System Manager Common Services Fundamentals

NN48014-100
Issue 06.01
August 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

Related Links

Purpose on page 6
Related resources on page 6

Purpose

This document provides information about the Avaya Aura® System Manager 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 System Manager-Common Services (SMGR-CS).

Related Links

Introduction on page 6

Related resources

Related Links

Introduction on page 6
Documentation on page 6
Training on page 8
Viewing Avaya Mentor videos on page 8
Support on page 8

Documentation

See the following related documents:

Title	Purpose	Link
Avaya Configuration and Orchestration Manager Administration	Administration	http://support.avaya.com
Avaya Configuration and Orchestration Manager Fundamentals	Fundamentals	http://support.avaya.com
Avaya Configuration and Orchestration Manager Installation	Installation	http://support.avaya.com
Avaya Bulk Configuration Manager Fundamentals	Fundamentals	http://support.avaya.com
Avaya Virtualization Provisioning Service Installation and Commissioning	Installation	http://support.avaya.com
Avaya Virtualization Provisioning Service Fundamentals	Fundamentals	http://support.avaya.com
Avaya Virtualization Provisioning Service Interface	Interface	http://support.avaya.com
Installation Avaya IP Flow Manager 2.1	Installation	http://support.avaya.com
Fundamentals Avaya IP Flow Manager 2.1	Fundamentals	http://support.avaya.com
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
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

Related Links

Related resources on page 6

Training

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

Related Links

Related resources on page 6

Viewing 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.

Procedure

- To find videos on the Avaya Support website, go to support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to 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 website.

    Note:

    Videos are not available for all products.

Related Links

Related resources on page 6

Support

Go to 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.

Related Links

Related resources on page 6

Chapter 2: New in this release

The following sections detail what is new in System Manager – Common Services (SMGR-CS), (NN48014-100), which supports the following applications:

- Avaya Configuration and Orchestration Manager (COM) Release 3.1
- Avaya IP Flow Manager (IPFM) Release 2.1
- Virtualization Provisioning Service (VPS) Release 1.1
- Avaya Visualization Performance and Fault Manager (VPFM) Release 3.0.3

Features

See the following section for information about feature changes.

Architecture

Prior releases of COM, IPFM, VPS, and VPFM applications were deployed on the Unified Communications Management-Common Services (UCM-CS) platform. COM 3.1, VPS 1.1, IPFM 2.1, and VPFM 3.0.3 are deployed on the System Manager-Common Services (SMGR-CS) platform.

As a result of Avaya's strategic decision to use a single platform for all J2EE applications, the System Manager (SMGR) platform was chosen. SMGR is a J2EE compliant platform already being used in Avaya's Aura products. All other SMGR applications migrate from the UCM-CS platform to SMGR-CS platform. SMGR-CS is a scaled down SMGR platform that contains only those platform services required for COM, IPFM, VPS, and VPFM applications. These applications that move to SMGR platform further provides a common integrated management solution for Avaya voice and data customers.

Browser support

SMGR-CS supports the following browsers:

- Internet Explorer 8.x, 9.x, 10.x
- Mozilla Firefox 19.0, 20.0, 21.0

For more information about browser support, see the applicable SMGR-CS application documentation.

Platform support

SMGR-CS is supported on the following platforms:

- Windows Server 2008 R2 (64-bit, standard and enterprise flavors)
- Red Hat Enterprise Linux v5.6 or v5.7 (both 64-bit only)

For more information about platform support, see the applicable SMGR-CS application documentation.

FQDN support is increased

With the SMGR-CS platform, the FQDN can be a maximum of 63 characters.

SAML Configuration support

SMGR-CS supports SAML Configuration. For more information about SAML Configuration, see SAML Configuration on page 26.

Other changes

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

Document title change

Avaya Visualization Performance and Fault Manager Common Services Fundamentals Unified Communications Management is renamed *System Manager Common Services Fundamentals*.

Chapter 3: SMGR overview

This chapter provides an overview of the System Manager-Common Services (SMGR-CS) for the following applications: IP Flow Manager (IPFM) Release 2.1, Configuration and Orchestration Manager (COM) Release 3.1, Virtualization Provisioning Service (VPS) Release 1.1, and Visualization Performance and Fault Manager (VPFM) and VPFM-Lite Release 3.0.3.

Introduction

The Avaya Aura® System Manager (SMGR) solution provides you with an intuitive, common interface to manage and run managed elements. SMGR is a container that stores several system management elements in a single repository. You have access to all network system management elements under the SMGR 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 SMGR Security Services to simplify security control for managed elements and system management applications. SMGR Security Services manages secure access to Web applications and provides authentication, authorization and accounting (AAA) with a single common service. SMGR secures the delivery of essential identity and application information.

With SMGR-Common Services (SMGR-CS), 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 SMGR-CS, 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

SMGR-CS is supported on the following platforms:

- Windows Server 2008 R2 (64–bit)
- RedHat Enterprise Linux v5.6 or v5.7 (64–bit)
- VMware ESXi (Windows 2008 or RHEL operating systems)
- Microsoft HyperV (Windows 2008 or RHEL operating systems)

Supported browsers

SMGR-CS supports the following browsers:

- Firefox 19, 20, and 21
- Internet Explorer 8.x, 9.x, and 10.x

For more information about supported platforms and browsers, see the applicable SMGR-CS application documentation.

Chapter 4: SMGR-CS login

The following section describes how to launch and log on to SMGR-CS.

Related Links

Logging on to SMGR-CS on page 14
Login information for users with user name admin on page 15

Logging on to SMGR-CS

Before you begin

Obtain a user account to log on to the SMGR-CS web interface. If you do not have a user account, go to the Avaya support website at http://support.avaya.com to create your account.

About this task

SMGR-CS web console is the main interface of Avaya Aura® System Manager. To perform any tasks, you must log on to SMGR-CS web console.

Important:

On SMGR-CS web console, do not use the back arrow on the top-left corner of the browser to navigate to the previous page. If you click the back arrow, the system might exhibit an inconsistent and unexpected behavior.

Use the following procedure to log on to SMGR-CS.

Procedure

1. On the Web browser, enter the System Manager URL `https://<FullyQualified Domain Name>/SMGR`.
2. In the **User ID** field, enter the user name.
3. In the **Password** field, enter the password.
4. Click **Log On**.

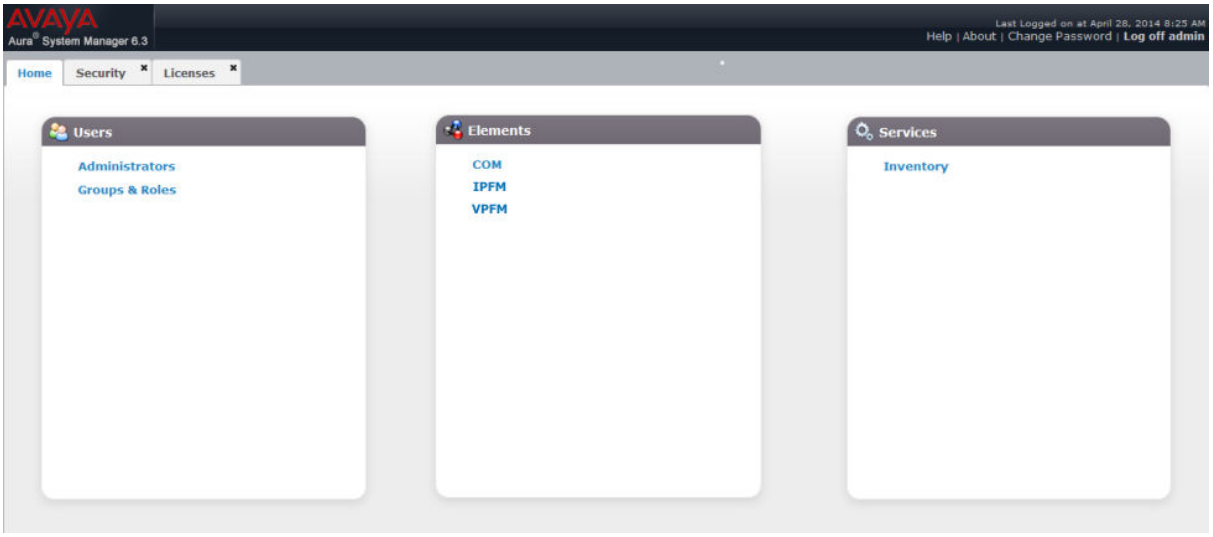
   The system validates the username and password with the SMGR-CS user account. Depending on the validity, the system displays one of the following screens:

   - If the username and password match, the system displays the System Manager home page with the System Manager *version_number*. The System Manager home page displays the navigation menu. The menu provides access to shared services to perform

various operations that System Manager supports. The tasks you can perform depends on your user role.

- If the username and password does not match, System Manager displays an error message and prompts you to re-enter the user name and password.

The following figure shows the SMGR-CS web console page.



Related Links

SMGR-CS login on page 14

Login information for users with user name admin

This login information applies only to users with user name admin.

- After installation, when you log on to the system for the first time, enter admin123 as the default password.

  You must change the password when you log on to the system using the default password.

- If you gain access to SMGR-CS using the IP address, and you log on to the system as admin for the first time, click **Change Password** to change the password.

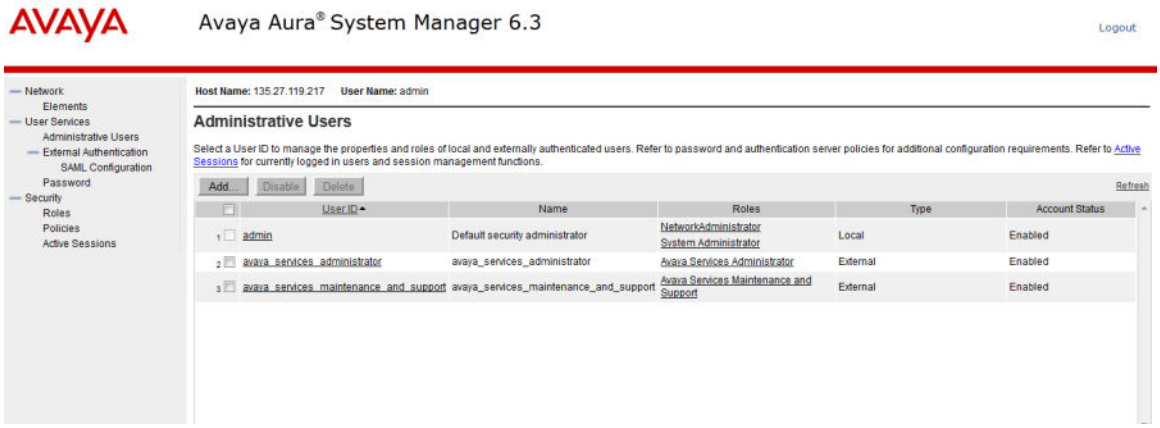
Related Links

SMGR-CS login on page 14

Chapter 5: Administrative Users

From the System Manager web console, click **Administrators** in the Users section. The SMGR-CS navigation tree is located on the left side of the Administrative Users page.

The following figure shows the Administrative Users page.



The root level items of the SMGR-CS navigation tree are:

- Network: The elements that are within the scope of the SMGR-CS security framework. You can define and browse to systems and servers within this secure network.
- User Services: User-related objects and identity management.
- Security: SMGR-CS Security Services objects and security policy management.

Related Links

Network on page 16
User services on page 20
Security on page 31

Network

This section provides information about managing the elements in the System Manager Common Services (SMGR-CS) network.

Related Links

Administrative Users on page 16

Elements management on page 17

Elements management

The Elements page 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, click **Reset** to return to the original list. The elements table lists all the nodes (primary/member) installed in the network.

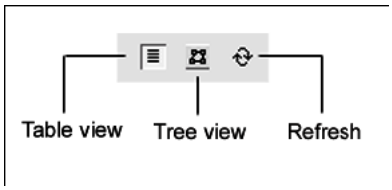
Important:

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 SMGR-CS 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 SMGR 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 displays in the navigation mode, only the elements that the administrator is authorized to access display. 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 Configuration and Orchestration Management 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 SMGR-CS main navigation page to change your view. To update the list, click **Refresh**.



Related Links

Launching a managed element

Before you begin

- You must have logged on to the SMGR 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 displays.

2. In the **Element Name** column, click an item. The management application for the element displays 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 SMGR security framework.

Adding an element

Before you begin

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

About this task

Perform this procedure to add or register an element into the SMGR network. Using the SMGR, 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 displays.

2. On the **Elements** page, click **Add**.

The Add New Element page displays.

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 display in the Elements pane.

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.
Address	URL for the bookmark element.
Description	A brief description of the element that you are adding to the SMGR-CS.

Editing element properties

Before you begin

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

About this task

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

Procedure

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

   The Elements page displays.
2. Select the Element name check box for which you want to edit the details, and then click **Edit**.

   The Elements Details page displays.
3. Make changes to the Elements fields as required.
4. In the Release field, click **Edit**. The Release page displays.
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.
Address	URL for the bookmark element.
Description	A brief description of the element that you are adding to the SMGR-CS.

Deleting selected elements

Before you begin

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

About this task

Perform this procedure to delete elements in the SMGR network.

Procedure

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

   The Elements page displays.

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

   The Delete Elements page displays.

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

User services

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

In the User Services branch of the SMGR-CS navigation tree, you can select the following items:

- Administrative Users: 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 SMGR-CS. The internal Open LDAP is the default authentication service used if you do not configure the external authentication server.

- SAML Configuration: Customize configuration on the Hosted Service Provider for external SAML authentication and on the Hosted Identity Provider for SAML authentication in the domain.

- Password: View the status for a password or to change the password.

Related Links

Administrative Users on page 16
Users administration on page 21
External authentication scheme and authentication server configuration on page 26
Password management on page 29

Users administration

This section provides information about managing users.

The administrator can perform the user management tasks required to manage users within the SMGR-CS.

Related Links

User services on page 20
Viewing existing users on page 21
Adding a new local or external user on page 22
Disabling a user on page 23
Deleting a user on page 23
Configuring user properties on page 24
Editing user role mapping on page 25

Viewing existing users

Before you begin

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

About this task

Perform this procedure to view the users who are configured for SMGR-CS access.

Procedure

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

   The Administrative Users page displays.

   The Administrative Users page lists users configured for access to SMGR-CS.

2. View the information for existing users.

Related Links

Users administration on page 21

Adding a new local or external user

Before you begin

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

About this task

Perform this procedure to create a new user of SMGR-CS and to assign roles to the new user.

Procedure

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

   The Administrative Users page displays.
2. Click **Add**. The Add New Administrative User page displays.
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 SMGR-CS 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 displays.
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 displays in the users list.

Related Links

Users administration on page 21
Variable definitions on page 22

Variable definitions

Variable	Value
User ID	ID of the user. This field can accept (1-31) characters and allows characters, a-z, A-Z, 0-9, ., @, - and _.
Authentication type	Type of user: Local user or External user.
Full Name	Full name of the user.

Variable	Value
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.

Related Links

Adding a new local or external user on page 22

Disabling a user

Before you begin

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

About this task

Perform this procedure to disable a user in the SMGR-CS 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.

Related Links

Users administration on page 21

Deleting a user

Before you begin

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

About this task

Perform this procedure to delete a user in the SMGR-CS network.

Procedure

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

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

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

Important:

Users cannot delete their own account.

Related Links

Users administration on page 21

Configuring user properties

Before you begin

- Ensure that you are logged on to the SMGR-CS 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**.

Related Links

Users administration on page 21
Variable definitions on page 24

Variable definitions

Variable		Value
User status	Enabled	Enables the user ID.
	Disabled	Disables the user ID.
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.
Authentication type	Local	The user is authenticated by the default Open LDAP service.

Variable		Value
	External	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.
User ID		ID of the user. This field can accept (1-31) characters and allows characters, a-z, A-Z, 0-9, ., @, - and _.

Related Links

Configuring user properties on page 24

Editing user role mapping

Before you begin

- Ensure that you are logged on to the SMGR-CS 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 displays.

2. Under **User ID**, click the User ID to which you want to set properties and assign roles.

   The Users Details (admin) page displays.

3. In the **Roles** section, click **Select Roles**.

   The User Roles page displays 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 displays.

5. Click **Save**.

Related Links

Users administration on page 21

External authentication scheme and authentication server configuration

This section provides information about configuring external authentication scheme and authentication server for SMGR-CS.

The SMGR-CS 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.

Related Links

User services on page 20
SAML Configuration on page 26
Editing the authentication scheme on page 27
Configuring authentication servers on page 27

SAML Configuration

The system automatically configures SMGR-CS as Hosted Service Provider during the installation or upgrade of SMGR-CS.

However, you can modify the configuration using the following procedure.

As an administrator, you can enable or disable SAML authentication in SMGR-CS from the SAML Configuration page.

Related Links

External authentication scheme and authentication server configuration on page 26
Editing SAML Hosted Service Provider properties on page 26

Editing SAML Hosted Service Provider properties

Procedure

1. In the navigation pane, click **User Services** > **External Authentication** > **SAML Configuration**.
2. Click **Edit**.
3. On the SAML Hosted Service Provider page, perform the following:
   a. Select the **NameID as UserID** check box.
   b. In the **Attribute Used as UserID** field, enter the name of the attribute that you want to use as the login ID of the user in SMGR-CS.

c. In the **Mapped Attributes** field, enter an attribute that you require to map between R-IDP and H-SP for a user.

4. Click **Save**.

   For more information about configuring SAML authentication, see *Administering Avaya Aura® System Manager*.

Related Links

SAML Configuration on page 26

Editing the authentication scheme

Before you begin

- Ensure that you are logged on to the SMGR-CS 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 displays.

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

   The Authentication Scheme page displays.

3. Select the required authentication scheme, and then click **Save**.

Related Links

External authentication scheme and authentication server configuration on page 26

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.

Related Links

External authentication scheme and authentication server configuration on page 26
Provisioning the LDAP server on page 28

Provisioning the RADIUS server on page 28
Provisioning the KERBEROS server on page 29

Provisioning the LDAP server

Before you begin

- Ensure that you are logged on to the SMGR-CS 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 displays.

2. In **Authentication Servers** section, click **Configure**.

   The Authentication Servers page displays.

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**.

Related Links

Configuring authentication servers on page 27

Provisioning the RADIUS server

Before you begin

- Ensure that you are logged on to the SMGR-CS 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**.

Related Links

Configuring authentication servers on page 27

Provisioning the KERBEROS server

Before you begin

- Ensure that you are logged on to the SMGR-CS 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 displays.

2. In **Authentication Servers** section, click **Configure**.

   The Authentication Servers page displays.

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**.

Related Links

Configuring authentication servers on page 27

Password management

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

Related Links

User services on page 20
Viewing password information on page 30
Changing password on page 30

Viewing password information

Before you begin

- Ensure that you are logged on to the SMGR-CS 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 displays.

Related Links

Password management on page 29

Changing password

Before you begin

- Ensure that you are logged on to the SMGR-CS 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**.

   The Password Status page displays.

2. Click **Change Password**.

   The Change Password page displays.

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**.

Related Links

Password management on page 29

Security

This section 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.

In the Security branch of the SMGR-CS 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. For more information about Roles, see Managing roles on page 45.
- Policies—Configure the authentication scheme and authentication servers, establish password policies, and edit security settings. For more information about Policies, see Policies on page 35.
- Active Sessions—Display all users who are currently logged on and the session time for each user. For more information about Active Sessions, see Active sessions on page 42.

Default roles

The SMGR-CS 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.

Related Links

Administrative Users on page 16
Roles on page 32
Policies on page 35
Active sessions on page 42

Roles

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

Related Links

Security on page 31
Viewing existing roles on page 32
Adding roles on page 32
Role mapping to a role assignment or edition on page 34
Selecting users on page 34
Copying user assignment on page 34
Editing a role on page 35
Deleting roles on page 35

Viewing existing roles

Before you begin

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

About this task

Perform this procedure to view the existing roles in the SMGR-CS.

Procedure

1. In the navigation panel, under **Security** , click **Roles**.
2. On the Roles page, select the role that you require to view.

   The system displays the role name, description, number of users, and the elements to which you can gain access using the role.

Related Links

Roles on page 32

Adding roles

Before you begin

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

About this task

Perform this procedure to add new role for specific access control policies in the SMGR-CS.

Procedure

1. In the navigation panel, click **Security** > **Roles**.

2. On the Roles page, select an existing role, and perform one of the following steps:
   - Click **New**.
   - Right-click and select **New**.

   The role that you selected becomes the parent of the role that you create. The permissions available to the new role limit to the permissions of the parent role.
3. On the Add New Role page, fill in the **Role Name** and **Role Description** fields.
4. Click **Commit and Continue**.

   The system displays the Role Details page.
5. On the **Element/Service Permissions** tab, click **Add mapping** to define permissions for a role.

   Alternatively, click **Copy All From** to copy all the permissions on all types of elements or services from an existing role.
6. Perform one of the following:
   - Perform the following:
     a. Select a group from the **Group Name** field.

        Ensure that you create a group before you select the group.
     b. (Optional) Select an element type from the Element or Resource **Type** field.
   - Perform the following:
     a. Leave the **Group Name** field blank, and select an element from the **Element or Resource Type** field.

        Based on the element type that you select, the system displays the available elements in the **Element or Resource Instance** field.
     b. In the **Element or Resource Instance** field, select in individual element or select **All**.
7. Click **Next**.

   The title of the Permission Mapping page displays the element type that you selected.
8. On the Permission Mapping page, modify the permissions that are available for this role as appropriate.

   The system displays permissions that are available for the parent of the role that you created. The system displays the permissions that are not assigned to the parent role as read-only. As an administrator, you can deny, modify, or view the permissions associated with a role.
9. Click **Commit**.

   The system displays the Role Details page with the permissions that you selected.
10. Click **Commit** to confirm your settings.

Related Links

Roles on page 32

Role mapping to a role assignment or edition

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.

Related Links

Roles on page 32

Selecting users

About this task

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

Procedure

1. On SMGR-CS Web Console, click **Users** > **Groups & Roles**.

   You can also access Roles from the navigation pane, under **Security** > **Roles**.
2. In the left navigation pane, click **Roles**.
3. On the Roles page, select the role that you require.
4. Click the **Assigned Users** tab.
5. Click **Select Users** to assign or edit a role to individual users.
6. Select one or more check boxes beside the user name to grant permissions associated with this role.
7. Click **Save**.

Related Links

Roles on page 32

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, click **Security** > **Roles**.
2. On the Roles page, select the role that you require.
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 displays. You can use this page to view the new permissions for that role.

Related Links

Roles on page 32

Editing a role

Before you begin

- Ensure that you are logged on to the SMGR-CS 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 left navigation pane, click **Security** > **Roles**.
2. On the Roles page, select the role that you require.
3. In the **Role Name** column, click a role name item to edit the description.

   The Role Details (Role Name) page displays.
4. In the **Description** field, edit the information as required.
5. Click **Save**. The Role page displays.

Related Links

Roles on page 32

Deleting roles

Before you begin

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

About this task

Perform this procedure to delete roles.

Procedure

1. In the navigation panel, click **Security** > **Roles**.
2. On the Roles page, select the role that you require.
3. Select the **Role Name** check box that you want to delete, and then click **Delete**.
4. After you are prompted to confirm the deletion of the Role Name, click **Delete**.

Related Links

Roles on page 32

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.

Related Links

Viewing security policies

Before you begin

- Ensure that you are logged on to the SMGR-CS 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 displays.

2. View the policy settings currently in the SMGR-CS.

Related Links

Policies on page 35

Editing password policies

Before you begin

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

About this task

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

An invalid logon message displays 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.
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.

Variable	Value
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 SMGR-CS 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 displays.
2. In the **Session Properties** section, click **Edit**.

   The Session Properties page displays.
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 SMGR-CS 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.

Prerequisites

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

Related Links

Policies on page 35

Editing login warning banner

About this task

Perform this procedure to customize the message for the login warning banner in SMGR-CS.

Procedure

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

   The Policies page displays.

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

   The Security Settings page displays.

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 SMGR-CS Security Policies web page.

Related Links

Policies on page 35
Adding a new image for a customized interface on page 40
Editing a customized interface on page 41
Removing an image from a customized interface on page 41

Adding a new image for a customized interface

Before you begin

Ensure that you are logged on to the SMGR-CS 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 SMGR-CS.

Related Links

Customized interface on page 40

Editing a customized interface

Before you begin

Ensure that you are logged on to the SMGR-CS 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 SMGR-CS.

Removing an image from a customized interface

Before you begin

Ensure you are logged on to the SMGR-CS 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 SMGR-CS.

Related Links

Customized interface on page 40

Editing the Single Sign-on Cookie Domain

Before you begin

- Ensure that you are logged on to the SMGR-CS 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 displays.

2. In the Single Sign-on Cookie Domain section, click **Edit**.

   The Edit Domain Name page displays.

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 SMGR-CS 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.

Active sessions

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

Related Links

Security on page 31
Viewing active sessions on page 42
Terminating active sessions on page 43

Viewing active sessions

Before you begin

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

About this task

Perform this procedure to view active sessions in the SMGR-CS and session time for the user.

Procedure

1. In the navigation pane, under **Security**, click **Active Sessions**. The Active Sessions window displays.

   The sessions are sorted in the User ID column.

2. View the active sessions currently in the SMGR-CS.

Terminating active sessions

Before you begin

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

About this task

Perform this procedure to terminate the active sessions in the SMGR-CS.

Procedure

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

   The Active Sessions page displays.

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 6: Managing groups

From the SMGR-CS web console, click **Groups & Roles** in the Users section. The Groups & Roles page displays.

Related Links

Group management on page 44
Manage resources on page 45
Managing roles on page 45

Group management

Group and Lookup Service (GLS) in SMGR-CS is a shared service that provides group administration and lookup service for managed resources. GLS encapsulates the mechanisms for creating, modifying, searching, and deleting groups and group memberships. Using GLS, you can group resources any way that works best for the business, such as, organizing resources by location, organization, and function.

With GLS, you can assign different roles to the administrators and allow the administrators to perform only limited tasks on group of resources from SMGR-CS Web Console. For example, you can create a group of users so that a user from the current group or a different group might manage only the users which are part of the current group.

GLS supports group administration for common resources shared across elements such as, roles and users, and unshared element-specific resources.

GLS maintains a repository of groups and memberships from SMGR-CS and other applications that use the GLS service. GLS synchronizes the resources with other Avaya applications and services that are managing these resources. GLS maintains resource IDs and their group memberships. Using GLS, you can search one or more resources based on their attribute values and obtain resource attributes for one or a set of resources

Using GLS, you can perform the following operations:

- Create groups
- View and modify groups
- Create duplicate groups by copying properties of existing groups
- Move groups across hierarchies
- Assign and remove resources for groups

- Delete groups
- Synchronize groups

As a shared service, GLS reduces the time and effort involved by defining reusable groups of managed resources that more than one application or service requires. For example, you can use the group of resources to assign permissions through Role Based Access Control (RBAC).

For more information about managing groups, see *Administering Avaya Aura® System Manager*.

Related Links

Managing groups on page 44

Manage resources

SMGR-CS contains different types of resources such as users and roles. You can view and filter these resources based on the search criteria. You can also add resources of the same or different types in a group.

For more information about managing resources, see *Administering Avaya Aura® System Manager*.

Related Links

Managing groups on page 44

Managing roles

You can perform various role management tasks required to manage roles within the SMGR-CS. This feature provides group-level authentication functions and element permissions.

Roles management tasks can also be performed in **Administrative Users** > **Security** > **Roles**.

For more information about managing roles, see *Administering Avaya Aura® System Manager*.

Related Links

Managing groups on page 44

Chapter 7: Launch SMGR-CS applications

The SMGR-CS web console page displays the installed applications in the Elements section. Click the link to launch the application.

Chapter 8: Inventory

From the SMGR-CS web console, click **Inventory** in the Services section. The Inventory page displays.

Inventory maintains a repository that records elements deployed on SMGR-CS, including their runtime relationships. An element in the inventory refers to a single or clustered instance of a managed element. Inventory provides a mechanism for creating, modifying, searching, and deleting elements and the access point information from the repository. Inventory retrieves information about elements that are added or deleted from the repository.

Inventory integrates the adopting products with the common console of SMGR-CS. Through Inventory, elements can provide a link that can redirect to the Web page of the element manager. Such links appear for only specific element types.

For more information about elements, see *Administering Avaya Aura® System Manager*.

Related Links

Device and Server Credentials tool on page 47

Device and Server Credentials tool

All applications can access the Device and Server Credentials tool to retrieve access credentials for devices.

Related Links

Inventory on page 47
Accessing the Device and Server Credentials tool on page 48
Device and Server Credentials Editor configuration on page 48
Adding a credential set on page 50
Deleting a credential set on page 50
Editing a credential set on page 51
Importing a credential set on page 51
Exporting a credential set on page 52
Refreshing the credential set list on page 52

Accessing the Device and Server Credentials tool

Before you begin

- Ensure that you are logged on to SMGR-CS as Administrator.

About this task

Perform the following procedure to access the Device and Server Credentials tool.

Procedure

1. In the SMGR-CS web console, under Services, click **Inventory**.

   The Inventory page displays.

2. Click **Device and Server Credentials**.

   The Device and Server Credentials Editor Configuration page displays.

Related Links

Device and Server Credentials tool on page 47

Device and Server Credentials Editor configuration

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

SMGR-CS 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 SMGR-CS 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, the application uses these credentials to discover network devices and servers.

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

Credential information	Attributes
	Write Community
SNMPv3	SNMPv3 User Authorization Protocol (MD5, SHA1, None) Authorization Key Privacy Protocol (AES128, DES, 3DES, None Privacy Key Context Management User Generic User
Telnet	Telnet User Password Port
CIM	CIM User Password
FTP	FTP User Password Port
SSH	SSH User Password Port
NetConf	Netconf User Password Port Management User
RLogin	RLogin User Password
Windows Server	Windows User Password Domain

Related Links

Device and Server Credentials tool on page 47

Adding a credential set

Before you begin

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

About this task

Perform this procedure to add a new credential set to SMGR-CS. 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 displays.

Procedure

1. Access the Device and Server Credentials tool. See Accessing the Device and Server Credentials tool on page 48.
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 61.
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 48.

   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 SMGR-CS as an administrator.

About this task

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

Procedure

1. Access the Device and Server Credentials tool. See Accessing the Device and Server Credentials tool on page 48.
2. Click the credential set or sets that you want to remove.

To select multiple credential sets at once, press and hold the CTRL key and then click 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 SMGR-CS 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. Access the Device and Server Credentials tool. See Accessing the Device and Server Credentials tool on page 48.
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 48
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 SMGR-CS as an administrator.

About this task

Perform this procedure to import the credential set to SMGR-CS.

Procedure

1. Access the Device and Server Credentials tool. See Accessing the Device and Server Credentials tool on page 48.
2. Click **Import Credentials**.

The Import Credential Set(s) window displays.

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 SMGR-CS as an administrator.

About this task

Perform this procedure to export credential set from the SMGR-CS to a local XML file.

Procedure

1. Access the Device and Server Credentials tool. See Accessing the Device and Server Credentials tool on page 48.
2. Click **Export Credentials**.

   The Export Credential Set(s) window displays.
3. Click **Export**.

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

   The File Download window displays.
4. Click **Save**.

Refreshing the credential set list

Before you begin

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

About this task

Perform this procedure to refresh the credential set list.

Use the manual refresh command to ensure that the information that displays 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. Access the Device and Server Credentials tool. See Accessing the Device and Server Credentials tool on page 48.

2. Click **Refresh** located at the bottom of the page.

   The list of available credential sets is refreshed from the SMGR-CS database.

Chapter 9: Licenses

SMGR-CS applications, such as COM, IPFM, VPS, and VPFM require a license to operate. Licenses are obtained through the FlexLM licensing service.

You require the License Authorization Code (LAC) for the software you want to license. Navigate to the **Electronic Licensing Portal** : http://www.avayadatalicensing.com.

Note:

When you upgrade an application on a VM environment, SMGR 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.

For more information about obtaining a FlexLM license for SMGR-CS applications, see the following documents:

- COM/VPS: *Avaya Configuration and Orchestration Manager Installation* (NN47226-300)
- IPFM: *Installation Avaya IP Flow Manager 2.1* (NN48015-300)
- VPFM: *Installing the Avaya Visualization Performance and Fault Manager* (NN48014-300)

Related Links

Installing a license file on page 54
Exporting a license file on page 55
Generating a licensing report on page 55
Refreshing license information on page 56

Installing a license file

Before you begin

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

About this task

Perform this procedure to install a license to an application.

Procedure

1. In the SMGR-CS web console page, under Services, click **Licenses**.

The Licensing page displays.

2. In the left navigation pane, click **FlexLM**.

   The Licensing Administration page displays.

3. Click **Add License**.

   The Add License dialog box displays.

4. Browse for the license file in the **License** field.
5. From the **License Host** list, select a license host.
6. Click **Add** to add the license to the SMGR-CS.

Exporting a license file

Before you begin

- Ensure that you are logged on to SMGR-CS 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 SMGR-CS web console page, under Services, click **Licenses**.

   The Licensing page displays.

2. In the left navigation pane, click **FlexLM**.

   The Licensing Administration page displays.

3. In the product name table, select the product license to be exported.
4. Click **Export License**.

   The File Download window displays.

5. Click **Save**.

Generating a licensing report

Before you begin

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

About this task

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

Procedure

1. In the SMGR-CS web console page, under Services, click **Licenses**.

   The Licensing page displays.
2. In the left navigation pane, click **FlexLM**.

   The Licensing Administration page displays.
3. In the product name table, select a product name.
4. Click **Report**.
5. 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 SMGR-CS as an administrator.

About this task

Perform this procedure to refresh the license information.

Procedure

1. In the SMGR-CS web console page, under Services, click **Licenses**.

   The Licensing page displays.
2. In the left navigation pane, click **FlexLM**.

   The Licensing Administration page displays.
3. Click **Refresh**. The license information in the product name table refreshes.

Chapter 10: Security

From the SMGR-CS web console, click **Security** in the Services section.

For information about administering the Certificate Authority (CA) and configuring the Enrollment Password to provision certificates, see *Administering Avaya Aura® System Manager*.

Chapter 11: Backup and Restore

You can back up and restore, on demand, all data within SMGR-CS applications. Backup and Restore functionality is accessed from the command line.

All backup files are stored in a folder named backups under the SMGR_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: SMGR_HOME. Backup archives are stored in [YY]-[MM]-[DD]_[HH].[mm].jar format (for example, 2014-05-01_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 [SMGR_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 SMGR files on page 58
- Restoring SMGR files on page 59

Related Links

Backing up SMGR files on page 58
Restoring SMGR files on page 59

Backing up SMGR files

Before you begin

- You must be logged on to the SMGR 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 SMGR files.

Important:

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

Procedure

1. From the command prompt or shell,
   - If using Windows, run the following script: `<INSTALL_DIR>\Avaya\smgr\bin\backupAllData.bat` or `<SMGR_HOME>\bin\backupAllData.bat`.
   - If using Linux, run the following script:`<INSTALL_DIR>/Avaya/smgr/bin/backupAllData.sh` or `<SMGR_HOME>/bin/backupAllData.sh`.

   Ensure there are no spaces in the path.
2. Enter the SMGR administrator login password when prompted. The system backs up all SMGR data.

   The system backs up all SMGR data.

Restoring SMGR files

Before you begin

- Ensure that you are logged on to the SMGR 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 can compromise system stability.

Procedure

1. From the command prompt or shell,
   - If using Windows, run the following script: `<INSTALL_DIR>\Avaya\smgr\bin\restoreAllData.bat` or `<SMGR_HOME>\bin\restoreAllData.bat`.
   - If using Linux, run the following script: `<INSTALL_DIR>/Avaya/smgr/bin/restoreAllData.sh` or `<SMGR_HOME>/bin/restoreAllData.sh`.

   Ensure there are no spaces in the path.
2. Enter the database administrator password when prompted.

3. Enter the name of the archive you wish to restore. The system restores data from the selected archive.

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

Chapter 12: 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

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)

Appendix A: Resetting the admin password

About this task

Perform the following procedure to reset the admin password.

Procedure

1. Log on to the “local-login” page of the SMGR primary server.

   https://fqdn/local-login

2. Type the username and password of a user who has administrative privileges to log on to the machine where the primary server is installed.
3. Change the URL to **https://fqdn/passwordReset** and enter the required details to change the password.

Appendix B: SMGR-CS provides CLI command for FQDN and IP changes on Linux after installation

If you reconfigure network interfaces (special for IP address), network connectivity is interrupted. Avaya recommends that you use a local terminal session for these procedures.

Run this command on the node (Linux OS only) where System Manager is installed. You can use the script for changing the IP or FQDN or both on System Manager. The node values of -OLDIP, -NEWIP or -OLDFQDN, -NEWFQDN are required for the script to work.

Login to the SMGR-CS console and issue following command:

```
sh /opt/Avaya/smgr/core/Mgmt/6.3.8/utils/ipfqdnchange/Ip-fqdn.sh -OLDIP
<> -NEWIP <> -OLDFQDN <> -NEWFQDN <> -INSTALLPATH <> -ENCRYPTKEY <> -
DBPASSWORD <> -GATEWAY <> -NETMASK <> -OLDDNS <> -NEWDNS <>
```

INSTALLPATH	Default value is /opt/Avaya/smgr/core if this argument is not passed.
ENCRYPTKEY	Default value is avaya if this argument is not passed.
DBPASSWORD	This is the password of DB user avaya_system_data. default value is taken if this argument is not passed.
GATEWAY	No default is taken and Gateway IP is the same if this argument is not passed.
NETMASK	No default is taken and Netmask IP is the same if this argument is not passed.
OLDDNS	No default is taken. Both OLD DNS / NEW DNS values must be present for the DNS value to be changed.
NEWDNS	No default is taken. Both OLD DNS / NEW DNS values must be present for the DNS value to be changed.
SEARCH	This is the search string for resolving hostnames. Default value is taken if this argument is not passed.

```
sh ip-fqdn.sh -OLDIP 148.147.w.x -NEWIP 148.147.y.z -OLDFQDN
a.platform.avaya.com -NEWFQDN b.platform.avaya.com -
INSTALLPATH /opt/Avaya/smgr/core -ENCRYPTKEY avaya -DBPASSWORD
```

```
asd123 -GATEWAY 148.147.162.1 -NETMASK 255.255.255.0 -OLDDNS
148.147.161.2 -NEWDNS 148.147.162.2
```