Application Notes for Engelbart esuits² myICT 1.0 with Avaya Aura® System Manager 8.1 and Avaya Aura® Application Enablement Services 8.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Engelbart esuits² myICT 1.0 to interoperate with Avaya Aura® System Manager 8.1.3.4 and Avaya Aura® Application Enablement Services 8.1.3.4. Engelbart esuits² myICT used User Management Webservices Application Programming Interface from Avaya Aura® System Manager and Management Service Web Service from Avaya Aura® Application Enablement Services.

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 required for Engelbart esuits² myICT 1.0 to interoperate with Avaya Aura® Communication Manager 8.1.3.4 and Avaya Aura® Application Enablement Services 8.1.3.4.

Engelbart esuits² myICT provides an innovative solution for the ordering and managing of telephone connections, sets and dependent services. Engelbart esuits² myICT allow administrator to reduce standard tasks for managing users, extensions, hunt groups, pick-up groups. It can also accept input from Active Directory and create provisioned users in Avaya Aura and place those users/extensions into groups (pickup, hunt, etc.,) based on information in Active Directory.

2. General Test Approach and Test Results

The general test approach was to validate the Engelbart esuits² myICT to administer users, extensions, hunt groups, and pick-up group.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connections to the Engelbart esuits² myICT server.

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 Engelbart esuits² SPC Framework did not include use of any specific encryption features as requested by Engelbart.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing. The feature testing focused on verifying the following Engelbart esuits² myICT:

- Administer users and extensions
- Administer pick up group and hunt group
- Administer user's voicemail, password, and email forwarding address
- Administer EC500 Mapping and call coverage path management

The serviceability testing focused on verifying the ability of Engelbart esuits² myICT to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connections to the Engelbart esuits² SPC myICT server.

2.2. Test Results

All test cases were executed and verified successfully.

2.3. Support

Technical support on Engelbart esuits² myICT can be obtained through the following:

Engelbart Software GmbH
Alpenstrasse 12
6300 Zug
Switzerland
Tel: +41 41 511 35 02
E-Mail: info@engelbart-software.com

Parkstrasse 40
88212 Ravensburg
Germany
Tel: +49 751 7642 4300
E-Mail: info@engelbart-software.com

3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**.

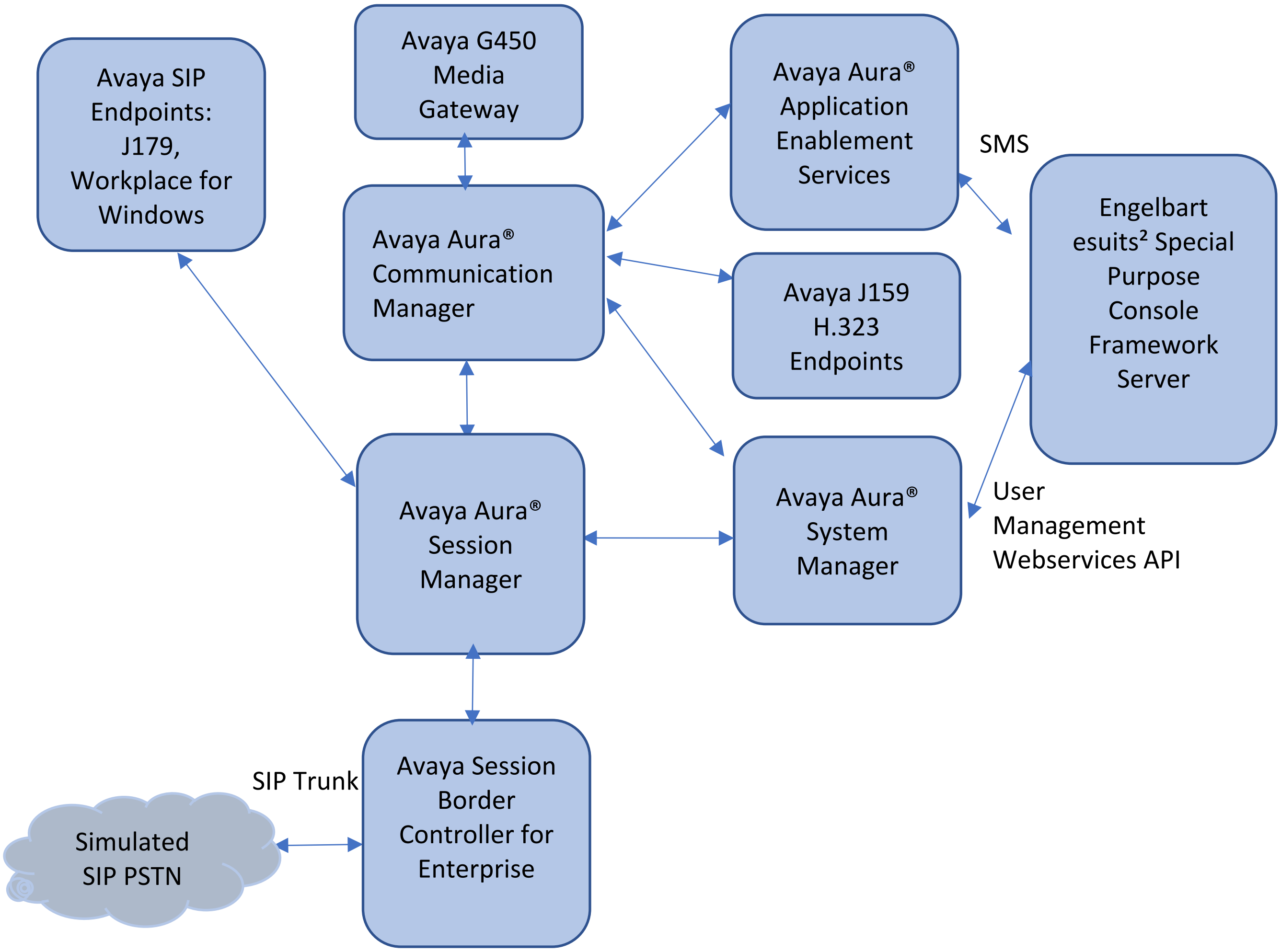

Avaya SIP Endpoints: J179, Workplace for Windows
Avaya G450 Media Gateway
Avaya Aura® Application Enablement Services
SMS
Engelbart esuits² Special Purpose Console Framework Server
Avaya Aura® Communication Manager
Avaya J159 H.323 Endpoints
Avaya Aura® Session Manager
Avaya Aura® System Manager
User Management Webservices API
SIP Trunk
Simulated SIP PSTN
Avaya Session Border Controller for Enterprise

Figure 1: Compliance Testing Configuration

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya Aura® System Manager in Virtual Environment	8.1.3.4.1014185
Avaya Aura® Session Manager in Virtual Environment	8.1.3.4.813401
Avaya Aura® Communication Manager in Virtual Environment	8.1.3.4 - 01.0.890.0-27348
Avaya G450 Media Gateway	41.34.1
Avaya Aura® Media Server in Virtual Environment	8.0.2.43
Avaya Aura® Application Enablement Services in Virtual Environment	8.1.3.4.0.2-0
Avaya Session Border Controller for Enterprise in Virtual Environment	8.1.3.1-38-21632
Avaya Workplace Client for Windows	3.22.0
Avaya J179 IP Deskphone (SIP)	4.0.9
Avaya J159 IP Deskphone (H.323)	6.8.5
Engelbart esuits² myICT	1.0.0

5. Configure Avaya Aura® System Manager

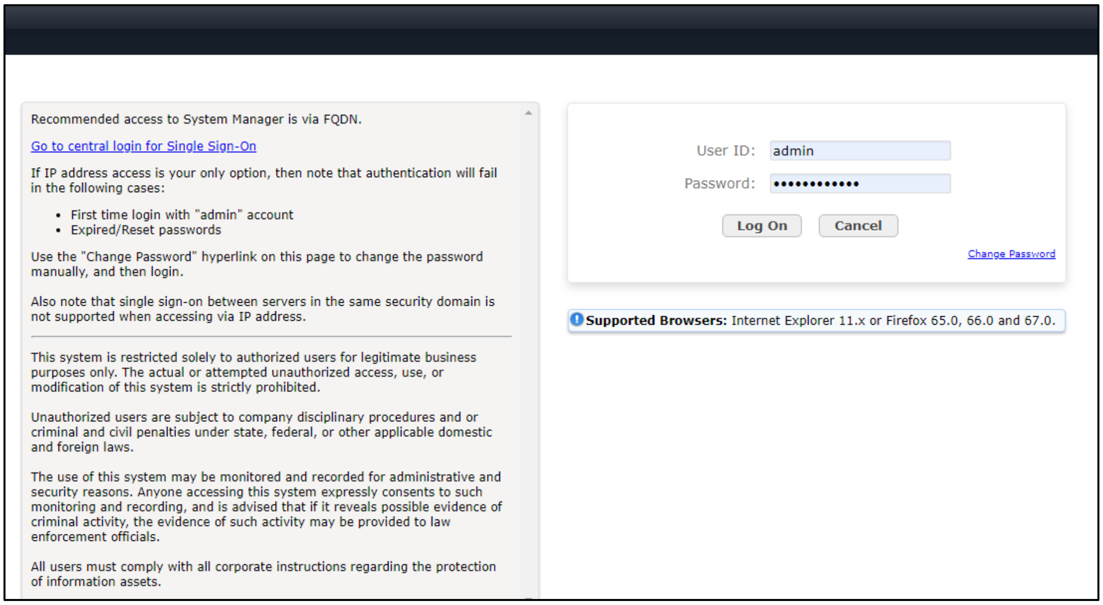
This section provides the procedures for configuring User Provisioning Rules on System Manager.

5.1. Create User Provisioning Rules on System Manager

A user provisioning rule includes a master communication profile template and a set of provisioning rules. A user provisioning rule enables predefined templates that consist of user attributes found in the communication profile of the user. In the user provisioning rule, the administrator specifies the following information to provision the user:

- Basic information that includes the communication profile password, time zone and language preference.
- The communication system that the user must use, for example, Communication Manager.
- The method to assign or create a communication profile for the user, for example, by assigning the next available extension for Communication Manager.

Configuration of User Provisioning Rules and is performed via
System Manager. Access the System Manager Administration web interface by entering the System Manager (SMGR) URL in a web browser. Log in using appropriate credentials.



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.

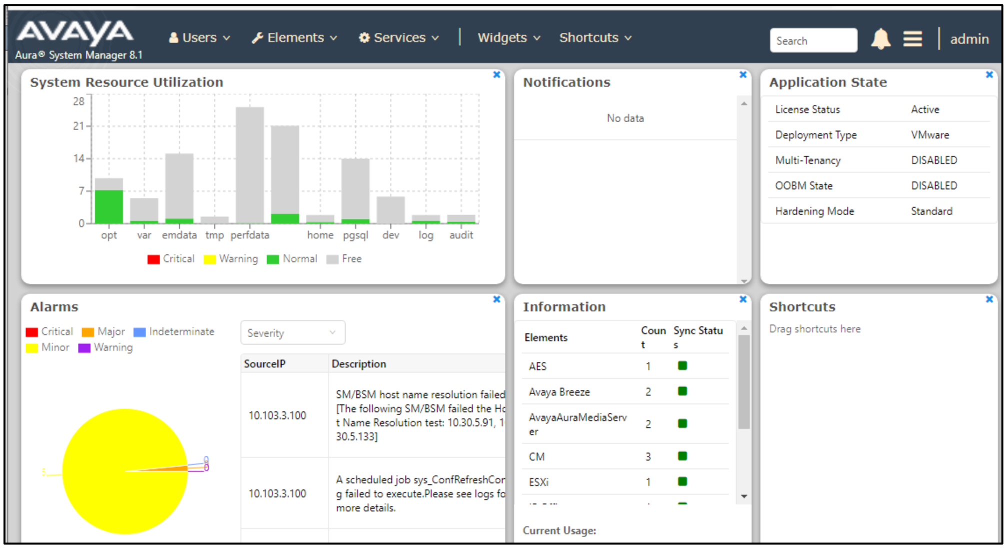
All users must comply with all corporate instructions regarding the protection of information assets.

User ID: admin

Password: ••••••••••••

Supported Browsers: Internet Explorer 11.x or Firefox 65.0, 66.0 and 67.0.

Once logged in, the following screen is displayed.



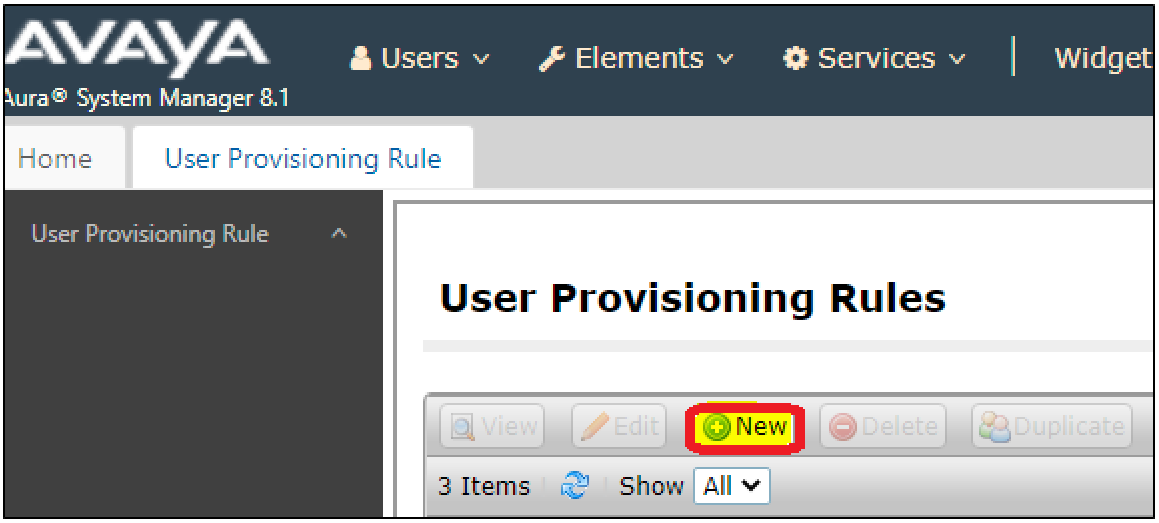
No data

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

SourceIP	Description
10.103.3.100	SM/BSM host name resolution failed [The following SM/BSM failed the Ho t Name Resolution test: 10.30.5.91, 1 30.5.133]
10.103.3.100	A scheduled job sys_ConfRefreshCon g failed to execute.Please see logs fo more details.

Elements	Count	Sync Status
AES	1	🟩
Avaya Breeze	2	🟩
AvayaAuraMediaServer	2	🟩
CM	3	🟩
ESXi	1	🟩

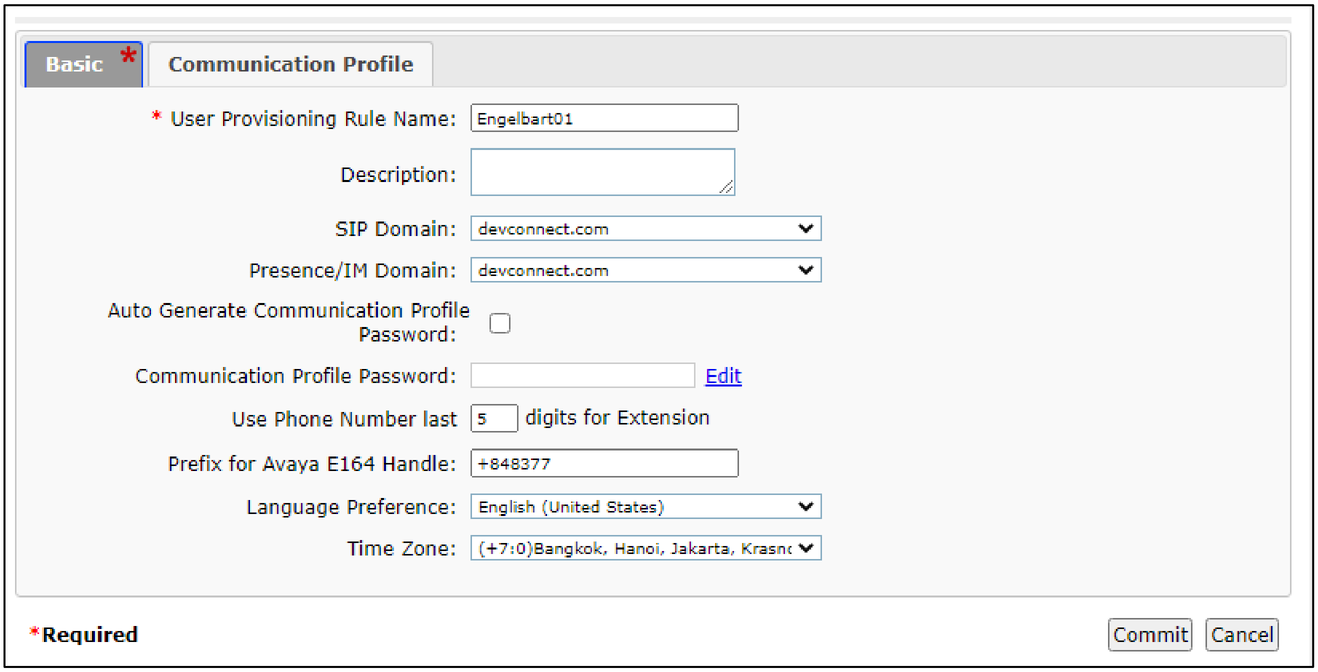
On SMGR Dashboard, select **Users → User Provisioning Rule**, click **New** to create new User Provisioning Rule.



User Provisioning Rules

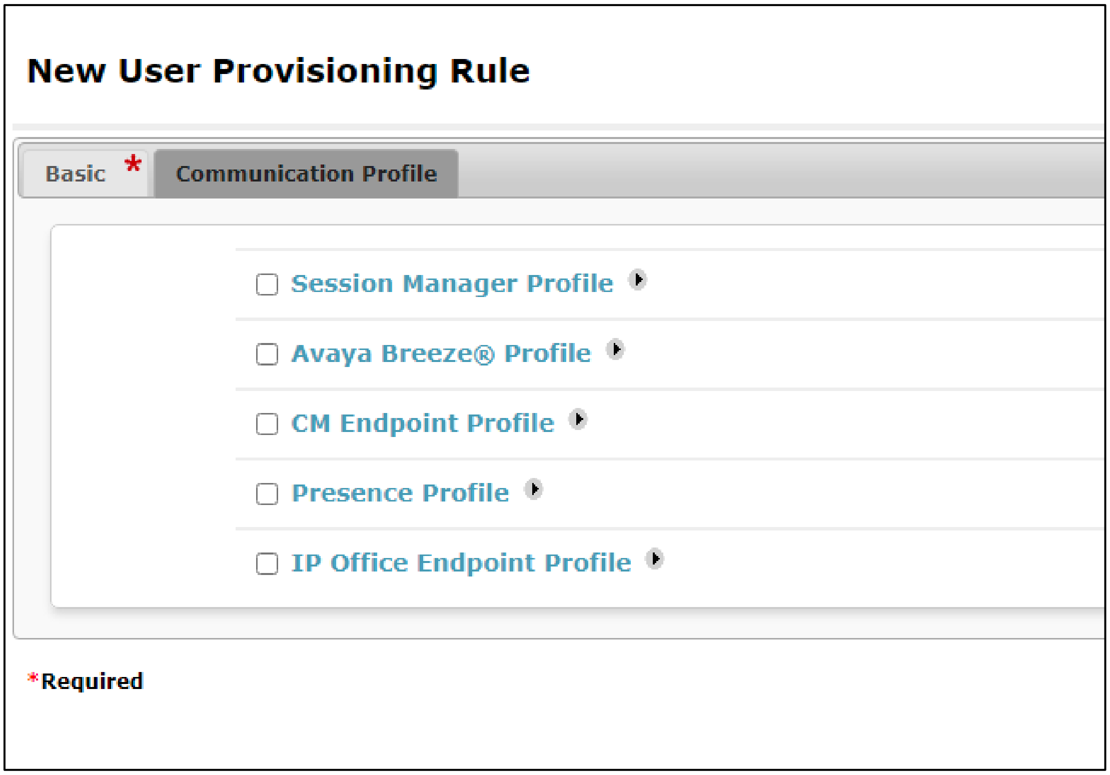
Enter following information:

User Provision Rule Name	Name of User Provision Rule Name. In this case "Engelbart01"
SIP Domain	Select a SIP Domain from Drop down list, devconnect.com
Presence/IM Domain	Select a Presence/IM Domain from Drop down list. In this case "devconnect.com"
Communication Profile Password	Enter a Password
Confirm Password	Enter Password again
User Phone Number last ... digits for Extension	Enter digits length for Communication Extension, In this case "**5**"
Prefix for Avaya E164 Handle	+848377
Language Preference	Select Language Preference in drop down list
Time Zone	Select Time Zone in drop down list



* User Provisioning Rule Name:	Engelbart01
Description:	
SIP Domain:	devconnect.com
Presence/IM Domain:	devconnect.com
Auto Generate Communication Profile Password:	□
Communication Profile Password:	Edit
Use Phone Number last	5 digits for Extension
Prefix for Avaya E164 Handle:	+848377
Language Preference:	English (United States)
Time Zone:	(+7:0)Bangkok, Hanoi, Jakarta, Krasnc

Select the **Communication Profile** tab.



New User Provisioning Rule

□ Session Manager Profile

□ Avaya Breeze® Profile

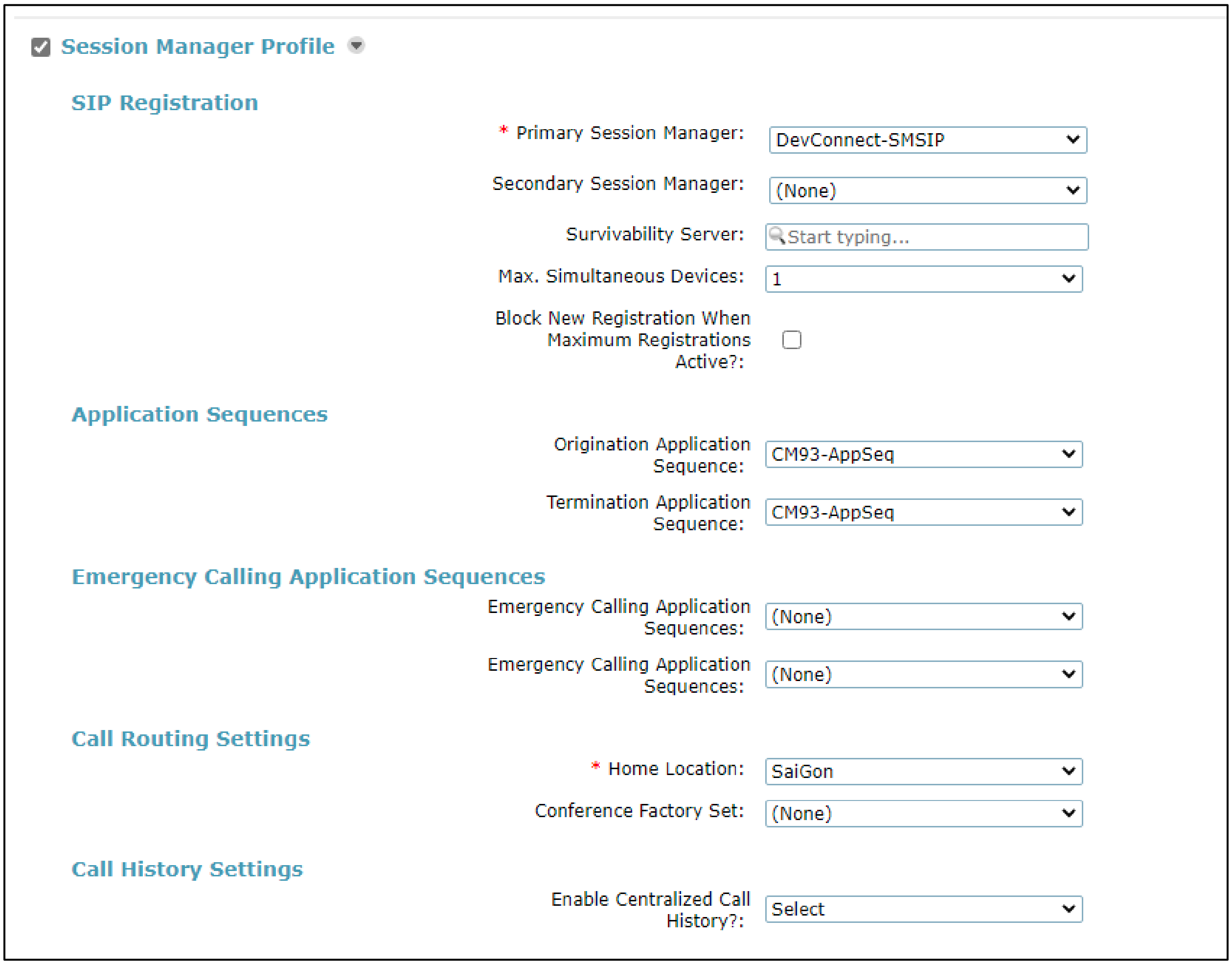
□ CM Endpoint Profile

□ Presence Profile

□ IP Office Endpoint Profile

*Required

Enable **Session Manager Profile** and enter the **Primary Session Manager**, **Origination Application Sequence**, **Termination Application Sequence** and **Home Location** relevant to the implementation.



☑ Session Manager Profile

SIP Registration

* Primary Session Manager:	DevConnect-SMSIP
Secondary Session Manager:	(None)
Survivability Server:	Start typing...
Max. Simultaneous Devices:	1
Block New Registration When Maximum Registrations Active?:	□

Application Sequences

Origination Application Sequence:	CM93-AppSeq
Termination Application Sequence:	CM93-AppSeq

Emergency Calling Application Sequences

Emergency Calling Application Sequences:	(None)
Emergency Calling Application Sequences:	(None)

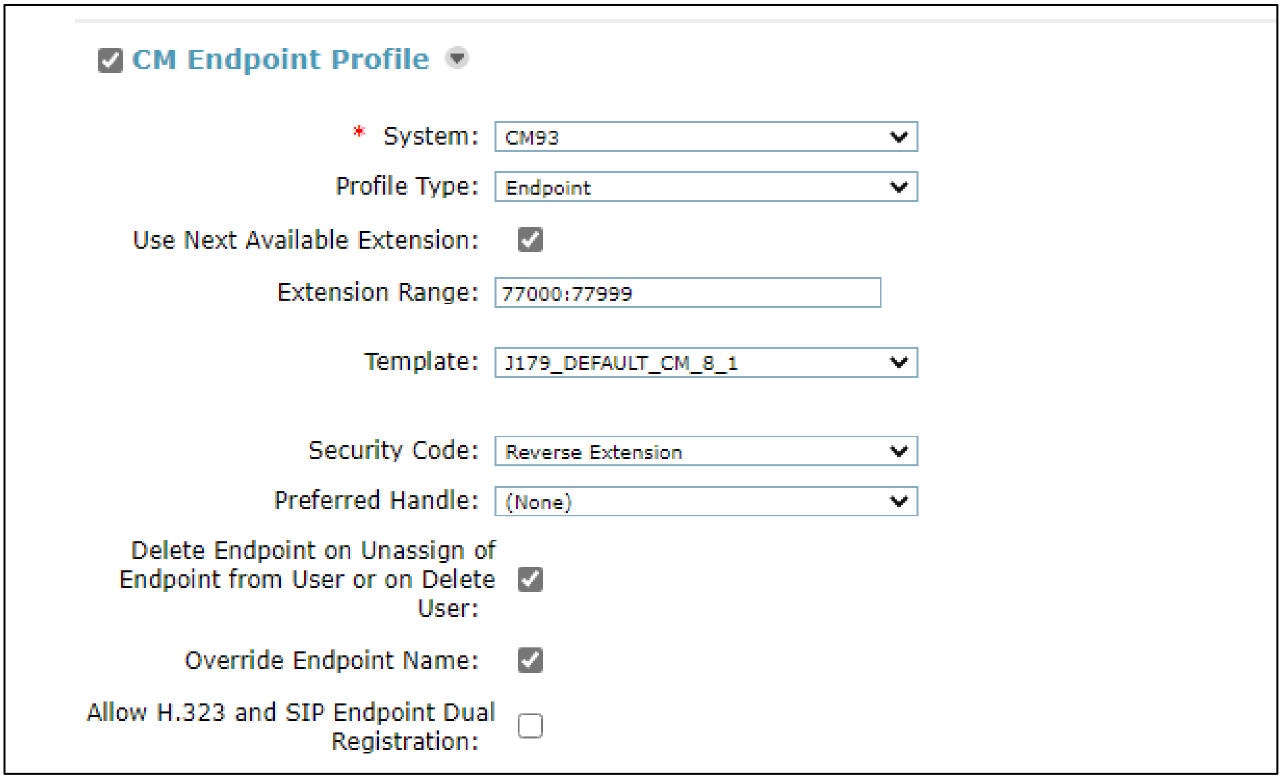
Call Routing Settings

* Home Location:	SaiGon
Conference Factory Set:	(None)

Call History Settings

Enable Centralized Call History?:	Select

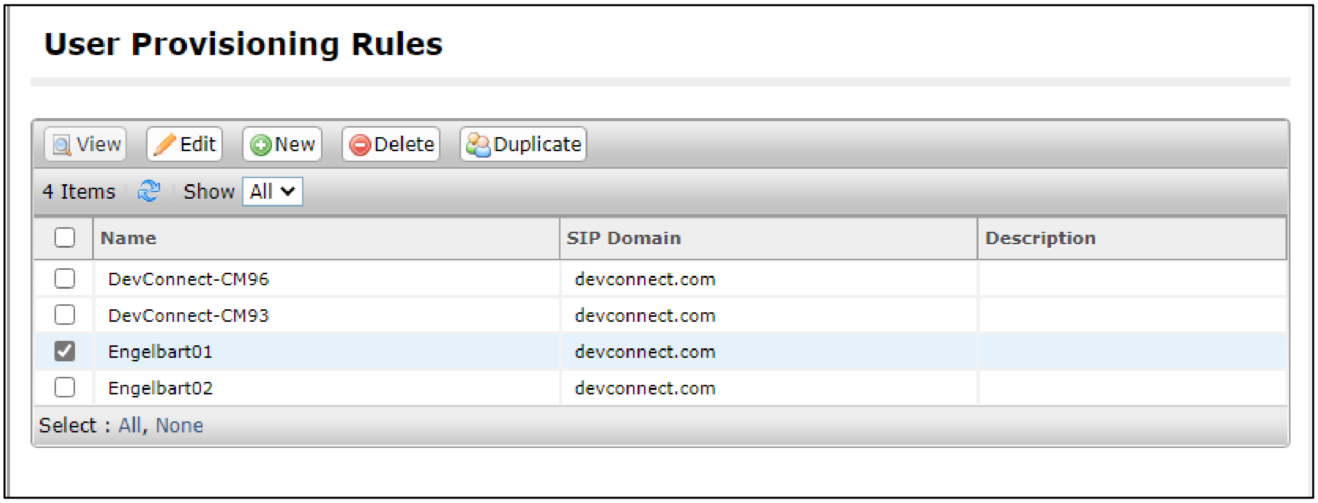
Scroll down the page and enable the **CM Endpoint Profile** section. Select the Communication Manager system from the **System** drop down box. Select **Endpoint** as the **Profile Type** and enter the appropriate **Extension Range** number. Select **J179_DEFAULT_CM_8_1** as the **Template** and select **Security Code** as **Extension/Reverse Extension**.



☑ CM Endpoint Profile

* System:	CM93
Profile Type:	Endpoint
Use Next Available Extension:	☑
Extension Range:	77000:77999
Template:	J179_DEFAULT_CM_8_1
Security Code:	Reverse Extension
Preferred Handle:	(None)
Delete Endpoint on Unassign of Endpoint from User or on Delete User:	☑
Override Endpoint Name:	☑
Allow H.323 and SIP Endpoint Dual Registration:	□

Click **Commit** to save **User Provisioning Rule**. The new User Provisioning Rule is shown in list below.



User Provisioning Rules

□	Name	SIP Domain	Description
□	DevConnect-CM96	devconnect.com	
□	DevConnect-CM93	devconnect.com	
☑	Engelbart01	devconnect.com	
□	Engelbart02	devconnect.com	

Select : All, None

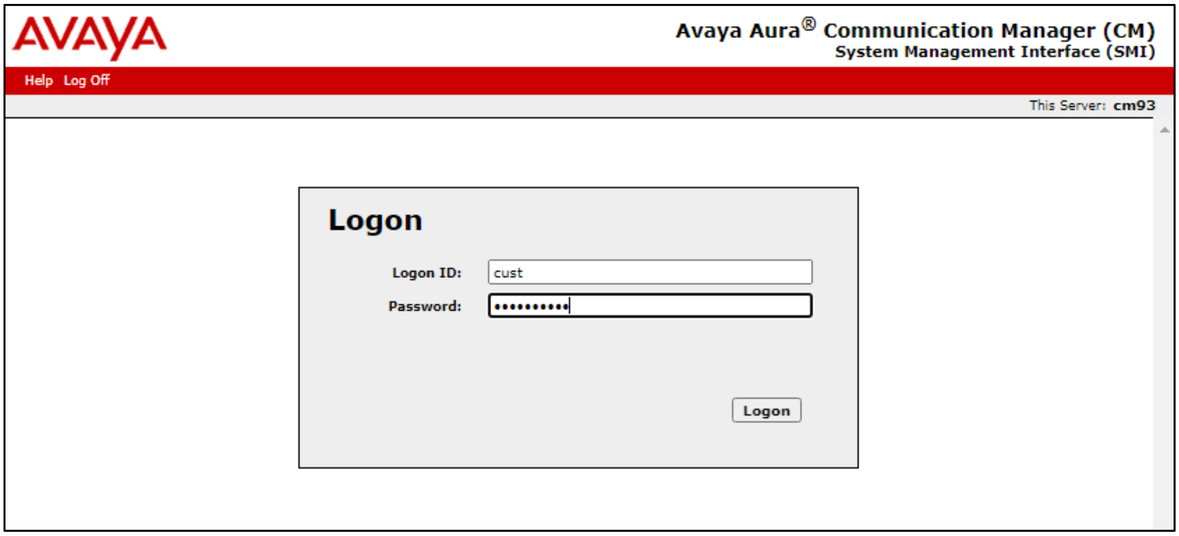
In this Compliance testing, using two User Provisioning Rule: **Engelbart01** and **Engelbart02**

6. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager to add new user on Communication Manager for SMS service.

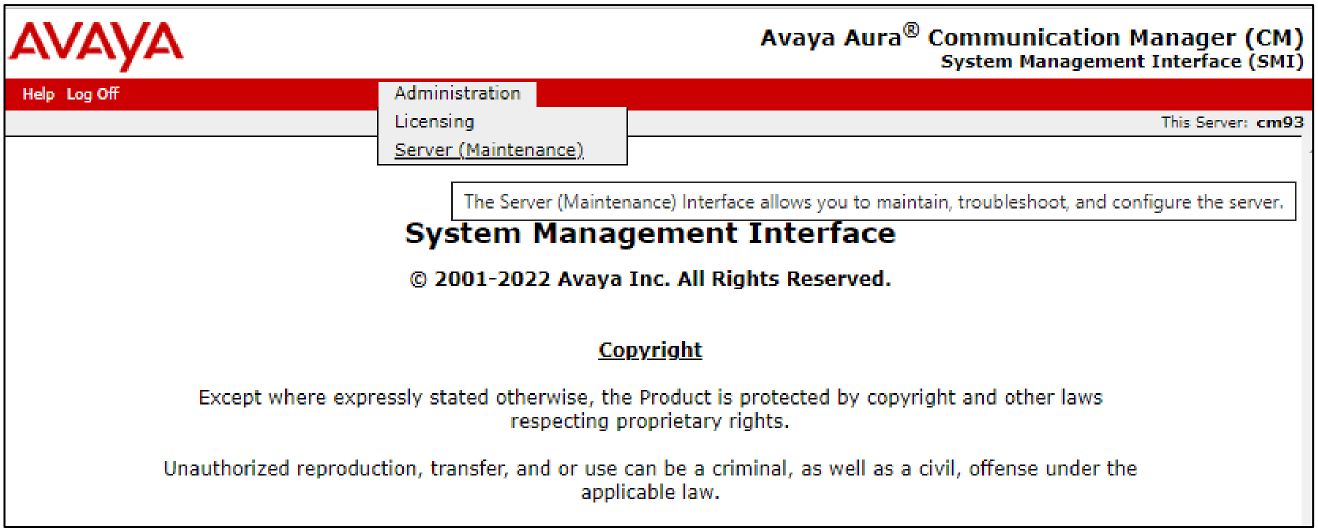
6.1. Add new user on Communication Manager for SMS service

A new user for SMS service needs to be created on Communication Manager. Open a browser session to Communication Manager and log in as shown below. Enter the proper credentials and click on **Logon**.


AVAYA
Avaya Aura® Communication Manager (CM)
System Management Interface (SMI)
Help
Log Off
This Server: cm93
Logon
Logon

Logon ID: cust
Password: ••••••••••

Once logged in, click on **Administration** at the top of the page and select **Server (Maintenance)** from the drop-down menu.



The Server (Maintenance) Interface allows you to maintain, troubleshoot, and configure the server.

System Management Interface

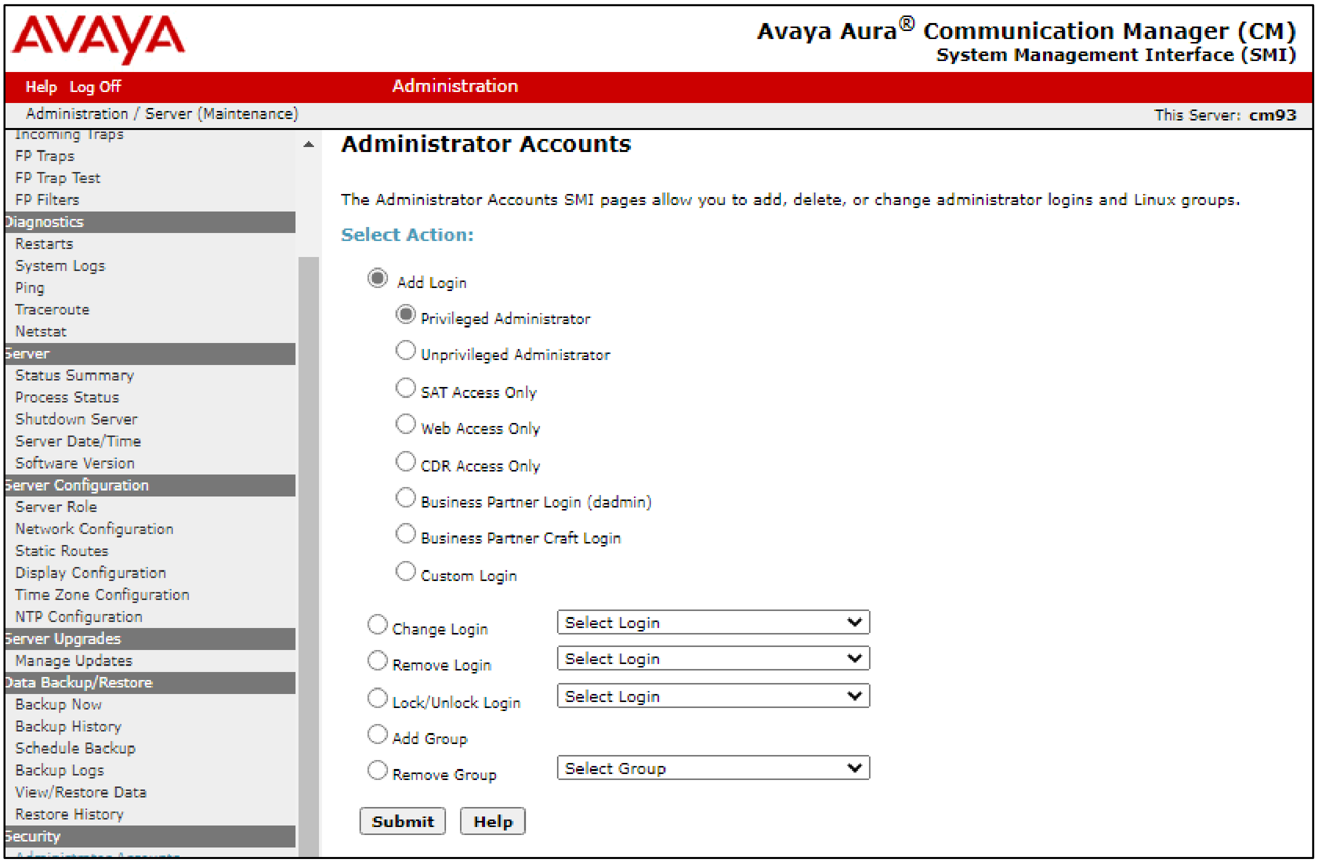
© 2001-2022 Avaya Inc. All Rights Reserved.

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.

In the left window select **Security → Administrator Accounts**. In the main window, select **Add Login**. For these compliance testing, **Privileged Administrator** was chosen to allow read and write to the Communication Manager. Select **Submit** when done.



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

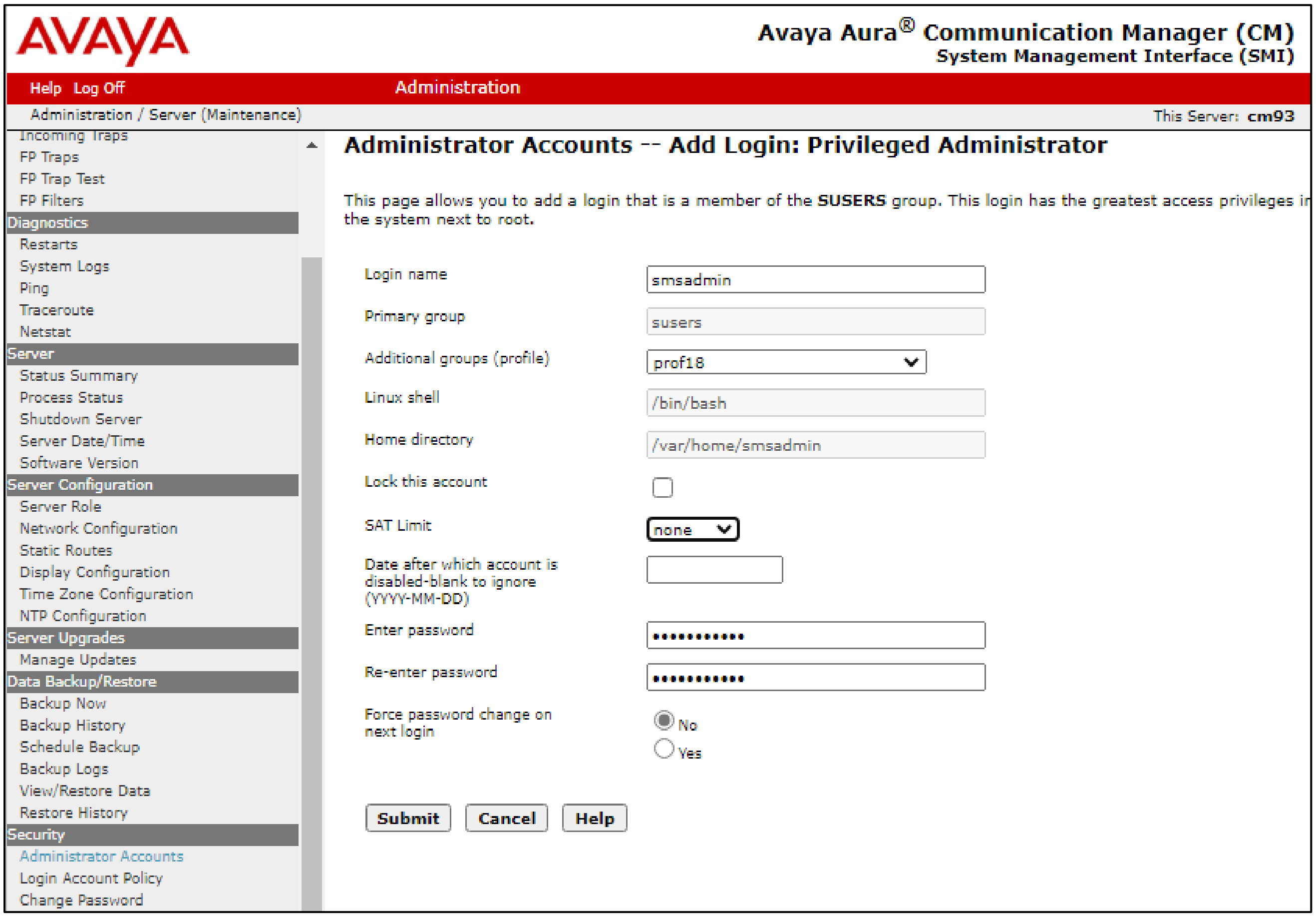
○ Remove Login — Select Login

○ Lock/Unlock Login — Select Login

○ Add Group

○ Remove Group — Select Group

Enter the **Login name** and a suitable **password**. Click on **Submit** when done.



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 access privileges in the system next to root.

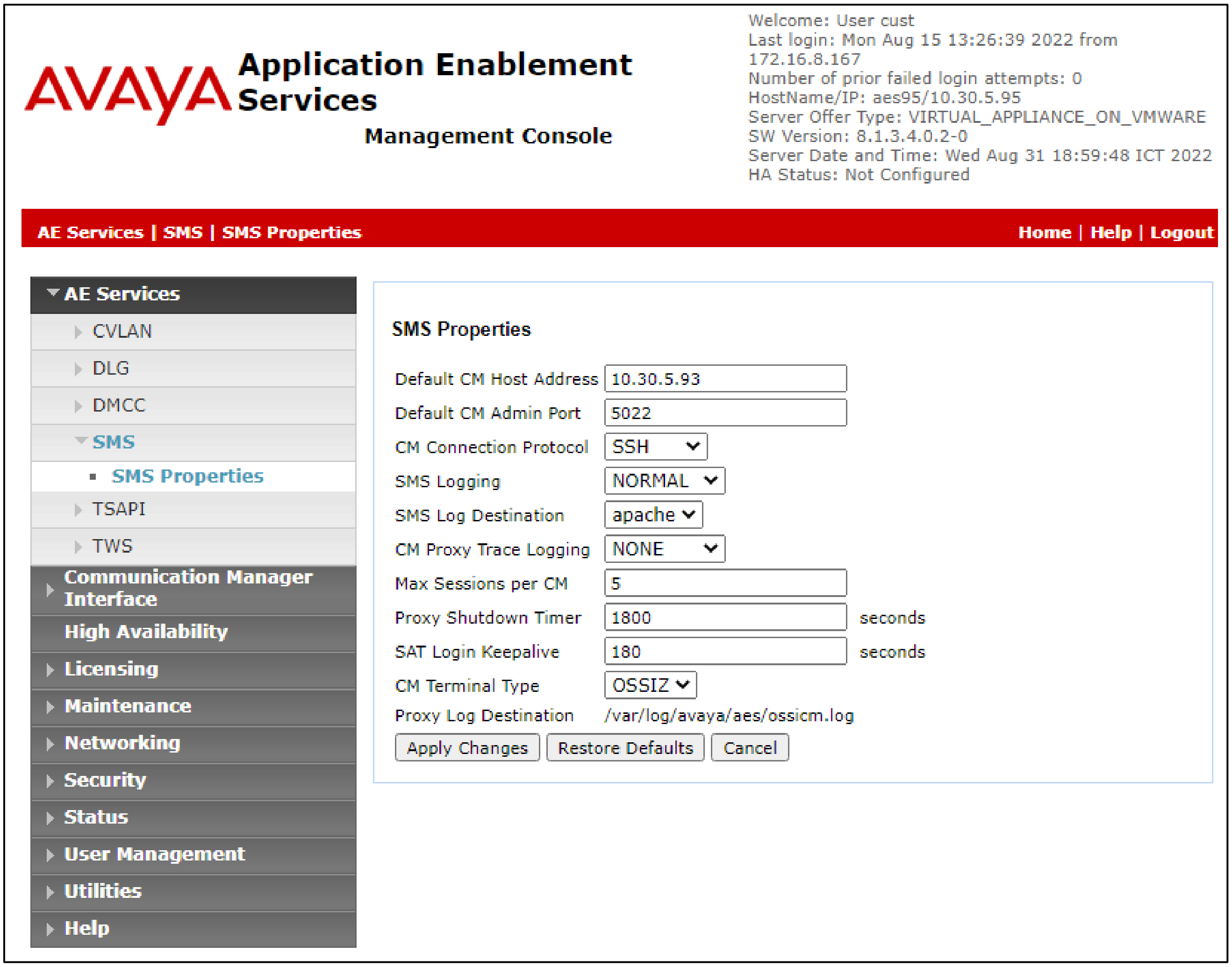
Login name	smsadmin
Primary group	susers
Additional groups (profile)	prof18
Linux shell	/bin/bash
Home directory	/var/home/smsadmin
Lock this account	□
SAT Limit	none
Date after which account is disabled-blank to ignore (YYYY-MM-DD)	
Enter password	•••••••••••
Re-enter password	•••••••••••
Force password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

7. Configure Avaya Aura® Application Enablement Services

This section provides the procedures for configuring Application Enablement Services to configure SMS.

7.1. Configure SMS

Select **AE Services** → **SMS** → **SMS Properties**. Configure all fields as in the screenshot below with **Default CM Host Address** using Communication Manager IP address and **Default CM Admin Port** with 5022.



Welcome: User cust
Last login: Mon Aug 15 13:26:39 2022 from 172.16.8.167
Number of prior failed login attempts: 0
HostName/IP: aes95/10.30.5.95
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.3.4.0.2-0
Server Date and Time: Wed Aug 31 18:59:48 ICT 2022
HA Status: Not Configured

SMS Properties

Default CM Host Address	10.30.5.93	
Default CM Admin Port	5022	
CM Connection Protocol	SSH	
SMS Logging	NORMAL	
SMS Log Destination	apache	
CM Proxy Trace Logging	NONE	
Max Sessions per CM	5	
Proxy Shutdown Timer	1800	seconds
SAT Login Keepalive	180	seconds
CM Terminal Type	OSSIZ	
Proxy Log Destination	/var/log/avaya/aes/ossicm.log	

8. Configure Engelbart esuits² myICT

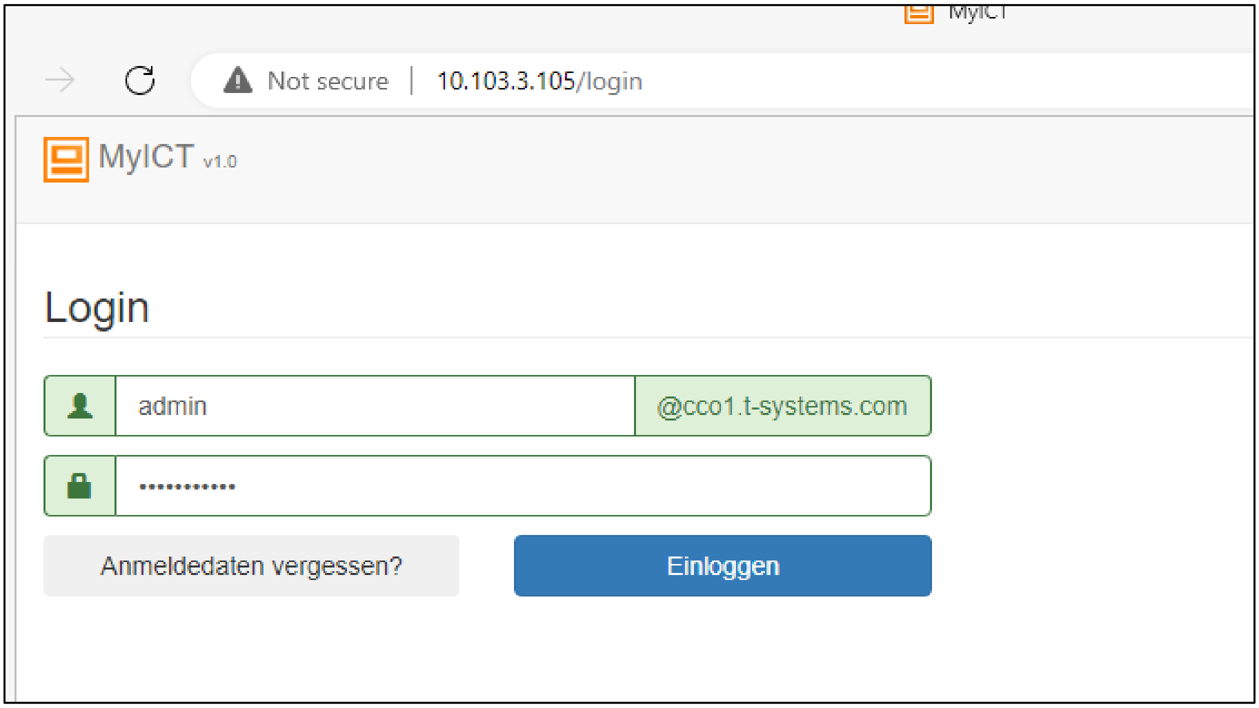
All installation and basic configuration related to Engelbart esuits² myICT is performed by Engelbart engineers and, thus is not documented.

9. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Engelbart esuits² myICT.

9.1. Verify Engelbart esuits² myICT

From the Windows PC, launch the web-based interface and login with user provided by Engelbart.



Not secure | 10.103.3.105/login

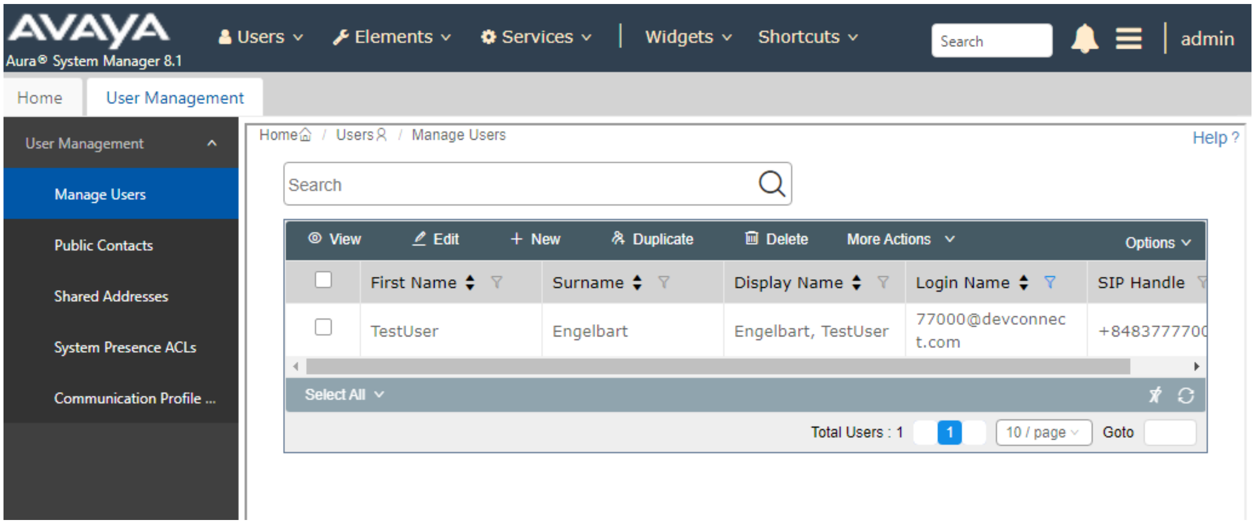
MyICT v1.0

Login

admin @cco1.t-systems.com

•••••••••••

From Engelbart esuits² myICT, creating new user follow Engelbart esuits² myICT support document. Login to System Manager and verify that the new user above is created.



☐	First Name	Surname	Display Name	Login Name	SIP Handle
☐	TestUser	Engelbart	Engelbart, TestUser	77000@devconnect.com	+848377770

10. Conclusion

These Application Notes describe the configuration steps required for the Engelbart esuits² myICT 1.0.0 to successfully interoperate with Avaya Aura® Communication Manager 8.1.3.4 and Avaya Aura® Application Enablement Services 8.1.3.4. All feature and serviceability test cases were completed successfully.

11. Additional References

This section references the Avaya and Engelbart esuits² myICT product documentation that are relevant to these Application Notes.

Product documentation for Avaya products may be found at http://support.avaya.com.

1. *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 12, July 2021
2. *Administering Avaya Aura® Session Manager*, Release 8.1.x, Issue 10, Sept 2021
3. *Administering Avaya Aura® System Manager*, Release 8.1.x, Issue 17, Nov 2021
4. *Administering Avaya Aura® Application Enablement Services*, Release 8.1.x, Issue 12, Oct 2021

Product Documentation for Engelbart products may be found at https://www.engelbart-software.com/

©2023 Avaya Inc. All Rights Reserved.
Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. 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.