Avaya Visualization Performance and Fault Manager Common Services Fundamentals
Unified Communications Management

Release 3.0.3
NN48014-100
Issue 05.01
March 2014

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 may generally make available to users of its products and Hosted Services. 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 Avaya hardware and software. 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 or such successor site as designated by Avaya. Please note that if you acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. 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 CHANNEL PARTNER; 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”).

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. “Software” means Avaya’s computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed , or remotely accessed on hardware products, and any upgrades, updates, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

Licence types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

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”, or such successor site as designated by Avaya. 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, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, 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 or Hosted Service 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”). As required, 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 or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components

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 or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

Avaya Aura® is a registered trademark of Avaya Inc.

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), 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, Hosted Service(s) 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. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for Product or Hosted Service notices and articles, or to report a problem with your Avaya Product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction

Purpose

This document provides information about the Avaya Unified Communications Management (UCM) common platform for integrating network management solutions such as Avaya IP Flow Manager (IPFM), Avaya Configuration and Orchestration Manager (COM), Avaya Virtualization Provisioning Service (VPS), Avaya Visualization Performance and Fault Manager (VPFM), and Avaya VPFM-Lite.

This document is intended for administrators who can configure Security Administration and the Device and Server Credentials Editor for network management products through the Unified Communications Management Common Services (UCM-CS).

Related resources

Related topics:

Documentation on page 9
Training on page 10
Avaya Mentor videos on page 11
Support on page 11

Documentation

See the following related documents:

Title	Purpose	Link
Avaya Visualization Performance and Fault Manager VPFM SCOM Connector Fundamentals (NN48014–101)	Fundamentals	http://support.avaya.com
Avaya VPFM Traps and Trends (NN48014–103)	Reference	http://support.avaya.com

Title	Purpose	Link
Avaya VPFM Supported Devices, Device MIBs, and Legacy Devices (NN48014–104)	Reference	http://support.avaya.com
Avaya Visualization Performance and Fault Manager Discovery Best Practices (NN48014–105)	Best Practices	http://support.avaya.com
Avaya Visualization Performance and Fault Manager Installation (NN48014–300)	Installation	http://support.avaya.com
Avaya Visualization Performance and Fault Manager VPFM SCOM Connector Installation (NN48014–301)	Installation	http://support.avaya.com
Avaya Visualization Performance and Fault Manager Quick Start (NN48014–302)	Quick Start	http://support.avaya.com
Avaya Visualization Performance and Fault Manager Configuration (NN48014–500)	Administration	http://support.avaya.com
Avaya Visualization Performance and Fault Manager Using Unified Communications Management to Manage the Converged Voice and Data Network (NN48014–501)	Deployment	http://support.avaya.com
Avaya Visualization Performance and Fault Manager Fault and Performance Management (NN48014–700)	Administration	http://support.avaya.com

Training

Ongoing product training is available. For more information or to register, you can access the Web site at http://avaya-learning.com/.

Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

- To find videos on the Avaya Support website, go to http://support.avaya.com, select the product name, and select the *videos* checkbox to see a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to http://www.youtube.com/AvayaMentor and perform one of the following actions:
    - Enter a key word or key words in the Search Channel to search for a specific product or topic.
    - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the site.

Note:

Videos are not available for all products.

Support

Visit the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Chapter 2: New in this release

The following sections detail what's new in *Avaya Unified Communications Management*, (NN48014-100) which supports COM, IPFM, VPS, and VPFM 3.0.3.

Features

See the following section for information about feature changes.

Customized interface

You can add a customized logo or banner on the application landing page. You can upload, remove, or change the customized logo or banner through the UCM Security Policies web page.

For more information, see Customized interface on page 51.

Chapter 3: UCM overview

This chapter provides an overview of the Avaya Unified Communications Management (UCM) Common Services for the following applications: IP Flow Manager (IPFM), Configuration and Orchestration Manager (COM), Avaya Virtualization Provisioning Service (VPS), and Visualization Performance and Fault Manager (VPFM) and VPFM-Lite 3.0.3.

Introduction

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

You can use the UCM Security Services to simplify security control for managed elements and system management applications. UCM Security Services manages secure access to Web applications and provides authentication, authorization and accounting (AAA) 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. This type of control is known as role based access control (RBAC).

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

Supported platforms

UCM Common Services is supported on the following platforms:

- Windows Server 2003 (all versions)
- Windows Server 2008 (all versions)
- RedHat Enterprise Linux 5.2, 5.4, or 5.6
- VMware ESXi (Windows 2003, 2008 or RHEL operating systems)
- Microsoft HyperV (Windows 2003, 2008 or RHEL operating systems)

Supported browsers

Avaya Unified Communications Manager supports the following browsers:

- Firefox 6.x or higher
- Internet Explorer 8 (IE8)
- Internet Explorer 9 (IE9)

Note:

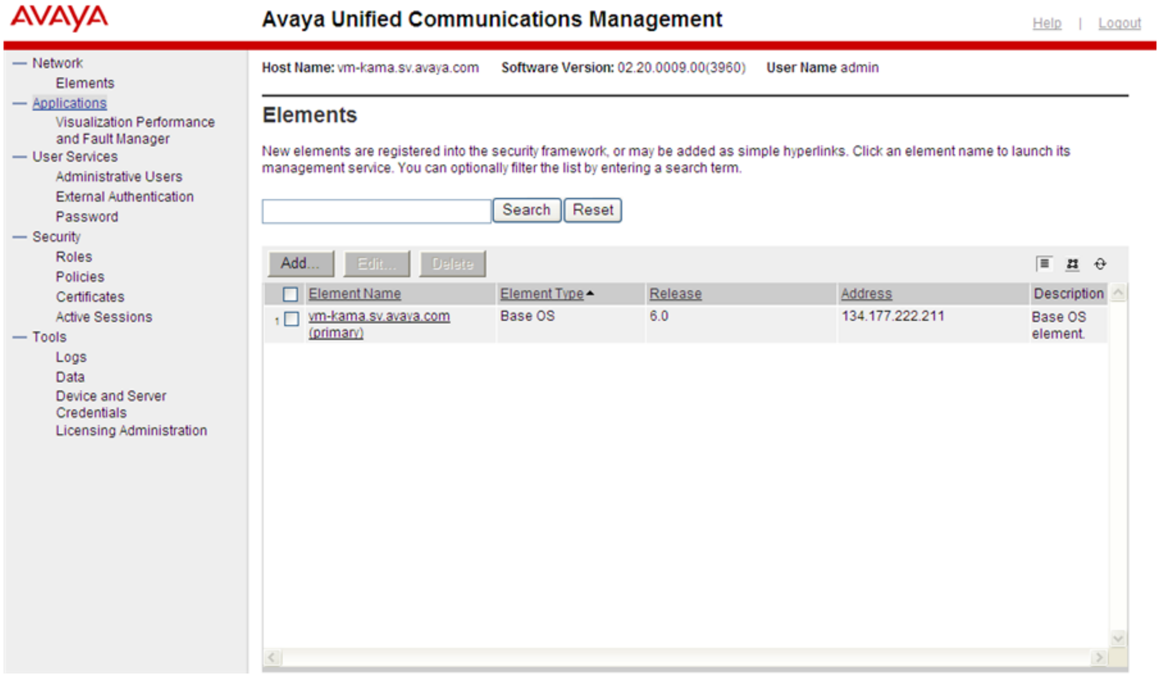
Internet Explorer 7 (IE7) is no longer supported with VPFM 3.0.3. If you use IE8 or IE9, the compatibility mode with IE7 must be turned off. You cannot access VPFM using IE9 browser on Windows XP and earlier versions. The system requirements for Internet Explorer 9 are Windows 7, Windows Server 2008 R2, Windows Vista Service Pack 2, or Windows Server 2008 SP2 with the Platform Update.

UCM navigation tree

The UCM navigation tree is located on the left side of the Web page. The root level items are:

- Network: The elements that are within the scope of the UCM security framework. You can define and browse to systems and servers within this secure network.
- Applications: The applications that are installed. For example, Visualization Performance and Fault Manager (VPFM), and other Avaya NMOS applications.
- User Services: User-related objects and identity management.
- Security: UCM Security Services objects and security policy management.
- Tools: Logging services, data tools, device and server credentials, and licensing administration.

The following figure depicts the UCM main navigation page.



Avaya Unified Communications Management

Host Name: vm-kama.sv.avaya.com **Software Version:** 02.20.0009.00(3960) **User Name** admin

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.

Network

The Network Elements page is the default Web page that appears when Unified Communications Management (UCM) Common Services starts. The Elements section contains links to the managed elements, such as application plug-ins and bookmarks. You can use the Search field to filter the list of elements. Afterwards, use the Reset button to return to the original list. The elements table lists all the nodes (primary/member/backup servers) installed in the network.

Important:

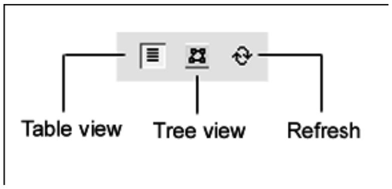
Users see only the elements that are enabled based on the assigned role permissions.

You can use the information on the Elements page by following methods:

- Table view: the default view. From the table view, you can add, edit, or delete elements. In this view, you see a list of UCM Common Services elements that are based on your role permissions. A network administrator can see all the 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.
- Tree view: a hierarchical view. From the tree view, you can create groups of elements according to your business needs. The Network group is the root level of the tree view. To browse, 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, you

do not require sign-on. 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 browse to the associated element. When the tree appears in the 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 VPFM. Elements in each folder are sorted alphabetically by element name. Click an element in a system group to browse to the management application running on that element.

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



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 optionally configure an external LDAP server, Radius server, or a Kerberos server. An internal Open LDAP is included with the UCM Common Services. The internal Open LDAP is the default authentication service used if you do not configure the external authentication server.
- Password: Use this link to 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.

Default roles

The UCM is configured with default roles. Network administrators use built-in roles to provide default access control policies for assigned users. You can edit built-in roles but cannot delete them. You can create custom roles to provide additional options for access control to managed elements. If the administrator is assigned multiple roles, permission is granted based on the most privileged role. The role with the highest privilege is assigned to the user. Built-in roles are assigned to default permissions when a new element is added.

The following table is a list of the built-in role permission assignments.

Role name	Description
MemberRegistrar	Provides limited access. You can register new members to the primary server.
NetworkAdministrator	Provides full privileges on the system. Provides emergency account access to any system, including situations where the primary server is out-of-service.
Patcher	Provides access to software maintenance functions.
UCMOperator	Provides application specific permissions.
UCMSystemAdministrator	Provides application specific permissions.

Tools

The UCM provides several tools, including Logs, Device and Server Credentials, and Licensing Administration.

- Logs: Use the log viewer tool to view system logs, or to export the logs to a comma-separated value (.CSV) file. No restrictions exist to the number of users who 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 be viewed using the log viewer tool. If the log file size exceeds 5 MB, a link is available to export and download the file.
- Data: Use the Data option to reload data from backup. Avaya recommends that you do not use the Data option, because reloading deletes data on this server and reloads the data from the peer server, terminates all active UCM sessions, and restarts the UCM web server.
- Device and Server Credentials: Use the Device and Server Credential Editor to set passwords, SNMP options, and other credentials for network devices. These configurations are common to all installed UCM applications, including IPFM, COM, VPFM or VPFM Lite.
- Licensing Administration: Use the Licensing Administration page to add and export licenses, or generate license reports. You can add a license either during the installation of UCM, or through the Licensing Administration after you install the application. You can use the Licensing Administration to add a license if you did not add a license during the installation of the UCM. However, during the installation of the application, since you can only select one license file, you need to use the Licensing Administration if you want to add multiple licenses. Use the export option to export the license for future reference if, for example, you reinstalled UCM. As for generating a license report, you can generate a report to view details about the licenses applied to the applications in the tabular format, and then save the report for future use.

Chapter 4: UCM login

The following section describes how to launch and log on to Unified Communications Management.

- Logging on to UCM on page 21
- Resetting the UCM admin password on page 22

Logging on to UCM

Before you begin

- You must install UCM.

About this task

Use the following procedure to log on to UCM.

Procedure

1. On the server where UCM is installed, choose **Start** > **Programs** > **Avaya** > **UCM** > **Unified Communications Management**.
    - On a client PC, point an internet browser to the FQDN of the server where UCM is installed.
    - If you use localhost or IP address in the address bar of the browser, on the UCM login screen, click **Go to central login for Single Sign-on** link to get to FQDN.
2. If a message appears telling you to select a security certificate, click **OK**.

    This certificate is pre-installed and cannot be changed.
3. When the dialog box appears, select the option to accept the certificate. This differs depending on the browser you are using.

    The UCM login screen appears.
4. Enter the **User ID**. The default is admin.
5. Enter the **password**. This is set during the installation of IPFM, COM, VPFM, or VPFM-Lite.
6. Click **Log in**.

Resetting the UCM admin password

About this task

Perform the following procedure to reset the UCM admin password.

Procedure

1. Log on to the local logon page of the UCM primary server.

   Example: https://fqdn/local-login
2. Enter the user name and password of a user having administrative user privileges on the machine where the primary server is installed.
3. After you log on, change the URL for password reset as shown in the following example.

   Example: https://fqdn/passwordReset
4. On the Password Reset page, enter **User ID**, **New password**, and **Confirm new password**.

Next steps

The password is temporary. After you change the password, you must log on to UCM, and apply a permanent password.

Chapter 5: Elements management

This chapter provides information about managing the elements in the UCM network.

Launching a managed element

Before you begin

- You must have logged on to the UCM as an administrator.

About this task

Perform this procedure to launch the management application for a selected element in the current or a new Web browser.

Procedure

1. In the navigation pane, under **Network**, click **Elements**.

   The Elements page appears.

   The Elements page is the default Web page that appears when the UCM is opened.

2. In the **Element Name** column, click an item. The management application for the element appears in the same Web browser window.

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

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

   Important:

   If the element you attempt to view is a secured element in the security framework, you require no authentication. If the element is an unsecured element, the administrator is subject to its authentication method, as single sign-on is not available for elements outside of the UCM security framework.

Adding an element

Before you begin

- Ensure that you are logged on to the UCM as an administrator.

About this task

Perform this procedure to add or register an element into the UCM network. Using the UCM, you can launch the added element and manage it from one place.

Procedure

1. In the navigation pane, under **Network**, click **Elements**.

   The Elements page appears.
2. On the **Elements** page, click **ADD**.

   The Add New Element page appears
3. In the **Name** field, enter the network element name.
4. In the **Description** field, enter the description of the network element.

   This field is optional.
5. In the **Type** list, select the element type.

   The default type is Hyperlink.
6. Click **Next** to go to the next page.
7. In the **Server Address** field, enter the URL for the bookmark element.
8. Click **Save**.

   The new element appears in the Elements pane.

Variable Definitions

Variable	Value
Element Name	Name of the element. The maximum length of this field is 256 characters.

Variable	Value
Element Type	Bookmark for the element.
Release	Release number for the element.
Address	URL for the bookmark element.
Description	A brief description of the element that you are adding to the UCM.

Editing element properties

Before you begin

- Ensure that you are logged on to the UCM as an administrator.

About this task

Perform this procedure to edit the properties of a element installed in the UCM network.

Procedure

1. In the navigation pane, under **Network**, click **Elements**.
   The Elements page appears.
2. Select the Element name check box for which you want to edit the details, and then click **Edit**.
   The Elements Details page appears.
3. Make changes to the Elements fields as required.
4. In the Release field, click **Edit**. The Release page appears.
5. In the **Release** list, select the release number as required and then click **Save** to go back to Elements Details page.
6. Click **Save**.

Variable Definitions

Variable	Value
Element Name	Name of the element. The maximum length of this field is 256 characters.
Element Type	Bookmark for the element.

Variable	Value
Release	Release number for the element.
Address	URL for the bookmark element.
Description	A brief description of the element that you are adding to the UCM.

Deleting selected elements

Before you begin

- Ensure that you are logged on to the UCM as an administrator.

About this task

Perform this procedure to delete elements in the UCM network.

Procedure

1. In the navigation pane, under **Network**, click **Elements**.

   The Elements page appears.

2. Select the Element name check box that you want to delete, and then click **Delete**.

   The Delete Elements page appears.

3. After you are prompted to confirm the deletion of the element, click **Delete**.

Chapter 6: User services

This chapter provides information about managing users using network services as subscribers or as administrators.

Users administration

This section provides information about managing users, and creating and managing the capabilities of users by assigning roles.

The administrator can perform the user management tasks required to manage users within the UCM.

Navigation

Viewing existing users

Before you begin

- Ensure that you are logged on to the UCM as an administrator.

About this task

Perform this procedure to view the users who are configured for UCM access.

Procedure

1. In the navigation pane, under **User Services**, click **Administrative Users**.

   The Administrative Users page appears.

   The Administrative Users page lists users configured for access to UCM.

2. View the information for existing users.

Adding a new local or external user

Before you begin

- Ensure that you are logged on to the UCM as an administrator.

About this task

Perform this procedure to create a new user of UCM and to assign roles to the new user.

Procedure

1. In the navigation pane, under **User Services**, click **Administrative Users**.

   The Administrative Users page appears.

2. Click **Add**. The Add New Administrative User page appears.
3. In the **User ID** field, enter the user ID.
4. In the **Authentication Type** option, select the user type.
5. In the **Full Name** field, enter the full name of the user.
6. In the **Temporary password** field, enter the temporary password.

   ! Important:

   The password that you enter for the new local user is temporary. After the new user logs on to the UCM for the first time, they are required to change this password. Therefore, Avaya recommends that users record the new password in a secure place.

7. In the **Re-enter password** field, reenter the temporary password, and then click **Save and Continue**.

   The Add New Administrative User Step 2 page appears.

8. In the **Role Name** column, select the Role Name check boxes that you want to assign to the user, and then click **Finish**.

The new user appears in the users list.

Variable Definitions

Variable	Value
User ID	ID of the user. This field can accept up to 31 characters and allows characters such as lowercase letters (a-z), uppercase letters (A-Z), numbers (0-9), and special characters (- and _).
Authentication type	Type of user: Local user or External user.
Full Name	Full name of the user.
Temporary password	New password for the user. This field allows characters such as lowercase letters (a-z), uppercase letters (A-Z), numbers (0-9) and special characters ({}|()<>,/.=[]_@!$%-+":?` \;). The minimum length of the password is 8 characters.
Re-enter password	Reenter the new password for the user.
Role Name	Roles that a new user can perform.

Disabling a user

Before you begin

- Ensure that you are logged on to the UCM as an administrator.

About this task

Perform this procedure to disable a user in the UCM network.

Procedure

1. In the navigation pane, under **User Services**, click **Administrative Users**.
2. On the Administrative Users page, under **User ID**, select the User ID check box that you want to disable, and then click **Disable**.

   The Account Status for the selected user changes to Disabled.

Deleting a user

Before you begin

- Ensure that you are logged on to the UCM as an administrator.

About this task

Perform this procedure to delete a user in the UCM network.

Procedure

1. In the navigation pane, under **User Services**, click **Administrative Users**.

   The Administrative Users page appears.

2. Under **User ID**, select the User ID check box that you want to delete, and then click **Delete**.

   The Delete Users page appears.

3. After you are prompted to confirm the deletion of user, click **Delete**.

   ❗ **Important:**

   Users cannot delete their own account.

Configuring user properties

Before you begin

- Ensure that you are logged on to the UCM as an administrator.

About this task

Perform this procedure to change the password and full name for a user, to disable and enable a user account.

Procedure

1. In the navigation pane, under **User Services**, click **Administrative Users**.
2. Under **User ID**, click the User ID to which you want to set properties and assign roles.
3. To disable or enable the user, select the disabled or enabled option button.
4. In the **Password Reset** section, in the **Password** field, enter a new password.

5. In the **Re-enter password** field, type the new password again.
6. (Optional.) In the **Full Name** field, edit the name of the user.
7. Click **Save**.

Variable Definitions

<table>
<tr><th colspan="2">Variable</th><th>Value</th></tr>
<tr><td rowspan="2">User status:</td><td>Enabled</td><td>Enables the user ID.</td></tr>
<tr><td>Disabled</td><td>Disables the user ID.</td></tr>
<tr><td colspan="2">Password</td><td>New password of the user. This field allows characters such as lowercase letters (a-z), uppercase letters (A-Z), numbers (0-9), and special characters ({}|()<>,/.=[_@]!$%-+":?`\;). The minimum length of the password is 8 characters.</td></tr>
<tr><td colspan="2">Re-enter password</td><td>Reenter the new password for the user.</td></tr>
<tr><td colspan="2">Full Name</td><td>Full name of the user.</td></tr>
<tr><td rowspan="2">Authentication type:</td><td>Local</td><td>The user is authenticated by the default Open LDAP service.</td></tr>
<tr><td>External</td><td>The user is authenticated by the external authentication service if it is configured. The External Identity Repositories Web page contains a summary page for authentication scheme and authentication servers. In the Authentication Servers page you can optionally configure an external LDAP server, Radius server, or a 9 Kerberos server.</td></tr>
<tr><td colspan="2">User ID</td><td>ID of the user. This field can accept up to 31 characters and allows characters such as lowercase letters (a-z), uppercase letters (A-Z), numbers (0-9), and special characters (- and _).</td></tr>
</table>

Editing user role mapping

Before you begin

- Ensure that you are logged on to the UCM as an administrator.

About this task

Perform this procedure to select roles to authorize a user for associated features and element permissions.

Procedure

1. In the navigation pane, under **User Services**, click **Administrative Users**.

   The Administrative Users page appears.
2. Under **User ID**, click the User ID to which you want to set properties and assign roles.

   The Users Details (admin) page appears.
3. In the **Roles** section, click Select Roles.

   The User Roles page appears for the selected user.
4. In the **Roles** section, select or deselect the **Role Name** check box, and then click **Save**. The User Details page appears.
5. Click **Save**.

External authentication scheme and authentication server configuration

This section provides information about configuring external authentication scheme and authentication server for UCM.

The Unified Communications Management supports up to four authentication authorities:

- local servers
- external RADIUS servers
- external LDAP servers, including Sun ONE or Microsoft active directory server
- KERBEROS servers

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

- Editing the authentication scheme on page 33
- Configuring authentication servers on page 33

Editing the authentication scheme

Before you begin

- Ensure that you are logged on to the UCM as an administrator.

About this task

Perform this procedure to edit the authentication scheme.

Procedure

1. In the navigation pane, under **User Services**, click **External Authentication**.
   The External Identity Repositories page appears.
2. In the **Authentication Scheme** section, click **Edit**.
   The Authentication Scheme page appears.
3. Select the required authentication scheme, and then click **Save**.

Configuring authentication servers

Perform this procedure to configure authentication servers.

When the target LDAP server is not the Microsoft Active Directory, the external user must have the UID attribute mapped to their logon name. When the LDAP server is the 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 login name.

The TCP port that is 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 backup primary security service. To check the status of the iptables rules, use service iptables status.

In the Authentication Servers page, the administrator has the option of provisioning a LDAP, RADIUS, or KERBEROS server.

- Provisioning the LDAP server on page 34
- Provisioning the RADIUS server on page 35
- Provisioning the KERBEROS server on page 36

Provisioning the LDAP server

Before you begin

- Ensure that you are logged on to the UCM as an administrator.
- Ensure the Linux iptable firewall setting on both the primary and backup security service allows the TCP port as source port.

About this task

Perform this procedure to complete the required information for the LDAP authentication server.

Procedure

1. In the navigation pane, under **User Services**, click **External Authentication**.

   The External Identity Repositories page appears.
2. In **Authentication Servers** section, click **Configure**.

   The Authentication Servers page appears.
3. Select the **Provision LDAP Server** check box.
4. In the **IP (or DNS)** field, enter the IP address or DNS name of the LDAP server.
5. In the **TCP Port** field, enter the TC port number of the LDAP server.
6. In the **Base Distinguished Name** field, enter the base DN of the LDAP server.
7. Select the **SSL/TLS Mode** option button if the LDAP server supports SSL/TLS connections.
8. Select the **Is Active Directory** option button if the active directory does not support anonymous binding.
9. In the **Distinguished Name for Root Binding** field, enter the distinguished name for the root binding.
10. In the **Password for Root Binding** field, enter the password for the root binding.
11. Click **Save**.

Variable Definitions

Variable	Value
IP (or DNS)	IP address or DNS name of the LDAP server.
TCP Port	TC port number of the LDAP server. For example, 389.
Base Distinguished Name	Base DN of the LDAP server. For example, dc=avaya, dc=com.
SSL/TLS Mode	SSL/TLS connections. Select it if LDAP server supports them.
Is Active Directory	Select this option button if the active directory does not support anonymous binding.
Distinguished Name for Root Binding	Distinguished Name for Root Binding. For example, cn=Bob, cn=Users, dc=avaya, dc=com.
Password for Root Binding	Password for root binding.

Provisioning the RADIUS server

Before you begin

- Ensure that you are logged on to the UCM as an administrator.
- Ensure the Linux iptable firewall setting on both the primary and backup security service allows the UDP port as source port.

About this task

Perform this procedure to complete the required information for the RADIUS authentication server.

Procedure

1. In the navigation pane, under **User Services**, click **External Authentication**.
2. In the **Authentication Servers** section, click **Configure**.
3. Select the **Provision Radius Server** check box.
4. In the **IP (or DNS)** field, enter the IP address or DNS name of the primary RADIUS server.

5. In the **UDP Port** field, enter the UDP port number of the primary RADIUS server.
6. In the **Shared Secret** field, enter the shared secret of the RADIUS server
7. Click **Save**.

Variable Definitions

Variable	Value
IP (or DNS)	IP address or DNS name of the primary RADIUS server.
UDP Port	UDP port number of the primary RADIUS server.
Shared Secret	Shared secret of the RADIUS serve.

Provisioning the KERBEROS server

Before you begin

- Ensure that you are logged on to the UCM as an administrator.

About this task

Perform this procedure to complete the required information for the KERBEROS server.

Procedure

1. In the navigation pane, under **User Services**, click **External Authentication**.
   The External Identity Repositories page appears.
2. In **Authentication Servers** section, click **Configure**.
   The Authentication Servers page appears.
3. Select the **Provision Kerberos Server** check box.
4. In the **DC Host Name (FQDN)** field, enter FQDN in the following format: machineName.domainName.com/net/.
5. In the **DC Computer Domain** field, enter the domain name of the Kerberos server.
6. In the **Keytab File** field, enter the encrypted Kerberos server key.

7. Click **Save**.

Variable Definitions

Variable	Value
DC Host Name (FQDN)	Enter FQDN in the following format: machineName.domainName.com/net.
DC Computer Domain	Domain name of the Kerberos server.
Keytab File	Encrypted Kerberos server key.

Password management

This section provides information about viewing password information and changing the password of an administrator.

- Viewing password information on page 37
- Changing password on page 38

Viewing password information

Before you begin

- Ensure that you are logged on to the UCM as an administrator. An external user cannot review or change the password.

About this task

Perform this procedure to view the last time you changed the password, when you can change the password, and when the password expires.

Procedure

In the navigation pane, under **User Services**, click **Password**.

The Password Status page appears.

Changing password

Before you begin

- Ensure that you are logged on to the UCM as an administrator.

About this task

Perform this procedure to change the administrator password.

Procedure

1. In the navigation pane, under **User Services**, click **Password**.
    - To launch the short cut on Windows, select **Start** > **All Programs** > **Avaya** > **UCM** > **UCM password change**
    - To launch the short cut on Linux, enter `/root/UCM Pasword Change`.

    The Password Status page appears.
2. Click **Change Password**.
    The Change Password page appears.
3. In the **Current password** field, enter the current password.
4. In the **New password** field, enter the new password.
5. In the **Confirm new password** field, enter the new password.
6. Click **Save**.

Variable Definitions

Variable	Value
Current password	Existing password of the administrator.
New password	New password of the administrator. Your new password must contain a minimum of eight characters with • at least one number from zero to nine • one special character such as an exclamation mark (!) • one uppercase and lowercase character

Variable	Value
	Allowed characters in the password are: a-zA-Z0-9{}|()<>,/.=[]^_@!$%&-+":?`\; You cannot use your previous six passwords.
Confirm new password	Type the password that you typed in the New password field.

Chapter 7: Security

This chapter provides information about managing users and roles, establishing password policies, distributing and maintaining Web SSL and SIP TLS security certificates, managing the private certificate authority, and managing sessions of logged on users.

Roles

This section provides information about performing the various role management tasks required to manage roles within the UCM. This feature provides group-level authentication functions and element permissions.

Viewing existing roles

Before you begin

- Ensure that you are logged on to the UCM as an administrator.

About this task

Perform this procedure to view the existing roles in the UCM.

Procedure

1. In the navigation pane, under **Security**, click **Roles**. The Roles page appears with a list of available roles.
2. Scroll down through the list of role names to get to the end.

Adding roles

Before you begin

- Ensure that you are logged on to the UCM as an administrator.

About this task

Perform this procedure to add new role for specific access control policies in the UCM.

Procedure

1. In the navigation pane, under **Security**, click **Roles**.

   The Roles page appears with a list of available roles.
2. Click **Add**.

   The Add New Role Step 1 page appears.
3. In the **Role Name** field, enter the unique role name.
4. In the **Role Description** field, enter a brief description for the new role.
5. Click **Save and Continue**.

   The Role Details (Role Name) page appears.
6. Click the **Element/Service Permission** mapping tab.
7. Click **Add Mapping**.

   The Select Element to Map to Role (Role Name) page appears.
8. Select an element to map to a role, and then click **Next**.

   The Permission Mapping page appears.
9. Assign permissions for this role by selecting one or more check boxes. If there is a list beside the permission name, the administrator has the option to deny, modify, or view the option for the permission associated with the role.
10. Click **Save**.

    The Role Details (Role Name) page appears.

Variable Definitions

Variable	Value
Role Name	Name of the role that you are adding for specific access control policies in the UCM. The role name must be between 1-26 characters in length. Allowed characters are: a-z, A-Z, 0-9, -, and _.
Role Description	A brief description of the role that you are adding.
Element Name	Name of the element to be mapped to role.

Role mapping to a role assignment or edition

Perform this procedure to assign or edit permission mapping to a role.

There are two options for assigning permission mapping to a role. You 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.

- Selecting users on page 43
- Copying user assignment on page 44

Prerequisites

- Ensure that you are logged on to the UCM as an administrator.

Selecting users

About this task

Perform this procedure to assign or edit a role to individual users.

Procedure

1. In the navigation pane, under Security, click **Roles**.
   The Roles page appears with a list of available roles.
2. In the Role Name column, click a role.

3. Click the **Assigned Users** tab.
4. Click **Select Users** to assign or edit a role to individual users.
5. Select one or more check boxes beside the user name to grant permissions associated with this role.
6. Click **Save**.

Copying user assignment

About this task

Perform this procedure to copy user assignments from another role to the new role.

Procedure

1. In the navigation pane, under Security, click **Roles**.
2. In the Role Name column, click a role.
3. Select the **Assigned Users** tab, and then click **Copy All From**.
4. From the Copy from Role list, select a role.
5. Click **Save**.

   The Role page appears. You can use this page to view the new permissions for that role.

Editing a role

Before you begin

- Ensure that you are logged on to the UCM as an administrator.

About this task

Perform this procedure to edit the role description, Element/Service Mapping, and Assigned Users. You cannot change role name from the Role Details page.

Procedure

1. In the navigation pane, under **Security**, click **Roles**. The Roles page appears.
2. In the **Role Name** column, click a role name item to edit the description.

The Role Details (Role Name) page appears.

3. In the **Description** field, edit the information as required.
4. Click **Save**. The Role page appears.

Deleting roles

Before you begin

- Ensure that you are logged on to the UCM as an administrator.

About this task

Perform this procedure to delete roles.

Procedure

1. In the navigation pane, under **Security**, click **Roles**. The Roles page appears.
2. Select the **Role Name** check box that you want to delete, and then click **Delete**.
3. After you are prompted to confirm the deletion of the Role Name, click **Delete**.

Policies

This section provides information about configuring password policies for locally authenticated users, managing session settings, security settings, and the single sign-on cookie domain.

- Viewing security policies on page 46
- Editing password policies on page 46
- Editing session properties on page 49
- Security settings on page 50
- Customized interface on page 51
- Editing the Single Sign-on Cookie Domain on page 53

Viewing security policies

Before you begin

- Ensure that you are logged on to the UCM as an administrator.

About this task

Perform this procedure to view the security policies.

Procedure

1. In the navigation pane, under **Security**, click **Policies**. The Policies page appears.
2. View the policy settings currently in the UCM.

Editing password policies

Before you begin

- Ensure that you are logged on to the UCM as an administrator.

About this task

Perform this procedure to edit password policies including aging, history, strength, and lockout password policies in the UCM.

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 has been reached.
- The password is expired.

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

Procedure

1. In the navigation pane, under Security, click **Policies**.
2. In the Password Policy (for locally authenticated users) section, click **Edit**.
3. In the Aging section, select the check box **Enforce password aging policies**.

4. (Optional) Select the check box **Enable expired password change**.
5. In the **Expiration period** field, enter the number of days for the password to expire.
6. In the **Expiration warning** field, enter the number of days to send a warning message to a user that the password is about to expire.
7. In the **Minimum age** field, enter the number for the minimum allowable days for password age.

   Important:

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

8. In the History section, select the check box **Enforce policy against previously used passwords**.
9. In the **Previous passwords blocked** field, enter the number for the number of passwords to remember in history.
10. In the Strength section, select the check box **Enforce password content standards**.
11. In the **Minimum Total Length** field, enter a number for the minimum number of total characters for the password.
12. In the **Minimum by character Type** fields, in the **Lower case** field, enter the minimum number of lowercase characters for the password from 6 to 25.

    Important:

    The sum of the total characters for the password cannot exceed minimum total length.

13. In the **Lower case** field, enter the minimum number of lowercase characters for the password.
14. In the **Upper case** field, enter the minimum number of uppercase characters for the password.
15. In the **Numeric case** field, enter the minimum number of numeric characters for the password.
16. In the **Special case** field, enter the minimum number of special characters for the password.

    Note:

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

    - Passwords must not have a character repeated more than twice consecutively.

- Passwords must not have the user login name, either in forward or reverse.

17. In the Lockout section, select the check box **Enforce user lockout after failed login attempts**.
18. In the **Consecutive Invalid Login Attempts** field, enter a number for failed attempts from 1 to 20.
19. In the **Interval for Consecutive Invalid Login Attempts** field, enter the interval in number of minutes from 0 to 120 for consecutive invalid logon attempts.
20. In the **Lockout Time** field, enter the number of minutes from 0 to 120 until the account is unlocked.
21. Click **Save**.

> ! **Important:**
>
> A user can log on successfully with a valid user name and password when the required time for a failed logon attempt is reached.
>
> The system sends a warning message when a password is about to expire. You must change the password.

Variable Definitions

Variable	Value
Expiration period	The maximum allowable days for the password to be active. Accepts a number from 1 to 365. The default value is 90.
Expiration warning	Number of days to send a warning message to a user that password is about to expire. Accepts a number from 1 to 15. The default value is 7.
Minimum age	The minimum allowable days for password age. Accepts a number between 0 to 7. The default value is 3.
Previous passwords blocked	Number from 1 to 99 for the number of passwords to remember in history. The default value is 6.
Minimum Total Length	The minimum number of total characters for the password. The minimum range is 6 to 25. The default value is 8.

Variable	Value
Lower case	The minimum number of lowercase characters for the password 1 to x. The default value is 1.
Upper case	The minimum number of uppercase characters for the password from 1 to x. The default value is 1.
Numeric case	The minimum number of numeric characters for the password from 1 to x. The default value is 1.
Special case	The minimum number of special characters for the password from 1 to x. The default value is 1.
Consecutive Invalid Login Attempts	The number for failed attempts from 1 to 20. The default value is 5.
Interval for Consecutive Invalid Login Attempts	The interval in number of minutes from 0 to 120 for consecutive invalid logon attempts. The default is 10 minutes.
Lockout Time	The number of minutes from 0 to 120 until the account is unlocked. The default is two minutes.

Editing session properties

Before you begin

- Ensure that you are logged on to the UCM as an administrator.

About this task

Perform this procedure to manage the properties of user sessions including maximum session time and maximum idle time.

Procedure

1. In the navigation pane, under **Security**, click **Policies**. The Policies page appears.
2. In the **Session Properties** section, click **Edit**.

   The Session Properties page appears.
3. In the **Maximum Session Time** field, enter a number for the maximum session time in minutes from 10 to 1440.

4. In the **Maximum Idle Time** field, enter a number for the maximum idle time in minutes from 10 to 1440.

   Important:

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

5. Click **Save**.

Variable Definitions

Variable	Value
Maximum Session Time	Number for maximum session time in minutes from 10 to 1440. The default value is 120.
Maximum Idle Time	Number for the maximum idle time in minutes from 10 to 1440. The default value is 30.

Security settings

The Unified Communication Management displays a customizable logon banner after you log on to the system. The customizable banner is intended for use by customers who have security policies that require network equipment to display a specific message to users when they log on.

- Editing login warning banner on page 50

Prerequisites

- Ensure that you are logged on to UCM as an administrator.

Editing login warning banner

About this task

Perform this procedure to customize the message for the login warning banner in UCM.

Procedure

1. In the navigation pane, under **Security**, click **Policies**. The Policies page appears.
2. In the **Security Settings** section, click **Edit**.

   The Security Settings page appears.
3. In the **Login Warning Banner text** area, edit the text as required.

   The maximum number of characters allowed is 2500.
4. Click **Save**.

Customized interface

You can add a customized logo or banner on the application landing page. You can upload, remove, or change the customized logo or banner through the UCM Security Policies web page.

Adding a new image for a customized interface

Before you begin

Ensure that you are logged on to the UCM as an administrator.

About this task

Perform this procedure to add a new customized logo or banner on the application landing page.

Procedure

1. In the navigation pane, select **Securities** > **Policies**.
2. In the Customized Interface section, click **Edit**.
3. To select a file to upload, click **Browse**, and then navigate to the required file.

   Note:

   The supported image file formats are JPG, PNG, GIF, and BMP. The supported image dimensions are 100*51px.
4. After you upload the file, click **Save**.

5. Refresh the Customized Interface page, or log off and log on to UCM.

Editing a customized interface

Before you begin

Ensure that you are logged on to the UCM as an administrator.

About this task

Perform this procedure to change the customized logo or banner on the application landing page.

Procedure

1. In the navigation pane, select **Security** > **Policies**.
2. In the Customized Interface section, click **Edit**.
3. Click **Change**.
4. To select a file to upload, click **Browse**, and then navigate to the required file.

   Note:

   The supported image file formats are JPG, PNG, GIF, and BMP. The supported image dimensions are 100*51px.
5. After you upload the file, click **Save**.
6. Refresh the Customized Interface page, or log off and log on to UCM.

Removing an image from a customized interface

Before you begin

Ensure you are logged on to the UCM as an administrator.

About this task

Perform this procedure to remove a customized logo or banner from the application landing page.

Procedure

1. In the navigation pane, select **Security** > **Policies**.

2. In the Customized Interface section, click **Edit**.
3. Click **Remove**.
4. To confirm the removal of the image, click **OK**.
5. Refresh the Customized Interface page, or log off and log on to UCM.

Editing the Single Sign-on Cookie Domain

Before you begin

- Ensure that you are logged on to the UCM as an administrator.

About this task

Perform this procedure to change the Single Sign-on Cookie Domain.

When you configure the primary and backup security servers 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.

Procedure

1. In the navigation pane, under **Security**, click **Policies**. The Policies page appears.
2. In the Single Sign-on Cookie Domain section, click **Edit**.

   The Edit Domain Name page appears.
3. From the **Single Sign-On Cookie Domain** list, select a URL to change the Single Sign-on Cookie Domain.
4. Click **Save**.

   > **Important:**
   >
   > After you change the SSO Cookie Domain name, you must clear the existing UCM related cookies from the cache in the Internet browser for all users. To clear the cache after you save the new domain name, log out and close all browser windows that have been logged in to this server.

Certificate management

This section provides information about distributing and maintaining SSL and SIP TLS security certificates, and managing the Private Certificate Authority.

There are two tabs in this window, Certificate Endpoints and Private Certificate Authority. The Certificate Endpoints tab is the default window.

Use the Certificate Endpoints tab to view details of certificates or update the Certificate Revocation List (CRL).

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

- Adding a certificate on page 54
- Enabling trust for a certificate on page 55
- Disabling trust for an element on page 56
- Deleting a certificate on page 56
- Updating the Certificate Revocation List on page 57
- Downloading Private Certificate Authority details on page 57
- Revoking a certificate on page 58
- Downloading the Certificate Revocation List details on page 58

Adding a certificate

Before you begin

- Ensure that you are logged on to the UCM as an administrator.

About this task

Perform this procedure to add a certificate.

Procedure

1. In the navigation pane, under **Security**, click **Certificates**. The Certificate Management page appears.
2. In the **Certificate Authorities** section, click **ADD**.

   The Add a CA to the Service window appears.

3. In the **Friendly name** field, enter a unique friendly name.
4. Copy the content of the certificate authority X.509 certificate, and then paste the content into the text area below.
5. Click **Submit**.

Variable Definitions

Variable	Value
Friendly name	Type a string used to identify the certificate, such as UCM Primary Security Server.

Enabling trust for a certificate

Before you begin

- Ensure that you are logged on to the UCM as an administrator.

About this task

Perform this procedure to enable trust for a certificate.

Procedure

1. In the navigation pane, under **Security**, click **Certificates**. The Certificate Management page appears.
2. In the **Certificate Authorities** section, select the friendly name option button that you want to enable the trust.
3. Click **Enable Trust**. The Trusted status for the selected certificate changes to "Yes".

Disabling trust for an element

Before you begin

- Ensure that you are logged on to the UCM as an administrator.

About this task

Perform this procedure to disable trust for a certificate.

> **Note:**
>
> If there is only one Certificate Authority, do not disable it.

Procedure

1. In the navigation pane, under **Security**, click **Certificates**. The Certificate Management page appears.
2. In the **Certificate Authorities** section, select the friendly name option button that you want to disable the trust.
3. Click **Disable Trust**. The Trusted status for the selected certificate changes to "No".

Deleting a certificate

Before you begin

- Ensure that you are logged on to the UCM as an administrator.

About this task

Perform this procedure to delete a certificate.

Procedure

1. In the navigation pane, under **Security**, click **Certificates**. The Certificate Management page appears.
2. In the **Certificate Authorities** section, select the friendly name option button that you want to delete.
3. Click **Delete**.

4. After you are prompted to confirm the deletion of the selected certificate, click **OK**.

Updating the Certificate Revocation List

Before you begin

- Ensure that you are logged on to the UCM as an administrator.

About this task

Perform this procedure to update a Certificate Revocation List for an endpoint.

Procedure

1. In the navigation pane, under **Security**, click **Certificates**. The Certificate Management page appears.
2. In the **Certificate Authorities** section, click **Update CRL**.

   The Update CRL window appears.
3. Paste the CRL in to the text area, and then click **Submit**.

Downloading Private Certificate Authority details

Before you begin

- Ensure that you are logged on to the UCM as an administrator.

About this task

Perform this procedure to download the Private Certificate Authority details.

Procedure

1. In the navigation pane, under **Security**, click **Certificates**. The Certificate Management page appears.
2. Click the **Private Certificate Authority** tab. The Private Certificate Authority page appears.
3. In the **Private Certificate Authority Details** section, click **Download** to download the certificate contents.

   The File Download - Security Warning window appears.

4. Click **Save**. The Certificate Details window appears showing the details of the certificate.
5. Click **OK**.

Revoking a certificate

Before you begin

- Ensure that you are logged on to the UCM as an administrator.

About this task

Perform this procedure to revoke a certificate.

Procedure

1. In the navigation pane, under **Security**, click **Certificates**. The Certificate Management page appears.
2. Click the **Private Certificate Authority** tab. The Private Certificate Authority page appears.
3. In the **Certificates** section, select one or more of the check boxes beside the Serial Number, and then click **Revoke** to revoke the selected certificates.

Downloading the Certificate Revocation List details

Before you begin

- Ensure that you are logged on to the UCM as an administrator.

About this task

Perform this procedure to download the Certificate Revocation List (CRL) details.

Procedure

1. In the navigation pane, under **Security**, click **Certificates**. The Certificate Management page appears.
2. Click the **Private Certificate Authority** tab. The Private Certificate Authority page appears.
3. In the Certificate Revocation List (CRL) details section, click **Get CRL**.

The File Download window appears.

4. Click **Save**.

Active sessions

This section provides information about viewing the session information for any user who is currently logged on.

- Viewing active sessions on page 59
- Terminating active sessions on page 59

Viewing active sessions

Before you begin

- Ensure that you are logged on to the UCM as an administrator.

About this task

Perform this procedure to view active sessions in the UCM and session time for the user.

Procedure

1. In the navigation pane, under **Security**, click **Active Sessions**. The Active Sessions page appears.

   The sessions are sorted in the User ID column.
2. View the active sessions currently in the UCM.

Terminating active sessions

Before you begin

- Ensure that you are logged on to the UCM as an administrator.

About this task

Perform this procedure to terminate the active sessions in the UCM.

Procedure

1. In the navigation pane, under **Security**, click **Active Sessions**. The Active Sessions page appears.
2. Select the check box beside the sessions that you want to terminate.
3. Click **Terminate**.

   The selected sessions are deleted from the current sessions table.

   The administrators with terminated sessions are required to log on again.

Chapter 8: Tools

This chapter provides information about logs, device and server credentials, and license administration.

- Logs on page 61
- Data on page 62
- Device and Server Credentials Editor configuration on page 62
- License administration on page 67

Logs

This section provides information about viewing management activity logs for all servers in your Common Manager framework. You can open log files directly or download them for offline.

- Viewing log files on page 61

Prerequisites

- Ensure that you are logged on to the UCM as an administrator.

Viewing log files

About this task

Perform this procedure to view log files in UCM.

Procedure

1. In the navigation pane, under **Tools**, click **Logs**.

   The Logs page appears. This page contains the directory list for recorded logs.
2. Click a **Filename** to view the file information.
3. To open a log file in a new browser window, right-click the name of a log file, and then select Open in new window.

4. To download a log file, right-click the name of a log file, and then select **Save target as**. Select a location on the computer to save the log file.

Data

The Data option is used to reload data from backup. Avaya Recommends that you not use the Data option, because reloading deletes data on this server and reloads the data from the peer server, terminates all active UCM sessions, and restarts the UCM web server.

Device and Server Credentials Editor configuration

This section provides information about configuring device credentials using the Device and Server Credentials Editor.

Avaya Unified Communications Management (UCM) applications use SNMP v1/v2/v3, Telnet, CIM, SSH, FTP, RLogin, or SSH protocols for communication with network infrastructure devices such as routers. The protocol required depends on the type of device and uses the WMI protocol to communicate to a windows server. Each set of credential information is referred to as a credential set. These credential sets allow UCM applications to retrieve information from the network elements and devices. The Device and Server Credentials Editor service maintains a list of credential sets for the devices that make up a network. You can enter credentials for every device, such as an IP address, or for a range of IP addresses. See the documentation for your network devices to determine which protocols your network devices use for authentication.

When using Network Discovery in VPFM, the application uses these credentials to discover network devices and servers. For more information about network discovery, see *Avaya Visualization Performance and Fault Manager—Configuration* (NN48014-500).

The following table lists the categories of credential information that you can manage in the Device and Server Credentials Editor.

Table 1: Device and Server Credentials Editor fields

Credential information	Attributes
Set Name	Credential set name
IP Address or Range	Device/Server IP Address or Address Range
SNMPv1/v2	Read Community Write Community
SNMPv3	SNMPv3 User

Credential information	Attributes
	Authorization Protocol (MD5, SHA1, None) Authorization Key Privacy Protocol (AES128, DES, 3DES, None Privacy Key Context Management User Generic User
Telnet	Telnet User name Telnet Password Telnet Port
CIM	CIM User name CIM Password
SSH	SSH User name SSH Password SSH Port
NetConf	Netconf User Netconf Password Netconf Port Management User
FTP	FTP User name FTP Password FTP Port
RLogin	RLogin User name RLogin Password
Windows Server	Windows User name Windows Password Windows Domain

Adding a credential set

Before you begin

- You must have installed the UCM. The Unified Communications Management is installed when you install a UCM application (VPFM, VPFM Lite, COM, or IPFM). For more information, see the installation guide for UCM application.
- Ensure that you are logged on to UCM as administrator.

About this task

Perform this procedure to add a new credential set to Unified Communications Management (UCM). You must add a credential set for each device you want to manage.

The set name accepts printable ASCII characters, but not special characters (%(/!\)). You can enter the space ( ), dash (-), and underscore (_) characters.

The set name must be unique. If you add a new entry or rename an existing one with a set name already used in another entry, a warning message appears.

Procedure

1. In the navigation pane, under **Tools**, click **Device and Server Credentials**.
2. Click **Add Credential Set**.
3. In the **Set Name** field, enter the **Set Name**.
4. In the **IP Address or Range** field, specify the IP address information for the credential.

   For a list of valid IP addresses and ranges, see IP addresses and ranges reference on page 73.
5. Add device credential information on the appropriate tab. For more information about the available tabs, see Device and Server Credentials Editor configuration on page 62.

   Each tab corresponds to an authentication protocol. The information you enter depends on the type of authentication your device uses.
6. Click **Save**.

Deleting a credential set

Before you begin

- Ensure that you are logged on to the UCM as an administrator.

About this task

Perform this procedure to remove a credential set from the Device and Server Credentials Editor.

Procedure

1. In the navigation pane, under **Tools**, click **Device and Server Credentials**.

   The Device and Server Credentials Editor page appears.
2. Click the credential set that you want to remove.

   You can select several credential sets at once by holding down the CTRL key, and then clicking the credential sets.
3. Click **Delete Credential Set(s)**.

4. After you are prompted to confirm the deletion of credential set, click **Delete**.

Editing a credential set

Before you begin

- Ensure that you are logged on to the UCM as an administrator.

About this task

Perform this procedure to edit a credential set to change the set name, IP address, and device credential information for a credential set.

Procedure

1. In the navigation pane, under **Tools**, click **Device and Server Credentials**.
2. Click the credential set that you want to change.
3. Click **Edit Credential Set**.
4. Make changes to the credential set as required.
5. If you want to specify a different type of device credential information, click the **Show All** tab, and then type the new device credential information in the appropriate tab.

   For more information about the available tabs, see Device and Server Credentials Editor configuration on page 62
6. Click **Save**.

   All specified IP addresses are validated after saving the changes.

Importing a credential set

Before you begin

- Ensure that you are logged on to UCM as an administrator.

About this task

Perform this procedure to import the credential set to UCM.

Procedure

1. In the navigation pane, under **Tools**, click **Device and Server Credentials**.

The Device and Server Credentials Editor page appears.

2. Click **Import Credentials**.

   The Import Credential Set(s) window appears.

3. Click **Browse**, and then choose the credentials XML file to import.
4. (Optional) To overwrite the existing entries of credential set, select the **Overwrite existing entries** check box.
5. Click **Import**.

Exporting a credential set

Before you begin

- Ensure that you are logged on to the UCM as an administrator.

About this task

Perform this procedure to export credential set from the UCM to a local XML file.

Procedure

1. In the navigation pane, under **Tools**, click **Device and Server Credentials**.

   The Device and Server Credentials Editor page appears.

2. Click **Export Credentials**.

   The Export Credential Set(s) window appears.

3. Click **Export**.

   The Credential Sets exports to a local XML file. The name of the XML file is autogenerated.

   The File Download window appears.

4. Click **Save**.

Refreshing the credential set list

About this task

Perform this procedure to refresh the credential set list.

Use the manual refresh command to ensure that the information that appears in the Device and Server Credentials Editor is up-to-date. Updates to the credential sets list cannot immediately be reflected in the Device and Server Credentials Editor until it is refreshed. Credential sets update automatically every 10 seconds.

Procedure

1. In the navigation pane, under **Tools**, click **Device and Server Credentials**.

   The Device and Server Credentials Editor page appears.
2. Click **Refresh** located at the bottom of the page.

   The list of available credential sets is refreshed from the UCM database.

License administration

This section provides information about adding a license file, exporting a license file, and refreshing license information.

- Adding a license file on page 67
- Exporting a license file on page 68
- Refreshing license information on page 69

Upgrade on a VM environment

When you upgrade an application on a VM environment, Unified Communication Management (UCM) removes the license associated with the application from the license file. Therefore, make a copy of the license file before you perform the upgrade; you can use the copy of the license file to return to the older release, if required.

Co-resident deployment in a virtual environment

In a co-residency deployment, after you upgrade an application to the current release on a VM server, you must obtain new licenses for other existing applications, even if you are installing or upgrading only one of the applications.

Adding a license file

Before you begin

- Ensure that you are logged on to UCM as an administrator.

About this task

Perform this procedure to add a license to an application.

Procedure

1. In the navigation pane, under **Tools**, click **Licensing Administration**.
2. On the License Administration page, click **Add License**.
3. From the Add License dialog box, in the **License** field, browse to locate the license file.
4. Select the host to which the license is to be deployed.
5. Click **Add**.

Exporting a license file

Before you begin

- Ensure that you are logged on to UCM as an administrator.

About this task

Perform this procedure to export a license from the product name table to the local machine.

Selection of one license file from an application exports all licenses for that application.

Procedure

1. In the navigation pane, under **Tools**, click **Licensing Administration**.
   The Licensing Administration page appears.
2. In the product name table, select the product license to be exported.
3. Click **Export License**. The File Download window appears.
4. Click **Save**.

Generating a licensing report

Before you begin

- Ensure that you are logged on to UCM as an administrator.

About this task

Perform the following procedure to generate a licensing report for a product.

Procedure

1. In the navigation pane, under Tools, click **Licensing Administration**.
2. Select a product name.
3. Click **Report**.
4. Click **Open**, or **Save**.
   The report for the product you selected is generated as an HTML document.

Refreshing license information

Before you begin

- Ensure that you are logged on to UCM as an administrator.

About this task

Perform this procedure to refresh the license information.

Procedure

1. In the navigation pane, under **Tools**, click **Licensing Administration**.
   The Licensing Administration page appears.
2. Click **Refresh**. The license information in the product name table refreshes.

Chapter 9: Backup and Restore

You can back up and restore, on demand, all data within Unified Communications Management applications. Backup and Restore functionality is accessed from the command line.

All backup files are stored in a folder named backups under the UCM_HOME/bin directory. Backup files are stored in JAR format. The application writes debug information of its operations into log files located in common services installation folder: UCM_HOME. Backup archives are stored in [YY]-[MM]-[DD]_[HH].[mm].jar format (for example, 2008-06-09_15.33.jar).

Within common services, you can backup the following data:

- jbossdb database in MySQL (for Device and Server Credentials data)
- users and roles data (only on primary with the same FQDN)
- profiles/device attributes xml file (located in [UCM_JBOSS_HOME]/server/default/conf)

You do not have to stop services (JBoss, MySQL, and license server) to run the backup process.

The following sections describe backup and restore procedures:

- Backing up UCM files on page 71
- Restoring UCM files on page 72

Backing up UCM files

Before you begin

- You must be logged on to the UCM server as an Administrator in a Windows environment, or as root in a Linux environment.
- You can only backup and restore the same major application version. Differences between minor versions are supported. For example, you can backup and restore from version 3.0 to 3.1.

About this task

Use the following procedure to backup UCM files.

Important:

Do not abort the backup or restore in the middle of the process; for example by pressing Ctrl+C. Doing so may compromise system stability.

Procedure

1. From the command prompt, run the following script:`C:\Program Files\Avaya\UCM\backupAllData.bat`
   - If using Linux, run the following script from the command shell: `/opt/Avaya/ucm/backupAllData.sh`
2. Enter the database administrator password when prompted.

   The system backs up all UCM data.

Restoring UCM files

Before you begin

- Ensure that you are logged on to the UCM server as an Administrator in a Windows environment, or as root in a Linux environment.
- You can only backup and restore the same major application version. Differences between minor versions are supported. For example, you can backup and restore from version 3.0 to 3.1.

About this task

Use the following procedure to restore a previously backed up archive.

Important:

Do not abort the backup or restore in the middle of the process; for example by pressing Ctrl+C. Doing so may compromise system stability.

Procedure

1. From the command prompt, run the following script:`C:\Program Files\Avaya\UCM\restoreAllData.bat`
   - If using Linux, run the following script from the command shell: `/opt/Avaya/ucm/restoreAllData.sh`
2. Enter the database administrator password when prompted.
3. Enter the name of the archive you wish to restore.

   The system restores the selected archive. You may be required to restart services after the restore is complete.

Chapter 10: IP addresses and ranges reference

This section provides details about the valid IP addresses and IP ranges used by the Device and Server Credentials Editor.

Valid IP addresses and ranges

The following section describes the valid IP addresses and ranges used for device credentials.

- Valid IP addresses on page 73
- Valid IP address ranges on page 74
- IP address format limitations on page 74

Valid IP addresses

IPv4 addresses must conform to the following format: [1-255].[0-255].[0-255].[0.255].

IPv6 addresses must conform to IPv6 rules:

- IPv6 addresses must contain eight groups of four hexadecimal digits.
- Each group must be separated by a colon (:).
- If one or more four-digit group or groups appears as 0000, the zeros may be omitted and replaced with two colons (::). For example, the following are valid IPv6 addresses:
    - 2001:0db8:85a3:08d3:1319:8a2e:0370:7334
    - 2001:0db8::1428:57ab

Valid IP address ranges

When specifying IP address ranges, only consecutive wild cards starting from the last octet of an address are supported. This guarantees one continuous range. For example, only the following combinations are valid:

- IPv4:
    - 17.0.9.* (same as 17.0.9.0-17.0.9.255)
    - 17.0.*.* (same as 17.0.0.0-17.0.255.255)
    - 17.*.*.* (same as 17.0.0.0-17.255.255.255)
    - *.*.*.* (same as 0.0.0.0-255.255.255.255)
    - 17.*.9.9 is invalid
    - 0.0.0.0 and 255.255.255.255 are considered to be valid IPs only if they are given within a range. For example, 0.0.0.0 as single IP is invalid, but 0.0.0.0-2.3.4.5 is a valid range.
- IPv6:
    - 2001:0db8:85a3:08d3:1319:8a2e:0370:* (same as 2001:0db8:85a3:08d3:1319:8a2e:0370:0000-2001:0db8:85a3:08d3:1319:8a2e:0370:ffff)
    - 2001:0db8:85a3:08d3:1319:8a2e:*:*
    - 2001::8a2e:0370:*
- IPs contained in a range cannot have wild cards. For example, 192.168.4.*-192.168.5.245 is an invalid range.

IP address format limitations

The following formats are not supported by Device and Server Credentials Editor:

- An address/subnet mask pair (for example, 10.127.100.0/255.255.255.0)
- Network prefix (CIDR) notation (for example, 10.127.100.0/24)