



Avaya Solution & Interoperability Test Lab

Application Notes for Integrated Research's Collaborate - Prognosis Server 12.1 with Avaya Session Border Controller for Enterprise R10.1 - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Collaborate - Prognosis Server R12.1 to interoperate with Avaya Session Border Controller for Enterprise (SBCE) R10.1.

Prognosis 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. Prognosis monitors directly to SBCE using SNMP connection. At the same time, Prognosis processes Real-time Transport Control Protocol (RTCP) from SBCE. Syslog is also used to collect data sent from Avaya SBCE for troubleshooting purpose.

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

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

1. Introduction

These Application Notes describe the compliance tested configuration used to validate Collaborate - Prognosis Server R12.1 (herein after referred to as Prognosis) with Avaya Session Border Controller for Enterprise (SBCE) R10.1.

Prognosis uses Simple Network Management Protocol (SNMP) to monitor SBCE server configuration, availability, utilization and alerts. In addition, SNMP also provides the SIP messages statistics like active call count and registration as well as count of certain SIP messages. Prognosis also uses Real Time Transport Control Protocol (RTCP) for voice streams display. Syslog is also used to collect data sent from Avaya SBCE for troubleshooting purpose.

2. General Test Approach and Test Results

The general test approach was to verify Prognosis using SNMP connection to monitor and display system status from SBCE. This included configuration, availability, utilization and alerts. For the collection of RTCP information, calls were made which include inbound and outbound PSTN 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.

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 the Prognosis did not include use of any specific encryption features as requested by Integrated Research.

2.1. Interoperability Compliance Testing

The feature test of the interoperability compliance testing was to verify Prognosis using web interface to display correct information of SBCE.

Verify that the server statistics information for the SBCE is populated on Prognosis display: SBCE IP Configuration, Prognosis Raised Alerts, Incidences, Call and Registrations, SIP Messages, Voice Streams and Network Hops. For collection of RTCP information, calls were made that include inbound and outbound trunk calls.

For serviceability testing, reboots were applied to Prognosis to simulate system unavailability. Loss of network connections by Prognosis and SBCE were also performed during testing.

2.2. Test Results

All test cases were passed and met the requirements as shown in **Section 2.1** with following observation:

- RADIUS is currently not supported.
- SBC – Performance data is not currently used in Prognosis for SBCE.
- Patch sbce-10.1.0.0-32-21432 is needed to resolve a syslog related issue.

2.3. Support

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

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

3. Reference Configuration

Figure 1 illustrates the test configuration used to verify the Prognosis application with Avaya Aura® Application Enablement Services. The configuration consists of a duplex Avaya Aura® Communication Manager with an Avaya G430 Media Gateway, and Avaya Aura® Media Server. Avaya SIP and H.323 endpoints were configured for making and receiving calls. Avaya Aura® Session Managers were configured via Avaya Aura® System Manager to provide SIP Deskphones. Avaya Session Border Controller for Enterprise was used to complete a SIP trunk connection to simulate a PSTN connection to the Enterprise solution. Prognosis was installed on Microsoft Windows Server 2019. Both the Monitoring Node and Web Application software were installed on this server.

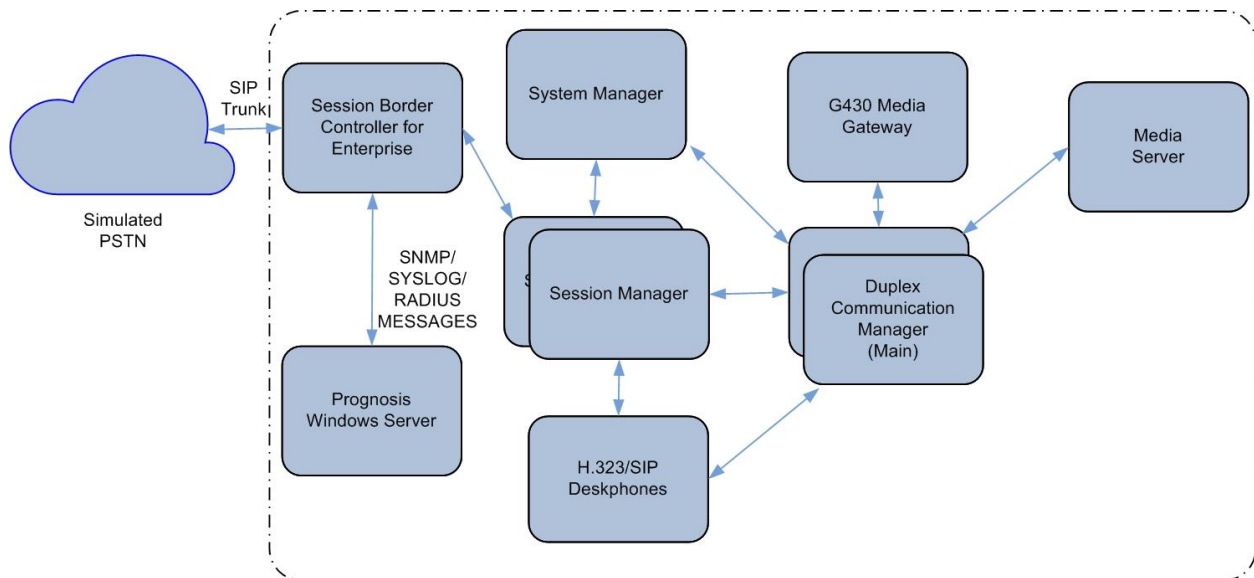


Figure 1: Test Configuration Diagram

4. Equipment and Software Validated

The following equipment and software were used for the compliance test provided:

Equipment/Software	Release/Version
Avaya Session Border Controller for Enterprise	10.1 (10.1.0.0-32-21432)
Avaya Aura® Communication Manager	10.1 (10.1.0.0.0.974.27293)
Avaya Aura® Media Server	10.1.0.77
Avaya G430 Media Gateway - MGP	42.4.0
Avaya Aura® System Manager	10.1 Build No. - 10.1.0.0.537353 Software Update Revision No: 10.1.0.0.0614119
Avaya Aura® Session Manager	10.1 (10.1.0.0.1010019)
J100 Series IP Telephones - J179 - J129	4.0.11.0 (SIP)
96x1 Series IP Telephones - 9641G - 9611G	9.8511 (H.323)
Collaborate – Prognosis Server running on Microsoft Windows Server 2019	12.1

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

5. Configure Avaya Aura® Communication Manager

The configuration of Communication Manager and SBCE is assumed to be in place and will not be discussed in this document. For more information of how to configure Communication Manager and SBCE, please refer to **Section 11**.

6. Configure Avaya Aura® Session Manager

The configuration of Session Manager is assumed to be in place and will not be discussed in this document. For more information of how to configure Session Manager, please refer to **Section 11**.

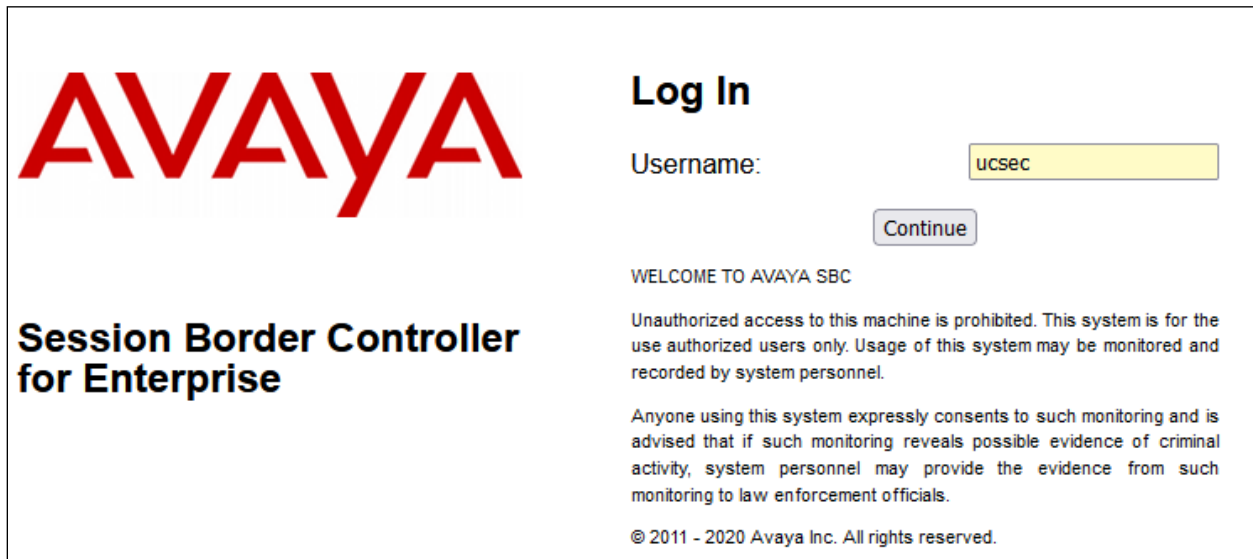
7. Configure Avaya Session Border Controller for Enterprise

The initial administration of SBCE and the connection to Session Manager, and Service Provider (simulated) is assumed to be in place and will not be covered here. This section covers the SBCE configuration of SYSLOG, SNMP and RTCP monitoring that is required for the purpose of administering Prognosis.

7.1. Configure SNMP

SNMP is used not only to capture the availability of the server but also include configuration, utilization and alerts. SNMP information also included statistics like SIP call counts and messages. All configurations are done via Avaya SBCE web interface.

Using a web browser, enter `https://<IP address of Avaya SBCE/sbc>` to connect to the Avaya SBCE server and log in using appropriate credentials as shown below.



The login page features the Avaya logo on the left and a 'Log In' section on the right. The 'Log In' section includes a 'Username:' label, a text input field containing 'ucsec', and a 'Continue' button. Below the login fields, there is a 'WELCOME TO AVAYA SBC' message, a disclaimer about unauthorized access, a consent statement, and a copyright notice: '© 2011 - 2020 Avaya Inc. All rights reserved.'

AVAYA

Log In

Username:

Session Border Controller for Enterprise

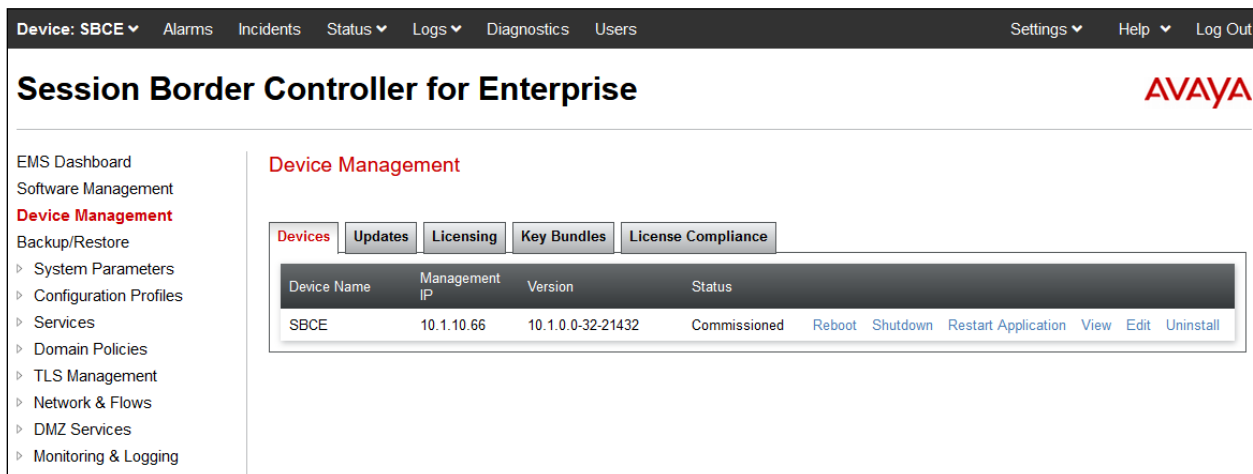
WELCOME TO AVAYA SBC

Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel.

Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials.

© 2011 - 2020 Avaya Inc. All rights reserved.

Once logged in, a dashboard is presented with a menu on the left-hand side for EMS (not shown). Select "SBCE" under **Device** from the left top drop-down options for SBCE configuration as shown below.



The dashboard has a top navigation bar with 'Device: SBCE' selected, and links for Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header reads 'Session Border Controller for Enterprise' with the Avaya logo. A left-hand menu lists various management options, with 'Device Management' highlighted. The main content area is titled 'Device Management' and contains tabs for Devices, Updates, Licensing, Key Bundles, and License Compliance. The 'Devices' tab is active, showing a table with one device entry.

Device: SBCE Alarms Incidents Status Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise **AVAYA**

EMS Dashboard
Software Management
Device Management
Backup/Restore
‣ System Parameters
‣ Configuration Profiles
‣ Services
‣ Domain Policies
‣ TLS Management
‣ Network & Flows
‣ DMZ Services
‣ Monitoring & Logging

Device Management

Devices Updates Licensing Key Bundles License Compliance

Device Name	Management IP	Version	Status	
SBCE	10.1.10.66	10.1.0.0-32-21432	Commissioned	Reboot Shutdown Restart Application View Edit Uninstall

Navigate to **Backup/Restore** → **Monitoring & Logging** → **SNMP** from the dashboard.

Session Border Controller for Enterprise

[EMS Dashboard](#)
[Software Management](#)
Device Management
[Backup/Restore](#)
‣ [System Parameters](#)
‣ [Configuration Profiles](#)
‣ [Services](#)
‣ [Domain Policies](#)
‣ [TLS Management](#)
‣ [Network & Flows](#)
‣ [DMZ Services](#)
‣ [Monitoring & Logging](#)
 SNMP

Device Management

Devices | Updates | Licensing | Key Bundles | License Compliance

Device Name	Management IP	Version	Status
SBCE	10.1.10.66	10.1.0.0-32-21432	Commissioned Reboot

The **SNMP** page is seen as shown below. Select **SNMP v3** tab. Click on the **Add** button.

Session Border Controller for Enterprise

[EMS Dashboard](#)
[Software Management](#)
[Device Management](#)
[Backup/Restore](#)
‣ [System Parameters](#)
‣ [Configuration Profiles](#)
‣ [Services](#)
‣ [Domain Policies](#)
‣ [TLS Management](#)
‣ [Network & Flows](#)
‣ [DMZ Services](#)
‣ [Monitoring & Logging](#)
 SNMP

SNMP: SBCE

SNMP v3 | Management Servers | Trap Severity Settings

User Name	Auth Schema	Auth Protocol	Priv Protocol	Privilege	Traps
-----------	-------------	---------------	---------------	-----------	-------

Add

In the **Add User** window shown below, configure the following.

- **User Name:** A descriptive name.
- **Authentication Scheme:** Select the radio button for **authPriv**.
- Enter a password for **AuthPassPhrase** and confirm in **Confirm AuthPassPhrase**.
- **Authentication Protocol:** Select the radio button for **SHA**.
- Enter a password for **PrivPassPhrase** and confirm in **Confirm PrivPassPhrase**.
- **Privacy Protocol:** Select **AES** radio button.
- **Privilege:** Select **Read** radio button.
- **Trap IP Address:** Enter the IP Address of the Prognosis Server.
- **Port:** Enter **162**.

Retain default values for all other fields and click on the **Finish** button.

The screenshot shows the 'Add User' window with the following configuration:

Field	Value
User Name	Prognosis
Authentication Scheme	<input type="radio"/> noAuthNoPriv <input type="radio"/> authNoPriv <input checked="" type="radio"/> authPriv
AuthPassPhrase	
Confirm AuthPassPhrase	
Authentication Protocol	<input checked="" type="radio"/> SHA
PrivPassPhrase	
Confirm PrivPassPhrase	
Privacy Protocol	<input checked="" type="radio"/> AES <input type="radio"/> DES
Privilege	<input checked="" type="radio"/> Read <input type="radio"/> Read/Write
Trap IP Address	10.1.10.125
Port	162
Trap Profile	default

Buttons: Add, Delete, Finish

Screen below shows the SNMP v3 configured for SBCE device. Select the **Management Servers** tab and click on the **Add** button.

SNMP: SBCE

SNMP v3 Management Servers Trap Severity Settings Add

User Name	Auth Schema	Auth Protocol	Priv Protocol	Privilege	Traps	
Prognosis	authPriv	SHA	AES	READ	10.1.10.125:162 [default]	Clone Edit Delete

In the **Add IP Address** window shown below, configure the Prognosis server IP Address and click the **Finish** button.

Add IP Address X

IP Address(es)
Separate entries with commas

10.1.10.125

Finish

Screen below shows the Management Servers configured for **SBCE** device

SNMP: SBCE

SNMP v3 Management Servers Trap Severity Settings Add

IP Address	
10.1.10.125	Clone Edit Delete

7.2. Configure RTCP Monitoring feature

To setup RTCP Monitoring, under **Device: SBCE** navigate to **Backup/Restore → Network & Flows → Advance Options**. Select the **RTCP Monitoring** tab and configure the following:

- Tick **Enabled** the **RTCP Monitoring Relay**.
- **Node Type:** **Core** since only one SBCE is setup.
- **Relay IP:** Select the internal interface as relay IP.
- **Port:** Enter **5005**.
- Tick **Enabled** the **RTCP Monitoring Report Generation**.
- **SBCE Interface IP:** Select the external interface as IP for public trunk. This feature is only for public SIP trunk with Avaya SBCE receiving RTCP streams without having specific control. Avaya SBCE converts the RTCP streams into Avaya specific format before sending it to the monitoring server.
- **SBCE Interface Port:** Enter **5005**.
- **Monitoring server IP/FQDN and Port:** Enter Prognosis server IP address and port **5005**.

Advanced Options

Periodic StatisticsFeature ControlSIP OptionsNetwork OptionsPort Ranges**RTCP Monitoring**Load Monitoring

Configuration update successful.

Changes to the settings below take effect immediately and will impact sessions that are using them. It is recommended to change these values only during a maintenance window.

RTCP Monitoring Configuration

RTCP Monitoring Relay	<input checked="" type="checkbox"/> Enabled
Node Type	Core
Relay IP	Internal A1 (A1, VLAN 0) 10.1.10.65
Port	5005
RTCP Monitoring Report Generation	<input checked="" type="checkbox"/> Enabled
SBCE Interface IP	External B1 (B1, VLAN 0) 10.1.60.65
SBCE Interface Port	5005
Monitoring server IP/FQDN and Port IP:Port	10.1.10.125 : 5005
Monitoring Frequency based on RTCP Report	2
Monitoring interval in absence of RTCP Report	10 seconds

Save

In a back-to-back Avaya SBCE deployment, two relay services need to be configured to send RTCP monitoring traffic to Prognosis server on each SBCE. This is needed for Core Avaya SBCE, DMZ Avaya SBCE and remote Avaya SBCE. In this compliance testing, only Core Avaya SBCE is setup. Refer to **Section** Error! Reference source not found. reference [6] for overview and further explanation.

To configure application relay services to send the RTCP monitoring traffic to Prognosis, under **Device: SBCE**, navigate to **Backup/Restore → DMZ Services → Relay**. Click **Add**.

Configure the following. A screen shot is shown on the next page.

- **Name:** Enter descriptive name.
- **Service Type:** **RTCP**.
- **Remote IP/FQDN:** Prognosis IP address.
- **Remote Port:** Enter **5005**.
- **Remote Transport:** Select **UDP**.
- **Listen IP:** Select internal private interface.
- **Listen Port:** Enter **5005**.
- **Connect IP:** Select another internal private interface to relay which is routable to Prognosis server.
- **Listen Transport:** Select **UDP**.
- Tick **Use Relay Actors** and select **Options** as **Hop-By-Hop Traceroute**.

Repeat the same for Relay 2 with the **Listen IP** using the external public interface.

The RTCP monitoring server i.e., the Listen IP where RTCP traffic will be received, needs to be configured on phone groups via System Manager for SIP endpoints in Session Manager, Media Server and Communication Manager. Refer to the reference [5] and [4] respectively in **Section 11**.

Edit Application Relay
X

General Configuration

Name
Relay 2

Service Type
RTCP

Remote Configuration

Remote IP/FQDN
10.1.10.125

Remote Port
5005

Remote Transport
UDP

Device Configuration

Listen IP
Internal A1 (A1, VLAN 0)
10.1.10.65

Listen Port
5005

Connect IP
External B1 (B1, VLAN 0)
10.1.60.65

Listen Transport
UDP

Additional Configuration

Whitelist Flows
☐

Use Relay Actors
☒

Options
Use Ctrl+Click to select or deselect multiple items.

RTCP Monitoring
End-to-End Rewrite
Hop-by-Hop Traceroute
Bridging

Finish

7.3. Configure SYSLOG

To setup SYSLOG, under **Device: EMS** navigate to **Backup/Restore → Monitoring & Logging → Syslog Management** and select the **Log Level** tab on the right pane. Configure the log level for the **Class**. In the following **LOG_LEVEL0** is setup for all **Class** except Audit which is not configurable and the appropriate information level.

The screenshot shows the 'Syslog Management: EMS' interface. On the left is a navigation menu with options like EMS Dashboard, Software Management, Device Management, System Administration, Templates, Backup/Restore, and Monitoring & Logging. The 'Monitoring & Logging' section is expanded, showing 'Syslog Management' and 'Log Collection'. The main area has two tabs: 'Log Level' (selected) and 'Collectors'. The 'Log Level' tab displays a table with columns for Class, Facility, and log levels (All, Info, Notice, Warning, Error, Critical, Alert, Emergency). The 'Platform' class is configured with LOG_LOCAL0 for all levels. The 'Trace' class is configured with LOG_LOCAL0 for Info, Notice, Warning, Error, Critical, Alert, and Emergency levels. The 'Security' class is configured with LOG_LOCAL0 for all levels. The 'Protocol' class is configured with LOG_LOCAL0 for all levels. The 'Incident' class is configured with LOG_LOCAL0 for all levels. The 'Audit' class is configured with LOG_LOCAL6 for all levels. A 'Save' button is at the bottom right of the table.

Class	Facility	All	Info	Notice	Warning	Error	Critical	Alert	Emergency
Platform	LOG_LOCAL0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Trace	LOG_LOCAL0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Security	LOG_LOCAL0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Protocol	LOG_LOCAL0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Incident	LOG_LOCAL0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Audit	LOG_LOCAL6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Next, click the **Collectors** tab. Click on **Edit** on any of the LOG_LOCALx entry except 5 and 6. In this compliance testing, **LOG_LOCAL0** was picked above and configured below for external SYSLOG server such as Prognosis.

In the **Edit Collector** window shown below, configure the following.

- **Collector Type:** Select the **Remote Syslog** radio button.
- **Protocol:** Select **UDP**.
- **Address:** Select the **(ip:port)** radio button and enter the IP Address of Prognosis and the port as **514**.

The screenshot shows the 'Edit Collector' window. At the top, a message states 'LOG_LOCAL5 and LOG_LOCAL6 are reserved for audit logging.' Below this, the 'Collector Settings' section shows 'Facility' set to 'LOG_LOCAL0'. The 'Collector Type' section has two radio buttons: 'File' and 'Remote Syslog', with 'Remote Syslog' selected. The 'Remote Syslog Settings' section shows 'Protocol' with three radio buttons: 'TCP', 'UDP', and 'TLS', with 'UDP' selected. The 'TLS Profile' is set to 'None'. The 'Address' section has two radio buttons: 'EMS' and '(ip:port)', with '(ip:port)' selected and the value '10.1.10.125:514' entered in the adjacent text field. A 'Finish' button is at the bottom.

The screen below shows the configured result. Repeat the above under **Device: SBCE**. Note that SYSLOG messages is only sent from SBCE via the Management IP Address and not through the other interfaces.

Syslog Management: EMS

Log Level

Collectors

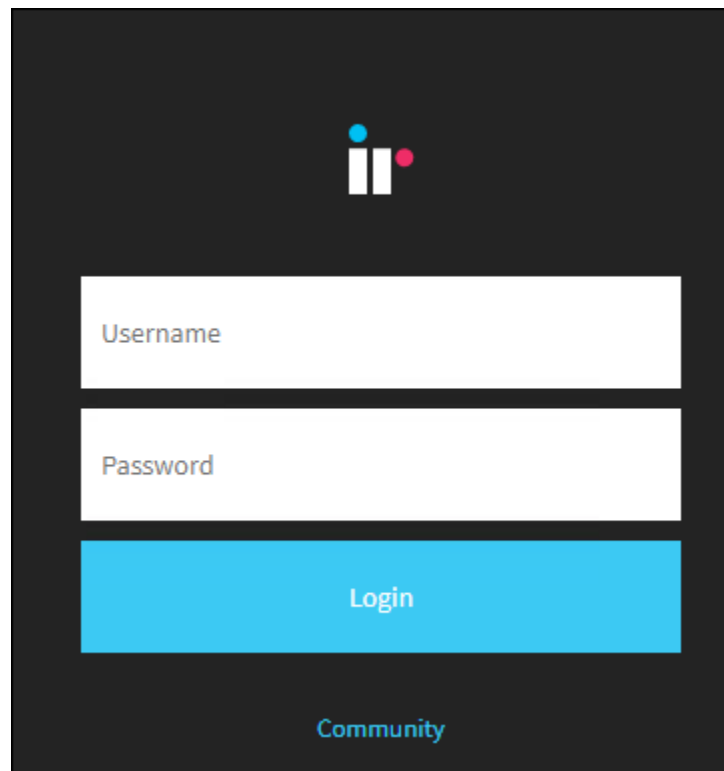
Add

Facility	Destination Location	
LOG_LOCAL1	/archive/syslog/pcs/pcs.log	<a>Edit <a>Delete
LOG_LOCAL2	/archive/syslog/pcs/pcs.log	<a>Edit <a>Delete
LOG_LOCAL3	/archive/syslog/pcs/pcs.log	<a>Edit <a>Delete
LOG_LOCAL4	/archive/syslog/pcs/pcs.log	<a>Edit <a>Delete
LOG_LOCAL5	/archive/syslog/pcs/slic.log	<a>Edit
LOG_LOCAL6	/archive/syslog/pcs/audit.log	<a>Edit
LOG_LOCAL7	/archive/syslog/pcs/pcs.log	<a>Edit <a>Delete
LOG_DAEMON	/archive/syslog/pcs/pcs.log	<a>Edit <a>Delete
LOG_LOCAL0	UDP:10.1.10.125:514	<a>Edit <a>Delete

8. Configure Prognosis

This section describes the configuration of Prognosis required to interoperate with SBCE. Initial setup and installation will be done by Integrated Research and will not be detailed here. Below is the configuration for information purposes only.

Log in to the Prognosis with administrative privileges. Launch the Prognosis Administration by clicking **Start → All Programs → Prognosis → Administration** and log in with the appropriate password.

The image shows a login interface for the Prognosis application. It features a dark gray background. At the top center is a logo consisting of three vertical bars of increasing height, with a blue dot above the first bar and a red dot above the third bar. Below the logo are two white rectangular input fields. The first field is labeled "Username" in a light gray font. The second field is labeled "Password" in a light gray font. Below these fields is a large, solid blue rectangular button with the word "Login" in white text. At the bottom center of the interface is a link labeled "Community" in a light blue font.

The **Prognosis Administration** homepage is displayed as shown below. Click **Add System**.

The screenshot shows the Prognosis Administration interface. The left sidebar has a 'Home' link highlighted. The main content area displays the 'Prognosis node - WIN-KKHMESF8NFQ' details. The 'Add System' button in the 'UC & Infrastructure Configuration' section is highlighted with a red box. Below this, the 'Databases' section lists several databases with 'Stop' buttons next to them.

Database	Status
AV-CDRs	Stop
AV-Contact Center Elite	Stop
AV-MedPro DSP Utilization	Stop
AV-Network Hops Historical	Stop
AV-Reporting	Stop

Scroll below to **Session Border Controllers**. Select **Avaya SBCE-E** from the drop-down menu. Click **Add** to add a new SBCE.

The screenshot shows the 'Session Border Controllers' section. It features a drop-down menu with 'Avaya SBC-E' selected and an 'Add' button next to it.

In this test configuration, the following entries are added for SBCE with display name of **SBCE101** and with IP addresses of **10.1.10.66**.

The following settings were used during the compliance test.

Basic Details:

- **Display Name: SBCE101**
- **IP address: 10.1.10.66**
- **Customer Name: Avaya**
- **Site Name: DevCon Lab**

SNMP Connection Details:

- Select **Use SNMP Version 3**
- Authentication Protocol: As configured in **Section 7.1**
- Authentication Password: As configured in **Section 7.1**
- Encryption Method: As configured in **Section 7.1**
- Encryption Password: As configured in **Section 7.1**

Leave the **Databases and Thresholds** as checked. Click **Add** to affect the addition (not shown).

Basic Details

Display Name: SBCE10

IP Address: * 10.1.10.66

Customer Name: Avaya

Site Name: DevCon Lab

RTCP Port: 5005

SNMP Connection Details

☐ Use SNMP Version 2c

☒ Use SNMP Version 3

User Name: * Prognosis

Authentication Protocol: SHA

Authentication Password: *

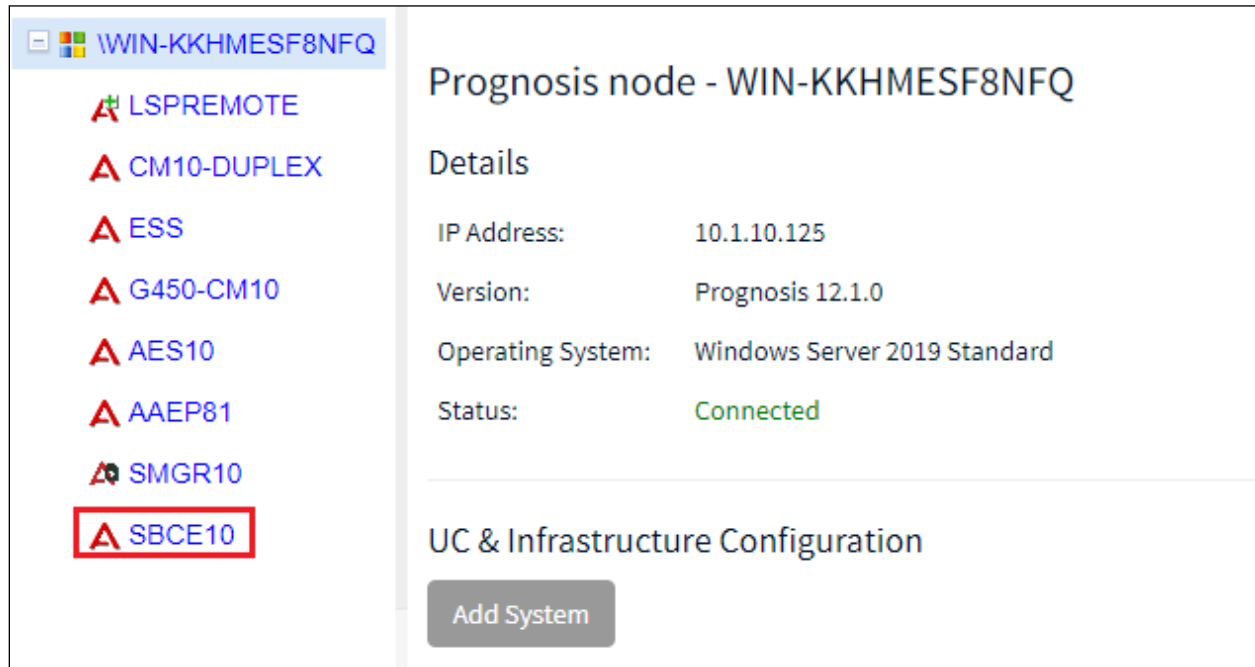
Encryption Method: AES

Encryption Password: *

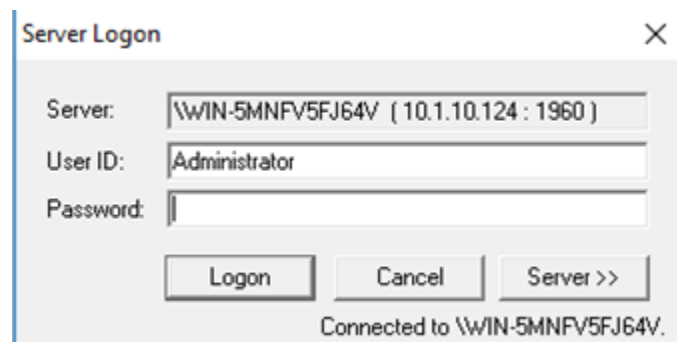
Databases and Thresholds

☒ Start standard databases and thresholds

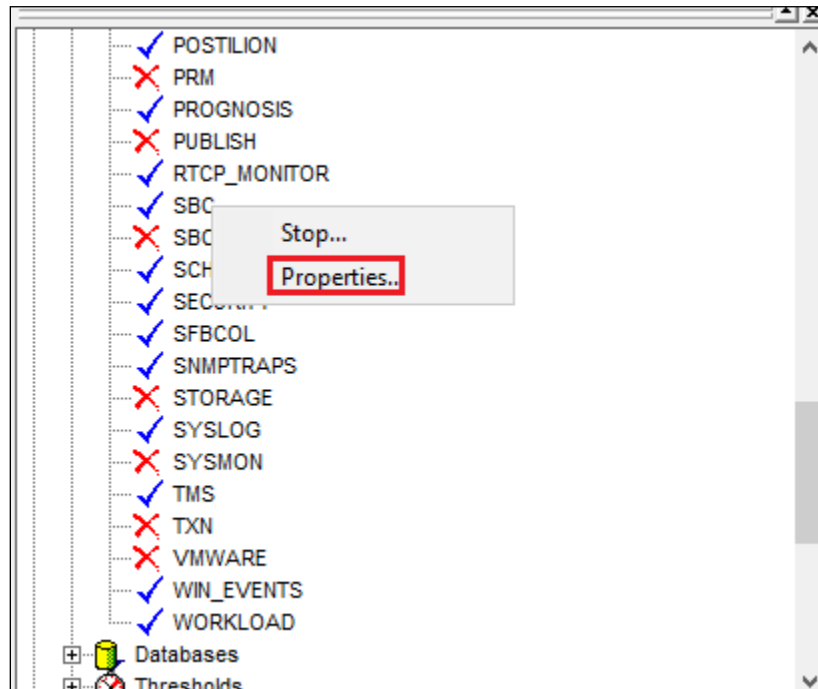
Below is the result of the addition of SBCE in the Admin home page.



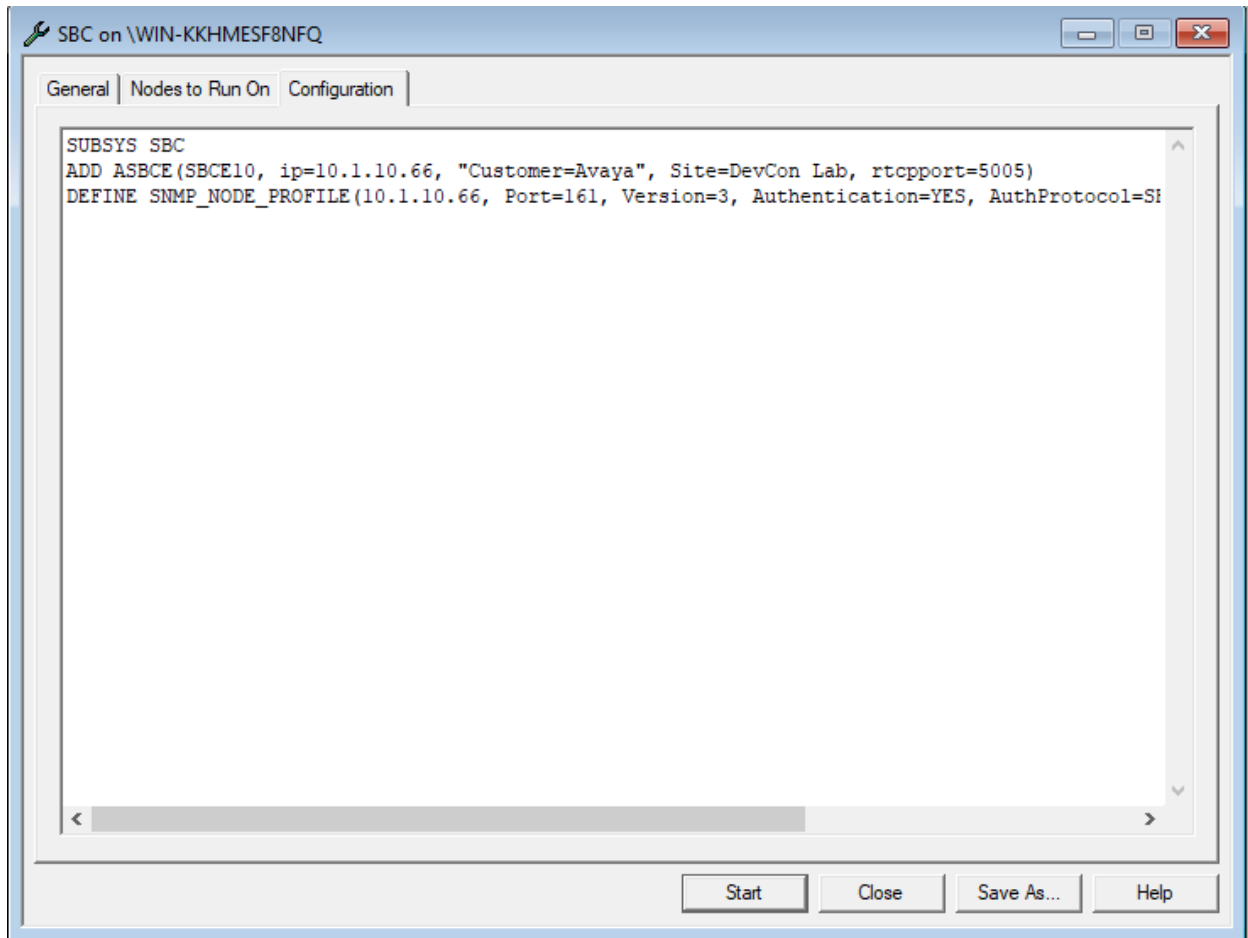
On Prognosis server, click **Start → All Programs → Prognosis → Prognosis Client** to start the Windows Client application. Log in with the appropriate credentials.



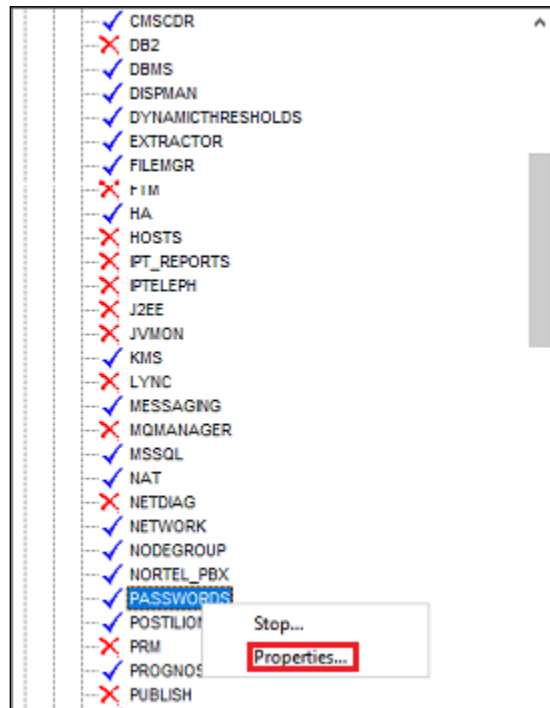
To check the configurations of the SBCE to be monitored, expand **Configurations** of the Monitoring Node on the left pane, right-click on **SBC** and select **Properties**.



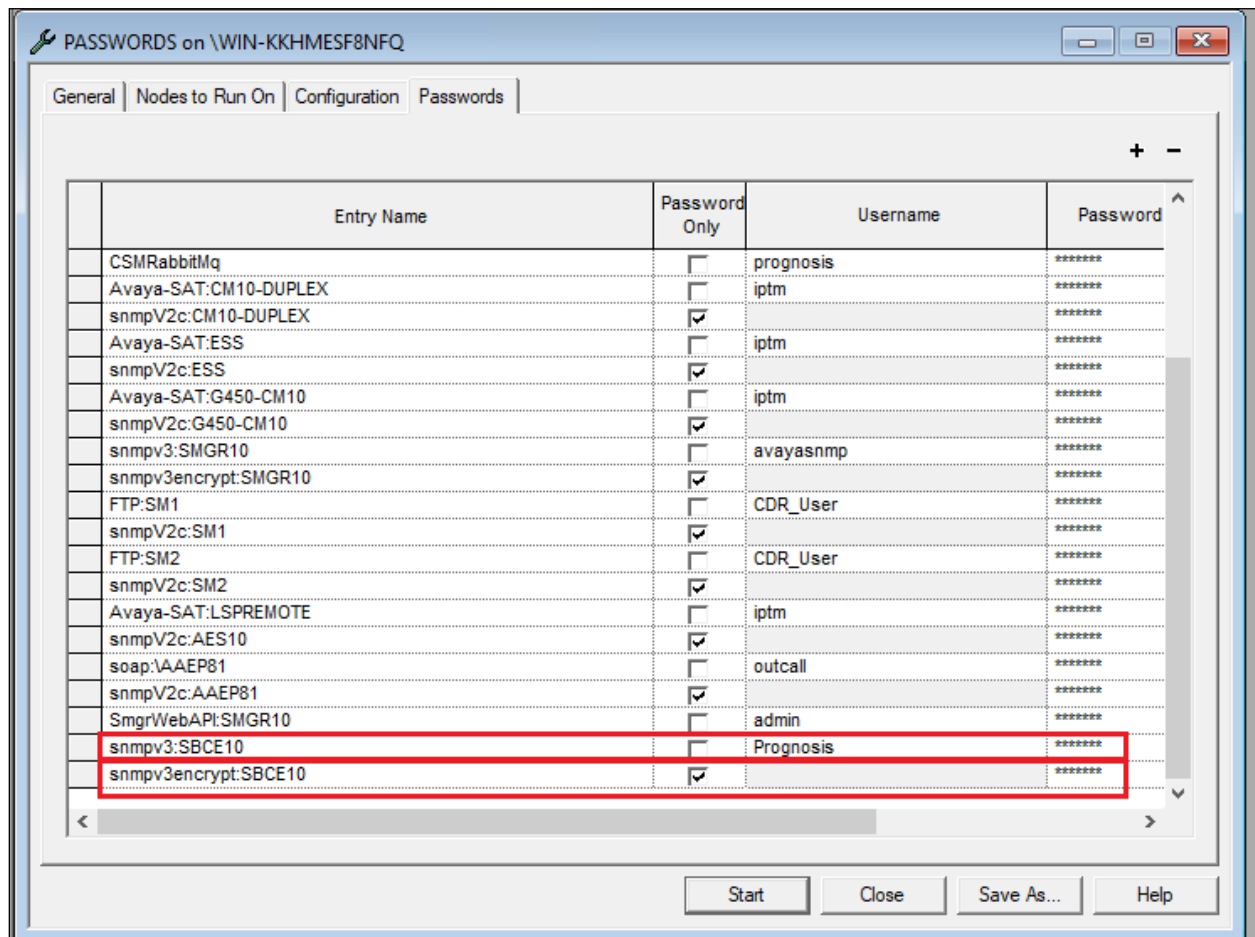
The **SBCE** entry configured earlier is displayed below:



To check the configurations of the password to be monitored, expand Configurations of the Monitoring Node on the left pane, right-click on **PASSWORDS** and select **Properties**.



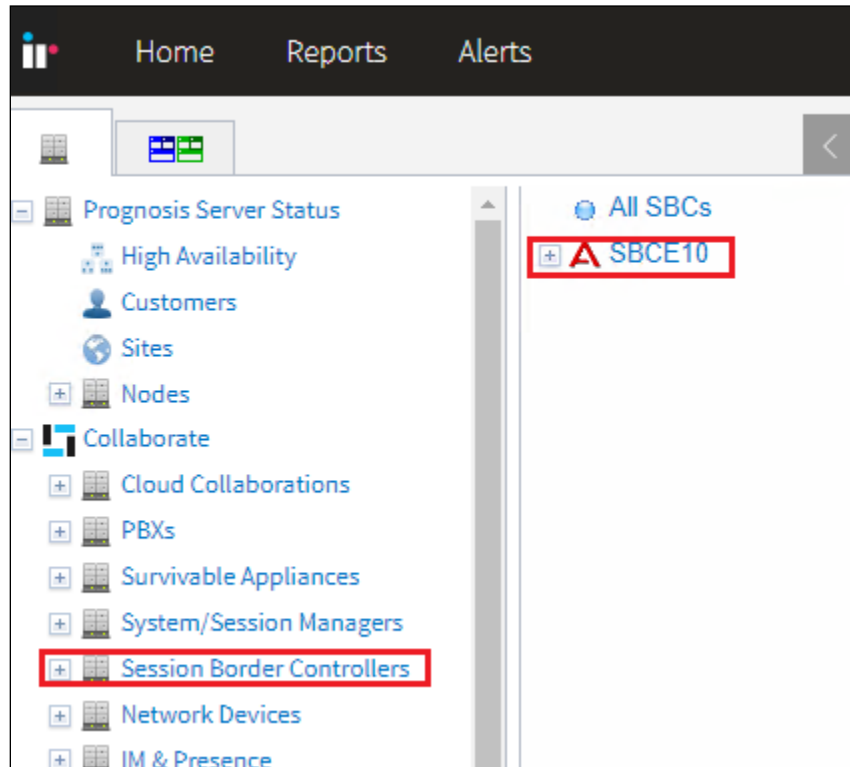
The password entries are displayed. In the compliance test, the first entry of SBCE was added **snmpv3:SBCE10** with the password (Community String) as configured in **Section 8.1**.



By default, Prognosis is listening to Syslog at UDP port 514. The Syslog DB database needs to be started which will not be detailed here.

9. Verification Steps

This section provides the tests that can be performed to verify proper configuration of SBCE and Prognosis. Log in to the Prognosis with administrative privileges. Navigate to **Collaborate** → **Session Border Controllers**. **SBCE10** is listed as one of the SBCs in the middle pane.



The right pane shows the **SBC – Welcome** screen below.

SBC - Welcome

[Print](#)
[Excel Export](#)
[Add to Mashup](#)

Connected to: WIN-KKHMF8NF
Alerts (0)
Voice Quality Central
Radius Listener Status

All Session Border Controllers

Name	IP Address	Customer	Site	Model	SBC Version	System Version	Vendor	Type	Concurrent Calls/Sessions	Redundancy State	Status	Mi
SBCE10	10.1.10.66	Avaya	DevCon Lab	AvayaSBCE			Avaya	ASBCE			Online	

Click on the **SBCE10** and below shows the details of the **SBCE IP Configuration**.

SBCE10 - IP Configuration

[Print](#)
[Excel Export](#)
[Add to Mashup](#)

Alerts (1)
Incidences (29)
Calls & Registrations
SIP Messages
Voice Streams
Network Hops

Interfaces

Index	Description	MAC Address	Status
1	lo		up
2	M1	00:50:56:A0:79:C2	up
3	M2	00:50:56:A0:38:02	down
4	A1	00:50:56:A0:9C:3E	up
5	A2	00:50:56:A0:44:F2	down
6	B1	00:50:56:A0:8F:69	up
7	B2	00:50:56:A0:CB:B6	down

IP Addresses

IP Address	Interface Index	Network Mask
10.1.10.65	4	255.255.255.0
10.1.10.66	2	255.255.255.0
10.1.60.65	6	255.255.255.0
127.0.0.1	1	255.0.0.0

Routing Table

Destination	Interface Index	Mask	Metric
0.0.0.0	2	0.0.0.0	1
10.1.10.0	2	255.255.255.0	0

ARP Table

Interface Index	IP Address	MAC Address	Type
2	10.1.10.1	00:04:96:27:A3:0A	dynamic
2	10.1.10.38	00:50:56:A0:CE:0C	dynamic
2	10.1.10.99	00:14:5E:95:5F:19	dynamic
2	10.1.10.101	00:15:C5:E1:50:2B	dynamic
2	10.1.10.124	00:50:56:A0:80:94	dynamic
2	10.1.10.125	00:50:56:A1:65:57	dynamic
2	10.1.10.154	34:17:EB:A0:89:15	dynamic
2	10.1.10.156	09:23:24:11:36:C9	dynamic
2	10.1.10.254	58:6D:8F:69:7F:14	dynamic
4	10.1.10.1	00:04:96:27:A3:0A	dynamic
4	10.1.10.12	00:50:56:A1:D5:A2	dynamic
4	10.1.10.13	00:0C:29:A1:6A:6F	dynamic
4	10.1.10.31	00:04:0D:6E:77:E0	dynamic
4	10.1.10.60	00:50:56:A1:A7:86	dynamic
4	10.1.10.101	00:15:C5:E1:50:2B	dynamic
4	10.1.10.164	84:80:17:8B:7C:12	dynamic
4	10.1.10.167	3C:B1:5B:5E:AB:26	dynamic
6	10.1.60.1	00:04:96:27:A3:0A	dynamic

Total Packets Per Interval

Verify the **Alerts** and **Incidences** on the Prognosis with the SBCE from the sub-header of the **SBCE10 IP Configuration**. Below shows the **Alerts** displayed.

All Avaya SBC-Es

SBCE10

Alerts

Calls & Registrations

SIP Messages

Voice Streams

Network Hops

Incidences

SBCE10 - Alerts

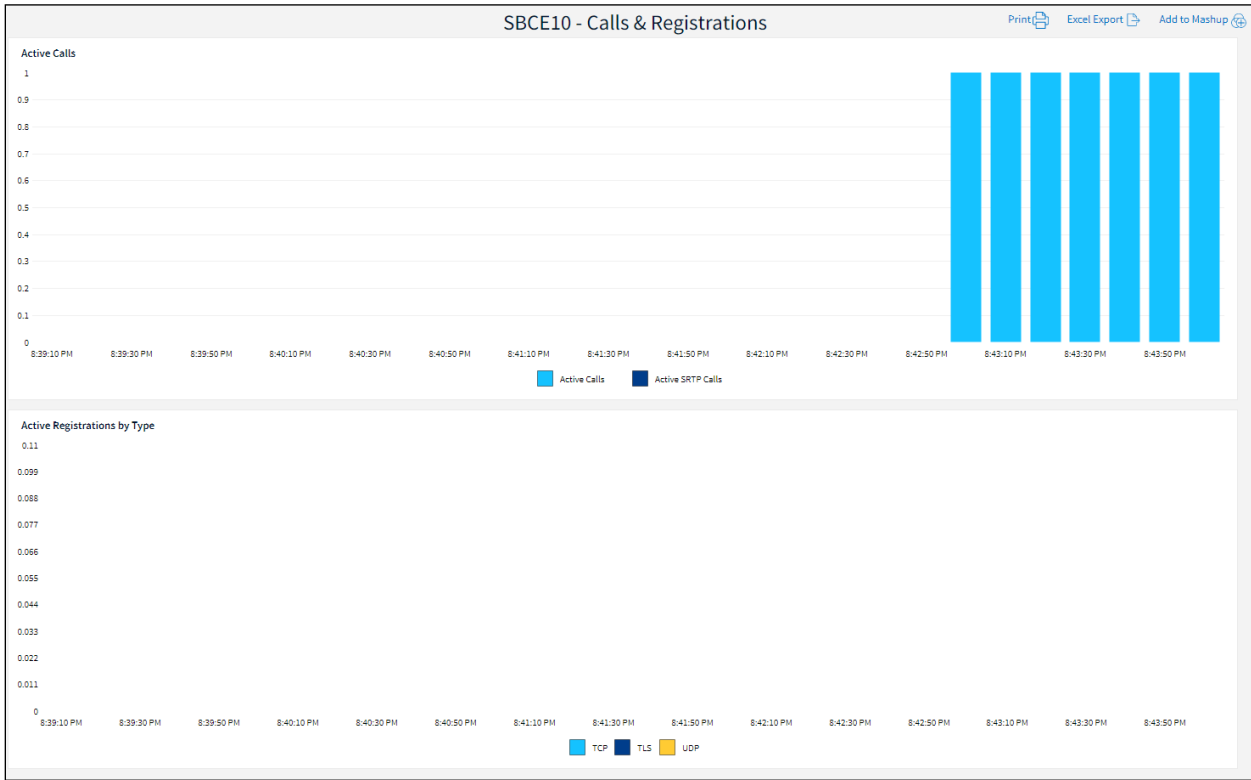
Print

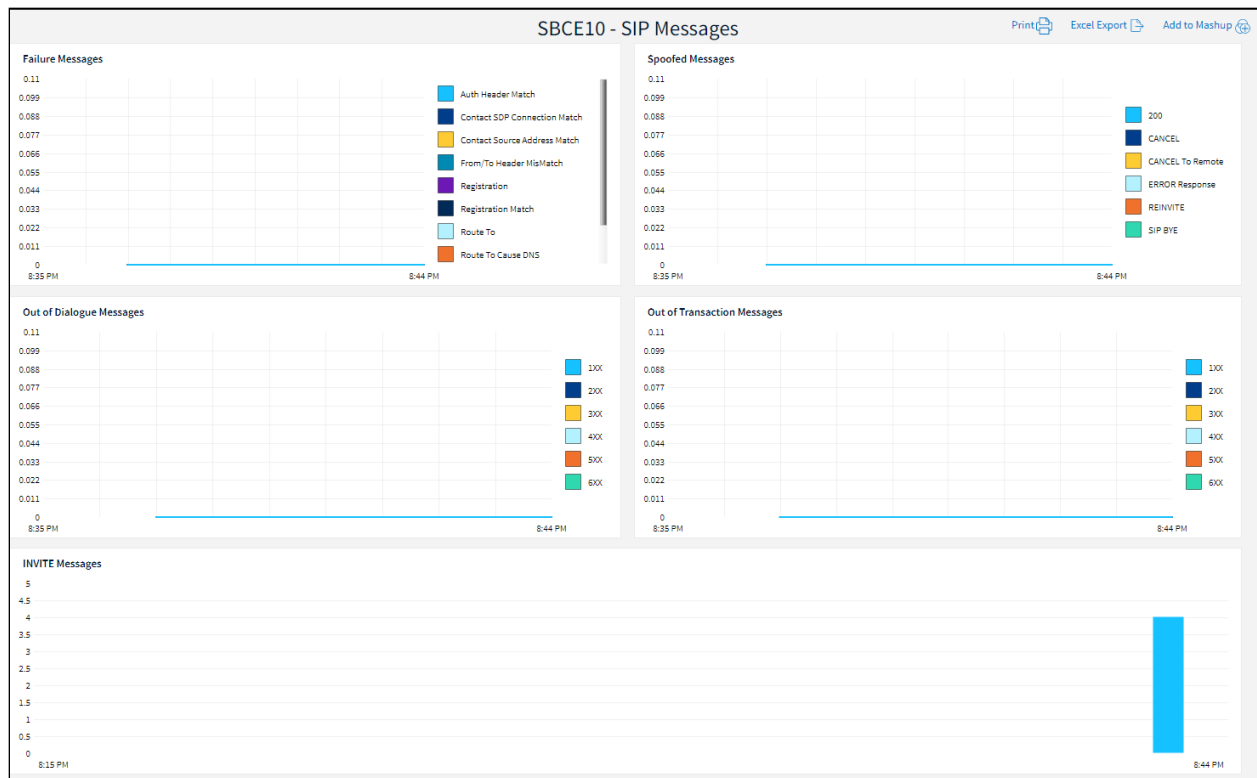
Excel Export

Add to Mashup

ID	Message	Name	Status	System
1	Test alarm	ipcsTestAlarm	0	IPCS0
14	DROP:SBCE:CRITICAL:Restarting slapd	ipcsProcessFail	0	IPCS2
19	RAISE:SBCE:CRITICAL:Certificate SMGRdefault.pem wi	ipcsCertificateExpiryAlert	active	IPCS2

Make an inbound or outbound call from/to Service Provider. Verify the details such as **Calls & Registrations** are displaying data as shown below and on the next page.

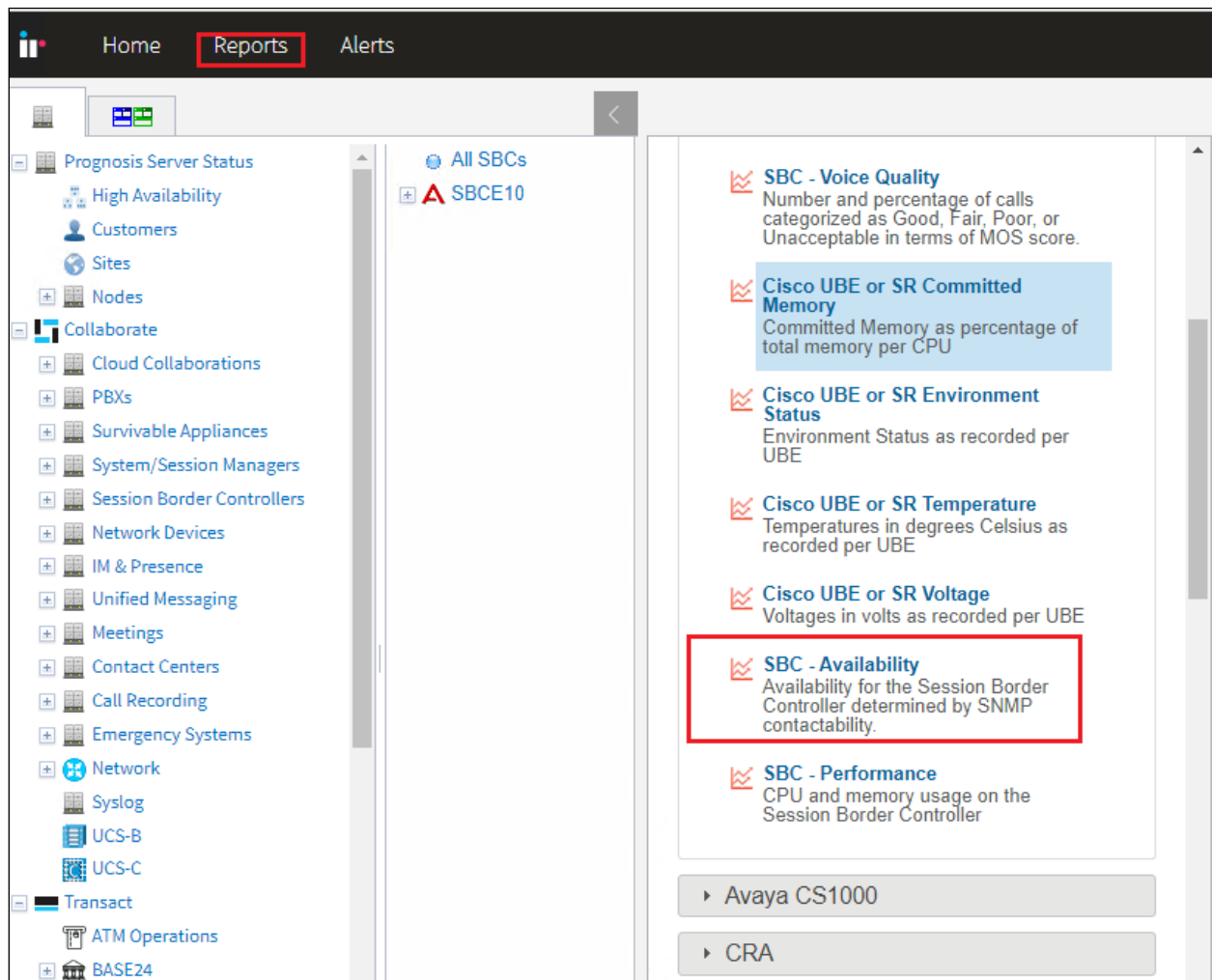




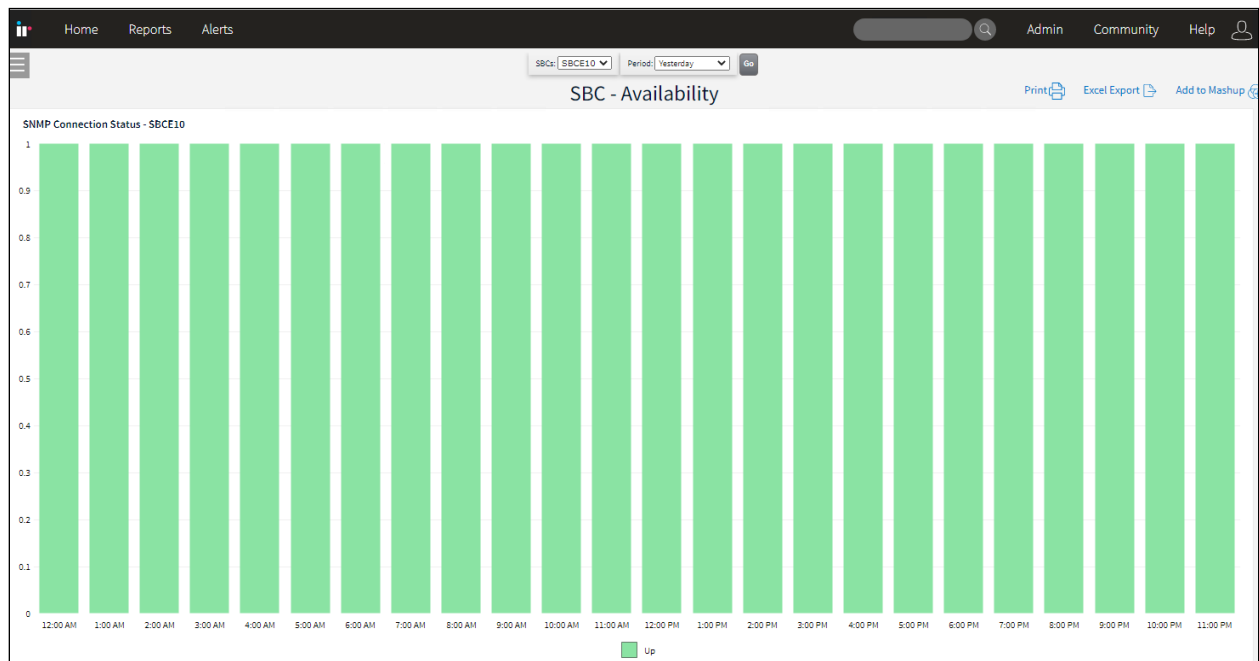
To view SYSLOG, from the home screen navigate to **Collaborate** → **Network** → **Syslog**. Below is a screenshot of the SYSLOG data collected from SBCE with IP Address shown below.



Reports can be generated for SBCE – Availability or Performance. From the login home screen in **Section 8**, select **Reports** and navigate to **Session Border Controller** (not shown) on the right pane. Select say **SBC – Availability** below.



The SBCE availability should be shown after selecting the SBC and duration as below by clicking **Go**. Note that **SBC – Performance** data is not currently being used as indicated in **Section 2.2** observations.



10. Conclusion

These Application Notes describe the procedures for configuring the Collaborate - Prognosis Server R12.1 to interoperate with Avaya Session Border Controller for Enterprise R10.1. During compliance testing, all test cases were completed successfully with observation noted in **Section 2.2**.

11. Additional References

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

- [1] *Administering Avaya Aura® Communication Manager*, Release 10.1.x, Issue 1, Dec 2021.
- [2] *Administering Avaya Aura® Session Manager*, Release 10.1, Issue 1, Dec 2021.
- [3] *Administering Avaya Session Controller for Enterprise*, Release 10.1.x, Issue 1, Dec 2021.
- [4] *Application Notes for Integrated Research's Collaborate - Prognosis Server R12.1 with Avaya Aura® Communication Manager R10.1*.
- [5] *Application Notes for Integrated Research's Collaborate - Prognosis Server R12.1 with Avaya Aura® Session Manager R10.1*.
- [6] *Avaya Session Border Controller for Enterprise Overview and Specification*, Release 10.1.x, Issue 1, Dec 2021.

Prognosis documentations are provided in the online help that comes with the software package.

©2022 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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