Application Notes for Configuring Micro-Tel Microcall with Avaya Session Border Controller for Enterprise – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Micro-Tel Microcall to interoperate with Avaya Session Border Controller for Enterprise.

Micro-Tel Microcall is a call accounting reporting solution that uses RADIUS method to collect and process Call Detail Recording records from Avaya Session Border Controller for Enterprise.

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

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

1. Introduction

The overall objective of this interoperability compliance testing is to verify that Micro-Tel Microcall can interoperate with Avaya Session Border Controller for Enterprise. Microcall is a call accounting reporting solution that collects Call Detail Recording (CDR) records from Avaya Session Border Controller for Enterprise (SBCE) over the local or wide area network using RADIUS method. SBCE is configured to produce CDR records.

Microcall provides traditional call record collection, rating, and reporting for any size businesses. Microcall can interface with most telephone systems - in particular, with Avaya SBCE - to collect and interpret the detailed records of inbound and outbound call through SIP trunk of Avaya SBCE. Microcall then calculates the appropriate charge for local, long distance, international & special calls and allocates them to responsible parties.

2. General Test Approach and Test Results

The general test approach was to manually place inbound and outbound calls from enterprise to PSTN and vice versa through SIP trunk in Avaya SBCE to verify that Microcall collects the CDR records, and properly classifies and reports the attributes of the call.

For serviceability testing, physical and logical links were disabled/re-enabled, Avaya Servers were reset, and Microcall connection and its server was restarted.

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 Microcall did not include use of any specific encryption features as requested by Microcall.

Encryption (TLS/SRTP) was used internal to the enterprise between Avaya products.

2.1. Interoperability Compliance Testing

The interoperability compliance testing included features and serviceability tests. The feature testing focused on verifying the proper parsing and displaying of CDR data by Microcall for call scenarios including inbound and outbound trunk calls.

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

2.2. Test Results

All executed test cases were verified and passed.

2.3. Support

Technical support on Microcall can be obtained through the following:

- Phone: +1 (800) 622-2285
- Email: information@microcall.com
- Web: https://www.microcall.com

For technical support on the Avaya products described in these Application Notes visit http://support.avaya.com

3. Reference Configuration

Figure 1 illustrates a sample configuration consisting SBCE, Avaya Aura® System Manager, Avaya Aura® Session Manager, Avaya Aura® Communication Manager, and Avaya Aura® Media Server running on Virtualized Environment, and Microcall.

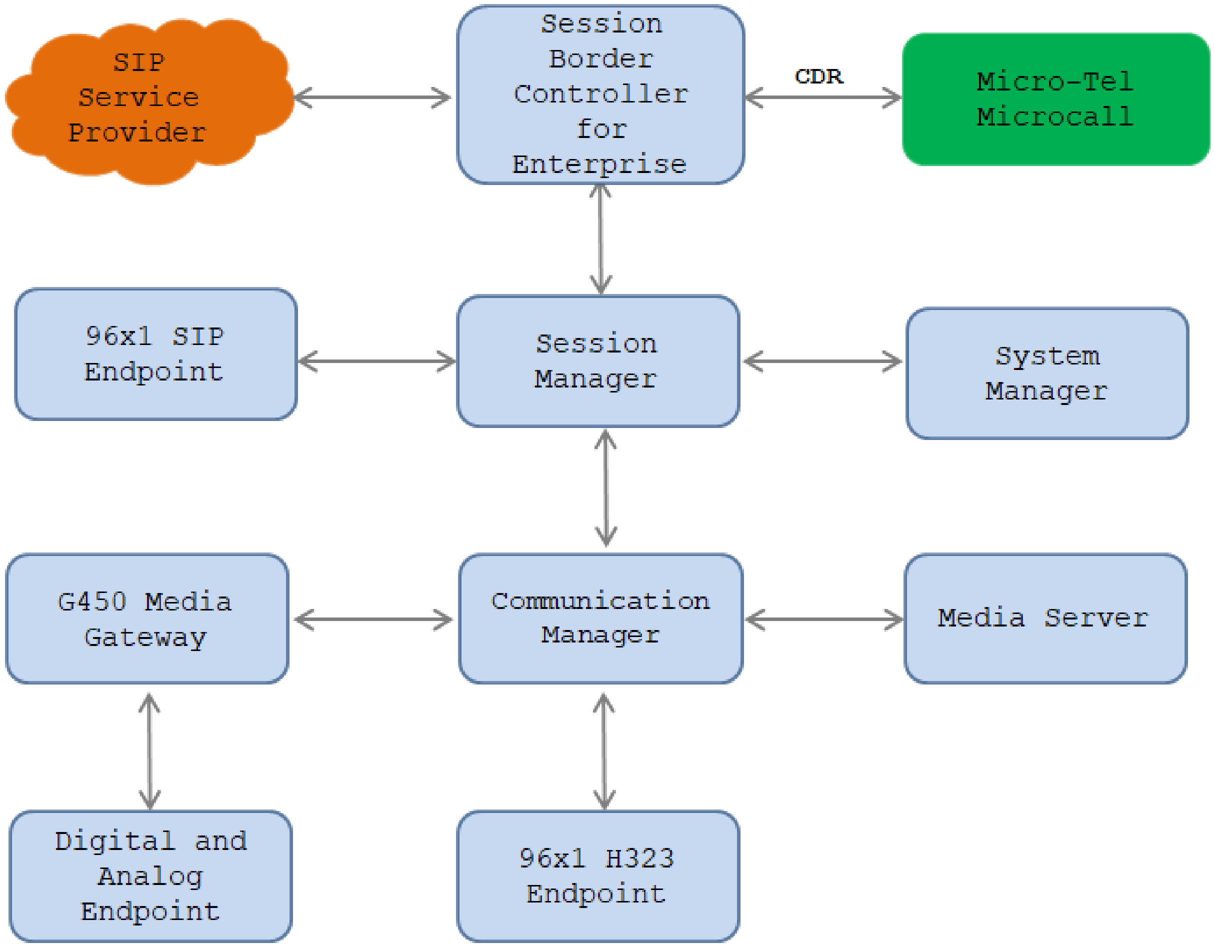


Figure 1: Test Configuration Diagram

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 running on Virtualized Environment	8.1.1 R018x.00.0.822.0
Avaya Aura® System Manager running on Virtualized Environment	8.1.1 Build 8.0.0.0.931077
Avaya Aura® Session Manager running on Virtualized Environment	8.1.1 Build 8.0.0.0.800035
Avaya Session Controller for Enterprise running on Virtualized Environment	8.0.0.019
Avaya Aura® Media Server running on Virtualized Environment	8.0.0.150
Avaya G450 Media Gateway • MGP	 41.10.0
Avaya 96x1 IP Deskphones	H.323 6.804 SIP 7.1.7
Avaya 1416 Digital Deskphone	FW1
Analog Deskphone	-
Micro-Tel Microcall	7.10.60.0

5. Configure Avaya Session Border Controller for Enterprise

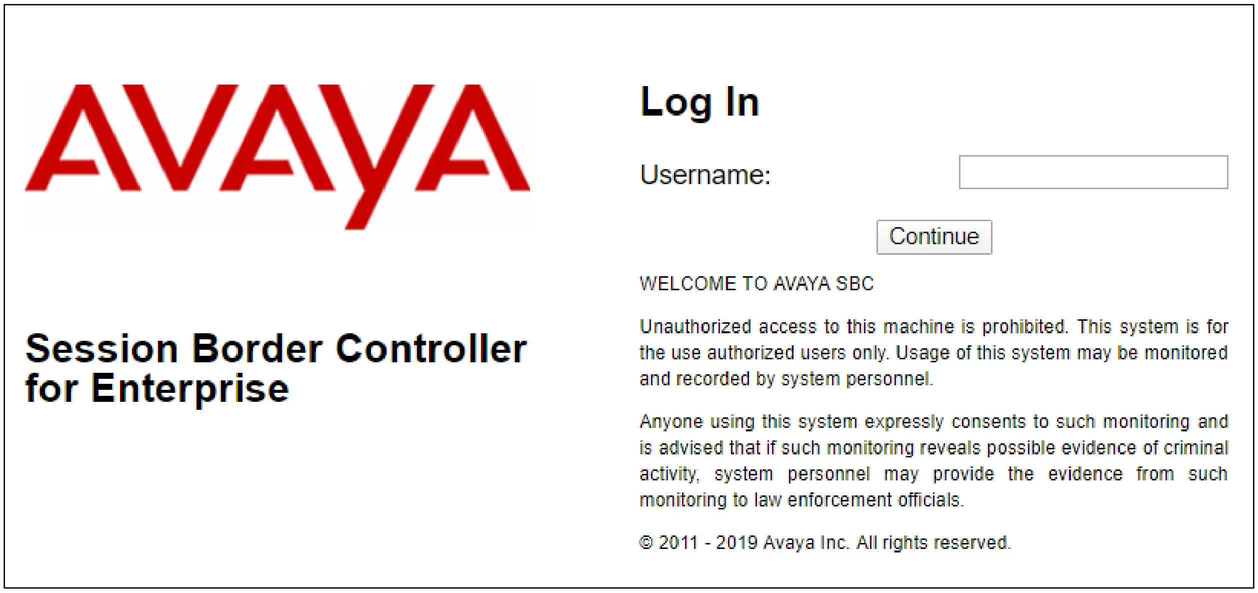
This section describes the configuration of the SBCE. It is assumed that the initial installation of the SBCE has been completed including the assignment of a management IP address. The management interface **must** be provisioned on a different subnet than either the SBCE private or public network interfaces (e.g., A1 and B1).

On all screens described in this section, it is assumed that parameters are left at their default values unless specified otherwise.

Note: For the samples of configuring SIP trunk to service provider in SBCE, please refer to **Section 9** for more detail.

5.1. Access the Management Interface

Use a web browser to access the web interface by entering the URL **https://<ip-addr>**, where **<ip-addr>** is the management IP address assigned during installation. The SBCE login page will appear as shown below. Log in with appropriate credentials.



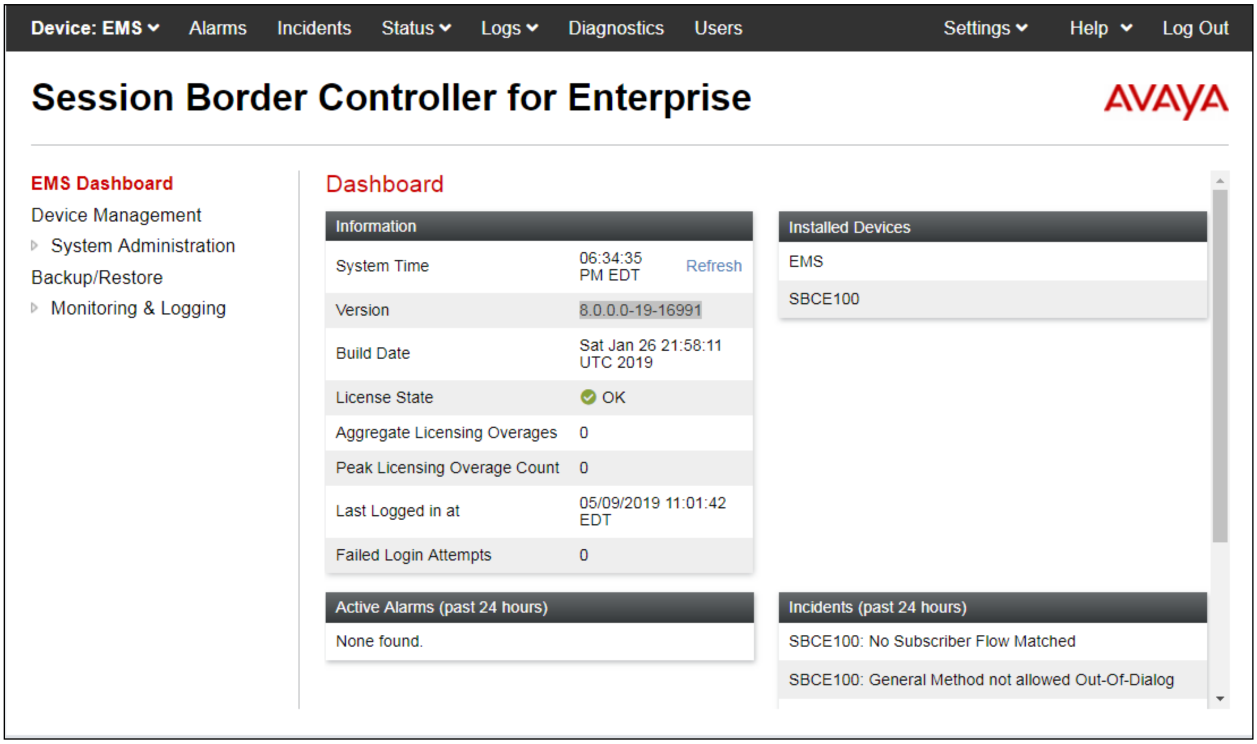
WELCOME TO AVAYA SBC

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 - 2019 Avaya Inc. All rights reserved.

After logging in, the **Dashboard** screen will appear as shown below. All configuration screens of the SBCE are accessed by navigating the menu tree in the left pane.



Dashboard

Information		
System Time	06:34:35 PM EDT	Refresh
Version	8.0.0.0-19-16991	
Build Date	Sat Jan 26 21:58:11 UTC 2019	
License State	✓ OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	05/09/2019 11:01:42 EDT	
Failed Login Attempts	0	

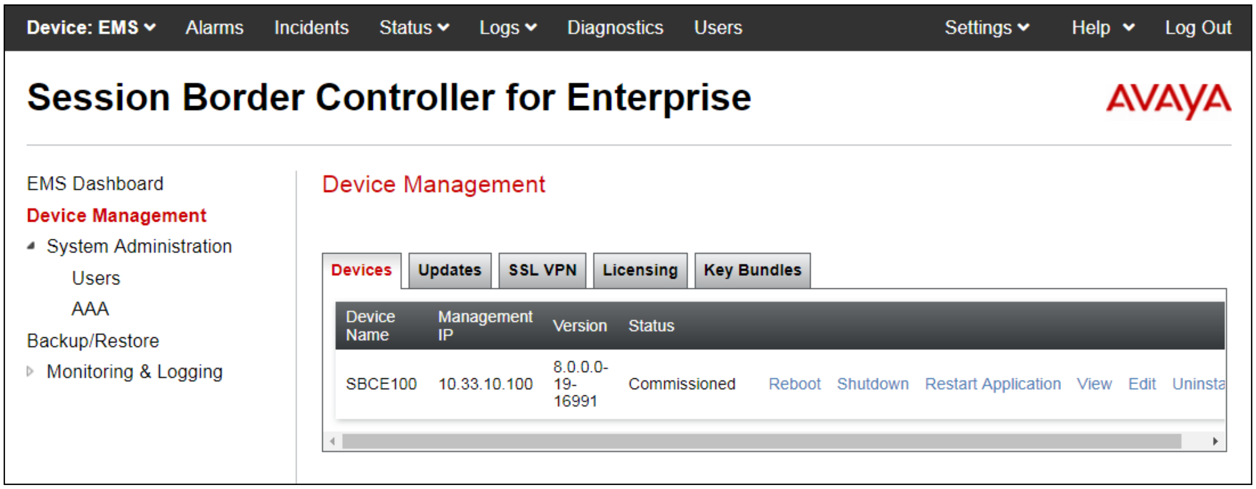
Installed Devices
EMS
SBCE100

Active Alarms (past 24 hours)
None found.

Incidents (past 24 hours)
SBCE100: No Subscriber Flow Matched
SBCE100: General Method not allowed Out-Of-Dialog

5.2. Verify Network Configuration and Enable Interfaces

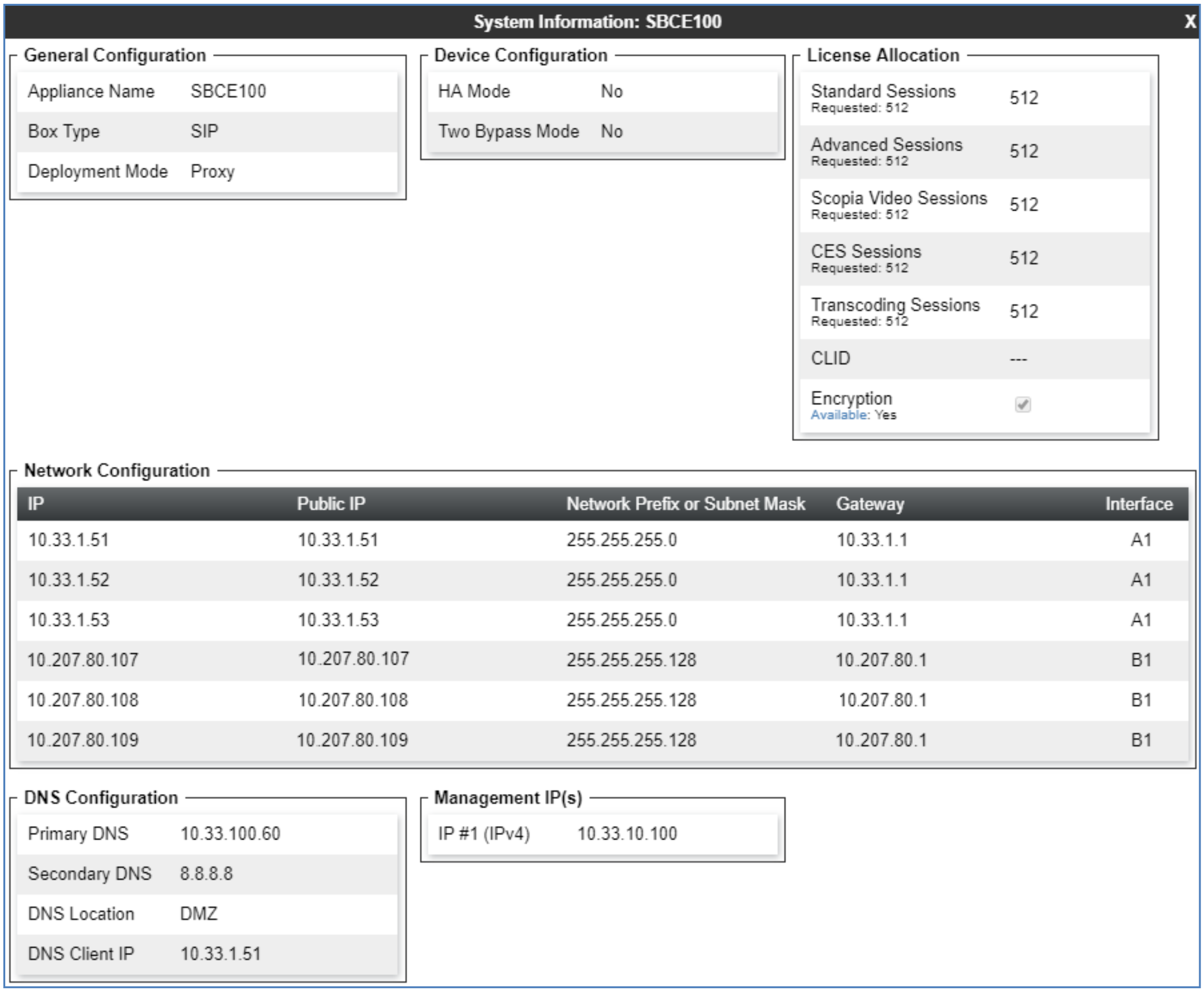
To view the network information provided during installation, navigate to **Device Management**. In the right pane, click **View** highlighted below.



Device Management

Device Name	Management IP	Version	Status						
SBCE100	10.33.10.100	8.0.0.0-19-16991	Commissioned	Reboot	Shutdown	Restart Application	View	Edit	Uninsta

A **System Information** page will appear showing the information provided during installation. In the **Appliance Name** field is the name of the device (**SBCE100**). This name will be referenced in other configuration screens. Interface **A1** and **B1** represent the private and public interfaces of the SBCE respectively. Each of these interfaces must be enabled after installation.



System Information: SBCE100

General Configuration

Appliance Name	SBCE100
Box Type	SIP
Deployment Mode	Proxy

Device Configuration

HA Mode	No
Two Bypass Mode	No

License Allocation

Standard Sessions Requested: 512	512
Advanced Sessions Requested: 512	512
Scopia Video Sessions Requested: 512	512
CES Sessions Requested: 512	512
Transcoding Sessions Requested: 512	512
CLID	---
Encryption Available: Yes	☑

Network Configuration

IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface
10.33.1.51	10.33.1.51	255.255.255.0	10.33.1.1	A1
10.33.1.52	10.33.1.52	255.255.255.0	10.33.1.1	A1
10.33.1.53	10.33.1.53	255.255.255.0	10.33.1.1	A1
10.207.80.107	10.207.80.107	255.255.255.128	10.207.80.1	B1
10.207.80.108	10.207.80.108	255.255.255.128	10.207.80.1	B1
10.207.80.109	10.207.80.109	255.255.255.128	10.207.80.1	B1

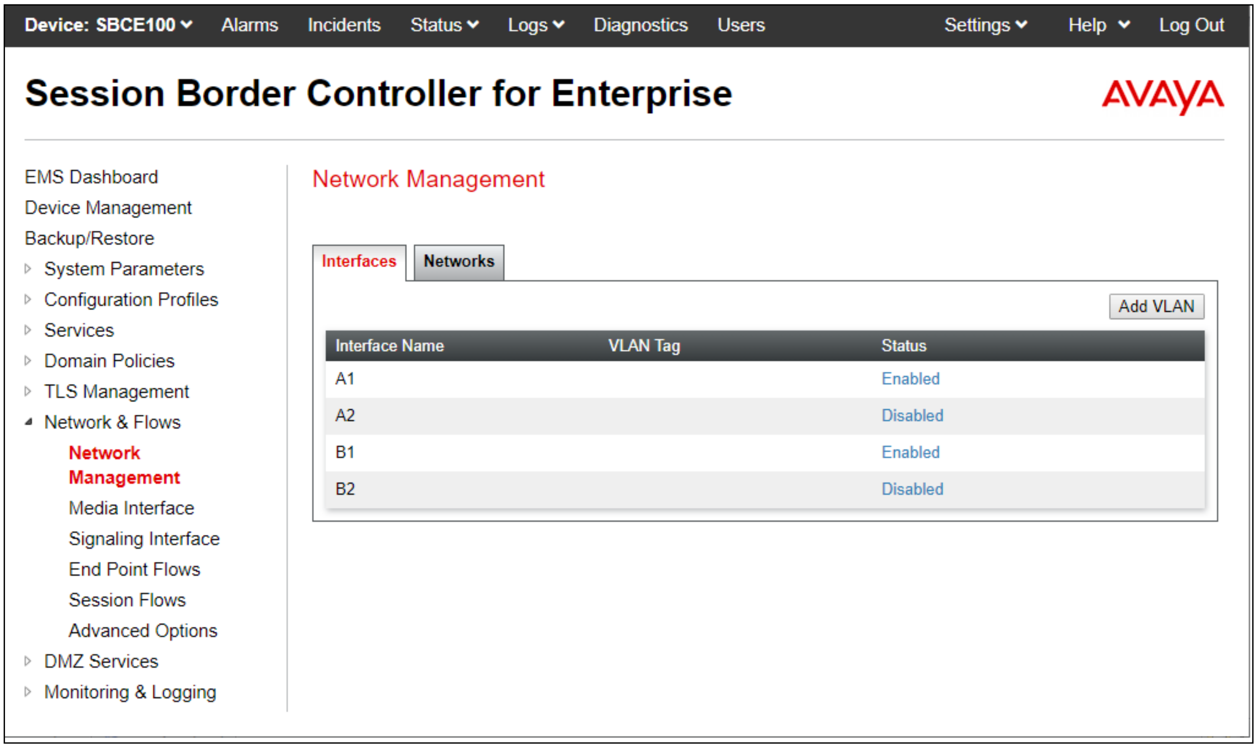
DNS Configuration

Primary DNS	10.33.100.60
Secondary DNS	8.8.8.8
DNS Location	DMZ
DNS Client IP	10.33.1.51

Management IP(s)

IP #1 (IPv4)	10.33.10.100

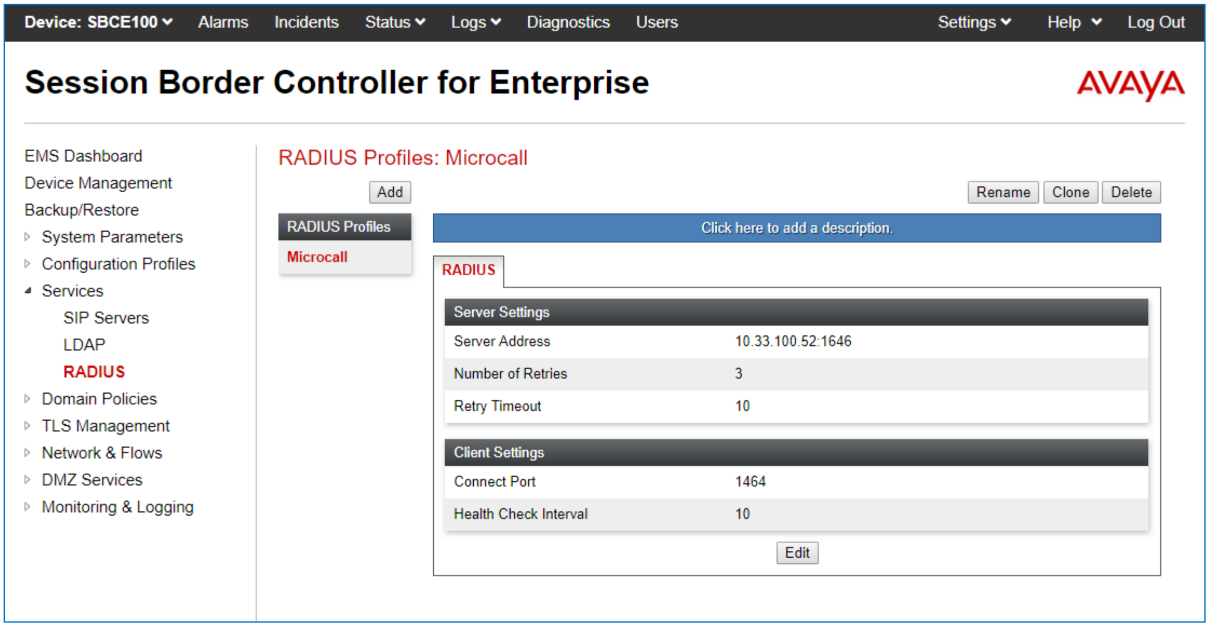
To enable the interfaces, first navigate on the left top menu and select the name of SBCE device in this case is "**SBCE100**". The reference options are displayed in the left pane. Navigate to **Network & Flows → Network Management** in the left pane and select the device being managed in the center pane. In the right pane, click on the **Interfaces** tab. Verify the **Status** is **Enabled** for both the **A1** and **B1** interfaces. If not, click the status **Enabled/Disabled** to toggle the state of the interface.



Interface Name	VLAN Tag	Status
A1		Enabled
A2		Disabled
B1		Enabled
B2		Disabled

5.3. Creating a RADIUS Profile

A RADIUS configuration profile defines the attributes of the physical server. To create a new profile, navigate to **Backup/Restore → Services → RADIUS** in the left pane. In the center pane, select **Add**. A pop-up window (not shown) will appear requesting the name of the new profile, followed by one or more pop-up windows in which the profile parameters can be configured.



RADIUS Profiles: Microcall

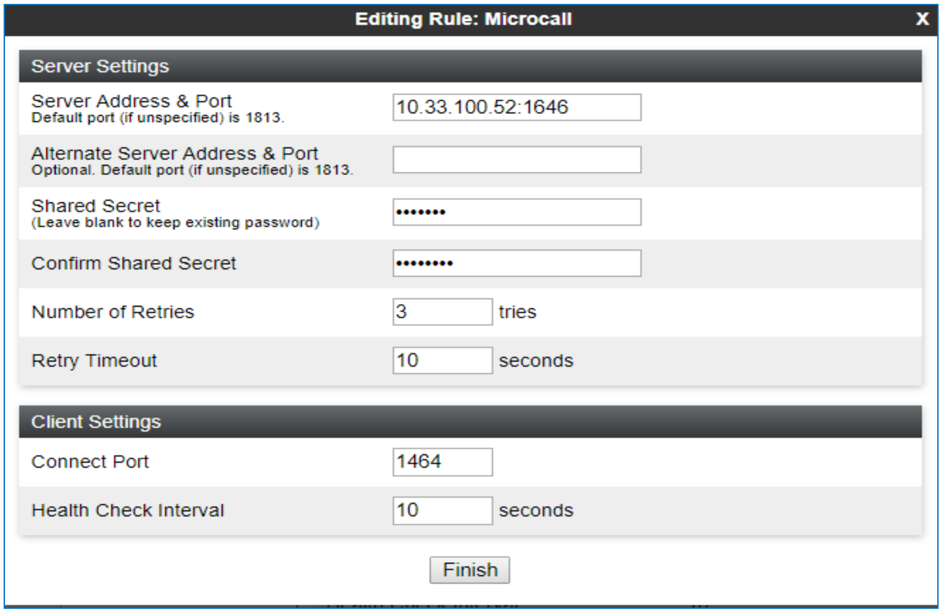
Server Settings	
Server Address	10.33.100.52:1646
Number of Retries	3
Retry Timeout	10

Client Settings	
Connect Port	1464
Health Check Interval	10

The screenshot below shows RADIUS profile Microcall configured for the compliance test. Enter the following values in the Server Settings section:

- Server Address & Port: enter the IP address of Microcall server and its dedicated port.
- Shared Secret: enter a share secret pass code.
- Confirm Shared Secret: re-enter the share secret pass code.

Keep other parameters at the default values.



Editing Rule: Microcall

Server Settings

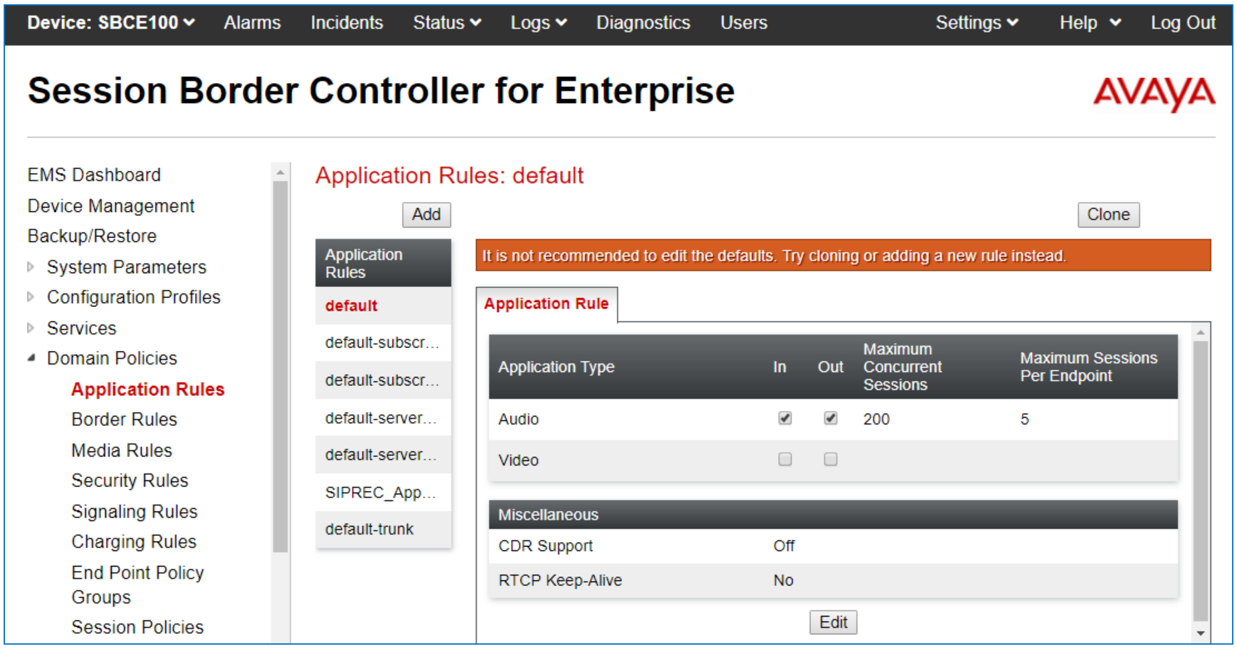
Server Address & Port Default port (if unspecified) is 1813.	10.33.100.52:1646
Alternate Server Address & Port Optional. Default port (if unspecified) is 1813.	
Shared Secret (Leave blank to keep existing password)	•••••••
Confirm Shared Secret	••••••••
Number of Retries	3 tries
Retry Timeout	10 seconds

Client Settings

Connect Port	1464
Health Check Interval	10 seconds

5.4. Enabling CDR in an Application

CDR must be enabled in an application that is associated with SIP trunk otherwise CDR data is not collected for that application. In the left navigation pane, select **Backup/Restore → Domain Policies → Application Rules**. The application pane displays the existing application rule sets.



Session Border Controller for Enterprise

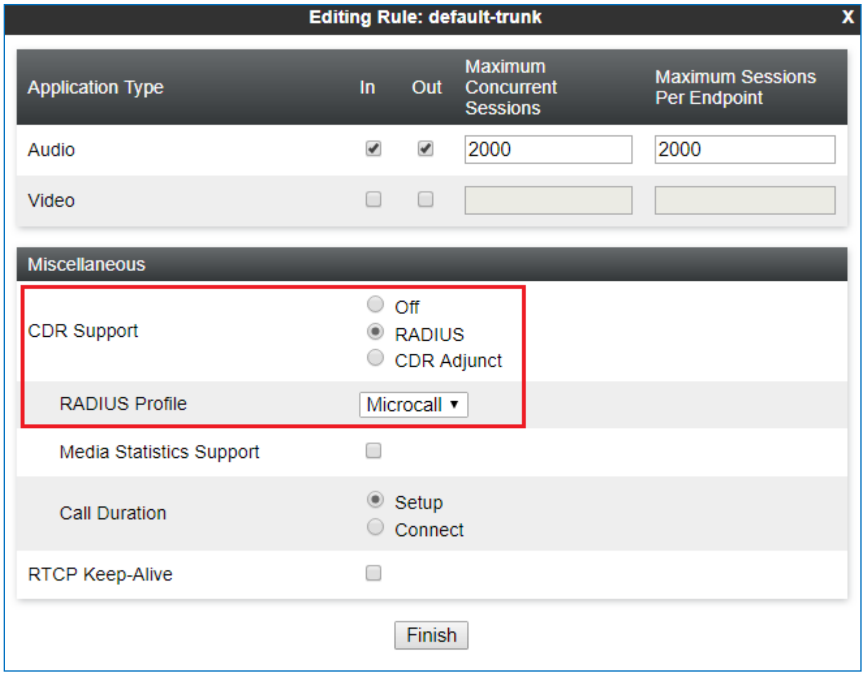
Application Rules: default

It is not recommended to edit the defaults. Try cloning or adding a new rule instead.

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	☑	☑	200	5
Video	□	□		

Miscellaneous	
CDR Support	Off
RTCP Keep-Alive	No

The screen below shows the **default-trunk** application that had **CDR Support** enabled with ***Microcall*** RADIUS profile created in **Section 5.3**.



Editing Rule: default-trunk

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	☑	☑	2000	2000
Video	□	□		

Miscellaneous	
CDR Support	○ Off ● RADIUS ○ CDR Adjunct
RADIUS Profile	Microcall ▾
Media Statistics Support	□
Call Duration	● Setup ○ Connect
RTCP Keep-Alive	□

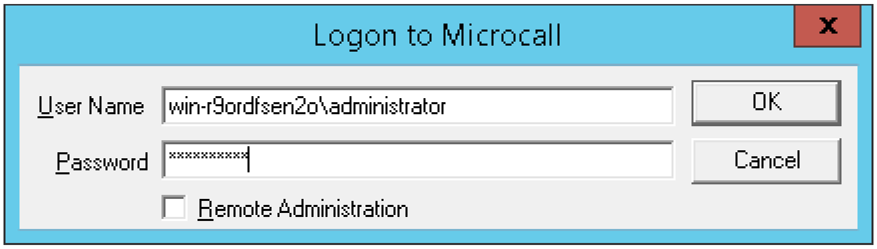
6. Configure Micro-Tel Microcall

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

- Configure Data Source
- Verify CDR Data

6.1. Configure Data Source

Open the Microcall application by double-click on the Microcall icon on the desktop (not shown). The **Logon to Microcall** window is displayed. Enter an appropriate password to log on.

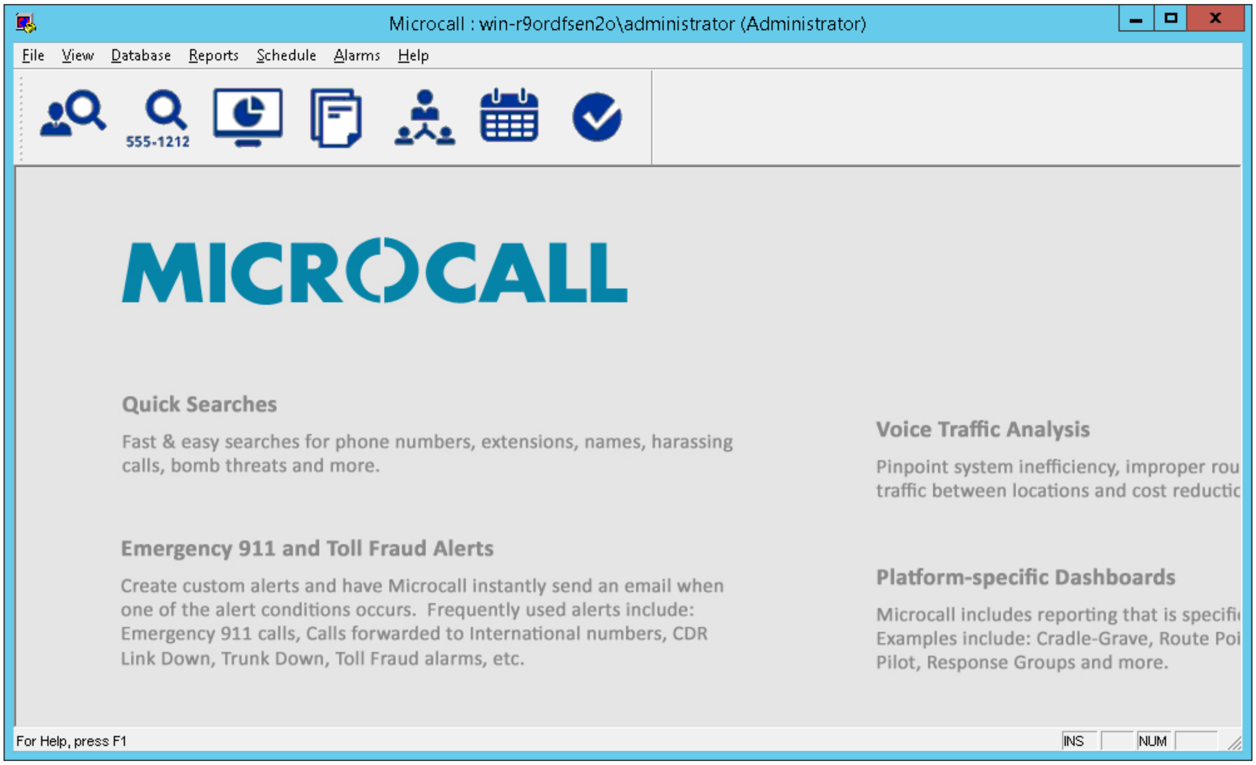


User Name: win-r9ordfsen2o\administrator

Password: **********

☐ Remote Administration

The **Microcall** window is displayed as shown below.


Microcall : win-r9ordfsen2o\administrator (Administrator)
File View Database Reports Schedule Alarms Help
555-1212
MICROCALL
For Help, press F1
INS
NUM

Quick Searches

Fast & easy searches for phone numbers, extensions, names, harassing calls, bomb threats and more.

Emergency 911 and Toll Fraud Alerts

Create custom alerts and have Microcall instantly send an email when one of the alert conditions occurs. Frequently used alerts include: Emergency 911 calls, Calls forwarded to International numbers, CDR Link Down, Trunk Down, Toll Fraud alarms, etc.

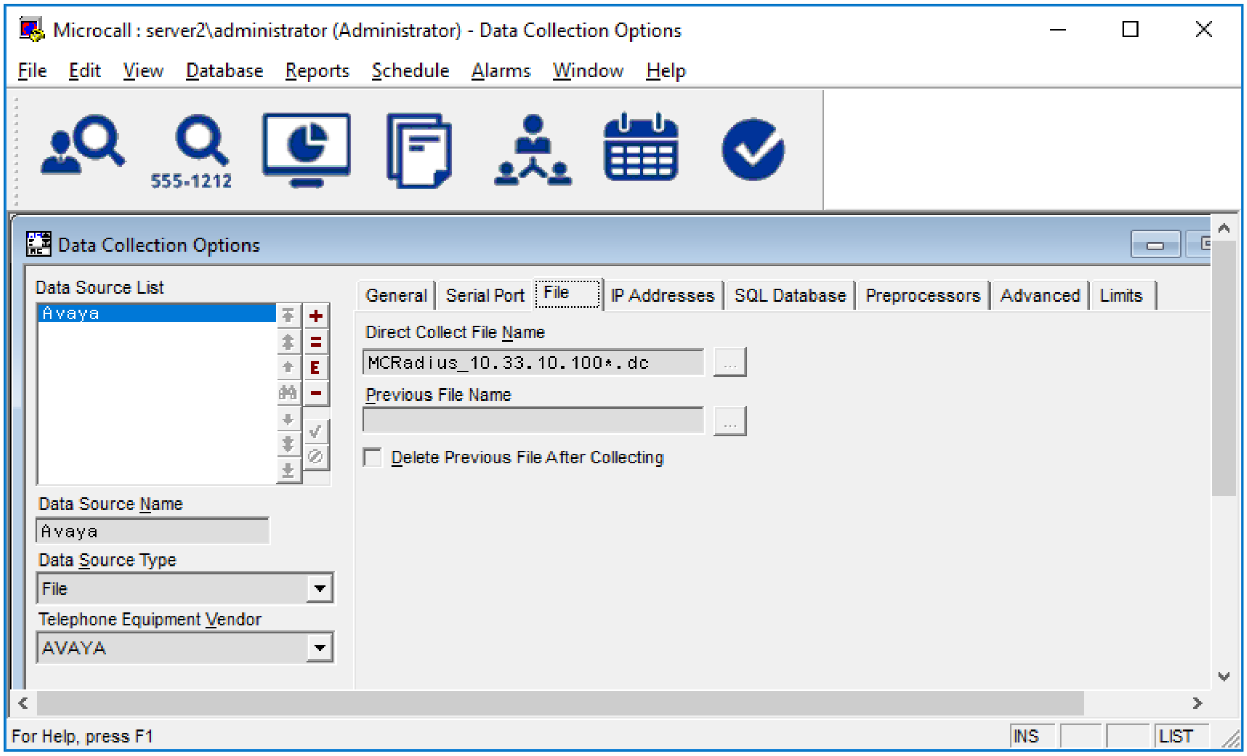
Voice Traffic Analysis

Pinpoint system inefficiency, improper rou traffic between locations and cost reductic

Platform-specific Dashboards

Microcall includes reporting that is specifi Examples include: Cradle-Grave, Route Poi Pilot, Response Groups and more.

From the **Microcall** window above, navigate to **File → Data Collection Options → Data Source** (not shown). The **Data Collection Options** window is displayed. In the compliance test, the **Data Source Name** "Avaya" was created and uses **Data Source Type** as "File". Browse to the directory where the CDR records are to be stored in the **Direct Collection File Name** of **File** tab shown in the right hand of the window.



Microcall : server2\administrator (Administrator) - Data Collection Options
File Edit View Database Reports Schedule Alarms Window Help
555-1212
Data Collection Options
General Serial Port File IP Addresses SQL Database Preprocessors Advanced Limits
For Help, press F1
INS
LIST

Data Source List
Avaya

Data Source Name
Avaya

Data Source Type
File

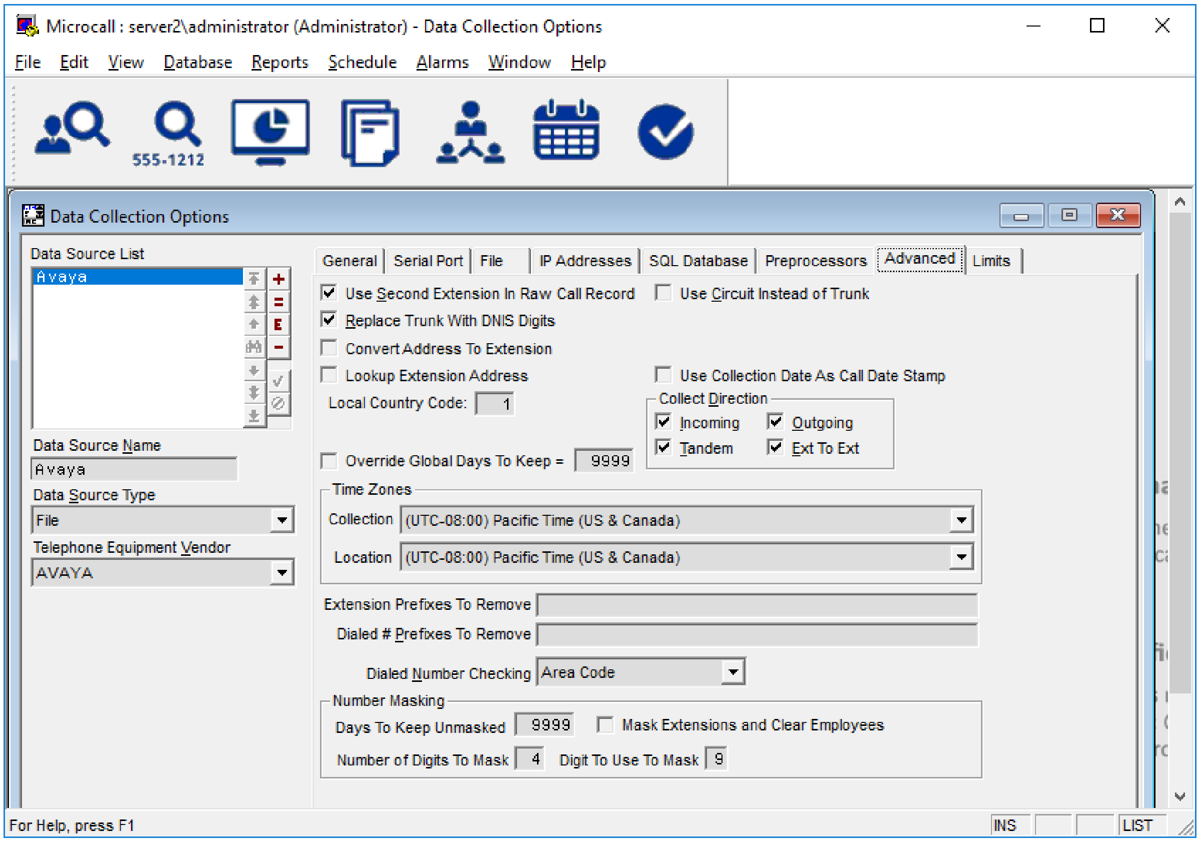
Telephone Equipment Vendor
AVAYA

Direct Collect File Name
MCRadius_10.33.10.100*.dc

Previous File Name

□ Delete Previous File After Collecting

In the **Advanced** tab, select all directions in the **Collection Direction** section.


Microcall : server2\administrator (Administrator) - Data Collection Options
File Edit View Database Reports Schedule Alarms Window Help
555-1212
Data Collection Options
General | Serial Port | File | IP Addresses | SQL Database | Preprocessors | Advanced | Limits
For Help, press F1
INS
LIST

Data Source List: Avaya

Data Source Name: Avaya

Data Source Type: File

Telephone Equipment Vendor: AVAYA

☑ Use Second Extension In Raw Call Record
☐ Use Circuit Instead of Trunk
☑ Replace Trunk With DNIS Digits
☐ Convert Address To Extension
☐ Lookup Extension Address
☐ Use Collection Date As Call Date Stamp
Local Country Code: 1

Collect Direction
☑ Incoming ☑ Outgoing
☑ Tandem ☑ Ext To Ext

☐ Override Global Days To Keep = 9999

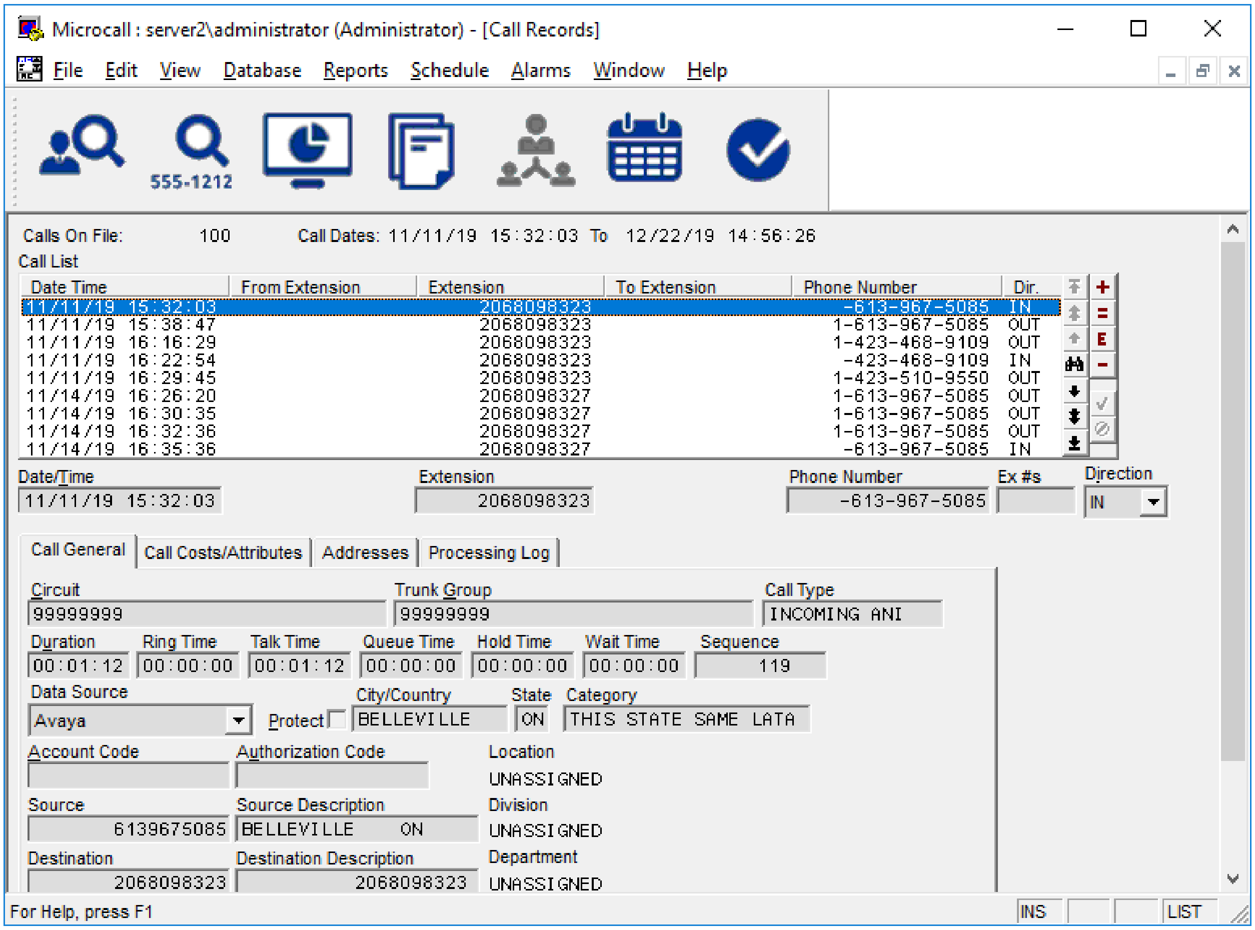
Time Zones
Collection: (UTC-08:00) Pacific Time (US & Canada)
Location: (UTC-08:00) Pacific Time (US & Canada)

Extension Prefixes To Remove:
Dialed # Prefixes To Remove:
Dialed Number Checking: Area Code

Number Masking
Days To Keep Unmasked: 9999 ☐ Mask Extensions and Clear Employees
Number of Digits To Mask: 4 Digit To Use To Mask: 9

6.2. Verify CDR Data

The raw CDR data can be verified by selecting **Call Records** from the **Database** menuto display all CDR records that Microcall receives and processes from the CDR records of SBCE.



Calls On File: 100 Call Dates: 11/11/19 15:32:03 To 12/22/19 14:56:26

Call List

Date Time	From Extension	Extension	To Extension	Phone Number	Dir.
11/11/19 15:32:03		2068098323		-613-967-5085	IN
11/11/19 15:38:47		2068098323		1-613-967-5085	OUT
11/11/19 16:16:29		2068098323		1-423-468-9109	OUT
11/11/19 16:22:54		2068098323		-423-468-9109	IN
11/11/19 16:29:45		2068098323		1-423-510-9550	OUT
11/14/19 16:26:20		2068098327		1-613-967-5085	OUT
11/14/19 16:30:35		2068098327		1-613-967-5085	OUT
11/14/19 16:32:36		2068098327		1-613-967-5085	OUT
11/14/19 16:35:36		2068098327		-613-967-5085	IN

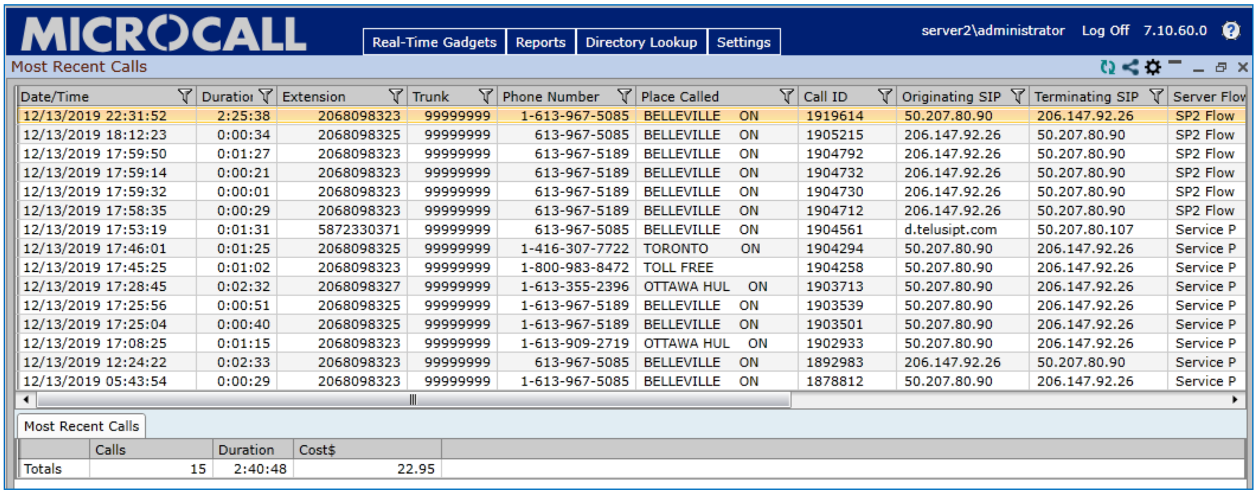
Date/Time: 11/11/19 15:32:03
Extension: 2068098323
Phone Number: -613-967-5085
Ex #s:
Direction: IN

Circuit: 99999999
Trunk Group: 99999999
Call Type: INCOMING ANI
Duration: 00:01:12
Ring Time: 00:00:00
Talk Time: 00:01:12
Queue Time: 00:00:00
Hold Time: 00:00:00
Wait Time: 00:00:00
Sequence: 119
Data Source: Avaya
Protect □
City/Country: BELLEVILLE
State: ON
Category: THIS STATE SAME LATA
Account Code:
Authorization Code:
Location: UNASSIGNED
Source: 6139675085
Source Description: BELLEVILLE ON
Division: UNASSIGNED
Destination: 2068098323
Destination Description: 2068098323
Department: UNASSIGNED

7. Verification Steps

The following steps may be used to verify the configuration:

- Make several different inbound and outbound SIP trunk calls via SBCE and verify that CDR records were collected by Microcall and showed up in the report.



Most Recent Calls

Date/Time	Duratioı	Extension	Trunk	Phone Number	Place Called	Call ID	Originating SIP	Terminating SIP	Server Flov
12/13/2019 22:31:52	2:25:38	2068098323	99999999	1-613-967-5085	BELLEVILLE ON	1919614	50.207.80.90	206.147.92.26	SP2 Flow
12/13/2019 18:12:23	0:00:34	2068098325	99999999	613-967-5085	BELLEVILLE ON	1905215	206.147.92.26	50.207.80.90	SP2 Flow
12/13/2019 17:59:50	0:01:27	2068098323	99999999	613-967-5189	BELLEVILLE ON	1904792	206.147.92.26	50.207.80.90	SP2 Flow
12/13/2019 17:59:14	0:00:21	2068098323	99999999	613-967-5189	BELLEVILLE ON	1904732	206.147.92.26	50.207.80.90	SP2 Flow
12/13/2019 17:59:32	0:00:01	2068098323	99999999	613-967-5189	BELLEVILLE ON	1904730	206.147.92.26	50.207.80.90	SP2 Flow
12/13/2019 17:58:35	0:00:29	2068098323	99999999	613-967-5189	BELLEVILLE ON	1904712	206.147.92.26	50.207.80.90	SP2 Flow
12/13/2019 17:53:19	0:01:31	5872330371	99999999	613-967-5085	BELLEVILLE ON	1904561	d.telusipt.com	50.207.80.107	Service P
12/13/2019 17:46:01	0:01:25	2068098325	99999999	1-416-307-7722	TORONTO ON	1904294	50.207.80.90	206.147.92.26	Service P
12/13/2019 17:45:25	0:01:02	2068098323	99999999	1-800-983-8472	TOLL FREE	1904258	50.207.80.90	206.147.92.26	Service P
12/13/2019 17:28:45	0:02:32	2068098327	99999999	1-613-355-2396	OTTAWA HUL ON	1903713	50.207.80.90	206.147.92.26	Service P
12/13/2019 17:25:56	0:00:51	2068098325	99999999	1-613-967-5189	BELLEVILLE ON	1903539	50.207.80.90	206.147.92.26	Service P
12/13/2019 17:25:04	0:00:40	2068098325	99999999	1-613-967-5189	BELLEVILLE ON	1903501	50.207.80.90	206.147.92.26	Service P
12/13/2019 17:08:25	0:01:15	2068098323	99999999	1-613-909-2719	OTTAWA HUL ON	1902933	50.207.80.90	206.147.92.26	Service P
12/13/2019 12:24:22	0:02:33	2068098323	99999999	613-967-5085	BELLEVILLE ON	1892983	206.147.92.26	50.207.80.90	Service P
12/13/2019 05:43:54	0:00:29	2068098323	99999999	1-613-967-5085	BELLEVILLE ON	1878812	50.207.80.90	206.147.92.26	Service P

Most Recent Calls

	Calls	Duration	Cost$
Totals	15	2:40:48	22.95

8. Conclusion

These Application Notes describe the procedures for configuring Micro-Tel Microcall with Avaya Session Border Controller for Enterprise. Testing was successful.

9. Additional References

This section references the Avaya and Resource Software International documentation that are relevant to these Application Notes. Product documentation for Avaya Aura® Session Manager, including the following, is available at: http://support.avaya.com/.

[1] *Administering Avaya Aura® Session Manager*, Document 03-300509, Issue 10, Release 8.1, July 2019
[2] *Administering Avaya Aura® System Manager*, Issue 9.0, Release 8.1, July 2019
[3] *Administering Avaya Session Border Controller for Enterprise*, Release 8.0, Release 8.0, February 2019

The Micro-Tel Microcall is available from Microcall website. Visit https://www.microcall.com/.

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.