



DevConnect Program

Application Notes for Integrated Research Collaborate Prognosis Server 12.2 with Avaya Aura® Communication Manager Call Center Elite 10.1 - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Integrated Research Collaborate Prognosis Server 12.2 to interoperate with Avaya Aura® Communication Manager Call Center Elite 10.1.

Integrated Research Collaborate Prognosis Server provides real-time monitoring and management solutions for IP telephony networks. Prognosis provides visibility of Avaya and other vendor's IP Telephony solutions from a single console and enables a reduction in complexity when managing complex IP telephony environments.

Integrated Research Collaborate Prognosis Server integrates directly to Avaya Aura® Communication Manager using Secure Shell (SSH) or Telnet and uses Simple Network Management Protocol (SNMP) to query Avaya Aura® Communication Manager for Call Center data. At the same time, it processes Real-time Transport Control Protocol (RTCP) and Call Detail Recording (CDR) information from Avaya Aura® Communication Manager. These Application Notes will focus on the relevant Call Center data collected in Collaborate Prognosis Server. SNMP and RTCP are not covered in these Application Notes.

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.

Introduction

These Application Notes describe the compliance tested configuration used to validate Collaborate Prognosis Server R12.2 (herein after referred to as Prognosis) with Avaya Aura® Communication Manager Call Center Elite R10.1.

1. Prognosis uses four integration methods to monitor a Communication Manager system.
 - System Access Terminal (SAT) - Prognosis uses a pool of Telnet/SSH connections to the SAT using the IP address of Communication Manager. By default, the solution establishes three concurrent SAT connections to each Communication Manager system and uses the connections to execute SAT commands.
 - Real Time Transport Control Protocol (RTCP) collection - Prognosis collects RTCP information sent by Avaya resources, including IP Media Processor (MEDPRO) boards, media gateways, media servers and IP Deskphones.
 - Call Detail Recording (CDR) collection - Prognosis collects CDR information sent by Communication Manager.
 - Simple Network Management Protocol (SNMP) - Prognosis uses SNMP to read Communication Manager name and IP address as this information cannot be collected via the standard SAT interface.

These Application Notes will focus on the collection of Call Center data via SAT in Prognosis, such as VDN, Vectors, call flows, Agents details, and Call Detail Records. RTCP and SNMP configuration is not covered in these Application Notes.

2. General Test Approach and Test Results

The general test approach was to use Prognosis Web (webui) to display the configuration of Call Center Elite information and verify against what is displayed on the SAT interface. The SAT interface is accessed by using Secure Shell (SSH) to Communication Manager. The basic configurations of SAT interface is detailed in reference [3]. Calls were placed between various Avaya endpoints and Prognosis webui was used to display the calls and CDR information collected. Information on the call flow such as VDN, Vectors and call flows and agent details collected were also checked.

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 Prognosis utilized capabilities of SSH for SAT as requested by Integrated Research.

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

For feature testing, Prognosis webui was used to view the configuration of Communication Manager via collected SAT data of resources for agents, such as media gateways, media servers, trunk groups, and Call Center Elite agents, stations, related VDN and vectors (including vector diagrams) information.

For the collection of CDR information, the endpoints included Avaya H.323 and SIP, and Avaya Agent for Desktop user. The types of calls made included inbound trunk calls, outbound trunk calls, and local calls.

For serviceability testing, reboots were applied to Prognosis and Communication Manager to simulate system unavailability. Interchanging of the duplex Communication Manager and loss of network connections were also performed during testing.

Test Results

All test cases passed successfully with observations below:

- Customized format and parameters settings is recommended Call Detail Records for the necessary data to be collected for linking of Agents and VDNs to calls in the CDR.

2.2. Support

For technical support on Integrated Research Prognosis, contact the Integrated Research Support Team at:

- 2.3.
- Hotline: +61 (2) 9966 1066
 - Email: support@ir.com

Reference Configuration

- Figure 1** illustrates the test configuration used to verify Prognosis interoperability with Communication Manager with Call Center Elite. The configuration consists of a duplex Communication Manager system (System A) with two Avaya G650 Media Gateways and an Avaya G430 Media Gateway with Communication Manager as a Local Survivability Processor (LSP). A simplex Enterprise Survivable Server (ESS) was also configured. Avaya J100 Series Deskphones using H.323 and SIP protocol endpoints, and Avaya Agent for Desktop (H.323 and SIP) are used as endpoints for agents for making and receiving calls. Avaya Aura® System Manager and Avaya Aura® Session Manager provided SIP support to the Avaya SIP endpoints. Prognosis was installed on Microsoft Windows Server 2019. Both the Monitoring Node and Web Application software are installed on this server. Avaya Session Border Controller for Enterprise was used to complete a SIP trunk connection to simulate a PSTN connection to the Enterprise solution.

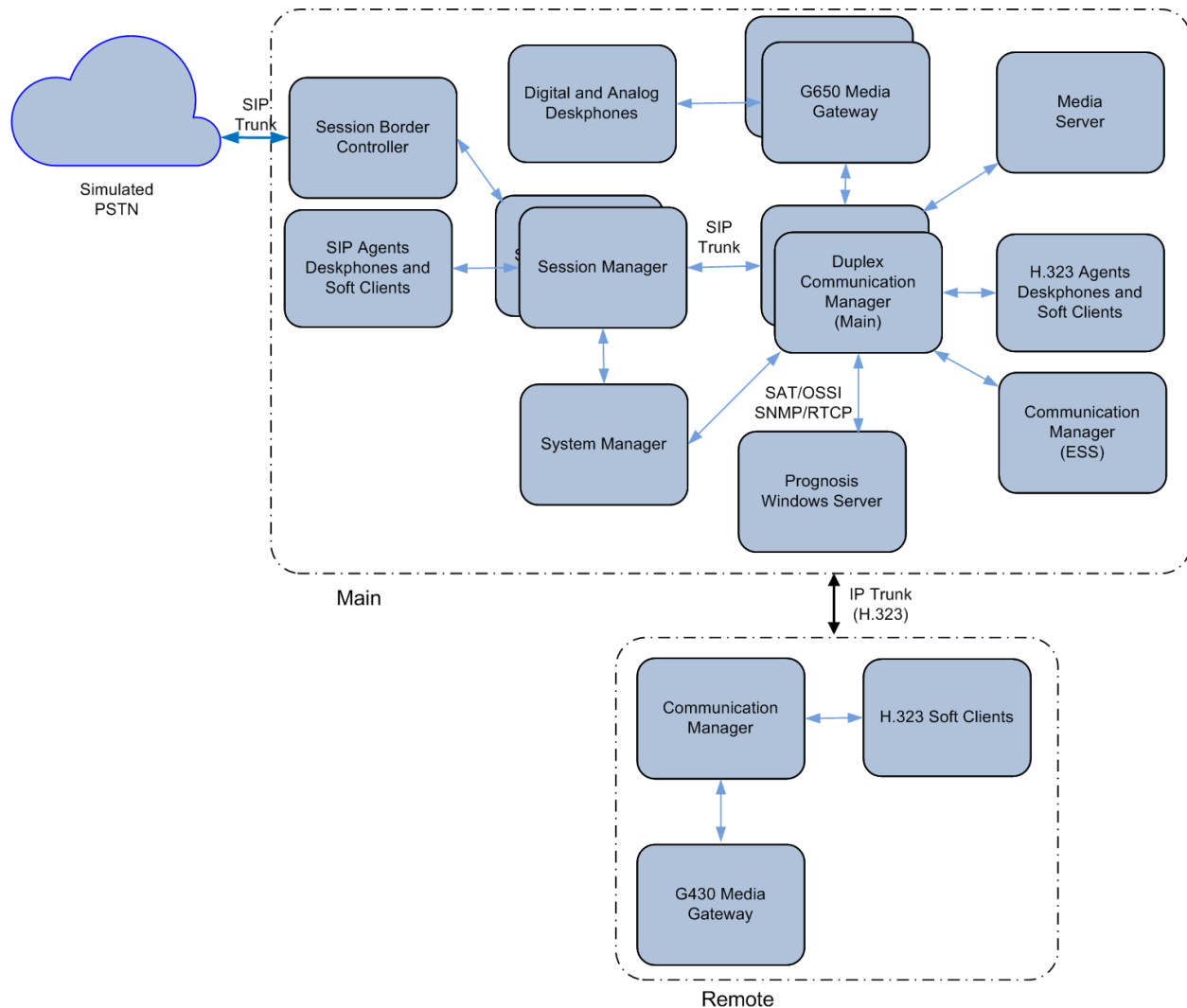


Figure 1: Test Configuration

Equipment and Software Validated

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

4.

Equipment/Software	Release/Version
Avaya Session Border Controller	10.1.0.0-32-21432
Avaya Aura® Communication Manager	10.1 FP3 (10.1.3.0.0.974.27867)
Avaya Aura® Media Server	10.1 FP3 (10.1.0.147)
Avaya G650 Media Gateway - TN2312BP IP Server Interface - TN799DP C-LAN Interface - TN2602AP IP Media Processor - TN2302AP IP Media Processor - TN2464BP DS1 Interface - TN2464CP DS1 Interface - TN793CP Analog Line - TN2214CP Digital Line - TN2501AP Announcement	HW07, FW058 HW01, FW044 HW02 FW067 HW20 FW121 HW05, FW025 HW02 FW025 HW09, FW012 HW08, FW016 HW03 FW024
Avaya Aura® Communication Manager	10.1 FP3 (10.1.3.0.0.974.27867)
Avaya G430 Media Gateway - MM712AP DCP MM - MM716AP Analog MM - MM711AP Analog MM - MM710AP DS1 MM	42.22.0 HW04 FW015 HW12 FW104 HW31 FW104 HW05 FW022
Avaya Aura® Communication Manager	10.1 FP3 (10.1. 3.0.0.974.27867)
Avaya Aura® System Manager	10.1 FP3 Build No. - 10.1.0.0.537353 Feature Pack 3 Latest Build 10.1.3.0.0715713
Avaya Aura® Session Manager	10.1 FP3 (10.1.0.3.1013007)
Avaya J100 Series IP Telephones	4.1,1.0 (SIP) 6.8541 (H.323)
Avaya Agent for Desktop	2.0.6.25.3006 (H.323/SIP)
Integrated Research Collaborate Prognosis Server running on Windows Server	12.2 Microsoft Windows Server 2019 Standard Edition

Note: All Avaya Aura® systems and Prognosis runs on VMware 7.x virtual platform.

Configure Avaya Aura® Communication Manager

Please note that basic configuration for Communication Manager to interoperate with Prognosis is detailed in DevConnect Application Notes (see reference [3] of **Section 9**). Hence, details will not be illustrated here. Other than CDR, data from forms below are collected through SAT by Prognosis.

5.

This section describes the steps needed to configure Call Center Elite to interoperate with Prognosis. This includes the following:

1. Configure System-Parameters CDR Form.
2. Configure Stations.
3. Configure Skill Hunt Group.
4. Configure Agents.
5. Configure VDN and Vectors.

Configure System-Parameters CDR Form

5.1. Enter the **change system-parameters cdr** command to set the parameters for the type of calls to track and the format of the CDR data. The following settings were used during the compliance test for the default CDR format recommended.

- **CDR Date Format: month/day**
- **Primary Output Format: unformatted**
- **Primary Output Endpoint: CDR1**

The remaining parameters define the type of calls that will be recorded and what data will be included in the record. See [2] for a full explanation of each field. The test configuration used some of the more common fields described below.

- **Use Legacy CDR Formats? y** [Specify the use of Communication Manager 3.x (“legacy”) formats in the CDR records produced by the system.]
- **Intra-switch CDR: y** [Allows call records for internal calls involving specific stations. Those stations must be specified in the **intra-switch-cdr** form (not illustrated)]
- **Record Outgoing Calls Only? n** [Allows incoming trunk calls to appear in the CDR records along with the outgoing trunk calls.]
- **Outg Trk Call Splitting? y** [Allows a separate call record for any portion of an outgoing call that is transferred or conferenced.]
- **Inc Trk Call Splitting? n** [Allow a separate call record for any portion of an incoming call that is transferred or conferenced.]

```

change system-parameters cdr                                     Page 1 of 1
                                CDR SYSTEM PARAMETERS
Node Number (Local PBX ID): 1                                CDR Date Format: month/day
Primary Output Format: unformatted    Primary Output Endpoint: CDR1
Secondary Output Format:
    CDR Retention (days): 20
    Use ISDN Layouts? n
    Use Enhanced Formats? n
    Use Legacy CDR Formats? y
Modified Circuit ID Display? n
                                Enable CDR Storage on Disk? n
                                Condition Code 'T' For Redirected Calls? n
                                Remove # From Called Number? n
                                Intra-switch CDR? y
                                Record Outgoing Calls Only? n    Outg Trk Call Splitting? y
Supress CDR for Ineffective Call Attempts? y    Outg Attd Call Record? y
    Disconnect Information in Place of FRL? n    Interworking Feat-flag? n
Force Entry of Acct Code for Calls Marked on Toll Analysis Form? n
    Calls to Hunt Group - Record: member-ext
Record Called Vector Directory Number Instead of Group or Member? n
Record Agent ID on Incoming? y    Record Agent ID on Outgoing? y
    Inc Trk Call Splitting? n
    Record Non-Call-Assoc TSC? n    Call Record Handling Option: warning
    Record Call-Assoc TSC? n    Digits to Record for Outgoing Calls: dialed
    Privacy - Digits to Hide: 0    CDR Account Code Length: 15
Remove '+' from SIP Numbers? y    Record UCID? n

```

For each trunk group for which CDR records are desired, verify that CDR reporting is enabled. Enter the **change trunk-group n** command, where **n** is the trunk group number, to verify that the **CDR Reports** field is set to **y**. Repeat for all trunk groups to be reported.

```

change trunk-group 7                                           Page 1 of 4
                                TRUNK GROUP
Group Number: 7                                Group Type: sip    CDR Reports: y
Group Name: SIP Trunk to SM1    COR: 1    TN: 1    TAC: #07
Direction: two-way    Outgoing Display? y
Dial Access? n
Queue Length: 0
Service Type: tie
                                Night Service:
                                Auth Code? n
                                Member Assignment Method: auto
                                Signaling Group: 7
                                Number of Members: 14

```


Configure Stations

H.323 and SIP deskphones were used for agents. The same agent used the same station when switching to Avaya Agent for Desktop (softphone). Note that the SIP station was configured through Avaya Aura® System Manager.

5.2.1. Configure Avaya H.323 Station

H.323 stations were used by Avaya Agents with a J100 Series Deskphone. The station form must have “IP Softphone” set to “y” for Avaya Agent for Desktop. Enter **change station x**, where x is the extension number of the station to be changed. Ensure that **IP Softphone** is set to y as shown below:

change station 10001		Page 1 of 5
STATION		
Extension: 10001	Lock Messages? n	BCC: 0
Type: 9611G	Security Code: *	TN: 1
Port: S000002	Coverage Path 1: 99	COR: 1
Name: Agent 1	Coverage Path 2:	COS: 1
Unicode Name? n	Hunt-to Station:	Tests? y
STATION OPTIONS		
Time of Day Lock Table:		
Loss Group: 19	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 10001	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english	Button Modules: 0	
Survivable GK Node Name:		
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? y	
	IP Video Softphone? n	
	Short/Prefixed Registration Allowed: default	
	Customizable Labels? y	

On **Page 4** below, check that the buttons highlighted below are configured for agents using Avaya Agent for Desktop.

change station 10001		Page 4 of 5
STATION		
SITE DATA		
Room: [B		Headset? y
Jack:		Speaker? n
Cable:		Mounting: d
Floor: #03-09/10		Cord Length: 0
Building: Rutherford		Set Color: blue
ABBREVIATED DIALING		
List1: system	List2:	List3:
BUTTON ASSIGNMENTS		
1:call-appr	5:manual-in	Grp:
2:call-appr	6:after-call	Grp:
3:call-appr	7:auto-in	Grp:
4:release	8:aux-work	RC: Grp:
voice-mail		

5.3. Configure Skill Hunt Group

Enter the command **add hunt-group x** where **x** is an appropriate hunt group number and configure as follows.

- **Group Number** – skill number when configuring the agent and vector.
- **Group Name** – enter an appropriate name.
- **Group Extension** – enter an extension appropriate to the dialplan.
- **Group Type** – set to **ead-mia**.
- **ACD?** – set to **y**.
- **Queue?** – set to **y**.
- **Vector?** – set to **y**.

add hunt-group 1		Page 1 of 4
HUNT GROUP		
Group Number: 1	ACD? y	
Group Name: n	Queue? y	
Group Extension: 13001	Vector? y	
Group Type: ead-mia		
TN: 1		
COR: 1	MM Early Answer? n	
Security Code:	Local Agent Preference? n	
ISDN/SIP Caller Display: grp-name		
Queue Limit: unlimited		
Calls Warning Threshold:	Port:	
Time Warning Threshold:	Port:	
SIP URI:		

On Page 2, set Skill to y.

add hunt-group 1		Page 2 of 4
HUNT GROUP		
Skill? y	Expected Call Handling Time (sec): 180	
AAS? n	Service Level Target (% in sec): 80 in 20	
Measured: both		
Supervisor Extension:		
Controlling Adjunct: none		
VuStats Objective:		
Multiple Call Handling: none		
Timed ACW Interval (sec):	After Xfer or Held Call Drops? n	

Configure Agents

Elite Agents login to use the skill group setup in **Section 5.3**. Enter the command **add agent-loginID x** where **x** is a valid extension for agent ID and configure as follows.

- 5.4.
- **Login ID** –note the configured **Login ID**.
 - **Name** – enter a descriptive name.
 - **Password** – enter a password for the agent.

```
add agent-loginID 11001                                     Page 1 of 3
                                AGENT LOGINID

      Login ID: 11001                                Unicode Name? n   AAS? n
      Name: Agent_1                                AUDIX? n
      TN: 1                                Check skill TNs to match agent TN? n
      COR: 1
      Coverage Path:                                LWC Reception: spe
      Security Code: 1234                        LWC Log External Calls? n
      Attribute:                                AUDIX Name for Messaging:

                                LoginID for ISDN/SIP Display? n
                                Password:1234
                                Password (enter again):1234
      MWI Served User Type:                                Auto Answer: none
      AUX Agent Remains in LOA Queue: system                MIA Across Skills: system
      AUX Agent Considered Idle (MIA): system                ACW Agent Considered Idle: system
      Work Mode on Login: system                Aux Work Reason Code Type: system
                                Logout Reason Code Type: system
      Maximum time agent in ACW before logout (sec): system
      Forced Agent Logout Time: :

      WARNING: Agent must log in again before changes take effect
```

On **Page 2**, enter the hunt group number configured in **Section 5.3** in the **SN (Skill Number)** column and enter an appropriate **SL (skill level)**.

```
add agent-loginID 11001                                     Page 2 of 3
                                AGENT LOGINID

      Direct Agent Skill:                                Service Objective? n
      Call Handling Preference: skill-level                Local Call Preference? n

      SN   RL   SL           SN   RL   SL           SN   RL   SL           SN   RL   SL
1: 1      1      1        16:          31:          46:
2:          17:          32:          47:
3:          18:          33:          48:
4:          19:          34:          49:
```

Configure VDN and Vectors

The following shows a sample of VDN and Vectors used for the ACD calls. Call is initially routed to VDN **14001** where Vector **1** is called upon.

5.5.

change vdn 14001	Page 1 of 3
VECTOR DIRECTORY NUMBER	
Extension: 14001	Unicode Name? n
Name*: Normal Q	
Destination: Vector Number	1
Attendant Vectoring? n	
Meet-me Conferencing? n	
Allow VDN Override? n	
COR: 1	
TN*: 1	
Measured: both	Report Adjunct Calls as ACD*? n
Acceptable Service Level (sec): 20	
VDN of Origin Annc. Extension*:	
1st Skill*:	
2nd Skill*:	
3rd Skill*:	
SIP URI:	
* Follows VDN Override Rules	

change vector 1	Page 1 of 6		
CALL VECTOR			
Number: 1	Name: Sales		
Multimedia? n	Attendant Vectoring? n	Meet-me Conf? n	Lock? n
Basic? y	EAS? y	G3V4 Enhanced? y	ANI/II-Digits? y
Prompting? y	LAI? y	G3V4 Adv Route? y	ASAI Routing? y
Variables? y	3.0 Enhanced? y	CINFO? y	BSR? y
01 wait-time	1 secs	hearing silence	
02 queue-to	skill 1	pri m	
03 wait-time	900 secs	hearing music	
04 disconnect	after announcement	none	
05			

Enter **save translation** to save the changes made.

save translation	
SAVE TRANSLATION	
Command Completion Status	Error Code
Success	0

Configure Avaya Aura® Session Manager

This section covers the configuration of a SIP user for Avaya Agents using J100 Series Deskphones and Avaya Agent for Desktop.

Configure Avaya SIP Station

6. Avaya Agents using SIP extension to log into a J100 Series Deskphone and Avaya Agent for Desktop.
 - 6.1. Changes of SIP Deskphone on Communication Manager must be carried out from System Manager. Access the System Manager using a web browser by entering **http://<FQDN>/network-login**, where <FQDN> is the fully qualified domain name of System Manager or **http://<IP Address>/network-login**. Log in using appropriate credentials.

Note: The following shows changes a SIP extension and assumes that the SIP extension has been programmed correctly and is fully functioning.

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.

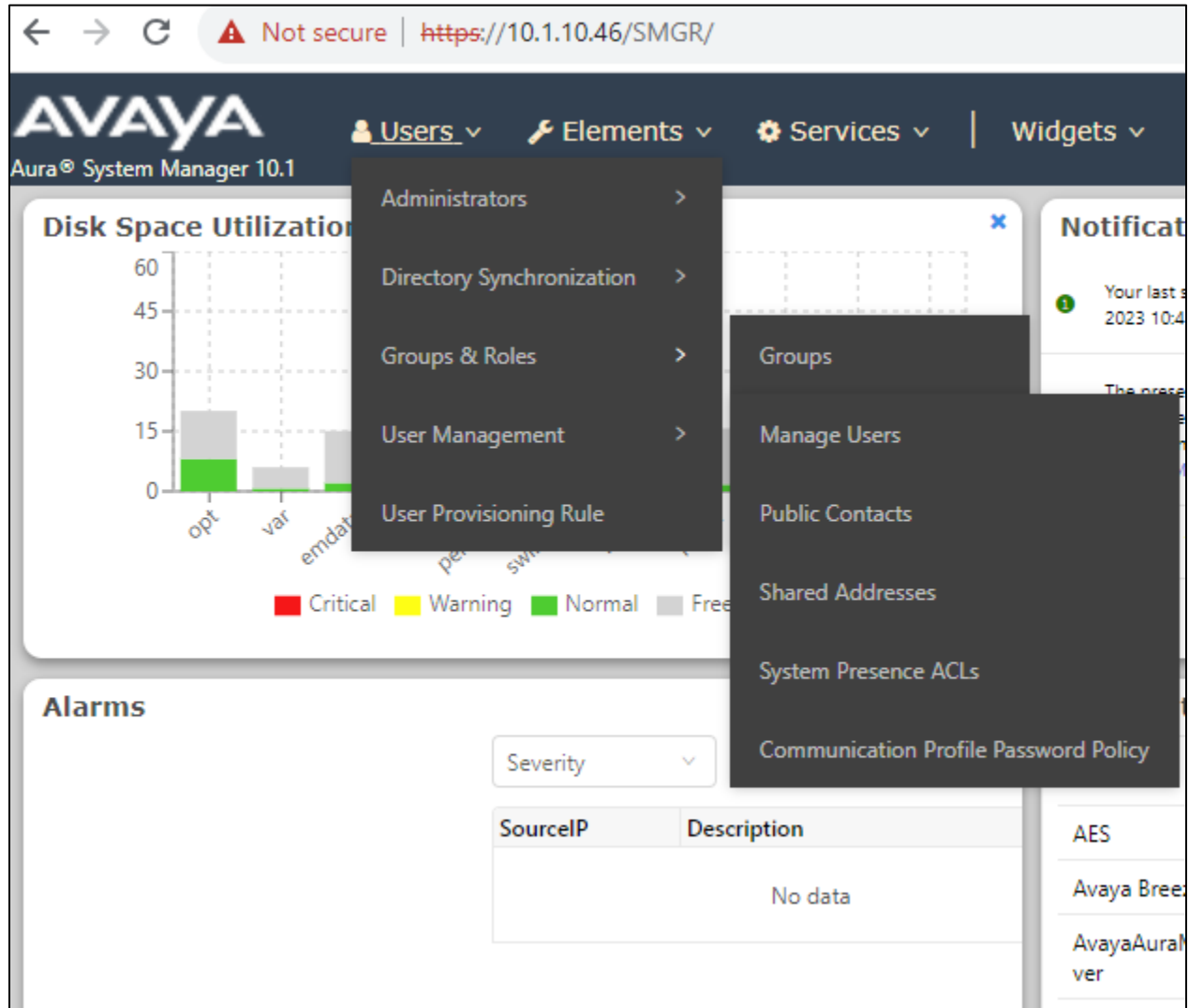
User ID:

Password:

[Change Password](#)

Supported Browsers: Firefox (minimum version 93.0), Chrome (minimum version 91.0) or Edge (minimum version 93.0).

From the home page, click on **Users** → **User Management** → **Manage Users**, as shown below.



Select the station to be edited and click on **Edit**.

	First Name	Surname	Display Name	Login Name	SIP Handle
<input type="checkbox"/>	devconnect	Avaya	Avaya, devconnect	devconnect@sglab.com	
<input type="checkbox"/>	SIP10048	AVAYA	AVAYA, SIP10048	10048@sglab.com	+10048
<input checked="" type="checkbox"/>	SIP10049	AVAYA	AVAYA, SIP10049	10049@sglab.com	+10049
<input type="checkbox"/>	SIP10050	AVAYA	AVAYA, SIP10050	10050@sglab.com	+10050
<input type="checkbox"/>	SIP10051	Avaya	AVAYA, SIP10051	10051@sglab.com	+10051
<input type="checkbox"/>	SIP10053	AVAYA	AVAYA, SIP10053	10053@sglab.com	+10053
<input type="checkbox"/>	SIP10069	AVAYA	AVAYA, SIP10069	10069@sglab.com	+10069
<input type="checkbox"/>	SIP10070	AVAYA	AVAYA, SIP10070	10070@sglab.com	+10070
<input type="checkbox"/>	SIP60049	AVAYA	AVAYA, SIP60049	60049@sglab.com	+60049
<input type="checkbox"/>	admin	admin	Default Administrator	admin	

Click on the **CM Endpoint Profile** tab in the left window. Click on **Endpoint Editor** to make changes to the SIP station.

User Profile | Edit | 10049@sglab.com

Identity | Communication Profile | Membership | Contacts

Communication Profile Password

PROFILE SET: Primary

Communication Address

PROFILES

Session Manager Profile ☒

Avaya Breze2® Profile ☐

CM Endpoint Profile ☒

OfficeInx Comm Profile ☐

IP Office Endpoint Profile ☐

Presence Profile ☒

System: DupelexCM

Use Existing Endpoints: ☐

Template: Start typing...

Security Code: Enter Security Code

Voice Mail Number: 70000

Calculate Route Pattern: ☐

SIP URI: Select

Profile Type: Endpoint

Extension: 10049

Set Type: J179CC

Port: S000138

Preferred Handle: 10049@sglab.com

Sip Trunk: aar

Enhanced Call-Info Display for 1-line phones: ☐

Override Endpoint Name and Localized Name: ☒

Delete on Unassign from User or on Delete User: ☒

Allow H.323 and SIP Endpoint Dual Registration: ☐

Under the **Feature Options** tab, ensure that **IP Softphone** is ticked, as shown below.

General Options (G) *		Feature Options (F)		Site Data (S)		Abbreviated Call Dialing (A)		Enhanced Call Fwd (E)																							
Button Assignment (B)		Profile Settings (P)		Group Membership (M)																											
Active Station Ringing	single ▼	Auto Answer	none ▼																												
MWI Served User Type	qsig-mwi ▼	Coverage After Forwarding	system ▼																												
Per Station CPN - Send Calling Number	None ▼	Display Language	english ▼																												
IP Phone Group ID		Hunt-to Station																													
Remote Soft Phone Emergency Calls	as-on-local ▼	Loss Group	19																												
LWC Reception	spe ▼	Survivable COR	internal ▼																												
AUDIX Name	None ▼	Time of Day Lock Table	None ▼																												
EC500 State	enabled ▼																														
Voice Mail Number	70000																														
Music Source		Bridging Tone for This Extension	no ▼																												
Features <table border="0"> <tr> <td><input type="checkbox"/> Always Use</td> <td><input type="checkbox"/> Idle Appearance Preference</td> </tr> <tr> <td><input type="checkbox"/> IP Audio Hairpinning</td> <td><input checked="" type="checkbox"/> IP SoftPhone</td> </tr> <tr> <td><input type="checkbox"/> Bridged Call Alerting</td> <td><input checked="" type="checkbox"/> LWC Activation</td> </tr> <tr> <td><input type="checkbox"/> Bridged Idle Line Preference</td> <td><input type="checkbox"/> CDR Privacy</td> </tr> <tr> <td><input checked="" type="checkbox"/> Coverage Message Retrieval</td> <td></td> </tr> <tr> <td><input checked="" type="checkbox"/> Direct IP-IP Audio Connections</td> <td></td> </tr> <tr> <td><input checked="" type="checkbox"/> Survivable Trunk Dest</td> <td><input type="checkbox"/> H.320 Conversion</td> </tr> <tr> <td><input type="checkbox"/> Bridged Appearance Origination Restriction</td> <td><input checked="" type="checkbox"/> IP Video Softphone</td> </tr> <tr> <td><input type="checkbox"/> Restrict Last Appearance</td> <td><input type="checkbox"/> Per Button Ring Control</td> </tr> <tr> <td><input type="checkbox"/> Turn on mute for remote off-hook attempt</td> <td></td> </tr> <tr> <td><input type="checkbox"/> IP Hoteling</td> <td></td> </tr> </table>										<input type="checkbox"/> Always Use	<input type="checkbox"/> Idle Appearance Preference	<input type="checkbox"/> IP Audio Hairpinning	<input checked="" type="checkbox"/> IP SoftPhone	<input type="checkbox"/> Bridged Call Alerting	<input checked="" type="checkbox"/> LWC Activation	<input type="checkbox"/> Bridged Idle Line Preference	<input type="checkbox"/> CDR Privacy	<input checked="" type="checkbox"/> Coverage Message Retrieval		<input checked="" type="checkbox"/> Direct IP-IP Audio Connections		<input checked="" type="checkbox"/> Survivable Trunk Dest	<input type="checkbox"/> H.320 Conversion	<input type="checkbox"/> Bridged Appearance Origination Restriction	<input checked="" type="checkbox"/> IP Video Softphone	<input type="checkbox"/> Restrict Last Appearance	<input type="checkbox"/> Per Button Ring Control	<input type="checkbox"/> Turn on mute for remote off-hook attempt		<input type="checkbox"/> IP Hoteling	
<input type="checkbox"/> Always Use	<input type="checkbox"/> Idle Appearance Preference																														
<input type="checkbox"/> IP Audio Hairpinning	<input checked="" type="checkbox"/> IP SoftPhone																														
<input type="checkbox"/> Bridged Call Alerting	<input checked="" type="checkbox"/> LWC Activation																														
<input type="checkbox"/> Bridged Idle Line Preference	<input type="checkbox"/> CDR Privacy																														
<input checked="" type="checkbox"/> Coverage Message Retrieval																															
<input checked="" type="checkbox"/> Direct IP-IP Audio Connections																															
<input checked="" type="checkbox"/> Survivable Trunk Dest	<input type="checkbox"/> H.320 Conversion																														
<input type="checkbox"/> Bridged Appearance Origination Restriction	<input checked="" type="checkbox"/> IP Video Softphone																														
<input type="checkbox"/> Restrict Last Appearance	<input type="checkbox"/> Per Button Ring Control																														
<input type="checkbox"/> Turn on mute for remote off-hook attempt																															
<input type="checkbox"/> IP Hoteling																															

*Required

Click on the **Button Assignment** tab (not shown), check that similar feature buttons except for **release** button in **Section 5.2.1** are assigned for agents using Avaya Agent for Desktop.

The screenshot shows the 'Button Assignment' tab in the Avaya system configuration. At the top, there are fields for System (DuplexCM), Extension (10049), Template (Select), Set Type (J179CC), Port (S000138), and Name (Admin). Below these are tabs for General Options (G), Feature Options (F), Site Data (S), Abbreviated Call Dialing (A), Enhanced Call Fwd (E), and Button Assignment (B). The Button Assignment tab is active, showing a table of Button Configurations. The table has columns for Button Feature, Argument-1, Argument-2, and Argument-3. The Button Feature column has a dropdown menu with options: call-appr, call-appr, call-appr, agnt-login, auto-in, manual-in, after-call, and aux-work. The Argument-1 column has a dropdown menu with options: auto-in Grp, manual-in Grp, after-call Grp, and Reason Code. The Argument-2 column has a dropdown menu with options: Hunt Grp and Reason Code. The Argument-3 column is empty. On the left side of the table, there are 'Endpoint Configurations' with a 'Favorite' checkbox and a 'Button Label' input field for each of the 8 endpoints.

Click on **Commit** once this is done to save the changes.

The screenshot shows the 'User Profile | Edit | 10049@sglab.com' page. The page has tabs for Identity, Communication Profile, Membership, and Contacts. The Communication Profile tab is active. On the left side, there are 'PROFILES' with checkboxes for Session Manager Profile, Avaya Breeze® Profile, CM Endpoint Profile (checked), OfficeInx Comm Profile, IP Office Endpoint Profile, and Presence Profile. The main area contains fields for System (DuplexCM), Profile Type (Endpoint), Extension (10049), Set Type (J179CC), Port (S000138), Preferred Handle (10049@sglab.com), Sip Trunk (aar), and SIP URI (Select). There are also checkboxes for 'Use Existing Endpoints', 'Calculate Route Pattern', 'Delete on Unassign from User or on Delete User', and 'Override Endpoint Name and Localized Name'. At the top right, there are buttons for 'Commit & Continue', 'Commit', and 'Cancel'.

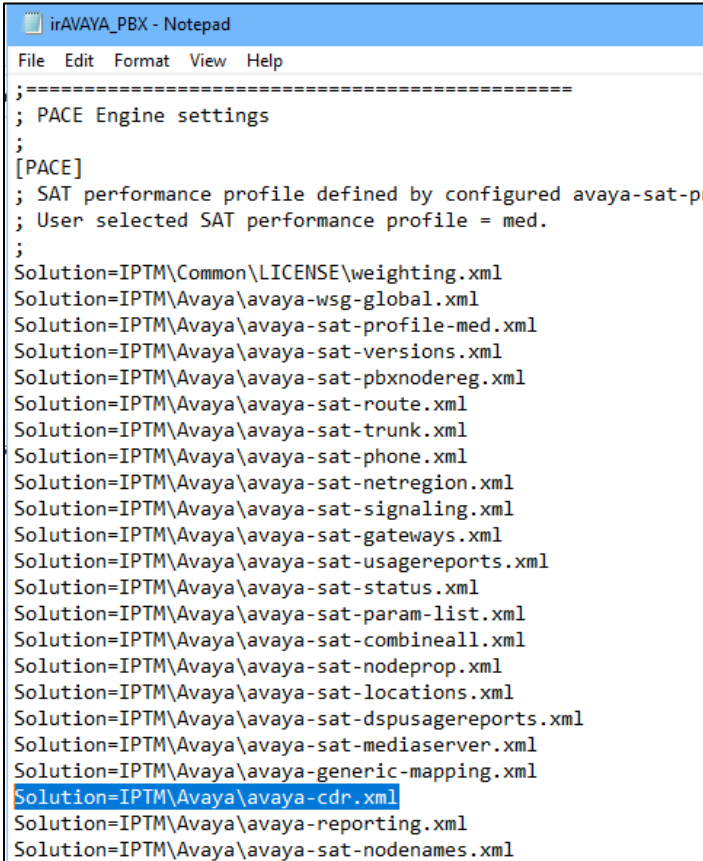
Configure Integrated Research Collaborate Prognosis Server

Configuration of Prognosis required to interoperate with Communication Manager can be referenced in [3] in **Section 9**. Additional configuration such as SAT performance profile or to disable the “list agent-loginID” SAT command can be adjusted. For details, refer to document in

7. [5] in **Section 9**.

In this compliance test, with the recommended customized CDR configured in **Section 5.1**, the *irAVAYA_PBX.ini* file in Prognosis needs to be edited. Locate the folder “..\Prognosis\Server\Configuration” in the Windows server and adjust the CDR format to comply with the format required for Collaborate.

In the *irAVAYA_PBX.ini* file, change “Solution=IPTM\Avaya\avaya-cdr.xml” below to “Solution=IPTM\Avaya\avaya-cdr-custom-mmdd.xml”.



```
irAVAYA_PBX - Notepad
File Edit Format View Help
;=====
; PACE Engine settings
;
[PACE]
; SAT performance profile defined by configured avaya-sat-pr
; User selected SAT performance profile = med.
;
Solution=IPTM\Common\LICENSE\weighting.xml
Solution=IPTM\Avaya\avaya-wsg-global.xml
Solution=IPTM\Avaya\avaya-sat-profile-med.xml
Solution=IPTM\Avaya\avaya-sat-versions.xml
Solution=IPTM\Avaya\avaya-sat-pbxnodereg.xml
Solution=IPTM\Avaya\avaya-sat-route.xml
Solution=IPTM\Avaya\avaya-sat-trunk.xml
Solution=IPTM\Avaya\avaya-sat-phone.xml
Solution=IPTM\Avaya\avaya-sat-netregion.xml
Solution=IPTM\Avaya\avaya-sat-signaling.xml
Solution=IPTM\Avaya\avaya-sat-gateways.xml
Solution=IPTM\Avaya\avaya-sat-usagereports.xml
Solution=IPTM\Avaya\avaya-sat-status.xml
Solution=IPTM\Avaya\avaya-sat-param-list.xml
Solution=IPTM\Avaya\avaya-sat-combineall.xml
Solution=IPTM\Avaya\avaya-sat-nodeprop.xml
Solution=IPTM\Avaya\avaya-sat-locations.xml
Solution=IPTM\Avaya\avaya-sat-dspusagereports.xml
Solution=IPTM\Avaya\avaya-sat-mediaserver.xml
Solution=IPTM\Avaya\avaya-generic-mapping.xml
Solution=IPTM\Avaya\avaya-cdr.xml
Solution=IPTM\Avaya\avaya-reporting.xml
Solution=IPTM\Avaya\avaya-sat-nodenames.xml
```

If a different custom CDR format is configured, then a new customized version of the *avaya-cdr.xml* file will be required, please contact Integrated Research Technical Support in this case.

Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager and Prognosis.

Verify Communication Manager

8. Verify that Prognosis has established three concurrent connections to the SAT by using the **status logins** command.

```
8.1. status logins
```

COMMUNICATION MANAGER LOGIN INFORMATION				
Login	Profile	User's Address	Active Command	Session
iptm	23	10.1.10.125		1
iptm	23	10.1.10.125		3
iptm	23	10.1.10.125		4
acpsnmp	17	127.0.0.1		5
dadmin	18	10.1.10.156		6
*dadmin	18	10.1.10.96	stat logins	7

```
Command successfully completed  
Command:
```

Using the **status cdr-link** command, verify that the **Link State** of the primary CDR link configured shows **up**.

```
status cdr-link
```

CDR LINK STATUS	
Primary	Secondary
Link State: up	CDR not admin
Date & Time: 2023/08/17 08:01:38	0000/00/00 00:00:00
Forward Seq. No: 0	0
Backward Seq. No: 0	0
CDR Buffer % Full: 0.00	0.00
Reason Code: OK	

Verify Prognosis

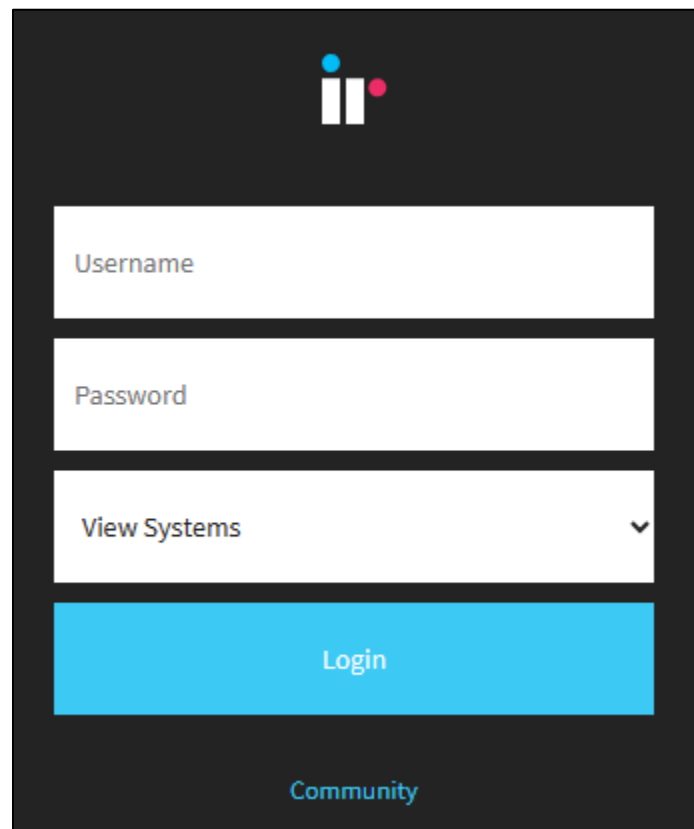
This section provides the tests that can be performed to verify proper configuration of Prognosis.

Log into the Prognosis server with administrative privileges. Launch the Prognosis

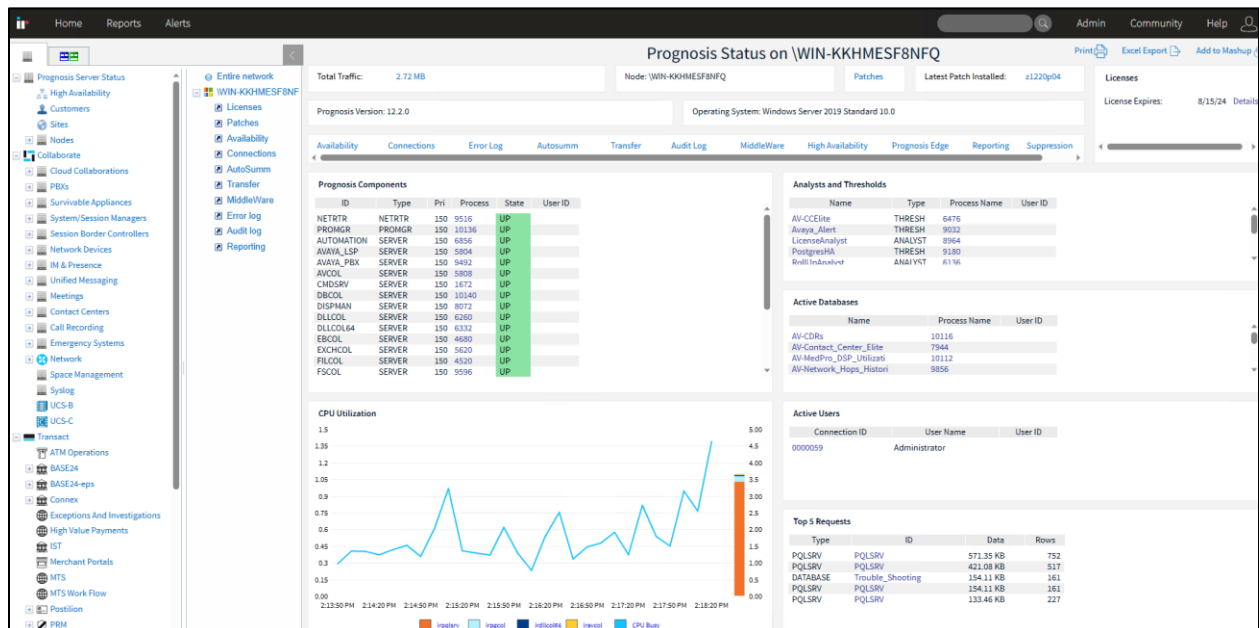
Administration by clicking **Start → All Programs → Prognosis → Prognosis View Systems**.

Login with the appropriate password. Click on the server where Prognosis is installed in the

8.2. middle panel.

The image shows a login interface for the Prognosis application. It features a dark background with a logo at the top center consisting of three vertical bars of different heights and colors (blue, white, red). Below the logo are three white input fields: 'Username', 'Password', and 'View Systems' (which includes a dropdown arrow). A large blue 'Login' button is positioned below the input fields. At the bottom of the interface, the word 'Community' is displayed in a light blue color.

The following screen is displayed. Click on the Prognosis Server in the middle pane with details on the right pane as shown below.



Go to **Collaborate** → **PBXs** from the left pane and a list of Communication Manager servers is displayed on the middle pane with details on the right pane. Select the main switch **CM10-DUPLEX** below and the status is shown on the right pane.

All PBXs

CM10-DUPLEX

ESS

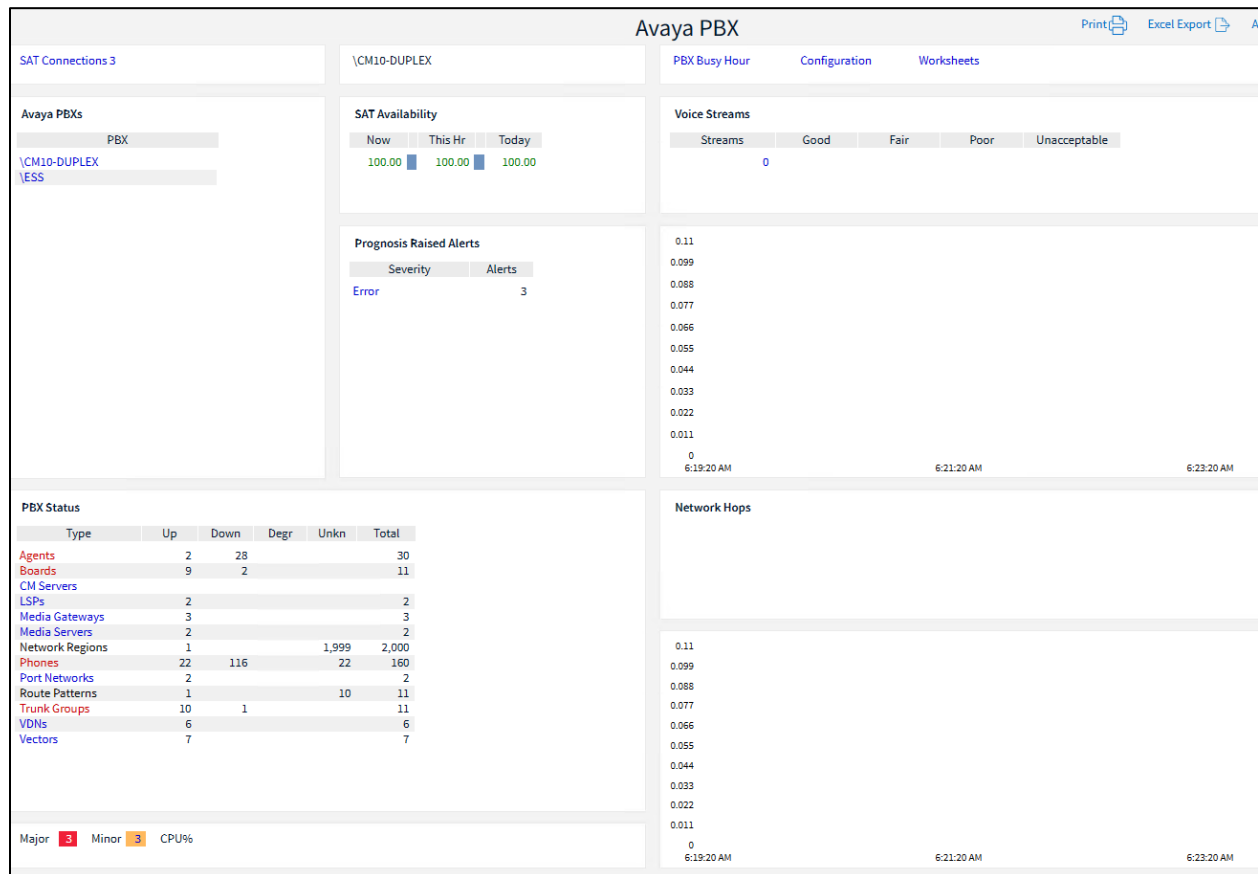
All PBXs

Entire Network

Licenses

Name	Vendor	Customer - Site	Cont	Alrts/Alrms	CPU	Endpoints	Destinations
ESS	Avaya CM ESS	Avaya - DevCon Lab	Yes	0 (Maj) 0 (Min)	1.00	10 of 160	1 of 11
CM10-DUPLEX	Avaya CM PBX	Avaya - DevCon Lab	Yes	3 (Maj) 3 (Min)	1.00	21 of 160	10 of 11

Verify that the **SAT Connections** field for each configured Communication Manager shows **3** connections. However, the number of SAT connections can be changed to 1 or 2. The instruction is found in the user guide in the software package installed.



8.2.1. Avaya Agents Screen

Click on the **Agents** in the PBX status at the bottom left area and select agent range **11xxx** on the middle pane under **Browse by Agent**. A list of agents for 11xxx range is shown on the far right pane under Agents in **Range 11xxx**.

Avaya Agents

Print

Ex

\CM10-DUPLEX

Browse by Agent

Range	Agents
11xxx	30

Agents in Range 11xxx

Login ID	Name	Extn	COR	Agent Pref	Direct Agt Skill
11001	Agent_1	10001	1		
11002	Agent_2	10049	1		
11003	Agent_3	unstaffed	1		
11004	Agent_4	unstaffed	1		
11005	Agent #5	unstaffed	1		
11006	Agent #6	unstaffed	1		
11007	Agent #7	unstaffed	1		
11008	Agent #8	unstaffed	1		
11009	Agent #9	unstaffed	1		
11010	Agent #10	unstaffed	1		
11011	Agent #11	unstaffed	1		
11012	Agent #12	unstaffed	1		
11013	Agent #13	unstaffed	1		
11014	Agent #14	unstaffed	1		
11015	Agent #15	unstaffed	1		
11201	Agent #1	unstaffed	1		

Click on **Login ID** for a login agent to see the details as shown in the sample below for **11002**:

Avaya SIP Phone Details

Print

\CM10-DUPLEX

Extension: 10049

Finished Calls

Phone Name

Type

Model

Agent 3

SIP

J179CC

Phone Port

S000138

Current

Checked

Previous

Changed

Up

8/14/23 4:11:20 AM

CoR

CoS

1

1

Active Voice Streams

Remote

Type

Local

Duration

MOS

Latency

Pkt Loss %

Jitter

View

8.2.2. Avaya VDN & Vectors Screen

Click on the **VDNs** and **Vectors** in the PBX status at the bottom left area (shown in **Section 6.2**) for further information below like VDN and Vectors relationship, status, vector steps details, vector diagrams, and historical changes as well **Vector Meta Information**. Calls information of VDN can also be viewed by clicking number under the **Calls count** link of each VDN.

\\CM10-DUPLEX

VDN Filter by Extension

0 1 2 3 4 5 6 7 8 9

VDN

Extension	Name	Vector	Status	Calls
10080	Test	1	Up	0
14000	FQ VDN	71	Up	0
14001	Normal Q	1	Up	0
14002	Priority	2	Up	0
14003	Backup Queue	3	Up	0
14004	Logistics	4	Up	0

Avaya VDNs & Vectors

Clear Filters : VDNs starting with 1


Historical

Vectors

Vector	Name	Status
1	Sales	Up
2	Priority Q	Up
3	Backup Queue	Up
4	Logistics	Up
13	DTMF check	Up
71	To SIP Gateway	Up
702	Music	Up

Vector Meta Information

Vector

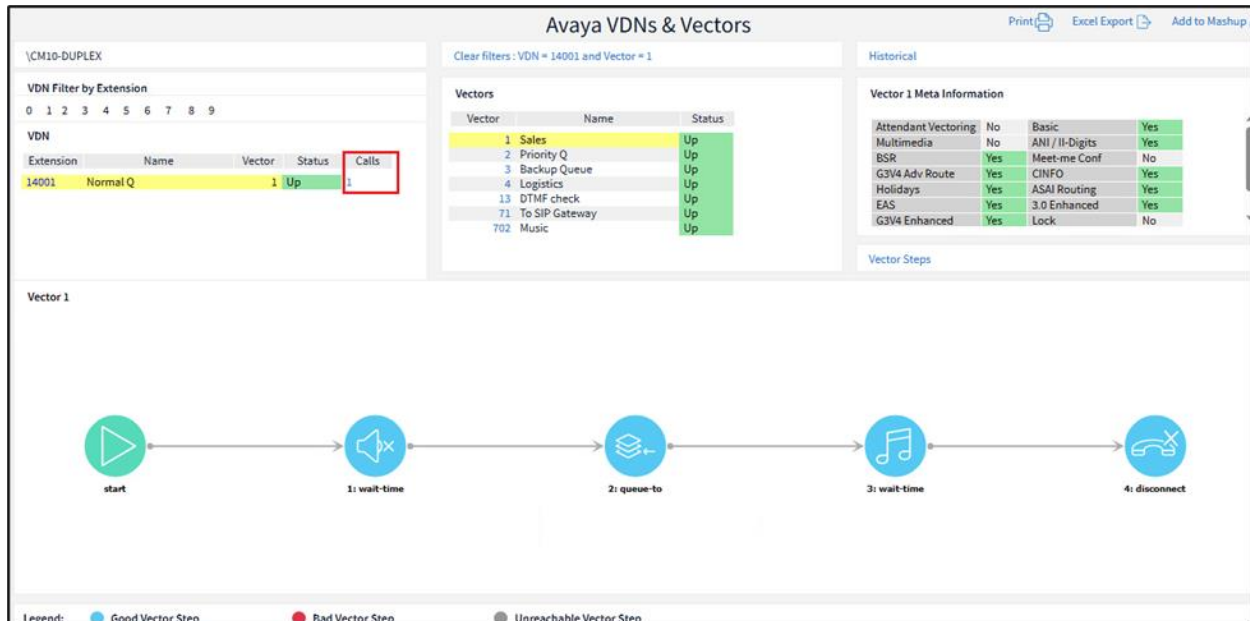


Not licensed for product ACD (Avaya Automatic Call Distribution Contact Centers)

In the first ten minutes after starting the software, while the vector steps are being collected, all the vector and VDN states will be shown as 'init'. An exception to this is when a VDN is referencing a non-existent vector, in this case a status description of 'No vector' will be shown and the item will be highlighted in red. If a VDN is created without a valid vector setup, the status state will show as 'No Vector'.

8.2.3. Avaya Calls Screen

Verify the CDR data by making inbound calls to agents on Communication Manager as well as outbound calls from agents. This can be obtained from **Calls** link as below for the last hour which shows one call.



The screenshot displays the 'Avaya VDNs & Vectors' interface. On the left, the 'VDN Filter by Extension' section shows a list of VDNs with a 'Calls' column highlighted in red. The main area shows 'Vector 1' with a flowchart of steps: start, 1: wait-time, 2: queue-to, 3: wait-time, and 4: disconnect. A legend at the bottom indicates 'Good Vector Step' (blue circle), 'Bad Vector Step' (red circle), and 'Unreachable Vector Step' (grey circle).

Extension	Name	Vector	Status	Calls
14001	Normal Q	1	Up	1

Vector	Name	Status
1	Sales	Up
2	Priority Q	Up
3	Backup Queue	Up
4	Logistics	Up
13	DTMF check	Up
71	To SIP Gateway	Up
702	Music	Up

Vector 1 Meta Information			
Attendant Vectoring	No	Basic	Yes
Multimedia	No	ANI / II-Digits	Yes
BSR	Yes	Meet-me Conf	No
G3V4 Adv Route	Yes	CINFO	Yes
Holidays	Yes	ASAI Routing	Yes
EAS	Yes	3.0 Enhanced	Yes
G3V4 Enhanced	Yes	Lock	No

A sample of captured inbound and outbound calls record for VDN 14001 were also shown below using the database slider on top right corner.

Avaya Calls														
CM10-DUPLEX														
Historical call data in selected hour														
Avaya CM	Calling Number	Dialed Number	Call Type	Duration	Condition Code	Call Start	Call End	In Trnk Group	In Trnk Member	Out Trnk Group	Out Trnk Member	VDN	Vect ID	Calling Agent
CM10-DUPLEX 33111311	11002	IB	15	9 - Incoming or Tandem Calls	Thu 8/24/23 4:53:25 PM	Thu 8/24/23 4:53:40 PM		1	0	14001	1			
CM10-DUPLEX 33111311	11001	IB	20	9 - Incoming or Tandem Calls	Thu 8/24/23 4:23:28 PM	Thu 8/24/23 4:23:48 PM		1	0	14001	1			
CM10-DUPLEX 33111311	11001	IB	8	9 - Incoming or Tandem Calls	Thu 8/24/23 4:22:51 PM	Thu 8/24/23 4:22:59 PM		1	0	14001	1			
CM10-DUPLEX 33111311	11001	IB	10	9 - Incoming or Tandem Calls	Thu 8/24/23 4:21:38 PM	Thu 8/24/23 4:21:48 PM		1	0	14001	1			
CM10-DUPLEX 11002	33111311	OB	24	7 - AAR/ARS Feature call	Thu 8/24/23 4:11:00 PM	Thu 8/24/23 4:11:24 PM		0	1					
CM10-DUPLEX 11001	33111311	OB	14	7 - AAR/ARS Feature call	Thu 8/24/23 4:08:43 PM	Thu 8/24/23 4:08:57 PM		0	1					

For inbound calls, verify a particular Agent CDR by clicking the CDR links in Agent Details screen. Below shows a record of inbound calls received by agent.

Avaya Agent Details 11001

\CM10-DUPLEX			Agent LoginID: 11001		CDRs
Name	TN	Cov Path	AAS?	AUDIX?	LWC Reception
Agent_1			n	n	spe
Auto Answer: none MIA Across Skills: system ACW Agent Considered Idle: system Aux Work Reason Code Type: system Logout Reason Code Type: system Maximum time Agent in ACW before logout (sec): system Forced Agent Logout Time:			Direct Agent Skill Call Handling Preference: skill-level Service Objective?: n Local Call Preference?: n		
Skill Number - Reserve Level - Skill Level					
Skill Number	Reserve Level	Skill Level			
1		1			


Avaya Calls for Agent 11001

[Print](#) [Excel Export](#)

From: 2023-08-30T11:00:00+08:00 (Wed)
 To: 2023-08-30T12:00:00+08:00 (Wed)

Historical call data in selected hour

Avaya CM	Calling Number	Dialed Number	Call Type	Duration	Condition Code	Call Start	Call End	In Trnk Group	In Trnk Member	Out Trnk Group	Out Trnk Member	VDN	Vect ID	Calling Agent	Dialed Agent
\CM10-DUPLEX	33111311	10004	IB	17	9 - Incoming or Tandem Calls	Wed 8/30/23 11:19:56 AM	Wed 8/30/23 11:20:13 AM		1		0	14001	1	11001	

Call Types


Inbound (1)

Inbound Trunk Calls

Outbound Trunk Calls

Conclusion

These Application Notes describe the procedures for configuring Integrated Research's Collaborate - Prognosis Server R12.2 to interoperate with Avaya Aura® Communication Manager with Call Center Elite R10.1. Compliance test was successfully completed with observations noted in **Section 2.2**.

9.

Additional References

The following Avaya documentations can be obtained on the <http://support.avaya.com>.

10.

1. *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 10.1, Issue 1, Feb 2022.
2. *Administering Avaya Aura® Communication Manager*, Release 10.1.x, Issue 1, Dec 2021.
3. *Application Notes for Integrated Research's Collaborate - Prognosis Server R12.1 with Avaya Aura® Communication Manager R10.1*.

Prognosis documentation can be obtained from links below:

4. [*Deployment and Installation Guide PROGNOSIS 12.2*](#).
5. [*Prognosis for Unified Communication Avaya Aura Call Center Elite User Guide PROGNOSIS 12.2*](#).

©2023 Avaya LLC. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya LLC. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya LLC. 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.