Avaya Solution & Interoperability Test Lab

Application Notes for Kurmi Unified Provisioning and Selfcare 7.4 with Avaya Aura® Communication Manager 8.1 and Aura® System Manager 8.1 - Issue 1.0

Abstract

These Application Notes describe the configuration steps required for configurating Kurmi Unified Provisioning and Selfcare with Avaya Aura® Communication Manager and Avaya Aura® System Manager.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration steps to integrate Avaya Aura® Communication Manager with Kurmi Unified Provisioning and Selfcare. Kurmi uses System Access Terminal (SAT) via SSH with Avaya Aura® Communication Manager and User Management Web Services (UMWS) with Avaya Aura® System Manager. Kurmi Unified Provisioning and Selfcare simplifies everyday telephone tasks and makes information available which allows optimization of the system management and provisioning. The Kurmi Unified Provisioning and Selfcare functions are divided into different connectors which may be used individually or combined, as required. The main components are installed on a CentOS based server, which is also responsible for the communication with the Avaya Aura environment. A Web client enables access to Kurmi Unified Provisioning and Selfcare functions by using a browser. Kurmi Unified Provisioning and Selfcare enables the user to Add, Change and Delete stations and Voicemail boxes. Session Initialization Protocol (SIP) stations can also be administered via the Avaya Aura® System Manager.

2. General Test Approach and Test Results

The general test approach was to configure the Kurmi Unified Provisioning and Selfcare (Kurmi) to communicate to the Avaya Aura environment including Communication Manager and System Manager as implemented on a customer site. See **Figure 1** for a network diagram. The interoperability compliance test included both feature functionality and serviceability tests.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interface between Avaya systems and Kurmi utilized capabilities of SSH for SAT access to Avaya Aura Communication Manager and UMWS via HTTPS port 443 to System Manager as requested by Kurmi.

This solution uses the System Access Terminal (SAT) interface to interact with Avaya Aura® Communication Manager. While this solution has successfully completed Compliance Testing for the specific release levels as described in these Application Notes, Avaya does not generally recommend use the SAT interface as a programmatic approach to integration of 3rd party applications. Avaya may make changes or enhancements to the SAT interface in any subsequent release, feature pack, service pack, or patch that may impact the interoperability of 3rd party applications using this SAT interface. Using the SAT interface in a programmatic manner may also result in a variety of operational issues, including performance impacts to the Avaya solution. If there are no other programmatic options available to obtain the required data or functionality, Avaya recommends that 3rd party applications only be executed during low call volume periods, and that real time delays be inserted between each command execution. NOTE: The scope of the compliance testing activities reflected in these Application Notes explicitly did not include load or performance evaluation criteria, and no guarantees or assurances are made by Avaya that the 3rd party application has implemented these recommendations. The vendor of the 3rd party application using this interface remains solely responsible for verifying interoperability with all later Communication Manager Releases, including feature packs, service packs, and patches as issued by Avaya. For additional details see Avaya Product Support Notices PSN002884u, PSN005085u, and PSN020295u, available at www.avaya.com/support.

2.1. Interoperability Compliance Testing

Feature functionality testing included:

- Verify synchronization between Kurmi and Communication Manager/System Manager/Avaya Messaging.
- Add/Change/Delete Analogue/Digital/IP stations (H.323 and SIP).
- Add/Change/Delete Voicemail boxes.
- Add/Change/Delete Hunt/Pickup groups.
- Change Abbreviation dialing lists.
- Schedule jobs.

Miscellaneous:

- Kurmi disconnect/reconnection
- Restart failed job synchronization

2.2. Test Results

Tests were performed to insure full interoperability between Kurmi Unified Provisioning and Selfcare and the Communication Manager/System Manager/Messaging. The tests were all functional in nature and performance testing was not included. The following were observed:

- All test cases completed successfully. Note that administration and synchronization of Avaya Messaging is done through System Manager.

2.3. Support

Technical support for Kurmi products can be found as follows:
Email: support@kurmi-software.com

3. Reference Configuration

Figure 1 illustrates the network topology used during compliance testing. The Avaya solution consists of Communication Manager, System Manager, Session Manager, Avaya Messaging, and a G430 Media Gateway. The Kurmi Unified Provisioning and Selfcare was installed on Virtual Machine running CentOS and connected to the same Network as the Avaya equipment. A client PC with a web browser was used to access the Kurmi application.

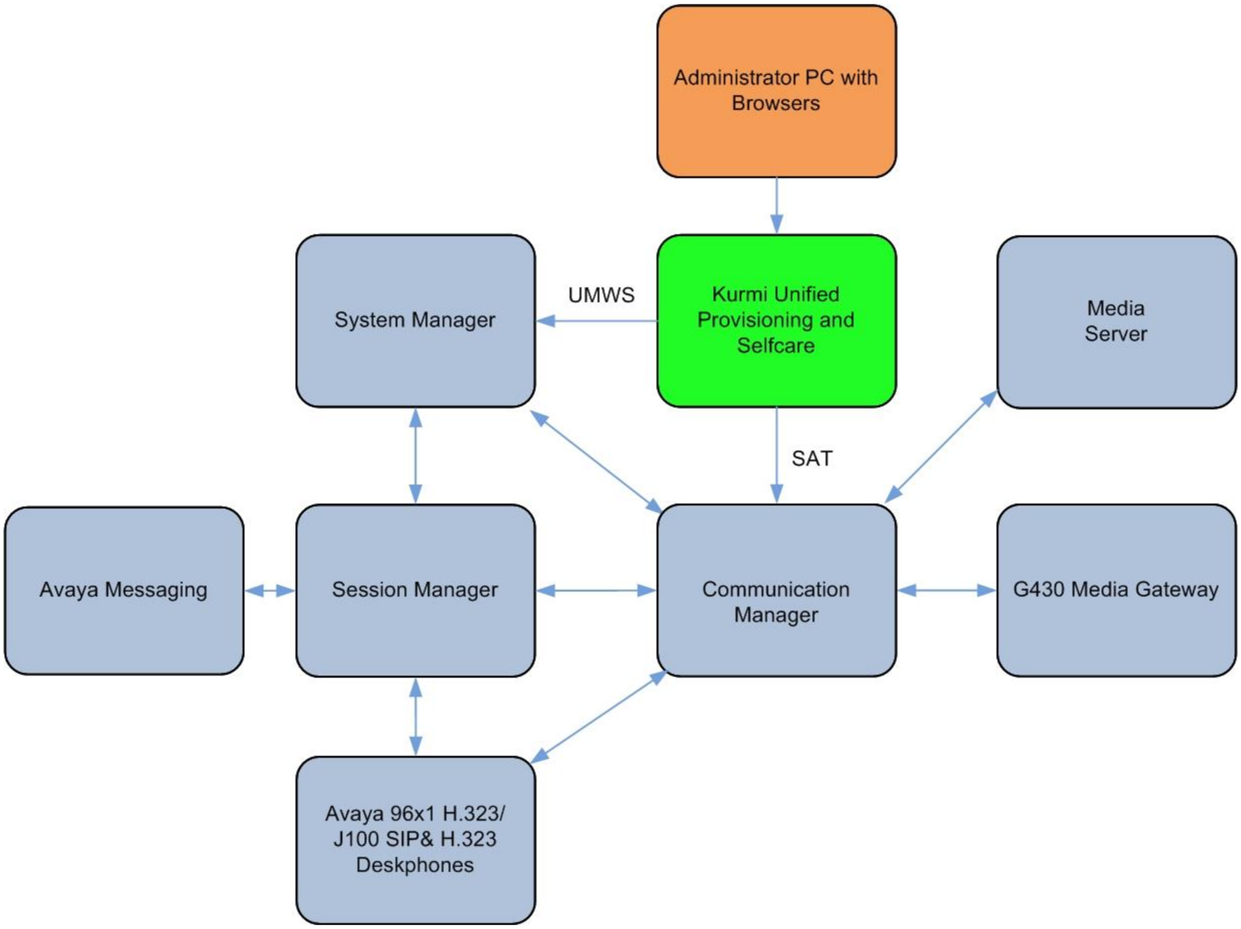

Administrator PC with Browsers
System Manager
UMWS
Kurmi Unified Provisioning and Selfcare
Media Server
SAT
Avaya Messaging
Session Manager
Communication Manager
G430 Media Gateway
Avaya 96x1 H.323/ J100 SIP& H.323 Deskphones

Figure 1: Test Configuration

4. Equipment and Software Validated

The following table describes the hardware components of the test configuration.

Avaya Equipment/Software	Release/Version
Avaya Aura® Communication Manager	8.1.3.2 (8.1.3.2.0.890.26989)
Avaya Aura® Session Manager	8.1.3.2 (8.1.3.2.813207)
Avaya Aura® System Manager	8.1.3.2 Build No. - 8.1.0.0.733078 Software Update Revision No: 8.1.3.2.1012646 SP 2
Avaya G430 Media Gateway	41.34.3
Avaya Aura Media Server	8.0.2.218
Avaya Messaging (Officelinx)	10.8 SP1SU2
Avaya J100 Series SIP Deskphones	4.0.10.0.4
Avaya 96x1/J100 Series H.323 Deskphones	6.8511
Kurmi Equipment/Software	**Release/Version**
Kurmi Unified Provisioning and Selfcare running on CentOS 7.9	Version 7.4.2

Note: *All Avaya Aura® and Kurmi systems runs on VMware 6.7 virtual platform.*

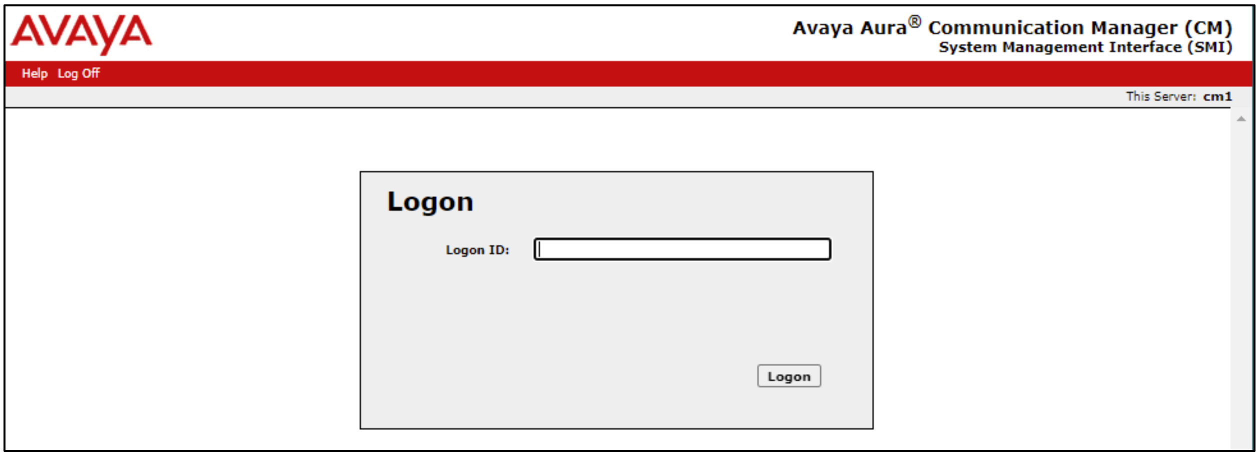
5. Configure Avaya Aura® Communication Manager

The only configuration relating to Communication Manager is that an Administrator account as a Privileged Administrator is required for Kurmi. Also, Server access of port 5022 needs to be enabled.

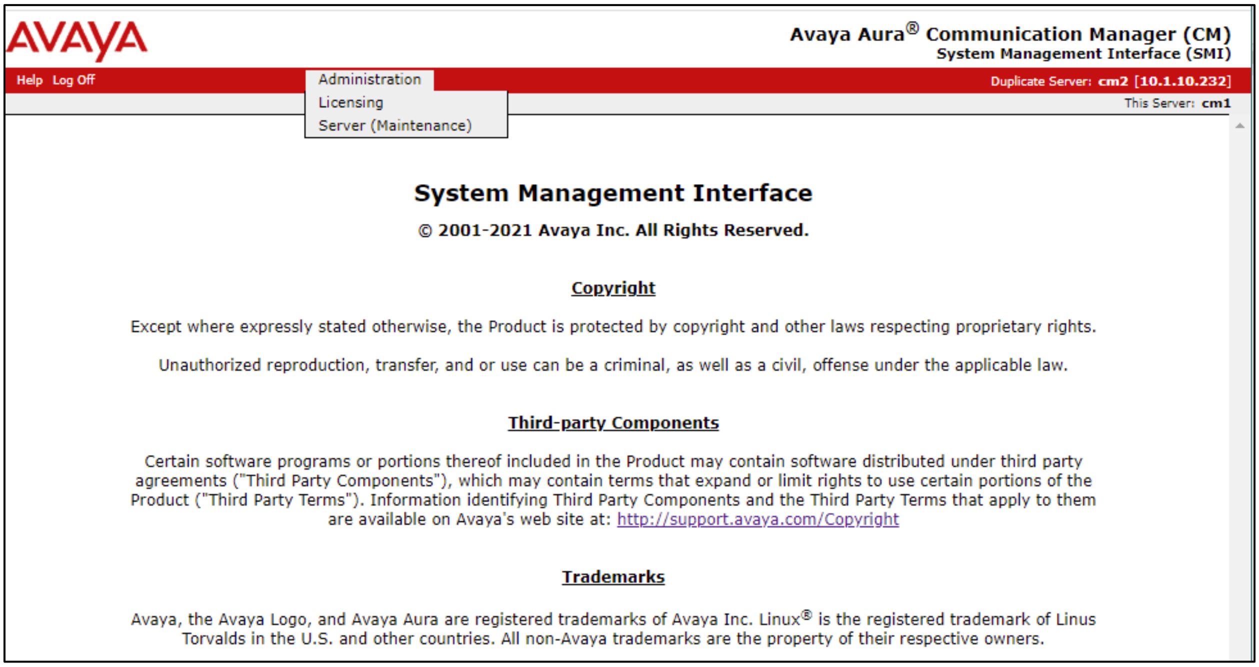
Note: The IP address and Release of the Communication Manager will be required for the Kurmi configuration.

5.1. Configure Privileged Administrator

To access the OAM web-based interface of Communication Manager use the URL https://x.x.x.x**,** where **x.x.x.x** is the selected IP address of Communication Manager. The Management console is displayed. Log in using the appropriate credentials and click on the **Logon** button.


AVAYA
Avaya Aura® Communication Manager (CM)
System Management Interface (SMI)
Help Log Off
This Server: cm1
Logon
Logon ID:
Logon

In the subsequent page, click on **Administration** followed by **Server (Maintenance)**.


AVAYA
Avaya Aura® Communication Manager (CM)
System Management Interface (SMI)
Help Log Off
Administration
Licensing
Server (Maintenance)
Duplicate Server: cm2 [10.1.10.232]
This Server: cm1

System Management Interface

© 2001-2021 Avaya Inc. All Rights Reserved.

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights.

Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

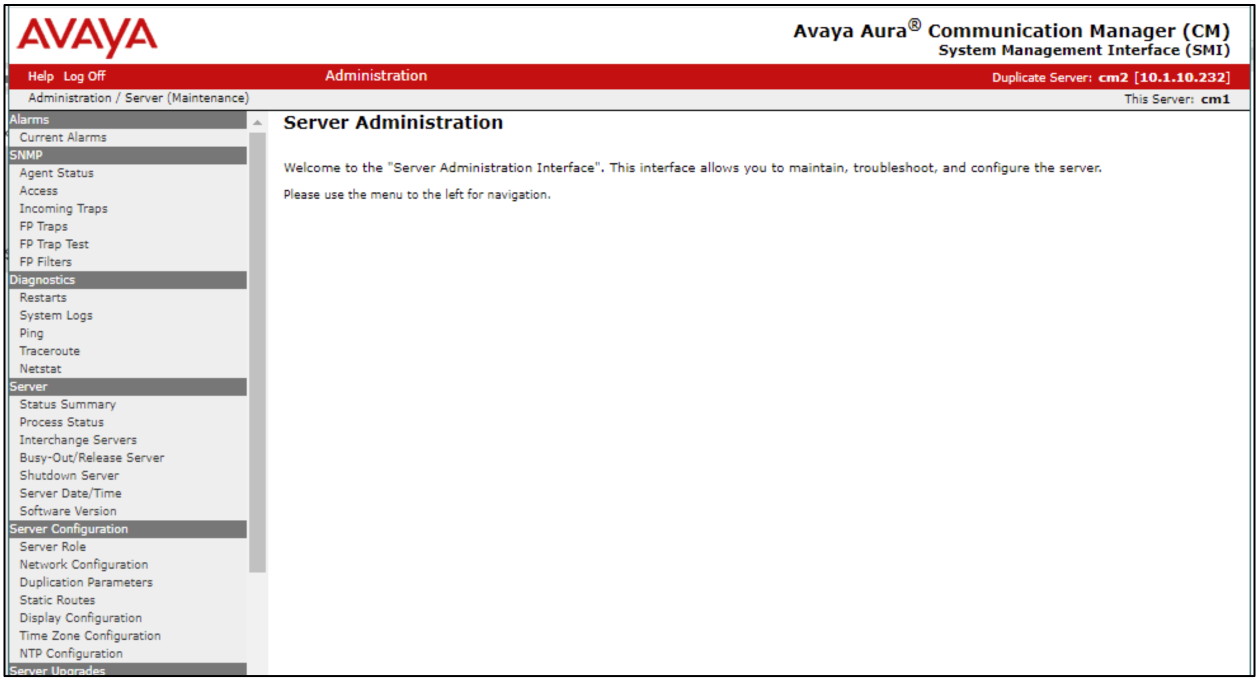
Third-party Components

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 identifying Third Party Components and the Third Party Terms that apply to them are available on Avaya's web site at: http://support.avaya.com/Copyright

Trademarks

Avaya, the Avaya Logo, and Avaya Aura are registered trademarks of Avaya Inc. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries. All non-Avaya trademarks are the property of their respective owners.

In the next page select **Security → Administrator Accounts** (not shown) from the left pane.

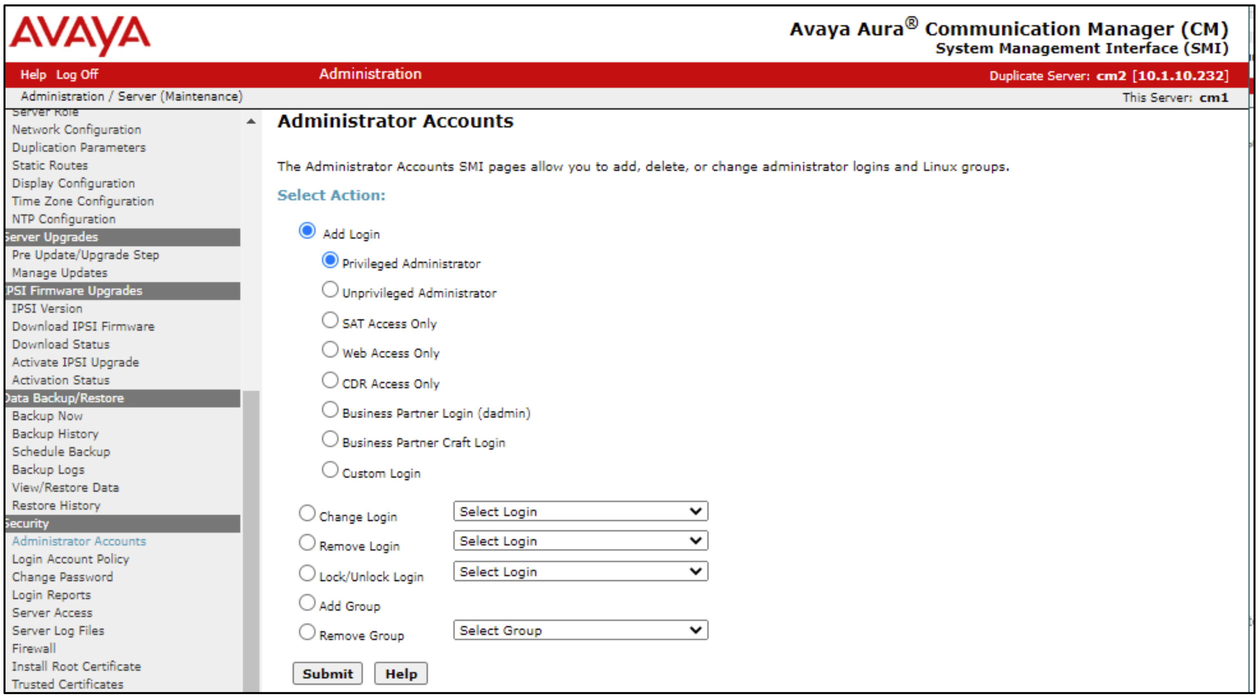


Server Administration

Welcome to the "Server Administration Interface". This interface allows you to maintain, troubleshoot, and configure the server.

Please use the menu to the left for navigation.

On the **Administrator Accounts** page, select the **Add Login** radio button followed by the **Privileged Administrator** radio button. Click on the **Submit** button to continue.



Administrator Accounts

The Administrator Accounts SMI pages allow you to add, delete, or change administrator logins and Linux groups.

Select Action:

● Add Login

- ● Privileged Administrator
- ○ Unprivileged Administrator
- ○ SAT Access Only
- ○ Web Access Only
- ○ CDR Access Only
- ○ Business Partner Login (dadmin)
- ○ Business Partner Craft Login
- ○ Custom Login

○ Change Login Select Login

○ Remove Login Select Login

○ Lock/Unlock Login Select Login

○ Add Group

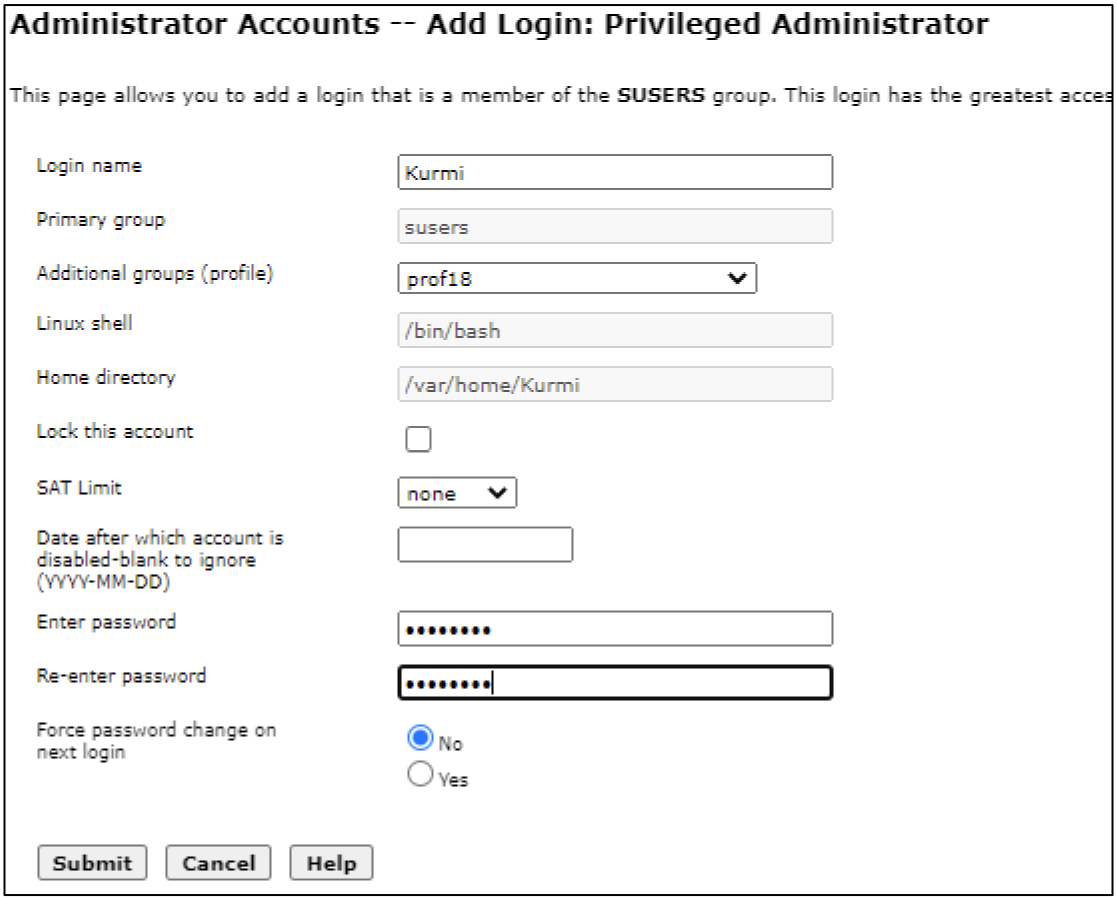
○ Remove Group Select Group

In the next page enter the following:

- **Login name** Enter **Kurmi**.
- **Additional groups** Select **prof18**.
- **Enter password** Enter appropriate login password.
- **Re-enter password** Re-enter the password.
- **Force password change on next login** Click the **No** radio button.

Leave the rest as default. The login with user profile 18 (**prof18**) has access to all possible Web Pages as members of the Linux group **susers** and is for customer with super user access.

Click the **Submit** radio button to save.



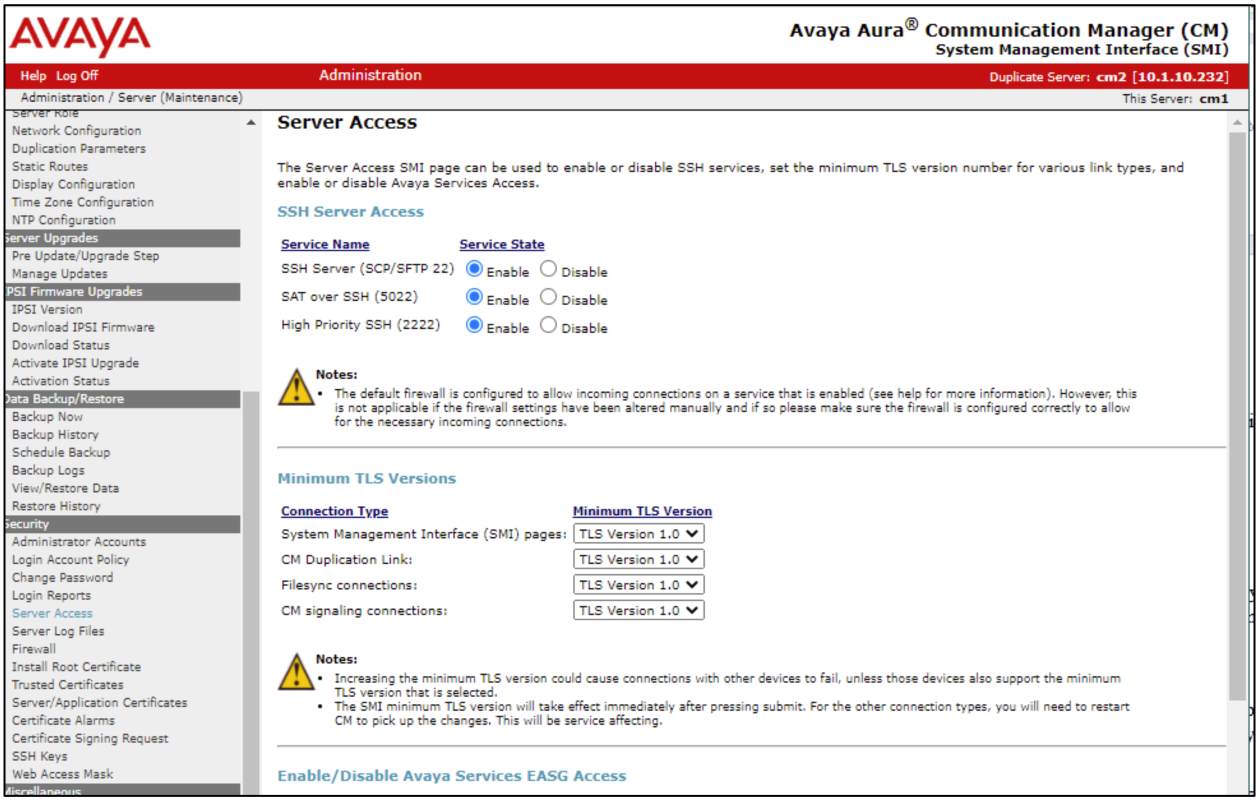
Administrator Accounts -- Add Login: Privileged Administrator

This page allows you to add a login that is a member of the **SUSERS** group. This login has the greatest acces

Login name	Kurmi
Primary group	susers
Additional groups (profile)	prof18
Linux shell	/bin/bash
Home directory	/var/home/Kurmi
Lock this account	□
SAT Limit	none
Date after which account is disabled-blank to ignore (YYYY-MM-DD)	
Enter password	••••••••
Re-enter password	••••••••
Force password change on next login	● No ○ Yes

5.2. Server Access

Port 5022 needs to be enabled so as allow Kurmi access to Communication Manager. Select **Security → Server Access** from the left pane. In the **SSH Server Access** section, click on the **Enable** radio button for **SAT**. In the **Minimum TLS Versions** section for **Connection Type System Management Interface (SMI) pages**, select the appropriate **Minimum TLS Version** supported. Click on the **Submit** (not shown) button to save.



Server Access

The Server Access SMI page can be used to enable or disable SSH services, set the minimum TLS version number for various link types, and enable or disable Avaya Services Access.

SSH Server Access

Service Name	Service State
SSH Server (SCP/SFTP 22)	● Enable ○ Disable
SAT over SSH (5022)	● Enable ○ Disable
High Priority SSH (2222)	● Enable ○ Disable

Notes:

- The default firewall is configured to allow incoming connections on a service that is enabled (see help for more information). However, this is not applicable if the firewall settings have been altered manually and if so please make sure the firewall is configured correctly to allow for the necessary incoming connections.

Minimum TLS Versions

Connection Type	Minimum TLS Version
System Management Interface (SMI) pages:	TLS Version 1.0
CM Duplication Link:	TLS Version 1.0
Filesync connections:	TLS Version 1.0
CM signaling connections:	TLS Version 1.0

Notes:

- Increasing the minimum TLS version could cause connections with other devices to fail, unless those devices also support the minimum TLS version that is selected.
- The SMI minimum TLS version will take effect immediately after pressing submit. For the other connection types, you will need to restart CM to pick up the changes. This will be service affecting.

Enable/Disable Avaya Services EASG Access

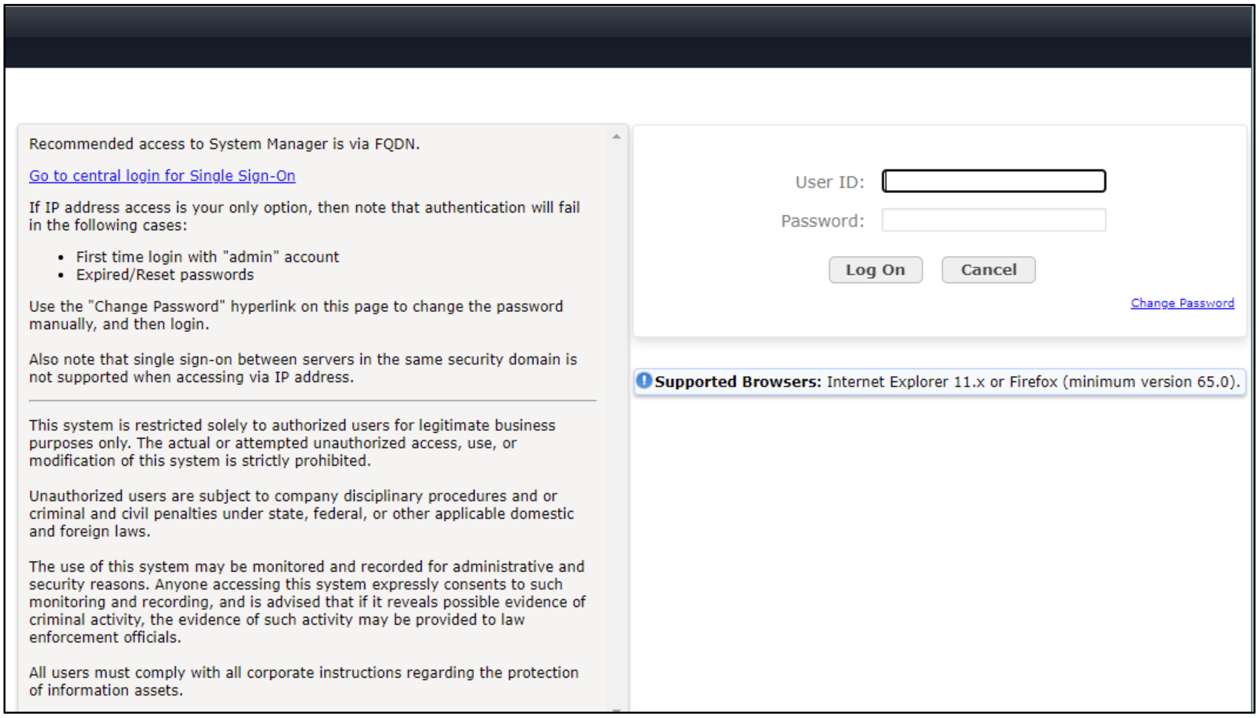
6. Configure Avaya Aura® System Manager

The only configuration relating to System Manager is that an Administrative User with a System Administrator Role is required for Kurmi. Also, HTTPs port 443 needs to be enabled which is opened by default.

Note: The IP address and Release of the System Manager will be required for the Kurmi configuration.

6.1. Configure Administrative User

To access the OAM web-based interface of the System Manager use the URL **https://x.x.x.x**, where **x.x.x.x** is the IP address of the System Manager. Once the System Manager Web page opens, log in with the appropriate credentials and click the **Log On** button.



Recommended access to System Manager is via FQDN.

Go to central login for Single Sign-On

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

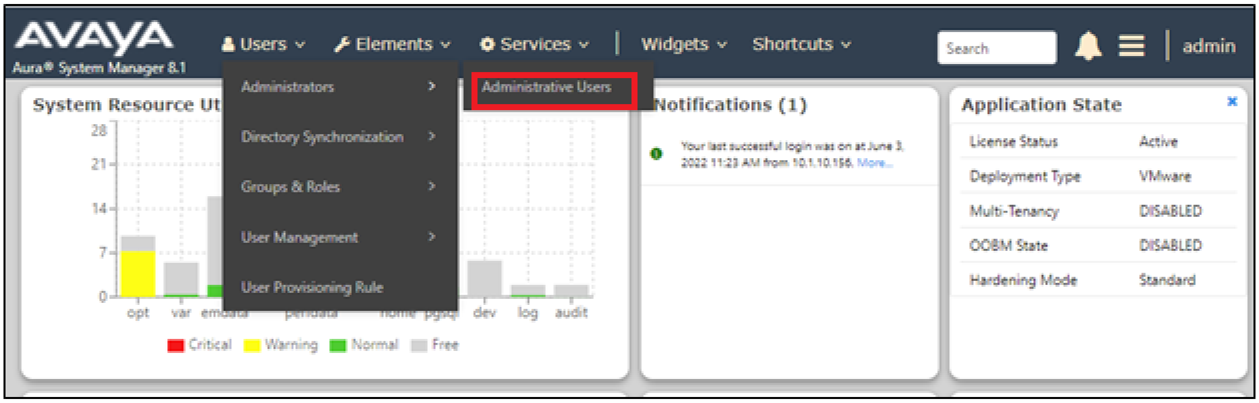
Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

Supported Browsers: Internet Explorer 11.x or Firefox (minimum version 65.0).

In the subsequent page, click on **Users → Administrators → Administrative Users** in the drop-down menu.



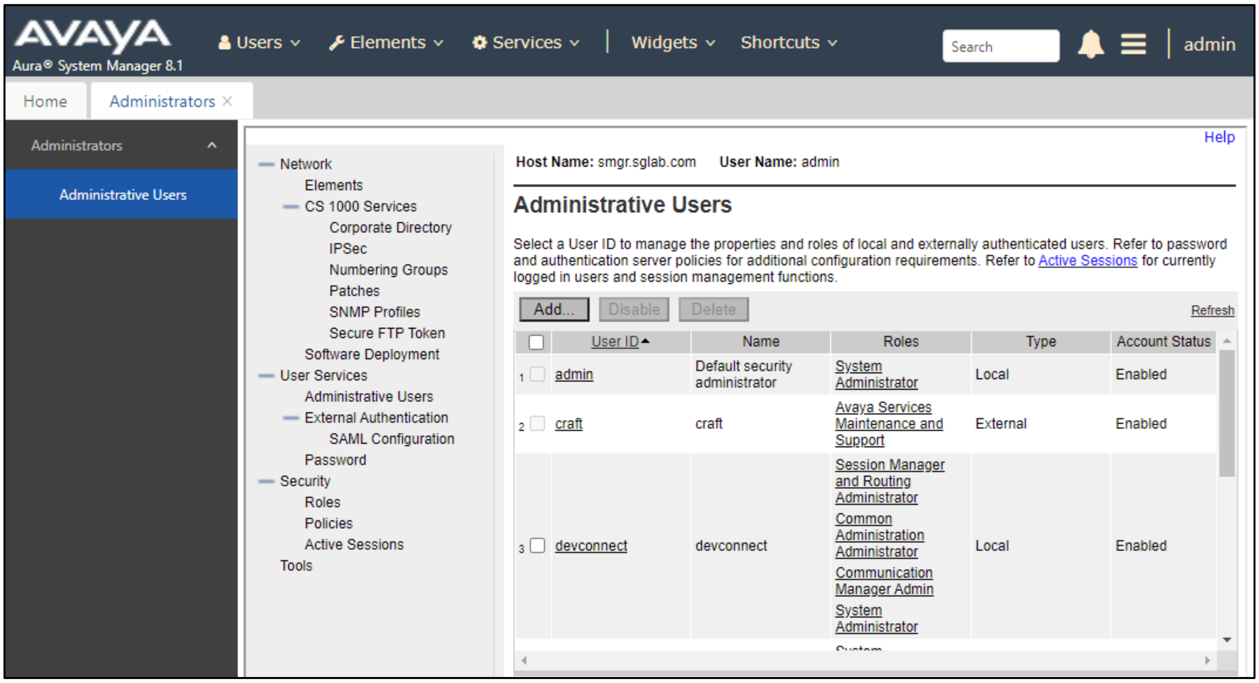
Notifications (1)

Your last successful login was on at June 3, 2022 11:23 AM from 10.1.10.156. More...

Application State

License Status	Active
Deployment Type	VMware
Multi-Tenancy	DISABLED
OOBM State	DISABLED
Hardening Mode	Standard

When the **Administrative Users** page opens, click on the **Add** button.



Host Name: smgr.sglab.com **User Name:** admin

Administrative Users

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

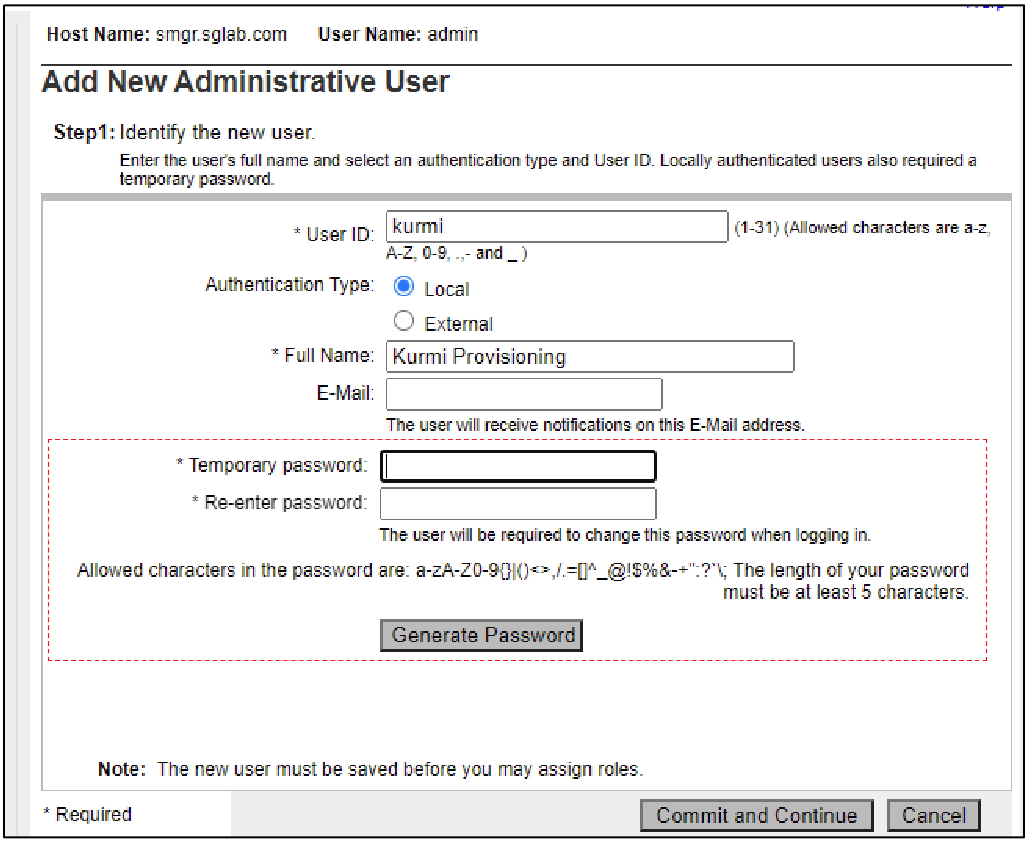
	User ID	Name	Roles	Type	Account Status
1 □	admin	Default security administrator	System Administrator	Local	Enabled
2 □	craft	craft	Avaya Services Maintenance and Support	External	Enabled
3 □	devconnect	devconnect	Session Manager and Routing Administrator Common Administration Administrator Communication Manager Admin System Administrator Custom	Local	Enabled

When the **Add New Administrative User** page opens enter the following:

• **User ID**	Enter user name.
• **Authentication Type**	Click **Local**.
• **Full Name**	Enter **Kurmi Provisioning**.
• **Password**	Enter a temporary password.
• **Re-enter password**	Re-enter the password.

Click on the **Commit and Continue** button.

Note: The next time the kurmi user logs on to the System Manager, the password will be required to be changed.



Host Name: smgr.sglab.com **User Name:** admin

Add New Administrative User

Step1: Identify the new user.

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

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

Authentication Type: ● Local ○ External

* Full Name: Kurmi Provisioning

E-Mail:

The user will receive notifications on this E-Mail address.

* Temporary password:

* Re-enter password:

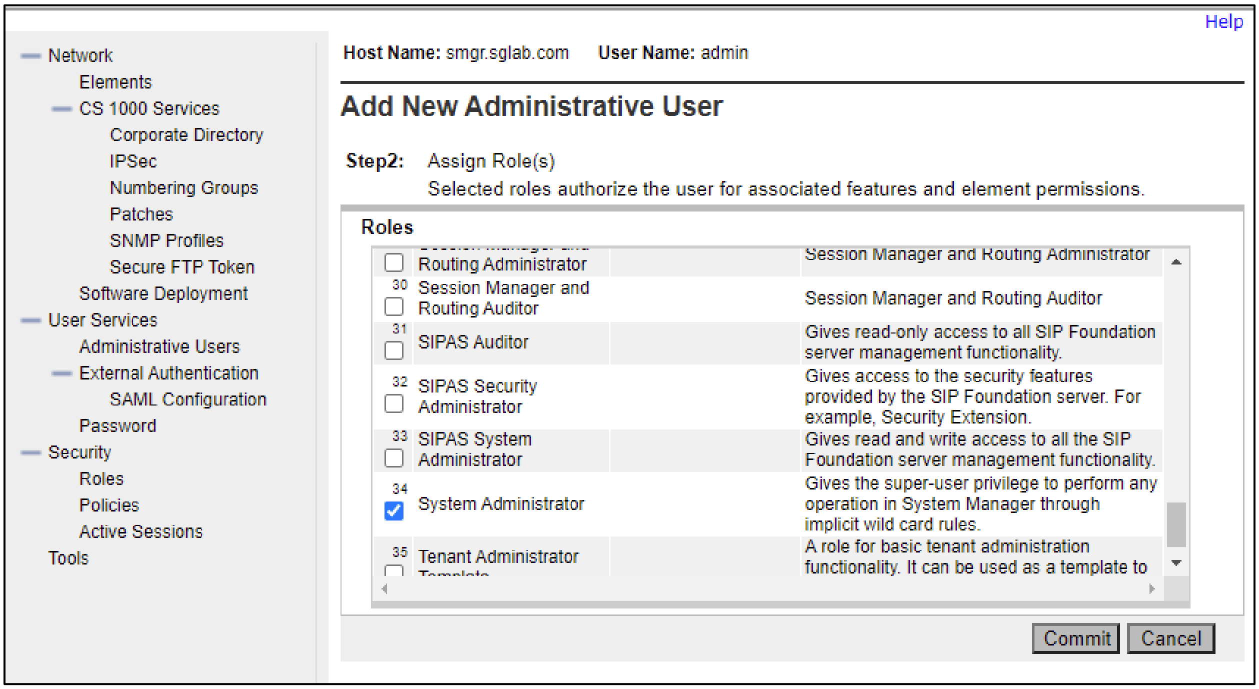
The user will be required to change this password when logging in.

Allowed characters in the password are: a-zA-Z0-9{}|()<>,/.=[]^_@!$%&-+":?`\; The length of your password must be at least 5 characters.

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

* Required

When the next page opens, using the scroll bar on the right side of the **Roles** pane scroll down and click the **System Administrator** box. Click on the **Commit** button to save.



Host Name: smgr.sglab.com **User Name:** admin

Add New Administrative User

Step2: Assign Role(s)

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

Roles

	☐	Routing Administrator	Session Manager and Routing Administrator
30	☐	Session Manager and Routing Auditor	Session Manager and Routing Auditor
31	☐	SIPAS Auditor	Gives read-only access to all SIP Foundation server management functionality.
32	☐	SIPAS Security Administrator	Gives access to the security features provided by the SIP Foundation server. For example, Security Extension.
33	☐	SIPAS System Administrator	Gives read and write access to all the SIP Foundation server management functionality.
34	☑	System Administrator	Gives the super-user privilege to perform any operation in System Manager through implicit wild card rules.
35	☐	Tenant Administrator	A role for basic tenant administration functionality. It can be used as a template to

7. Configure Avaya Aura® Session Manager

There is no specific configuration of Session Manager.

Note: Release of the Session Manager will be required for the Kurmi configuration.

8. Configure Avaya Messaging

There is no specific configuration of Messaging as administration of voicemail box is through System Manager.

9. Configure Kurmi Unified Provisioning and Selfcare

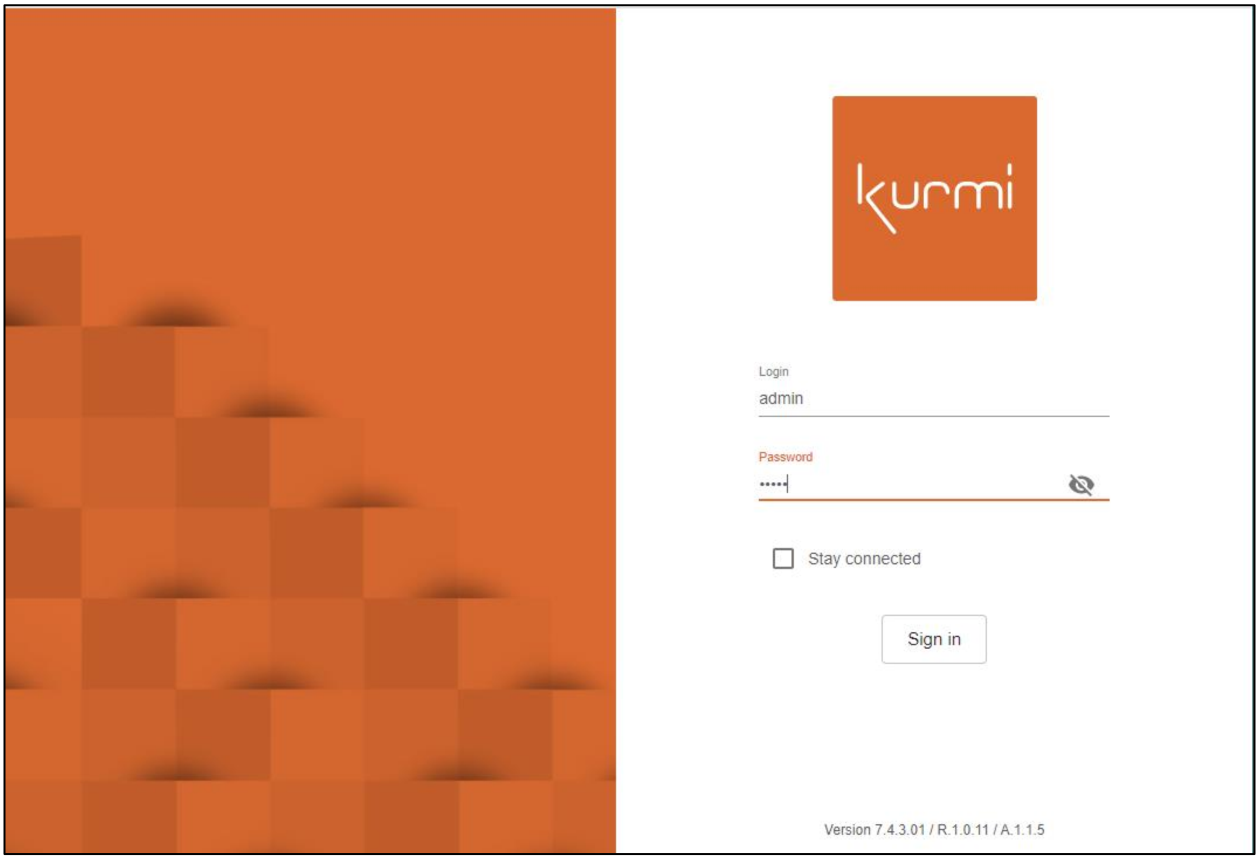
At the request of Kurmi, the configuration of Kurmi Unified Provisioning and Selfcare is excluded from these Application Notes. Kurmi Unified Provisioning and Selfcare is installed and configured by Kurmi Professional Services or trained Kurmi partners.

10. Verification Steps

This section provides tests that can be performed to verify correct configuration of the Avaya and Kurmi solution.

10.1. Verify synchronization

To access the OAM web-based interface of Kurmi use the URL **http://x.x.x.x,** where **x.x.x.x** is the IP address of Kurmi. The **Sign in** page is displayed. Log in using the appropriate credentials and click on the **Sign in** button to continue.

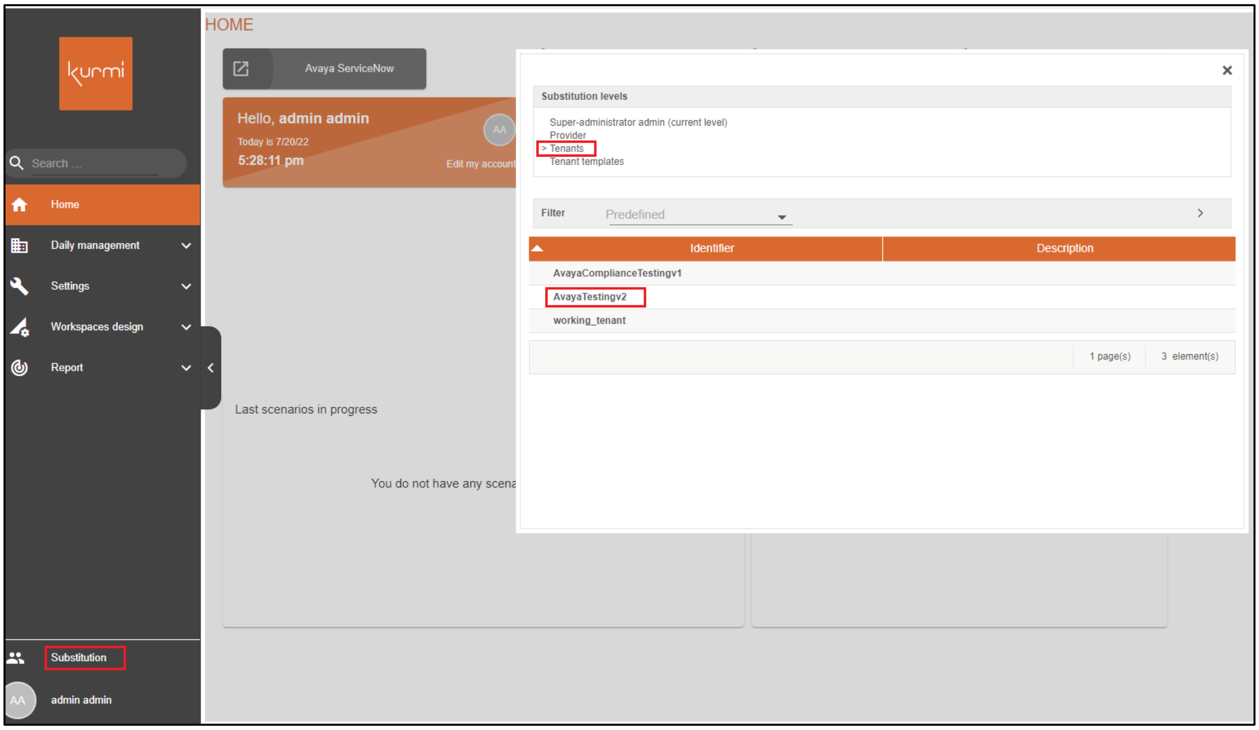


Login
admin

Password
•••••

□ Stay connected

Click on **Substitution** in the left pane below and select the **Tenants** under **Substitution levels** on the right. Select the appropriate **Tenants** from the list to administer. In this compliance testing, **AvayaTestingv2** is selected.



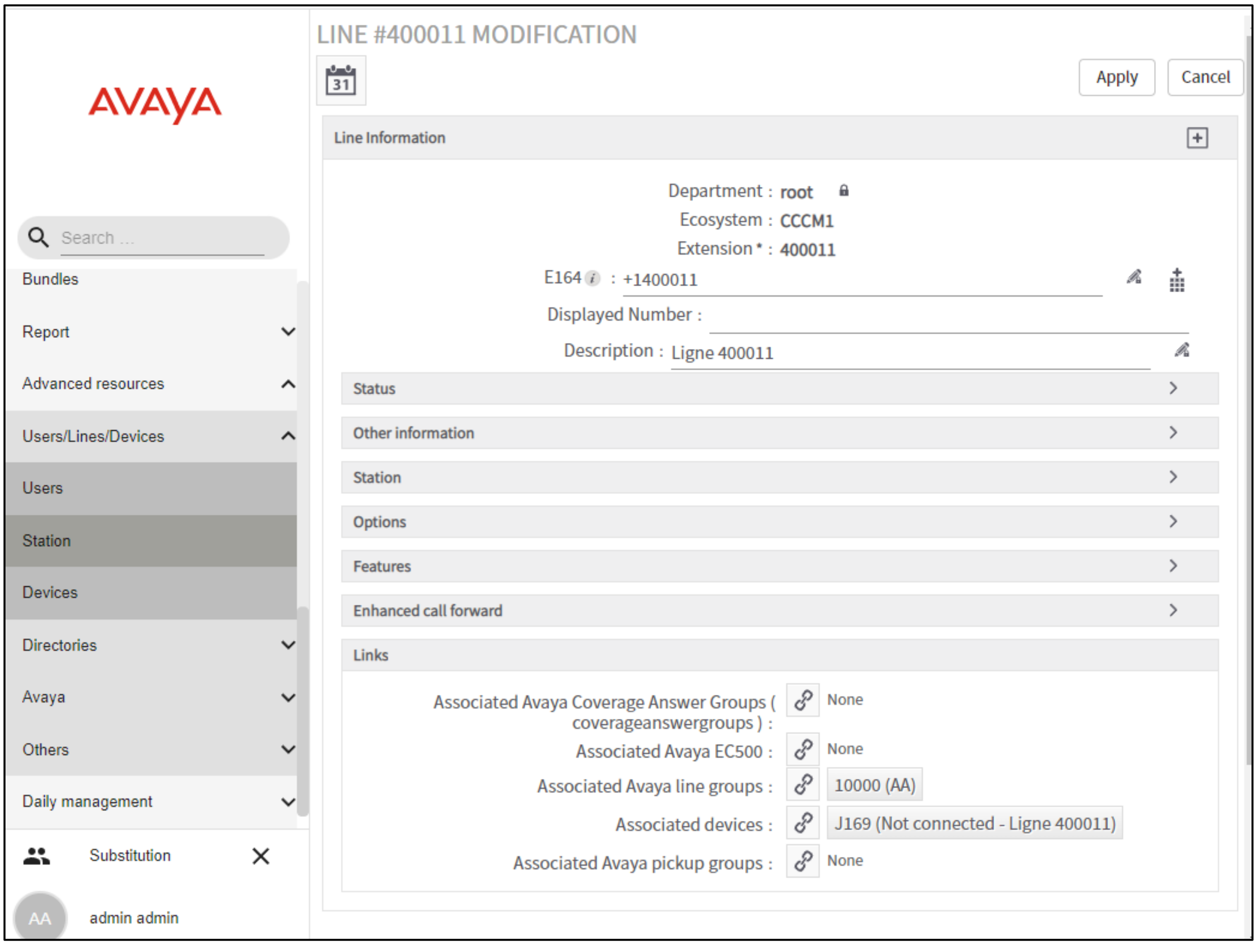
Substitution levels

Super-administrator admin (current level)
Provider
> Tenants
Tenant templates

Identifier	Description
AvayaComplianceTestingv1	
AvayaTestingv2	
working_tenant	

10.1.1. Verify Avaya Station synchronization

Navigate from the left pane **Settings → Advanced resources → Users/Lines/Devices → Station**. Select a station on the right pane (not shown) say 400011 as shown below. The station details should match the station details configured on Communication Manager (See **Section 10.1.2**).



LINE #400011 MODIFICATION

Line Information

Department : root

Ecosystem : CCCM1

Extension * : 400011

E164 : +1400011

Displayed Number :

Description : Ligne 400011

Links

Associated Avaya Coverage Answer Groups (coverageanswergroups) : None

Associated Avaya EC500 : None

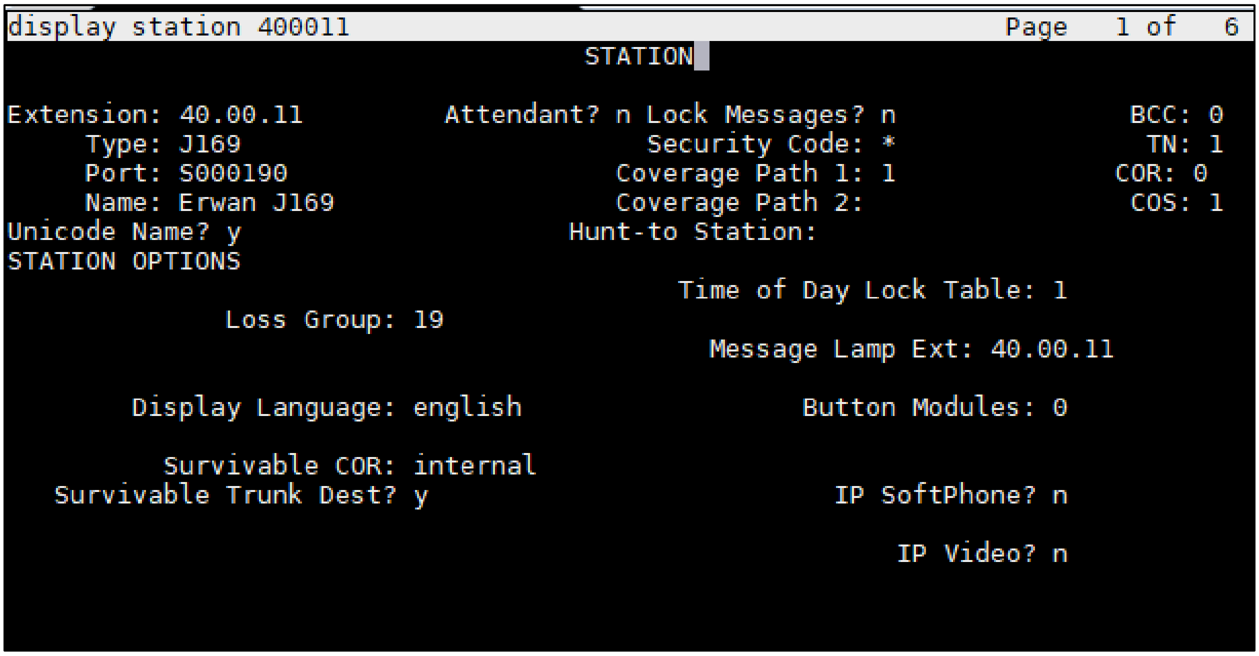
Associated Avaya line groups : 10000 (AA)

Associated devices : J169 (Not connected - Ligne 400011)

Associated Avaya pickup groups : None

10.1.2. Display Extensions on Avaya Aura® Communication Manager

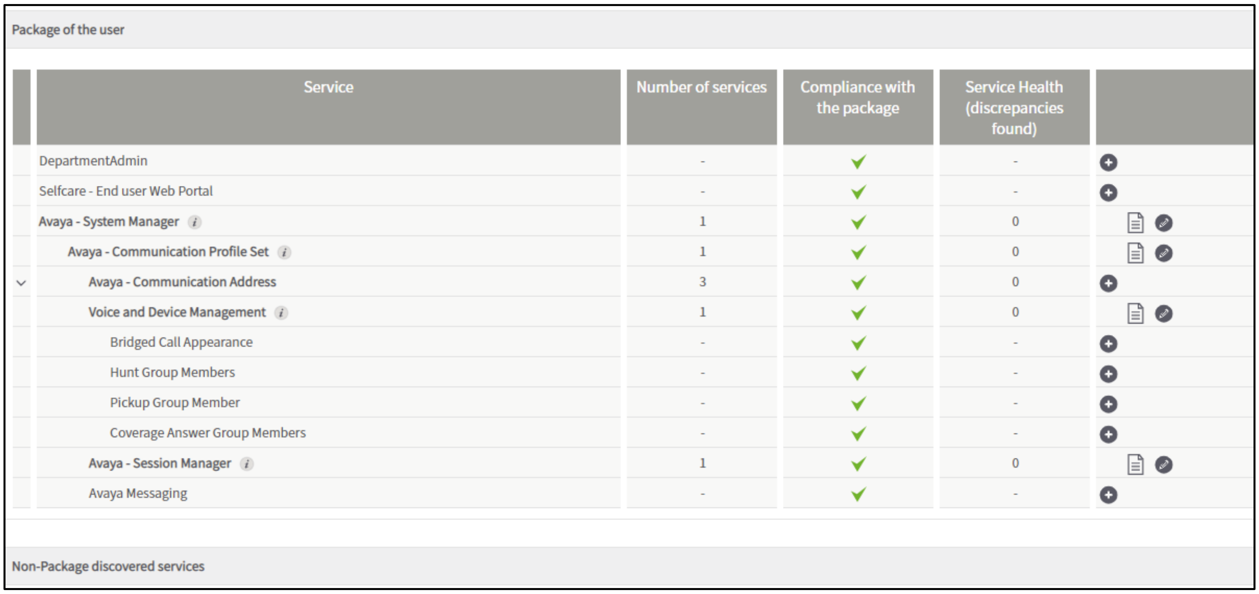
Using SAT use the **display station** command to display the extension created on Communication Manager.



```
display station 400011                                          Page   1 of   6
                                     STATION

Extension: 40.00.11         Attendant? n Lock Messages? n               BCC: 0
     Type: J169                          Security Code: *                TN: 1
     Port: S000190                     Coverage Path 1: 1              COR: 0
     Name: Erwan J169                  Coverage Path 2:                 COS: 1
Unicode Name? y                     Hunt-to Station:
STATION OPTIONS
                                           Time of Day Lock Table: 1
              Loss Group: 19
                                             Message Lamp Ext: 40.00.11

        Display Language: english                  Button Modules: 0

          Survivable COR: internal
   Survivable Trunk Dest? y                              IP SoftPhone? n

                                                         IP Video? n
```

10.1.3. Mail box creation

From the home screen, navigate to **Users** from the left pane and select say user **10069** from the right pane (not shown). Scroll down the user details screen and click the **+** sign beside **Avaya Messaging**.

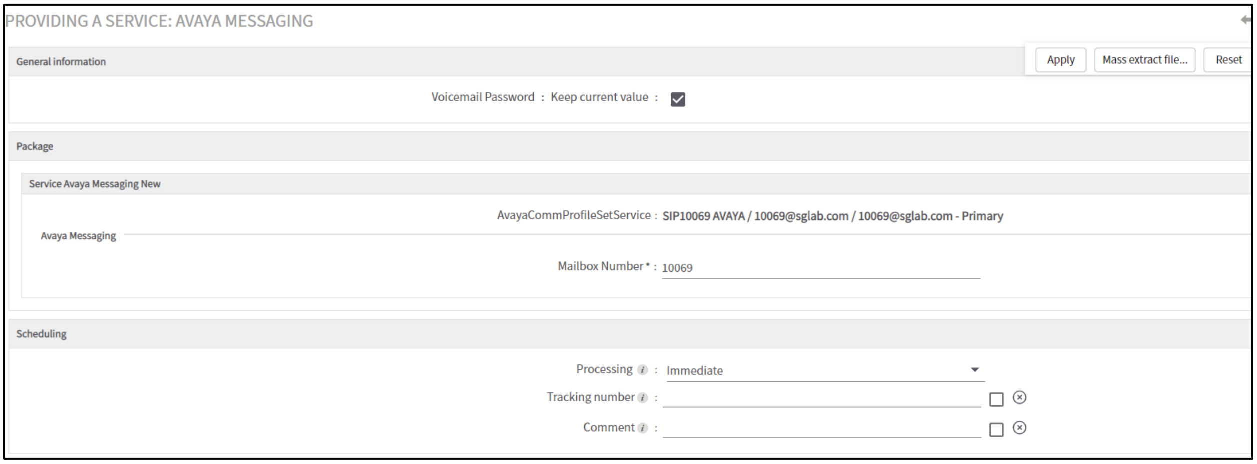


Package of the user

Service	Number of services	Compliance with the package	Service Health (discrepancies found)	
DepartmentAdmin	-	✓	-	⊕
Selfcare - End user Web Portal	-	✓	-	⊕
Avaya - System Manager	1	✓	0	🗎 ✎
Avaya - Communication Profile Set	1	✓	0	🗎 ✎
Avaya - Communication Address	3	✓	0	⊕
Voice and Device Management	1	✓	0	🗎 ✎
Bridged Call Appearance	-	✓	-	⊕
Hunt Group Members	-	✓	-	⊕
Pickup Group Member	-	✓	-	⊕
Coverage Answer Group Members	-	✓	-	⊕
Avaya - Session Manager	1	✓	0	🗎 ✎
Avaya Messaging	-	✓	-	⊕

Non-Package discovered services

The next screen is shown below. Click the **Apply** button and the creation is in progress.



PROVIDING A SERVICE: AVAYA MESSAGING

General information

Voicemail Password : Keep current value : ☑

Package

Service Avaya Messaging New

Avaya Messaging

AvayaCommProfileSetService : SIP10069 AVAYA / 10069@sglab.com / 10069@sglab.com - Primary

Mailbox Number * : 10069

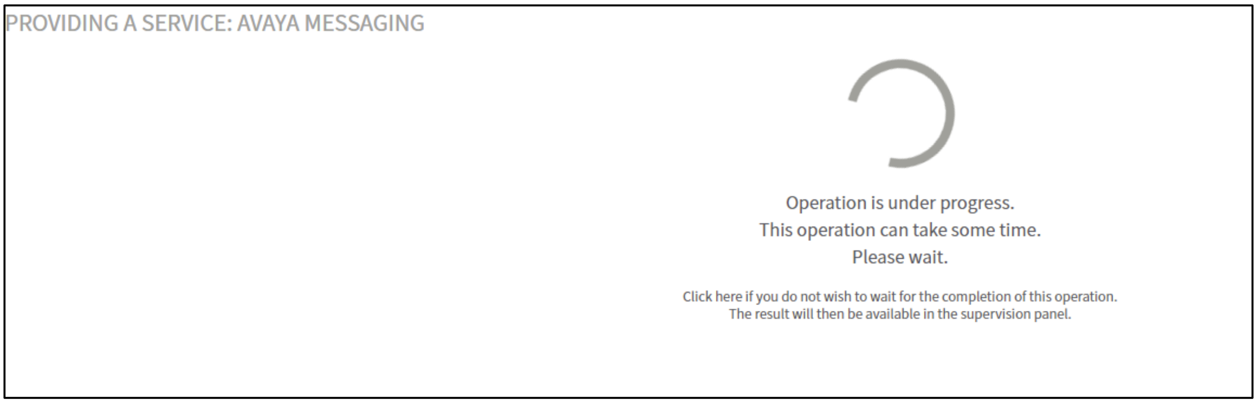
Scheduling

Processing : Immediate

Tracking number : □

Comment : □

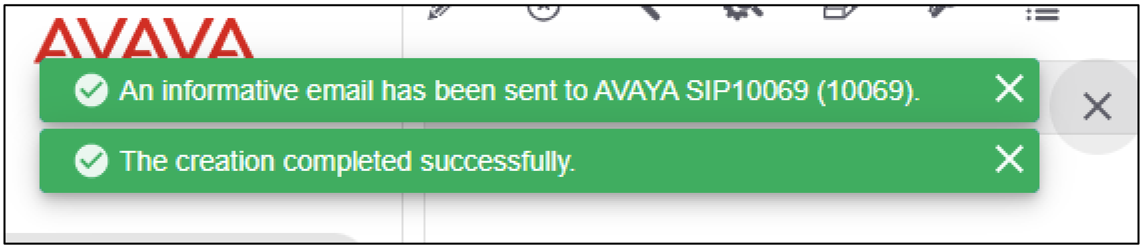
The screen shows the operation is in progress and once completed successfully, the completion screen is shown on the next screen below.



PROVIDING A SERVICE: AVAYA MESSAGING

Operation is under progress.
This operation can take some time.
Please wait.

Click here if you do not wish to wait for the completion of this operation.
The result will then be available in the supervision panel.

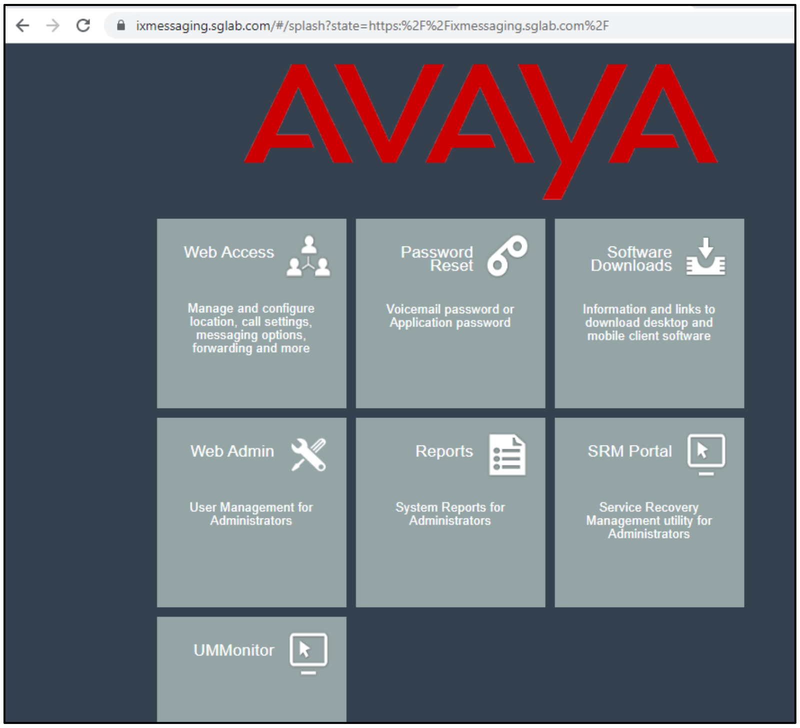


✓ An informative email has been sent to AVAYA SIP10069 (10069). ✕

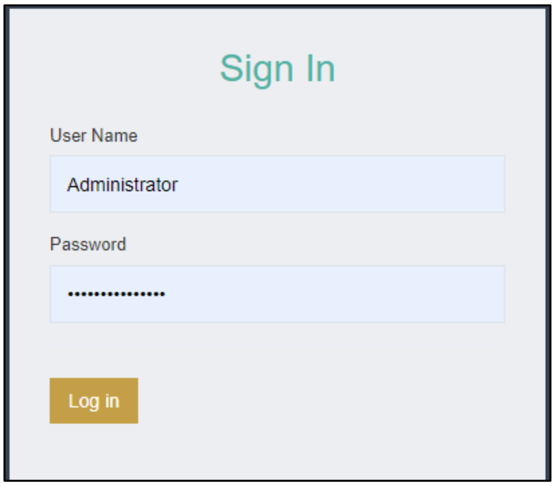
✓ The creation completed successfully. ✕

10.1.4. Verifying User on Avaya Messaging

Access the OAM web-based interface of Avaya Messaging and select **Web Admin**.


ixmessaging.sglab.com/#/splash?state=https:%2F%2Fixmessaging.sglab.com%2F
AVAYA
Web Access
Manage and configure location, call settings, messaging options, forwarding and more
Password Reset
Voicemail password or Application password
Software Downloads
Information and links to download desktop and mobile client software
Web Admin
User Management for Administrators
Reports
System Reports for Administrators
SRM Portal
Service Recovery Management utility for Administrators
UMMonitor

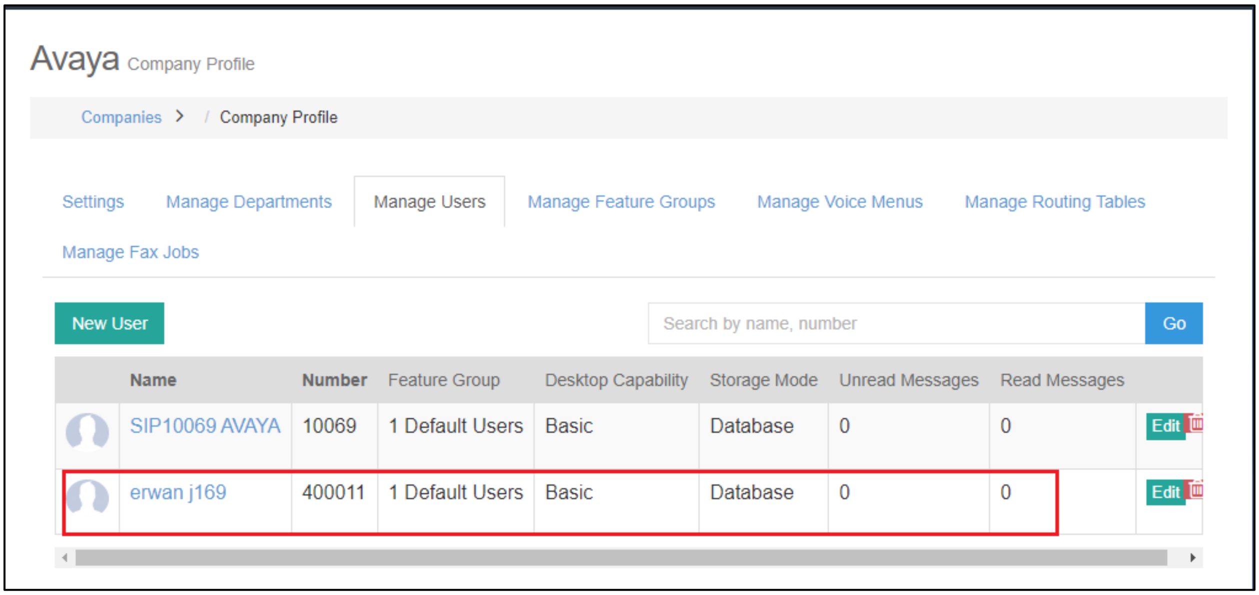
When the **Sign In** page pops-up, enter appropriate **User Name** and **Password**.


Sign In

User Name: Administrator

Password: •••••••••••••••

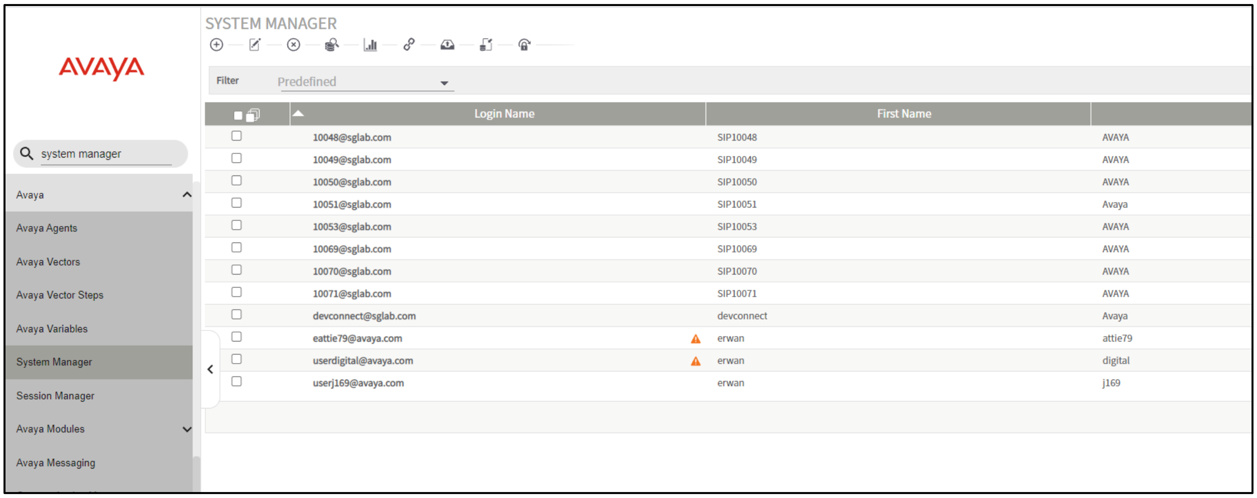
In the **Manage Users** page that is now displayed, verify that this matches the mail box created in **Section 10.1.3**.



	Name	Number	Feature Group	Desktop Capability	Storage Mode	Unread Messages	Read Messages	
	SIP10069 AVAYA	10069	1 Default Users	Basic	Database	0	0	Edit
	erwan j169	400011	1 Default Users	Basic	Database	0	0	Edit

10.1.5. Verify Avaya Aura® System Manager synchronization

Navigate from the left pane **Settings → Avaya → System Manager**. A list of SIP Users that are configured will be displayed. This list should match the SIP Users configured on System Manager (See **Section 10.1.6**).



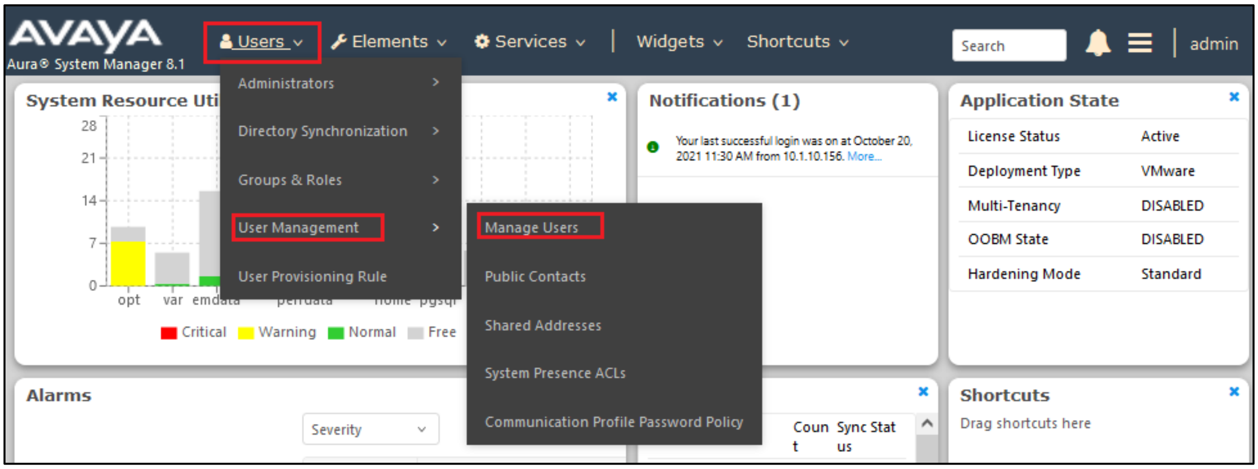
SYSTEM MANAGER

Filter: Predefined

	Login Name	First Name	
□	10048@sglab.com	SIP10048	AVAYA
□	10049@sglab.com	SIP10049	AVAYA
□	10050@sglab.com	SIP10050	AVAYA
□	10051@sglab.com	SIP10051	Avaya
□	10053@sglab.com	SIP10053	AVAYA
□	10069@sglab.com	SIP10069	AVAYA
□	10070@sglab.com	SIP10070	AVAYA
□	10071@sglab.com	SIP10071	AVAYA
□	devconnect@sglab.com	devconnect	Avaya
□	eattie79@avaya.com ⚠	erwan	attie79
□	userdigital@avaya.com ⚠	erwan	digital
□	userj169@avaya.com	erwan	j169

10.1.6. User Management on Avaya Aura® System Manager

Access the OAM web-based interface of System Manager (not shown) and navigate to **Users → User Management → Manage Users**.



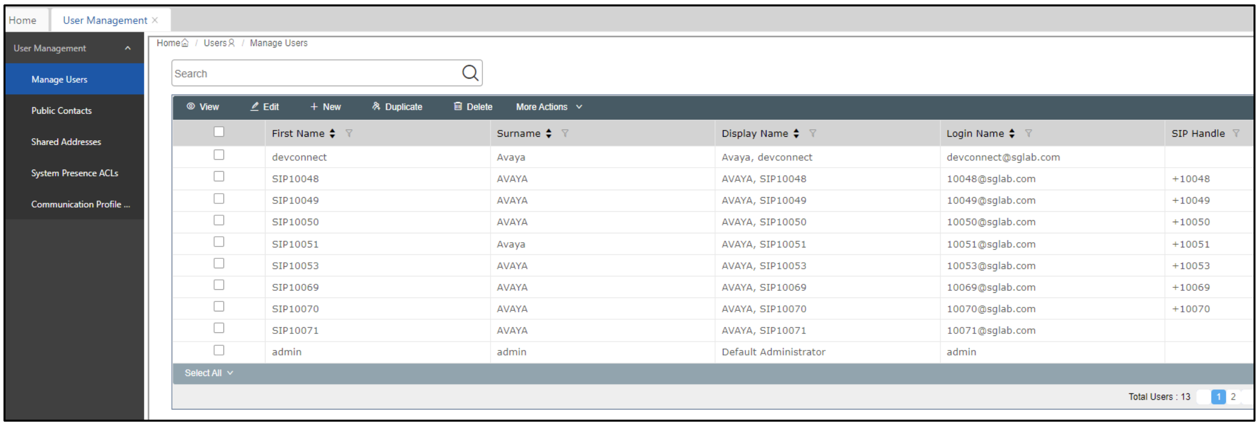
Notifications (1)

Your last successful login was on at October 20, 2021 11:30 AM from 10.1.10.156. More...

Application State

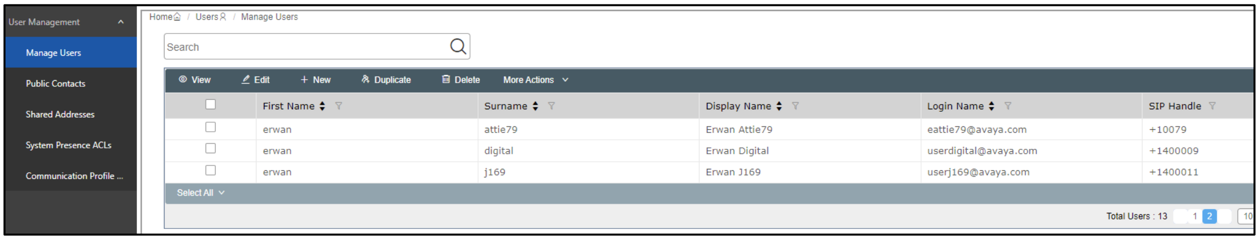
License Status	Active
Deployment Type	VMware
Multi-Tenancy	DISABLED
OOBM State	DISABLED
Hardening Mode	Standard

When the **User Manager** page opens, verify that this list matches the list shown in **Section 10.1.5**.



□	First Name	Surname	Display Name	Login Name	SIP Handle
□	devconnect	Avaya	Avaya, devconnect	devconnect@sglab.com	
□	SIP10048	AVAYA	AVAYA, SIP10048	10048@sglab.com	+10048
□	SIP10049	AVAYA	AVAYA, SIP10049	10049@sglab.com	+10049
□	SIP10050	AVAYA	AVAYA, SIP10050	10050@sglab.com	+10050
□	SIP10051	Avaya	AVAYA, SIP10051	10051@sglab.com	+10051
□	SIP10053	AVAYA	AVAYA, SIP10053	10053@sglab.com	+10053
□	SIP10069	AVAYA	AVAYA, SIP10069	10069@sglab.com	+10069
□	SIP10070	AVAYA	AVAYA, SIP10070	10070@sglab.com	+10070
□	SIP10071	AVAYA	AVAYA, SIP10071	10071@sglab.com	
□	admin	admin	Default Administrator	admin	

Total Users : 13 1 2



□	First Name	Surname	Display Name	Login Name	SIP Handle
□	erwan	attie79	Erwan Attie79	eattie79@avaya.com	+10079
□	erwan	digital	Erwan Digital	userdigital@avaya.com	+1400009
□	erwan	j169	Erwan J169	userj169@avaya.com	+1400011

Total Users : 13 1 2 10

11. Conclusion

A full and comprehensive set of feature functional test cases were performed during compliance testing. All test cases passed and met all objectives. Kurmi Unified Provisioning and Selfcare 7.4 is considered compliant with Avaya Aura® Communication Manager 8.1 and Avaya Aura® System Manager 8.1. Observations are noted in **Section 2.2**.

12. Additional References

These documents form part of the Avaya official technical reference documentation suite. Further information may be had from *http://support.avaya.com* or from your Avaya representative.

[1] *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 12, Jul 2021.
[2] *Administering Avaya Aura® System Manager*, Release 8.1.x, Issue 19, Apr 2022.
[3] *Administering Avaya Aura® Session Manager,* Release 8.1.x, Issue 10, Sep 2021.
[4] *IX Messaging™ Server Configuration Guide,* Version 10.8, Apr 2021.

Product Documentation for Kurmi can be obtained at link below where login account is required.
http://extranet.kurmi-software.com/extranet

[1] *Avaya Aura System Manager Connector dated 2020*
[2] *Avaya Communication Manager Connector dated 2021*

The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.