a new password.
6. In the Confirm new password field, type the new password again.
7. Click **Save**.

A confirmation page appears when you change the password.

Chapter 7: Logon and logoff options in UCM

This chapter describes logging on to UCM for the first time and changing your password, and other log on and log off options in UCM.

Navigation

- [Logon modes in UCM](#) on page 71
- [Central logon mode](#) on page 71
- [Network logon mode](#) on page 72
- [Switching from network logon mode to central logon mode](#) on page 74
- [Disabling digital certificate pop-up](#) on page 74
- [SSO using FQDN without DNS infrastructure](#) on page 75
- [Logoff options](#) on page 75

Logon modes in UCM

Use the following procedures to log on to UCM using the central or network logon mode and switching from network logon mode to central logon mode.

Central logon mode

Avaya recommends logging on to UCM by entering the FQDN. This is called central logon mode. Central logon supports SSO, centralized access control, password changes, resets, and password expiry notices. You can also manage network resources.

The password reset page appears when logging on for the first time, after a password reset, and when your password is about to expire.

Important:

Avaya recommends using the central logon mode (FQDN) for UCM.

Logging on to UCM in Central logon mode for the first time

Use the following procedure to log on to UCM for the first time using central logon mode.

1. In the Web browser Address bar, type `https://<FQDN>` and press **Enter**. For example, `https://primary.ca.avaya.com`.
2. Type a valid User ID and password.
3. The Password change page appears.
4. Type your new password and confirm your password by typing it again and click **Change**.

Logging on using the FQDN in central logon mode

Log on to UCM using the central logon page by entering the FQDN. Central logon supports SSO, centralized access control, and password changes and resets. You can also manage network resources with central logon.

1. In the Web browser Address bar, type `https://<FQDN>` and press **Enter**. For example, `https://primary.ca.avaya.com`.
2. Type a valid User ID and password.
3. On the Elements page, click an element item.

When the element management URL is on a different UCM, the user is redirected to the Web page of the selected element without reauthentication.

Network logon mode

Log on to UCM by entering the IP address. This is called network logon mode. SSO and Kerberos based SSO with Microsoft Windows is not supported when you log on from the network logon page. Failover works in network logon mode when the primary server is down. The member server redirects you to the backup security server. Network logon can also manage network resources and supports centralized access control. The administrator cannot change or reset passwords in network logon mode.

Logging on to UCM in Network logon mode for the first time

If logging on to UCM for the first time in Network logon mode, you must manually change the default password.

Follow the default password strength policy as defined by the administrator. For more information, see [The password strength policy enforcement](#) on page 52.

1. Open the Web browser.
2. Type the IP address in the Address bar, and press **Enter**.

The Logon Web page appears.

3. Click **Change Password**.

Important:

If you attempt to logon using your temporary password, you will receive the error message "Login error. Please check your username and password." You must click the Change Password link before logging on for the first time.

The Password Change screen appears.

4. Type the following information:

- User ID
- Current password
- New password
- Confirm password

Important:

User IDs in UCM are not case-sensitive. However, Linux-based User IDs that are independent of UCM are case-sensitive.

5. Click **Save**.

Important:

On the Internet Explorer browser, you may see a digital certificate pop-up. To disable, see [Disabling digital certificate pop-up](#) on page 74.

Logging on using the IP address in network logon mode

Log on to UCM using the network logon page by entering the IP address. Avaya recommends using central logon mode. For more information, see [Logging on using the FQDN in central logon mode](#) on page 72.

1. In the Web browser Address bar, type the IP address of the Primary Security Server, and press **Enter**.

The Logon Web page appears.

2. Type a valid User ID and password.
3. Click **Login**.

The application Web page appears.

4. Click the link of an element in the same Web browser window.

If an element is installed on the same UCM, the selected element Web page appears without reauthentication.

Switching from network logon mode to central logon mode

Switch from network logon mode to central logon mode to allow for Single Sign-On.

1. In the Web browser Address bar, type the IP address of the Primary Security Server, and press **Enter**.
2. Click **Go to central login for Single Sign-On**.
3. Type a valid User ID and password at the central Logon page.
4. Click **Login**.

You do not have to reauthenticate to switch between Web servers in the same security domain.

Disabling digital certificate pop-up

Disable digital certificate pop-ups from Internet Explorer when no certificates are listed during logon attempt.

1. On the Internet Explorer browser, choose **Tools > Internet Options**.
2. Select the **Security** tab, and click **Custom Level**.
3. Scroll to select the option **Don't prompt for client certificate selection when no certificate or only one certificate exists** and click **Enable**.
4. Click **OK**.
5. Click **Yes** at the prompt "Are you sure you want to change the settings for this zone?".

SSO using FQDN without DNS infrastructure

The FQDN uses an IP address with DNS. To use SSO for Web access without DNS infrastructure, you must include the FQDN in the local `\winnt\system32\drivers\etc\hosts\etc\hosts` file on your computer.

If you use a non-Windows OS for Web clients, see the OS document to configure the corresponding setup.

The IP address to FQDN mapping in the `\winnt\system32\drivers\etc\hosts\etc\hosts` must be the same as the IP address in the Linux `/etc/hosts` file where UCM is installed.

Important:

A User ID and password that is not in the local user database is denied access to the Linux host CLI.

Logoff options

The following table describes how to log off UCM Common Services and how to log off globally for elements within the same or different UCM system.

Table 11: Logoff options in UCM

Logoff method	Action	Result
Log off UCM Common Services	Click Logout at the top right corner of the window.	A Web page appears confirming the logoff was successful.
Log off globally	Click Logout at the top right corner of the window and then, from the same browser window, type the URL of another Web application running within the same UCM server.	You are redirected to the UCM logon Web page.
Log off globally for Web applications in a different UCM	Click Logout at the top right corner of the window and then, from the same browser window, type the URL of a Web application that runs	You are redirected to the UCM logon Web page.

Logoff method	Action	Result
	within a different UCM server.	
Session or idle timeout	You are automatically logged off when the maximum session or idle time is reached.	You are redirected to the UCM logon Web page.

Important:

You can log on multiple times using the same User ID. If you close the UCM Web page window without clicking Logout, you can log on to a new session with the same User ID. The previous Logon session is no longer accessible and continues to use resources until the idle timeout period is reached. Avaya recommends that you click Logout to end your session.

Chapter 8: UCM Network configuration

This chapter contains information about managing elements in UCM Common Services. The Elements page is the default Web page when you log on to UCM. The Elements page has two views: table view and tree view. For more information about the views, see [Table view](#) on page 24 and [Tree view](#) on page 24.

This chapter covers the following topics:

- [Elements](#) on page 77
- [CS 1000 Services](#) on page 94
- [Software Deployment](#) on page 95

Navigation

- [Elements](#) on page 77
- [CS 1000 Services](#) on page 94
- [Software Deployment](#) on page 95

Elements

The following sections contain procedures to manage elements by using the tree or table view.

Manage elements using the edit navigation tree

Perform the procedures in the following sections to manage the elements using the navigation tree.

Important:

The Edit Tree button is only visible to authorized administrators.

Adding a group

Use the following procedure to add a new group to the navigation tree.

1. On the Elements page, click the tree view icon.

The tree view appears, as shown in [Figure 8: Tree view](#) on page 79.

2. Click **Edit Tree**.

The Edit Navigation Tree window appears, as shown in [Figure 10: Edit navigation tree](#) on page 81.

3. Right-click on the parent in the right Element tree pane.
4. Choose **Add Group** from the shortcut menu.

OR

Select the parent from the right Element tree pane, and click **Add Group**.

A New Group window appears.

Important:

The parent of the new group must be a group. Elements cannot contain other groups or elements, but a group can contain both elements and other groups.

5. Complete the following fields:
 - Type a name for the new group. In the figure [Figure 7: New group](#) on page 79, the name of the new group is called newGroup. The name can be up to 32 characters. Special characters are allowed.
 - Type an optional description of the new group. The description can contain up to 500 characters.
 - Type an optional URL of an element associated with the group. The administrator can navigate to the associated element by clicking the group in navigation mode if the URL is specified. The administrator can also associate a primary cluster element with a group of elements in a cluster when the URL is specified.
6. Click **OK**.

The new group appears as the last child of the parent, as shown in the following figure.

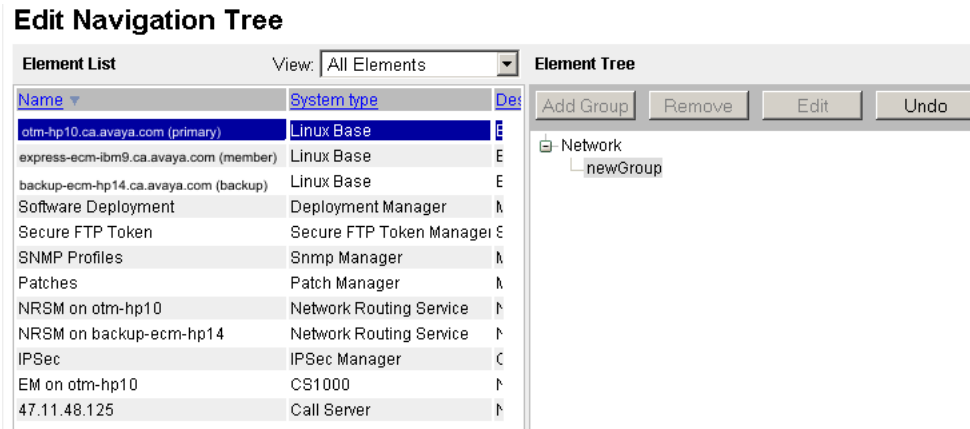


Figure 7: New group

Adding elements

You cannot add an element to a group in which it already exists. IPsec must be disabled before elements are added to the security domain. Use the following procedures to move an element to a specific position.

1. On the Elements page, click the tree view icon.

The tree view appears, as shown in the following figure.

Elements

Select an Element to launch its management service

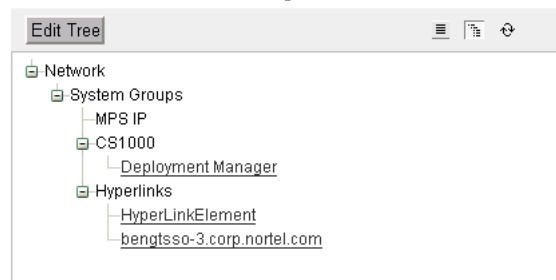


Figure 8: Tree view

2. Click **Edit Tree**.

The Edit Navigation Tree window appears, as shown in [Figure 10: Edit navigation tree](#) on page 81.

3. Select an element from the Element List in the left pane and drag the element to the destination group in the Element Tree in the right pane. In the following figure, the IPSec element in the left pane is moved to newGroup under the selected parent. The green check mark indicates the IPSec element can be added to the group. If the folder is collapsed, hold the pointer over the group in the Element Tree pane to expand it.

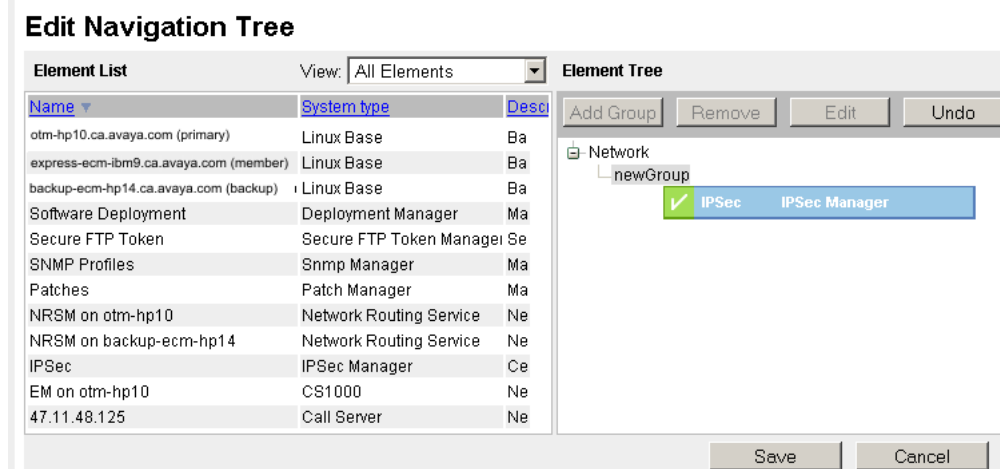


Figure 9: Add elements to a group

Important:

The parent of the new element must be a group. Elements cannot contain other groups or elements. You cannot add an element to a group in which it already exists. Duplicate group name are not permitted under the same parent branch, if the user tries to add an element with a duplicate group name, a pop-up message appears indicating the group name already exists.

When a new item is added to the tree, it appears as the last child of the parent group by default.

4. Click **Save** to add the element to the tree and make this element available to other administrators.

Editing an element

Edit an element using the Edit Navigation Tree.

Important:

The Edit Tree button is only visible to authorized administrators. Edit the tree view using a single logon session. Editing the tree view simultaneously from two or more sessions can cause an inconsistent state to the tree.

1. On the Elements page, click the tree view icon.

The tree view appears, as shown in [Figure 8: Tree view](#) on page 79.

2. Click **Edit Tree**.

The Edit Navigation Tree window appears, as shown in the following figure.

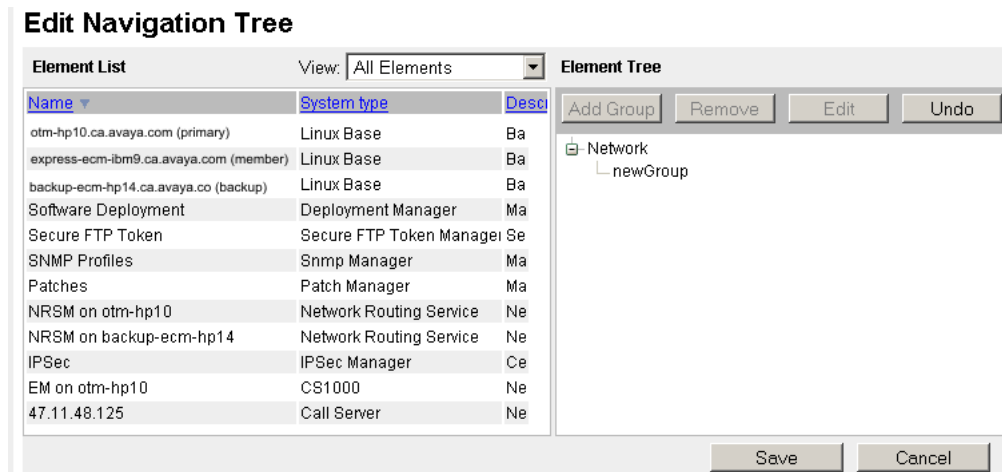


Figure 10: Edit navigation tree

3. Use the **View** list to show all elements or only the elements not added to the tree. Sort the list by clicking on any column header.
4. Use the Element Tree pane to select the element and click **Add Group**, **Remove**, **Edit**, or **Undo**.

OR

Right-click a group or element in the Element List pane to invoke a shortcut menu and choose **Add Group**, **Edit**, **Cut**, **Copy** or **Remove**.

5. Click **Save** to commit the changes to the element tree and make them available to all administrators.

OR

Click **Cancel** to discard any changes made to the element tree, and exit edit mode.

Important:

Click the Save button to save changes to the tree. If the administrator logs off, navigates away from the page, or a session timeout occurs, the unsaved changes to the tree are lost.

Editing a group

Edit a group using the Edit Navigation Tree.

Important:

Items in the tree cannot be siblings of a Network group.

1. On the Elements page, click the tree view icon.

The tree view appears, as shown in [Figure 8: Tree view](#) on page 79.

2. Click **Edit Tree**.

The Edit Navigation Tree window appears, as shown in [Figure 10: Edit navigation tree](#) on page 81.

3. Right-click a group in the right pane and choose **Edit** from the shortcut menu or click the **Edit** button.

The Rename Group window appears.

4. In the Rename Group window, edit the following fields as required:

- Name
- Description
- URL

5. Click **OK** to accept your changes.

6. Click **Save** to save your changes.

Important:

You must click **Save** in the Edit Navigation Tree to save the changes.

Removing items using the Edit Navigation Tree

Remove items using the Edit Navigation Tree.

1. On the Elements page, click the tree view icon.

The tree view appears, as shown in [Figure 8: Tree view](#) on page 79.

2. Click **Edit Tree**.

The Edit Navigation Tree window appears, as shown in [Figure 10: Edit navigation tree](#) on page 81.

3. Right-click a group in the right pane, and choose **Remove** from the shortcut menu or click the **Remove** button.

A Confirm item(s) removal dialog box appears.

4. Click **Yes** to remove the selected item from the tree.

Important:

If you remove a group, all children are removed from the tree. Removed elements appear in the Element List in the left pane under Ungrouped Elements, if there are no other instances of them in the tree.

Items are removed from the tree view. To remove the items from Security Services, you must click **Save** in the Edit Navigation Tree.

Assigning an element alias

The administrator can assign an alias to an element instance to allow for a more descriptive name. Different instances of an element can have different aliases assigned. Aliases appear in an italicized font to indicate an alias in the navigation tree. Move the pointer over an alias element to display element name, type, IP address, and trust status details.

1. On the Elements page, click the tree view icon.

The tree view appears, as shown in [Figure 8: Tree view](#) on page 79.

2. Click **Edit Tree**.

The Edit Navigation Tree window appears, as shown in [Figure 10: Edit navigation tree](#) on page 81.

3. Right-click the element and choose **Create Alias** from the shortcut menu as shown in the following figure.

Edit Navigation Tree

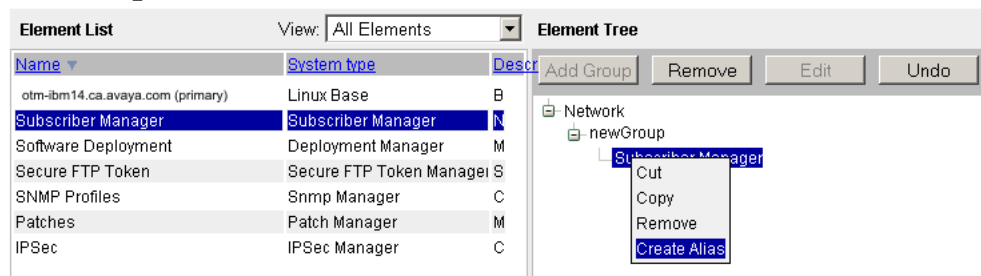


Figure 11: Create alias

4. Type a new name for the element, and press **Enter** to accept the change or **Escape** to cancel renaming the element.
5. Commit the change to the Edit Navigation Tree by clicking **Save**.

Important:

You cannot assign the same alias to different elements although you can assign aliases to various instances of the same element in the navigation tree. You cannot assign an alias name that is already the name of another element.

Removing an element alias

Remove an element alias.

1. Right-click the element alias.
2. Choose **Remove Alias** from the shortcut menu.
The original element name is restored.
3. Commit the change to the Edit Navigation Tree by clicking **Save**.

Manage elements using table view

Use the procedures in this section to manage elements in UCM common services.

To add a hyperlink type element to UCM, the element must be named and the management address (URL) defined so you can navigate to it. The element must then be incorporated into Security Services by mapping authorization permissions offered by the element to user roles created in UCM. Role permission mapping allows group-based authorization across all elements. Individual user capabilities are limited by the roles to which they are assigned.

For more information about Element permissions, see [Editing user role mapping](#) on page 100.

Use the following procedures to manage applications using the table view.

Important:

Your role permissions determine the elements you can see. Network administrators can see all elements.

Starting a managed element

Start the management application for a selected element in the current or a new Web browser.

1. Log on to UCM.
2. In the navigation tree, click **Elements**.

The Elements Web page is the default Web page that appears when UCM is opened, as shown in the following figure.

Elements

New elements are registered into the security framework, or may be added as simple hyperlinks. Click an element name to launch its management service.

<input type="checkbox"/>	Element Name	System Type	Release	Address	Description
1 <input type="checkbox"/>	EM on backup-ecm-hp14	CS1000	6.0	47.11.46.66	new element.
2 <input type="checkbox"/>	EM on co-res-cs	CS1000	6.0	47.11.48.130	new element.
3 <input type="checkbox"/>	EM on express2-ecm-dell	CS1000	6.0	47.11.48.82	new element.
4 <input type="checkbox"/>	EM on otm-ecm-ibm9	CS1000	6.0	47.11.46.34	new element.
5 <input type="checkbox"/>	NRSM on new-topdell	Network Routing Service	6.0	47.11.48.205	new element.
6 <input type="checkbox"/>	NRSM on otm-hp10	Network Routing Service	6.0	47.11.48.220	new element.
7 <input type="checkbox"/>	backup : backup-ecm-hp14.ca.nortel.com	Linux Base	6.0	47.11.49.104	Base OS element.
8 <input type="checkbox"/>	ibm9	CS1000	6.0	47.11.10.36	
9 <input type="checkbox"/>	member : co-res-cs.ca.nortel.com	Linux Base	6.0	47.11.49.101	Base OS element.
10 <input type="checkbox"/>	member : express2-ecm-dell.ca.nortel.com	Linux Base	6.0	47.11.49.210	Base OS element.

Figure 12: Elements Web page

3. In the Element Name column, click an item.

The application for the element appears in the same Web browser window.

To start an element in a new browser window, right-click the element and select **Open in new window**.

To bookmark management applications for an element in a new Web browser window, right-click the element item and select **Add to favorites**.

Important:

If the element you attempt to view is a secured element in Security Services, you do not require authentication. If the element is an unsecured element, the administrator is subject to the authentication method because single sign-on is not available for elements outside of UCM .

Adding a Hyperlink

Add an external hyperlink element in UCM.

1. Log on to UCM as an administrator.
2. In the navigation tree, click **Network > Elements**.

The Elements Web page appears, as shown in [Figure 12: Elements Web page](#) on page 85.

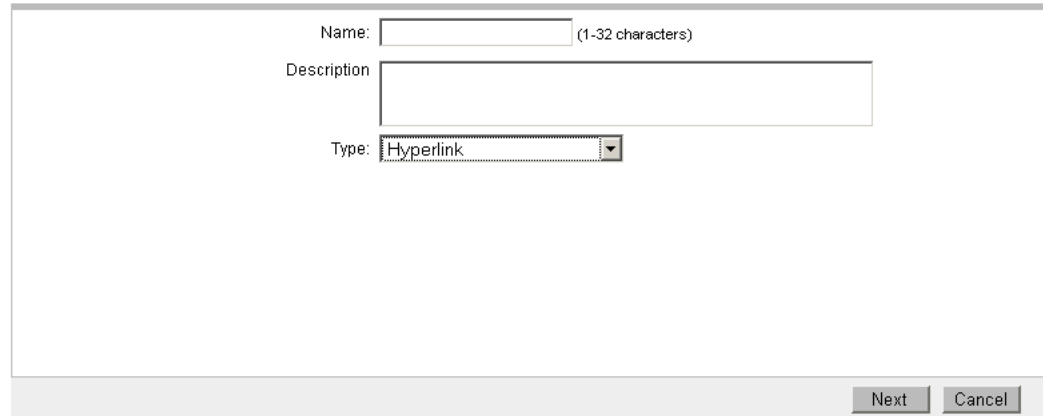
3. Click **Add**.

The Add New Element page appears, as shown in the following figure.

Add New Element

Step1: Identify the new element.

Enter a name and optional description. Depending on the selected element Type, additional steps may be required.



The screenshot shows a web form titled "Add New Element". Below the title, there is a sub-header "Step1: Identify the new element." followed by a note: "Enter a name and optional description. Depending on the selected element Type, additional steps may be required." The form itself is enclosed in a light gray border and contains three input fields: "Name:" with a text box and a "(1-32 characters)" label, "Description:" with a larger text box, and "Type:" with a dropdown menu showing "Hyperlink". At the bottom right of the form, there are two buttons: "Next" and "Cancel".

Figure 13: Add New Element Step 1 Web page

4. In the **Name** field, type the element name.

Important:

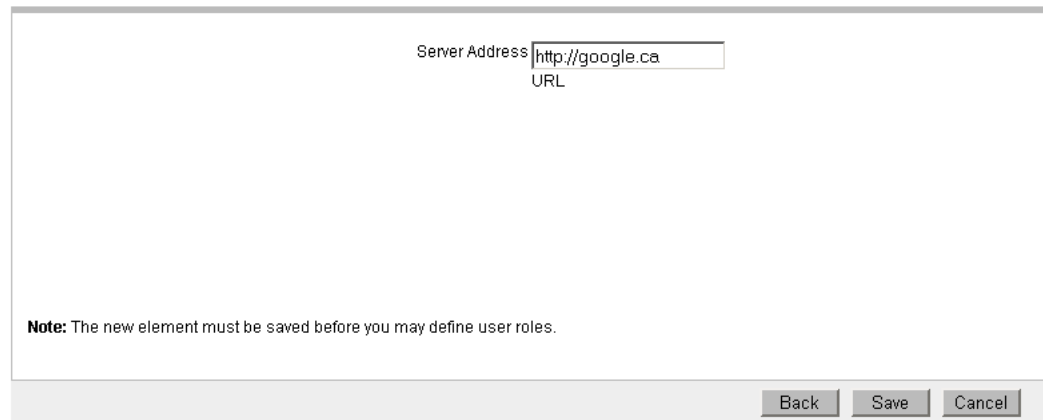
The name must be from 1 to 32 characters. Special characters are permitted.

5. In the optional **Description** field, type a description.
6. Select **Hyperlink** in the Type list.
7. Click **Next**.

The Add New Element Web page appears for the element, as shown in the following figure.

Add New Element

Step2: Identify the element's management server in your network.



Server Address

URL

Note: The new element must be saved before you may define user roles.

Back Save Cancel

Figure 14: Add New Element

8. In the Management URL field, type the URL for the element.
9. Click **Save**.

The Elements Web page appears and the new element appears in the list.

Adding a CallPilot Messaging element

When Subscriber Manager is deployed, you can add an external CallPilot Messaging element in UCM.

1. Log on to UCM as an administrator.
2. In the navigation tree, click **Network >Elements**.
3. The Elements Web page appears, as shown in [Figure 12: Elements Web page](#) on page 85
4. Click **Add**.

The Add New Element page appears.

5. In the Name field, type the element name. The name must be between 1 to 256 characters in length.
6. In the optional Description field, type a description.
7. Select **CallPilot Messaging** in the Type list.
8. Click **Next**.

The Add New Element Web page appears for the element.

9. Configure the following CallPilot element management information:
 - CallPilot Manager address
 - CallPilot server address
 - Administrator mailbox number: The Mailbox number to use when communicating with the CallPilot. CallPilot requires the mailbox number to be from 3- to 18-digits in length; however, the element definition does not enforce this restriction.
 - Administrator password: The password to use when communicating with the CallPilot. Although CallPilot requires the password to be 4- to 16-digits, the element definition does not enforce this restriction.
10. Click **Save**.

The Elements Web page appears and the new element appears in the list.

Edit Element properties

Perform the procedures in this section to edit the properties and role-permission mapping of a hyperlink element, CS 1000 element, Linux base or Network Routing Service element installed in UCM.

Editing the properties of a hyperlink element

Edit the properties of a hyperlink element in UCM.

1. Log on to UCM as an administrator.
2. In the navigation tree, click **Elements**.

The Elements Web page appears, as shown in [Figure 12: Elements Web page](#) on page 85.
3. On the Elements Web page, select the check box beside the hyperlink element, and click **Edit**.
4. The Element Details Web page for the selected hyperlink element appears, as shown in the following figure.

Element Details (testelement2)

Identification

Name:

Type: Hyperlink

Description:

Release: Release 6.0

Server Address URL

Figure 15: Edit Hyperlink properties

5. Modify the following fields:

- Name
- Description
- Release
- Server Address

6. Click **Save**.

Important:

You cannot modify the element type after you create the element.

Editing the properties for a CS 1000 element

Edit the properties of a CS 1000 element.

1. Log on to UCM as an administrator.
2. In the navigation tree, click **Elements**.

The Elements Web page appears, as shown in [Figure 12: Elements Web page](#) on page 85.

3. On the Elements Web page, select the check box beside the CS 1000 element to edit, and click **Edit**.
4. The Element Details Web page appears, as shown in the following figure.

Element Details (47.11.48.249)

Identification

Name:

Type: CS1000

Release: Release 6.0

Element Internal Id

Tape ID/System Serial Number

Description:

Management Address

Call Server IP Address

Base URL

Base URL

CS1000 admin username

CS1000 admin user

CS1000 admin password

CS1000 admin password

Figure 16: Element Details Web page

5. In the Identification section, edit the following fields as required:

- Release

If the Release is incorrect, click **Edit**.

The CS 1000 Release Web page appears.

On the **Release** list, select the desired Release from the available list. Click **Save** to save the changes or click **Cancel** to make no change.

- Name

- Description

- Element Internal Id (Tape ID/System Serial Number)

- Management Address (Call Server IP Address)

- Base URL (where Element Manager is installed)

- CS1000 admin username

- CS1000 admin password

- IPsec Level (select protection level for communication between synchronized targets as Optimized, Functional, or Full)

- Preshared key for configuring IPSec (16–32 characters, do not include "Space ~ * ` @ [] #")

6. Click **Save**.

Editing the properties of a Linux base element

Edit the properties of a Linux base element.

1. Log on to UCM as an administrator.
2. In the navigation tree, click **Elements**.

The Elements Web page appears, as shown in [Figure 12: Elements Web page](#) on page 85.

3. On the Elements Web page, select the check box beside the Linux base element to edit, and click **Edit**.

The Element Details Web page appears.

4. Modify the following fields:

- Name
- Description
- Release
- Linux Base Version (read only)
- Call Server IP (read only)
- Cluster ID (read only)
- Default Gateway (read only)
- Deployed Applications (read only)
- Deployed Application Version (read only)
- TLAN Fully Qualified Domain (read only)
- ELAN Gateway (read only)
- TLAN Gateway (read only)
- Host Name (read only)
- HW Platform Type (read only)
- MAC Address (read only)
- ELAN IP Address (read only)
- TLAN IP Address (read only)
- Management Address (IP address)
- Management URL (Base URL)
- ELAN Subnet Mask (read only)
- TLAN Subnet Mask (read only)

- Deployment Status

5. Click **Save**.

Editing the properties of a Network Routing Service element

Edit the properties of a Network Routing Service element.

1. Log on to UCM as an administrator.

2. In the navigation tree, click **Elements**.

The Elements Web page appears, as shown in [Figure 12: Elements Web page](#) on page 85.

3. On the Elements Web page, select the check box beside the Network Routing Service element to edit, and click **Edit**.

4. The Element Details Web page appears.

5. In the Identification section, edit the following fields as required:

- Name
- Description
- Release
- Management Address
- Base URL (where NRS Manager is installed)

6. Click **Save**.

Editing the properties of a CallPilot Messaging element

Edit the properties of a CallPilot Messaging element in UCM.

1. Log on to UCM as an administrator.

2. In the navigation tree, click Elements.

The Elements Web page appears.

3. In the Identification section, edit the following fields as required:

- Name
- Description
- Release
- CallPilot Manager address
- CallPilot server address

- Administrator mailbox number
 - Administrator password
4. Click Save.

Important:

You cannot modify the element type after you create the element.

Deleting selected elements

Delete elements that are no longer required.

Important:

If the backup security server is deleted, the trust between the primary and backup server is broken and the backup server cannot function as a backup server in the security domain. If the Linux base element from the elements table is removed, it reregisters but is not physically removed. Click the Refresh link on the Elements page if you cannot add new elements or delete selected elements after the security service is restarted.

Prerequisites

Elements must be physically decommissioned prior to deleting the element from the elements table.

1. Log on to UCM as an administrator.
2. In the navigation tree, click Elements.

The Elements Web page appears, as shown in [Figure 12: Elements Web page](#) on page 85.

3. On the Elements Web page, select the check box beside one or more elements.

Important:

The Primary security server element cannot be deleted from the element table. Any attempt to delete the primary server is blocked in UCM.

4. Click **Delete**.

The Delete Elements Web page appears, as shown in the following figure.

Delete Elements

The following element(s) will be permanently deleted. All references to them will be removed from the system, including related permissions in administrative user roles.

Elements to be deleted:

testelement2

Elements should be decommissioned before deletion, to ensure that any dependencies are removed from other applications.

Warning: Some elements may be re-registered by restarting the operating system on the element. However, a backup security server cannot be re-registered with a restart because the trust relationship between primary and backup servers will no longer exist.

To confirm deletion of the listed element(s), click Delete.

Delete Cancel

Figure 17: Delete Elements Web page

5. Click **Delete** to proceed or **Cancel** to cancel the deletion.

Important:

You can access management applications of a deleted element. UCM maintains an in-memory cache for all elements accessed from the current Web server. When a user deletes an element, the in-memory cache contains the information for the element; however, all permissions on an element are denied after the user deletes the element.

CS 1000 Services

This section contains information about configuring servers on the Avaya Communication Server 1000 including patching, IP Security, and SNMP.

IPsec

Use IPsec for network-wide policy implementation and synchronization of preshared keys across network targets. IPsec is included as part of the UCM installation and is configured on the Primary Security server.

In the Network branch of the UCM navigation tree, click CS 1000 Services, IPsec. You can administer several aspects of IP security, such as configuring domain-wide security policy, adding and removing of IPsec targets, enabling or disabling of IPsec for network elements, and scheduling of IPsec synchronization and activation. For more information about using IPsec, see *Avaya Security Management Fundamentals*, NN43001-604.

Patches

In the Network branch of the UCM navigation tree, click CS 1000 Services, Patches. Use Patching Manager on the primary security server to remotely deploy patches from a central

location to other Linux servers on the same security domain. The Patching Manager screen appears with a list of all Linux servers (or Linux Base Elements) in the same security domain.

You can also install patches locally. Local Patching is accessible from the Base Manager of each Linux Element. Patching Manager can be reached by logging on to the primary security server and clicking an element or by logging on locally to the element. For more information about Patching Manager, see *Avaya Patching Fundamentals, NN43001-407*.

SNMP Profiles

In the Network branch of the UCM navigation tree, click CS 1000 Services, SNMP Profiles. You can add an SNMP profile, configure an existing SNMP profile, and delete an SNMP profile. For more information about SNMP profiles, see [SNMP Profiles](#) on page 29.

For more information about configuring SNMP Profiles, see *Avaya Communication Server 1000 Fault Management — SNMP (NN43001-719)*.

Secure FTP token

In the Network branch of the UCM navigation tree, click CS 1000 Services, Secure FTP Token. The Secure FTP Token Management screen appears on which you can view the date of the last generated token, refresh the status of the current token, and regenerate a new token for distribution throughout the network. For more information about Secure FTP Token, see *Avaya Security Management Fundamentals, NN43001-604*.

Software Deployment

In the Network branch of the UCM navigation tree, click Network, Software Deployment. Use Software Deployment on the primary security server to remotely deploy the Linux Base and application software from a central location to other Linux servers in the same security domain.

On the Deployment Manager Web page, you can select the following items:

- Deployment View
- Software Loads
- Backups
- 6.0 Deployment Targets

You can also deploy software locally prior to the server joining the security domain; however, Avaya recommends using the central deployment method.

For more information about Software Deployment, see *Avaya Linux Platform Base and Applications Installation and Commissioning, NN43001-315*.

Deployment targets

From the Deployment Targets page, you can choose from the following buttons:

- Backup
- Restore
- Deploy

For information about the procedures to backup, restore, or deploy, see *Avaya Linux Platform Base and Applications Installation and Commissioning* , NN43001-315.

Chapter 9: UCM User Services configuration

This chapter describes the features found in the Unified Communications Management (UCM) navigation pane under the User Services branch.

Navigation

- [Administrative Users](#) on page 97
- [External Authentication](#) on page 104
- [Password](#) on page 109

Administrative Users

In the User Services branch of the UCM navigation tree, click Administrative Users. The Administrative Users Web page appears. Administrators with the NetworkAdministrator role can perform the user management tasks required to manage users within UCM.

Reviewing existing users

View the users that are configured for UCM access.

1. Log on to UCM as an administrator.
2. In the navigation tree, click **User Services, Administrative Users**.

The Administrative Users Web page lists users configured for access to UCM. The User ID, Name, Roles, Type, and Account Status are displayed, as shown in the following figure.

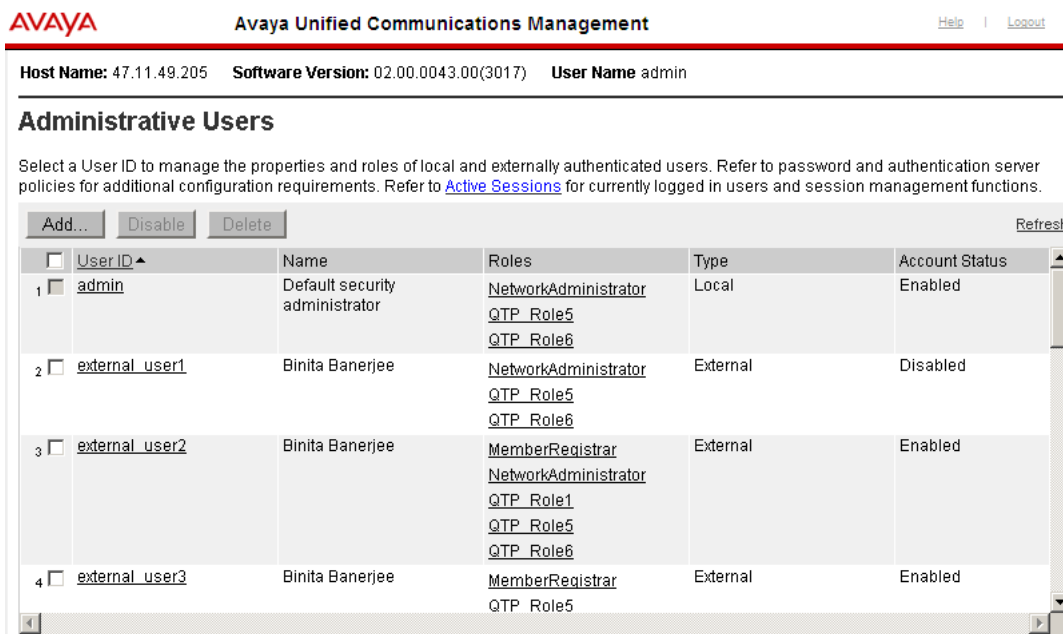


Figure 18: Administrative Users Web page

3. Review the information for existing users.

Important:

The check box for the admin user ID appears dimmed. The admin user ID cannot be changed.

Adding a new local or external user

Use the following procedures to create a new user of UCM and to assign roles to the new user. For more information about local and external users, see [Authentication](#) on page 47.

1. Log on to UCM as an administrator.
2. In the navigation tree, click **User Services > Administrative Users**.

The Administrative Users Web page appears, as shown in [Figure 18: Administrative Users Web page](#) on page 98.

3. Click **Add**.

The Add New Administrative User Web page appears, as shown in the following figure.

AVAYA Avaya Unified Communications Management Help | Logout

Host Name: 47.11.49.228 Software Version: 02.00.0036.03(2899) User Name admin

Add New Administrative User

Step1: Identify the new user.
Enter the user's full name and select an authentication type and User ID. Locally authenticated users also required a temporary password.

User ID: (1-31) (Allowed characters are a-z, A-Z, 0-9, - and _)

Authentication Type: ☒ Local ☐ External

Full Name:

Temporary password:

Re-enter password:

The user will be required to change this password when logging in.

Allowed characters in the password are: a-zA-Z0-9(){}<>.,/=[^_@\$%&-+~:~"; The length of your password should be at least 8 characters.

Note: The new user must be saved before you may assign roles.

Figure 19: Add New Administrative User Step 1 Web page

4. In the User ID field, type the User ID. The User ID can be up to 31 characters in length.
5. In the Authentication Type, select **Local** or **External**. For more information about local and external users, see [Authentication](#) on page 47
6. In the Full Name field, type the name of the user.
7. In the Temporary password field, type the new password.
8. In the Re-enter password field, type the new password.

Important:

The password that is entered for the new local user is temporary. For the first time logon to UCM, the user is prompted to change the password.

9. Click **Save and Continue**.

The Add New Administrative User Step 2 Web page appears, as shown in the following figure.

Add New Administrative User

Step2: Assign Role(s)

Selected roles authorize the user for associated features and element permissions.

<input type="checkbox"/>	Role Name	Elements	Description
<input type="checkbox"/>	1 MemberRegistrar	All elements of type: Linux Base	Member Registrar Role
<input type="checkbox"/>	2 NetworkAdministrator	All elements of type: CS1000 All elements of type: Deployment Manager All elements of type: Hyperlink All elements of type: IPSec Manager All elements of type: Linux Base All elements of type: Network	Network Administrator Role

Finish Cancel

Figure 20: Add New Administrative User Step 2 Web page

10. Assign roles to the new local user by selecting one or more **Role Name** boxes.
11. Click **Finish**.

The Administrative Users Web page appears.

Editing user role mapping

Select roles to authorize a user for associated features and element permissions.

1. Log on to UCM as an administrator.
2. In the navigation tree, click **User Services > Administrative Users**.

The Administrative Users Web page appears, as shown in [Figure 18: Administrative Users Web page](#) on page 98.

3. Click the **User ID** to edit role mapping.

The User Details Web page appears, as shown in the following figure.

AVAYA Avaya Unified Communications Management Help | Logout

Host Name: 47.11.49.205 Software Version: 02.00.0043.00(3017) User Name admin

User Details (admin)

Set user properties and assign predefined Roles.

☒ Enabled
☐ Disabled

Password Reset: Password:
 Re-enter password:

The user will be required to change this password when logging in.

Allowed characters in the password are: a-zA-Z0-9(){}<>./!@#\$%&-*~?`~\; The length of your password must be at least 8 characters.

Full Name:

Authentication Type: ☒ Local
☐ External

User ID:

Roles

Select Roles...

Role Name	Elements	Description
NetworkAdministrator	All elements of type: CS1000 All elements of type: Deployment Manager All elements of type: ...	Network Administrator Role

Figure 21: User Details Web page

4. Click **Select Roles**.

The User Roles Web page appears for the selected user, as shown in the following figure.

AVAYA Avaya Unified Communications Management Help | Logout

Host Name: 47.11.49.205 Software Version: 02.00.0043.00(3017) User Name admin

User Roles (admin)

Selected roles authorize the user for associated features and element permissions.

Roles

<input type="checkbox"/> Role Name	Elements	Description
<input type="checkbox"/> ¹ MemberRegistrar	All elements of type: Linux Base	Member Registrar Role
<input checked="" type="checkbox"/> ² NetworkAdministrator	All elements of type: CS1000 All elements of type: Deployment Manager All elements of type: Hyperlink All elements of type: IPSec Manager All elements of type: Linux Base	Network Administrator Role

Figure 22: User Roles Web page

5. Select or clear the roles for the selected user.

6. Click **Save**.

The User Details Web page appears, as shown in [Figure 21: User Details Web page](#) on page 101.

7. Click **Save**.

Configure the properties of a local user

An administrator with NetworkAdministrator role permission assignment can edit the full name and reset the password for local and built-in administrators. An administrator can also enable or disable accounts and edit the selected administrator's role assignment.

The administrator can change the password and full name for a local user, to disable and enable a local user account, and to delete a user.

Editing the password and full name for a local user account

Use the following procedures to change the password and full name for a local user account.

1. Log on to UCM as a network administrator.
2. In the navigation tree, click **User Services > Administrative Users**.

The Administrative Users Web page appears, as shown in [Figure 18: Administrative Users Web page](#) on page 98.

3. Click the **User ID** to edit the password and full name.

The User Details Web page appears, as shown in [Figure 21: User Details Web page](#) on page 101.

4. In the Full Name field, edit the name of the user.
5. In the Password Reset section, in the Password field, type a new password.
6. In the Re-enter password field, type the new password again.

Note:

For the first time logon, the user is prompted to change the password.

7. Click **Save**.

The Administrative Users Web page appears, as shown in [Figure 18: Administrative Users Web page](#) on page 98.

Disabling a user account

Disable one or more user accounts in UCM.

1. Log on to UCM as a network administrator.
2. In the navigation tree, click **User Services > Administrative Users**.

The Administrative Users Web page appears, as shown in [Figure 18: Administrative Users Web page](#) on page 98.

3. Click the User ID of the account to be disabled.

The User Details Web page appears, as shown in [Figure 21: User Details Web page](#) on page 101.

4. Select the **Disabled** option, and click **Save**.

OR

Select the check box beside the User ID of one or more user accounts, as shown in [Figure 18: Administrative Users Web page](#) on page 98, and click **Disable**.

Log on as the selected user to verify the change.

A user can disable built-in accounts; however, the UCM Security Services does not notify the Linux servers when this occurs. The built-in accounts remain valid in the Linux host account database.

Enabling a user account

Enable one or more user accounts in UCM.

1. Log on to UCM as a network administrator.
2. In the navigation tree, click **User Services > Administrative Users**.

The Administrative Users Web page appears, as shown in [Figure 18: Administrative Users Web page](#) on page 98.

3. Click the **User ID** for the disabled user account.

The User Details Web page appears, as shown in [Figure 21: User Details Web page](#) on page 101.

4. In the User Details Web page, select **Enabled**.
5. Click **Save**.

Deleting a user account

Delete one or more user accounts in UCM.

1. Log on to UCM as a network administrator.
2. In the navigation tree, click **User Services >Administrative Users**.

The Administrative Users Web page appears, as shown in [Figure 18: Administrative Users Web page](#) on page 98.

3. Select the check box beside the User ID of one or more user accounts.
4. Click **Delete**.

The Delete Users Web page appears, as shown in the following figure.

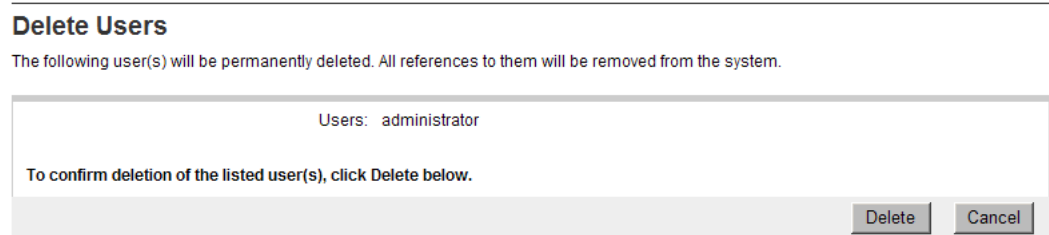


Figure 23: Delete Users Web page

5. Click **Delete** to proceed with the deletion or **Cancel** to cancel the deletion.

Important:

Users cannot delete their own accounts.

External Authentication

In the User Services branch of the UCM navigation tree, click External Authentication. The External Identity Repositories Web page contains a summary page for Authentication scheme and Authentication Servers. You can configure the authentication scheme and the authentication servers for UCM.

UCM supports up to three authentication authorities:

- local users
- external RADIUS users
- external LDAP users

The authentication scheme policy determines the order that the three authentication authorities are used. The supported order is as follows:

- local users (default)
- external RADIUS users then local users
- external LDAP users then local users
- external LDAP users, then external RADIUS users, then local users.
- external RADIUS users, then external LDAP users, then local users.
- external KERBEROS server

The authentication servers policy controls the settings for the external LDAP, RADIUS, and KERBEROS servers.

You can edit the authentication scheme, as shown in [Editing the authentication scheme](#) on page 105 and configure the authentication servers as shown in [Provision the authentication servers](#) on page 106.

Authentication scheme policy

UCM supports up to three authentication authorities:

- local servers
- external RADIUS servers
- external LDAP servers (including Sun ONE or Microsoft active directory server)
- Kerberos server

Editing the authentication scheme

Use the following procedure to edit the authentication scheme.

1. Log on to UCM Common Services as a network administrator.
2. In the navigation tree, click **User Services > External Authentication**.

The External Identity Repositories page appears, as shown in the following figure.

Figure 24: External Identity Repositories

3. In the Authentication Scheme section, click **Edit**.

The Authentication Scheme Web page appears, as shown in the following figure.

Figure 25: Authentication Scheme Web page

4. Select the required authentication scheme, and click **Save**.

Provision the authentication servers

When the LDAP server is Microsoft Active Directory, the full name of the external user must be the same as the logon name that makes the cn attribute of the external users the same as the logon name.

The TCP port used for the external LDAP server and the UDP port used for the external RADIUS server must be open in the Linux iptables firewall on both the primary security service and back up primary security service. To check the status of the iptables rules, use service iptables status.

In the Authentication Servers page, you can provision an LDAP, a Radius, or a Kerberos Server, as shown in [Figure 26: Authentication Servers Web page](#) on page 107.

Provisioning the LDAP Server

Configure the required information for the LDAP authentication server.

1. Log on to UCM Common Services as a network administrator.
2. In the navigation tree, click **User Services > External Authentication**.

The External Identity Repositories page appears, as shown in [Figure 24: External Identity Repositories](#) on page 106.

3. In the Authentication Servers section, click Configure.

The Authentication Servers Web page appears, as shown in the following figure.

Authentication Servers

☐ **Provision LDAP Server**

IP (or DNS):

TCP Port (for example 389):

Base Distinguished Name (for example dc=nortel,dc=com):

SSL/TLS Mode: ☐

Is Active Directory (Active directory does not support Anonymous Binding): ☐

Distinguished Name for Root Binding (for example cn=Bob,cn=Users,dc=nortel,dc=com):

Password for Root Binding:

☐ **Provision Radius Server**

IP (or DNS):

UDP Port:

Shared Secret:

☐ **Provision Kerberos Server**

DC Host Name (FQDN):

DC Computer Domain:

Keytab File:

Figure 26: Authentication Servers Web page

4. In the Provision LDAP Server section, complete the following information:
 - **IP (or DNS):** Type the IP address or DNS name of the LDAP server.
 - **TCP Port:** Type the TC port number of the LDAP server.
 - **Base Distinguished Name:** Type the base DN of the LDAP server.
 - Select **SSL/TLS Mode** if the LDAP server supports SSL/TLS connections.
 - Select **Is Active Directory** if active directory does not support anonymous binding.

- Select **Supports Anonymous Binding** if supported.
- In the **Distinguished Name for Root Binding** field, type the distinguished name for the root binding.
- In the **Password for Root Binding** field, type the password for the root binding.

5. Click **Save**.

Important:

Ensure the Linux iptable firewall setting on both the primary and backup security service allows the TCP port as source port.

Provisioning the Radius Server

Configure the required information for the RADIUS authentication server.

1. Log on to UCM Common Services as a network administrator.
2. In the navigation tree, click **User Services > External Authentication** , as shown in [Figure 24: External Identity Repositories](#) on page 106.

The External Identity Repositories page appears.

3. In the Authentication Servers section, click **Configure**.

The Authentication Servers Web page appears, as shown in [Figure 26: Authentication Servers Web page](#) on page 107.

4. In the Provision RADIUS Server section, complete the following information:
 - **IP (or DNS):** Type the IP address or DNS name of the primary RADIUS server.
 - **UDP Port:** Type the UDP port number of the primary RADIUS server.
 - **Shared Secret:** Type the shared secret of the RADIUS server.

Important:

You must create two records in the external RADIUS server with the same shared secret for both the primary security server and backup security server IP address.

5. Click **Save**.

Important:

Ensure the Linux iptable firewall setting on both the primary and backup security service allows the UDP port as source port.

Provisioning the Kerberos Server

Configure the required information for the Kerberos server.

1. Log on to UCM Common Services as a network administrator.
2. In the navigation tree, click **User Services > External Authentication**, as shown in [Figure 24: External Identity Repositories](#) on page 106.

The External Identity Repositories page appears.

3. In the Authentication Servers section, click **Configure**.

The Authentication Servers Web page appears, as shown in [Figure 26: Authentication Servers Web page](#) on page 107.

4. In the Provision Kerberos Server section, complete the following information:
 - **DC Host Name (FQDN):** Type your FQDN in the following format: `machineName.domainName.com/net/`
 - **DC Computer Domain:** Type the domain name of the Kerberos server.
 - **Keytab File:** Type the encrypted Kerberos server key.
5. Click **Save**.

Important:

When logged on to the Kerberos server using Single Sign-on (SSO), you cannot exit from UCM using the Logout link because in this context, SSO automatically authenticates you inside the Domain Controller (DC) domain. You must manually close the browser to exit the application.

Password

In the User Services branch of the UCM navigation tree, click Password. The Password Status Web page appears. From the Password Status Web page, users can view the status for a local account password and change a local account password.

Reviewing the status of a local account password

Determine when a local password can change and when the password expires.

1. Log on to the UCM common services.
2. In the navigation tree, click **User Services > Password**.

The Password Status Web page appears.

Important:

An external user cannot review or change the password.

Changing a local account password

Change the current password.

1. Log on to UCM Common Services.
2. In the navigation tree, click **User Services > Password**.

The Password Status Web page appears, as shown in [ReviewingTheStatusOfALocalAccountPassword](#) on page 109.

3. Click **Change Password**.

The Change Password Web page appears, as shown in the following figure.

The screenshot shows the Avaya Unified Communications Management interface. At the top, the AVAYA logo is on the left, and the text 'Avaya Unified Communications Management' is on the right. Below this, a status bar displays 'Host Name: 47.11.48.243', 'Software Version: 02.00.0039.00(2959)', and 'User Name admin'. The main heading is 'Change Password (admin)'. Below the heading, it says 'Change your password.' and provides three input fields: 'Current password:', 'New password:', and 'Confirm new password:'. To the right of these fields are 'Save' and 'Cancel' buttons. Below the input fields, a section titled 'New passwords must satisfy the following rules:' lists several requirements:

- Passwords can only have the following characters: a-zA-Z0-9{ }() < > , = [] ^ _ @ ! \$ % & - + " ' ? ~ ;
- Passwords must have a length of at least 8 characters.
- Passwords must have at least 1 lowercase characters.
- Passwords must have at least 1 uppercase characters.
- Passwords must have at least 1 numeric characters.
- Passwords must have at least 1 special characters.
- Passwords must not have a character repeated more than twice consecutively.
- Passwords must not have the user's login name, either in forward or reverse.
- Users can not use any of their previous 6 passwords.

Figure 27: Change Password Web page

4. In the Current password field, type the current password.
5. In the New password field, type the new password.

Important:

The default password strength policy is defined by your network administrator. Follow the password strength policy requirements shown on the Change Password Web page.

6. In the Confirm new password field, type the new password.
7. Click **Save**.

Chapter 10: UCM Security configuration

This chapter describes the security features found in the Unified Communications Management (UCM) navigation pane under the Security branch.

UCM provides the tools network administrators need to manage and maintain security within the UCM infrastructure. From the security section, a network administrator can perform the following tasks:

- Roles: manage users and roles
- Policies: manage password policies, single sign-on cookie domain, and logon warning banner
- Certificates: manage certificates
- Active Sessions: view and terminate active sessions

For information about Security, see *Avaya Security Management Fundamentals*, NN43001-604.

Use the procedures in this chapter to manage security in UCM.

Navigation

- [Roles](#) on page 113
- [Policies](#) on page 123
- [Certificates](#) on page 130
- [Active Sessions](#) on page 134

Roles

In the Security branch of the UCM navigation tree, click Roles. The Roles Web page appears. From the Roles Web page, network administrators can perform the various role management tasks required to manage roles within UCM.

In UCM, users must be given permissions to perform tasks. UCM Security Services supports two types of roles—built-in and custom roles. The built-in roles that can be assigned to users are MemberRegistrar, NetworkAdministrator, Patcher, CS1000_Admin1, CS1000_Admin2, CS1000_CLI_REGISTRAR and CS1000_PDT2, as shown in [Figure 28: Roles Web page](#) on page 114. Within these roles, you have access to various elements and from there you can choose specific permission mappings. The built-in roles in UCM are not editable. For more information about built-in roles, see [Built-in roles](#) on page 55.

For more information about creating custom roles, see [Adding a custom role](#) on page 114.

Important:

If an administrator has multiple roles assigned, the permission is granted based on the highest privileged algorithm.

Roles

User Roles provide group-level authentication functions and element permissions. Users with a given role may only perform functions that are authorized for that role

Add... Delete		Refresh	
<input type="checkbox"/> Role Name ^	Users	Elements	Description
1 <input type="checkbox"/> CS1000_Admin1	0	All elements of type: CS1000 All elements of type: Deployment Manager All elements of type: Linux Base All elements of type: Patch Manager All elements of type: Snmp Manager	General OAM (call server and related elements)
2 <input type="checkbox"/> CS1000_Admin2	0	All elements of type: CS1000 All elements of type: Deployment Manager All elements of type: IPSec Manager All elements of type: Linux Base All elements of type: Patch Manager All elements of type: Secure FTP Token Manager All elements of type: Snmp Manager	General OAM and Security Administration (call server and related elements)
3 <input type="checkbox"/> CS1000_PDT2	0	All elements of type: CS1000	Full diagnostic access,

Figure 28: Roles Web page

Reviewing existing roles

View the current roles in UCM.

1. Log on to UCM as a network administrator.
2. In the navigation tree, click **Security > Roles**.

The Roles Web page appears with a list of available roles, as shown in [Figure 28: Roles Web page](#) on page 114.

3. Use the scroll bar to review the existing roles within UCM.

Adding a custom role

A network administrator can add custom roles to map to specific elements, for example a single CS 1000 element, and then customize permissions for that element.

1. Log on to UCM as a network administrator.
2. In the navigation tree, click **Security > Roles**.

The **Roles** Web page appears with a list of available roles, as shown in [Figure 28: Roles Web page](#) on page 114.

3. Click **Add**.

The Add New Role Web page appears, as shown in the following figure.

Figure 29: Add New Role Web page

Note:

The role name must be from 1 to 26 characters in length. Allowed characters are a-z, A-Z, 0-9, - and _

4. In the Role Name field, type the unique role name.
5. In the Role Description field, type a description for the new role.
6. Click **Save and Continue**.

The Role Details (newRole) Web page appears, as shown in the following figure.

AVAYA Avaya Unified Communications Management Help | Logout

Host Name: 47.11.49.228 Software Version: 02.00.0036.03(2899) User Name admin

Role Details (newRole)

Identification

Role Name:

Description: 1-x characters

Element/Service Permission **Assigned Users**

<input type="checkbox"/>	Name	Permissions
<input type="checkbox"/>		

Figure 30: Role Details Web page

7. Click the **Element/Service Permission** mapping tab.
8. Click **Add Mapping**.

The Select Element and/or Network Service to Map to Role page appears, as shown in the following figure.

Select Element and/or Network Service to Map to Role (test)

Group Name

Element and/or Network Service Name

Figure 31: Select Element and/or Network Service to Map to Role

9. Select a **Group Name** and an **Element and/or Network Service Name** from the list to create a role that provides access to elements of a particular type and belonging to a specified group. After a group name is selected, the **Element and/or Network Service Name** list shows only the element types subcategory. Click **Next**.

The following page appears indicating the mapping available for the selected group and element type.

Permission Mapping (All elements of type: CS1000 under Multi-core New York for test)

Users with this role will be authorized to perform all management functions associated with the selected permissions on the indicated element.

Template for permission set: Default CS1000 Permissions

Role: test

Administration (PWD)

- ☐ None
- ☒ Specified OAM privileges, specified customers
Only those features explicitly enabled in the corresponding section below.
- ☐ General OAM, all customers
- ☐ General OAM, all customers, plus Security Administration

Diagnostic (PDT)

Diagnostic permissions may be combined with any of the above Admin permission sets.

- ☒ None
- ☐ PDT1
Limited diagnostic shell.
- ☐ PDT2

Save Cancel

Figure 32: Permission mapping when a Group Name is selected

OR

If you do not select a **Group Name** from the list, you can select items from one of the following subcategories in the **Element and/or Network Service Name** list.

- individual element by name
- element by type
- network service

Click **Next**.

Depending on the Element and/or Network Service Name selection, you may see different Permission Mapping pages. See the following figure for an example of the Permission Mapping page with elements of type LinuxBase.

Permission Mapping (All elements of type: Linux Base for newRole)

Users with this role will be authorized to perform all management functions associated with the selected permissions on the indicated element.

Template for permission set: CS1000_Admin1

Role: newRole

<input checked="" type="checkbox"/> Backup Administrator	<input checked="" type="checkbox"/> Database Administrator	<input checked="" type="checkbox"/> Log Administrator
<input checked="" type="checkbox"/> Maintenance Administrator	<input checked="" type="checkbox"/> Patch Administrator	<input checked="" type="checkbox"/> Security Administrator
<input checked="" type="checkbox"/> System Administrator	<input checked="" type="checkbox"/> Time Administrator	

Save Cancel

Figure 33: Permission Mapping—with element type of LinuxBase

10. Assign permissions as required for the new role, and click **Save**.
11. Click **Save** on the Role Details (newRole) page to confirm your settings, as shown in the following figure.

AVAYA Avaya Unified Communications Management Help | Logout

Host Name: 47.11.49.228 Software Version: 02.00.0043.00(3017) User Name admin

Role Details (newRole)

Identification

Role Name:

Description: 1-x characters

Save Cancel

Element/Service Permissi	Assigned Users
<input type="button" value="Add Mapping..."/> <input type="button" value="Delete Mapping"/> <input type="button" value="Copy All From..."/>	
<input type="checkbox"/> Name	Permissions
1 <input type="checkbox"/> Software Deployment	System Administrator
2 <input type="checkbox"/> All elements of type: Linux Base	Backup Administrator, Patch Administrator, System Administrator

Figure 34: Role Details page with Assigned Users tab

Using templates for permission mapping

You can assign permissions by selecting a preconfigured permission template or you can create a custom permission template. A custom permission template can be created for a given element type by creating a custom role that maps to all elements of a given type, editing, and saving the permission mapping for all elements of a given type. The custom permission template then has the name of the custom role to where it belongs and appears in the Template for permission set option list, as shown in [Figure 35: Modifying the permission mapping](#) on page 120. The Permission mapping template also contains built-in roles to mapping permissions for an individual element or for all elements of a given type.

1. Log on to UCM as a network administrator.
2. In the navigation tree, click **Security > Roles**.

The Roles Web page appears, as shown in [Figure 28: Roles Web page](#) on page 114.

3. Click a role from the Role Name column.
4. Click the **Element/Service Permissions** tab and click **Add Mapping**.
5. Select an Element Name, for example, CS1000, from the list and click **Next**.

The Permission Mapping (All elements of type: CS1000 for newrole) appears.

6. You can modify the permissions by selecting or clearing check boxes. You can also select another permission set by choosing another template from the list, as shown in the following figure.

Permission Mapping (All elements of type: CS1000 for newRole)

Users with this role will be authorized to perform all management functions associated with the selected permissions on the indicated element.

Template for permission set: Default CS1000 Permissions

Administration (PWD)

☐ None

☒ Specified OAM privileges, specified customers
Only those features explicitly enabled in the corresponding section below.

☐ General OAM, all customers

☐ General OAM, all customers, plus Security Administration

D diagnostic (PDT)

D diagnostic permissions may be combined with any of the above Admin permission sets.

☒ None

☐ PDT1
Limited diagnostic shell.

☐ PDT2

Save Cancel

Figure 35: Modifying the permission mapping

7. Click **Save**.

Assign or edit role mapping

The following procedures are used to assign or edit permission mapping. In the Role Details page, click the Assigned Users tab. There are two options for assigning permission mapping to a role. The administrator can select an element to add to a role by clicking Select Users or by copying the mapping from another role by selecting Copy All From.

Note:

The Copy All From command allows you to copy user assignments from one role to another role.

Selecting users

1. In the **Assigned Users** tab.
2. Click **Select Users** to assign or edit a role to individual users.

The Assigned Users (newRole) page appears, as shown in the following figure.

Assigned Users (newRole)

Selected Users will be granted the permissions associated with this role.

<input type="checkbox"/>	User Name	Full Name:	Type
1 <input type="checkbox"/>	1	111	local
2 <input type="checkbox"/>	admin	Default security administrator	local
3 <input type="checkbox"/>	binita	banerjee	local
4 <input type="checkbox"/>	jin	jinpeng	local
5 <input type="checkbox"/>	justin	justin	local
6 <input type="checkbox"/>	justin2	justin2	local
7 <input type="checkbox"/>	justpatch	m	local
8 <input type="checkbox"/>	justview	vdvd	local
9 <input checked="" type="checkbox"/>	user1	Chris Smith	local

Figure 36: Assigned Users

3. Select one or more check boxes beside the User ID to grant permissions associated with this role.
4. Click **Save**.

The Role Details (newRole) page appears, as shown in [Adding a custom role](#) on page 114. You can use this page to view the new permissions for that role.

Copying user assignment

1. An administrator can copy user assignments from another role to the new role. In the **Assigned Users** tab, click **Copy All From**.
2. The Permission Mapping (all Permissions for newrole) page appears, as shown in the following figure.

Permission Mapping (all Permissions for newrole)

Select a role to copy all permission mappings for all elements/services. Additional changes can be made later if required.

Figure 37: Permission Mapping (all Permissions for newrole)

Important:

The copy from Role list does not contain the NetworkAdministrator role. The NetworkAdministrator role has underlying permissions that cannot be copied.

3. Select a role from the Copy from Role list.
4. Click **Copy**.

The Role Details (newRole) page appears, as shown in [Adding a custom role](#) on page 114.

5. Click **Save**.

The Roles page appears, as shown in [Figure 28: Roles Web page](#) on page 114. You can use this page to view the new permissions for that role.

Editing a role description

Edit the role description, Element/Service Mapping, and Assigned Users. The role name cannot be changed from the Role Details page.

1. Log on to UCM.
2. On the navigation tree, click **Security > Roles**.

The Roles Web page appears, as shown in [Figure 28: Roles Web page](#) on page 114.

3. In the Role Name column, click a Role Name item to edit the description.

The Role Details (newRole) Web page appears, as shown in [Adding a custom role](#) on page 114.

4. In the Description field, edit the information as required.
5. Click **Save** to save your changes or **Cancel** to return to the Roles page without saving your changes.

The Roles Web page reappears, as shown in [Figure 28: Roles Web page](#) on page 114.

Deleting custom roles

Only custom roles can be edited or deleted. Log on as network administrator to delete a custom role. User role assignments for administrators assigned to the deleted roles are also deleted.

1. Log on to UCM as a network administrator.
2. On the navigation tree, click **Security > Roles..**
3. In the Roles Web page, select one or more check boxes beside the custom role to delete.

The Delete Roles Web page appears with the selected roles for deletion, as shown in the following figure.

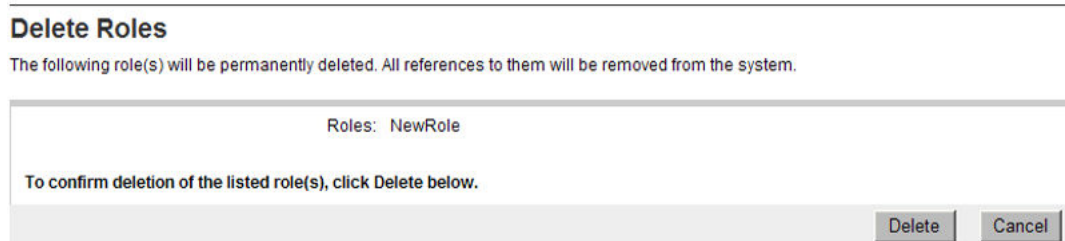


Figure 38: Delete Roles Web page

4. Click **Delete** to proceed with the deletion or **Cancel** to cancel the deletion and return to the Roles page.

Policies

In the Security branch of the navigation tree, click Policies. The Policies Web page appears. A network administrator can configure the Password policy (for locally authenticated users), Security Settings, and the Single Sign-on (SSO) Cookie Domain.

Reviewing security policies

Review the currently configured security policies within the UCM.

1. Log on to UCM Common Services as a network administrator.
2. In the navigation tree, click **Security > Policies.**

The Policies Web page appears, as shown in the following figure.

Policies

Establish password policies, single sign-on cookie domain, and login/legal warnings.

Password Policy (for locally authenticated users)
Edit...

Aging: Passwords can not be changed in 3 days after the last changes. Passwords expire in 90 days after the last changes. Show password expiration warning during login 7 days before passwords become expired.
 History: Previous 6 passwords cannot be reused.
 Strength: Allowed characters in the password are: a-zA-Z0-9(){}<>./=:^_@!\$%&+~?'\; Passwords must have at least 8 characters. Passwords must have at least 1 lower case characters. Passwords must have at least 1 upper case characters. Passwords must have at least 1 numeric characters. Passwords must have at least 1 special characters.
 Lockout: Accounts are locked for 2 minutes if 5 failed login attempts occur with consecutive failed attempts happen within 10 minutes.

Session Properties
Edit...

Maximum Session Time: 120 minutes.
 Maximum Idle Time: 30 minutes.

Security Settings
Edit...

Login Warning Banner: This computer system and network is PRIVATE and PROPRIETARY of [company name] and may only be accessed by authorized users. Unauthorized use of this computer system or network is strictly prohibited and may be subject to criminal prosecution, employee discipline up to and including discharge, or the termination of the vendor/service contracts. The owner, or its agents, may monitor any activity or communication on the computer system or network.

Single Sign-on Cookie Domain
Edit...

nortel.com

Figure 39: Policies Web page

3. Review the policy settings currently in UCM.

Editing password policies

Configure the local account password policies including, aging, history, strength, and lockout password policies in UCM according to business requirements.

1. Log on to UCM Common Services as a network administrator.
2. On the navigation tree, click **Security > Policies**.

The Policies Web page appears, as shown in [Figure 39: Policies Web page](#) on page 124.

3. In the Password Policy (for locally authenticated users) section, click **Edit**.

The Password Policy Web page appears, as shown in the following figure.

Password Policy

Aging: ☒ Enforce password aging policies

Enable expired password change: ☒

Expiration period: (1-365 days)

Expiration warning: (1-15 days)

Minimum age: (0-7 days)

A minimum age prevents password recycling that could otherwise defeat the history policy.

History: ☒ Enforce policy against previously used passwords

Previous passwords blocked: (1-99)

Strength: ☒ Enforce password content standards

Minimum Total Length: (6-25)

Minimum by character Type: (sum cannot exceed minimum total length)

Lower case: (0 = not required)

Upper case: (0 = not required)

Special case: (0 = not required)

When the strength policy is enabled, passwords must also meet the following requirements:

- Passwords must not have a character repeated more than twice consecutively.
- Passwords must not have the user's login name, either in forward or reverse.

Lockout: ☒ Enforce user lockout after failed login attempts

Consecutive Invalid Login Attempts: (1-20)

Interval for Consecutive Invalid Login Attempts: (0-120 minutes)

Lockout Time: (0-120 minutes)

Figure 40: Password Policy Web page

4. In the Aging section, perform the following actions:

- Select the **Aging** check box.
- In the Expiration period field, type a number from 1 to 365 for the maximum allowable days to maintain the password. The default value is 90.
- In the Expiration warning field, type a number from 1 to 15 to send a warning message to a user that the password is about to expire. The default value is 7.
- In the Minimum age field, type a number from 0 to 7 for the minimum allowable days for password age. The default value is 3.

Ensure that the number for the expiration period is greater than the minimum password age number.

Important:

All passwords expire. If an administrator password expires, the administrator can reset the password through the UCM user interface.

5. In the History section, perform the following actions:

- Select the **History** check box.
- In the Previous passwords blocked field, type a number from 1 to 99 for the number of passwords to maintain in history. The default value is 6.

6. In the Strength section, perform the following actions:

- Select the **Strength** check box.
- In the Minimum Total Length field, type a number from 6 to 25 for the minimum number of total characters for the password. The default value is 8.

In the Minimum by character Type fields, perform the following steps:

- In the Lower case field, type the minimum number of lowercase characters for the password. The default value is 1.
- In the Upper case field, type the minimum number of uppercase characters for the password. The default value is 1.
- In the Numeric case field, type the minimum number of numeric characters for the password. The default value is 1.
- In the Special case field, type the minimum number of special characters for the password. The default value is 1.

Important:

The sum of the character types cannot exceed the minimum total length.

7. In the Lockout section, perform the following actions:

- Select the **Lockout** check box.
- In the Consecutive Invalid Login Attempts field, type a number for failed attempts from 1 to 20. The default value is 5.
- In the Interval for Consecutive Invalid Login Attempts field, type the interval in number of minutes from 0 to 120 for consecutive invalid logon attempts. The default is 10 minutes.
- In the Lockout Time field, type the number of minutes from 0 to 120 until the account is unlocked. The default is 2 minutes.

Important:

An invalid logon message appears for the following scenarios:

- A logon attempt is made on a disabled account.

- The password is invalid.
- The maximum number of log on attempts is reached.
- The password is expired.

For each scenario, the system responds with a message that invalid logon credentials were used. You must contact the network administrator for additional information.

Important:

The system sends a warning message when a password is about to expire. The password must be changed.

8. Click **Save**.

Editing Session Properties

Manage the global properties of user sessions including maximum session time and maximum idle time.

1. Log on to UCM Common Services as a network administrator.
2. On the navigation tree, click **Security > Policies**.

The Policies Web page appears, as shown in [Figure 39: Policies Web page](#) on page 124.

3. In the Session Properties section, click **Edit**.

The Session Properties page appears, as shown in the following figure.

Session Properties

Manage global properties of user sessions. Saved modifications will only apply to newly logged in users.

Maximum Session Time: (10-1440 minutes)

Maximum Idle Time: (10-1440 minutes)

The maximum idle time must not exceed the maximum session time.

Figure 41: Session Properties

4. Perform the following actions:
 - In the Maximum Session Time field, type a number for maximum session time in minutes from 0 to 1440.
 - In the Maximum Idle Time field, type a number for the maximum idle time in minutes from 0 to 1440.
5. Click **Save**.

Security Settings

UCM provides a customizable logon banner that appears when a user logs on to the system. The customizable banner is intended for use by customers with security policies that require network equipment to display a specific message to users when they log on. The following figure show the default logon warning banner message.

Table 12: Default Login warning message

WARNING! This computer system and network is PRIVATE and PROPRIETARY of [company name] and may only be accessed by authorized users. Unauthorized use of this computer system or network is strictly prohibited and may be subject to criminal prosecution, employee discipline up to and including discharge, or the termination of the vendor/service contracts. The owner, or its agents, may monitor any activity or communication on the computer system or network.

Editing the login warning banner

Customize the message for the logon warning banner in UCM.

1. Log on to UCM Common Services as a network administrator.
2. On the navigation tree, click **Security > Policies**.

The Policies Web page appears, as shown in [Figure 39: Policies Web page](#) on page 124.

3. In the Security Settings section, click **Edit**.

The Logon Warning Banner Web page appears, as shown in the following figure.

Figure 42: Login Warning Banner Web page

4. In the Login Warning Banner text area, edit the text as required.

Note:

The maximum number of characters allowed is 2500.

5. Click **Save**.

Editing the Single Sign-on Cookie Domain

Change the Single Sign-on (SSO) cookie domain when the primary and backup security servers are configured in different domains, Single Sign-on (SSO) requires authentication to switch from the primary to backup security server. For authentication, the primary and backup security server domain names must match.

1. Log on to UCM Common Services as a network administrator.
2. On the navigation tree, click **Security > Policies**.

The Policies Web page appears, as shown in [Figure 39: Policies Web page](#) on page 124.

3. In the Single Sign-On Cookie Domain section, click **Edit**.

The Edit Domain Name page appears.

4. From the Single Sign-On Cookie Domain list, select a URL to change the Single Sign-on Cookie Domain.
5. Click **Save** to save the change.

Important:

- When the SSO cookie domain changes, you must clear the existing UCM related cookies from the cache in the Internet browser for all users.
- When selecting an SSO cookie domain, ensure that all servers in the security domain share the same cookie domain. For example, if you are in the domain ca.avaya.com

and you want to access servers using single sign-on in the domain europe.avaya.com, you need to change the SSO to avaya.com.

- Top level domains such as com.ca or com.au cannot be assigned as the SSO cookie domain as these can be rejected by some Internet browsers.

Certificates

In the Security branch of the navigation tree, click Certificates. The Certificate Management Web page appears. From the Security Certificates Web page, a network administrator can access the Certificate Endpoints tab and the Private Certificate Authority tab, as shown in [Figure 43: Certificate Management](#) on page 131. You can search and filter a certificate endpoint by typing an endpoint friendly name or endpoint address. You can search and filter all certificates generated by the UCM private certificate authority from the Certificate Management page by typing the certificate serial number or subject DN. The search field can be used to search Certificate Endpoints as well as the certificates generated by the UCM private CA. For a successful endpoint search, the search criteria must contain at least a part of an Endpoint Address or Element Name. For a successful certificate search, the search criteria must contain at least a part of the certificate Serial Number or Subject DN.

Perform the following procedures to view the Certificate Endpoints and the Private Certificate Authority. For more information about certificates, see *Avaya Security Management Fundamentals*, NN43001-604.

Viewing the details of a certificate endpoint

View the details of a certificate endpoint.

1. Log on to UCM Common Services as a network administrator.
2. In the navigation tree, click **Security > Certificates**.

The Certificate Management Web page appears, as shown in the following figure.

Certificate Management

Distribute and maintain Web SSL and SIP TLS security certificates, and manage the Private Certificate Authority.

Certificate Endpoints

Private Certificate Authority

Display the details of a certificate endpoint by selecting the radio button associated with that endpoint. When an endpoint is associated with multiple elements, it is listed once for each of the corresponding elements.

	Endpoint Address	Element Type	Element Name	Number of Service Profiles
1	<input checked="" type="radio"/> 47.11.49.211	Linux Base	member13-express-ecm-ibm5.ca.avaya.co	4
2	<input type="radio"/> 47.11.49.104	Linux Base	backup-ecm-hp14.ca.avaya.com (backup)	4
3	<input type="radio"/> 47.11.49.228	Linux Base	otm-hpt10.ca.avaya.com (primary)	4

Endpoint Details

Details for the selected endpoint.

Certificates

	Service Profile	Status	Friendly name	Expiration date
1	Default Certificate	signed	member3-express-ecm-ibm5.ca.avaya.com	Oct 15, 2018
2	Web SSL	none		
3	DTLS	none		
4	SIP TLS	none		

Certificate Authorities

<div>Add...</div>	<div>Enable Trust</div>	<div>Disable Trust</div>	<div>Delete</div>	<div>Update CRL</div>	
	Friendly name	Expiration date	Trusted	Issued by	Last CRL Update
1	<input checked="" type="radio"/> ffeb	Oct 13, 2018	yes	/O=veriffST=on/L=bww/C=CA/CN:	
2	<input type="radio"/> otm-hp10.ca.avaya.c	Feb 1, 2035	yes	/O=veriffST=on/L=bww/C=CA/CN:	Oct 17, 2008

Figure 43: Certificate Management

3. In the Certificate Endpoints section, click the option next to the endpoint for which you want to view the details.

The certificate information related to the selected endpoint appears in the Endpoint Details section. To access the service profile, click the **Service Profile** column header.

Updating the CRL

Update a CRL for a certificate endpoint.

1. Log on to UCM Common Services as a network administrator.
2. On the navigation tree, click **Security > Certificates**.

The Certificate Management Web page appears, as shown in [Figure 43: Certificate Management](#) on page 131.

3. In the Certificate Authorities section, click the option button next to the certificate authority for which you want to update the CRL.

4. Click **Update CRL**.
5. A popup window appears.
6. Copy the contents of the CRL and paste in the text area.
7. Click **Submit**

Downloading Private Certificate Authority Details

Use the Private Certificate Authority tab to display a list of all the issued and revoked certificates.

1. Log on to UCM Common Services as a network administrator.
2. On the navigation tree, click **Security > Certificates**.

The Certificate Management Web page appears, as shown in [Figure 43: Certificate Management](#) on page 131.

3. Click the **Private Certificate Authority** tab.

The Private Certificate Authority window appears.

4. In the Private Certificate Authority Details section, click **Download** to download the certificate contents as a security certificate file.

The File Download - Security Warning window appears.

5. Click **Save**.

The Certificate Details window appears showing the details of the certificate.

6. Click **Ok**.

Revoking a certificate

Revoke a certificate.

1. Log on to UCM Common Services as administrator.
2. On the navigation tree, click **Security > Certificates**.

The Certificate Management Web page appears.

3. Click the **Private Certificate Authority** tab.

4. In the Certificates section, select one or more of the check boxes beside the Serial Number and click **Revoke** to revoke the selected certificates.

Downloading the Certificate Revocation List (CRL) Details

Download details of the Certificate Revocation List.

1. Log on to UCM Common Services as a network administrator.
2. On the navigation tree, click **Security > Certificates**.

The Certificate Management Web page appears, as shown in [Figure 43: Certificate Management](#) on page 131.

3. Click the Private Certificate Authority tab.
4. In the Certificate Revocation List (CRL) Details section, click **Get CRL**, as shown in the following figure.

Certificate Revocation List (CRL) Details

CRL number: 1 Expiration date: Dec 8, 2008 Contents: <input type="button" value="Get CRL"/>

Figure 44: Certificate Revocation List (CRL) Details section

The File Download window appears.

5. Click **Save**.

Adding a CallPilot certificate

The CallPilot certificate must be added to the UCM manually. The Web browser cannot prompt a user to accept a certificate when communicating internally between UCM and CallPilot because CallPilot is not integrated in the UCM security framework. Use the following procedure to manually add the CallPilot certificate.

1. In the Internet Explorer Web browser, type `https://<CallPilot IP>/cpmgr`. Where <CallPilot IP> is the IP or FQDN of the CallPilot Manager requiring the certificate.

2. For Internet Explorer 6.0:

In the Security Alert dialog box, click **View Certificate** and go to [6](#) on page 134.

For Internet Explorer 7.0 or 8.0:

Click **Continue to this website (not recommended)**.

The CallPilot Managerpage appears.

3. When the certificate is signed by a Trusted Certificate Authority, right-click the lock icon that appears to the right of the Web address bar.

OR

4. When the certificate is not signed by a Trusted Certificate Authority, right-click **Certificate Error** on the pink bar, as shown in the figure below.

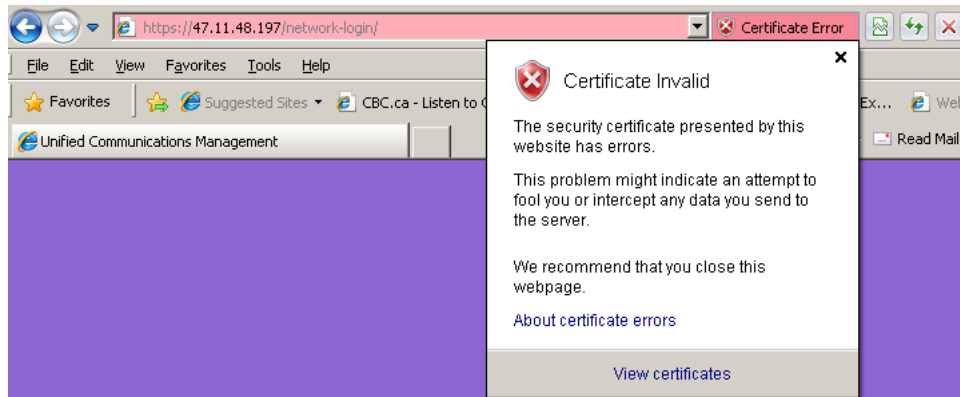


Figure 45: Certificate Error

5. Click **View Certificates**.

The Certificate window appears.

6. Click the **Details** tab.
7. In the Certificate export Wizard window, click **Copy to File** and click **Next**.
8. Select the **Base-64 encoded X.509 (.CER)** option and click **Next**.
9. Click **Finish** to exit the Certificate Export Wizard.
10. Log on to UCM. In the UCM navigation tree, click **Security > Certificates**.

The Certificate Management Web page appears.

11. On the Certificate Endpoints tab, click the option button next to the endpoint address for which you want to view the details. In this case, the UCM server.
12. In the Certificate Authorities section, click **Add**.
13. Open the .CER file from [8](#) on page 134 in a text editor and copy the contents into the Add a CA to the Service dialog box and click **Submit**.
14. The CallPilot certificate is displayed in the Certificate Authorities table and all communication to the CallPilot is secured over SSL.
15. Log off and log on to UCM for the change to take effect.

Active Sessions

Access the Active Sessions Web page from the Security branch of the UCM navigation tree to review user session information and to terminate user sessions. With the appropriate

permissions, a network administrator can view the session information for any user who is currently logged on.

Viewing active sessions

View the current sessions in UCM. Network administrators can see all users who are currently logged on to UCM and view the session time for the user.

1. Log on to UCM as a network administrator.
2. On the navigation tree, click **Security > Active Sessions**.

The Active Sessions Web page appears, as shown in the following figure.

The sessions are sorted in the User ID column.

Active Sessions			
Manage sessions of logged in users.			
<input type="button" value="Terminate"/>		<input type="button" value="Refresh"/>	
<input type="checkbox"/> User ID	Name	Session Duration (hh:mm:ss)	Is Current
1 <input type="checkbox"/> cnt5	Mary	0:47:40	Yes

Figure 46: Active Sessions Web page

Terminating Single Sign-On sessions

Terminate selected Single Sign-On (SSO) sessions in UCM.

1. Log on to UCM as a network administrator.
2. In the navigation tree, click **Security > Active Sessions**.

The Active Sessions Web page appears, as shown in [Figure 46: Active Sessions Web page](#) on page 135.

3. Select the check box beside the required sessions to terminate.
4. Click **Terminate**.

The selected sessions are deleted from the current sessions table. Administrators with terminated sessions are required to log on again.

Chapter 11: UCM Tools configuration

This chapter contains information on the Tools branch in the Unified Communications Management (UCM) navigation pane.

Navigation

[Logs](#) on page 137

Logs

Access the Logs Web page from the Tools branch of the UCM navigation tree to view log files. You can view logs by OAM Events and Security Events type, use the date or search function, configure or edit the configuration of logs for third-party OSS, and export the logs as comma-separated value (CSV) files. From Base Manager, you can also configure forwarding of logs that are generated on the backup and member servers for consolidation on the primary security server.

Important:

The Security Event log type and Log Forwarding button are not available when you are logged on as a non-network administrator.

Enabling OAM and Security logs for consolidation

Configure consolidation of OAM and Security logs to the primary security server from the backup and member security server.

Important:

By default, log consolidation is not configured.

1. Log on to the UCM member security server as a network administrator to access Base Manager.
2. On the navigation tree, click **Tools > Logs > OAM**, as shown in the following figure.

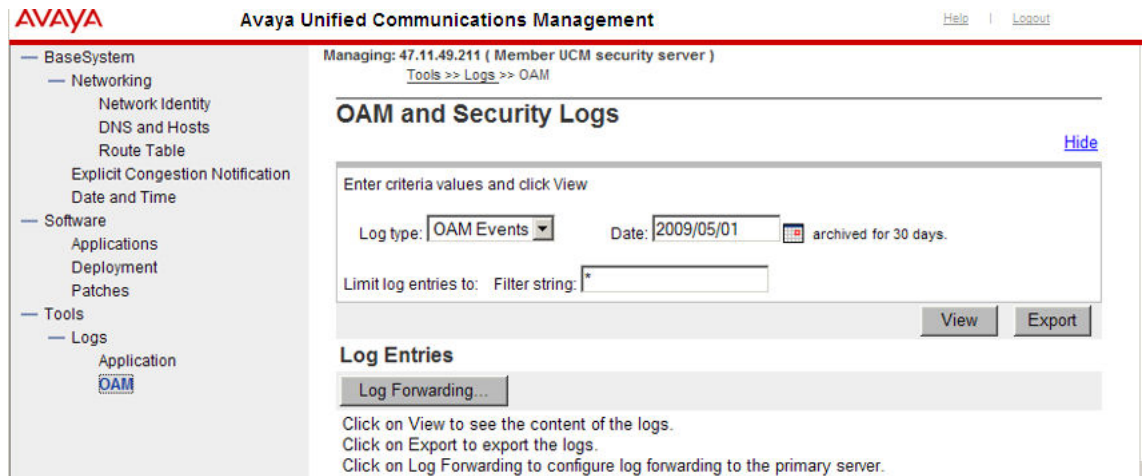


Figure 47: Log Forwarding Base Manager

3. Click **Log Forwarding**.

The Log consolidation Web page appears, as shown in the following figure.

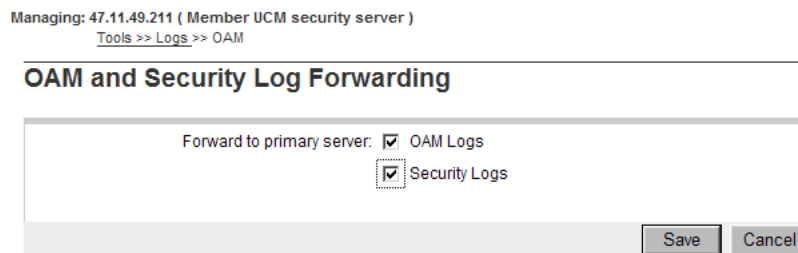


Figure 48: Logs consolidation Web page

4. In the Forward to primary server field, select **OAM logs** and **Security Logs** to enable consolidation of logs.
5. Click **Save**.

Viewing log types with the network administrator role

View log types when you log on with the network administrator role.

1. Log on to UCM as a network administrator.
2. In the navigation tree, click **Tools > Logs**.

The Logs Web page appears, as shown in the following figure.

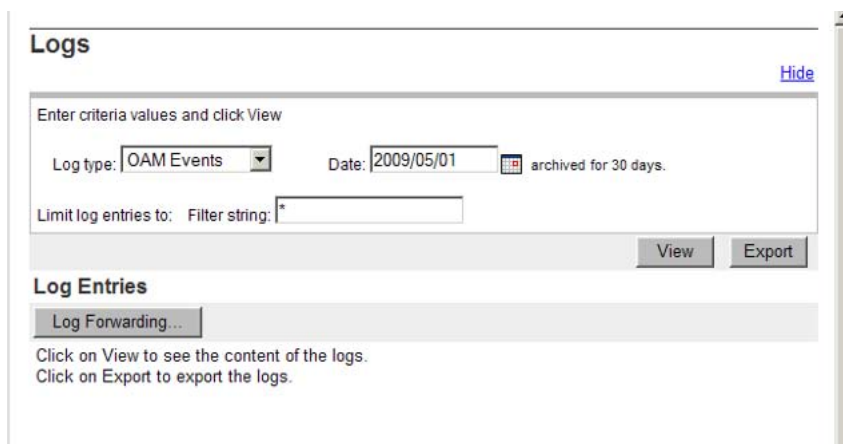


Figure 49: Logs page with network administrator role

3. In the Log type field, select **OAM Events** or **Security Events** from the list.
4. Click **View**.

Configuring or editing the configuration of logs for forwarding to third-party OSS

Configure or edit the configuration of logs for forwarding to third-party Operational Support System (OSS) Syslog servers when you log on with the network administrator role. Network administrators can forward OAM Events and Security Event logs.

Important:

Application logs from any type of server cannot be forwarded to third party OSS. When configuring member and primary servers between a firewall or SMC, the firewall must be enabled with the syslog port UDP 514 to allow the messages from the members to reach the primary.

1. Log on to UCM as a network administrator.
2. On the navigation tree, click **Tools > Logs**.

The Logs Web page appears, as shown in [Figure 49: Logs page with network administrator role](#) on page 139.

3. Click **Log Forwarding**.

The Log Forwarding page appears, as shown in the following figure.

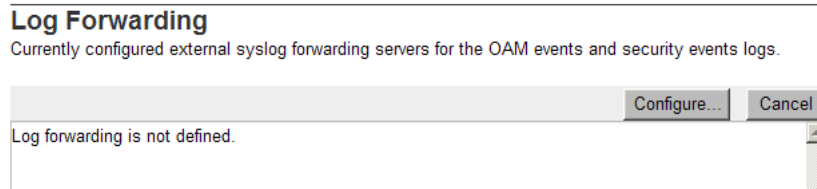


Figure 50: Log Forwarding

4. Click **Configure** to configure log forwarding.

The Log Forwarding configuration page appears, as shown in the following figure.

Figure 51: Configuring log forwarding

5. Configure external syslog forwarding servers by completing the following fields:

Name: Type hostname of the third party system. It must be between 1 to 32 characters.

IP address: Type the IP address of the syslog server.

UDP port: Type the UDP port number of the syslog server. Default is 514.

Log type: Select **OAM Events** and choose the Severity from the list (options are: All, Debug, Information, Notice, Warning, Error, Critical, Alert, Emergency)

OR

Select **Security Events** as the Log type.

Important:

Severity is listed in order of lowest priority. All messages with the selected priority and the priorities below it are forwarded, for example, selecting Alert forwards Alert and Emergency messages.

6. Click **Save**.

Viewing audit logs by date

View logs by selecting a date.

1. Log on to UCM.
2. On the navigation tree, click **Tools > Logs**.

The Logs Web page appears, as shown in [Figure 49: Logs page with network administrator role](#) on page 139.

3. In the Date field, type a date within the last 30 days using the format YYYY/MM/DD, or click the calendar icon to select a date.
4. Click **View**.

The results of the search appear on the same page.

Important:

The selected date cannot be older than 30 days from the current date; otherwise, an error message appears.

Viewing Audit logs using the search functionality

View logs using the search functionality.

1. Log on to UCM.
2. On the navigation tree, click **Tools > Logs**.

The Logs Web page appears, as shown in [Figure 49: Logs page with network administrator role](#) on page 139.

3. In the Limit log entries to section, type a search string in the Filter string field. For example, info.
4. Click **View**.

The results of the search appear on the same page.

Exporting the log file as a CSV file

Export the log file as a CSV file.

Important:

Non-network administrators can export only OAM event logs.

1. Log on to UCM.
2. On the navigation tree, click **Tools > Logs**.

The Logs Web page appears, as shown in [Figure 49: Logs page with network administrator role](#) on page 139.

3. Click **Export**.

The File Download dialog box appears.

4. Click **Save** to export the log file as a CSV file.

Data

Use the Data tool for disaster recovery purposes or to synchronize the data on the primary security server data with the backup security server after one of the servers has been restored or upgraded. The backup data store synchronizes with the primary data store.

Caution:

This tool deletes data. Use with caution.

Reloading from UCM primary:

1. Log on to the backup security server as Administrator
2. On the navigation tree, click **Tools > Data**.

The Data Tools Web page appears.

3. Click **Reload from UCM primary** to delete data from the backup data store and begin copying everything from the primary data store.

After the data is deleted, you are notified that the web server is restarting and the data reload is in progress.

4. Close the window.

Appendix A: Migration to System Manager

This appendix contains the information required to migrate from Communication Server 1000 Unified Communications Management (UCM) to Avaya Aura® System Manager 6.2.

There are two options for migrating Communication Server 1000 systems to Avaya Aura System Manager and Session Manager.

- Option 1: For systems that have already upgraded to Communication Server 1000 Release 7.5 but have not migrated to System Manager and Session Manager. See [Migration option 1](#) on page 144.
- Option 2: For migrating to System Manager and Session Manager before upgrading the Communication Server 1000 and the registered elements to Release 7.5. See [Migration option 2](#) on page 153.

Note:

With the migration to System Manager, the existing Communication Server 1000 UCM primary security domain is decommissioned and a new System Manager primary security domain is established. All elements are unregistered from the Communication Server 1000 UCM security domain and registered to the new System Manager UCM primary security domain.

Navigation

- [Migration option 1](#) on page 144
- [Migration option 2](#) on page 153
- [ConfiguringUCMtoappearonSystemManager](#) on page 158
- [Migratesystemelementstaskflow](#) on page 159
- [Registeringcs1klinuxmembers](#) on page 160
- [Registering VxWorks servers to SMGR](#) on page 161
- [Registeringcs1kucmandcores](#) on page 162
- [softwaredeployment](#) on page 162
- [Manuallyredefiningdeploymentdistributionsandgroupings](#) on page 164
- [Additional information](#) on page 165

Documentation references

For more information about the installation and administration of Session Manager and System Manager, see the following documents at <https://support.avaya.com/css/appmanager/css/support>.

- *Installing and Upgrading Avaya Aura® System Manager*
- *Administering Avaya Aura® System Manager*
- *Avaya Aura® Session Manager Overview*
- *Installing and Configuring Avaya Aura® Session Manager*
- *Administering Avaya Aura® Session Manager*

Migration option 1

Migration option 1 is for Communication Server 1000 Release 4.x to Release 7.0 systems that have already upgraded to Communication Server 1000 Release 7.5 but have not migrated to Avaya Aura System Manager and Session Manager.

System Manager supports the following Communication Server 1000 services:

- Deployment Manager
- Patch Manager
- Subscriber Manager

Note:

Within System Manager 6.2 Subscriber Manager has been replaced with User Management. For more information about migrating subscriber data, see the section “Importing users from CS 1000 Subscriber Manager to User Management” in *Administering Avaya Aura® System Manager*.

- Secure FTP token
- SNMP

The following table provides a checklist of the tasks required for migration option 1.

Table 13: High level checklist for migration option 1

Step	Task	Action	✓
1	Upgrade the Communication Server 1000 system to Release 7.5.	For more information, see the following documents: <ul style="list-style-type: none"> • For Release 6.0 and 7.x software upgrades only, see <i>Linux Platform Base and Application Installation and Commissioning, NN43001–</i> 	

Step	Task	Action	✓
		<p>315 and <i>Software Upgrades</i>, NN43041–458.</p> <ul style="list-style-type: none"> For Release 5.x software with ECM to UCM upgrade, see <i>Unified Communications Management Common Services Fundamentals</i>, NN43001–116 and <i>Linux Platform Base and Application Installation and Commissioning</i>, NN43001–315 For Release 4.x hardware and software with Element Manager/ Telephony Manager, you must upgrade to UCM, see <i>Linux Platform Base and Application Installation and Commissioning</i>, NN43001–315 and <i>Hardware Upgrade Procedures</i>, NN43041–464. 	
2	Decommission the backup UCM server.	The UCM server can be shutdown. You can reformat and reuse the server for another purpose.	
3	Install the Communication Server 1000 UCM CND Service Update patch on the Communication Server 1000 UCM primary server.		
4	Run the system backup command.	<p>Log on to the UCM Primary Linux console (through SSH) as nortel for Release 7.0 or admin2 for (Release 7.5.</p> <p>A tar file is generated on a USB memory stick or on an SFTP server.</p>	
5	Install System Manager SP4 using the existing UCM IP and FQDN on an isolated network.	Install Session Manager and configure Session Manager on the network.	
6	On System Manager/UCM server, copy the UCM backup tar file to the System Manager/UCM location / home/admin.	—	
7	Swap Ethernet systems.	Move the Ethernet cable from the UCM primary server to the System Manager/UCM server Ethernet port.	

Step	Task	Action	✓
8	Run the migration/restore script on the System Manager/UCM location <code>/home/admin</code>	Note: Do not interact with the system until the “CS 1000 Migration Completed Successfully.” message is printed.	
9	Configure UCM to appear on System Manager.	See Configuring UCM to appear on System Manager on page 158.	
10	Ensure the System Manager/UCM is operating correctly.	View elements, users, and roles as configured in the Communication Server 1000 UCM.	
11	Confirm all elements and features are operational.	Reregister the Call Server to the System Manager/UCM server FQDN/IP address.	

Migration task flow (option 1)

The following task flows provide a high level overview of migration option 1.

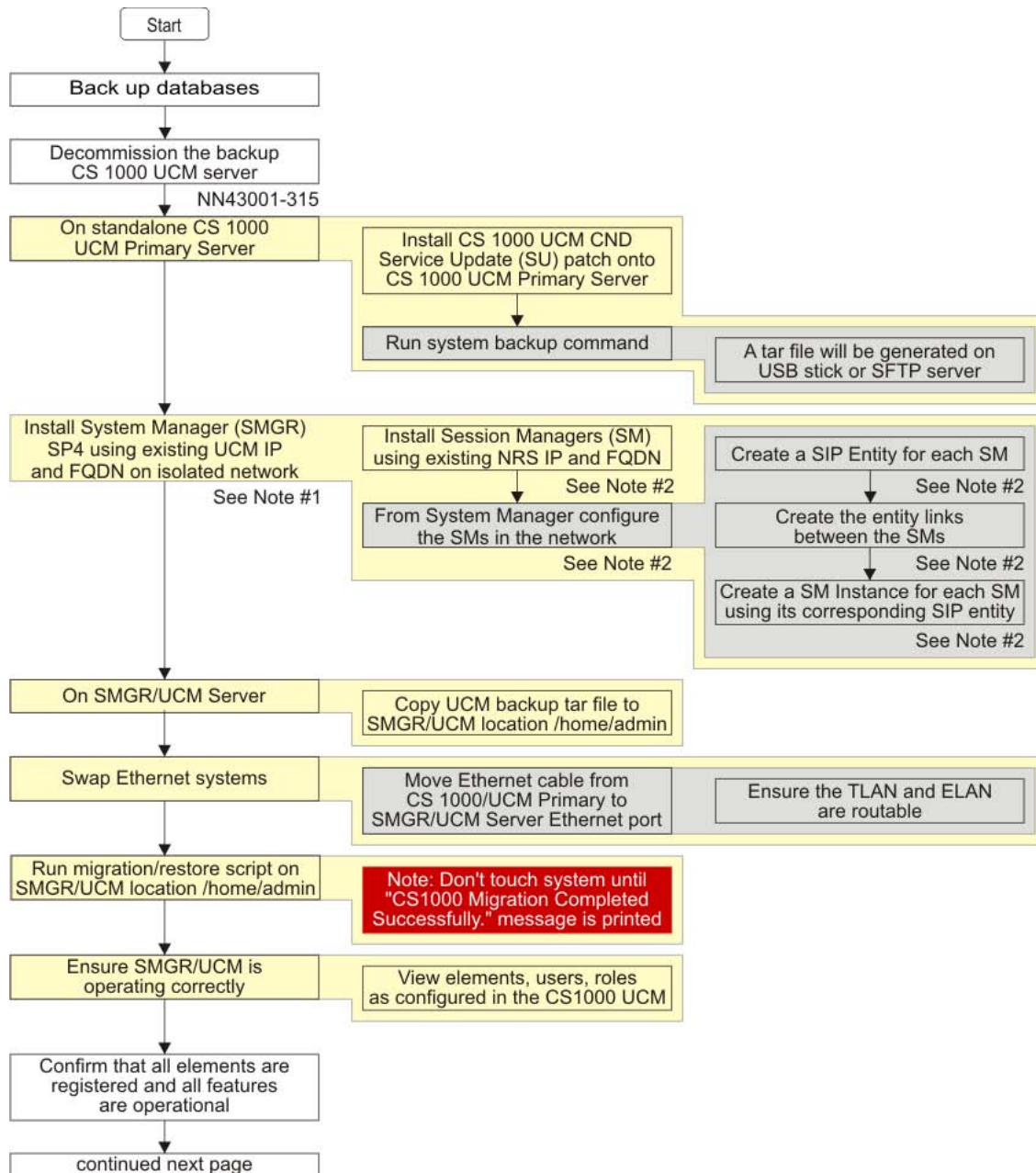


Figure 52: Migration option 1 (Part 1 of 3)

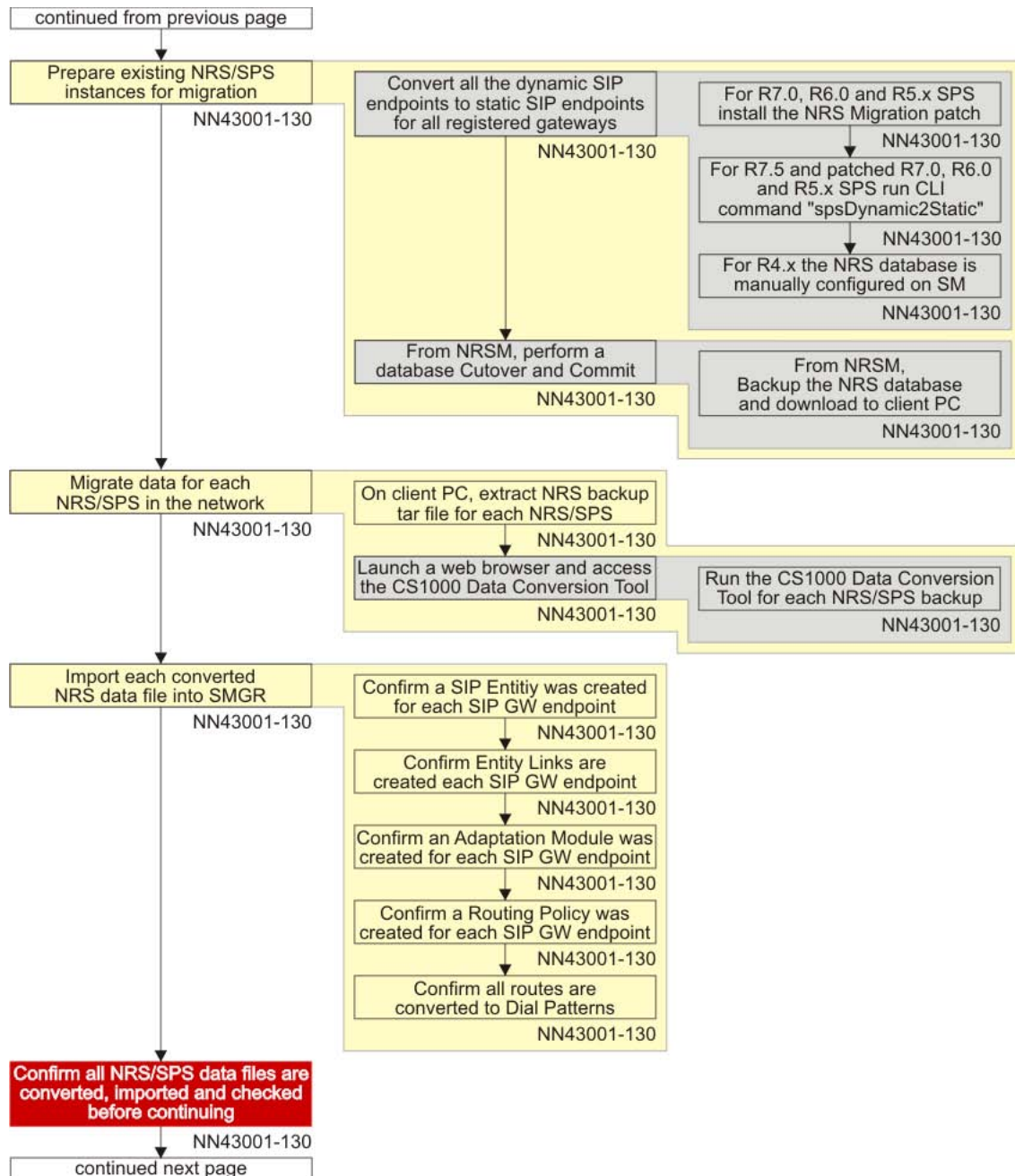
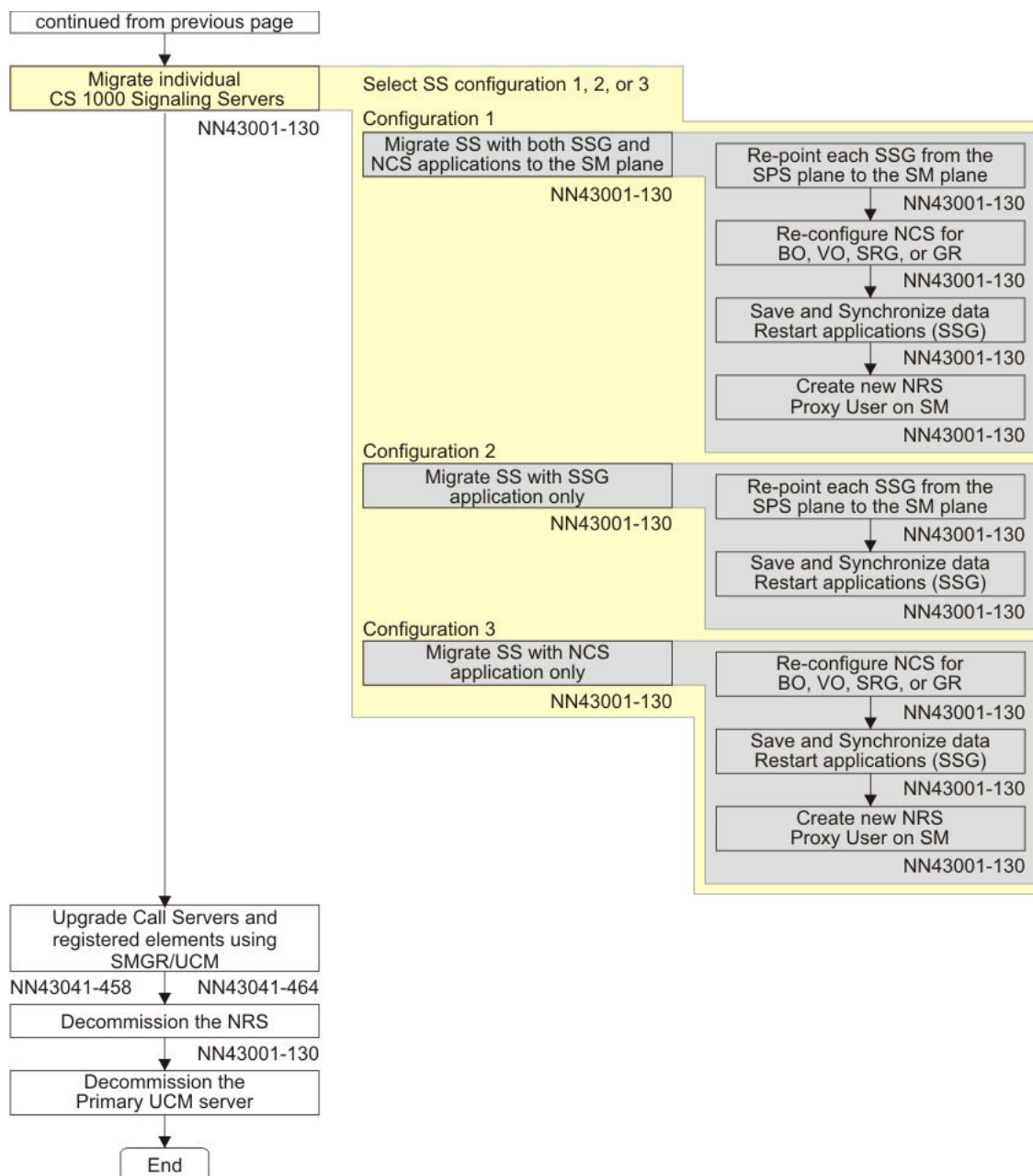


Figure 53: Migration Option 1 (Part 2 of 3)



Avaya Aura Documentation
 Note #1: Installing and Upgrading Avaya Aura™ System Manager
 Note #2: Installing and Configuring Avaya Aura™ Session Manager

Figure 54: Migration Option 1 (Part 3 of 3)

Premigration requirements

Prior to migrating, review the following requirements.

- Unified Communications Manager (UCM) must be on a standalone server platform. You must remove the Network Routing Service (NRS), Element Manager, and Call Server components if they are installed because System Manager does not support these components.
- UCM backup server is not supported so it must be removed from service and deleted from the UCM primary element list prior to migration.
- ELAN and TLAN must be routable because System Manager supports only one Ethernet port.

Note:

Avaya recommends connecting the TLAN. You are prompted to connect the TLAN to the System Manager Ethernet port in [Step 6](#) on page 152 for [Migrating CS 1000 systems already upgraded to Release 7.5](#) on page 150.

- If IPsec is enabled on the UCM primary server, you must disable it prior to migration.

For the migration procedures for option 1, see [Migrating CS 1000 systems already upgraded to Release 7.5](#) on page 150.

Migrating CS 1000 systems already upgraded to Release 7.5

Use the following procedure to migrate Communication Server 1000 Release 4.x to Release 7.0 systems that have already upgraded to Communication Server 1000 Release 7.5 but have not migrated to Avaya System Manager and Session Manager.

1. Ensure the Communication Server 1000 UCM server is operational.
2. Install the necessary patches on the Communication Server 1000 UCM server.
 - Download cs1000-linuxbase-7.50.17.16-3.i386.000 and avaya-cs1000-cnd-4.0.20-00.i386 Service Updates from the PEP library and save to `/var/opt/nortel/patch/`. Install these service updates on the UCM Primary server.

Note:

You must install the Linux Base SU before installing the CND SU.

For information about patches and service updates, see *Avaya Patching Fundamentals*, NN43001–407.

3. Use Secure Shell (SSH) to log on to the Communication Server 1000 UCM Primary Linux console as admin2, and run the system backup command. Select either Option 1 or Option 2, as shown in the following two figures.

```
[admin2@otm-ibml~]$ sysbackup -b

1. Backup to USB device.

2. Backup to SFTP server.

Enter your choice (q for exit): 1
Backup started. Please wait...
Executing all application 'backup' scripts .....
```

Figure 55: Option 1—System back up to a USB device

OR

```
admin2@otm-ibml~]$ sysbackup -b

1. Backup to USB device.

2. Backup to SFTP server.

Enter your choice (q for exit): 2
Enter the secure FTP server's IP address: xx.xx.xx.xx
Enter the SFTP login: admin2
Enter the SFTP password:
Enter the remote SFTP directory: /home/admin2
Remote Configuration File Validation

SFTP server IP: xx.xx.xx.xx
SFTP userid: admin2
SFTP password: *****

SFTP directory: /home/admin2

Is this information correct (Y/N) [Y]? y
Backup started. Please wait...
Executing all application 'backup' scripts .....
```

Figure 56: Option 2—System back up to an SFTP server

A tar file is generated on the USB memory stick or the SFTP service/server at xx.xx.xx.xlocation /home/admin2.

4. Perform a fresh installation of System Manager in an isolated LAN environment using the same IP and FQDN as the Communication Server 1000 UCM Primary server. For information about installing System Manager, see the document *Installing and Upgrading Avaya Aura® System Manager* at <https://support.avaya.com/css/appmanager/css/support>.
5. Copy the Communication Server 1000 UCM backup file generated in [Step 3](#) on page 150 to the System Manager/UCM location /home/admin.

6. Swap Ethernet systems. Unplug the Ethernet cable associated with the UCM FQDN/IP address (usually TLAN) from the Communication Server 1000 UCM Primary server and plug it into the System Manager/UCM server Ethernet port.

Note:

It is important to ensure that the TLAN and ELAN are routable; auto migration does not work if TLAN is not routable to ELAN.

7. Run the migration/restore script on System Manager (using the root account user ID) from the location `/home/ucmdeploy/quantumBackupRestore`.

```
[admin2@otm-ibm1~]$ su -  
Using major release number R016x on System Platform  
Password:  
[root@otm-ibm1~1]# cd /home/ucmdeploy/quantum/quantumBackupRestore  
[root@otm-ibm1~1]# perl cs1kmigrate /home/admin/otm-ibm15-2011_05_03-12_09_03.tar.gz
```

Do not interact with the system until the “CS 1000 Migration Completed Successfully.” message is printed, as shown in the following figure.

```
2011-05-03 15:03:28 : CS1000 Migration Completed Successfully.
```

8. Ensure the System Manager/UCM is operating correctly. All the elements, users, and roles that were visible in the Communication Server 1000 UCM will be visible from System Manager/UCM.
9. Confirm that all elements and features are operational. You must reregister the Call Servers to the System Manager/UCM server FQDN/IP address.

Note:

To finalize the migration, see [Post migration requirements](#) on page 152 for additional instructions.

Post migration requirements

The following identifies the post migration requirements and migration limitations.

Elements:

The Communication Server 1000 Call Server has an ELAN address. If you register the Call Server with the Communication Server 1000 Unified Communications Manager (UCM) Primary server, you are using the CS 1000 UCM Primary ELAN address. The Call Server remembers the ELAN address and after the migration, the System Manager/UCM server FQDN/IP address is the only valid address. You must then reregister the Call Server to the System Manager/UCM server FQDN/IP address.

Password policy:

The password policy is lost after migration. A default password is provided and can be modified after migration.

Groups:

Numbering group data is lost after migration. This is not supported by the migration tool.

ISSS configuration data:

Data is not migrated. You must configure IPsec after the migration.

SNMP:

Data is not migrated. You must configure SNMP after the migration.

Migration option 2

Migration option 2 is for Communication Server 1000 Release 4.x to Release 7.0 systems that are migrating to Avaya Aura System Manager 6.1 and Session Manager but have not upgraded the Communication Server 1000 Call Servers and registered elements to Release 7.5.

Requirements:

Review the following requirements before you upgrade the Communication Server 1000 Call Servers and the registered elements to Release 7.5

- Apply the NRS Migration Patch for Release 5.x to Release 7.0. You cannot migrate the Release 4.x NRS database to Session Manager.
- Obtain access to the Routing Data Conversion tool. The tool can be found at <https://nrstool.avaya.com/default.aspx>.
- System Manager 6.1 is already installed and you have logged on using the admin user ID and password as defined during the initial System Manager installation. Log on to all migration procedures with the admin user ID.
- Determine the elements to move to System Manager 6.1.
 - Identify VxWorks based systems and devices
 - Identify Co-resident Call Server and Signaling Server systems
 - Identify Signaling Servers
 - Identify elements where TLS is enabled
- Ensure that all elements are active and known to the Call Server.

The following table provides a high level checklist for migration option 2.

Table 14: High level checklist for migration option 2

Step	Task	Action	√
1	Upgrade the Primary Security server and Member servers to Communication Server 1000 Release 6.0 or later.	For more information, see <i>Linux Platform Base and Application Installation and Commissioning</i> , NN43001–315.	
2	Configure UCM to appear on the System Manager home page.	See Configuring UCM to appear on System Manager on page 158.	
3	Unregister system elements from UCM security domain and register system elements to the System Manager primary security domain.	<ul style="list-style-type: none"> Linux servers, see Registering CS 1000 UCM Linux members to System Manager on page 160 Vxworks servers, see Registering VxWorks servers to SMGR on page 161 Co-resident servers, see Registering CS 1000 Primary security server and co-resident applications to System Manager on page 162 <p>For VxWorks servers, use LD 117:</p> <ul style="list-style-type: none"> STAT UCMSECURITY INFO UNREGISTER UCMSECURITY SYSTEM REGISTER UCMSECURITY SYSTEM <p>For additional commands, see Additional information on page 165.</p>	
4	Upgrade the Call Server and registered elements.	See software deployment on page 162.	
5	Decommission the UCM Primary and Backup servers.	The UCM server can be shutdown. You can reformat and reuse the server for another purpose.	

Migration task flow (option 2)

The following task flows provide a high level overview for migration option 2.

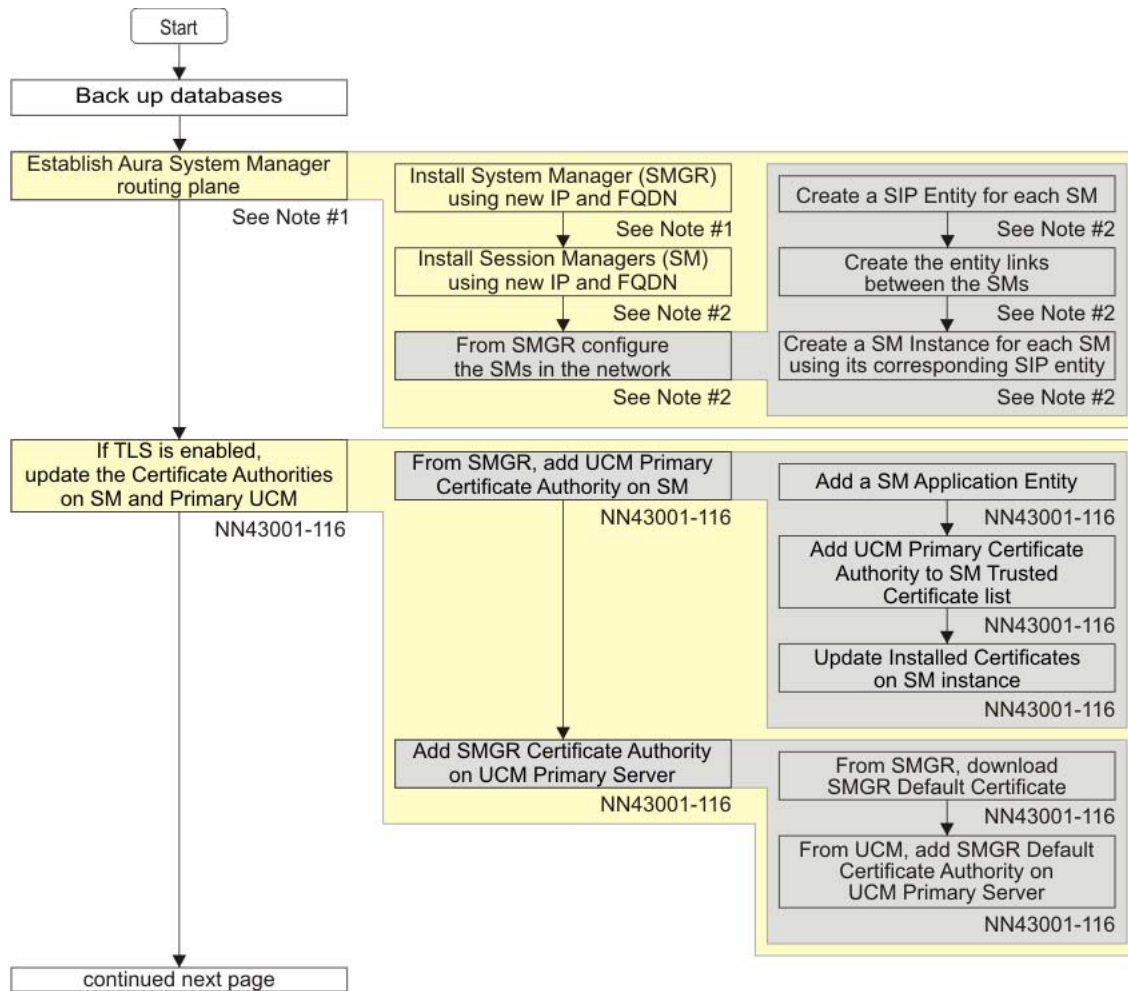


Figure 57: Migration option 2 (Part 1 of 4)

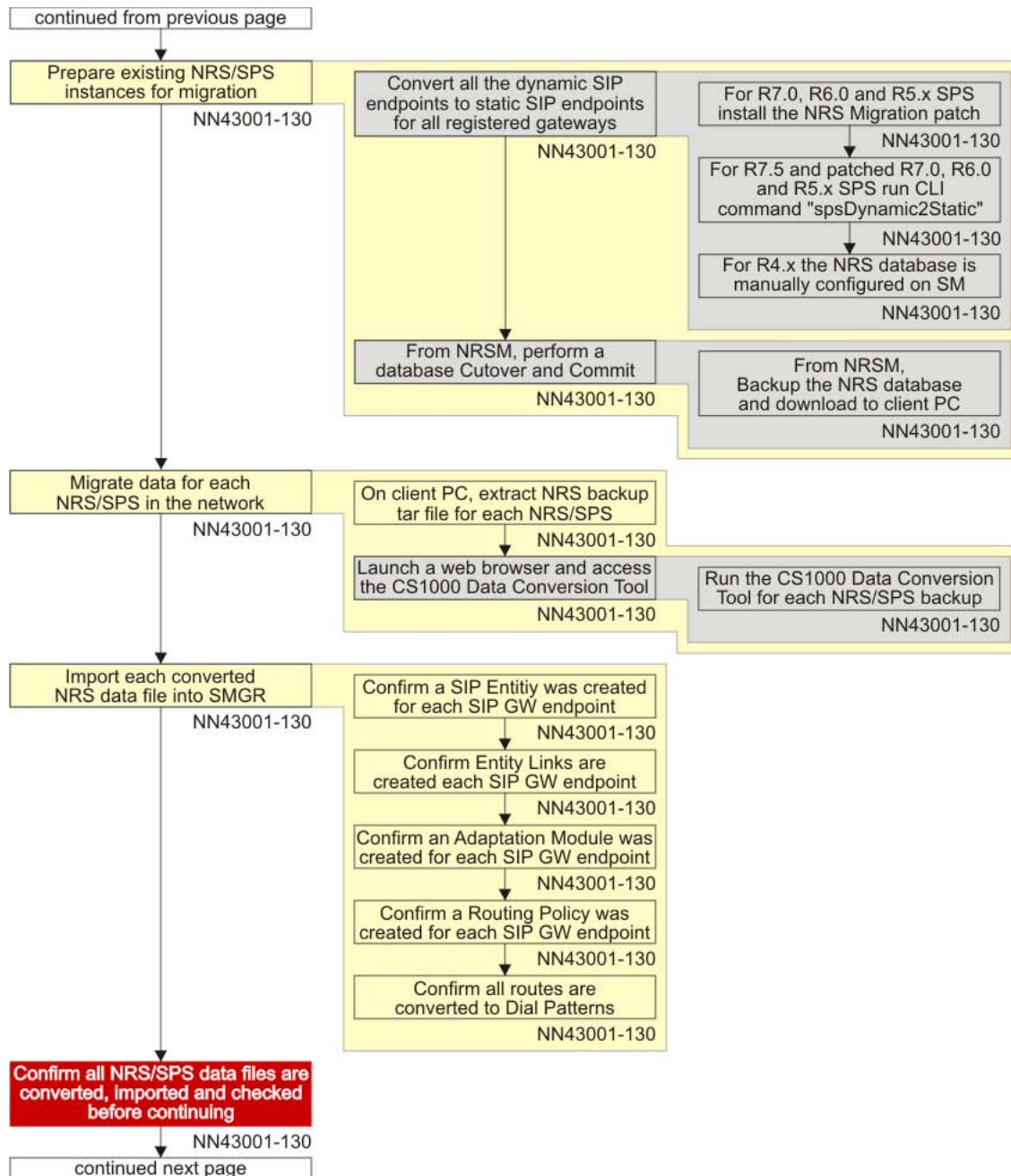


Figure 58: Migration option 2 (Part 2 of 4)

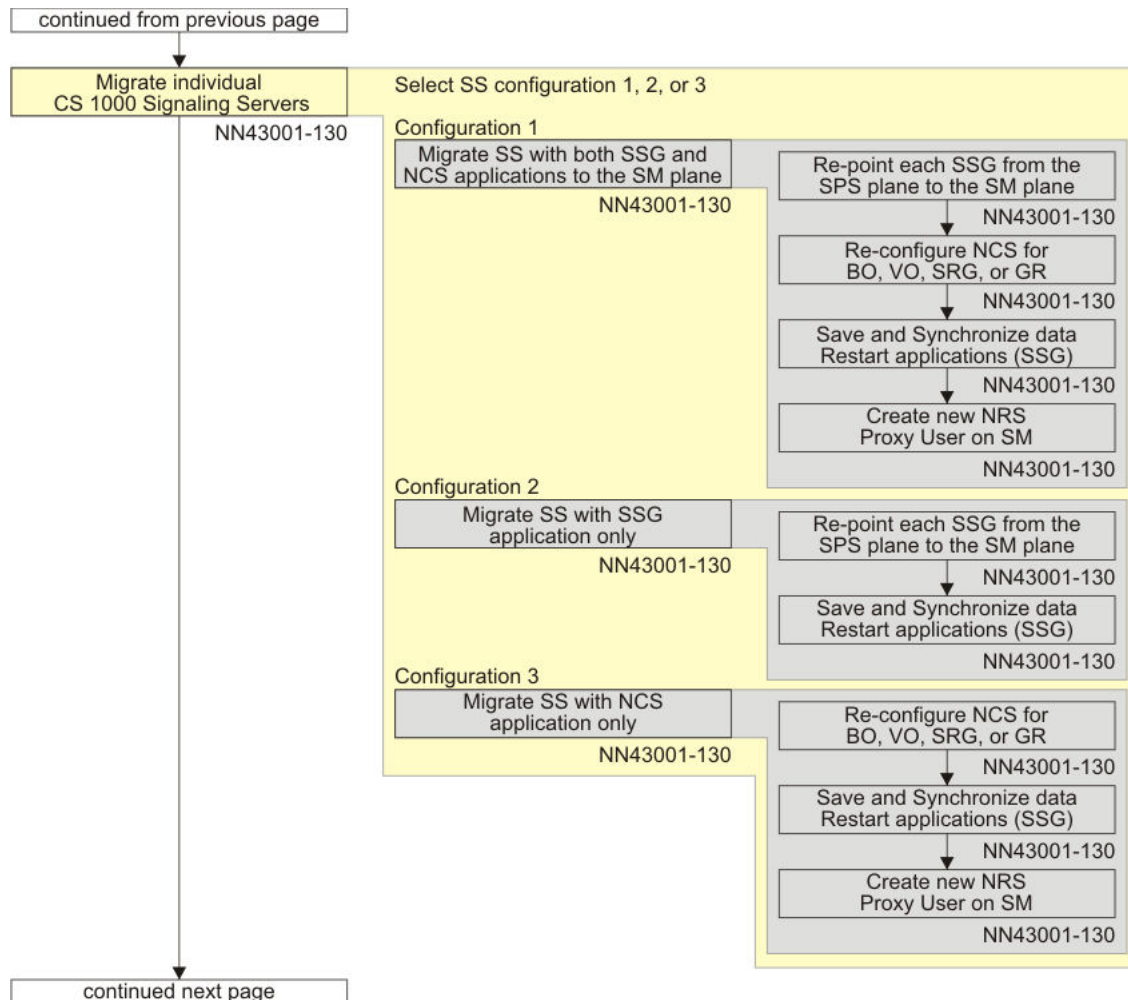
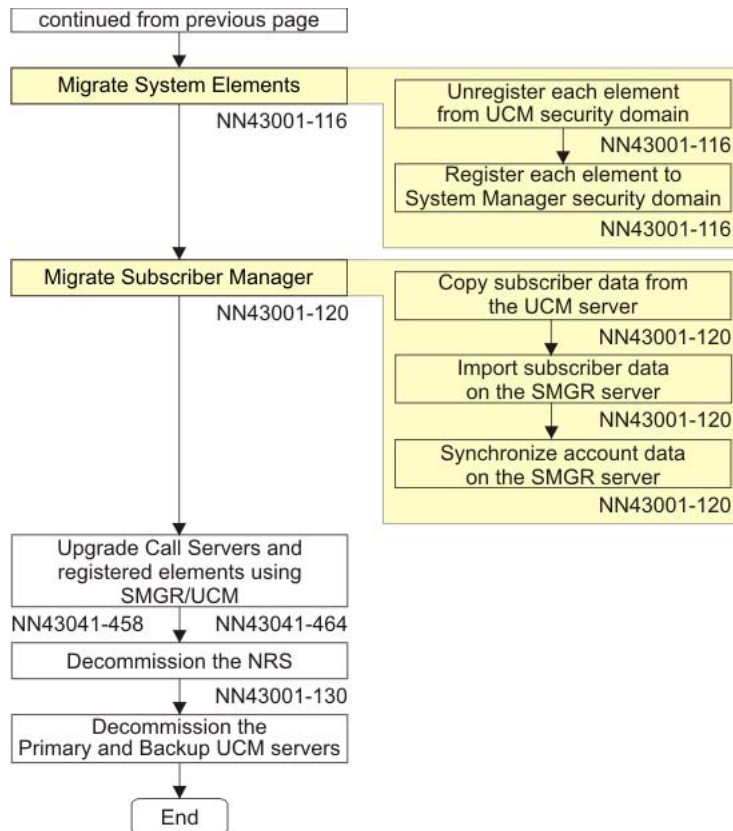


Figure 59: Migration option 2 (Part 3 of 4)



Avaya Aura Documentation
 Note #1: Installing and Upgrading Avaya Aura™ System Manager
 Note #2: Installing and Configuring Avaya Aura™ Session Manager

Figure 60: Migration option 2 (Part 4 of 4)

Configuring UCM to appear on System Manager

Use the following procedure to get UCM Services to appear on the System Manager home page.

1. In System Manager, navigate to **Services > Configurations**.
2. In the navigation tree, click **Settings > SMGR**, and click **Common Console**.
The Common Console screen appears.
3. Click **Edit**.
4. In the **ucm_configured** field, type `true`.
5. Click **Commit**.

6. Click **Done**.
7. Log off and Log on from System Manager for the UCM Services field to appear on the System Manager home page in the Services column, as shown in the following figure.

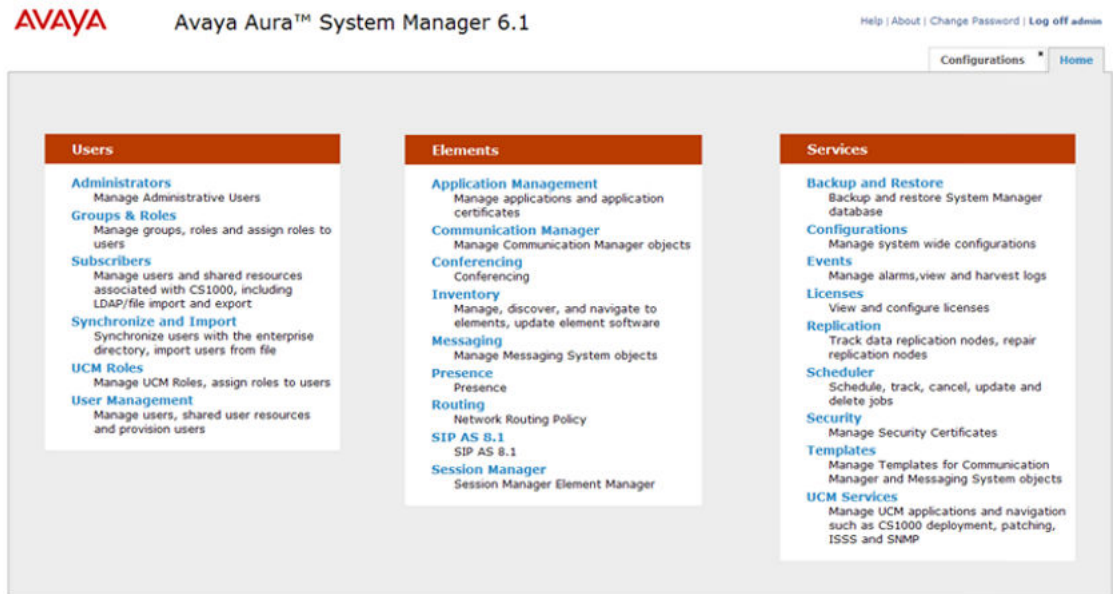


Figure 61: System Manager home page with UCM Services

System Elements migration task flow

The following task flow provides a high-level task flow to assist you with migrating system elements to the System Manager security domain.

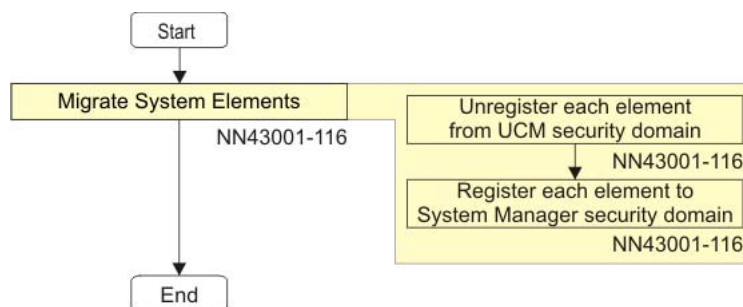


Figure 62: System Elements migration task flow

Registering CS 1000 UCM Linux members to System Manager

You can register the Communication Server 1000 UCM members on System Manager by logging on locally to each member server and running the member configuration wizard. Use the admin userid and admin password to log on to System Manager as defined during the initial System Manager installation.

1. Log on to the UCM member server by typing `https://<FQDN:port>/local-login`.
2. Type the local Linux Base userid and password and click **Log In**. For Release 7.5 systems, type admin2 as userid and for Release 7.0 systems, type nortel.
3. If the DNS server is already configured on your network, go to [Step 8](#) on page 160.

Click **Local Administration**.

4. Click **Networking > DNS and Hosts**.
5. In the Hosts section, click **Add**.
6. Type IP address and hostname of the System Manager.
7. Click **Logout**.

After you have registered the UCM member server, you must configure the UCM member server as a member of the System Manager.

8. Log on to the UCM member server again by typing `https://<FQDN:port>/local-login`.
9. Type the local Linux Base userid and password, and click **Log In**. For Release 7.5 systems, type admin2 as userid and for Release 7.0 systems, type nortel.
10. Click **Security Configuration**.
11. Configure the UCM member server as a member of the System Manager server as follows:
 - Validate that the Member FQDN validation is correct.
 - Validate that the Select server type is configured to be a member server.
 - Ensure the Enter server information reflect the FQDN or IP address of the System Manager active server.
12. Upon completion of the security configuration of the member, restart the server.
13. Verify that the CS 1000 member server is now a member server on System Manager as follows:
 - Log on to System Manager by typing `https://FQDN:port/network-login`.

- On the System Manager home page, click **UCM Services**.
- In the navigation tree, click **Network Elements**.
 - Ensure the System Manager server shows the CS 1000 member server on the Elements page.
 - Ensure the System Manager server shows the CS 1000 member Element Manager.

Registering VxWorks servers to SMGR

Register all VxWorks devices to System Manager (SMGR).

Prerequisites:

- Ensure your CS 1000 Media Gateway and Media card ELAN IP addresses can route to the SMGR IP address.
- You have identified the devices to migrate and have unregistered them. For example, STAT UCMSECURITY INFO and UNREGISTER UCMSECURITY SYSTEM.
- Change the SMGR Linux Base CLI admin password to match the SMGR GUI admin password. See [ChangeYourSMGRLinuxBaseCLIAdminPassword](#) on page 162.

Procedure steps:

1. For each Call Server you are registering to SMGR, log on as admin2 and do the following in LD 117:

- Type REGISTER UCMSECURITY CS

This command is for the Call Server, you must now register elements connected to that Call Server. The Call Server MUST register first.

Type REGISTER UCMSECURITY SYSTEM to register or reregister the Call Server and any associated Gateway Controllers or Voice Gateway Media Cards.

- For a Co-res CS, central authentication is turned on because registration is part of the Linux Base.
- This command works the same as the REGISTER UCMSECURITY SYSTEM command found in Release 6.0.

For additional commands, see [AddOrRemoveElementsFromTheUCMSecurityDomain](#) on page 167.

Note:

If the Communication Server 1000 UCM primary server has been demoted or redeployed, you must log on using the emergency account, for example, the admin account with the NetworkAdministrator role assigned.

2. At the prompt, type the IP address of the System Manager.
3. Type the user name you configured as your SMGR Linux Base CLI admin user name.
4. Type the password you configured as your SMGR Linux Base CLI admin password.

Changing your SMGR Linux Base CLI admin password

Avaya recommends that you change the SMGR Linux Base CLI admin password to match the SMGR GUI admin password.

1. Log on to System Manager using `admin` as the UCM User Name and password.
2. At the prompt, type `passwd` to change the password as defined during the initial SMGR installation.
3. At the prompt, type the `admin` password.
4. Type a new UNIX password when prompted.
5. Retype the new UNIX password when prompted.

A message appears indicating that all authentication tokens are updated successfully.

6. Continue to [Step 1](#) on page 161 for Registering VxWorks servers to SMGR.

Registering CS 1000 Primary security server and co-resident applications to System Manager

The Primary security server demotion feature is not supported. You must perform a new installation of co-resident applications on System Manager.

Software deployment

This section describes the software deployment changes from UCM to System Manager 6.2.

Linux Base system upgrade

The CS 1000 Linux Base image can be copied to the System Manager server from the client machine for system upgrades and NFS installation of member servers.

Uploading the CS 1000 Linux Base image to System Manager from the client machine

The Communication Server 1000 management applications cannot be deployed on a System Manager server; therefore, you must use Deployment Manager to deploy software on the member servers.

1. Log on to System Manager as a UCM administrator and navigate to **UCM Services > Software Deployment**.

2. On the **UCM Deployment Manager** page, click **Software Loads**.

The Software Loads screen appears.

3. In the **CS1000 Linuxbase image** section, click **Add**.

The Software Loads screen appears when the upload is complete.

4. In the **Upload CS1000 Linuxbase Image** section, browse to select the image to upload from the client machine, and click **Add image**.

Note:

The linuxbase .iso image is required.

For more information about Deployment Manager for deploying applications, see *Linux Platform Base and Applications Installation and Commissioning, NN43001–315*.

Deleting a CS 1000 Linux Base image from System Manager

Use the following procedure to delete a Communication Server 1000 Linux Base image from System Manager.

1. Log on to System Manager as an administrator and navigate to **UCM Services > Software Deployment**.

2. On the **UCM Deployment Manager** page, click **Software Loads**.

The Software Loads screen appears.

3. In the **CS1000 Linuxbase image** section, click **Delete**.

Adding a software load from the client machine

Software .nai files must be uploaded from the client machine. You can no longer upload from the Deployment Server using a USB Device or CD/DVD-ROM. Use the following procedure to upload .nai files from the client machine.

1. Log on to System Manager as an administrator and navigate to **UCM Services > Software Deployment**.

2. On the **UCM Deployment Manager** page, click **Software Loads**.

The Software Loads screen appears, as shown in the following figure.

3. In the Specify software load file section, click **Browse** to locate the software load on the client machine.

The Software Loads screen appears when the upload is complete.

4. Click **Add Load**.

The Software Loads screen appears when the upload is complete.

User management

In System Manager, you can create users as follows:

- Navigate to **Users > Administrators** to create and manage traditional UCM users. For more information, see [AdministrativeUsers](#) on page 97.
- Navigate to **Users > User Management** to create System Manager users. You can add UCM roles to these accounts.

Manually redefining deployment distributions and server groupings

You must manually redefine deployment distributions and server groupings.

1. Log on to SMGR as an administrator and navigate to **UCM Services > Software Deployment**.
2. Define new Linux servers. In the navigation tree, click **Deployment View** and select **Linux Server** from the list, and click **Add**.
3. On **Deployment View** page, choose **Network Services** from the View list.

4. Choose a Network Service, and click **Add**. Repeat this step for each Network Service you want to add. For example, MAS and SIP Trunk Bridge.

Note:

IM Presence and NRS are not supported.

5. Choose **CS1000 Systems** from the View list.
6. Choose one of the following, and click **Add**. Repeat this step for each CS 100 system.
 - CS1000
 - CS1000 HS
7. Define new VxWorks Call Servers. In **Deployment View**, choose **VxWorks Call Server** from the list, and click **Add**.

For more information about server groupings, see *Linux Platform Base and Applications Installation and Commissioning, NN43001–315*.

Additional information

The following sections provide additional information to assist with migrating the UCM primary server to System Manager.

VxWorks systems and devices

Note:

You need a CLI (telnet, rlogin or ssh) connection to use security domain registration commands.

VxWorks based systems and devices can join the Unified Communications Management security domain using the following modes:

- User mode (preferred)—the joining and leaving of the Unified Communications Management security domain operation is performed centrally from the Call Server, where the administrator confirms the list of devices to be added or removed:
 - LD 117 command: **[REGISTER / UNREGISTER] UCMSECURITY SYSTEM**
- Manual mode—the joining and leaving of the Unified Communications Management security domain operation is performed on each individual Call Server, Gateway Controller and Voice Media Gateway Card using the following commands:
 - LD 117 command: **[REGISTER / UNREGISTER] UCMSECURITY DEVICE**
 - OAM/PDT/IPL commands: **joinSecDomain** or **leaveSecDomain**

Before issuing the commands to register to the security domain, ensure that all elements are active and known to the Call Server. Also, when upgrading a pre-Release 6.0 Communication Server 1000 system to Release 6.0 or higher, ensure that secure transfer (sFTP) is disabled before transferring loadware and registering all MGCs, VGMCs and MCs to the Call Server. You can then enable sFTP after successfully registering these devices to the Call Server and before registering them to the security domain.

Note:

If `REG UCM SYS` is executed after upgrade and data files were preserved during the upgrade, there is a possibility that old files are stored in `/e/sdm` and therefore no prompt for UCM IP is given. In this case, command `REG UCM SYS FORCE` must be used. For more information, see [AddOrRemoveElementsFromTheUCMSecurityDomain](#) on page 167.

Adding elements to the security domain when ISSS is enabled

Before adding a non-Linux element (such as Media Card and Gateway Controller) to a security domain where ISSS is enabled, do the following:

- Add a new manual IPsec target with the IP address as the ELAN IP address of the non-Linux element. Ensure that the **Enable IPsec** check box is not selected.
- Synchronize and activate the IPsec configuration using Graceful mode.

Note:

If ISSS is enabled in FULL mode and is hardened, you must enable FTP as it is disabled on the Call Server and Signaling Server during the hardening process (sFTP is used by default). FTP is required for updating the loadware on the card, which enables it to register to the UCM security domain.

This process allows the non-Linux element to communicate with the Call Server or Element Manager without using IPsec so that any required updates can be applied to the element prior to registering with the security domain. The manual IPsec target is replaced with the correct automatic target when the element registers with UCM.

If you are replacing a non-Linux element (such as Media Card and Gateway Controller), instead of adding a new manual ISSS target you must disable IPsec for the appropriate automatic target in UCM. Do this as follows:

- Select the radio button beside the target being replaced and click **IPsec Not Required**.
- Synchronize and activate the IPsec configuration using Graceful mode.

To minimize the required steps during an upgrade or new installation, Avaya recommends that you register all (or most) elements before enabling ISSS.

Co-resident Call Server and Signaling Server systems

Co-resident systems can join the Unified Communications Management security domain using the following modes:

- User mode—the joining and leaving of the Unified Communications Management security domain operation is performed centrally from the Call Server, where the administrator confirms the list of devices to be added or removed:

- LD 117 command: **[REGISTER / UNREGISTER] UCMSECURITY SYSTEM**

This command can only be used to join the associated Gateway Controllers and Voice Gateway Media Cards to the security domain and not the Call Server itself. In the Co-resident Call Server and Signaling Server configuration, the Call Server is joined to the security domain with Linux base during installation.

Add or remove elements from the UCM security domain

Use the commands in [Table 15: Commands for adding or removing elements from the UCM security domain](#) on page 167 to add or remove elements from the Unified Communications Management security domain.

Before issuing the commands to join the security domain, ensure that all elements are active and known to the Call Server.

Table 15: Commands for adding or removing elements from the UCM security domain

Command	Type	Preconditions	Description
joinSecDomain	OAM/PDT CLI	<ul style="list-style-type: none"> • PWD2 privilege • UCM security IP address • Username and password for a UCM administrator whose UCM role includes the Security Administrator 	Establish mutual trust with the primary security server. Note: To use this command, you must first Telnet into the ELAN IP.
leaveSecDomain	OAM/PDT CLI	<ul style="list-style-type: none"> • PWD2 privilege • Member of UCM security domain 	Remove the primary security server mutual trust information from the device. Note: To use this command, you must first Telnet into the ELAN IP.

Command	Type	Preconditions	Description
statSecDomain	OAM/PDT CLI	<ul style="list-style-type: none"> • PWD2 privilege • Member of UCM security domain 	Display the primary security server IP address and fingerprint. Note: To use this command, you must first Telnet into the ELAN IP.
Register UCMSecurity CS	LD 117	<ul style="list-style-type: none"> • admin1 or admin2 privilege 	Establish mutual trust with the primary security server for the Call Server. If the Call Server is already registered, it reregisters.
Register UCMSecurity Device [<ip_address>]	LD 117	<ul style="list-style-type: none"> • admin1 or admin2 privilege • username and password for a UCM administrator whose UCM role includes the Security Administrator Linux base element 	Establish mutual trust with the primary security server for the element specified by <ip_address>, where <ip_address> is a VGMC or Gateway Controller registered to a Call Server belonging to the UCM security domain.
Register UCMSecurity System [Force]	LD 117	<ul style="list-style-type: none"> • admin1 or admin2 privilege • UCM security IP address • username and password for a UCM administrator whose UCM role includes the Security Administrator Linux Base element 	All associated elements, such as Gateway Controllers and VGMCs, join the UCM security domain after prompting for user approval. (If the system is a redundant system, the inactive Call Server joins the security domain automatically.) Use FORCE to request all elements to register to the primary security server. Elements that are already registered will reregister.

Command	Type	Preconditions	Description
Stat UCMSecurity info	LD 117	<ul style="list-style-type: none"> • An account with the NetworkAdministrator role assigned • Member of UCM security domain 	Display the primary security server IP address and fingerprint.
Stat UCMSecurity System [Refresh]	LD 117	<ul style="list-style-type: none"> • No privilege requirement • Member of UCM security domain 	Display all known CS 1000 elements (such as Gateway Controller, MC32, MC32S) and their current UCM security domain status as Registered or Unregistered. Use [Refresh] to refresh the list.
Unregister UCMSecurity CS	LD 117	<ul style="list-style-type: none"> • An account with the NetworkAdministrator role assigned 	Remove the mutual trust information from the primary security server for the Call Server.
Unregister UCMSecurity Device [<ip_address>]	LD 117	<ul style="list-style-type: none"> • An account with the NetworkAdministrator role assigned 	Remove the mutual trust information from the primary security server for the device specified by <ip_address>.
Unregister UCMSecurity System	LD 117	<ul style="list-style-type: none"> • An account with the NetworkAdministrator role assigned 	Remove the mutual trust information from the primary security server for the Call Server and all of its associated Gateway Controllers and VGMCs.

Note:

When using the OAM/PDT CLI, you must telnet to the ELAN IP to access security-related commands.

Note:

When you reboot Media Gateway devices after upgrade (except for MC32S), log messages dsLOG003 tAccountTransfer and LOG003 tBannerTransfer display due to the account database and banner file transfer failing while the device waits to register with the UCM security domain.

Note:

PWD2 is the pre-membership system password. It does not exist after the system joins the security domain.

Note:

If /e/keys/known_host or /e/keys/<IP address>.pub files exist prior to the upgrade from 5.5, it is not possible to join the security domain via executing the command, `reg ucm sys`. Perform the following steps to join the security domain:

1. Remove the pub files manually.
2. Execute the command `unreg ucm sys`.
3. Execute the command `reg ucm sys force`.

Appendix B: Certificate authorities

This appendix contains the information required to migrate your certificate authorities to System Manager 6.2 as required with migration Option 2.

Prerequisites:

- Identify elements where TLS is enabled
- Ensure that all elements are active and known to the Call Server.

The following figures shows the System Manager Home page.

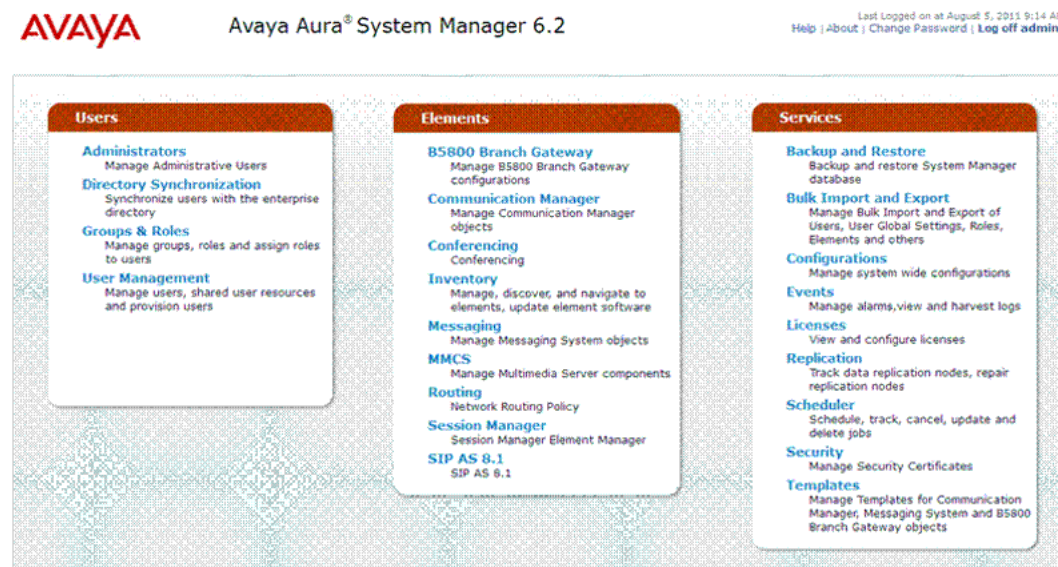


Figure 63: System Manager Home page

Table 16: High level checklist

Step	Task	Action	✓
1	Upgrade the Primary Security Server and member servers to Communication Server 1000 Release 6.0 and later.	For more information, see <i>Linux Platform Base and Application Installation and Commissioning</i> , NN43001–315.	
2	Migration option 1 only: If TLS is enabled, add the UCM primary certificate authority on Session Manager.	See Adding a UCM primary certificate authority on Session Manager on page 173.	
3	Migration option 1 only: Add a System Manager certificate authority on the UCM primary server.	See Retrieving the System Manager certificate authority on page 175.	

Step	Task	Action	✓
4	Migrate System elements using LD 117: <ul style="list-style-type: none"> • Get the status of the elements you want to move from UCM to System Manager. • Unregister all elements from the UCM security domain. • Register all elements to the new System Manager security domain. 	LD 117: <ul style="list-style-type: none"> • STAT UCMSECURITY INFO • UNREGISTER UCMSECURITY DEVICE • REGISTER UCMSECURITY DEVICE For additional commands, see Registering VxWorks servers to SMGR on page 161.	

Navigation

- [TLS certificate authorities on Session Manager and Primary UCM](#) on page 172
- [TLS certificate authorities for One-X Communicator](#) on page 179

For more information about the installation and administration of Session Manager and System Manager, see the following documents at <https://support.avaya.com/css/appmanager/css/support>:

- *Installing and Upgrading Avaya Aura® System Manager*
- *Administering Avaya Aura® System Manager*
- *Avaya Aura® Session Manager Overview*
- *Installing and Configuring Avaya Aura® Session Manager*
- *Administering Avaya Aura® Session Manager*

TLS certificate authorities on Session Manager and Primary UCM

This section provides a high level task flow and the procedures to add a UCM primary certificate authority on System Manager, a System Manager certificate authority on the UCM primary server when TLS is enabled, and to add a TLS certificate authority on Session Manager with UCM on System Manager.

TLS certificate authorities task flow

The following task flow provides a high-level task flow to assist you with managing the certificate authorities on Session Manager and the UCM primary server.

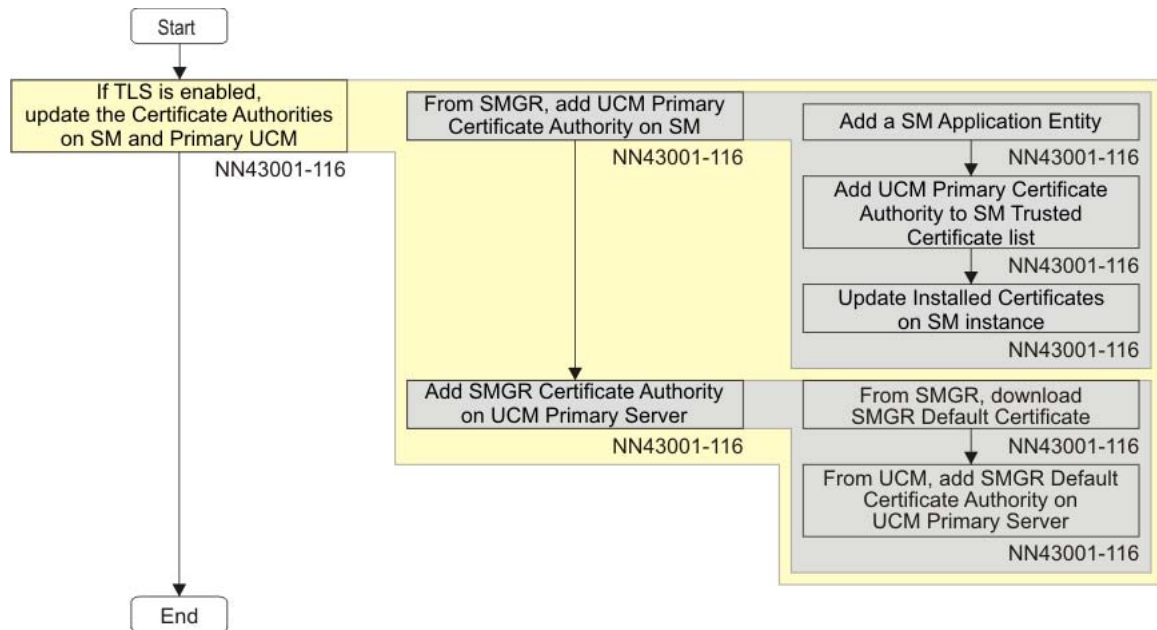


Figure 64: TLS certificate task flow

Adding a UCM primary certificate authority on Session Manager

Use the following procedure to add a UCM primary certificate authority on Session Manager when TLS is enabled.

1. In System Manager, navigate to **Elements > Inventory**.
The Inventory page appears.
2. In the navigation tree, click **Manage Elements**.
3. Click **New** to create a new Session Manager Application entity.
4. From the **Type** list, choose **Session Manager**.
The screen refreshes to show additional fields.
5. In the Application section, configure the following fields:
 - **Name**: type the name of the instance.
 - **Description**: type a brief description about the instance.

- **Note:** the node on which the application runs. Type the Management Access Point IP address.
6. In the **Access Point** section, click the button beside the pre-populated Access Point in the table, and click **Edit**.
 7. In the Access Point Details section, configure the following fields:
 - **Name:** type the name of the access point.
 - **Host:** the name of the host on which the application instance is running. Type the Management Access Point IP address.
 - **URI:** type a value.
- Note:**
Do not make any changes to the other fields.
8. Click **Save**.
 9. Click **Commit** to add the application entity.

Adding a UCM primary certificate authority to a Session Manager trusted certificate list

Use the following procedure to add a Communication Server 1000 UCM primary certificate authority to a Session Manager trusted certificate list.

1. In System Manager, navigate to **Elements > Inventory**.
The Inventory page appears.
2. In the navigation tree, click **Manage Elements**.
3. In the Entities section, select a Session Manager Application from the table for the required Session Manager instance.
4. From the **More Actions** menu, choose **Configure Trusted Certificates**.
The certificates that are currently installed on Session Manager appear.
5. Click **Add** to add a UCM Primary certificate.
6. Choose **All** for the Select Store Type to add the trusted certificate.
7. Import the certificate using one of four methods:
 - Import from existing
 - Import from file
 - Import as PEM Certificate
 - Import using TLS
8. Click **Browse** to select a file.

9. Click **Retrieve Certificate** and review the certificate details before you continue.
10. Click **Commit** to add the trusted certificate.

For more information about certificate management, see *Security Management Fundamentals, NN43001–604*.

Updating installed certificates

Use the following procedure to update installed certificates.

1. In System Manager, navigate to **Elements > Session Manager > System Status**.

The System Status page appears.

2. In the navigation tree, click **Security Module Status**.
3. In the Entities section, select a Session Manager Application from the table for the Session Manager instance you require.
4. Click **Update Installed Certificates** to update the imported UCM certificates.
5. Click **Confirm** to confirm the selected Session Manager.

System Manager certificate authorities on the UCM primary server

The following procedures describe retrieving the System Manager certificate authority from UCM and adding the System Manager default certificate on the UCM primary server.

Retrieving the System Manager certificate authority

Use the following procedure to retrieve the System Manager certificate authority from UCM.

1. In System Manager, navigate to **Services > Security**.
The Security page appears.
2. In the navigation tree, click **Certificates > Authority**.
The CA Functions page appears.
3. Click **Download pem file** and **Save** the certificate to a file.

Adding the System Manager default certificate

Use the following procedure to add the System Manager default certificate on the UCM primary server.

1. In the UCM navigation tree, click **Security > Certificates**.
2. In the Certificate Authorities section, click **Add**.
3. Type a unique **Friendly Name** in the **Add a CA to the Service** window.
4. Copy the content of the certificate authority X.509 certificate and paste into the text area provided.

Note:

Make sure that the certificate content is encoded in Base-64 format including the Begin Certificate and End Certificate lines.

5. Click **Submit** to install the CA on the server.
6. Log off and log on to UCM for the change to take effect.

For more information about certificate management for CS 1000, see *Security Management Fundamentals*, NN43001–604.

Adding a TLS certificate authority on Session Manager with UCM on System Manager

Use the following procedure to add a TLS certificate authority to Session Manager when the Unified Communication Manager (UCM) is part of System Manager. Configure the SIP TLS trunk from the CS 1000 SIP Gateway to Session Manager.

Note:

Avaya recommends using a third party certificate. To use the third party certificate, you must remove the limited Linux patch (if installed) and then upgrade to Session Manager 6.1 SP1.

If you do not upgrade to System Manager 6.1 SP1 as recommended in the preceding paragraph, you must install the limited Linux patch and use the default Avaya SIP CA. For more information about CS 1000 Linux patching, see *Patching Fundamentals*, NN43001–407.

1. In System Manager, navigate to **Services > UCM Services**.
2. From UCM navigation tree, click **Security > Certificates**.
3. Click the **Certificate Endpoints** tab.
4. In the **Certificate Endpoints** section, click the option next to the SIP Signaling Gateway endpoint.
5. In the **Endpoint Details** section, under **Certificates**, click **SIP TLS**.
6. Click the option **Create a new certificate, signed by local private Certificate Authority** to assign a certificate to your server, and click **Next**.
7. Type values for **Friendly Name** and **Bit length**, and click **Next**.

For example:

- Friendly name: Type a string that identifies the SIP TLS certificate.
- Bit Length: Type a value that represents the number of bits used for encryption. Values can be 512, 1024, and 2048. More CPU is required for processing as the bit value increases.

8. Type the **Organization** and **Organization Unit**, and click **Next**.

For example:

- Organization: Your company name.
- Organization unit: A division within your company.

9. Type a value for **Common Name**. For example, type the Fully Qualified Domain Name (FQDN) of the CS 1000 SIP Signaling Gateway you are configuring. The default is a combination of the Windows environment variables Computername and Userdnsdomain. Ensure this field matches the hostname of the system the certificate is on.
10. In the **Subject Alt Name** field, choose **None** from the list.

Note:

If SIP Line is enabled on the CS 1000 server and One-X Communicator is used, you must choose **Other** from the list, and type `critical,DNS:domain name`, where *domain name* is the domain name of the SIP Line Gateway.

11. Complete the fields for **Country/Region**, **State/Province**, and **City/Locality**, and click **Next**.

For example:

- In the Country/Region field, type the country or region of where the server you are configuring is located.
- In the State/Province field, type the state or province.
- In the City/Locality field, type the city or locality.

The Certificate Request Summary window appears.

12. Click **Commit** to generate a certificate in the X.509 format.

The Certificate summary window appears with the certificate information.

13. Click **Finish**.

The status changes to signed.

14. Restart the server that you changed in this procedure.

The changes take effect only after the server restarts.

15. Log on to Element Manager to configure the TLS Security policy for the SIP Gateway.

- a. Click **System > IP Network > Nodes: Servers, Media Cards**.

The IP Telephony Nodes page appears.

- b. Click the Node ID to view the node properties.

The Node Details page appears.

- c. Under Applications, click **Gateway (SIPGw)**.

The Virtual Trunk Gateway Configuration Details page appears.

- d. In the **SIP Gateway Settings** section, select a security policy from the **TLS Security** list menu. The options are as follows:

- Security Disabled
- Best effort
- Secure Local
- Secure End to End

- e. In the **Port** field, type a value, for example, 5061 is typically used.

- f. Optionally, select the **Client Authentication** check box to enable Client Authentication.

OR

Select the **X509 certificate authority** check box to enable X.509 certificate authentication.

Important:

If you select X.509 certificate authority, you cannot use self-signed certificates with SIP TLS.

- g. In the **Proxy Or Redirect Server** section, under **Proxy Server Route 1**, in the **Primary TLAN IP Address** field, type the IP address of the Session Manager Security Module.

- h. In the **Port** field, type 5061.

- i. In the **Transport Protocol** field, select **TLS** from the list.

- j. Click **Save**.

The following warning appears: Please reboot the following Signaling Server after the save and transfer is done:
<list of SIP enabled Signaling Servers IPs>.

- k. Click **OK**.

For more information about certificate management for CS 1000, see *Security Management Fundamentals, NN43001–604*.

16. On Session Manager, create or modify the SIP entity link for CS 1000 to use TLS port 5061.
17. Log on to UCM and download the UCM Private Certificate Authority to your PC.
 - a. In the UCM navigation tree, click **Security > Certificates**.
The Certificate Management Web page appears.
 - b. Click the **Private Certificate Authority** tab.
The Private Certificate Authority page displays.
 - c. Click **Download**.
 - d. Click **Save** to save the ca.cer file to your PC.
18. Add the UCM ca.cer file as a trusted certificate for Session Manager.
 - a. In System Manager, navigate to **Elements > Inventory**.
 - b. In the navigation tree, click **Manage Elements**.
 - c. In the Entities section, select a Session Manager Application from the table for the required Session Manager instance.
 - d. From the **More Actions** menu, choose **Configure Trusted Certificates**.
 - e. Click **Add** to add a UCM Primary certificate.
 - f. Choose **Import from file**.
 - g. Click **Browse** to select the ca.cer file on your PC.
 - h. Click **Retrieve Certificate** and review the certificate details before you continue.
 - i. Click **Commit** to add the trusted certificate.
19. Update the Session Manager Security Module by following the procedure at [Updating installed certificates](#) on page 175.

TLS certificate authorities for One-X Communicator

This section provides the procedures to install certificate authorities for the One-X Communicator when registering to the SIP Line Gateway (SLG) over TLS.

Adding a UCM primary certificate authority for the One-X Communicator

Use the following procedure to add a UCM primary certificate authority on the PC where the One-X Communicator is installed.

1. In System Manager, navigate to **Services > UCM Services**.
2. From UCM navigation tree, click **Security > Certificates**.
3. Click the **Private Certificate Authority** tab.

The private Certificate Authority window appears.

4. In the Private Certificate Authority Details section, click **Download** to download the certificate contents as a security certificate file to the PC.

The File Download – Security Warning window appears.

5. Click **Save**.

The Certificate Details window appears showing the details of the certificate.

6. Click **Ok**.

7. After the UCM certificate is saved to the One-X client PC, open the certificate file and follow the instructions for installation to your Windows PC.

Adding a One-X Communicator root CA to UCM

Use the following procedure to add the One-X Communicator root CA to UCM.

1. In System Manager, navigate to **Services > UCM Services**.
2. From UCM navigation tree, click **Security > Certificates**.
3. Click the **Certificate Endpoints** tab.

The private Certificate Endpoints window appears.

4. In the Certificate Endpoints section, click the option next to the SIP Line Gateway (SLG) node.
5. In the Certificate Authorities section, click **Add**.
6. Copy the One-X Communicator root CA contents and paste into the text area.
7. Click **Submit**.

Adding a certificate for SIP TLS

Use the following procedure to create a certificate for SIP TLS.

1. From the UCM navigation tree, click **Security > Certificates**.
2. Click the **Certificate Endpoints** tab.
3. In the Certificate Endpoints section, click the option next to the SLG node you want to configure.
4. Click **SIP TLS**.
5. Click **Create a new certificate**, and click **Next**.
6. Type values for **Friendly name** and **Bit Length**, and click **Next**.

For example:

- **Friendly name:** Type a string that would be used to identify the certificate, for example, SIP TLS.
- **Bit Length:** Type a value that represents the number of bits used for encryption. Values can be 512, 1024, and 2048. More CPU is required for processing as the bit value increases.

7. Type the **Organization** and **Organization unit**, and click **Next**.

For example:

- **Organization:** Your company name.
- **Organization unit:** A division within your company.

8. Type a value for **Common Name**. For example, type the FQDN of the server you are configuring. The default is a combination of Windows environment variables Computername and Userdnsdomain. Ensure this field matches the hostname of the system the certificate is on.
9. In the **Subject Alt Name** field, choose **Other**, and type `critical,DNS:<domain name>`.

The domain name is the domain name on the SIP Line Gateway.

Index

A

Access Control Lists (ACL)	53
Access control policies	53
Access to installed elements in UCM	25
Accounts	48
Active Sessions	134
Add a CallPilot Messaging element	87
Add a Hyperlink	85
Add a new external user	98
Add a new local user	98
Add a new role	114 , 119
Adding a CallPilot certificate	133
Administrative Users	97
Assign an element alias	83
Assign new role mapping	120
Edit existing role mapping	120
Authentication	47
Authentication scheme policy	104
Authentication Servers Web page	107

B

Backup security server	42
Built-in account	49
Built-in roles	55

C

Central logon	50
Certificate management	40
Change a local account password	110
Change the UCM default password	72
Configure logs for forwarding to third party OSS	139
Configure the properties of a local user	102
Copy all user assignments from role	121
Custom roles	58

D

Data	142
Data Tool	31
Delete a user	104
Delete custom roles	123
Delete selected elements	93
Domain Name System	44

E

Edit a group	81
Edit a role description	122
Edit element properties	88
Edit local account password policies	124
Edit logs for forwarding to third-party OSS	139
Edit the authentication scheme	105
Edit the full name for a local user account	102
Edit the login warning banner	128
Edit the properties for a CS 1000 element	89
Edit the properties for a hyperlink element	88
Edit the properties for a Linux base element	91
Edit the properties for a Network Routing Service element	92
Edit the properties of a CallPilot messaging element	92
Edit the Single Sign-on Cookie Domain	129
Edit the tree view	80
Edit user role mapping	100
Enable or disable a user account	103
Export logs using csv	142
External account	50
External authentication	104

H

High availability configuration	44
---------------------------------------	--------------------

I

Identity management	48
Inactive session termination	53
Instance Level Access Control (ILAC)	53
IPsec	94

L

Local account	48
Log off options in UCM	75
Log on in network logon mode (IP address)	73
Log on using the central logon page (FQDN)	72
Login warning banner	53
Logs	31 , 137

M	
Manage elements	77
Manage elements using table view	84
Manage elements using the edit navigation tree	77
Add elements	77
Add groups	77
Member server	43
Migration from UCM to System Manager	143
Migration of Certificate Authorities to System Manager	171
P	
Password	109
Password aging policy	51
Password guessing prevention policy	52
Password history policy	52
Password Policy Web page	124
Password strength policy	52
Permission mapping	119
See also Add a new role	
Policies	123
Policies Web page	123
Primary security server	42
Provision the Kerberos Server	109
Provision the LDAP Server	107
Provision the Radius Server	108
R	
Removing an element alias	83
Removing items using the edit navigation tree	82
Reset the password for a local user account	102
Review existing roles	114
Review existing user	97
Review security policies	123
Review the status of a local account password	109
Role Based Access Control (RBAC)	53
Roles	113
S	
Secure Shell Trust (SSH)	40
Security domain	38
Security policies	50
Security Services overview	47
Start a managed element using table view	84
T	
Terminate SSO sessions	135
U	
UCM benefits and features	37
Unified Communications Management client capacity	36
V	
View active sessions	135
View audit log using the search functionality	141
View audit logs by date	141
Viewing details of a certificate endpoint	130
Viewing log types	138
W	
Web SSL	40