Avaya Solution & Interoperability Test Lab

Application Notes for Hitachi Recware III with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services R6.3 using VoIP Recording – Issue 1.1

Abstract

These Application Notes describe the configuration steps required for Hitachi Recware III to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services R6.3 using VoIP recording. Hitachi Recware III is a call recording solution that uses a port mirroring method to capture media.

In the compliance testing, Hitachi Recware III used the Telephony Services Application Programming Interface from Avaya Aura® Application Enablement Services to monitor skill groups and agent stations on Avaya Aura® Communication Manager, and the port mirroring method to capture the media associated with the monitored agents for call recording.

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 Hitachi Recware III to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services R6.3 using VoIP recording. For RTP recording, Hitachi Recware III uses a port mirroring method.

In the compliance testing, Hitachi Recware III used the Telephony Services Application Programming Interface (TSAPI) from Avaya Aura® Application Enablement Services to monitor skill groups and agent stations on Avaya Aura® Communication Manager, and a port mirroring method to capture the media associated with the monitored agents for call recording.

The TSAPI interface is used by Hitachi Recware III to monitor skill groups and agent stations on Avaya Aura® Communication Manager. When there is an active call at the monitored agent/station, Hitachi Recware III is informed of the call via event reports from the TSAPI interface. Hitachi Recware III starts the call recording by using the replicated media from the port mirroring method. The TSAPI event reports are also used to determine when to stop the call recordings.

2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of the Recware III application, the application automatically requests monitoring on skill groups and agent stations and performs device queries using TSAPI.

For the manual part of the testing, each call was handled manually on the agent telephone with generation of unique audio content for the recordings. Necessary user actions such as hold and resume were performed from the agent telephones to test the different call scenarios.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to Recware III.

The verification of tests included use of Recware III logs for proper message exchanges, and use of the Recware III Client application for proper logging and playback of calls.

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.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on Recware III:

- Handling of TSAPI messages in areas of event notification and value queries.
- Proper recording, logging, and playback of calls for scenarios involving inbound, outbound, internal, external, ACD, non-ACD, hold/resume, multiple calls, multiple agents, conference, and transfer.

The serviceability testing focused on verifying the ability of Recware III to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to Recware III.

2.2. Test Results

All test cases were executed, and the following were observations on Recware III:

- When the TSAPI client queries for "cstaGetDeviceList", a worktop name has to be selected. Without it, no device list will be returned. During the Compliance test, the AES firmware used was 6.3.3. However, the image that Hitachi brought in for installation of the TSAPI client was 6.1.1. Thus, the combination of AES 6.3.3 and TSAPI client 6.1.1 was tested.

2.3. Support

Technical support on Recware III can be obtained through the following:

- **Phone:** +81-50-3163-1797 (English, available 9:00 – 17:00 Japan time/ business days)
  +81-50-3101-2431 (Japanese, available 9:00 – 17:00 Japan time/ business days)
- **Email:** www-info-recware@ml.itg.hitachi.co.jp

3. Reference Configuration

Recware III is a call recording solution the can record voice calls between endpoints and VoIP gateways. Recware III consists of a Manager Server (MNG), Logger Server (SLGR) and a Gateway Server (AS-GW).

- The Logger Server receives duplicated data from the mirror port of a network switch that voice data streams traverse. The Logger Server filters out RTP stream from the duplicated data and generates it into a recording file. It also has a function to monitor H.323 registration from phones to gather extension number information automatically.

- The Gateway Server receives call interaction information from Communication Manager and Application Enablement Services through the TSAPI interface, and adds the metadata to each recorded VoIP data to be easily queried.

- The Manager Server handles multiple Logger Servers and provides a centralized operation for a large system environment.

Recware III uses a Client PC (Windows 7 Enterprise – Japanese Edition) to review and playback the call recordings. The RTP streams for agents with Avaya IP Deskphones were mirrored from the layer 2 switch, and replicated over to the SLGR.

The detailed administration of basic connectivity between Communication Manager, Application Enablement Services, System Manager, Session Manager, and of contact center devices are not the focus of these Application Notes and will not be described. In addition, the port mirroring of the layer 2 switch is also outside the scope of these Application Notes and will not be described.

In the compliance testing, Recware III monitored the skill groups and agent station extensions shown in the table below.

Device Type	Extension
VDN	72079
Skill Group	72089
Supervisor	72003
Agent ID	72091 - 72095
Agent Station	H.323 - 72001,72002 SIP – 72021, 72022

Figure 1 displays the network topology used during compliance testing.

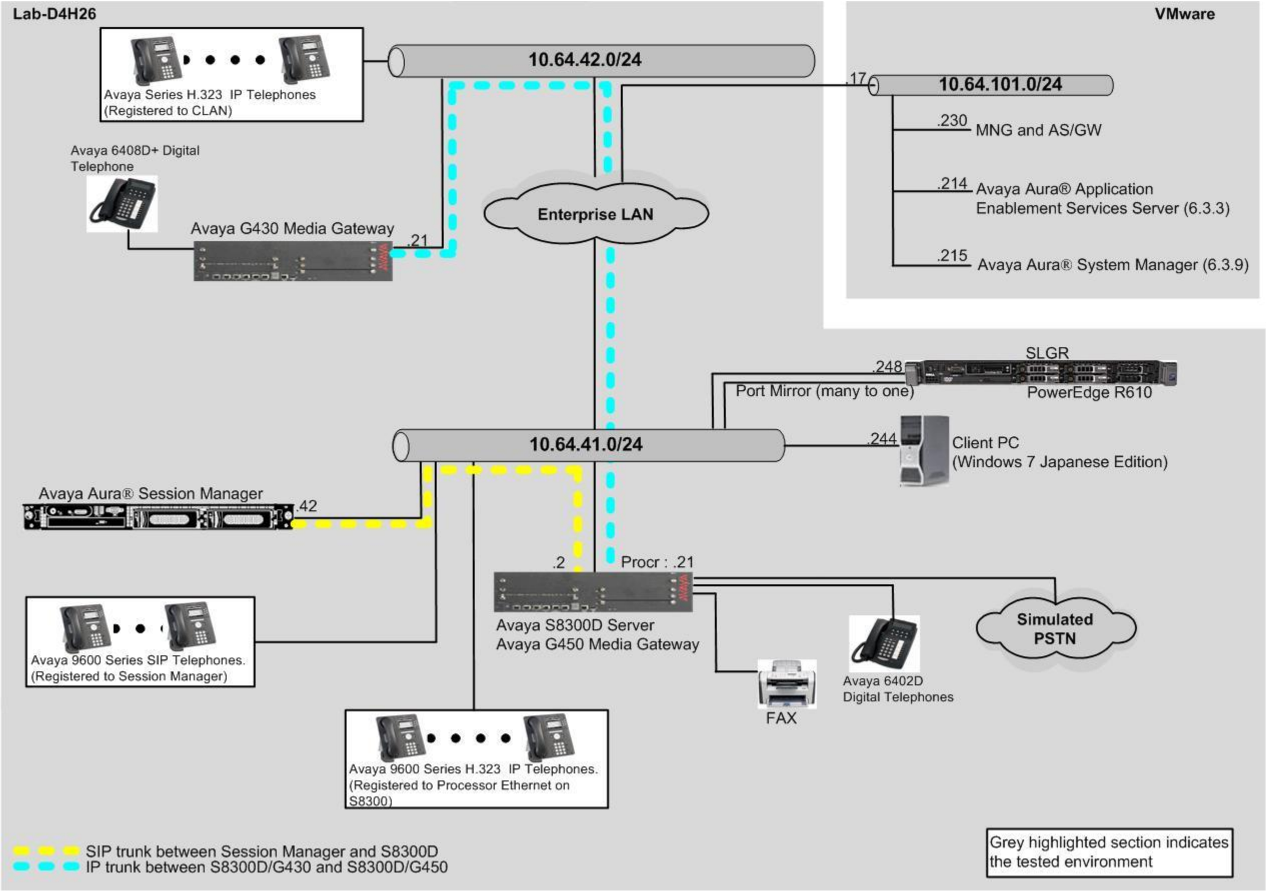

Lab-D4H26
VMware
Avaya Series H.323 IP Telephones
(Registered to CLAN)
10.64.42.0/24
.17
10.64.101.0/24
.230
MNG and AS/GW
.214
Avaya Aura® Application Enablement Services Server (6.3.3)
.215
Avaya Aura® System Manager (6.3.9)
Avaya 6408D+ Digital Telephone
Enterprise LAN
Avaya G430 Media Gateway
.21
SLGR
.248
Port Mirror (many to one)
PowerEdge R610
10.64.41.0/24
.244
Client PC
(Windows 7 Japanese Edition)
Avaya Aura® Session Manager
.42
.2
Procr : .21
Avaya S8300D Server
Avaya G450 Media Gateway
Simulated PSTN
Avaya 9600 Series SIP Telephones.
(Registered to Session Manager)
FAX
Avaya 6402D Digital Telephones
Avaya 9600 Series H.323 IP Telephones.
(Registered to Processor Ethernet on S8300)
SIP trunk between Session Manager and S8300D
IP trunk between S8300D/G430 and S8300D/G450
Grey highlighted section indicates the tested environment

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® Communication Manager on Avaya S8300D Server with Avaya G450 Media Gateway	R016x.03.0.124.0-21754 36.9
Avaya Aura® Application Enablement Services TSAPI Client	6.3.3 (6.3.3.0.10-0) 6.1.1
Avaya Aura® Session Manager	6.3.9
Avaya Aura® System Manager	6.3.9
Avaya 96x1 IP Deskphone (H.323)	6.2.3
Avaya 9641G IP Deskphone (SIP)	6.4.1.25
Avaya 96xx IP Deskphone (H.323)	3.1
Hitachi Recware III • MNG • AS-GW • SLGR • IP/DNM Type A	 03-40 03-30-/B 03-40 03-20
Hitachi Recware III Client PC	Windows 7 Enterprise SP1 (Japanese Edition)

5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager. The procedures include the following areas:

- Verify license
- Administer CTI link
- Configure AES connection

5.1. Verify License

Log in to the System Access Terminal to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the “display system-parameters customer-options” command to verify that the **Computer Telephony Adjunct Links** customer option is set to “y” on **Page 3**. If this option is not set to “y”, then contact the Avaya sales team or business partner for a proper license file.

```
change system-parameters customer-options                       Page   3 of  11
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? y           Audible Message Waiting? y
        Access Security Gateway (ASG)? n               Authorization Codes? y
        Analog Trunk Incoming Call ID? y                        CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? y                          CAS Main? n
Answer Supervision by Call Classifier? y                 Change COR by FAC? n
                                  ARS? y  Computer Telephony Adjunct Links? y
                 ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? n                       DCS (Basic)? y
          ASAI Link Core Capabilities? n                 DCS Call Coverage? y
          ASAI Link Plus Capabilities? n                DCS with Rerouting? y
       Async. Transfer Mode (ATM) PNC? n
  Async. Transfer Mode (ATM) Trunking? n    Digital Loss Plan Modification? y
              ATM WAN Spare Processor? n                           DS1 MSP? y
                                 ATMS? y             DS1 Echo Cancellation? y
                  Attendant Vectoring? y
```

5.2. Administer CTI Link

Add a CTI link using the “add cti-link n” command, where “n” is an available CTI link number. Enter an available extension number in the **Extension** field. Note that the CTI link number and extension number may vary. Enter “ADJ-IP” in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.

```
add cti-link 4                                                  Page   1 of   3
                                    CTI LINK
 CTI Link: 4
Extension: 72000
     Type: ADJ-IP
                                                                        COR: 1

     Name: TSAPI
```

5.3. Configure Avaya Aura® Application Enablement Services Connection

Add an AES connection using the “change ip-services” command. On Page 1, set **Service Type** to “AESVCS”, and enable the service.

```
change ip-services                                              Page   1 of   4

                                   IP SERVICES
 Service      Enabled     Local         Local        Remote       Remote
  Type                    Node          Port         Node         Port
AESVCS         y       procr           8765
CDR1                   procr           0        microcall        9000
CDR2                   procr           0        rdtt-2           9001
```

On Page 4, enter a valid **AE Services Server** name, enter the password, and enable the connection. When there is a connection between Communication Manager and Application Enablement Services, the status will change to “in use”.

```
change ip-services                                              Page   4 of   4
                           AE Services Administration

  Server ID    AE Services        Password          Enabled    Status
                  Server
     1:       AES-1            *                     y        in use
     2:
     3:
     4:
     5:
```

6. Configure Avaya Aura® Application Enablement Services

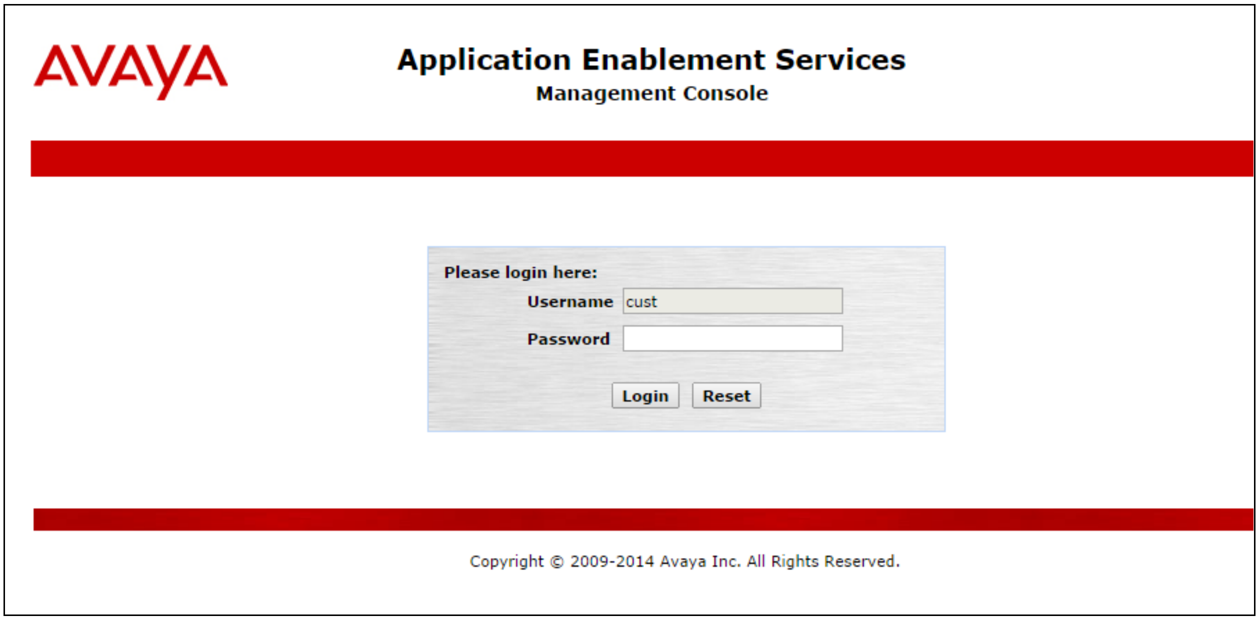
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Enable security database
- Restart TSAPI service
- Obtain Tlink name
- Create Devices
- Create Devices Groups
- Create Worktops
- Administer Recware III user

6.1. Launch OAM Interface

Access the OAM web-based interface by using the URL https://<ip-address> in an Internet browser window, where "ip-address" is the IP address of the Application Enablement Services server.

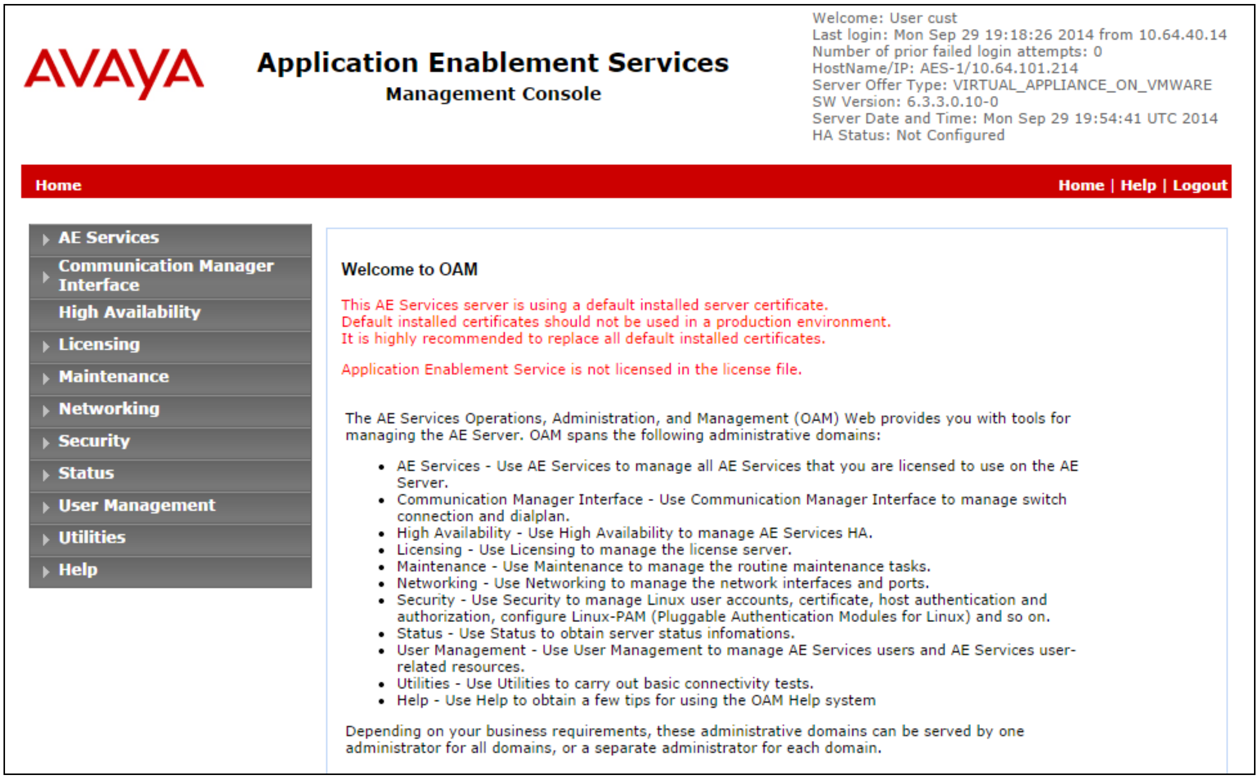
The **Please login here** screen is displayed. Log in using the appropriate credentials.


AVAYA
Application Enablement Services
Management Console
Please login here:
Login
Reset
Copyright © 2009-2014 Avaya Inc. All Rights Reserved.

Username cust

Password

The **Welcome to OAM** screen is displayed next.



Welcome: User cust
Last login: Mon Sep 29 19:18:26 2014 from 10.64.40.14
Number of prior failed login attempts: 0
HostName/IP: AES-1/10.64.101.214
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.3.0.10-0
Server Date and Time: Mon Sep 29 19:54:41 UTC 2014
HA Status: Not Configured

Welcome to OAM

This AE Services server is using a default installed server certificate.
Default installed certificates should not be used in a production environment.
It is highly recommended to replace all default installed certificates.

Application Enablement Service is not licensed in the license file.

The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

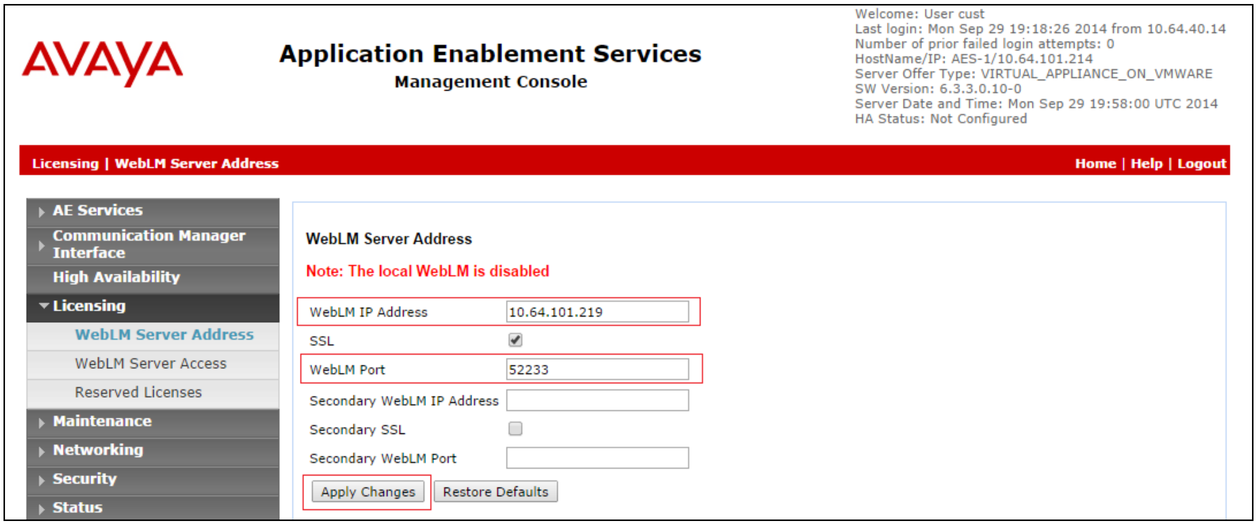
- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- High Availability - Use High Availability to manage AE Services HA.
- Licensing - Use Licensing to manage the license server.
- Maintenance - Use Maintenance to manage the routine maintenance tasks.
- Networking - Use Networking to manage the network interfaces and ports.
- Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.
- Status - Use Status to obtain server status infomations.
- User Management - Use User Management to manage AE Services users and AE Services user-related resources.
- Utilities - Use Utilities to carry out basic connectivity tests.
- Help - Use Help to obtain a few tips for using the OAM Help system

Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain.

6.2. Verify License

Select **Licensing → WebLM Server Address** in the left pane, to display the **Server Address** screen. Provide the WebLM server IP address and port. Click **Apply Changes**.

During the compliance test, a WebLM server was created in VMware.



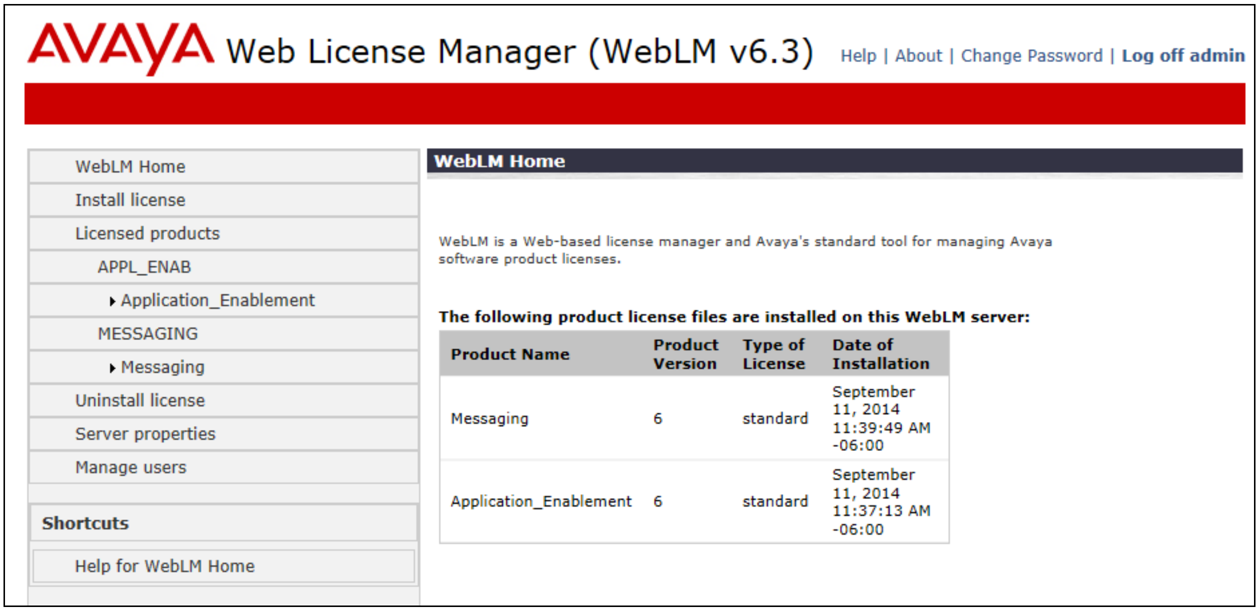
Welcome: User cust
Last login: Mon Sep 29 19:18:26 2014 from 10.64.40.14
Number of prior failed login attempts: 0
HostName/IP: AES-1/10.64.101.214
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.3.0.10-0
Server Date and Time: Mon Sep 29 19:58:00 UTC 2014
HA Status: Not Configured

WebLM Server Address

Note: The local WebLM is disabled

WebLM IP Address	10.64.101.219
SSL	☑
WebLM Port	52233
Secondary WebLM IP Address	
Secondary SSL	☐
Secondary WebLM Port	

Select **Licensing → WebLM Server Access** in the left pane, to display the **WebLM License Administration** screen (not shown). Provide appropriate credentials to access. The **WebLM Home** page is then displayed.



WebLM Home

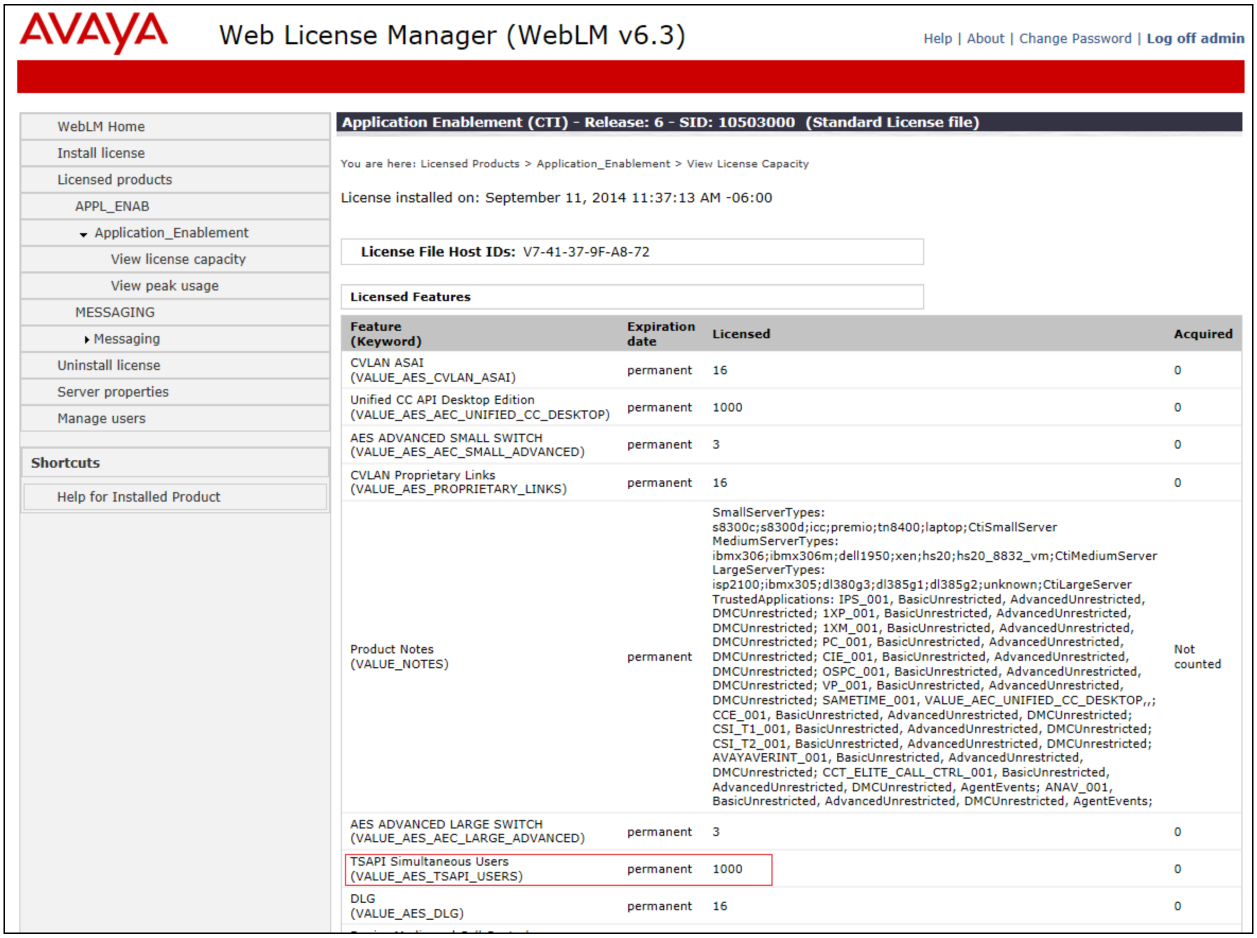
WebLM is a Web-based license manager and Avaya's standard tool for managing Avaya software product licenses.

The following product license files are installed on this WebLM server:

Product Name	Product Version	Type of License	Date of Installation
Messaging	6	standard	September 11, 2014 11:39:49 AM -06:00
Application_Enablement	6	standard	September 11, 2014 11:37:13 AM -06:00

Select **Licensed products → APPL_ENAB → Application_Enablement** in the left pane, to display the **Application Enablement (CTI)** screen in the right pane.

Verify that there are sufficient licenses for **TSAPI Simultaneous Users**, as shown below.



Application Enablement (CTI) - Release: 6 - SID: 10503000 (Standard License file)

You are here: Licensed Products > Application_Enablement > View License Capacity

License installed on: September 11, 2014 11:37:13 AM -06:00

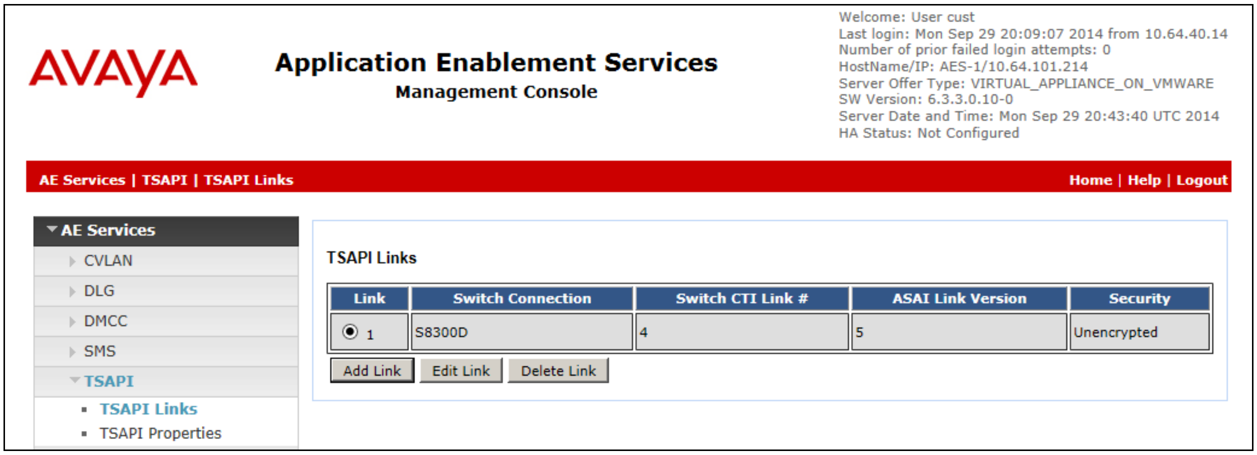
License File Host IDs: V7-41-37-9F-A8-72

Licensed Features

Feature (Keyword)	Expiration date	Licensed	Acquired
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	permanent	16	0
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	permanent	1000	0
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	permanent	3	0
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	permanent	16	0
Product Notes (VALUE_NOTES)	permanent	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiSmallServer MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_8832_vm;CtiMediumServer LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;unknown;CtiLargeServer TrustedApplications: IPS_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XM_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; PC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CIE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; OSPC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; VP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AEC_UNIFIED_CC_DESKTOP,,; CCE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T1_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T2_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; AVAYAVERINT_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CCT_ELITE_CALL_CTRL_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents; ANAV_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents;	Not counted
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	permanent	3	0
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	permanent	1000	0
DLG (VALUE_AES_DLG)	permanent	16	0

6.3. Administer TSAPI Link

To administer a TSAPI link, select **AE Services** → **TSAPI** → **TSAPI Links** from the left pane of the **Application Enablement Services Management Console**. The **TSAPI Links** screen is displayed, as shown below. Click **Add Link**.



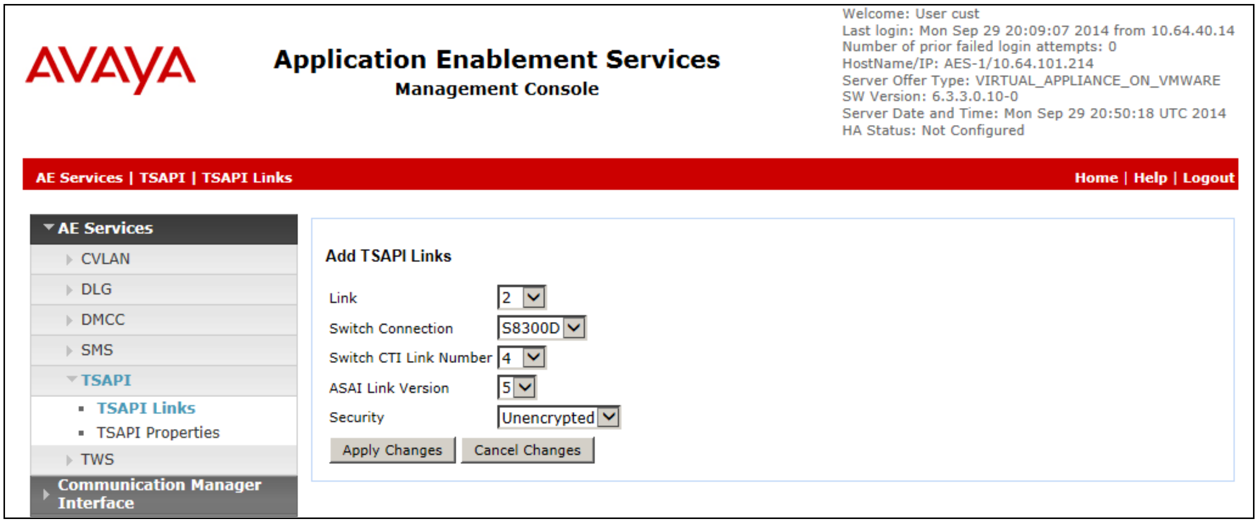
Welcome: User cust
Last login: Mon Sep 29 20:09:07 2014 from 10.64.40.14
Number of prior failed login attempts: 0
HostName/IP: AES-1/10.64.101.214
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.3.0.10-0
Server Date and Time: Mon Sep 29 20:43:40 UTC 2014
HA Status: Not Configured

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
● 1	S8300D	4	5	Unencrypted

The **Add TSAPI Links** screen is displayed next.

The **Link** field is only local to the Application Enablement Services server, and may be set to any available number. For **Switch Connection**, select the relevant switch connection from the drop-down list. In this case, the existing switch connection "S8300D" is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Retain the default values in the remaining fields.



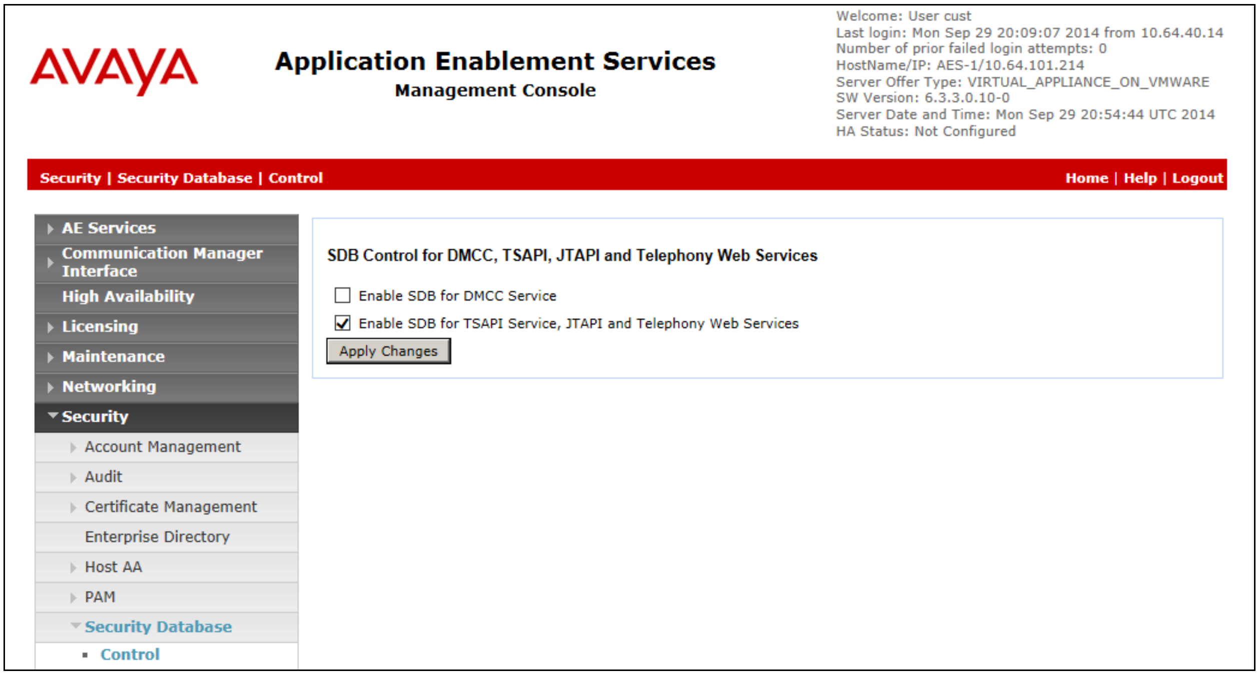
Welcome: User cust
Last login: Mon Sep 29 20:09:07 2014 from 10.64.40.14
Number of prior failed login attempts: 0
HostName/IP: AES-1/10.64.101.214
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.3.0.10-0
Server Date and Time: Mon Sep 29 20:50:18 UTC 2014
HA Status: Not Configured

Add TSAPI Links

Link: 2
Switch Connection: S8300D
Switch CTI Link Number: 4
ASAI Link Version: 5
Security: Unencrypted

6.4. Enable Security Database

Select **Security → Security Database → Control** from the left pane, to display the **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** screen in the right pane. Verify the checkbox is checked for the **Enable SDB for TSAPI Service, JTAPI and .Telephony Web Services** field.



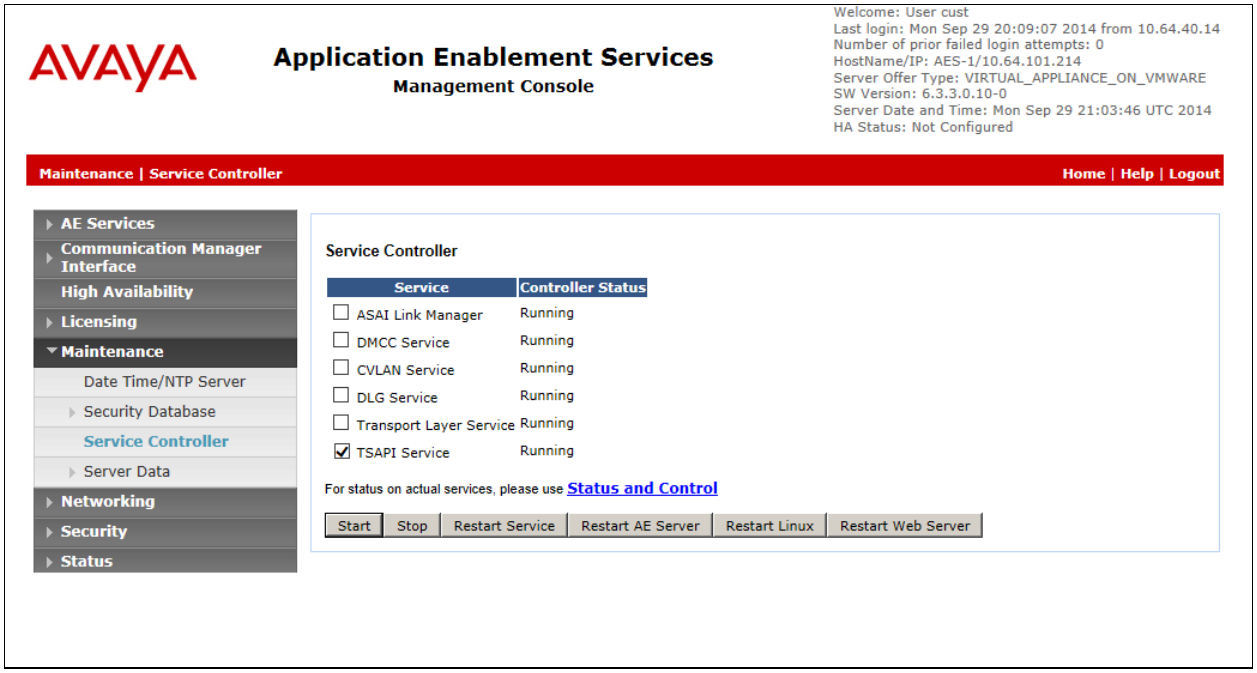
Welcome: User cust
Last login: Mon Sep 29 20:09:07 2014 from 10.64.40.14
Number of prior failed login attempts: 0
HostName/IP: AES-1/10.64.101.214
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.3.0.10-0
Server Date and Time: Mon Sep 29 20:54:44 UTC 2014
HA Status: Not Configured

SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services

☐ Enable SDB for DMCC Service
☑ Enable SDB for TSAPI Service, JTAPI and Telephony Web Services

6.5. Restart TSAPI Service

Select **Maintenance → Service Controller** from the left pane, to display the **Service Controller** screen in the right pane. Check **TSAPI Service**, and click **Restart Service**.



Welcome: User cust
Last login: Mon Sep 29 20:09:07 2014 from 10.64.40.14
Number of prior failed login attempts: 0
HostName/IP: AES-1/10.64.101.214
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.3.0.10-0
Server Date and Time: Mon Sep 29 21:03:46 UTC 2014
HA Status: Not Configured

Service Controller

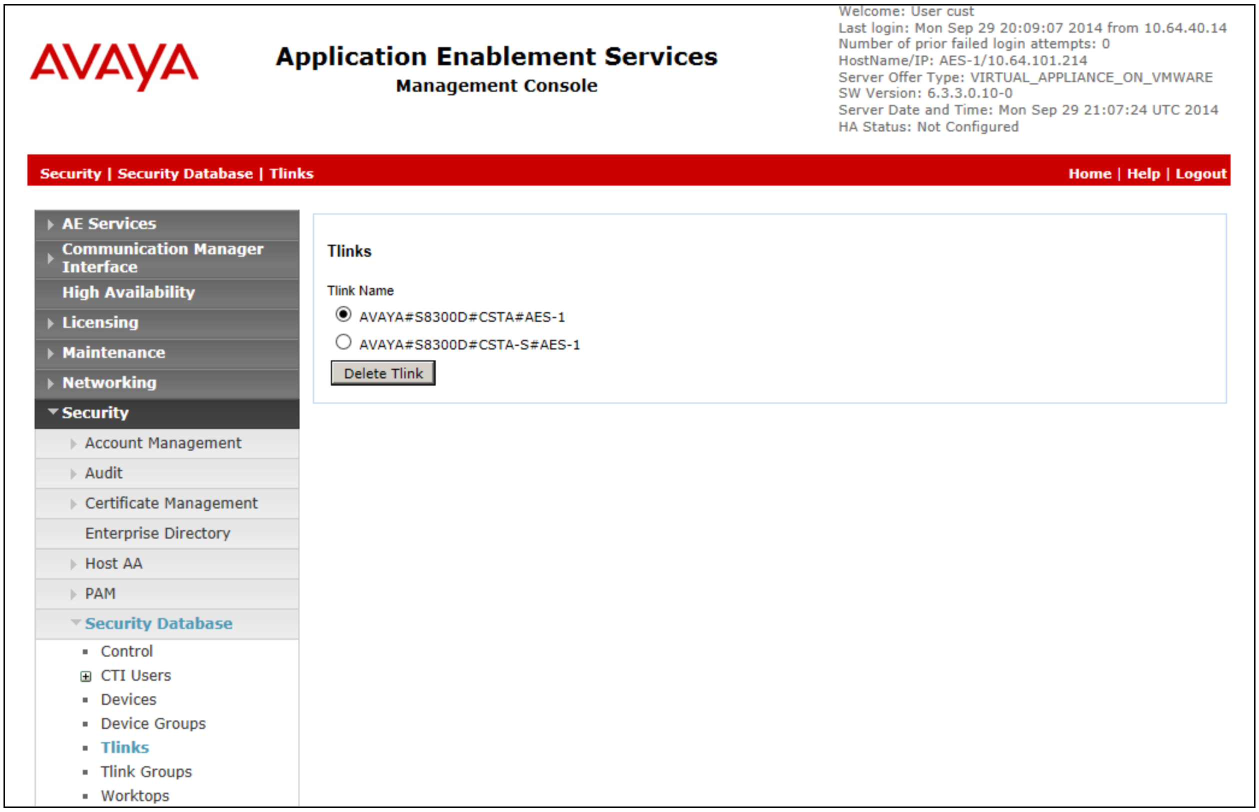
Service	Controller Status
☐ ASAI Link Manager	Running
☐ DMCC Service	Running
☐ CVLAN Service	Running
☐ DLG Service	Running
☐ Transport Layer Service	Running
☑ TSAPI Service	Running

For status on actual services, please use Status and Control

6.6. Obtain Tlink Name

Select **Security** → **Security Database** → **Tlinks** from the left pane. The **Tlinks** screen shows a listing of the Tlink names. A new Tlink name is automatically generated for the TSAPI service. Locate the Tlink name associated with the relevant switch connection, which would use the name of the switch connection as part of the Tlink name. Make a note of the associated Tlink name, to be used later for configuring Recware III.

In this case, the associated Tlink name is "AVAYA#**S8300D**#CSTA#AES-1". Note the use of the switch connection "S8300D" from **Section 6.3** as part of the Tlink name.



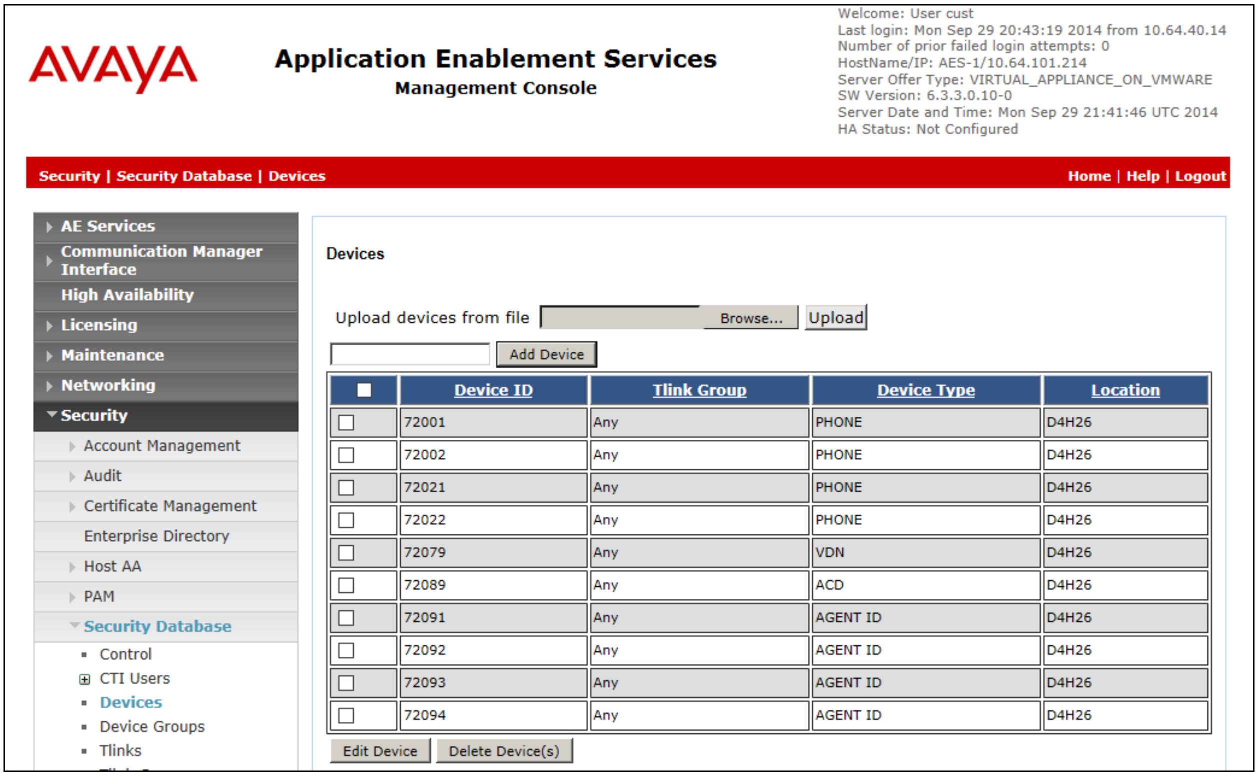
Welcome: User cust
Last login: Mon Sep 29 20:09:07 2014 from 10.64.40.14
Number of prior failed login attempts: 0
HostName/IP: AES-1/10.64.101.214
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.3.0.10-0
Server Date and Time: Mon Sep 29 21:07:24 UTC 2014
HA Status: Not Configured

Tlinks

Tlink Name
● AVAYA#S8300D#CSTA#AES-1
○ AVAYA#S8300D#CSTA-S#AES-1

6.7. Create Devices

Select **Security → Security Database → Devices** from the left pane. Enter a device to add (extension (H.323, SIP), VDN, Skill, agent) then click on **Add Device**. The following screen shows devices that are already added.

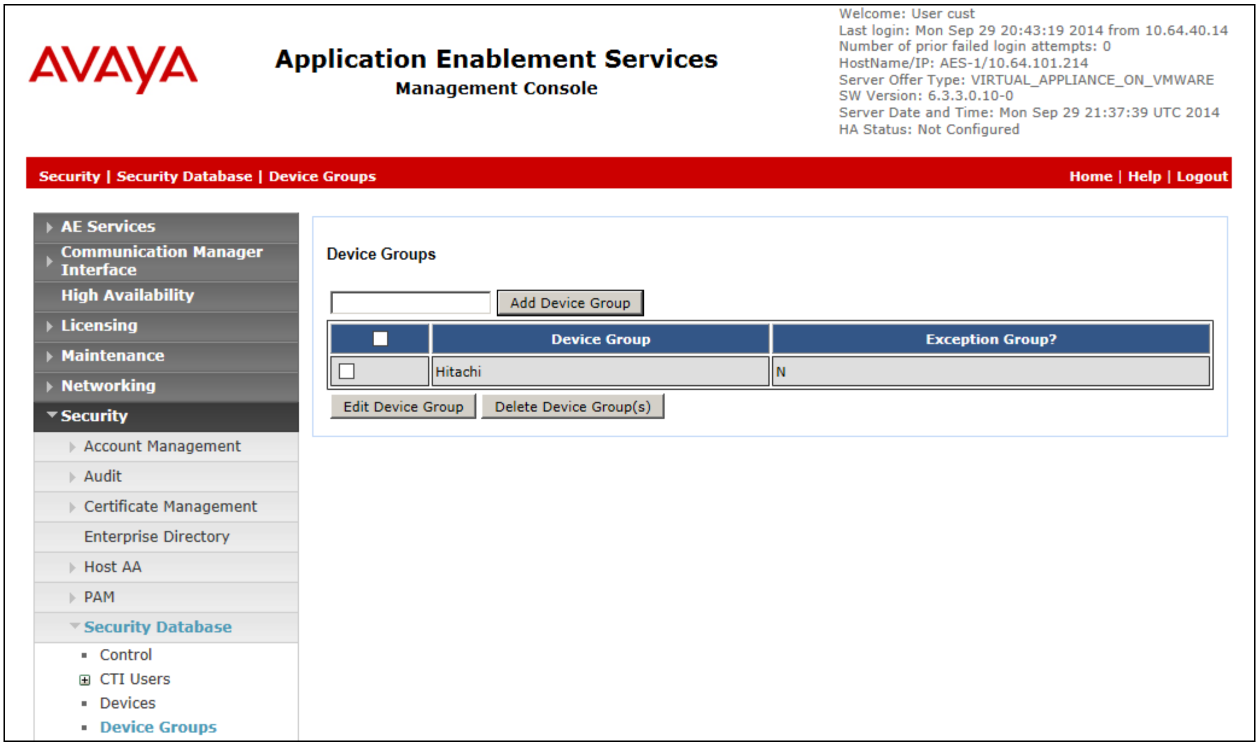


Welcome: User cust
Last login: Mon Sep 29 20:43:19 2014 from 10.64.40.14
Number of prior failed login attempts: 0
HostName/IP: AES-1/10.64.101.214
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.3.0.10-0
Server Date and Time: Mon Sep 29 21:41:46 UTC 2014
HA Status: Not Configured

☐	Device ID	Tlink Group	Device Type	Location
☐	72001	Any	PHONE	D4H26
☐	72002	Any	PHONE	D4H26
☐	72021	Any	PHONE	D4H26
☐	72022	Any	PHONE	D4H26
☐	72079	Any	VDN	D4H26
☐	72089	Any	ACD	D4H26
☐	72091	Any	AGENT ID	D4H26
☐	72092	Any	AGENT ID	D4H26
☐	72093	Any	AGENT ID	D4H26
☐	72094	Any	AGENT ID	D4H26

6.8. Create Device Groups

Select **Security → Security Database → Device Groups** from the left pane. Enter and device group to create and click on **Add Device Group**. During the compliance test, a device group, Hitachi, was created. Check the device group checkbox, and click **Edit Device Group**.



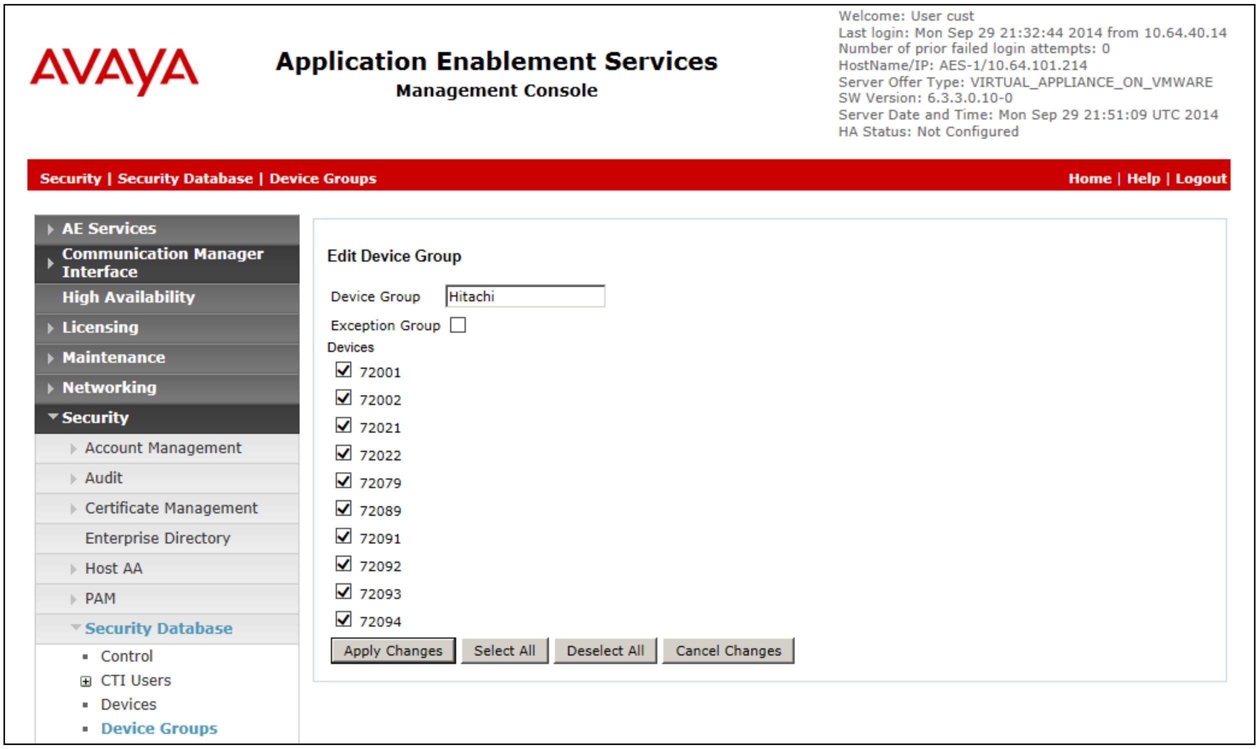
Welcome: User cust
Last login: Mon Sep 29 20:43:19 2014 from 10.64.40.14
Number of prior failed login attempts: 0
HostName/IP: AES-1/10.64.101.214
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.3.0.10-0
Server Date and Time: Mon Sep 29 21:37:39 UTC 2014
HA Status: Not Configured

Device Groups

☐	Device Group	Exception Group?
☐	Hitachi	N

The following screen shows the devices that are included in the device group. Click the **Apply Changes** button.

Note: Unless a device has the checkmark, the device is not a part of the device group.



Welcome: User cust
Last login: Mon Sep 29 21:32:44 2014 from 10.64.40.14
Number of prior failed login attempts: 0
HostName/IP: AES-1/10.64.101.214
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.3.0.10-0
Server Date and Time: Mon Sep 29 21:51:09 UTC 2014
HA Status: Not Configured

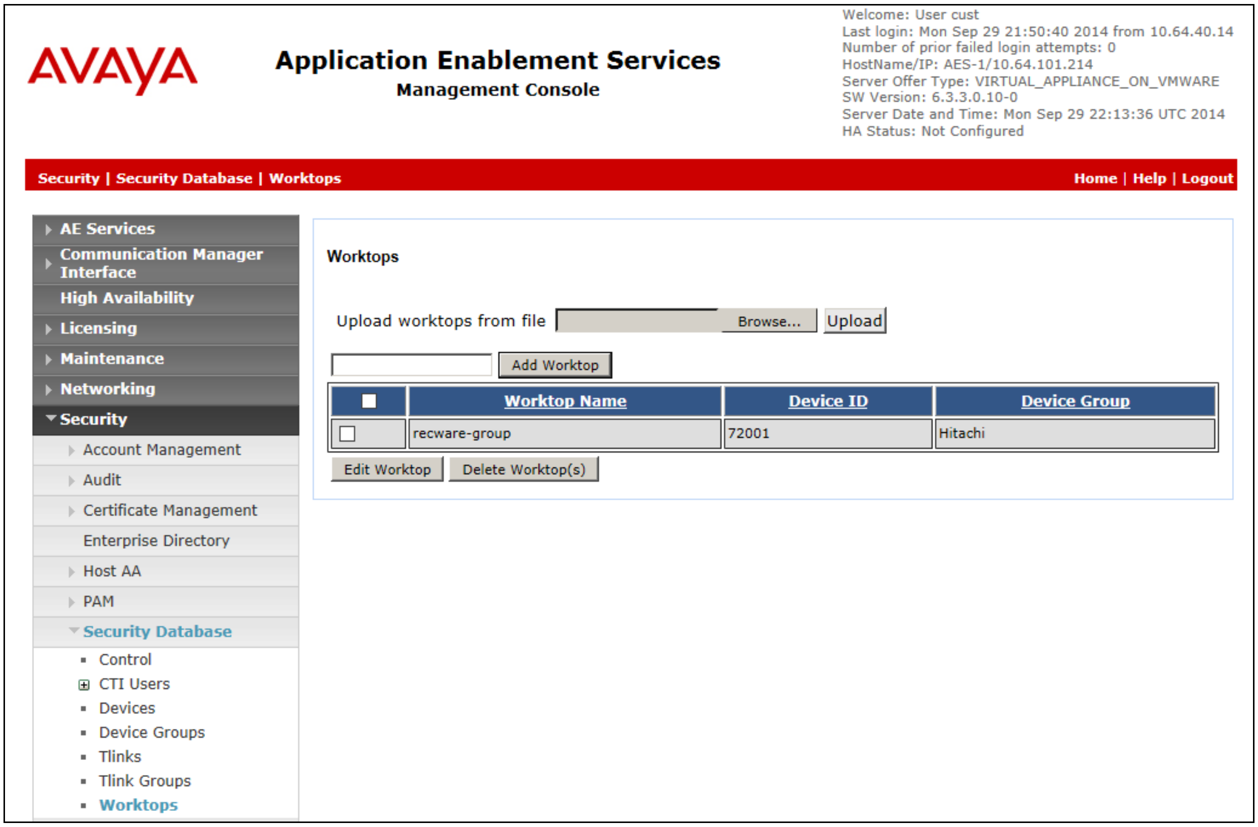
Edit Device Group

Device Group: Hitachi
Exception Group ☐
Devices
☑ 72001
☑ 72002
☑ 72021
☑ 72022
☑ 72079
☑ 72089
☑ 72091
☑ 72092
☑ 72093
☑ 72094

6.9. Create Worktops

Select **Security → Security Database → Worktops** from the left pane, to display the **Worktops** screen in the right pane.

Enter a descriptive worktop name and click **Add Worktop**. In the compliance test, “recware-group” was created. Check the checkbox of the worktop, and click the **Edit Worktop** button.

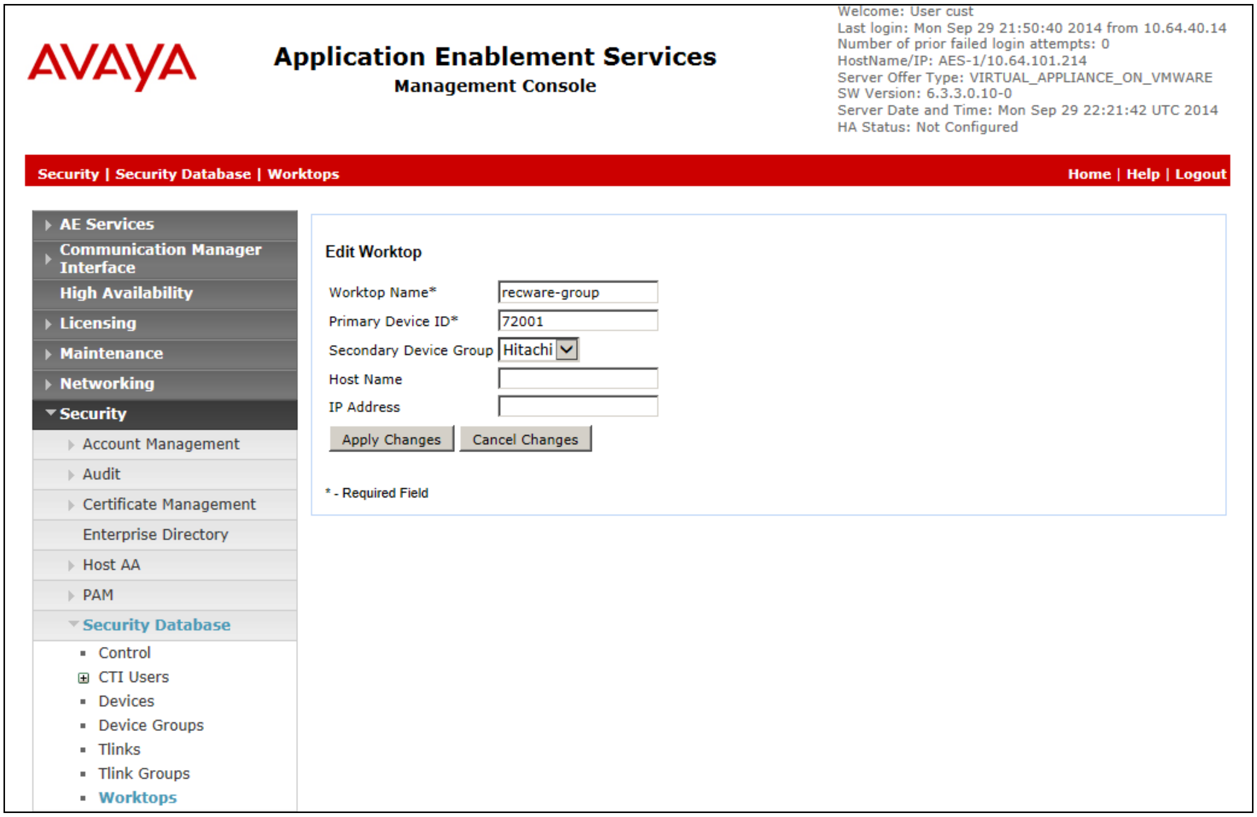


Welcome: User cust
Last login: Mon Sep 29 21:50:40 2014 from 10.64.40.14
Number of prior failed login attempts: 0
HostName/IP: AES-1/10.64.101.214
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.3.0.10-0
Server Date and Time: Mon Sep 29 22:13:36 UTC 2014
HA Status: Not Configured

☐	Worktop Name	Device ID	Device Group
☐	recware-group	72001	Hitachi

The following displays the worktop screen.
Enter a device ID (any monitored station) in the **Primary Device ID** field. Select a secondary device group, using drop-down menu. In the compliance test, **Hitachi** was selected, which was created in **Section 6.8**.

Click the **Apply Changes** button.



Welcome: User cust
Last login: Mon Sep 29 21:50:40 2014 from 10.64.40.14
Number of prior failed login attempts: 0
HostName/IP: AES-1/10.64.101.214
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.3.0.10-0
Server Date and Time: Mon Sep 29 22:21:42 UTC 2014
HA Status: Not Configured

Edit Worktop

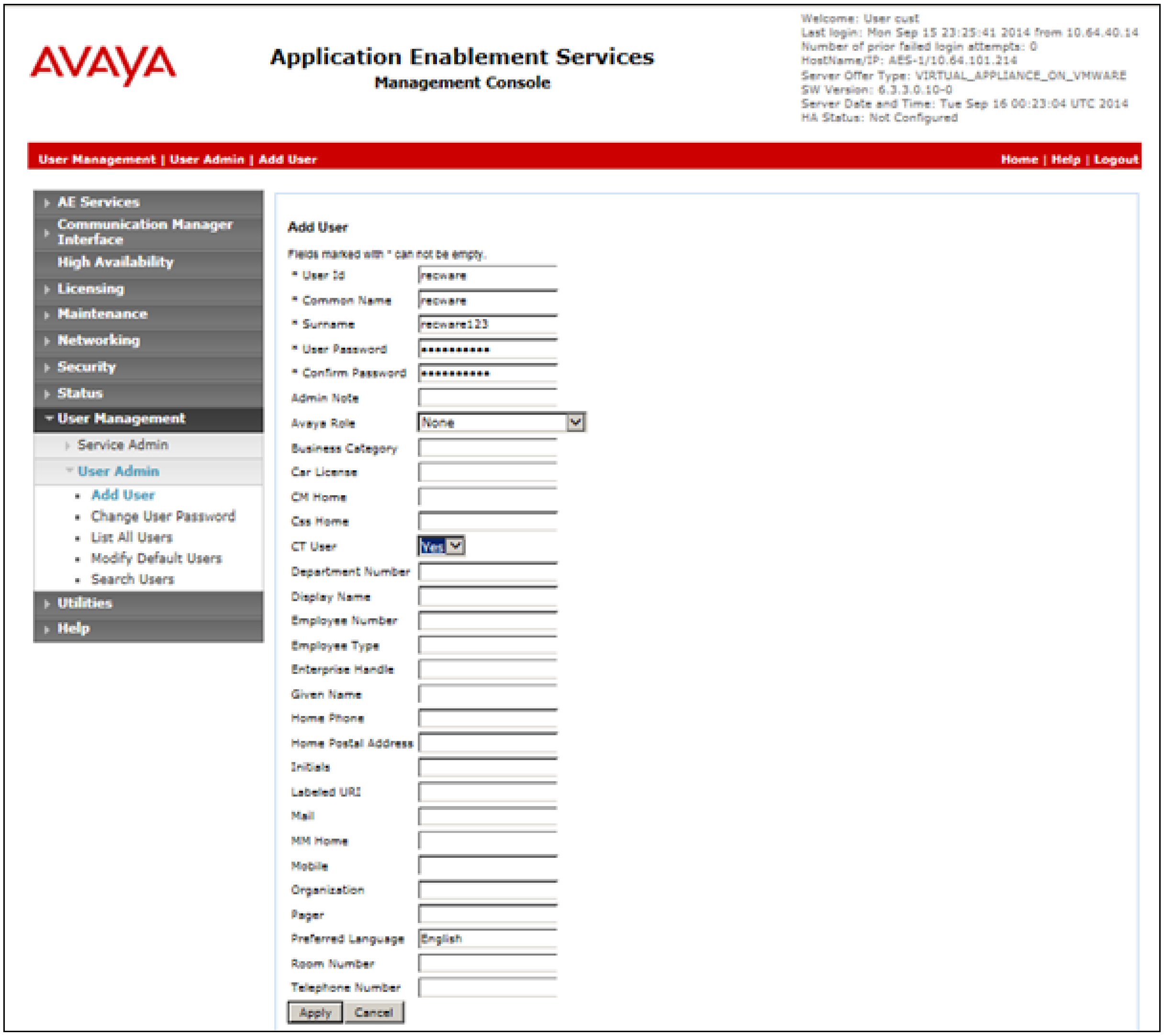
Worktop Name* recware-group
Primary Device ID* 72001
Secondary Device Group Hitachi
Host Name
IP Address

6.10. Administer Recware III User

To create a Recware user, select **User Management** → **User Admin** → **Add User** from the left pane, to display the **Add User** screen in the right pane.

Enter desired values for **User Id**, **Common Name**, **Surname**, **User Password**, and **Confirm Password**. For **CT User**, select "Yes" from the drop-down list. Retain the default value in the remaining fields.

Click **Apply**.



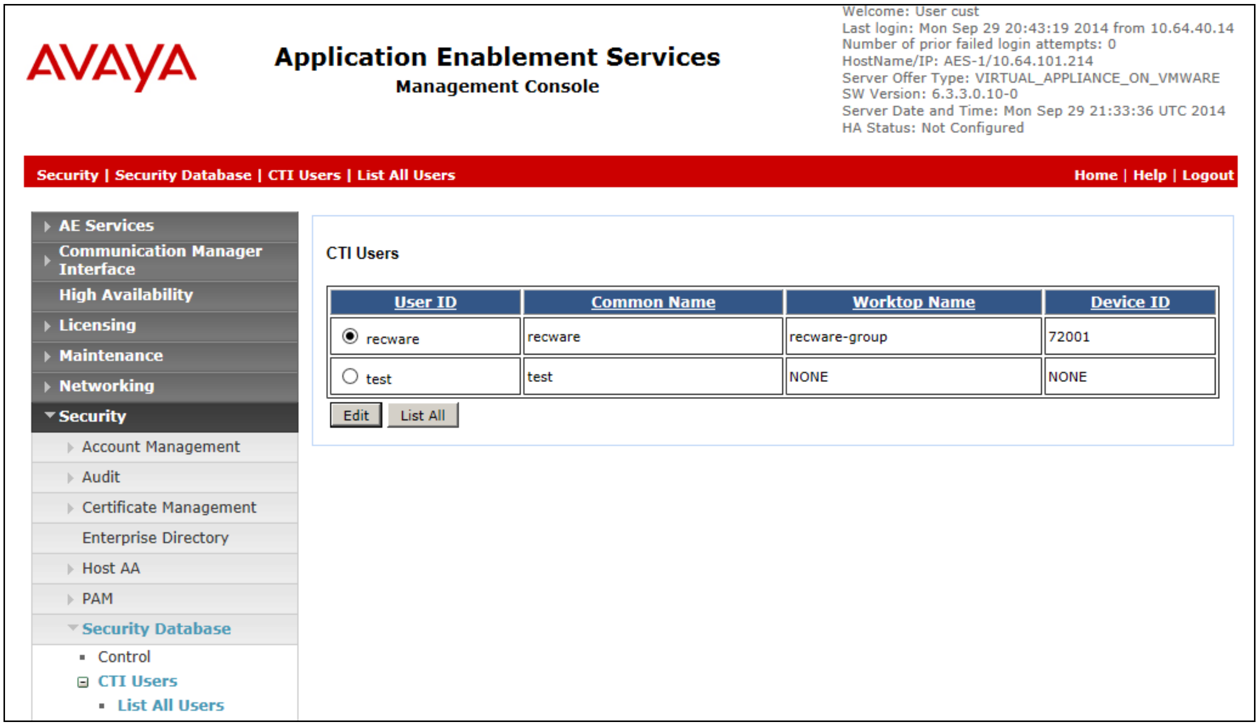
Welcome: User cust
Last login: Mon Sep 15 23:25:41 2014 from 10.64.40.14
Number of prior failed login attempts: 0
HostName/IP: AES-1/10.64.101.214
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.3.0.10-0
Server Date and Time: Tue Sep 16 00:23:04 UTC 2014
HA Status: Not Configured

Add User

Fields marked with * can not be empty.

* User Id	recware
* Common Name	recware
* Surname	recware123
* User Password	•••••••••••
* Confirm Password	•••••••••••
Admin Note	
Avaya Role	None
Business Category	
Car License	
CM Home	
Css Home	
CT User	Yes
Department Number	
Display Name	
Employee Number	
Employee Type	
Enterprise Handle	
Given Name	
Home Phone	
Home Postal Address	
Initials	
Labeled URI	
Mail	
MM Home	
Mobile	
Organization	
Pager	
Preferred Language	English
Room Number	
Telephone Number	

Navigate to **Security → Security Database → CTI Users → List All Users.** Select the user created above and click the **Edit** button.



AVAYA
Application Enablement Services
Management Console
Welcome: User cust
Last login: Mon Sep 29 20:43:19 2014 from 10.64.40.14
Number of prior failed login attempts: 0
HostName/IP: AES-1/10.64.101.214
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.3.0.10-0
Server Date and Time: Mon Sep 29 21:33:36 UTC 2014
HA Status: Not Configured
Security | Security Database | CTI Users | List All Users
Home | Help | Logout
AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
Security
Account Management
Audit
Certificate Management
Enterprise Directory
Host AA
PAM
Security Database
Control
CTI Users
List All Users
Edit
List All

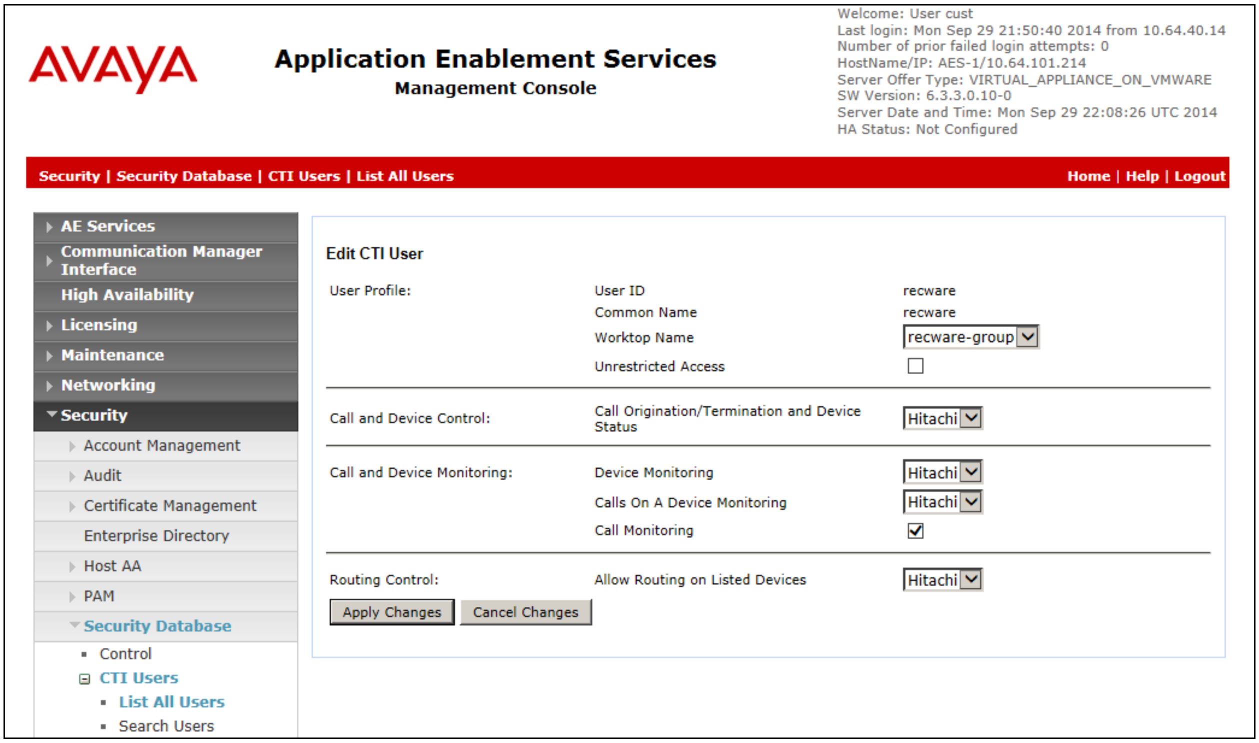
CTI Users

User ID	Common Name	Worktop Name	Device ID
● recware	recware	recware-group	72001
○ test	test	NONE	NONE

On the Edit CTI User screen, provide the following information:

- Select a worktop name, using a drop-down menu. During the compliance test**, "**recware-group" was used. To query "cstaGetDeviceList" from a Hitachi TSAPI client, the worktop name has to be selected. Without it, no device list will be returned.
- Select a device group for the **Device Monitoring** field. During the compliance test, "Hitachi" was used.
- Select a device group for the **Calls On A Device Monitoring** field. During the compliance test, "Hitachi" was used.

Click **Apply Changes**.



Welcome: User cust
Last login: Mon Sep 29 21:50:40 2014 from 10.64.40.14
Number of prior failed login attempts: 0
HostName/IP: AES-1/10.64.101.214
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.3.0.10-0
Server Date and Time: Mon Sep 29 22:08:26 UTC 2014
HA Status: Not Configured

Edit CTI User

User Profile:	User ID	recware
	Common Name	recware
	Worktop Name	recware-group
	Unrestricted Access	☐
Call and Device Control:	Call Origination/Termination and Device Status	Hitachi
Call and Device Monitoring:	Device Monitoring	Hitachi
	Calls On A Device Monitoring	Hitachi
	Call Monitoring	☑
Routing Control:	Allow Routing on Listed Devices	Hitachi

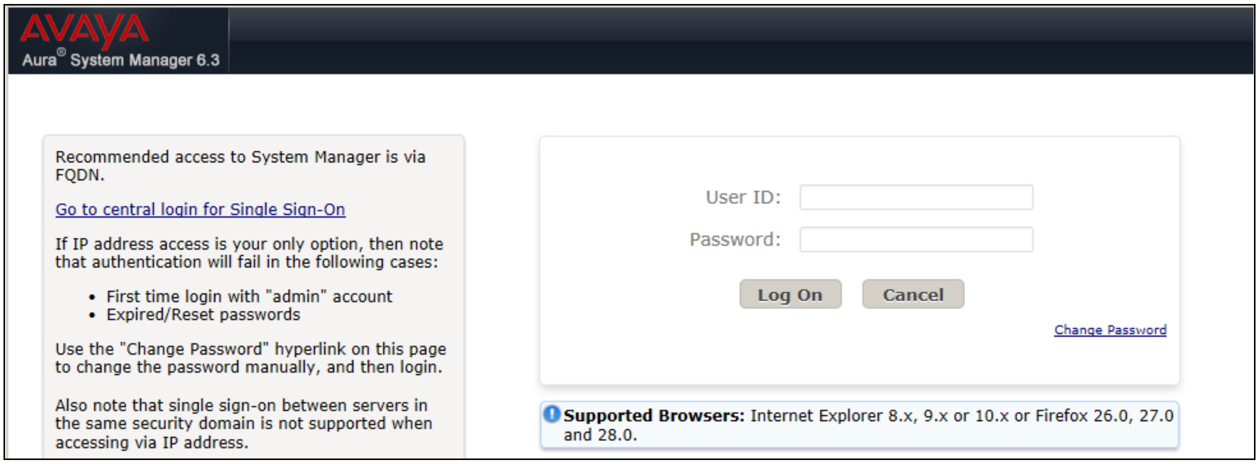
7. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. The procedures include the following areas:

- Launch System Manager
- Administer users

7.1. Launch Avaya Aura® System Manager

Access the System Manager web interface by using the URL "https://ip-address/SMGR" in an Internet browser window, where "ip-address" is the IP address of System Manager. Log in using the 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.

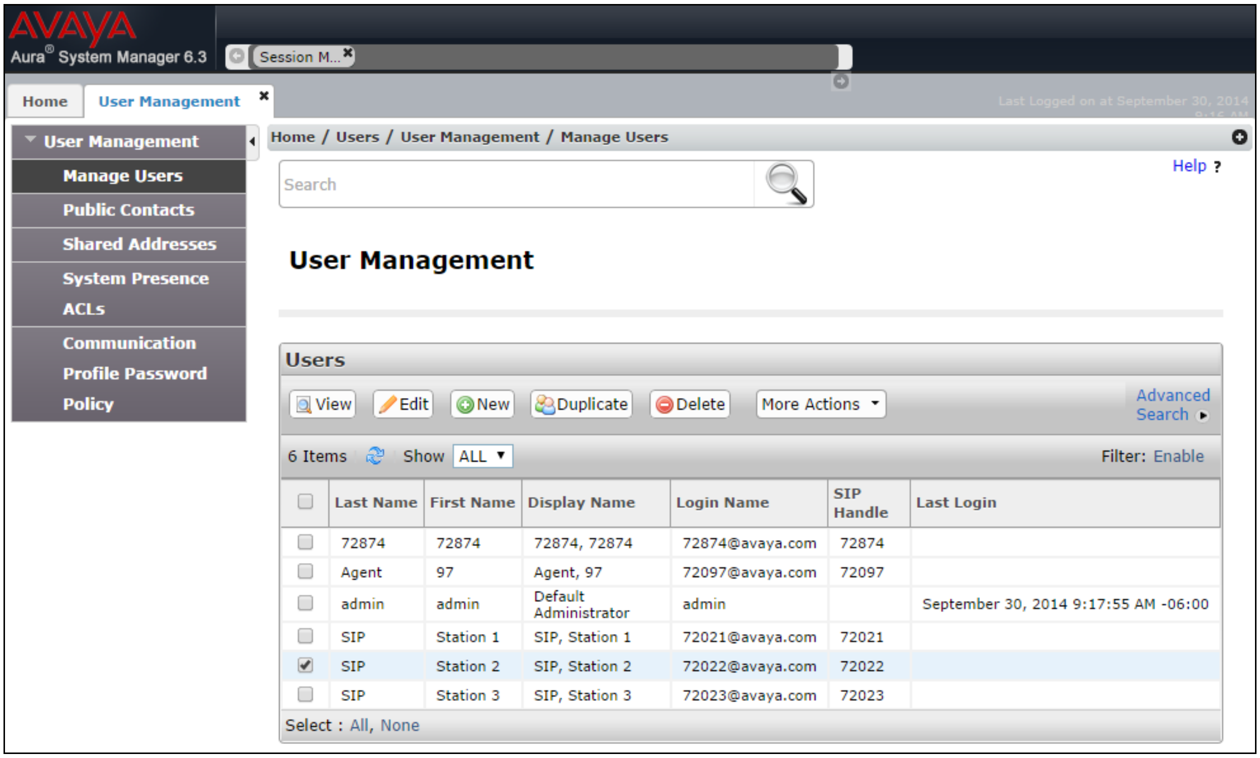
Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

Supported Browsers: Internet Explorer 8.x, 9.x or 10.x or Firefox 26.0, 27.0 and 28.0.

7.2. Administer Users

In the subsequent screen (not shown), select **Users → User Management → Manage Users** to display the **User Management** screen below. Select an entry associated with a SIP agent station from **Section 3**, in this case “72022”, and click **Edit**.

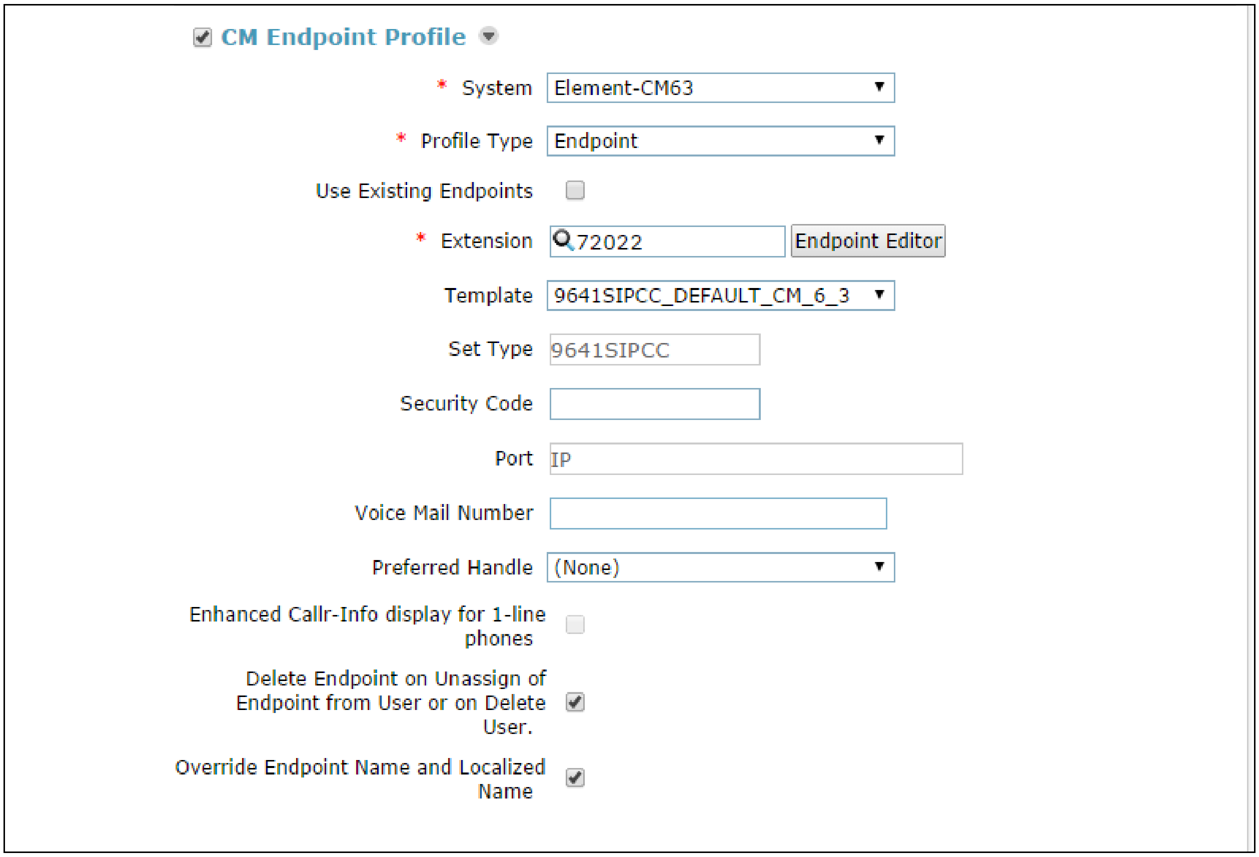
Note: Users were already created prior to the actual test, the creation of users will not be covered in this application note.



☐	Last Name	First Name	Display Name	Login Name	SIP Handle	Last Login
☐	72874	72874	72874, 72874	72874@avaya.com	72874	
☐	Agent	97	Agent, 97	72097@avaya.com	72097	
☐	admin	admin	Default Administrator	admin		September 30, 2014 9:17:55 AM -06:00
☐	SIP	Station 1	SIP, Station 1	72021@avaya.com	72021	
☑	SIP	Station 2	SIP, Station 2	72022@avaya.com	72022	
☐	SIP	Station 3	SIP, Station 3	72023@avaya.com	72023	

The **User Profile Edit** screen (not shown) is displayed. Select the **Communication Profile** tab (not shown). Navigate to the **CM Endpoint Profile** sub-section, and click **Endpoint Editor**.

Note: The template was selected as "9641SIPCC_DEFAULT_CM_6_3", and the set type was selected as "9641SIPCC".

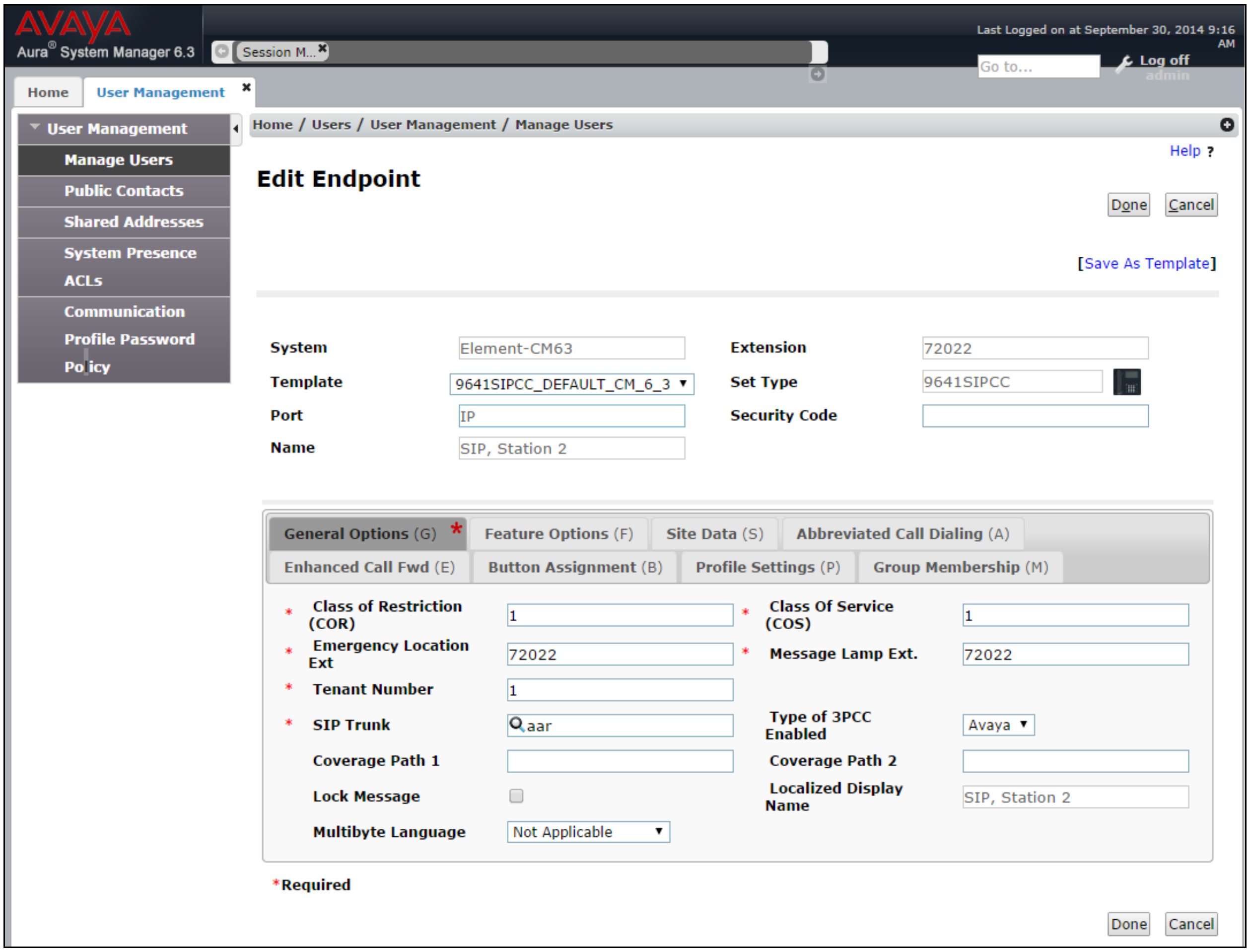


☑ CM Endpoint Profile

* System	Element-CM63
* Profile Type	Endpoint
Use Existing Endpoints	☐
* Extension	72022
Template	9641SIPCC_DEFAULT_CM_6_3
Set Type	9641SIPCC
Security Code	
Port	IP
Voice Mail Number	
Preferred Handle	(None)
Enhanced Callr-Info display for 1-line phones	☐
Delete Endpoint on Unassign of Endpoint from User or on Delete User.	☑
Override Endpoint Name and Localized Name	☑

The **Edit Endpoint** screen is displayed next. For **Type of 3PCC Enabled**, select “Avaya” from the drop-down list as shown below. Retain the default values in the remaining fields.

Repeat this section for all SIP agent users.

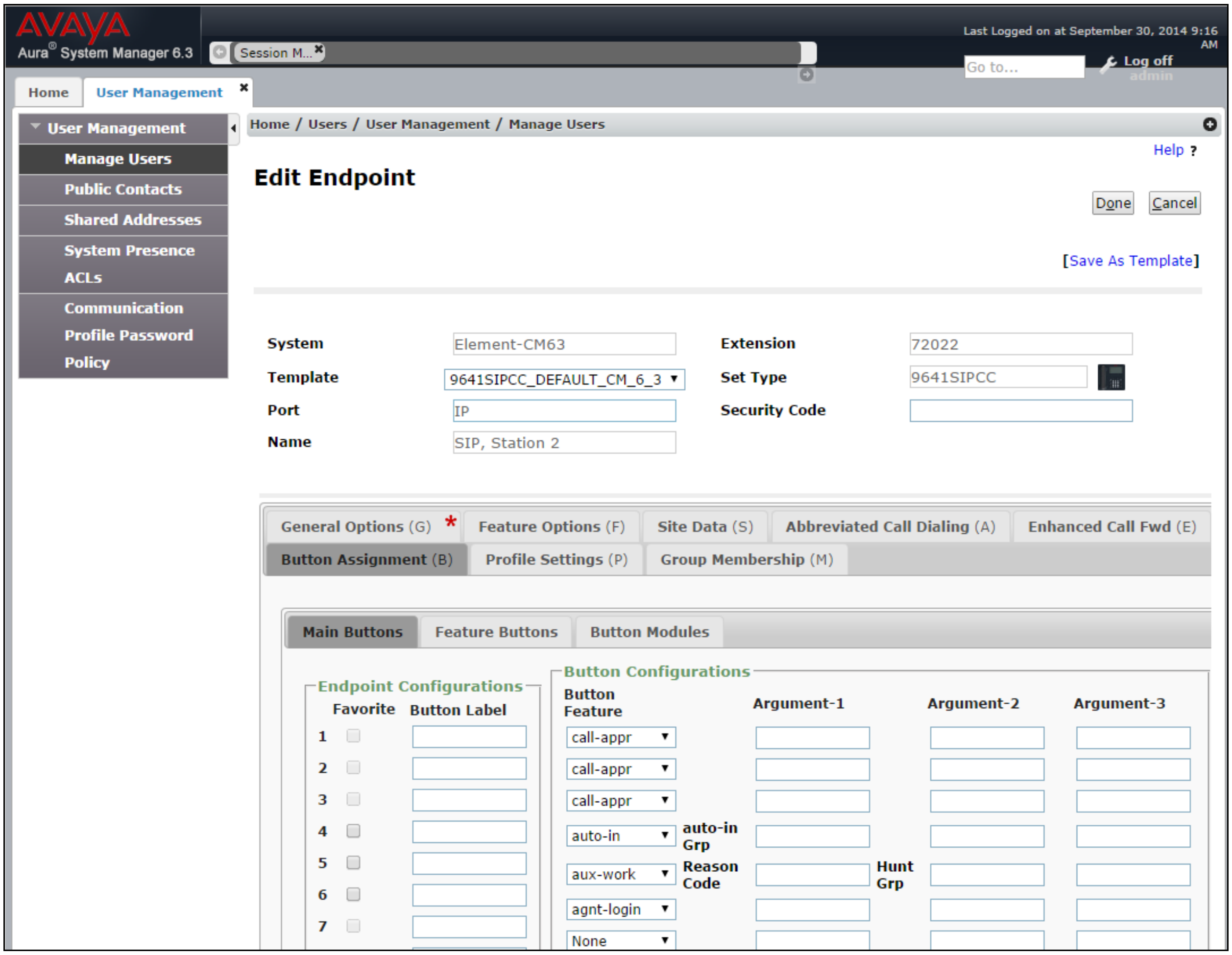


Edit Endpoint

System: Element-CM63
Template: 9641SIPCC_DEFAULT_CM_6_3
Port: IP
Name: SIP, Station 2
Extension: 72022
Set Type: 9641SIPCC
Security Code:

* Class of Restriction (COR): 1
* Class Of Service (COS): 1
* Emergency Location Ext: 72022
* Message Lamp Ext.: 72022
* Tenant Number: 1
* SIP Trunk: aar
Type of 3PCC Enabled: Avaya
Coverage Path 1:
Coverage Path 2:
Lock Message: ☐
Localized Display Name: SIP, Station 2
Multibyte Language: Not Applicable

Select the Button Assignment tab, and provide buttons for auto-in, aux-work and agnt-login. The a**gnt –login** button will toggle between login and logout on the SIP phone display. Click the **Done** button when complete.



Edit Endpoint

System	Element-CM63	Extension	72022
Template	9641SIPCC_DEFAULT_CM_6_3	Set Type	9641SIPCC
Port	IP	Security Code	
Name	SIP, Station 2		

Endpoint Configurations

Button Configurations

	Favorite	Button Label	Button Feature		Argument-1		Argument-2	Argument-3
1	☐		call-appr					
2	☐		call-appr					
3	☐		call-appr					
4	☐		auto-in	auto-in Grp				
5	☐		aux-work	Reason Code		Hunt Grp		
6	☐		agnt-login					
7	☐		None					

8. Configure Hitachi Recware III

This section provides the procedures for configuring Recware III. For the compliance test, images for MNG, AS-GW, SLGR, and Client PC were brought in and installed by Hitachi engineers. Due to the language used, the device installation is in Japanese, the installation steps are included separately in Appendix A for reference.

9. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Application Enablement Services, and Recware III.

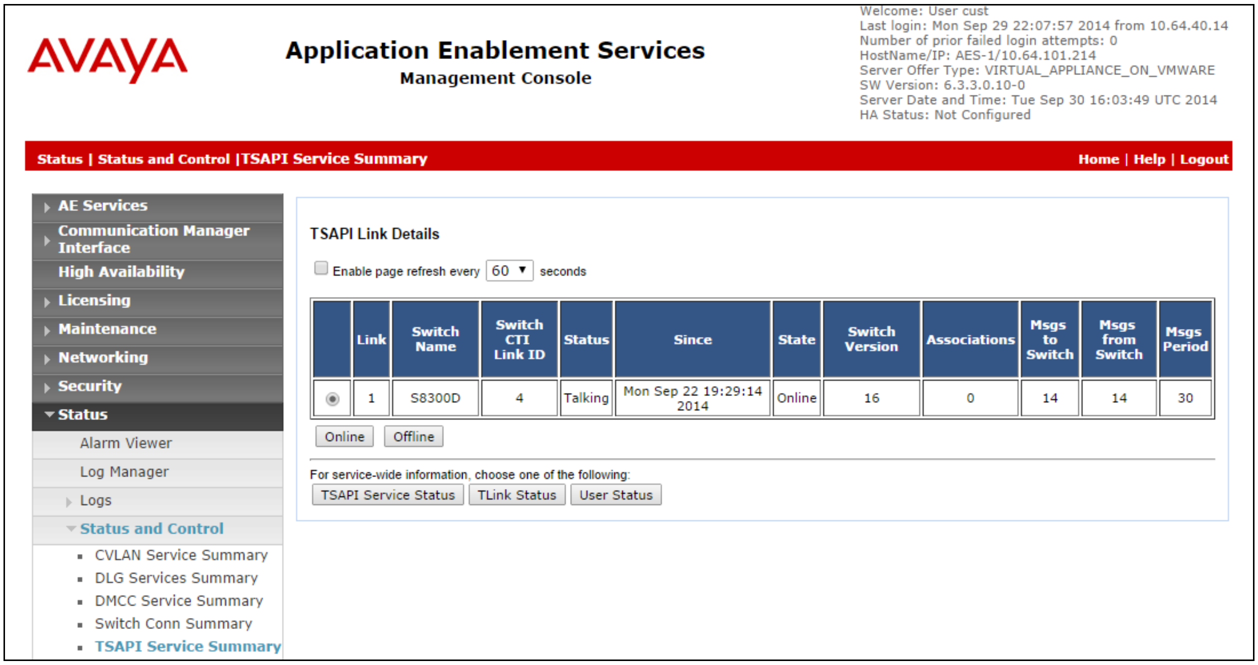
9.1. Verify Avaya Aura® Communication Manager

On Communication Manager, verify the status of the administered CTI link by using the "status aesvcs cti-link" command. Verify that the **Service State** is "established" for the CTI link number administered in **Section 5.2**, as shown below.

```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

CTI   Version  Mnt   AE Services       Service        Msgs      Msgs
Link           Busy  Server            State          Sent      Rcvd

1              no                      down           0         0
4     5        no    AES-1             established    15        15
```

9.2. Verify Avaya Aura® Application Enablement Services

On the Application Enablement Services, verify the status of the TSAPI link by selecting **Status → Status and Control → TSAPI Service Summary** from the left pane (not shown). The **TSAPI Link Details** screen is displayed. Verify the **Status** is "Talking" for the TSAPI link administered in **Section 6.3**, and that the **Associations** column reflects the total number of monitored skill groups and agent stations from **Section 3**.



Welcome: User cust
Last login: Mon Sep 29 22:07:57 2014 from 10.64.40.14
Number of prior failed login attempts: 0
HostName/IP: AES-1/10.64.101.214
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.3.0.10-0
Server Date and Time: Tue Sep 30 16:03:49 UTC 2014
HA Status: Not Configured

TSAPI Link Details

☐ Enable page refresh every 60 seconds

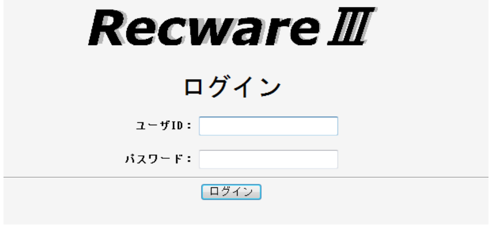
	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
●	1	S8300D	4	Talking	Mon Sep 22 19:29:14 2014	Online	16	0	14	14	30

For service-wide information, choose one of the following:

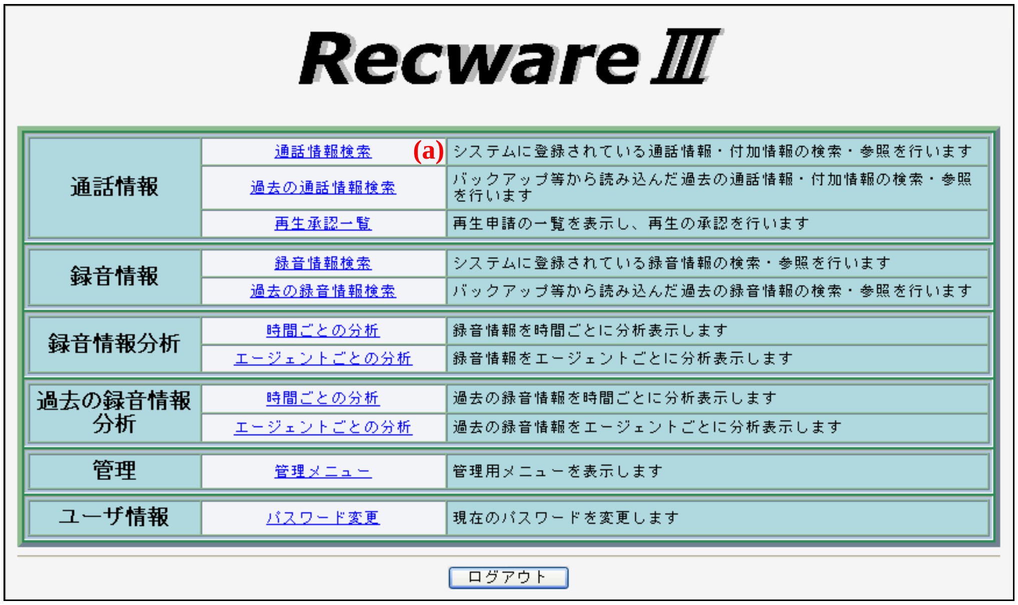
9.3. Verify Hitachi Recware III

The following are typical steps to verify the integration between Hitachi Recware III recording application and the Application Enablement Services.

Access MNG web page of URL, http://<ip-address>/RecIP in an Internet browser window, where <ip-address> is the IP address of MNG. Then, log in using the appropriate credentials.



The subsequent web page of Recware III MNG Main Menu web page appears as shown below.



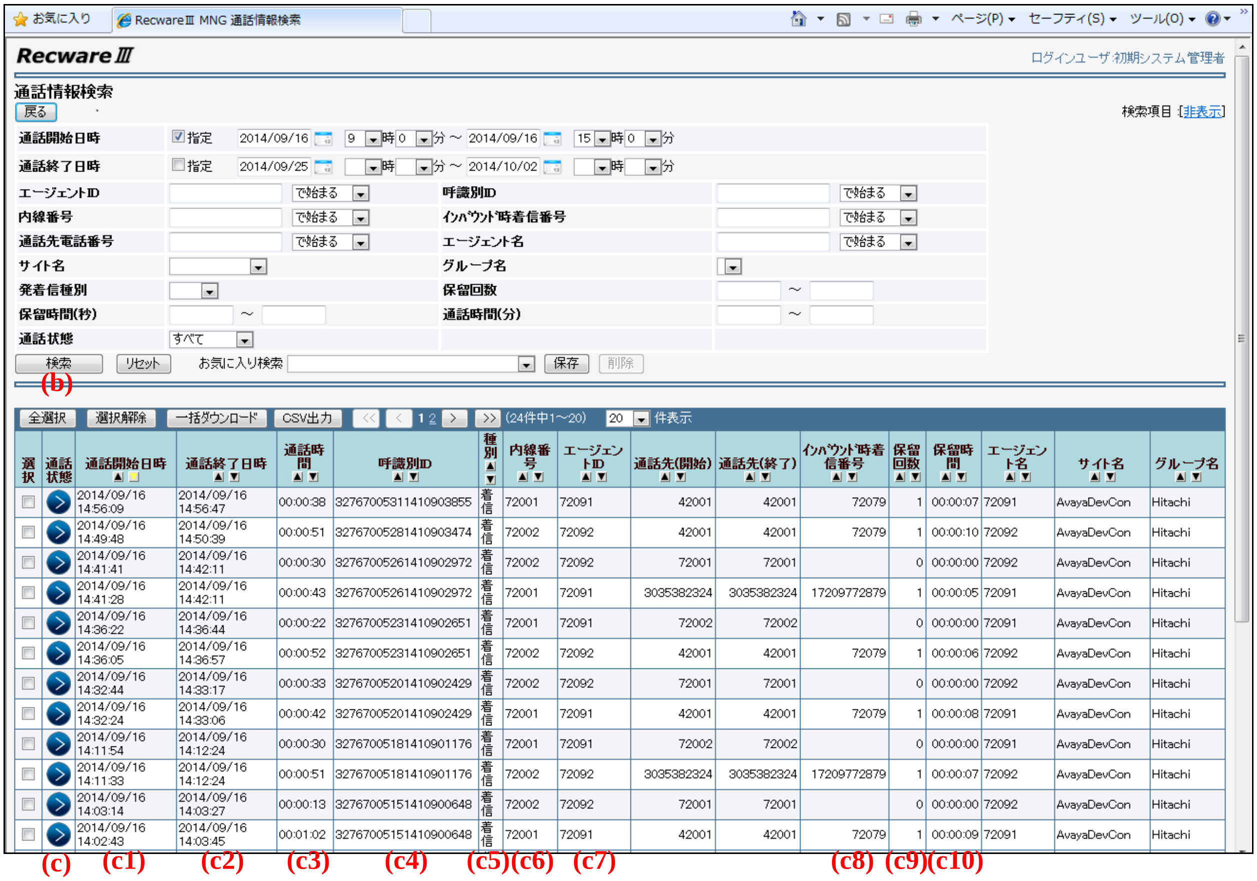
通話情報	通話情報検索	システムに登録されている通話情報・付加情報の検索・参照を行います
	過去の通話情報検索	バックアップ等から読み込んだ過去の通話情報・付加情報の検索・参照を行います
	再生承認一覧	再生申請の一覧を表示し、再生の承認を行います
録音情報	録音情報検索	システムに登録されている録音情報の検索・参照を行います
	過去の録音情報検索	バックアップ等から読み込んだ過去の録音情報の検索・参照を行います
録音情報分析	時間ごとの分析	録音情報を時間ごとに分析表示します
	エージェントごとの分析	録音情報をエージェントごとに分析表示します
過去の録音情報分析	時間ごとの分析	過去の録音情報を時間ごとに分析表示します
	エージェントごとの分析	過去の録音情報をエージェントごとに分析表示します
管理	管理メニュー	管理用メニューを表示します
ユーザ情報	パスワード変更	現在のパスワードを変更します

By clicking (**a**) in the MNG Main Menu web page above, Current Interaction Logs web page appears as shown below. By clicking “Search (**b**)” button, a list of the call recordings will appear.

Verify that the first entry reflects the last call, with proper values in the Start Time, End Time, Duration Time, Call ID, Type (incoming or outgoing), Extension number, Agent ID, Dial to (DNIS), Call Held Count and Call Held Duration Time.

Verify the detail information of the interaction record. Click icon(c) to view the detail voice recording of the interaction record.

- Start Time (c1)
- End Time (c2)
- Duration Time (c3)
- Call ID (c4)
- Type (incoming call or outgoing call) (c5)
- Extension number (c6)
- Agent ID (c7)
- Dial to (DNIS) (c8)
- Call Held Count (c9)
- Call Held Duration Time (c10)



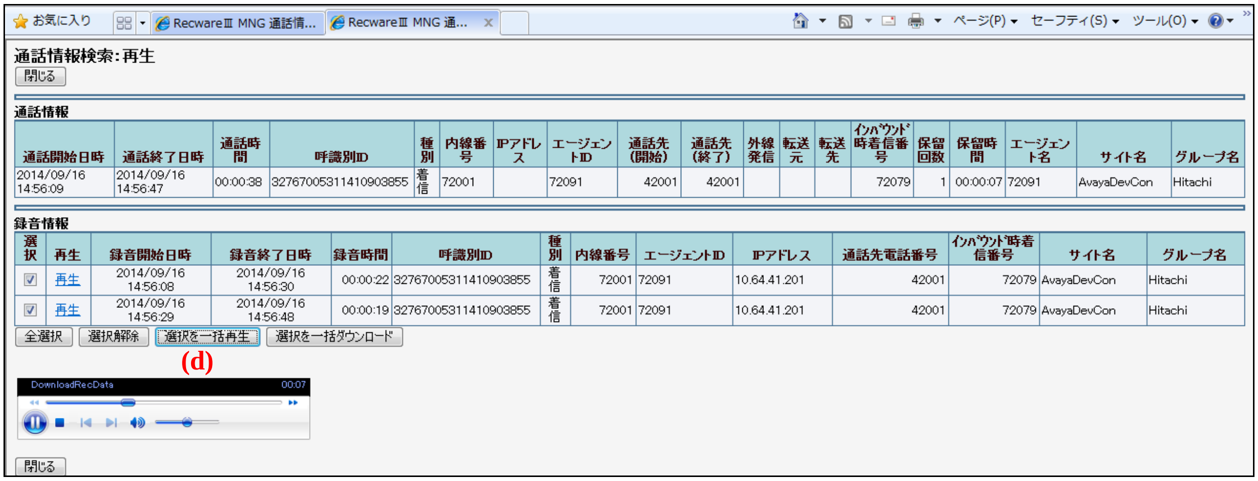
通話情報検索

通話開始日時 ☑指定 2014/09/16 9 時 0 分 ～ 2014/09/16 15 時 0 分
通話終了日時 ☐指定 2014/09/25 時 分 ～ 2014/10/02 時 分
エージェントID で始まる
呼識別ID で始まる
内線番号 で始まる
インバウンド時着信番号 で始まる
通話先電話番号 で始まる
エージェント名 で始まる
サイト名
グループ名
発着信種別
保留回数 ～
保留時間(秒) ～
通話時間(分) ～
通話状態 すべて
お気に入り検索

(24件中1～20) 20 件表示

選択	通話状態	通話開始日時	通話終了日時	通話時間	呼識別ID	種別	内線番号	エージェントID	通話先(開始)	通話先(終了)	インバウンド時着信番号	保留回数	保留時間	エージェント名	サイト名	グループ名
☐	>	2014/09/16 14:56:09	2014/09/16 14:56:47	00:00:38	32767005311410903855	着信	72001	72091	42001	42001	72079	1	00:00:07	72091	AvayaDevCon	Hitachi
☐	>	2014/09/16 14:49:48	2014/09/16 14:50:39	00:00:51	32767005281410903474	着信	72002	72092	42001	42001	72079	1	00:00:10	72092	AvayaDevCon	Hitachi
☐	>	2014/09/16 14:41:41	2014/09/16 14:42:11	00:00:30	32767005261410902972	着信	72002	72092	72001	72001		0	00:00:00	72092	AvayaDevCon	Hitachi
☐	>	2014/09/16 14:41:28	2014/09/16 14:42:11	00:00:43	32767005261410902972	着信	72001	72091	3035382324	3035382324	17209772879	1	00:00:05	72091	AvayaDevCon	Hitachi
☐	>	2014/09/16 14:36:22	2014/09/16 14:36:44	00:00:22	32767005231410902651	着信	72001	72091	72002	72002		0	00:00:00	72091	AvayaDevCon	Hitachi
☐	>	2014/09/16 14:36:05	2014/09/16 14:36:57	00:00:52	32767005231410902651	着信	72002	72092	42001	42001	72079	1	00:00:06	72092	AvayaDevCon	Hitachi
☐	>	2014/09/16 14:32:44	2014/09/16 14:33:17	00:00:33	32767005201410902429	着信	72002	72092	72001	72001		0	00:00:00	72092	AvayaDevCon	Hitachi
☐	>	2014/09/16 14:32:24	2014/09/16 14:33:06	00:00:42	32767005201410902429	着信	72001	72091	42001	42001	72079	1	00:00:08	72091	AvayaDevCon	Hitachi
☐	>	2014/09/16 14:11:54	2014/09/16 14:12:24	00:00:30	32767005181410901176	着信	72001	72091	72002	72002		0	00:00:00	72091	AvayaDevCon	Hitachi
☐	>	2014/09/16 14:11:33	2014/09/16 14:12:24	00:00:51	32767005181410901176	着信	72002	72092	3035382324	3035382324	17209772879	1	00:00:07	72092	AvayaDevCon	Hitachi
☐	>	2014/09/16 14:03:14	2014/09/16 14:03:27	00:00:13	32767005151410900648	着信	72002	72092	72001	72001		0	00:00:00	72092	AvayaDevCon	Hitachi
☐	>	2014/09/16 14:02:43	2014/09/16 14:03:45	00:01:02	32767005151410900648	着信	72001	72091	42001	42001	72079	1	00:00:09	72091	AvayaDevCon	Hitachi

Click icon (d) to verify the proper playback of the call recording.



(d)

通話情報検索:再生

通話情報

通話開始日時	通話終了日時	通話時間	呼識別ID	種別	内線番号	IPアドレス	エージェントID	通話先(開始)	通話先(終了)	外線発信	転送元	転送先	ｲﾝﾊﾞｳﾝﾄﾞ時着信番号	保留回数	保留時間	エージェント名	サイト名	グループ名
2014/09/16 14:56:09	2014/09/16 14:56:47	00:00:38	32767005311410903855	着信	72001		72091	42001	42001				72079	1	00:00:07	72091	AvayaDevCon	Hitachi

録音情報

選択	再生	録音開始日時	録音終了日時	録音時間	呼識別ID	種別	内線番号	エージェントID	IPアドレス	通話先電話番号	ｲﾝﾊﾞｳﾝﾄﾞ時着信番号	サイト名	グループ名
☑	再生	2014/09/16 14:56:08	2014/09/16 14:56:30	00:00:22	32767005311410903855	着信	72001	72091	10.64.41.201	42001	72079	AvayaDevCon	Hitachi
☑	再生	2014/09/16 14:56:29	2014/09/16 14:56:48	00:00:19	32767005311410903855	着信	72001	72091	10.64.41.201	42001	72079	AvayaDevCon	Hitachi

10. Conclusion

These Application Notes describe the configuration steps required for Hitachi Recware III to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services R6.3 using VoIP recording. All feature and serviceability test cases were successfully completed with an observation noted in **Section 2.2**.

11. Additional References

This section references the product documentation relevant to these Application Notes.

1. *Administering Avaya Aura® Communication Manager*, Document 03-300509, Issue 10, Release 6.3, June 2014, available at http://support.avaya.com.
2. *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 6.3, 02-300357, June 2014, available at http://support.avaya.com.
3. *RecwareIII_MNG_03-40_Operation_Manual*, January 2014, available upon request to Hitachi Information & Telecommunication Engineering, Ltd at http:/www.hitachi-ite.co.jp/products/recware3/index.html.

Appendix A

Configuring Hitachi Recware III
This section provides the procedures for configuring Recware III. The procedures include the following components:

- Recware III MNG
- Recware III AS-GW
- Recware III SLGR (including IP/DNM Type A)
- Client PC

A.1. Recware III MNG Settings

(1) Launch MNG Management pages
Access MNG web interface by using the URL "http://<ip-address>/RecIP" in an Internet browser window, where "ip-address" is the IP address of MNG. Then, log in using the appropriate credentials.

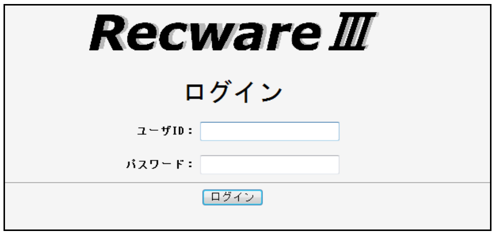
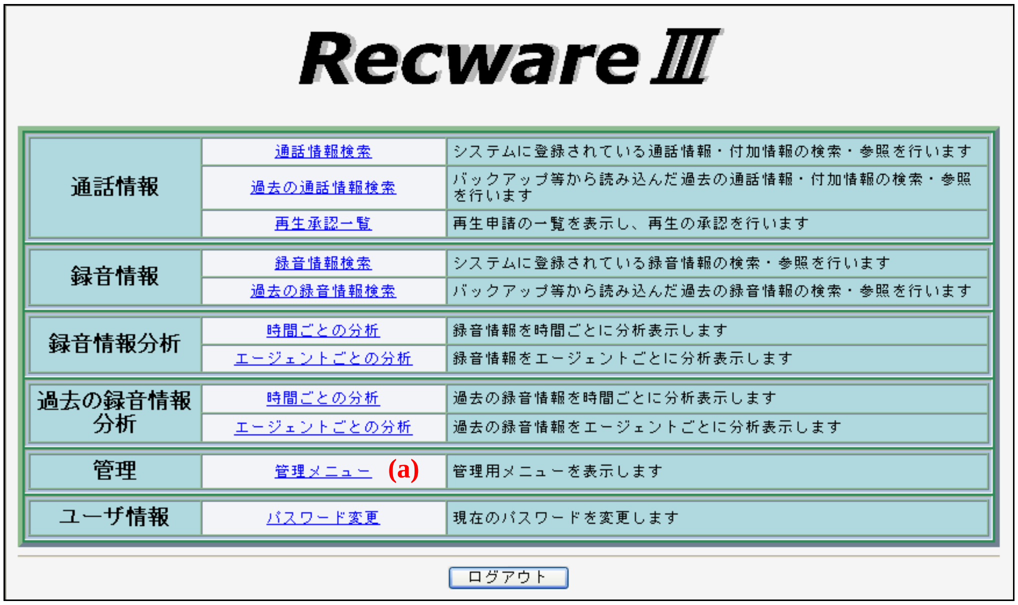


Figure A-1-1

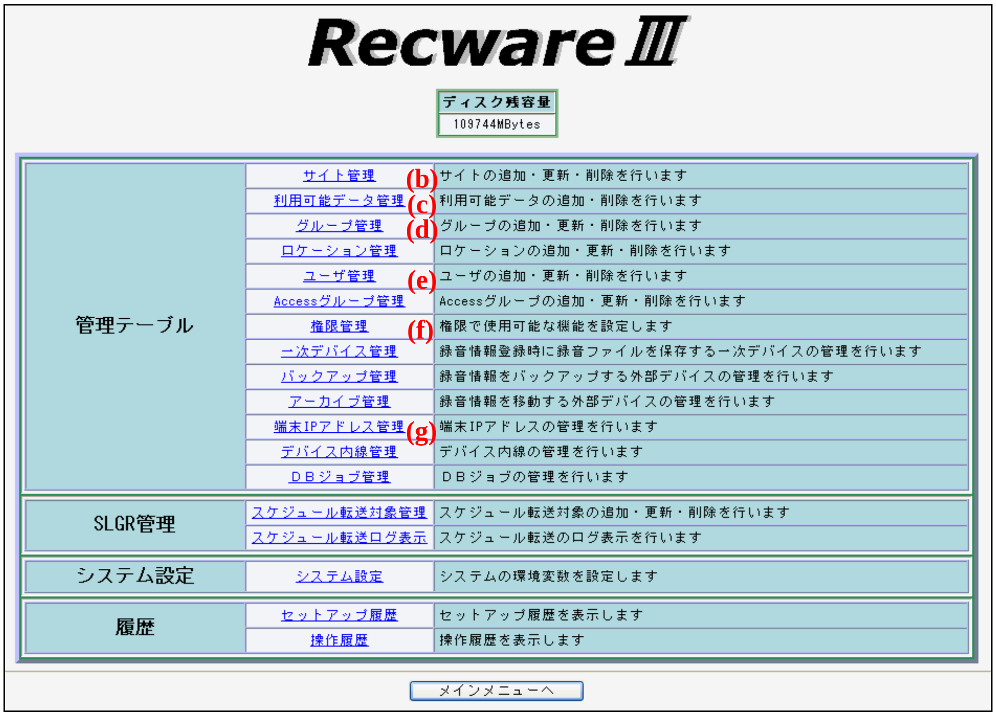
The subsequent web page shows the main menus.



通話情報	通話情報検索	システムに登録されている通話情報・付加情報の検索・参照を行います
	過去の通話情報検索	バックアップ等から読み込んだ過去の通話情報・付加情報の検索・参照を行います
	再生承認一覧	再生申請の一覧を表示し、再生の承認を行います
録音情報	録音情報検索	システムに登録されている録音情報の検索・参照を行います
	過去の録音情報検索	バックアップ等から読み込んだ過去の録音情報の検索・参照を行います
録音情報分析	時間ごとの分析	録音情報を時間ごとに分析表示します
	エージェントごとの分析	録音情報をエージェントごとに分析表示します
過去の録音情報分析	時間ごとの分析	過去の録音情報を時間ごとに分析表示します
	エージェントごとの分析	過去の録音情報をエージェントごとに分析表示します
管理	管理メニュー (a)	管理用メニューを表示します
ユーザ情報	パスワード変更	現在のパスワードを変更します

Figure A-1-2

By clicking the management menu (a) in the above figure A-1-2, the subsequent management menu appears as shown in figure A-1-3.

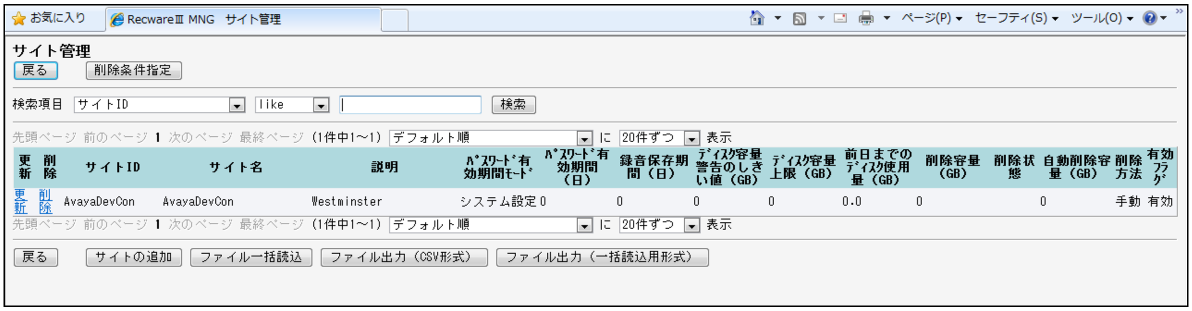

Recware Ⅲ

ディスク残容量
109744MBytes

管理テーブル	サイト管理 (b)	サイトの追加・更新・削除を行います
	利用可能データ管理 (c)	利用可能データの追加・削除を行います
	グループ管理 (d)	グループの追加・更新・削除を行います
	ロケーション管理	ロケーションの追加・更新・削除を行います
	ユーザ管理 (e)	ユーザの追加・更新・削除を行います
	Accessグループ管理	Accessグループの追加・更新・削除を行います
	権限管理 (f)	権限で使用可能な機能を設定します
	一次デバイス管理	録音情報登録時に録音ファイルを保存する一次デバイスの管理を行います
	バックアップ管理	録音情報をバックアップする外部デバイスの管理を行います
	アーカイブ管理	録音情報を移動する外部デバイスの管理を行います
	端末IPアドレス管理 (g)	端末IPアドレスの管理を行います
	デバイス内線管理	デバイス内線の管理を行います
	ＤＢジョブ管理	ＤＢジョブの管理を行います
SLGR管理	スケジュール転送対象管理	スケジュール転送対象の追加・更新・削除を行います
	スケジュール転送ログ表示	スケジュール転送のログ表示を行います
システム設定	システム設定	システムの環境変数を設定します
履歴	セットアップ履歴	セットアップ履歴を表示します
	操作履歴	操作履歴を表示します

Figure A-1-3

(2) Administer configuration settings;
Site configuration settings web page invoked by clicking (b) in figure A-1-3 provides a function of creating a Site (or a Tenant) as shown in figure A-1-4.



サイト管理

検索項目 サイトID like

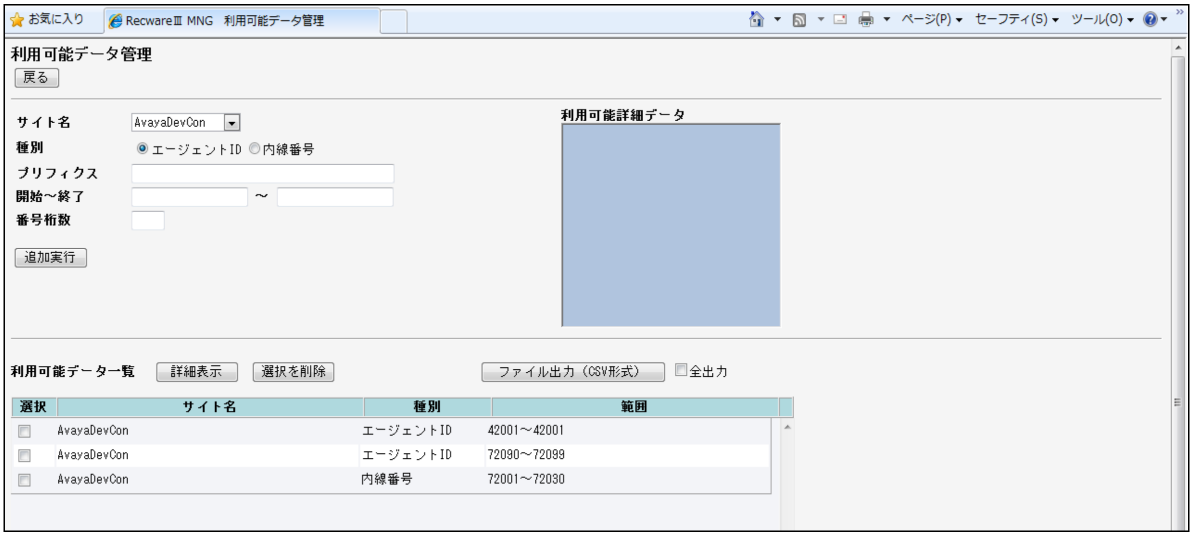
先頭ページ 前のページ 1 次のページ 最終ページ (1件中1～1) デフォルト順 に 20件ずつ 表示

更新	削除	サイトID	サイト名	説明	パスワード有効期間モード	パスワード有効期間（日）	録音保存期間（日）	ディスク容量警告のしきい値（GB）	ディスク容量上限（GB）	前日までのディスク使用量（GB）	削除容量（GB）	削除状態	自動削除容量（GB）	削除方法	有効フラグ
更新	削除	AvayaDevCon	AvayaDevCon	Westminster	システム設定	0	0	0	0	0.0	0		0	手動	有効

先頭ページ 前のページ 1 次のページ 最終ページ (1件中1～1) デフォルト順 に 20件ずつ 表示

Figure A-1-4

Resource configuration settings web page invoked by clicking (c) in figure A-1-3 provides a function of assigning the range of IP phone extensions and agent IDs to a Site shown in figure A-1-5.



利用可能データ管理

サイト名　AvayaDevCon
種別　● エージェントID ○ 内線番号
プリフィクス
開始～終了　～
番号桁数

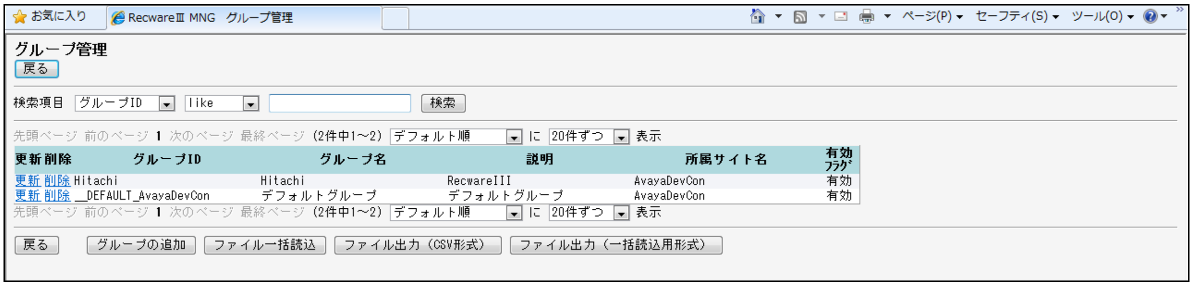
利用可能詳細データ

利用可能データ一覧　☐全出力

選択	サイト名	種別	範囲
☐	AvayaDevCon	エージェントID	42001～42001
☐	AvayaDevCon	エージェントID	72090～72099
☐	AvayaDevCon	内線番号	72001～72030

Figure A-1-5

Group configuration settings web page invoked by clicking (d) in figure A-1-3 provides a function of creating a Group in a Site as shown in figure A-1-6.



グループ管理

検索項目　グループID　like

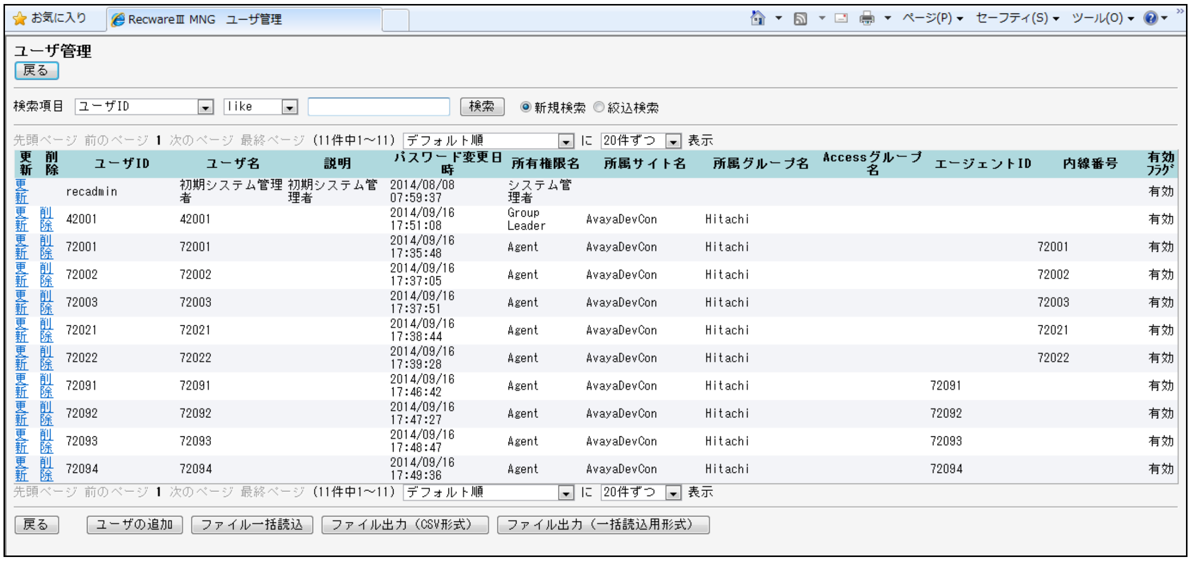
先頭ページ　前のページ　1　次のページ　最終ページ　(2件中1～2)　デフォルト順　に　20件ずつ　表示

更新 削除	グループID	グループ名	説明	所属サイト名	有効フラグ
更新 削除	Hitachi	Hitachi	RecwareIII	AvayaDevCon	有効
更新 削除	__DEFAULT_AvayaDevCon	デフォルトグループ	デフォルトグループ	AvayaDevCon	有効

先頭ページ　前のページ　1　次のページ　最終ページ　(2件中1～2)　デフォルト順　に　20件ずつ　表示

Figure A-1-6

User configuration settings web page invoked by clicking (e) in figure A-1-3 provides a function to add a user such as an IP phone, an agent, a group leader, business manager and site manager in a Site to login to RecwareIII MNG web page as shown in figure A-1-7. A user profile needs to be defined to belong to a site, a group and access privilege profile in the site, and to be charged to a specific phone extension number or agent ID.



検索項目 ユーザID like ● 新規検索 ○ 絞込検索

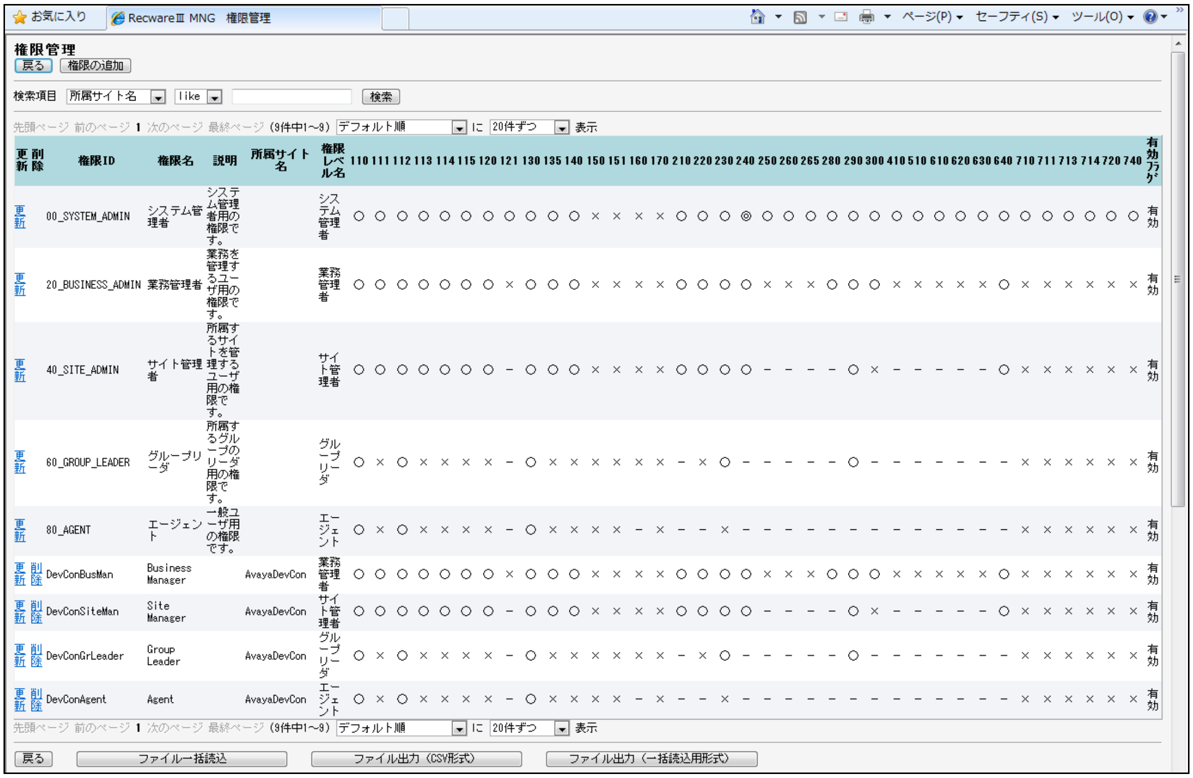
(11件中1～11) デフォルト順 に 20件ずつ 表示

更新	削除	ユーザID	ユーザ名	説明	パスワード変更日時	所有権限名	所属サイト名	所属グループ名	Accessグループ名	エージェントID	内線番号	有効フラグ
更新		recadmin	初期システム管理者	初期システム管理者	2014/08/08 07:59:37	システム管理者						有効
更新	削除	42001	42001		2014/09/16 17:51:08	Group Leader	AvayaDevCon	Hitachi				有効
更新	削除	72001	72001		2014/09/16 17:35:48	Agent	AvayaDevCon	Hitachi			72001	有効
更新	削除	72002	72002		2014/09/16 17:37:05	Agent	AvayaDevCon	Hitachi			72002	有効
更新	削除	72003	72003		2014/09/16 17:37:51	Agent	AvayaDevCon	Hitachi			72003	有効
更新	削除	72021	72021		2014/09/16 17:38:44	Agent	AvayaDevCon	Hitachi			72021	有効
更新	削除	72022	72022		2014/09/16 17:39:28	Agent	AvayaDevCon	Hitachi			72022	有効
更新	削除	72091	72091		2014/09/16 17:46:42	Agent	AvayaDevCon	Hitachi		72091		有効
更新	削除	72092	72092		2014/09/16 17:47:27	Agent	AvayaDevCon	Hitachi		72092		有効
更新	削除	72093	72093		2014/09/16 17:48:47	Agent	AvayaDevCon	Hitachi		72093		有効
更新	削除	72094	72094		2014/09/16 17:49:36	Agent	AvayaDevCon	Hitachi		72094		有効

(11件中1～11) デフォルト順 に 20件ずつ 表示

Figure A-1-7

Access privilege configuration settings web page invoked by clicking (f) in figure A-1-3 provides a function to define flexible hierarchy of access privilege profiles in each Site as shown in figure A-1-8.



検索項目 所属サイト名 like

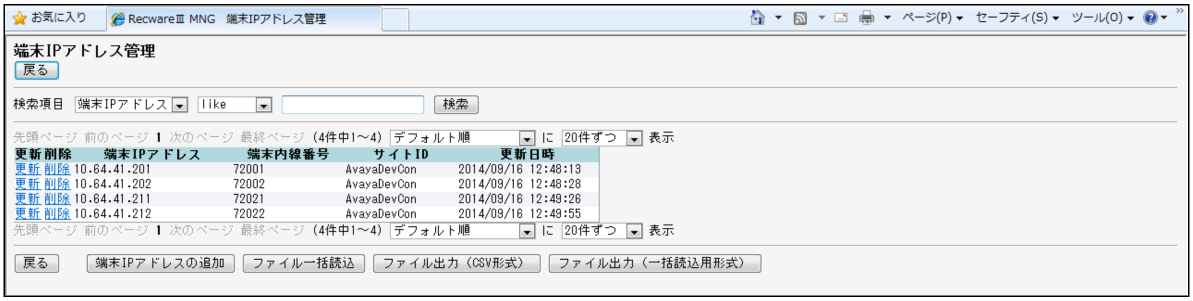
先頭ページ 前のページ **1** 次のページ 最終ページ (9件中1~9) デフォルト順 に 20件ずつ 表示

更新 削除	権限ID	権限名	説明	所属サイト名	権限レベル名	110	111	112	113	114	115	120	121	130	135	140	150	151	160	170	210	220	230	240	250	260	265	280	290	300	410	510	610	620	630	640	710	711	713	714	720	740	有効フラグ
更新	00_SYSTEM_ADMIN	システム管理者	システム管理者用の権限です。		システム管理者	○	○	○	○	○	○	○	○	○	○	○	×	×	×	×	○	○	○	◎	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	有効
更新	20_BUSINESS_ADMIN	業務管理者	業務を管理するユーザ用の権限です。		業務管理者	○	○	○	○	○	○	○	×	○	○	○	×	×	×	×	○	○	○	○	×	×	×	○	○	○	×	×	×	×	×	○	×	×	×	×	×	×	有効
更新	40_SITE_ADMIN	サイト管理者	所属するサイトを管理するユーザ用の権限です。		サイト管理者	○	○	○	○	○	○	○	－	○	○	○	×	×	×	×	○	○	○	○	－	－	－	－	○	×	－	－	－	－	－	○	×	×	×	×	×	×	有効
更新	60_GROUP_LEADER	グループリーダ	所属するグループのリーダ用の権限です。		グループリーダ	○	×	○	×	×	×	×	－	○	×	×	×	×	×	×	－	×	○	－	－	－	－	－	○	－	－	－	－	－	－	－	×	×	×	×	×	×	有効
更新	80_AGENT	エージェント	一般ユーザ用の権限です。		エージェント	○	×	○	×	×	×	×	－	○	×	×	×	×	－	×	－	－	×	－	－	－	－	－	－	－	－	－	－	－	－	－	×	×	×	×	×	×	有効
更新 削除	DevConBusMan	Business Manager		AvayaDevCon	業務管理者	○	○	○	○	○	○	○	×	○	○	○	×	×	×	×	○	○	○	○	×	×	×	○	○	○	×	×	×	×	×	○	×	×	×	×	×	×	有効
更新 削除	DevConSiteMan	Site Manager		AvayaDevCon	サイト管理者	○	○	○	○	○	○	○	－	○	○	○	×	×	×	×	○	○	○	○	－	－	－	－	○	×	－	－	－	－	－	○	×	×	×	×	×	×	有効
更新 削除	DevConGrLeader	Group Leader		AvayaDevCon	グループリーダ	○	×	○	×	×	×	×	－	○	×	×	×	×	×	×	－	×	○	－	－	－	－	－	○	－	－	－	－	－	－	－	×	×	×	×	×	×	有効
更新 削除	DevConAgent	Agent		AvayaDevCon	エージェント	○	×	○	×	×	×	×	－	○	×	×	×	×	－	×	－	－	×	－	－	－	－	－	－	－	－	－	－	－	－	－	×	×	×	×	×	×	有効

先頭ページ 前のページ **1** 次のページ 最終ページ (9件中1~9) デフォルト順 に 20件ずつ 表示

Figure A-1-8

Phone IP address mapping web page invoked by clicking (g) in figure A-1-3 provides a function to view the map dynamically captured by port mirroring of H.323 registration from each station as shown in figure A-1-9. For uncaptured devices, each phone IP address needs to be statically added



検索項目 端末IPアドレス like

先頭ページ 前のページ **1** 次のページ 最終ページ (4件中1~4) デフォルト順 に 20件ずつ 表示

更新 削除	端末IPアドレス	端末内線番号	サイトID	更新日時
更新 削除	10.64.41.201	72001	AvayaDevCon	2014/09/16 12:48:13
更新 削除	10.64.41.202	72002	AvayaDevCon	2014/09/16 12:48:28
更新 削除	10.64.41.211	72021	AvayaDevCon	2014/09/16 12:49:26
更新 削除	10.64.41.212	72022	AvayaDevCon	2014/09/16 12:49:55

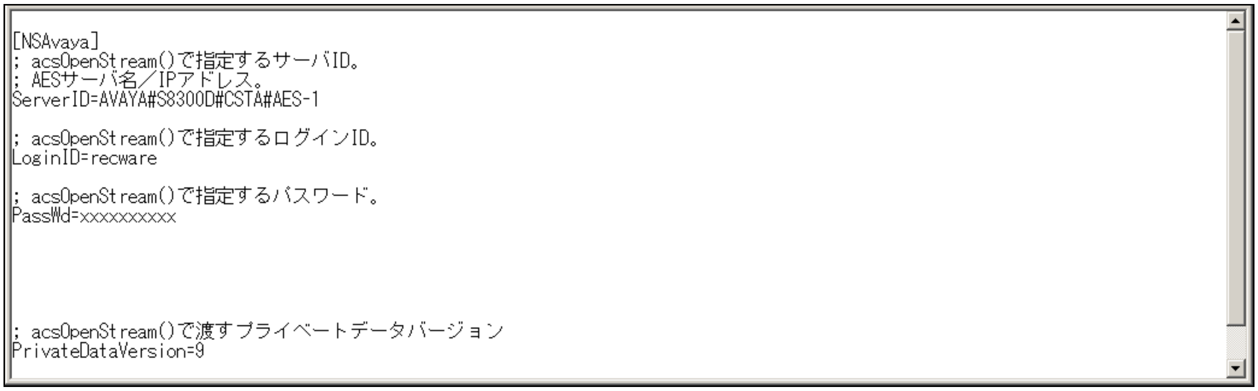
先頭ページ 前のページ **1** 次のページ 最終ページ (4件中1~4) デフォルト順 に 20件ずつ 表示

Figure A-1-9

A.2. Recware III AS-GW Settings

(1) The AS-GW configuration settings to connect to Application Enablement Services:
The *D:\AS-GW\AS-GW\Config\NSCommon.ini* file should be modified as shown in figure A-2-1.

- Modify ServerID part to the same value as **Section 6.6 Obtain Tlink Name**
- Modify LoginID and PassWd parts to the same value as **Section 6.10 Administer Recware III User**
- Modify PrivateDataVersion part as follows;
  8: for the connection with AES 5.2 or earlier
  9: for the connection with AES 6.1 or later

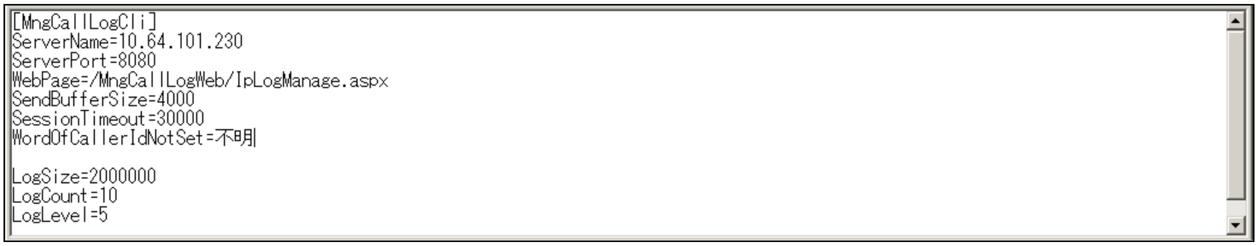


```
[NSAvaya]
; acsOpenStream()で指定するサーバID。
; AESサーバ名／IPアドレス。
ServerID=AVAYA#S8300D#CSTA#AES-1

; acsOpenStream()で指定するログインID。
LoginID=recware

; acsOpenStream()で指定するパスワード。
PassWd=xxxxxxxxxx





; acsOpenStream()で渡すプライベートデータバージョン
PrivateDataVersion=9
```

Figure A-2-1

(2) AS-GW configuration settings to connect to Recware III MNG:
The *D:\AS-GW\LNK\MngCallLogCli.ini* file should be modified as shown in figure A-2-2.

- Modify the ServerName to the value of MNG IP address



```
[MngCallLogCli]
ServerName=10.64.101.230
ServerPort=8080
WebPage=/MngCallLogWeb/IpLogManage.aspx
SendBufferSize=4000
SessionTimeout=30000
WordOfCallerIdNotSet=不明

LogSize=2000000
LogCount=10
LogLevel=5
```

Figure A-2-2

A.3. Recware III SLGR Settings

(1) Recware III SLGR License Key:

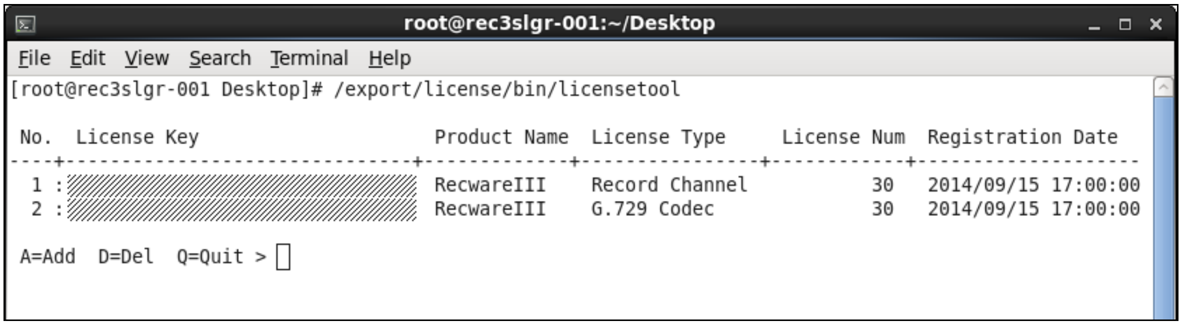
Log into SLGR Linux by root user with the appropriate credentials. Register Recware III SLGR license key according to the steps below.

(i) Start the license registration tool by executing the following command
/export/license/bin/licensetool [Enter]

(ii) Enter the command below to select adding a license among the menu of actions displayed.
A [Enter]

(iii) Type the same exact license key value, which is case-sensitive, at the cursor position prompted. When done, hit the Enter key and verify the license key shows simultaneous recording channels and G.729 encoding/ decoding channels given to the Recware III system.

(iv) Upon confirming a successful completion message, finish the license registration tool by executing the command below.
Q [Enter]

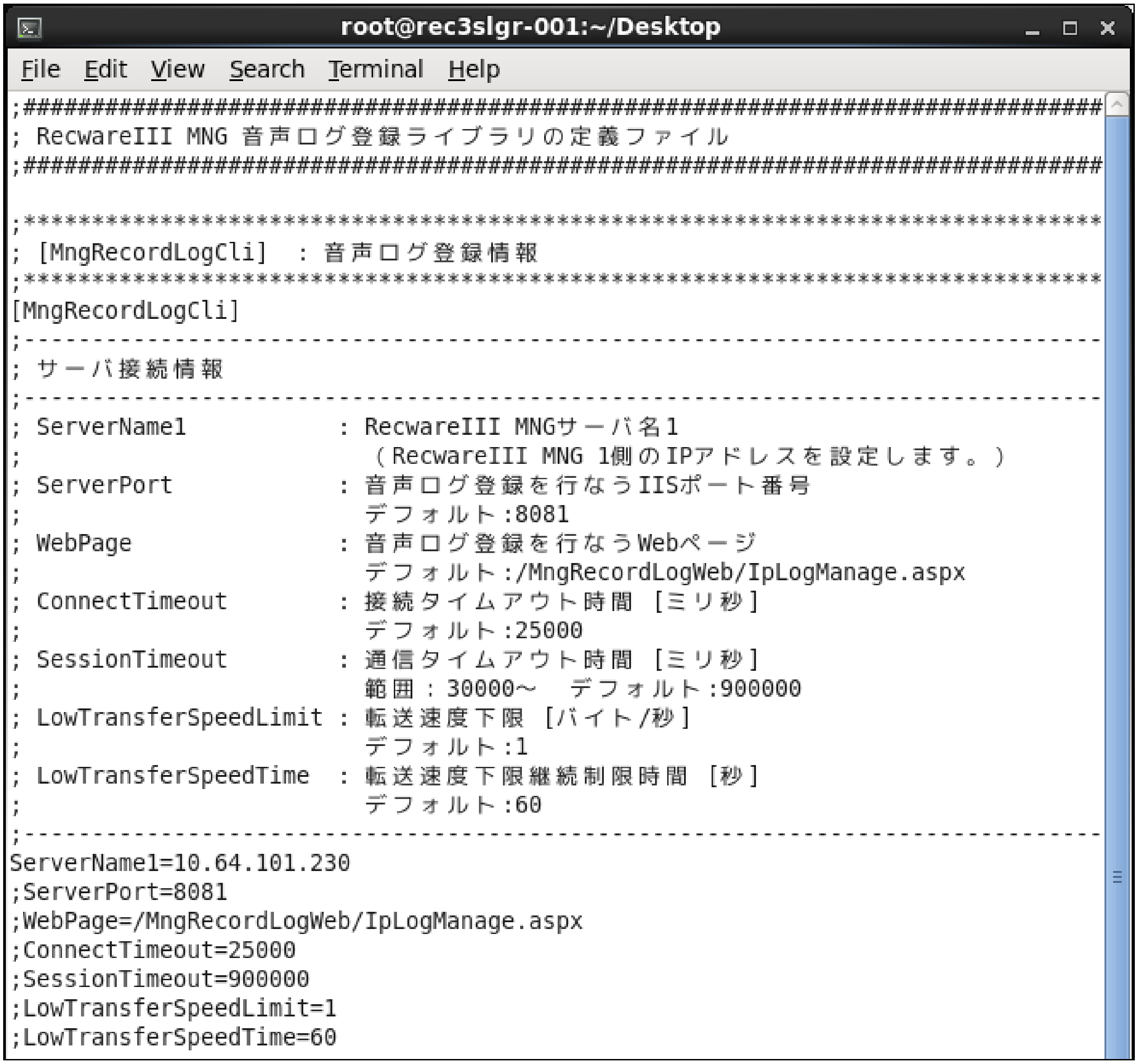

root@rec3slgr-001:~/Desktop
File Edit View Search Terminal Help

```
[root@rec3slgr-001 Desktop]# /export/license/bin/licensetool

 No.  License Key                     Product Name  License Type     License Num  Registration Date
----+-------------------------------+-------------+----------------+------------+--------------------
  1 :[redacted]                       RecwareIII    Record Channel            30   2014/09/15 17:00:00
  2 :[redacted]                       RecwareIII    G.729 Codec               30   2014/09/15 17:00:00

 A=Add  D=Del  Q=Quit >
```

Figure A-3-1

(2) SLGR configuration settings to connect to Recware III MNG:
The *\export\slgr\ini\mngrecordlogcli.ini* file should be modified as shown in figure A-2-2.

- Modify **ServerName1** which is part of the [MngRecordLogCli] section, to the value of MNG IP address.



root@rec3slgr-001:~/Desktop
File Edit View Search Terminal Help

```
;###############################################################################
; RecwareIII MNG 音声ログ登録ライブラリの定義ファイル
;###############################################################################

;*******************************************************************************
; [MngRecordLogCli]  : 音声ログ登録情報
;*******************************************************************************
[MngRecordLogCli]
;-------------------------------------------------------------------------------
; サーバ接続情報
;-------------------------------------------------------------------------------
; ServerName1           : RecwareIII MNGサーバ名1
;                         （RecwareIII MNG 1側のIPアドレスを設定します。）
; ServerPort            : 音声ログ登録を行なうIISポート番号
;                         デフォルト:8081
; WebPage               : 音声ログ登録を行なうWebページ
;                         デフォルト:/MngRecordLogWeb/IpLogManage.aspx
; ConnectTimeout        : 接続タイムアウト時間 [ミリ秒]
;                         デフォルト:25000
; SessionTimeout        : 通信タイムアウト時間 [ミリ秒]
;                         範囲：30000～  デフォルト:900000
; LowTransferSpeedLimit : 転送速度下限 [バイト/秒]
;                         デフォルト:1
; LowTransferSpeedTime  : 転送速度下限継続制限時間 [秒]
;                         デフォルト:60
;-------------------------------------------------------------------------------
ServerName1=10.64.101.230
;ServerPort=8081
;WebPage=/MngRecordLogWeb/IpLogManage.aspx
;ConnectTimeout=25000
;SessionTimeout=900000
;LowTransferSpeedLimit=1
;LowTransferSpeedTime=60
```

Figure A-3-2

A.4. Client PC Settings

(1) Internet Explore Settings:

In order to operate Recware III MNG on the Web interface, Internet Explorer (IE8, IE9, IE10 or IE11) settings may require several changes. Modify such settings according to the subsections below.

(A) General Settings

Modify the Browsing Settings tab on the General tab of “Internet Options” dialog according to the steps below.

- (i) IE8 only: Select “Check Always switch to new tabs when they are created”
- (ii) Select “Always open pop-ups in a new tab”.

(B) Security Settings

Change the Security Settings of Internet Explorer according to the steps below.

- (i) Start your MNG Web page operation using the URL http://ServerName/RecIP/ (for ServerName, type the computer name or IP address of Management Server).
- (ii) In Internet Explorer status bar of “Log In” page (when “Interact with Active Directory” feature is not used) or “Main Menu” page (when “Interact with Active Linkage” feature is enabled according to Recware III SE Manual), check for the security zone display and remember which is shown: “Internet” or “Local intranet"
- (iii) Select Local intranet zone and click Default level button on Security tab in “Internet Options” resulting security level in this zone set to Medium-low.
- (iv) If the security zone display you remembered at Step (ii) is "Local intranet", go to Step (vi). Otherwise, go to Step (v).
- (v) Click Sites button to open "Local intranet" dialog and click Advanced button to open child dialog of the same title. Type http://ServerName (for ServerName, type the computer name or IP address of Management Server) in the text box. And after confirming the entered URL in "Websites" list, click Close button to close this child dialog. In "Local intranet" parent dialog revisited, click OK button.
- (vi) Select Local intranet zone on Security tab of "Internet Options" dialog, and click Custom level button to open “Security Settings” dialog. Specify the following settings:
  - Under “ActiveX controls and plug-ins”
    - ✓ “Run ActiveX controls and plug-ins”: Select Enable radio button.
    - ✓ “Script ActiveX controls marked safe for scripting”: Select Enable radio button.
  - Under “Scripting” “Active scripting”: Select Enable radio button.
  - Under “Downloads” “File download”: Select Enable radio button.

In “Internet Options” dialog revisited, click OK button.

(C) Add-on Management for Windows Media Player

Check and, if necessary, modify the add-on management of Internet Explorer for Windows.

- (i) From menu or tool bar, click Tools and click Manage Add-ons.

(ii) In the left pane of “Manage Add-ons” dialog opened, click the drop-down menu under “Show” and select Run without permission. In the right pane, scroll the list and select Windows Media Player to see if the value in “Status” field shows “Enabled”.

(iii) If the value in "Status" field shows "Disabled" instead of “Enabled”, enable this add-on according to the substeps below. Otherwise, click Close button.

- Click Enable button while Windows Media Player is still selected.
- Click Close button and restart Internet Explorer.

(D) Advanced Settings

Change the advanced settings of Internet Explorer according to the steps below.

(i) From menu or tool bar, click Tools and click Internet Options. In “Internet Options” dialog opened, click the Advanced tab.

(ii) Scroll the list and specify the following settings:

- Security: Check the check box of “Empty Temporary Internet Files folder when browser is closed”
- Browsing: [Optional] Check the check box of “Notify when downloads complete”
- Underline links: [Recommended] Select “Always” radio button
- Multimedia: Show pictures: [Recommended] Check the check box of “Shows pictures”

(iii) Click OK button to save the settings.

(E) Compatibility View Settings

Add MNG Web pages to Compatibility View according to the steps below.

(i) From menu or tool bar, click Tools and click Compatibility View.

(ii) In the text box of “Compatibility View” dialog, type the computer name or IP address of Management Server. Click Add button.

(iii) After confirming the entered value in “Websites you've added to Compatibility View” list, click Close button.

(iv) Exit Internet Explorer.

(2) Microsoft IME Settings

While Windows Vista and Windows 7 support JIS X2004-unique characters in addition to conventional Shift-JIS characters, Recware III MNG does not accept JIS X2004-unique characters. To exclude JIS X2004-unique characters from input to Recware III MNG, modify Microsoft IME settings according to the steps below.

(i) Right-click IME Pad on the desktop and click Settings.

(ii) In "Text Services and Input Languages" dialog opened, click General tab if not selected. In "Installed services" list, click Microsoft IME. Click Properties button.

(iii) In "Properties for Microsoft IME" dialog opened, click Conversion tab. Click Character conversion control button.

(iv) "Microsoft IME Character conversion control" dialog opens. Check Convert words and characters using only JIS X 0208 characters check box and click OK button.

(v) In "Properties for Microsoft IME" dialog revisited, click OK button.

(vi) In "Text Services and Input Languages" dialog revisited, click OK button.

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.