Avaya Visualization Performance and Fault Manager — Using Unified Communications Management to Manage the Converged Voice and Data Network

2.3
NN48014-501
01.05
June 2011

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 Web sites 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 Web site: 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.

Licenses

Copyright

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Product (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

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 Web site: http://support.avaya.com.

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your Product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://support.avaya.com.

Contents

Chapter 1: 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 5
- Getting product training on page 5
- Getting help from a distributor or reseller on page 5
- Getting technical support from the Avaya Web site on page 6

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, you can access the Web site at www.avaya.com/support. From this Web site, you can locate the Training contacts 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 2: Introduction

The Avaya Unified Communications Management (Avaya UCM) portfolio provides comprehensive management capabilities for key products in the Avaya Enterprise portfolio, and simplifies functionality associated with managing subscribers, faults, configuration, performance and security. Through features like single sign-on, common look and feel, information sharing, heterogeneous network support, and consistent user interfaces, Avaya UCM provides decreased complexity, lowered capital and operational expenses, improved workflows, reduced error potential, and quicker time-to-resolution.

Key management products that have adopted the Avaya UCM solution model include data products and voice products.

Data products supported on Avaya UCM include the following:

- Avaya Visualization Performance and Fault Manager (Avaya VPFM) version 2.3
- Network Resource Manager (NRM) version 2.1
- Enterprise Policy Manager (EPM) version 5.1
- IP Flow Manager (IPFM) version 2.0

Voice products supported on Avaya UCM include the following:

- Avaya Communication Server 1000 (Avaya CS 1000) Release 6.0 and Release 7.0 system management applications (such as, Business Element Manager, Deployment Manager, NRS Manager)
- Subscriber Manager Release 2.0

Upon initial release of the above mentioned products, full integration/co-residency of Voice management products with Data management products (that is, within a single UCM security infrastructure), was not immediately supported, as full solution verification had not yet been complete. However, final solution-level verification of UCM-based voice management applications (CS 1000 Release 6.0 and Release 7.0 applications and Subscriber Manager 2.0) and data management applications (EPM 5.1, VPFM 2.3, IPFM 2.0, and NRM 2.1) have now been completed. This guide provides key information required to unify these voice and data management applications within a single UCM deployment.

Note:

The terms Data product and Voice product are used in this document to identify a group of system and network management applications that are most closely associated to Avaya's Enterprise Data and Enterprise Voice product portfolios respectively. Applications such as Avaya VPFM and Subscriber Manager have been developed to provide more general functionality, and the usefulness of these products and applications spans more than just one Avaya portfolio area. Avaya retains the Voice and Data distinction primarily because, until now, these applications could not coexist in a single management domain, and it remains a convenient nomenclature in a discussion about Avaya UCM solution convergence. The distinction between Data and Voice management becomes increasingly less meaningful as Avaya's system and network management products become increasingly integrated.

Chapter 3: Deploy a converged data and voice Avaya UCM infrastructure

The following topics are covered in this chapter.

Before deploying a converged Data and Voice Avaya UCM solution

Before you proceed with deployment of a converged data and voice Avaya UCM deployment, you must first be very familiar with UCM, including the concept of Primary, Backup, and Member UCM Servers, and the process of deploying individual UCM-based applications.

You must be very familiar with the following documentation:

- Avaya UCM documentation for Voice Network Management. For more information, see *Avaya Call Server 1000 Unified Communications Management Common Services Fundamentals* (NN43001–116), Release 7, Document Revision 04.01.
- Avaya CS 1000 Linux Base documentation for Voice Network Management. For more information, see *Avaya Communication Server 1000 Linux Platform Base and Applications Installation and Commissioning* (NN43001–315), Release 7, Document Revision 04.01.
- Avaya UCM documentation for Data Network Management. For more information, see *Avaya Unified Communications Management Common Services Fundamentals* (NN48014–100), Release 2.0, Document Revision 02.01.

You can obtain the latest version of these documents from the Avaya Technical Support portal: www.avaya.com/support.

Converged data and voice Avaya UCM deployments supported scenarios

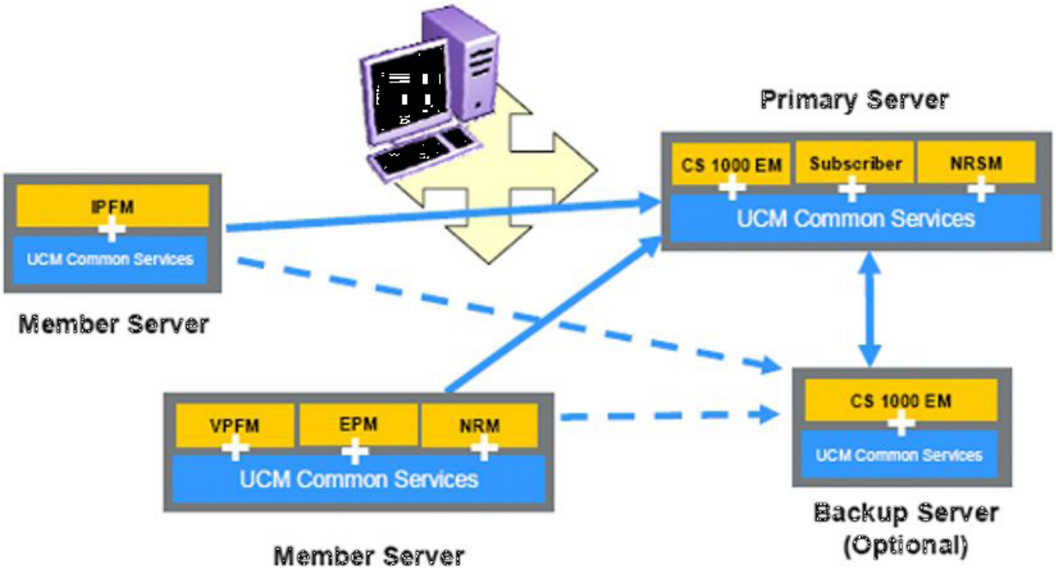
Avaya extends support to a number of Avaya UCM deployment scenarios that span both voice and data management products. All supported scenarios require the use of an Avaya CS 1000-based system as the UCM Primary security server.

The use of an Avaya UCM Backup security server is an optional piece of the security domain and is deployed to provide redundancy for the authentication and authorization service. The Backup security server role can be held by either a CS 1000-based system, such as a Voice system, or on a server hosting one or more of the Data management applications. You can join any combination of Member servers, such as Voice and Data, to the security domain lead by a CS 1000 primary.

For more information about the security domain, the types of UCM servers that can participate in the domain (Primary, Backup, and Member), and engineering recommendations and limitations, see *Avaya Call Server 1000 Unified Communications Management Common Services Fundamentals* (NN43001-116).

Avaya CS 1000 is deployed as Avaya UCM Primary and Backup UCM servers

The following figure outlines a typical Avaya UCM security domain topology when a Primary and a Secondary server are both hosted on Avaya CS 1000 (Voice) systems.



The following table outlines the typical deployment scenario described in the preceding figure.

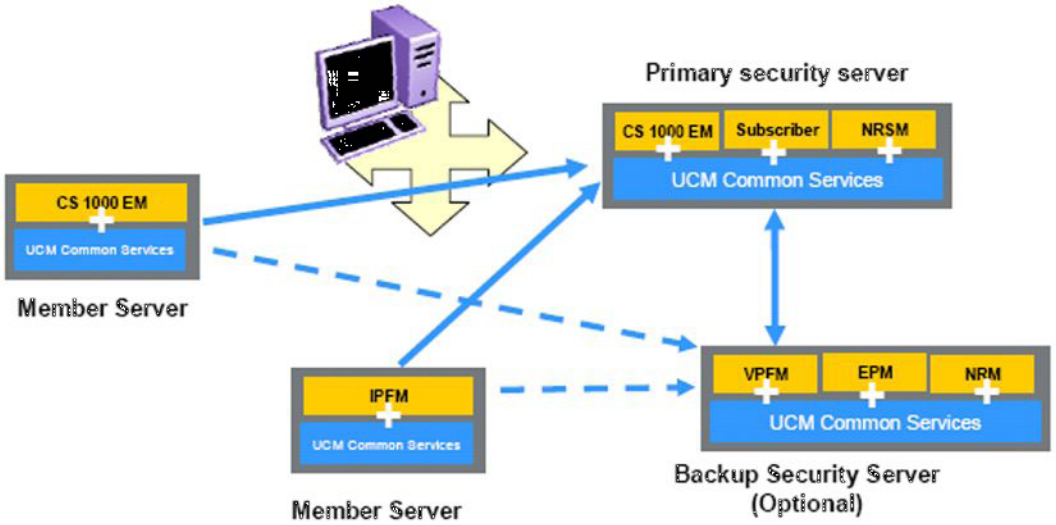
Primary	Backup	Each Member
CS 1000	CS 1000	(VPFM and/or EPM and/or NRM and/or IPFM) or CS 1000)

The following list outlines characteristics of a typical deployment of Avaya CS 1000 as a Primary server and Backup server.

- The Backup server is optional, and is deployed to provide authentication and authorization redundancy in the event that Primary is failed and unreachable.
- CS 1000 is any valid combination of CS 1000-based system management applications, including Subscriber Manager.
- CS 1000 is only supported in RHEL 5.2.
- VPFM/EPM/NRM/IPFM is supported in RHEL 5.2, Windows 2003 Server, and Windows 2008 Server.
- VPFM, EPM, and NRM can be co-resident within a single server acting as a member.
- Due to resources requirements, Avaya strongly recommends to not install IPFM co-resident with the other data products.

Avaya CS 1000 is deployed as a Primary server and one of data network management products is deployed as a Backup server

The following figure outlines a typical Avaya UCM security domain topology when a Primary server is hosted on a Voice system and the Backup server is hosted on a Data system; that is, a server hosting one or more data-focused management applications.



The following table outlines the typical deployment scenario described in the preceding figure

Primary	Backup	Each Member
CS 1000	VPFM and/or EPM and/or NRM and/or IPFM	(VPFM and/or EPM and/or NRM and/or IPFM) or CS 1000

The following list outlines characteristics of a typical deployment of Avaya CS 1000 as a Primary server and Data Server as a Backup server.

- The Backup server is optional, and is deployed to provide authentication and authorization redundancy in the event that Primary is failed or unreachable.
- All data network management products must have the same OS to work with each other in the same security domain.
- CS 1000 is any valid combination of CS 1000-based system management applications, including Subscriber Manager.
- CS 1000 is only supported in RHEL 5.2.
- VPFM/EPM/NRM/IPFM is supported in RHEL 5.2, Windows 2003 Server, and Windows 2008 Server.
- VPFM, EPM, and NRM can be co-resident within a single server acting as a member or as a backup.
- Due to resources requirements, Avaya strongly recommends to not install IPFM co-resident with the other data products.

Browser support

In a converged data and voice Avaya UCM deployment, only Internet Explorer 7 and 8 is supported across all the products.

Integration workflows

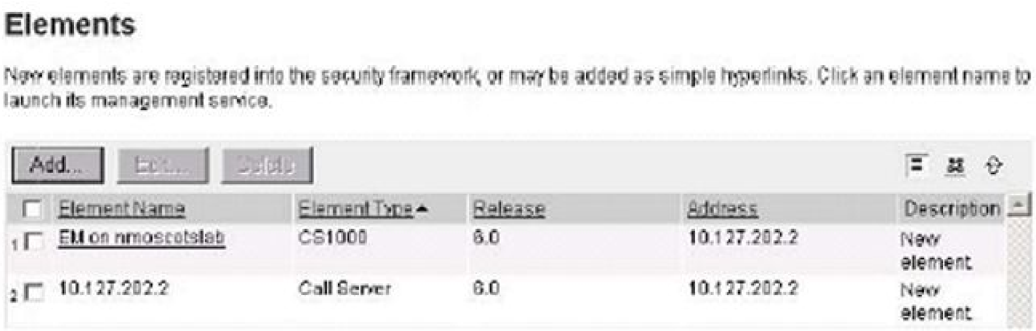
The following workflows are applicable only when there is already an Avaya CS 1000-based Primary server deployed in the network. For more information about installation and deployment of an Avaya UCM security domain lead by a CS 1000-based Primary server, which may or may not include CS 1000-based Secondary and Member servers, see *Avaya Call Server 1000 Unified Communications Management Common Services Fundamentals* (NN43001-116).

- Joining a new data product (VPFM/EPM/NRM/IPFM) member server to an Avaya CS 1000 based primary server on page 13
- Demoting an existing data product primary server to a member server on page 20
- Demoting an existing data product backup server to a member server on page 20
- Promoting an existing data product member server to a backup server on page 23
- Assigning voice and data products related roles and permissions to a single user on page 25

Joining a new data product (VPFM/EPM/NRM/IPFM) member server to an Avaya CS 1000 based primary server

This workflow applies when Avaya CS 1000 (a combination of CS 1000 EM, NRSM, and Subscriber Manager) is the first product installed and is configured as a primary server. If a data product (VPFM/EPM/NRM/IPFM) is already installed as a primary server or a backup server in a separate security domain, the data product must be uninstalled first before joining the CS 1000 security domain.

The following figure is an example of the Avaya CS 1000 installed as a primary server.



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.

☐	Element Name	Element Type ▲	Release	Address	Description
1 ☐	EM on nmoscotslab	CS1000	6.0	10.127.202.2	New element
2 ☐	10.127.202.2	Call Server	6.0	10.127.202.2	New element

Prerequisites

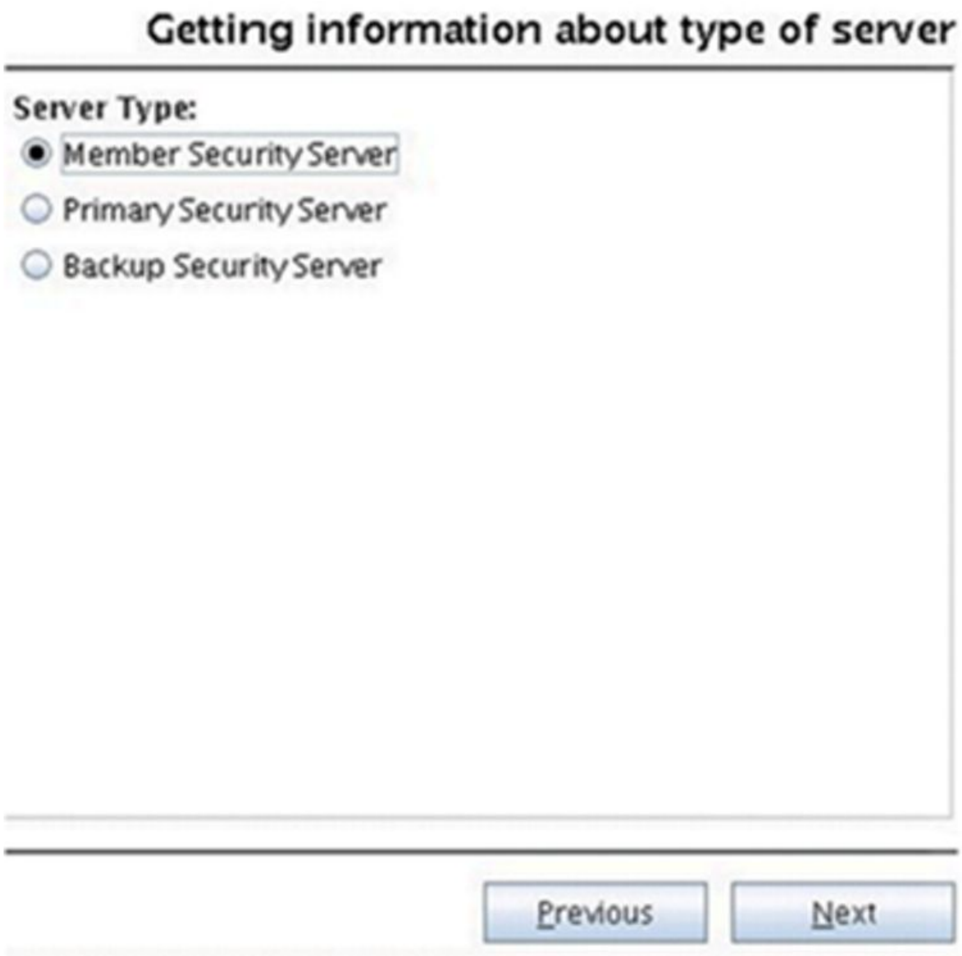
Avaya CS 1000 must be the first product installed and configured as a primary server.

To install a data network management product, perform the following procedure.

1. Configure the server type.

   You can install data network management products as either a member or a backup.

   The following figure is an example of a data network management product installed as a member.



Getting information about type of server

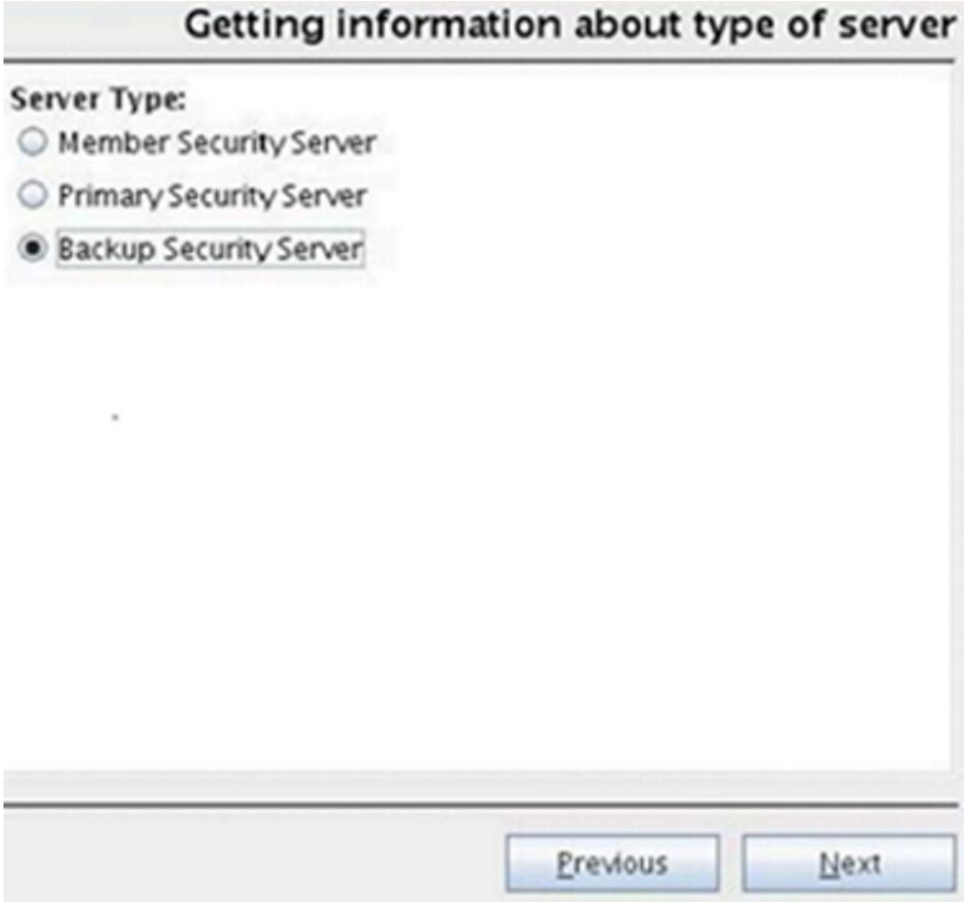
Server Type:

● Member Security Server

○ Primary Security Server

○ Backup Security Server

The following figure is an example of a data network management product installed as a backup.



Getting information about type of server

Server Type:

○ Member Security Server

○ Primary Security Server

● Backup Security Server

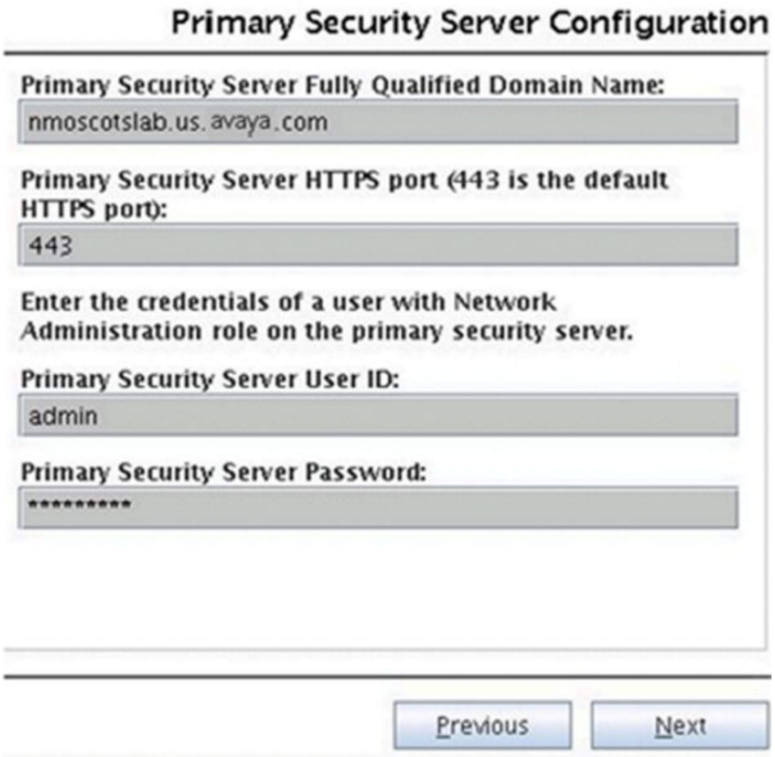
Note:

If another CS 1000 product is already deployed as a backup server, the data network management products are only installed as members.

2. Configure the primary server information.

   Enter the CS 1000 primary server FQDN, HTTPS port number, admin user ID and password.

   The following figure is an example of a Primary Security Server Configuration screen.



Primary Security Server Configuration

Primary Security Server Fully Qualified Domain Name:

nmoscotslab.us.avaya.com

Primary Security Server HTTPS port (443 is the default HTTPS port):

443

Enter the credentials of a user with Network Administration role on the primary security server.

Primary Security Server User ID:

admin

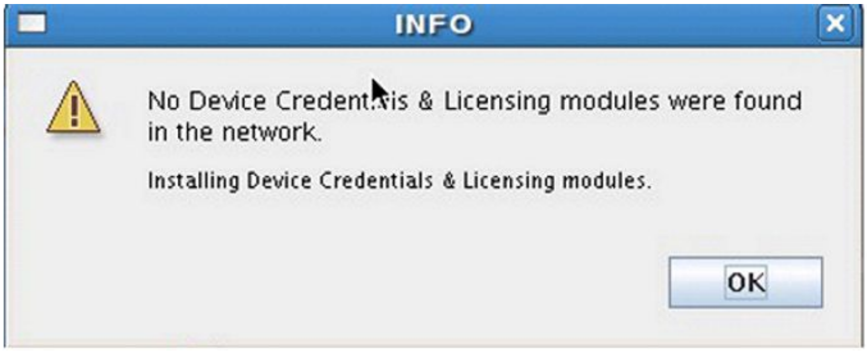
Primary Security Server Password:

****

3. Install device credentials and licensing modules.

   After the first data network management product is deployed in the CS 1000 security domain, device credentials and licensing modules are installed. If the device credentials and licensing modules cannot be found, a dialog box appears prompting you to install them.

   The following screen appears if the device credentials and licensing modules are not detected in the security domain.



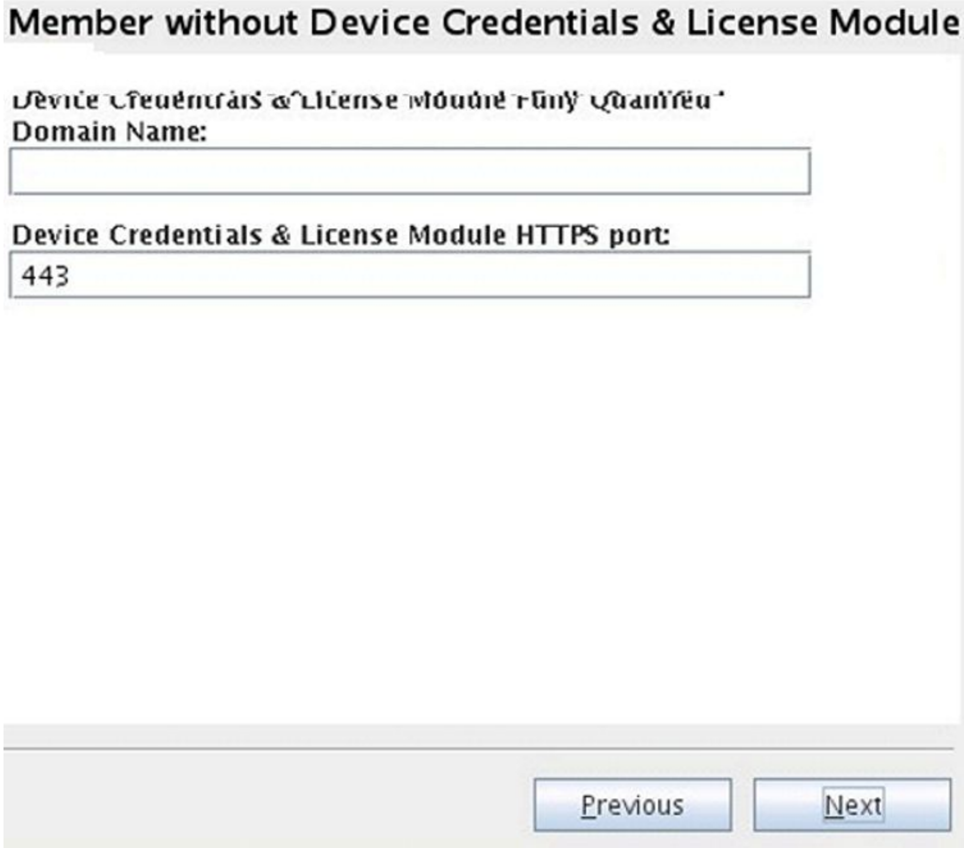
INFO

No Device Credentials & Licensing modules were found in the network.

Installing Device Credentials & Licensing modules.

   If the device credentials and licensing modules are detected, the installer prompts you for the FQDN and HTTPS port number of the server where the device credentials and licensing modules reside.

   The following screen appears prompting you to configure the FQDN and HTTPS port number for device credentials and license module.



Member without Device Credentials & License Module

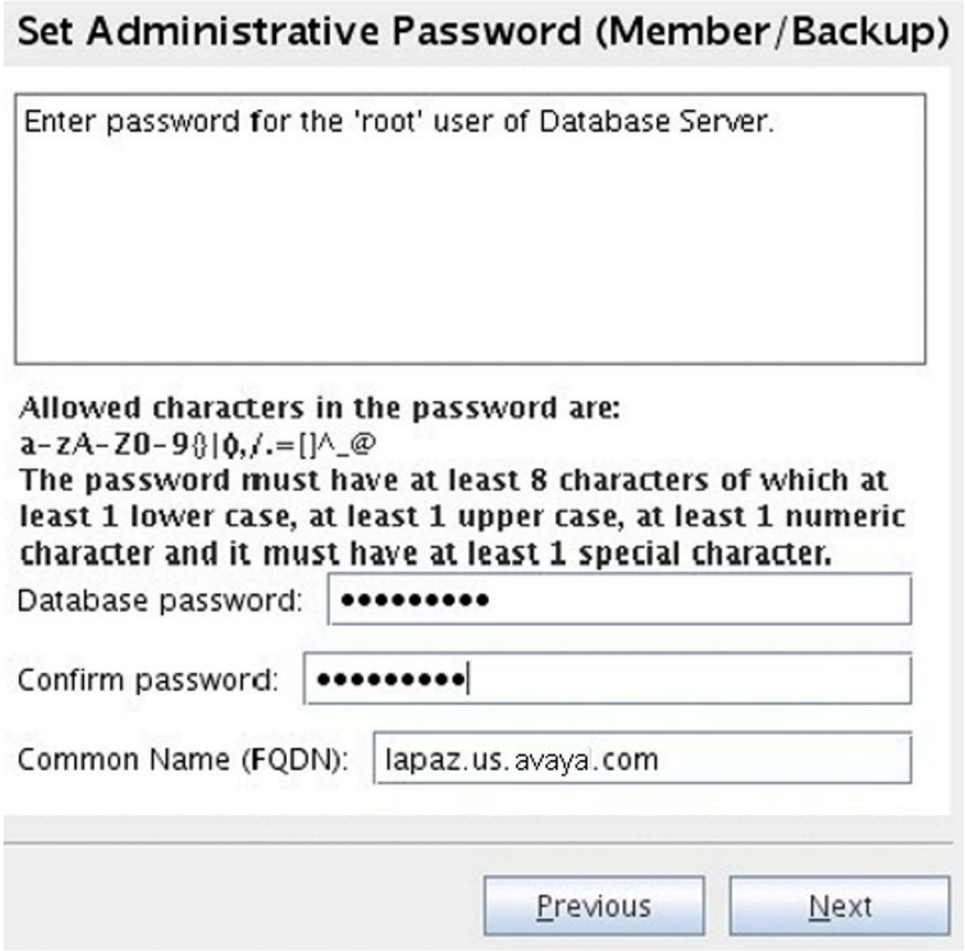
Device Credentials & License Module Fully Qualified Domain Name:

Device Credentials & License Module HTTPS port: 443

4. Set administrative password.

   Configure the server database password and UCM admin password.

   The following figure is an example of the Set Administrative Password (Member/Backup) screen.



Set Administrative Password (Member/Backup)

Enter password for the 'root' user of Database Server.

Allowed characters in the password are:
a-zA-Z0-9{}|(),/.=[]^_@
The password must have at least 8 characters of which at least 1 lower case, at least 1 upper case, at least 1 numeric character and it must have at least 1 special character.

Database password: ●●●●●●●●●

Confirm password: ●●●●●●●●●

Common Name (FQDN): lapaz.us.avaya.com

Note:

After installing each application, launch UCM and ensure the related launch points are added to UCM navigator before installing another application.

Next steps

After upgrading to Avaya Visualization Performance and Fault Manager (Avaya VPFM) 2.3, in a distributed environment you must restart all servers (primary, backup, member) in the following order:

1. Primary
2. Backup
3. Member

Demoting an existing data product primary server to a member server

Perform this procedure to demote an existing data product (VPFM/EPM/NRM/IPFM) primary server to a member server status to join the data product to an Avaya CS 1000–based primary server.

This workflow applies when a data network management product is deployed in a separate security domain and must be reconfigured to join another Avaya CS 1000-based security domain. To demote an existing data product primary server to a member server status, you must uninstall the product entirely and reinstall the product with a member server type configuration. Additionally, the provided backup and restore utilities must be invoked to preserve the applications data and configurations.

1. Invoke the backup process.

   Use the following backup script to backup the product data and configurations.

   - In Linux: `$UCM_HOME/bin/backupAllData.sh`
   - In Windows: `%UCM_HOME%\bin\backupAllData.bat`

   The backed-up data is stored as a .jar file inside folder UCM_HOME/backups.
2. Uninstall the existing data product.

   Use the provided uninstaller executable to uninstall the product.
3. Install the same product with member server type configuration.

   For installation procedure, see Joining a new data product (VPFM/EPM/NRM/IPFM) member server to an Avaya CS 1000 based primary server on page 13.
4. Invoke the restore process.

   Use the following restore script to restore the product data and configurations.

   - In Linux: `$UCM_HOME/bin/restoreAllData.sh`
   - In Windows: `%UCM_HOME%\bin\restoreAllData.bat`

   The restore script prompts for the name of the backup .jar file.

Demoting an existing data product backup server to a member server

Perform this procedure to demote an existing data product (VPFM/EPM/NRM/IPFM), backup server to a member server status.

This workflow applies after a data network management product is deployed in the same security domain as the Avaya CS 1000 and must be reconfigured from backup server to member server. You must uninstall the product entirely and reinstall the product with a different server type configuration. The provided backup and restore utilities must be invoked to preserve the applications data and configurations.

1. Invoke backup process.

   Use the following backup script to backup the product data and configurations.

   - In Linux: `$UCM_HOME/bin/backupAllData.sh`
   - In Windows: `%UCM_HOME%\bin\backupAllData.bat`

   The backed-up data is stored as a .jar file inside folder UCM_HOME/backups.

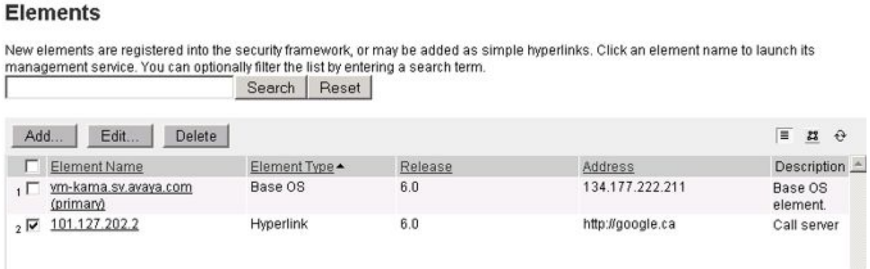
2. Uninstall the existing data product.

   Use the provided uninstaller executable to uninstall the product.

3. Cleanup the Elements Table from the GUI.

   The current uninstaller does not remove the added elements from the GUI, therefore you must remove the added elements manually. The following figures illustrate the before, during and after states of the manual cleanup.

   The following figure is an example the screen that appears before the manual removal of the Elements.

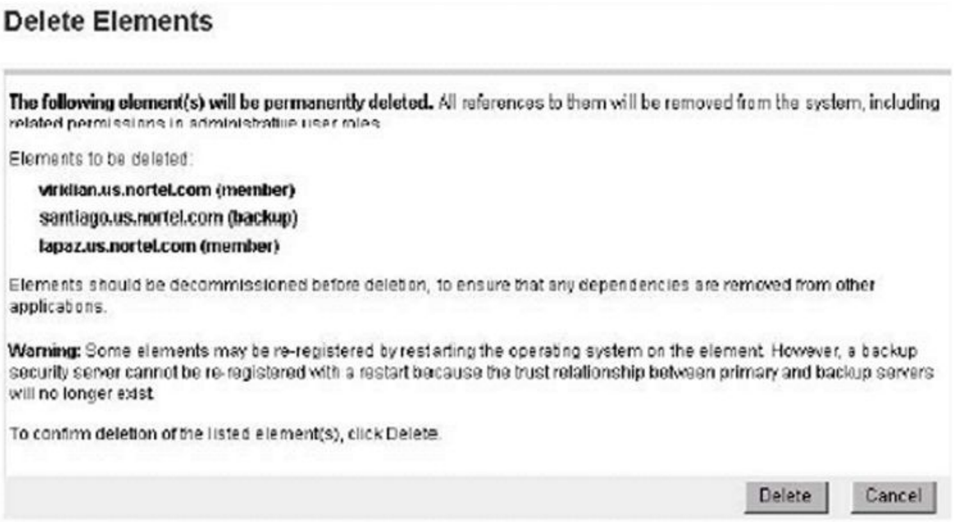


Elements

New elements are registered into the security framework, or may be added as simple hyperlinks. Click an element name to launch its management service. You can optionally filter the list by entering a search term.

	□	Element Name	Element Type ▲	Release	Address	Description
1	□	vm-kama.sv.avaya.com (primary)	Base OS	6.0	134.177.222.211	Base OS element.
2	☑	101.127.202.2	Hyperlink	6.0	http://google.ca	Call server

   The following figure is an example of the screen that appears during the manual removal of the Elements.



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:

viridian.us.nortel.com (member)
santiago.us.nortel.com (backup)
lapaz.us.nortel.com (member)

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

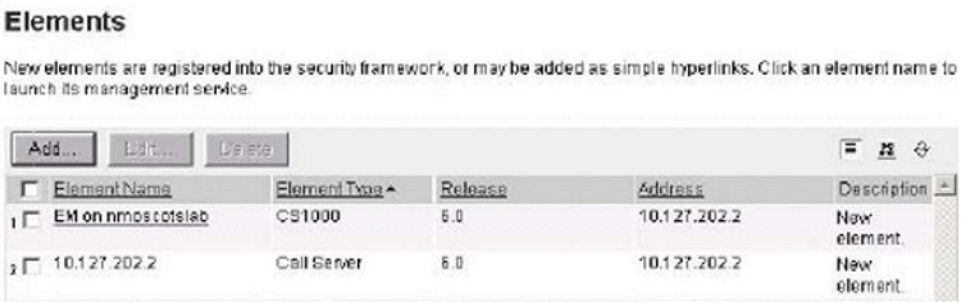
Warning: Some elements may be re-registered by restarting the operating system on the element. However, a backup security server cannot be re-registered with a restart because the trust relationship between primary and backup servers will no longer exist.

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

Note:

Deleting elements from the UCM in this workflow is the expected behavior, and should not be a concern if the product data and configurations have been properly backed up in the step 1.

The following figure is an example of the screen that appears after the manual removal of the Elements.



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.

	☐	Element Name	Element Type ▲	Release	Address	Description
1	☐	EM on nmoscotslab	CS1000	6.0	10.127.202.2	New element.
2	☐	10.127.202.2	Call Server	6.0	10.127.202.2	New element.

4. Roles and permissions remain.

   The current uninstaller does not remove the added data products roles and permissions, and you cannot remove them manually. They remain in the system.

5. Install the same product with a different server type configuration.

   For installation procedure, see Joining a new data product (VPFM/EPM/NRM/IPFM) member server to an Avaya CS 1000 based primary server on page 13.

6. Invoke the restore process.

   Use the following restore script to restore the product data and configurations.

   - In Linux: `$UCM_HOME/bin/restoreAllData.sh`
   - In Windows: `%UCM_HOME%\bin\restoreAllData.bat`

The restore script prompts for the name of the backup .jar file.

Promoting an existing data product member server to a backup server

Perform this procedure to promote an existing data product (VPFM/EPM/NRM/IPFM), member server to backup server status.

This workflow applies when a data network management product is deployed in the same security domain as the Avaya CS 1000 and must be reconfigured from member server to backup server. You must uninstall the product entirely and reinstall the product with a different server type configuration. The provided backup and restore utilities must be invoked to preserve the applications data and configurations.

1. Invoke backup process.

   Use the following backup script to backup the product data and configurations.

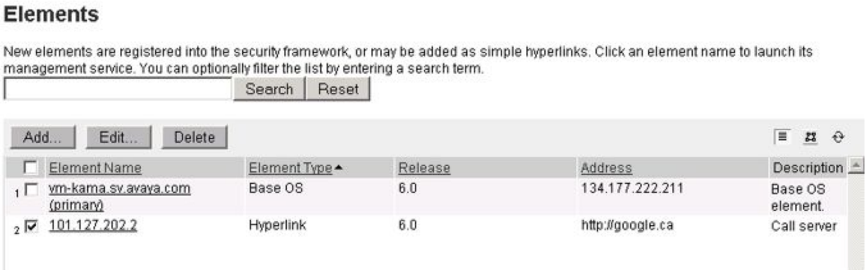
   - In Linux: `$UCM_HOME/bin/backupAllData.sh`
   - In Windows: `%UCM_HOME%\bin\backupAllData.bat`

   The backed-up data is stored as a .jar file inside folder UCM_HOME/backups.
2. Uninstall the existing data product.

   Use the provided uninstaller executable to uninstall the product.
3. Cleanup the Elements Table from the GUI.

   The current uninstaller does not remove the added elements from the GUI, therefore you must remove the added elements manually. The following figures illustrate the before, during and after states of the manual cleanup.

   The following figure is an example the screen that appears before the manual removal of the Elements.

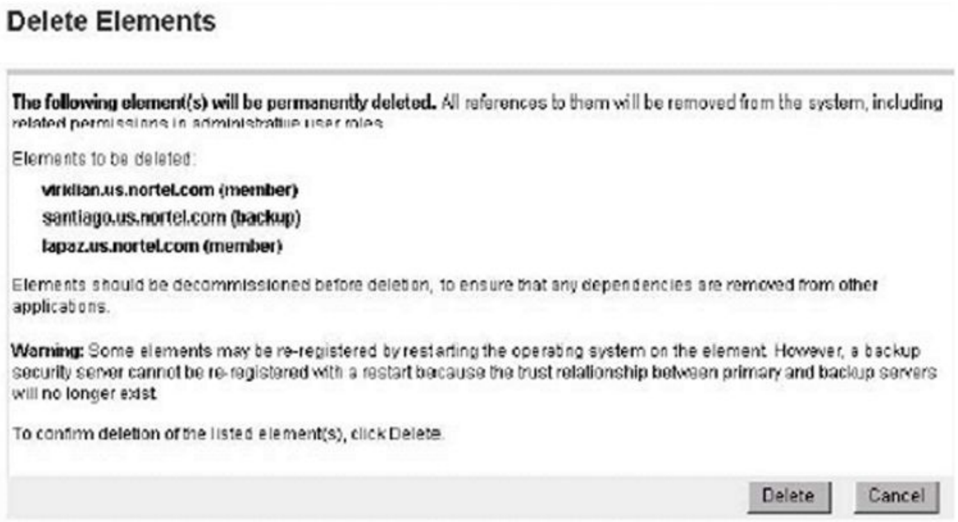


Elements

New elements are registered into the security framework, or may be added as simple hyperlinks. Click an element name to launch its management service. You can optionally filter the list by entering a search term.

	☐	Element Name	Element Type▲	Release	Address	Description
1	☐	vm-kama.sv.avaya.com (primary)	Base OS	6.0	134.177.222.211	Base OS element.
2	☑	101.127.202.2	Hyperlink	6.0	http://google.ca	Call server

   The following figure is an example of the screen that appears during the manual removal of the Elements.



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:

viridian.us.nortel.com (member)

santiago.us.nortel.com (backup)

lapaz.us.nortel.com (member)

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

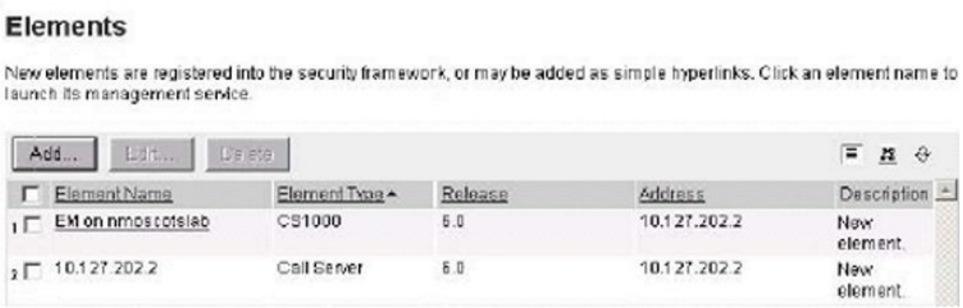
Warning: Some elements may be re-registered by restarting the operating system on the element. However, a backup security server cannot be re-registered with a restart because the trust relationship between primary and backup servers will no longer exist

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

Note:

Deleting elements from the UCM in this workflow is the expected behavior, and should not be a concern if the product data and configurations have been properly backed up in the step 1.

The following figure is an example of the screen that appears after the manual removal of the Elements.



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.

	□	Element Name	Element Type ▲	Release	Address	Description
1	□	EM on nmoscotslab	CS1000	6.0	10.127.202.2	New element.
2	□	10.127.202.2	Call Server	6.0	10.127.202.2	New element.

4. Roles and permissions remain.

   The current uninstaller does not remove the added data products roles and permissions, and you cannot them manually. They remain in the system.

5. Install the same product with a different server type configuration.

   For installation procedure, see Joining a new data product (VPFM/EPM/NRM/IPFM) member server to an Avaya CS 1000 based primary server on page 13.

6. Invoke the restore process.

   Use the following restore script to restore the product data and configurations.

   - In Linux: `$UCM_HOME/bin/restoreAllData.sh`
   - In Windows: `%UCM_HOME%\bin\restoreAllData.bat`

The restore script prompts for the name of the backup .jar file.

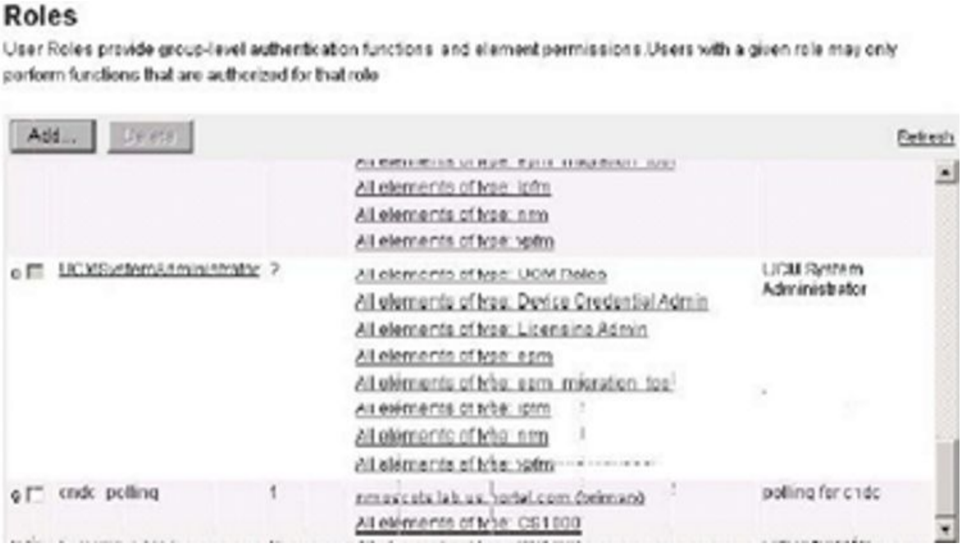
Assigning voice and data products related roles and permissions to a single user

If a single user is required to manage both data and voice network, use this procedure to assign voice and data management roles and permissions to the single user.

1. Assign elements permissions to roles

   Data products use three predefined roles: UCMOperator, UCMSystemAdministrator, and NetworkAdministrator. For more information about these roles, see *Avaya Unified Communications Management Common Services Fundamentals* (NN48014–100). Only the data elements permissions are assigned to UCMOperator and UCMSystemAdministrator, but both data and voice elements permissions are assigned to the NetworkAdministrator.

   The following figure is an example of data elements permissions assigned to UCMSystemAdministrator.

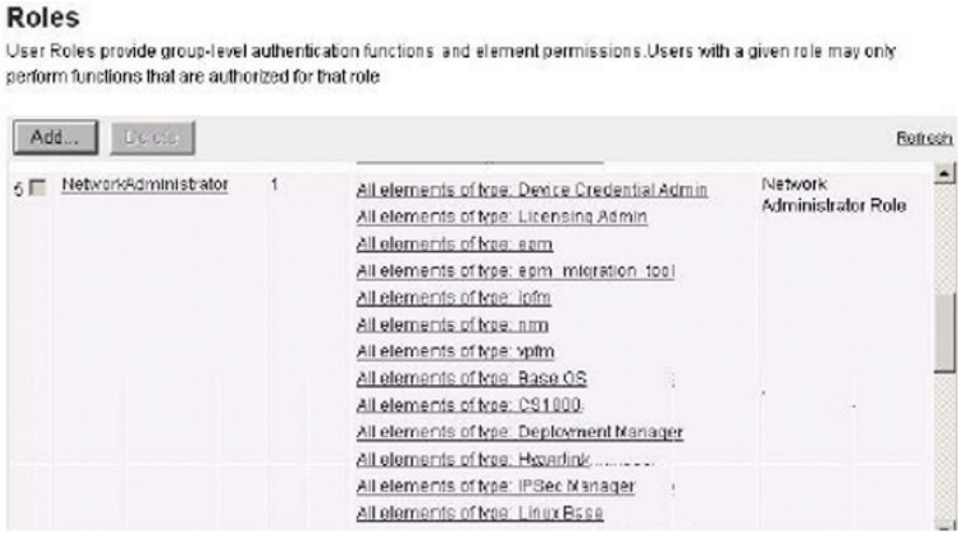


Roles

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

			[illegible] All elements of type: ipfm All elements of type: nrm All elements of type: vpfm	
○ □	UCMSystemAdministrator	7	All elements of type: UCM Deleg All elements of type: Device Credential Admin All elements of type: Licensing Admin All elements of type: epm All elements of type: epm_migration_tool All elements of type: ipfm All elements of type: nrm All elements of type: vpfm	UCM System Administrator
○ □	cndc polling	1	[illegible]lab.us.nortel.com [illegible] All elements of type: CS1000	polling for c1dc

   The following figure is an example of voice and data elements permissions assigned to the NetworkAdministrator.



Roles

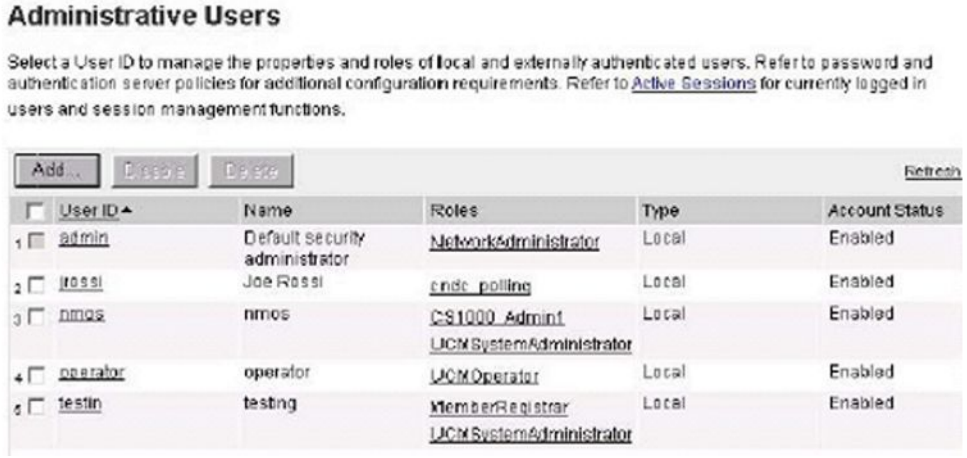
User Roles provide group-level authentication functions and element permissions.Users with a given role may only perform functions that are authorized for that role

5 □	NetworkAdministrator	1	All elements of type: Device Credential Admin All elements of type: Licensing Admin All elements of type: epm All elements of type: epm_migration_tool All elements of type: ipfm All elements of type: nrm All elements of type: vpfm All elements of type: Base OS 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

Voice products use predefined and administrator configurable roles. For more information about Management of Voicecentric roles and permissions, see *Avaya Call Server 1000 Unified Communications Management Common Services Fundamentals* (NN43001-116).

2. Assign roles to users.

   The following figure illustrates how the data related roles, such as UCMSystemAdministrator, and voice related roles, such as CS 1000 Admin, are assigned to the same user (NMOS).



Administrative Users

Select a User ID to manage the properties and roles of local and externally authenticated users. Refer to password and authentication server policies for additional configuration requirements. Refer to Active Sessions for currently logged in users and session management functions.

	□	User ID ▲	Name	Roles	Type	Account Status
1	□	admin	Default security administrator	NetworkAdministrator	Local	Enabled
2	□	jrossi	Joe Rossi	cndc_polling	Local	Enabled
3	□	nmos	nmos	CS1000_Admin1 UCMSystemAdministrator	Local	Enabled
4	□	operator	operator	UCMOperator	Local	Enabled
5	□	testin	testing	MemberRegistrar UCMSystemAdministrator	Local	Enabled

Chapter 4: Application server coresidency

This document outlines the extension of support to various scenarios in which Avaya Unified Communications Management (Avaya UCM) Security domains contain both voice applications on one or more servers, and data applications on one or more servers. However, while domain coresidency support is being introduced, support is not currently being extended to the installation of voice and data functionality onto the same server, that is, server coresidency.

Existing support for coresidency of voice management applications on a single server remains unchanged. For more information, see the following documents:

- *Avaya Call Server 1000 Unified Communications Management Common Services Fundamentals* (NN43001-116)
- *Avaya Communication Server 1000 Linux Platform Base and Applications Installation and Commissioning* (NN43001-315)

Existing support for coresidency of data management applications on a single server remains unchanged. For more information, see *Avaya Unified Communications Management Common Services Fundamentals* (NN48014-100).

Chapter 5: Converged Avaya UCM deployments – known issues and resolutions

The following section provides resolutions to known issues with converged Avaya Unified Communications Management (Avaya UCM) deployments.

1. **Issue**

   No data network management application links (VPFM, EPM, NRM or IPFM) are added to the Avaya Communications Server 1000 (Avaya CS 1000) primary server if these data network management applications are installed as backup or member to the primary, then uninstalled and then reinstalled.

   Resolution

   After the backup/member data management applications are uninstalled, perform the following steps:

   - Stop the primary server
   - Stop the backup server
   - Stop all member servers
   - Start the primary server
   - Start the backup server
   - Start all member servers

2. **Issue**

   When a data application (VPFM, EPM, NRM, or IPFM) is installed as the first member server and points to an Avaya CS 1000 primary server, sometimes the Avaya UCM roles (UCMOperator and UCMSystemAdministrator) do no appear on the Roles page. But, while creating a new role, and adding permissions mapping, the UCM permissions appear in the list. (CR Q02060973).

   Resolution

   Perform the following steps:

   - On the member server, go to the following folder:

     ```
     /opt/avaya/ucm/jboss-4.2.3.GA/server/default/conf/
     elementRegistry/elementType/deployed
     ```

- Modify version number from 1.0 to 1.1 (that is, <version>1.1<version>) in the following xml files:
  - UCMRolesElementType.xml
  - deviceCredentialAdminElementType.xml
  - licensingAdminElementType.xml
  - VPFMmoduleElementType.xml (only for VPFM)
  - EPMmoduleEleemntType.xml (only for EPM)
  - EPM_MIGRATION_TOOLmoduleElementType.xml (only for EPM)
  - NRMmoduleElementType.xml (only for NRM)
  - IPFMmoduleElementType.xml (only for IPFM)
- Go to `https://[member-server-fqdn]/local-login`, where `[member-server-fqdn]` is the fully qualified domain name of the member server.
- Enter User ID as `root` (Linux), or `Administrator` (Windows), and the corresponding password of the system user. You must have administrative rights to the server, otherwise contact your system administrator.
- Choose the **Full security configuration** option, and click on the **Security Configuration** button. This reregisters the member server to the primary server and republishes the roles element types.
- You are only required to restart the primary server if you notice incorrect localization words for the above element types permission name.

3. **Issue**

   In a security domain where Avaya CS 1000 is installed as primary and the data applications (VPFM, EPM, NRM, or IPFM) are installed as backup or member servers, occasionally the user cannot access the UCM login page after the CS 1000 primary server is restarted (CR Q02082801).

   Resolution

   Perform the following steps:

   - Stop the primary server.
   - Stop the backup server (if deployed).
   - Stop all member servers.
   - Start the primary server.
   - Start the backup server (if deployed).
   - Start all member servers.