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

2.3
NN48014-100, 02.03
June 2011

© 2011 Avaya Inc.

All Rights Reserved.

Notice

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

Documentation disclaimer

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

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked 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

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

Copyright

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

Third-party components

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: New in this release

The following sections detail what's new in *Avaya Unified Communications Management, NN48014-100*, which supports NRM 2.1, EPM 5.1, and VPFM 2.3:

Features

See the following sections for information about feature changes:

- Security on page 5
- Device and Server credentials editor on page 5
- License administration on page 5

Security

You can manage users and roles, establish password policies, distribute and maintain Web SSL and SIP TLS security certificates, manage the private certificate authority, and manage sessions of logged on users using Security. For more information, see Security on page 33.

Device and Server credentials editor

You can import a credential set to the UCM and export credential set from the UCM to a local XML file using Device and Server Credentials Editor. For more information, see Device and Server Credentials Editor configuration on page 52.

License administration

You can add a license file, export a license file, generate a license report, and refresh the license information using Licensing Administration. For more information, see License administration on page 56.

Chapter 2: Introduction

Avaya Unified Communications Management (UCM) provides the common platform for integrating network management products, such as Network Resource Manager (NRM), Enterprise Policy Manager (EPM), Visualization Performance and Fault Manager (VPFM), and VPFM-Lite. UCM contains administrative services for all of these products through Unified Communications Management Common Services (UCM-CS), which includes Security Administration and Device and Server Credentials Editor. It also provides a home page from which to access any of these installed products.

Chapter 3: UCM overview

This chapter provides an overview of the Avaya Unified Communications Management (UCM) Common Services for the following applications: Network Resource Manager (NRM 2.1), Enterprise Policy Manager (EPM) 5.1, and Visualization Performance and Fault Manager (VPFM) and VPFM-Lite 2.0.

Introduction

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

UCM Security Services simplifies security control for managed elements and system management applications. UCM Security Services manages secure access to Web applications and provides authentication and authorization with a single unified common service. UCM secures the delivery of essential identity and application information.

With UCM Common Services, administrators can control which users have access to specific managed elements. They can assign users to roles and map the permissions to those roles to control which operations a user can perform on an assigned managed element. Users can access only assigned elements and perform only the tasks specific to their assigned role and permissions for an element.

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

UCM Common Services is supported on the following platforms:

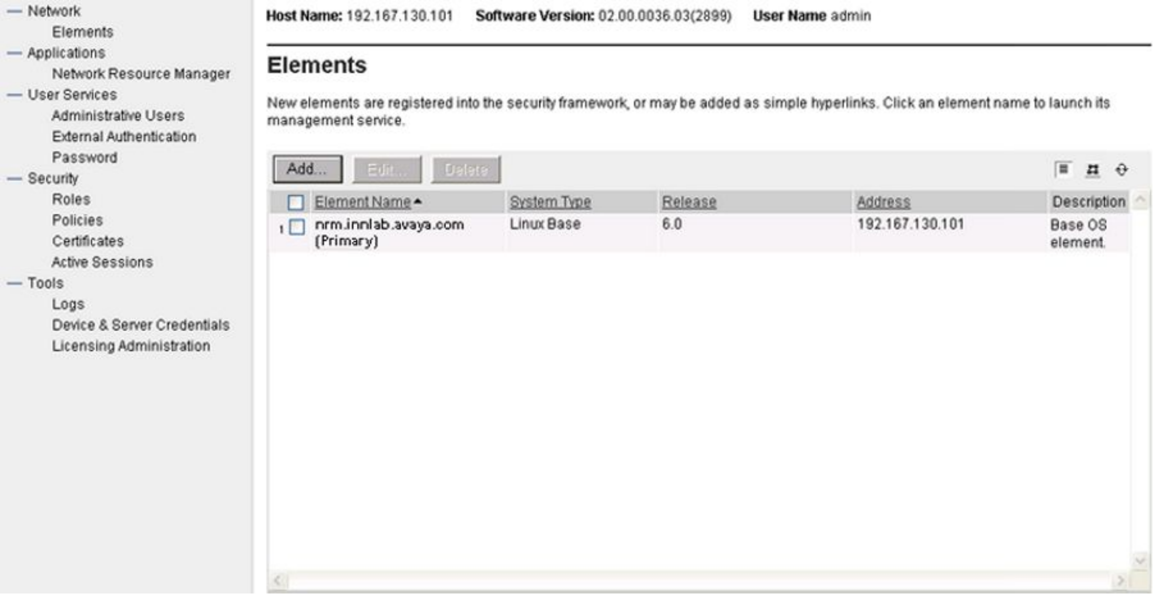
- Windows Server 2003 (all version)
- Windows Server 2008 (all versions)
- RedHat Enterprise Linux 5.2

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, Network Resource Manager (NRM), 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, device credentials, and licensing administration.

The following figure depicts the UCM main navigation page.



Host Name: 192.167.130.101 **Software Version:** 02.00.0036.03(2899) **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.

	□	Element Name ▲	System Type	Release	Address	Description
1	□	nrm.innlab.avaya.com (Primary)	Linux Base	6.0	192.167.130.101	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 (application plug-ins and bookmarks). The elements table lists all the nodes (primary/member/backup servers) installed in the network.

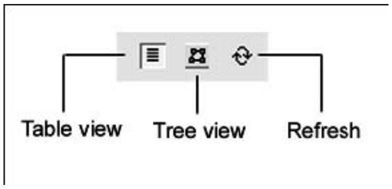
Important:

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 NRM or 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 configure an LDAP server, Radius server, or a Kerberos 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. Users 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 algorithm. 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. It allows you to register new members to the primary server.
NetworkAdministrator	Provides full privileges on the system. Provides emergency account access to any

Role name	Description
	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.
- Device and Server Credentials: You can use the Device and Server Credential Editors to set passwords, SNMP options, and other credentials for network devices. These configurations are common to all installed UCM applications, including VPFM (or VPFM Lite), EPM, and NRM.
- Licensing Administration: You can use the Licensing Administration page to add licenses, export licenses, or generate license reports. You can add a license during the installation of the application or using the Licensing Administration. If you have not provided license information during the installation of the UCM, the Licensing Administration provides the functionality of adding license after the installation of the UCM. During the installation of the application, it provides option to select only one license file. If you want to add more than one licenses for the application, the Licensing Administration lets you to add the licenses. You can export the license and keep it for future reference. For example, you can refer it when the application is reinstalled. The license report provides details about the licenses applied to the applications in the tabular format. You can save it for further use.

Chapter 4: UCM login

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

Logging onto UCM

Use the following procedure to log onto UCM.

Prerequisites

- You must install UCM.
- You require Internet Explorer 7, or Internet Explorer 8, or Firefox 2 if logging in with a client PC.

1. On the server where UCM is installed, choose Start>Programs>Avaya>UCM>Unified Communications Management.

   Or

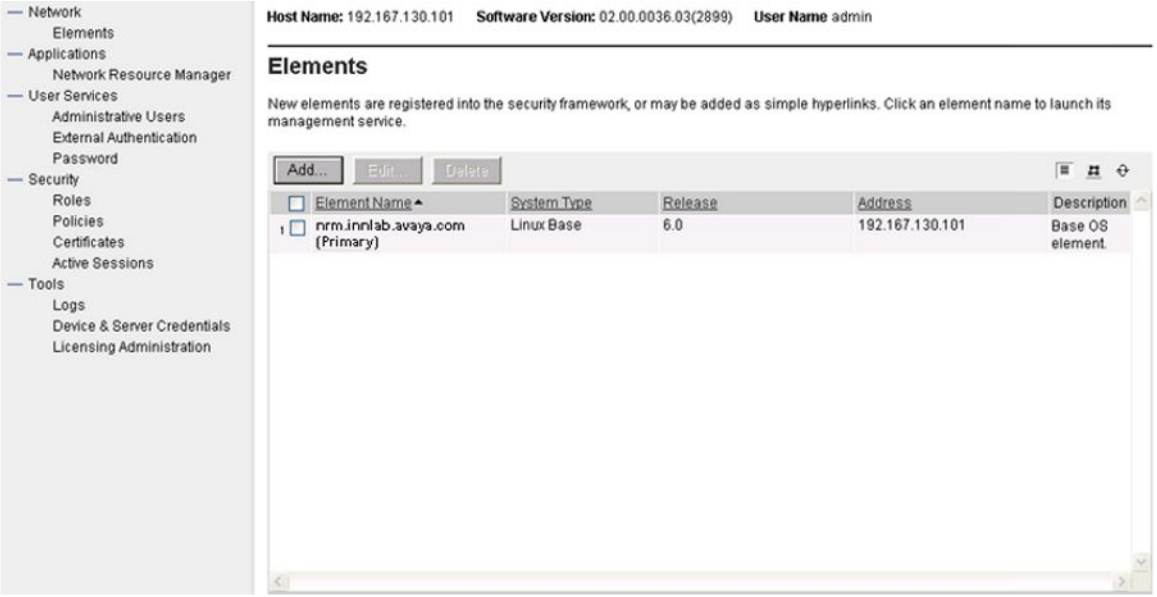
   On a client PC, point an internet browser to the FQDN of the server where UCM is installed.

   If you use localhost or IP address in the address bar of the browser, in the UCM login screen, click ‘Go to central login for Single Sign-on’ link to get to FQDN.
2. Click OK if a message appears telling you to select a security certificate.

   This certificate is pre-installed and cannot be changed.
3. When the dialog box appears, select the option to accept the certificate. This will differ 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 NRM, EPM, VPFM, or VPFM-Lite.
6. Click Log in.

   The Unified Communications Management home page appears.



Host Name: 192.167.130.101 **Software Version:** 02.00.0036.03(2899) **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.

	□	Element Name ▲	System Type	Release	Address	Description
1	□	nrm.innlab.avaya.com (Primary)	Linux Base	6.0	192.167.130.101	Base OS element.

Chapter 5: Elements management

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

Launching a managed element

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

Prerequisites

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

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

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.

Prerequisites

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

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
Name	Name of the element. The maximum length of this field is 256 characters.
Description	A brief description of the element that you are adding to the UCM.
Type	Bookmark for the element.
Server Address	URL for the bookmark element.

Editing element properties

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

Prerequisites

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

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
Name	Name of the element. The maximum length of this field is 256 characters.
Description	A brief description of the element that you are adding to the UCM.
Type	Bookmark for the element.
Release	Release number for the element.
Server Address	URL for the bookmark element.

Deleting selected elements

Perform this procedure to delete elements in the UCM network.

Prerequisites

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

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 on page 21
- External authentication scheme and authentication server configuration on page 26
- Password management on page 30

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 on page 21
- Adding a new local or external user on page 22
- Disabling an user on page 23
- Deleting an user on page 24
- Configuring user properties on page 24
- Editing user role mapping on page 25

Viewing existing users

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

Prerequisites

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

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

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

Prerequisites

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

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 an user

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

Prerequisites

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

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 disable and then click Disable.

   The Account Status for the selected user changes to Disabled.

Deleting an user

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

Prerequisites

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

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

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

Prerequisites

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

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. 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 theFull Name field, edit the name of the user.
7. Click Save.

Variable Definitions

Variable	Value
Enabled	Enables the user ID.
Disabled	Disables the user ID.
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 _).
Password	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.
Re-enter password	Reenter the new password for the user.
Full Name	Full name of the user.

Editing user role mapping

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

Prerequisites

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

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

Navigation

- Editing the authentication scheme on page 26
- Configuring authentication servers on page 27

Editing the authentication scheme

Perform this procedure to edit the authentication scheme.

Prerequisites

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

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.

Navigation

- Provisioning the LDAP server on page 27
- Provisioning the RADIUS server on page 29
- Provisioning the KERBEROS server on page 30

Provisioning the LDAP server

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

Prerequisites

- 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.

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 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	Password for root binding.

Provisioning the RADIUS server

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

Prerequisites

- 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.

1. In the navigation pane, under User Services, click External Authentication.
   The External Identity Repositories page appears.
2. In the Authentication Servers section, click Configure.
   The Authentication Servers page appears.
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

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

Prerequisites

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

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

Navigation

- Viewing password information on page 31
- Changing password on page 31

Viewing password information

Perform this procedure to determine when the password was changed and when it expires.

Prerequisites

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

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

The Password Status page appears.

Changing password

Perform this procedure to change the administrator password.

Prerequisites

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

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

   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 Allowed characters in the password are: a-zA-Z0-9{}|(),/.=[]^~_@!`; You cannot use your previous six passwords.

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 on page 33
- Policies on page 37
- Certificate management on page 43
- Active sessions on page 48

Roles

This chapter 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.

Navigation

- Viewing existing roles on page 33
- Adding roles on page 34
- Role mapping to a role assignment or edition. on page 35
- Editing a role on page 36
- Deleting roles on page 37

Viewing existing roles

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

Prerequisites

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

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

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

Prerequisites

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

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.

Navigation

- Selecting users on page 35
- Copying user assignment on page 36

Prerequisites

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

Selecting users

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

1. Click the Assigned Users tab.
2. Click Select Users to assign or edit a role to individual users. The Assigned Users (Role Name) page appears.

3. Select one or more check boxes beside the user name to grant permissions associated with this role.
4. Click Save. The Role Details (Role Name) page appears.

Copying user assignment

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

1. In the Assigned Users tab, click Copy All From.

   The Permission Mapping (all Permissions for Role Name) page appears.
2. Select a role from the Copy from Role list.

   The Role Details (Role Name) page appears.
3. Click Save.

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

Editing a role

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

Prerequisites

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

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

Perform this procedure to delete roles.

Prerequisites

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

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

Navigation

- Viewing security policies on page 37
- Editing password policies on page 38
- Editing session properties on page 40
- Security settings on page 41
- Editing the Single Sign-on Cookie Domain on page 42

Viewing security policies

Perform this procedure to view the security policies.

Prerequisites

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

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

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.

Prerequisites

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

1. In the navigation pane, under Security, click Policies. The Policies page appears.
2. In the Password Policy (for locally authenticated users) section, click Edit. The Password Policy page appears.
3. In the Aging section, select the Aging check box.
4. In the Expiration period field, enter the number of days for the password to expire.
5. 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.
6. 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.
7. In the History section, select the History check box

8. In the Previous passwords blocked field, enter the number for the number of passwords to remember in history.
9. In the Strength section, in the Minimum Total Length field, enter a number for the minimum number of total characters for the password.
10. 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.
11. In the Upper case field, enter the minimum number of uppercase characters for the password.
12. In the Numeric case field, enter the minimum number of numeric characters for the password.
13. In the Special case field, enter the minimum number of special characters for the password.
14. In the Lockout section, select the Lockout check box.
15. In the Consecutive Invalid Login Attempts field, enter a number for failed attempts from 1 to x.
16. In the Interval for Consecutive Invalid Login Attempts field, enter the interval in number of minutes from 0 to x for consecutive invalid logon attempts.
17. In the Lockout Time field, enter the number of minutes from 0 to x until the account is unlocked.
18. 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.

Variable	Value
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.
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

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

Prerequisites

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

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 provides a customizable logon banner that appears after a user logs on to the system. The customizable banner is intended for use by customers that have security policies that require network equipment to display a specific message to users when they log on.

Navigation

Editing login warning banner on page 42

Prerequisites

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

Editing login warning banner

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

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.

Editing the Single Sign-on Cookie Domain

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.

Prerequisites

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

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, users must clear the existing UCM related cookies from the cache in the Internet browser for all users.

Certificate management

This chapter 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.

Navigation

Adding a certificate

Perform this procedure to add a certificate.

Prerequisites

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

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 that in to 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

Perform this procedure to enable trust for a certificate.

Prerequisites

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

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

Perform this procedure to disable trust for a certificate.

Prerequisites

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

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

Perform this procedure to delete a certificate.

Prerequisites

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

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

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

Prerequisites

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

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

Perform this procedure to download the Private Certificate Authority details.

Prerequisites

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

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

Perform this procedure to revoke a certificate.

Prerequisites

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

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

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

Prerequisites

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

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. Click the Private Certificate Authority tab.
4. In the Certificate Revocation List (CRL) details section, click Get CRL.

   The File Download window appears.
5. Click Save.

Active sessions

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

Navigation

- Viewing active sessions on page 48
- Terminating active sessions on page 48

Viewing active sessions

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

Prerequisites

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

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

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

Prerequisites

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

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 51
- Device and Server Credentials Editor configuration on page 52
- License administration on page 56

Logs

This chapter 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.

Navigation

Viewing log files on page 51

Prerequisites

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

Viewing log files

Perform this procedure to view log files in the UCM.

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.

Device and Server Credentials Editor configuration

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

Avaya Unified Communication Management (UCM) applications use SNMP v1/v2/v3, Telnet, CIM/XML, SSH, FTP, RLogin, or SSH protocols for communication with network infrastructure devices such as routers. The protocol required depends on the type of device. It 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 (IP address) or for a range of IP addresses. See the documentation for your network devices to determine which protocols they 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 can be managed in the Device and Server Credentials Editor.

Table 1: Device and Server Credentials Editor fields

Credential information	Attributes
Name	Credential set name
IP Address or Range	Device/Server IP Address or Address Range
SNMPv1/v2	Read Community Write Community
SNMPv3	SNMPv3 User Authorization Protocol (MD5, SHA1, None) Authorization Key Privacy Protocol (AES128, DES, 3DES, None) Privacy Key
Telnet	Telnet User name Telnet Password Telnet Port
FTP	FTP User name FTP Password FTP Port
SSH	SSH User name SSH Password SSH Port
CIM-XML	CIM User name CIM Password
RLogin	RLogin User name RLogin Password
Windows Server	Windows User name Windows Password Windows Domain

- Adding a credential set on page 53
- Deleting a credential set on page 54
- Editing a credential set on page 54
- Importing a credential set on page 55
- Exporting a credential set on page 55
- Refreshing the credential set list on page 56

Adding a credential set

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.

Prerequisites

You must have installed the UCM. The Unified Communications Management is installed when you install a UCM application (VPFM, VPFM Lite, EPM, or NRM). For more information, see the installation guide for UCM application.

Ensure that you are logged on to UCM as administrator.

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

   The Device and Server Credentials Editor page appears.
2. Click Add Credential Set.

   The Add Credential Set dialog box appears.
3. In the Set Name field, enter the Set Name.
4. In the IP Address/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 61.
5. Add device credential information on the appropriate tab. For more information about the available tabs, see Table 1: Device and Server Credentials Editor fields on page 52.

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

The credential set appears in the panel.

Deleting a credential set

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

Prerequisites

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

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

Editing a credential set

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

Prerequisites

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

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 change.
3. Click Edit Credential Set.
   The Edit Credential Set dialog box appears.
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.
6. Click Save.

   All specified IP addresses are validated after saving the changes.

Importing a credential set

Perform this procedure to import the credential set to the UCM.

Prerequisites

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

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

   The Device and Server Credentials Editor page appears.
2. Click Import Credentials button.

   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

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

Prerequisites

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

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

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.

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 chapter provides information about adding a license file, exporting a license file, generating a license report, and refreshing license information.

Navigation

- Adding license file on page 56
- Exporting license file on page 57
- Refreshing license information on page 57

Adding license file

Perform this procedure to add a license to an application.

Prerequisites

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

1. In the navigation pane, under Tools, click Licensing Administration.
   The Licensing Administration page appears.
2. Click Add License. The Add License dialog box appears.
3. In the License field, browse to locate the license file.
4. Click Add.

Exporting license file

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.

Prerequisites

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

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.

Refreshing license information

Perform this procedure to refresh the license information.

Prerequisites

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

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)
- license files
- 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 59
- Restoring UCM files on page 60

Backing up UCM files

Use the following procedure to backup UCM files.

Prerequisites

- You must be logged on to the UCM server as and "Administrator" (in a Windows environment), or as "root" (in Linux).
- 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 1.0 to 1.1, but not from 1.0 to 2.0.

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.

1. From the command prompt, run the following script:C:\Program Files\Avaya\UCM \backupAllData.bat

   OR

   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

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

Prerequisites

- Ensure that you must have logged on to the UCM server as and "Administrator" (in a Windows environment), or as "root" (in Linux).
- 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 1.0 to 1.1, but not from 1.0 to 2.0.

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.

1. From the command prompt, run the following script:C:\Program Files\Avaya\UCM \restoreAllData.bat

   OR

   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 61
- Valid IP address ranges on page 62
- IP address format limitations on page 62

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)