



Avaya Solution & Interoperability Test Lab

Application Notes for Assertion® SBC Security with Avaya Session Border Controller for Enterprise – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Assertion® SBC Security to interoperate with Avaya Session Border Controller for Enterprise (Avaya SBCE) 8.1.3.

Assertion® SBC Security is a Software as a Service (SaaS) solution that provides SBCs with AI based real-time threat detection and monitoring. The solution is comprised of two components: the Assertion® SBC Security Cloud service and the Assertion® Scanner deployed on the customer's premises or in VPC (AWS, Azure, Google Cloud, Oracle Cloud) of the enterprise.

In the reference configuration used in these Application Notes the Assertion® Scanner software is installed on a Red Hat Enterprise Linux server at the customer's premises. The Assertion® Scanner extracts log and configuration information from the Avaya SBCE at the enterprise. The data is then transmitted to the Assertion® SBC Security Cloud service, where it is analyzed and presented in Summary and Detailed Reports to the user.

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.

Assertion® is a member of the Avaya DevConnect program. 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.

Table of Contents

1. Introduction.....	3
2. General Test Approach and Test Results.....	4
2.1. Interoperability Compliance Testing.....	6
2.2. Test Results	6
2.3. Support	6
3. Reference Configuration.....	7
4. Equipment and Software Validated	8
5. Avaya Session Border Controller for Enterprise	9
6. Install and Configure Assertion® Scanner	10
6.1. RHEL Server Preparation.....	10
6.2. Download and Install Software from Assertion Cloud	11
6.2.1. Register user in Assertion® SBC Security	11
6.2.2. Download and Install Assertion® Scanner Software	13
6.3. Add Avaya SBCE Device for Real Time Scanning	17
6.4. Summary Report	20
6.5. Detailed Report	23
7. Verification Steps.....	25
7.1. Assertion® Scanner Log Data Collection Verification.....	25
7.2. Assertion® Scanner Configuration Data Collection Verification.....	26
7.3. Verify Connectivity to Assertion® Cloud	27
8. Conclusion	28
9. Additional References.....	28

1. Introduction

These Application Notes describe the procedures for configuring Assertion® SBC Security to interoperate with Avaya Session Border Controller for Enterprise 8.1.3.

Assertion® SBC Security is a Software as a Service (SaaS) solution that provides SBCs with AI based real-time threat detection and monitoring. The software detects attacks, intrusions and breaches. This solution can be used to protect customers who have deployed SBC in their Unified Communication (UC) and Contact Center (CC) setup as remote worker or as a trunk gateway.

The solution is comprised of two components:

- Assertion® SBC Security Cloud service.
- Assertion® Scanner, deployed on the customer's premises or in VPC (AWS, Azure, Google Cloud, Oracle Cloud) of the enterprise.

In the reference configuration used in these Application Notes, the Assertion® Scanner software is installed on a Red Hat Enterprise Linux server on the customer's enterprise network. The Assertion® Scanner is configured to extract log and configuration information from the Avaya SBCE at the enterprise. The data is transmitted to the Assertion® SBC Security Cloud service, where it is analyzed and presented in Summary and Detailed Reports to the user. The Assertion® SBC Security Cloud service additionally includes REST APIs, intended to be consumed by SOC (Security Operation) and SOAR (Security Orchestration and Automatic Response) centers for real time incident management.

The Avaya SBCE functioned as the enterprise edge. The public facing interfaces of the Avaya are used to connect SIP signaling and related media messages to and from Remote Workers and a simulated PSTN SIP trunk over the public Internet. The private interfaces of the SBCE are used to connect to the enterprise Avaya Aura® infrastructure.

The Avaya Aura® reference architecture consists of Avaya Aura® Communication Manager, (Communication Manager), Avaya Aura® System Manager (System Manager) and Avaya Aura® Session Manager (Session Manager). Communication Manager is configured as an evolution server and acts as the telephony application server for Session Manager. The role of Session Manager in the reference architecture is to act as a Registrar for Avaya SIP endpoints and provide a centralized dial-plan for least-cost and time-of-day based routing.

2. General Test Approach and Test Results

A simulated enterprise site containing the Avaya SBCE and the rest of the Avaya Aura® infrastructure was installed at the Avaya Solution and Interoperability Lab. The Assertion® Scanner software was installed on a Red Hat Enterprise Linux server also located at the simulated enterprise site.

The compliance testing focused on verifying that the Assertion Scanner was able to connect to the management interface of the Avaya Session Border Controller for Enterprise, extract the pertinent logs and configuration data, and transmit the filtered logs to the Assertion® SBC Security Cloud service. Different attack, intrusion and breach scenarios were simulated using the Assertion Attack Simulation Labs via the Avaya SBCE public interfaces. The attacks were verified to be proactively detected and presented by Assertion® SBC Security in reports.

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 the Avaya SBCE and the Assertion® Scanner over the enterprise network utilized encrypted capabilities of SSH and HTTPS. The connection between the Assertion® Scanner and the Assertion® SBC Security Cloud service over the public Internet used encrypted HTTPS.

This test was conducted in a lab environment simulating a basic customer enterprise network environment. The testing focused on the standards-based interface between the Avaya solution and the third party solution. The results of testing are therefore considered to be applicable to either a premise-based deployment or to a hosted or cloud deployment where some elements of the third party solution may reside beyond the boundaries of the enterprise network, or at a different physical location from the Avaya components.

Readers should be aware that network behaviors (e.g., jitter, packet loss, delay, speed, etc.) can vary significantly from one location to another, and may affect the reliability or performance of

the overall solution. Different network elements (e.g., session border controllers, soft switches, firewalls, NAT appliances, etc.) can also affect how the solution performs.

If a customer is considering implementation of this solution in a cloud environment, the customer should evaluate and discuss the network characteristics with their cloud service provider and network organizations, and evaluate if the solution is viable to be deployed in the cloud.

The network characteristics required to support this solution are outside the scope of these Application Notes. Readers should consult the appropriate Avaya and third party documentation for the product network requirements. Avaya makes no guarantee that this solution will work in all potential deployment configurations.

The configuration shown in **Figure 1** was used to exercise the features and functionality tests listed in **Section 2.1**.

2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following areas and functionality:

- User account creation in Assertion® SBC Security.
- Assertion® Scanner software installation on RHEL server on the enterprise.
- Addition of the Avaya SBCE device for real-time scanning.
- Real time logs pull verification on the Assertion® Scanner.
- Retrieval of the Summary Report in the user's dashboard in Assertion® SBC Security, containing the scan findings and the current security posture.
- Retrieval of the Detailed Report in the user's dashboard in Assertion® SBC Security, with specific vulnerabilities, evidence trail and remediation recommendations.
- Several attack scenarios were simulated, originated from the Assertion Labs Attack Simulation via the public Internet to one of the Avaya SBCE public interfaces:
 - Toll Fraud Attempt
 - Toll Fraud Breach
 - Enumeration Attack
 - Brute Force Attack
 - Suspicious User Agent

The attacks were verified to be captured in the scanner log file, and reflected on the Incident Timeline of the Summary Report after 10 minutes of launching the attack.

- The events were additionally verified to be present in the event pipeline of the REST API on the Assertion® Cloud. cURL commands were used to retrieve events on specific time ranges, and compared with the ones shown on the Incident Timeline.
- Changes were made to the Avaya SBCE configuration, based on the security recommendations included in the generated Detailed Report, to remediate different vulnerabilities detected by the Assertion® Scanner. These changes were reflected in the improvement of the Avaya SBCE score in the SBC Risk Profile, on the subsequent Detailed Report generated after the next scheduled configuration collection.
- Verification of the Assertion® Scanner recovery and functionality after a network disconnection and reboot of the RHEL server.

2.2. Test Results

All test cases completed successfully.

2.3. Support

Visit <https://support.assertion.cloud> for information and support on the Assertion® SBC Security solution.

Optionally, the Assertion® support team can be reached via email at support@assertion.cloud.

3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**. The two main components of the Assertion® SBC Security solution are the Assertion® Scanner and the Assertion® SBC Security Cloud service. The Assertion® Scanner connects to the Avaya SBCE Management interface over the private network using SSH and HTTPS, and to the Assertion® SBC Security Cloud service over the public network using HTTPS.

In the reference configuration, a standalone Avaya EMS + SBCE was used. The SBCE had a public facing interface B1 used by Remote Workers and a simulated PSTN SIP trunk. The private interface A1 connects to Session Manager and the rest of the Avaya infrastructure.

The Assertion Lab Attack Simulator was used to launch different threat scenarios via the Avaya SBCE public interface. In the DevConnect Lab testing environment, a rule was added to the Enterprise Firewall to allow the Attack Simulator to be able to reach the Avaya SBCE B1 interface.

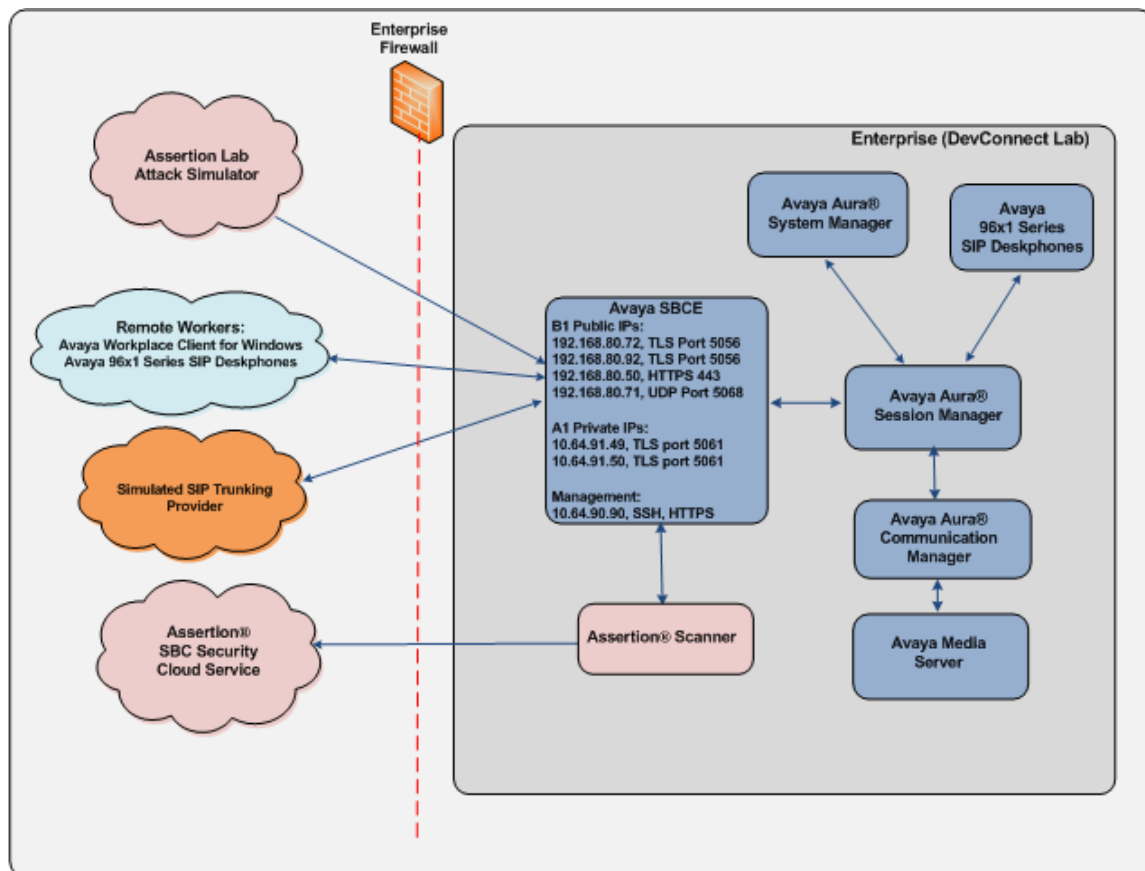


Figure 1: Test Configuration

Note: For security reasons, the public IP addresses used in the reference configuration on the Avaya SBCE interface B1 are masked in the diagram above.

4. Equipment and Software Validated

The following equipment and software were used in the sample configuration.

Equipment/Software	Release/Version
Avaya	
Avaya Session Border Controller for Enterprise	8.1.3.0-31-21052
Avaya Aura® System Manager	8.1.3.2.1012646 Service Pack 2
Avaya Aura® Session Manager	8.1.3.2.813207
Avaya Aura® Communication Manager	8.1.3.2.0-FP3SP2 (patch 26989)
Avaya Aura® Media Server	8.0.2.163
Avaya 96x1 Series IP Deskphone (SIP)	7.1.12.8
Avaya Workplace Client for Windows	3.19.0.72.19
Assertion	
Assertion® Scanner	Version 1.0.1, running on RHEL 8.4 server

Table 1: Equipment and Software Used in the Sample Configuration

5. Avaya Session Border Controller for Enterprise

The following Avaya SBCE information should be gathered, as it will be required during installation and device configuration:

- IP address / FQDN of the Management Interface (EMS) of the Avaya SBCE
- Web Login credentials with System Administrator role
- SSH Login credentials of the EMS

In the reference configuration, the Avaya SBCE is deployed in a standalone configuration, with the EMS and the SBCE being co-residents on the same server. The EMS management IP address was **10.64.90.90** as shown on the screen below.

Device Name	Management IP	Version	Status
SBCE8-90	10.64.90.90	8.1.3.0-31-21052	Commissioned

No special configuration was required on the Avaya SBCE for the connection to the Assertion Scanner on the enterprise.

6. Install and Configure Assertion® Scanner

This section describes the configuration necessary to install and configure the Assertion® Scanner software on a customer RHEL server on the enterprise.

6.1. RHEL Server Preparation

The following pre-requisites need to be met for a successful installation of the Assertion® Scanner software on the customer's network.

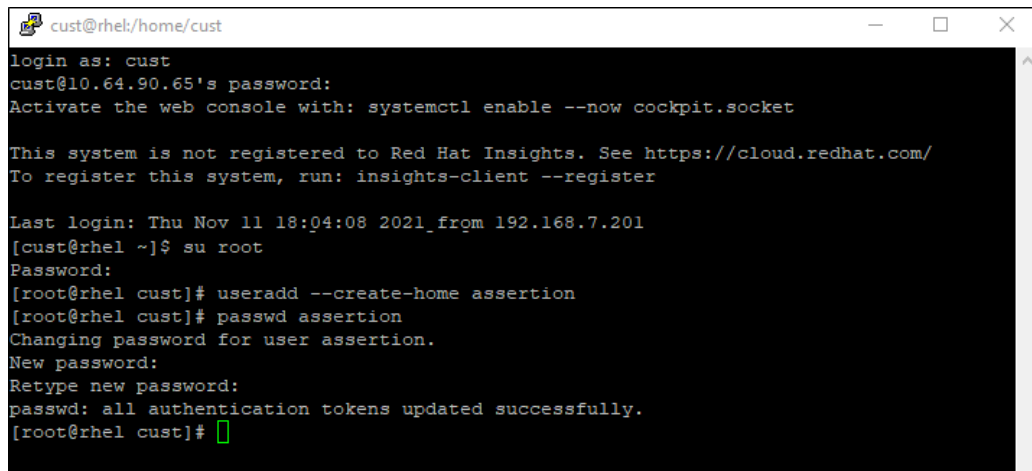
- Server with Red Hat Enterprise Linux version 8.2 or later operating system
- Internet connectivity on the Linux server. The server should be able to reach the Assertion cloud service at <https://scan.assertion.cloud>, using HTTPS port 443.
- Network connectivity on the enterprise network. The Linux server needs to be able to access the Avaya SBCE Management Interface (EMS):
 - Standard HTTPS port 443 is used to collect configuration data.
 - Trace logs of the SBC are collected using secured SSH on port 222.
- tar command should be present on Linux server.

Note: The configuration to meet the above pre-requisites is assumed to be in place and it is not discussed in this document.

SSH to the RHEL server where the scanner is going to be installed. Create a privileged user, that will be used for the software installation. In the reference configuration, a user named “assertion” was created.

Login as root. Enter the following commands:

- **useradd --create-home assertion**
- **passwd assertion.** Enter a password



```
cust@rhel:/home/cust
login as: cust
cust@10.64.90.65's password:
Activate the web console with: systemctl enable --now cockpit.socket

This system is not registered to Red Hat Insights. See https://cloud.redhat.com/
To register this system, run: insights-client --register

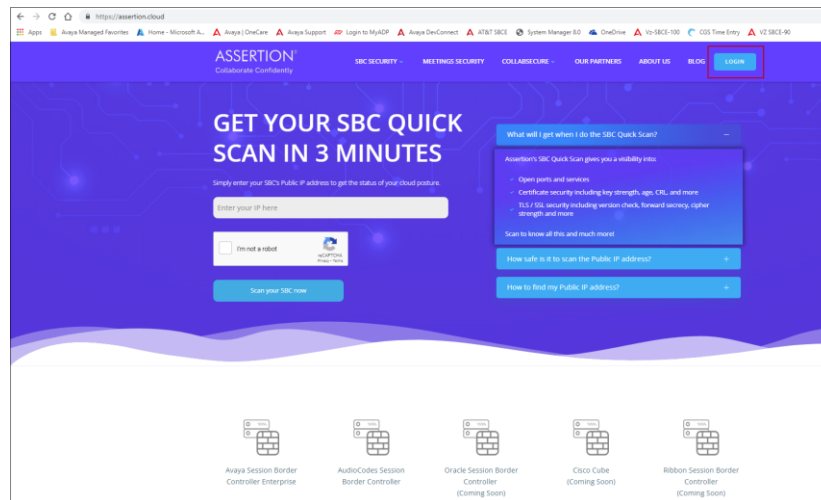
Last login: Thu Nov 11 18:04:08 2021 from 192.168.7.201
[cust@rhel ~]$ su root
Password:
[root@rhel cust]# useradd --create-home assertion
[root@rhel cust]# passwd assertion
Changing password for user assertion.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@rhel cust]#
```

- Enter the **visudo** command, to assign the sudo privileges to the user.
- Add the line below at the end of the file:
assertion ALL=(ALL) NOPASSWD: ALL
- Press **Esc** then **:wq** to save and exit

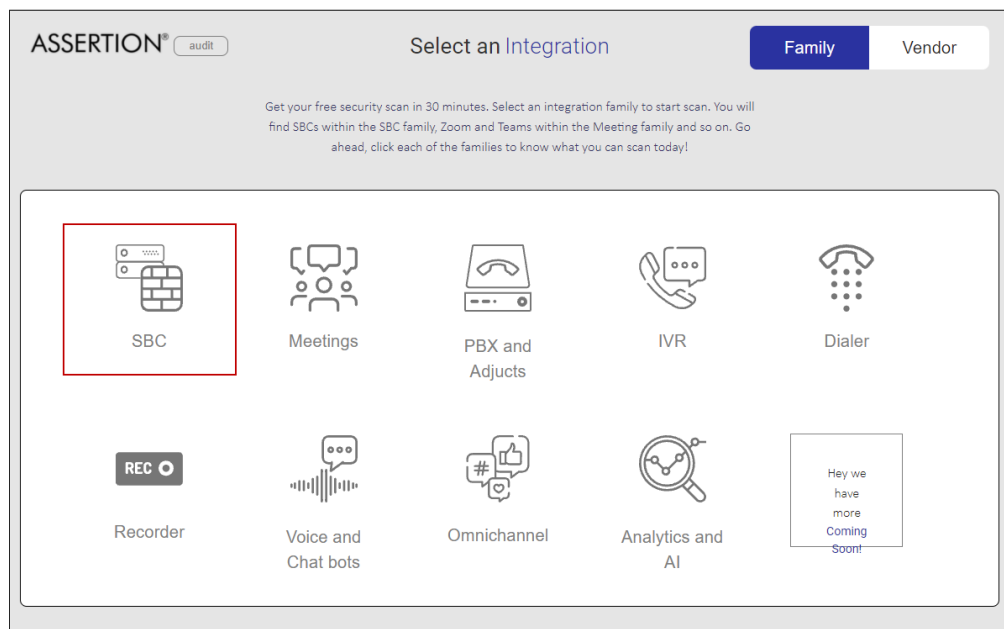
6.2. Download and Install Software from Assertion Cloud

6.2.1. Register user in Assertion® SBC Security

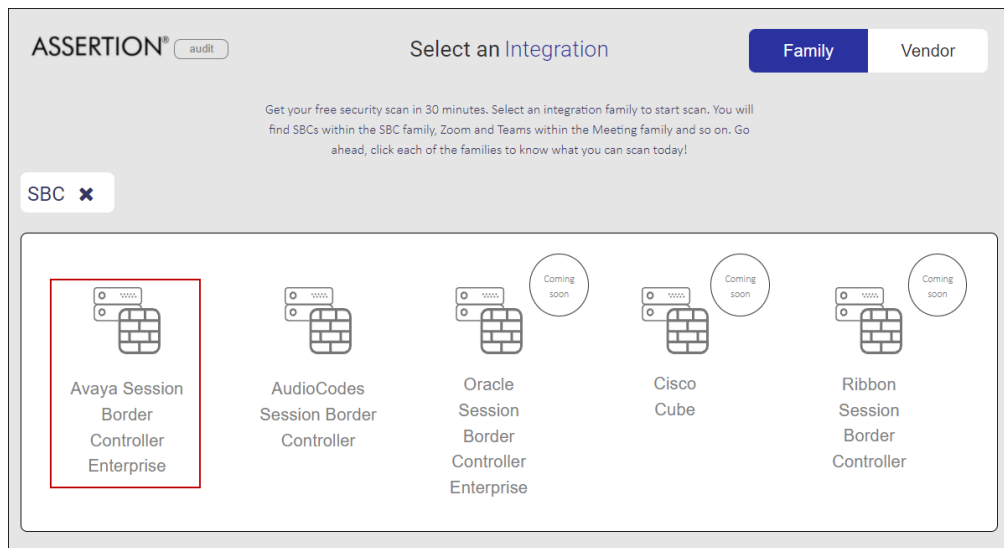
Open a browser on a local PC and navigate to <https://assertion.cloud>. Click **Login**.



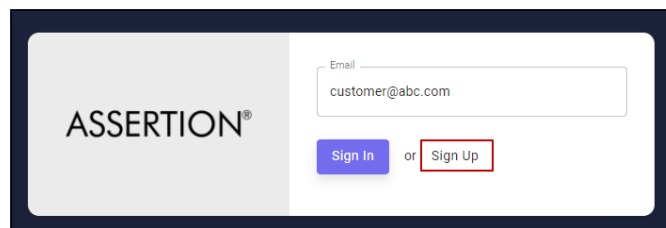
The user is directed to the landing page <https://scan.assertion.cloud>. Select **SBC** for Integration.



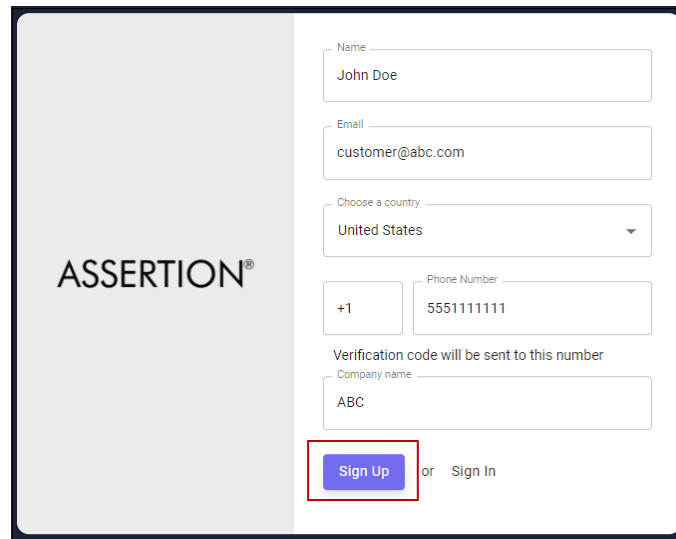
Select **Avaya Session Border Controller**:



On the next screen enter your corporate email and click **Sign Up**:



Enter the required information and click **Sign Up**.

A screenshot of a web form for signing up with Assertion. The form is titled "ASSERTION®" on the left. On the right, there are input fields for "Name" (John Doe), "Email" (customer@abc.com), "Choose a country" (United States), "Phone Number" (+1 5551111111), and "Company name" (ABC). Below these fields is a "Sign Up" button, which is highlighted with a red rectangle. To the right of the button is a link for "Sign In".

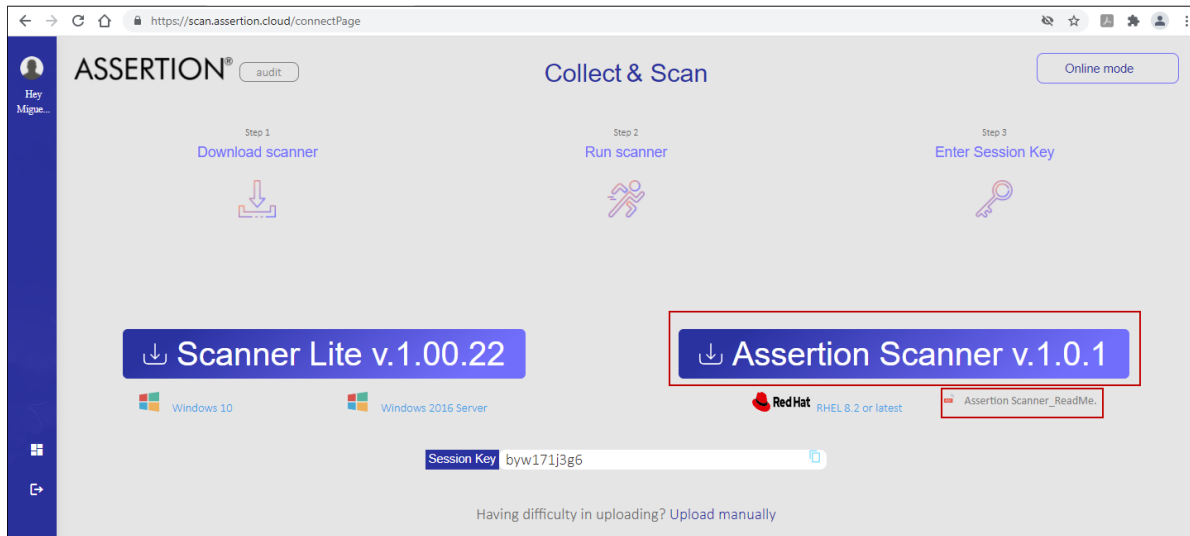
A pop up screen is presented where the user needs to enter a verification code (not shown). A verification code is sent to the email address and phone number specified above. Enter the verification code and click **Verify** to continue (not shown).

At this point the user is presented with information regarding how to purchase a subscription license from Assertion or its partners for real-time threat detection and monitoring of their SBC (not shown). Alternatively, the user can scan start a one-time scan using Scanner Lite and then purchase a one-time scan license from Assertion or its partner that will enable the detailed report.

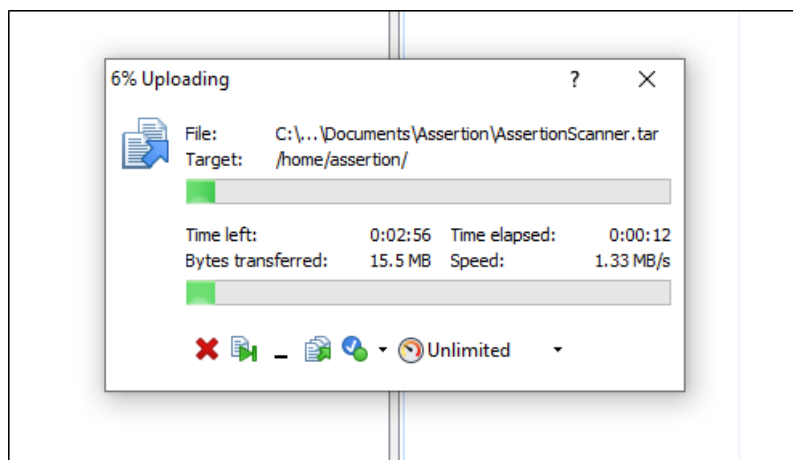
6.2.2. Download and Install Assertion® Scanner Software

Once the user is registered and verified, the **Collect & Scan** page is presented. Click the **Assertion Scanner Readme** link to download a pdf file with detailed and updated information on system requirements, installation instructions, etc.

Click **Assertion Scanner v.1.0.1** to download the software to the local PC.



Use WinSCP or a similar utility to copy the downloaded **AssertionScanner.tar** file to the `/home/assertion` folder on the Linux server



Login to the RHEL server using the user account previously created. Extract the file using the command:

- **tar -xvf AssertionScanner.tar**

```
assertion@rhel:~  
login as: assertion  
assertion@10.64.90.65's password:  
Activate the web console with: systemctl enable --now cockpit.socket  
  
This system is not registered to Red Hat Insights. See https://cloud.redhat.com/  
To register this system, run: insights-client --register  
  
Last login: Fri Nov 12 06:21:09 2021 from 192.168.120.5  
[assertion@rhel ~]$ pwd  
/home/assertion  
[assertion@rhel ~]$ ls -ltr  
total 257540  
-rw-rw-r--. 1 assertion assertion 263720960 Nov 15 05:05 AssertionScanner.tar  
[assertion@rhel ~]$ tar -xvf AssertionScanner.tar
```

The file is extracted and new folders are created. The installer file is located on the **deployment_scripts** folder.

```
[assertion@rhel ~]$ pwd  
/home/assertion  
[assertion@rhel ~]$ ls -ltr  
total 257540  
drwxr-xr-x. 6 assertion assertion 125 Nov 11 20:35 third_party  
-rw-rw-r--. 1 assertion assertion 263720960 Nov 15 05:05 AssertionScanner.tar  
drwxrwxr-x. 2 assertion assertion 94 Nov 15 05:15 deployment_scripts  
drwxr-xr-x. 5 assertion assertion 85 Nov 15 05:46 assertion-scanner  
[assertion@rhel ~]$
```

Enter the following commands:

- `cd /home/assertion/deployment_scripts`
- `./install_scanner.sh`

The installer asks to enter the scanner username. Enter the **assertion** username defined previously and press Enter.

```
[assertion@rhel ~]$ cd /home/assertion/deployment_scripts
[assertion@rhel deployment_scripts]$ ls -ltr
total 12
-rwxr-xr-x. 1 assertion assertion 3173 Nov  8 22:42 install_scanner.sh
-rwxr-xr-x. 1 assertion assertion 1332 Nov 15 06:15 add_device.sh
-rwxr-xr-x. 1 assertion assertion  818 Nov 15 06:15 schedule_config_log_collecti
on.sh
[assertion@rhel deployment_scripts]$ ./install_scanner.sh
-- Creating Assertion Scanner user
Enter Assertion scanner username: assertion
```

The installer proceeds with the installation. Verify that all the packages are installed and the process is completed without any errors. An “Installation Completed” message should be displayed at the end of the process.

```
Installing collected packages: pycryptodomex, pycparser, cffi, six, bcrypt, pynacl, cryptograp
hy, paramiko, jproperties, charset-normalizer, idna, urllib3, certifi, requests
WARNING: The script propconv is installed in '/usr/local/bin' which is not on PATH.
Consider adding this directory to PATH or, if you prefer to suppress this warning, use --no-
warn-script-location.
WARNING: The script normalizer is installed in '/usr/local/bin' which is not on PATH.
Consider adding this directory to PATH or, if you prefer to suppress this warning, use --no-
warn-script-location.
Successfully installed bcrypt-3.2.0 certifi-2021.10.8 cffi-1.15.0 charset-normalizer-2.0.7 cry
ptography-35.0.0 idna-3.3 jproperties-2.1.1 paramiko-2.8.0 pycparser-2.21 pycryptodomex-3.11.0
pynacl-1.4.0 requests-2.26.0 six-1.16.0 urllib3-1.26.7
warning: /home/assertion/third_party/web-driver-rpm/libdrm-2.4.103-1.el8.x86_64.rpm: Header V3
RSA/SHA256 Signature, key ID fd431d51: NOKEY
Verifying... ##### [100%]
Preparing... ##### [100%]
Updating / installing...
 1:libwayland-server-1.17.0-1.el8 ##### [ 20%]
 2:libpciaccess-0.14-1.el8 ##### [ 40%]
 3:libdrm-2.4.103-1.el8 ##### [ 60%]
 4:mesa-libgbm-20.3.3-2.el8 ##### [ 80%]
 5:libxshmfence-1.3-2.el8 ##### [100%]

Installation Completed
[assertion@rhel deployment_scripts]$
```


6.3. Add Avaya SBCE Device for Real Time Scanning

For this section, the user needs to be logged in as the registered user on the Assertion® SBC Security Cloud service at <https://assertion.cloud> web page. Navigate to the **SBC → Avaya Session Border Controller for Enterprise**. The **Collect & Scan** page is presented.

Once the Assertion® Scanner software is successfully installed, the next step is to add the Avaya SBCE that will be monitored and protected by the scanner.

On the RHEL server, navigate to the **assertion_scanner** folder to run the add device script.

Enter the following commands:

- **cd /home/assertion/assertion_scanner**
- **./add_device**

The **add_device** script executes and the user is prompted to enter the registered email address, configured in **Section 6.2**. A verification code is received on the above email address. Once the code is entered a “Verification successful” message is shown. The user is asked to enter the Session Key shown in the browser. This is found on the “Collect & Scan” page in the Assertion web page. Note that a new Session Key is generated every time this page is loaded.

```
[assertion@rhel ~]$ cd assertion-scanner
[assertion@rhel assertion-scanner]$ ls -ltr
total 4
drwxr-xr-x. 2 assertion assertion 37 Nov 9 02:57 DataCollector
drwxr-xr-x. 3 assertion assertion 45 Nov 11 20:25 log-collector
-rwxr-xr-x. 1 assertion assertion 1332 Nov 15 05:15 add_device.sh
[assertion@rhel assertion-scanner]$ ./add_device.sh
=====
ASBCE Data Scanner 1.00.22.18

Avaya SBCE Scanner Utility collects Security Configuration from EMS and logs from your selected SBC. Please keep your EMS Web Credentials (System Administrator) and SBC Shell Credentials handy.

Disclaimer

Third-party software and license information

Copyright Assertion
=====
Connecting to https://scanapi.assertion.cloud ...

Enter your registered Email ID : 
Please enter the Verification Code received on your email ID: 
Verification successful!
Please enter the session key shown in your browser: gbcij5karg
Verification successful!
Key verification successful !!

Collecting essential information ..

Waiting for input values .. Please follow the instructions on your browser.
```

Once the Session Key verification is completed, the scanner informs the user to input the next information on the browser. Do not close the scanner utility.

The Collect & Scan screen changes, prompting the user to enter the EMS IP address and the SSH and GUI credentials of the Avaya SBCE. Press **Connect** once completed.

ASSERTION® audit Collect & Scan Online mode

1 Element Management System (EMS) Access

EMS access credential

EMS IP

SSH access credential

SSH username

SSH password

GUI access credential

GUI username

GUI password

Note: The SSH and GUI credentials are not stored on Assertion servers.

2 Select a SBC Awaiting EMS connection Connect


The credentials are validated and next screen is presented. The SBC list is presented. In the reference configuration a single EMS-SBCE device named **SBCE8-90** was present. Select the device.

ASSERTION® audit Collect & Scan

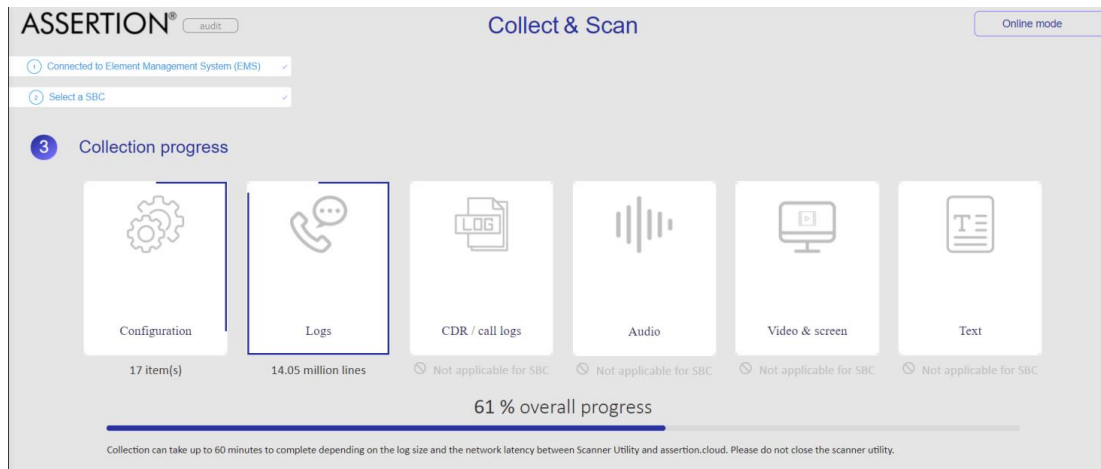
1 Connected to Element Management System (EMS) ✓

2 Select SBC

Select an SBC

 SBCE8-90
10.64.90.90

A screen showing the log collection and configuration collection progress is presented. The collection completes and the collected file is uploaded. Note that the collection process make take up to 60 minutes, depending upon the number of historical logs and the quality of the network connection. The user is informed that he will get a mail after the scan is completed.



Back at the scanner utility, the script completes the add-device process. The user is asked to press Enter to start the Real-time Log-Collection. The CRON job is started, the user is informed of the location where the scanner will store the logs collected from the SBCE, and the script exits.

```
Waiting for input values .. Please follow the instructions on your browser.
SBCE Version      : 8.1.3.0-31-21052
Done
Total objects to collect: 48

Waiting for input values .. Please follow instructions on your browser.
Adding sbc to inventory
Devices list sbcName=SBCE8-90,mgmtIP=10.64.90.90

You have selected SBCE8-90
Starting log collection (background)
  Start: Mon Nov 15 03:15:28 MST 2021 to End: Mon Nov 15 04:15:03 MST 2021
Upload of collected data is successful.
clean up ..
Cleaning up
Process complete. Press Enter to start the Real-time Log-Collection.

*/5 * * * * python3.8 /home/assertion/assertion-scanner/log-collector/scripts/collector/LogCollector.py -c /home/assertion/assertion-scanner/DataCollector -l /home/assertion/assertion-scanner/log-collector
0 22 * * * cd /home/assertion/assertion-scanner/DataCollector && java -cp /home/assertion/assertion-scanner/DataCollector/DataCollector-1.0.1.jar com.assertion.asbce.IncrementalScanner

Logs will be stored at /home/assertion/assertion-scanner/log-collector/logs directory

Process is completed
[assertion@rhel assertion-scanner]$
```

6.4. Summary Report

After the initial data collection is completed, a scan completion mail is sent to the user. Click the link sent in the mail to see the Summary Report.

Alternatively, the report can be seen by logging in to the Assertion® SBC Security web page, navigating to **SBC → Avaya Session Border Controller for Enterprise** and selecting the Dashboard icon on the left side panel of the screen.

Select **Real-time Scans** on the Dashboard. The SBC that is being monitored is shown, with information about the **Application** (Avaya Session Border Controller Enterprise), **SBC ID** (sbcname_IP-address), **Active Until** (Date until the license is active), **Status** (Online) and **Plan** (Real time).

Click the link under **SBC ID**.

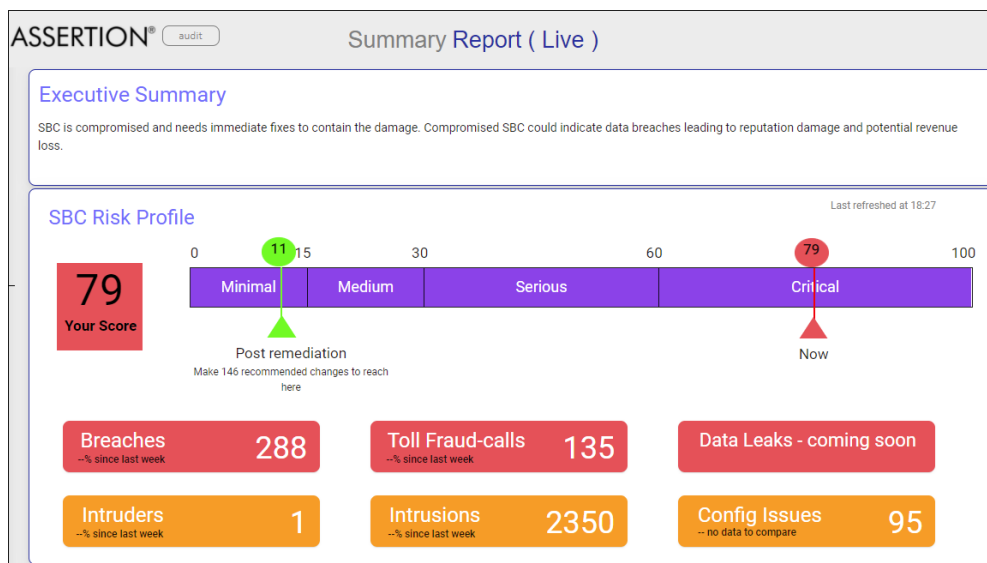
Your scan history				
One-Time Scans Real-time Scans				
Application	SBC ID	Active Until	Status	Plan
Avaya Session Border Controller Enterprise	SBCE8-90_10.64.90.90	14-Nov-2022	Online	Real Time Security
< page 1 of 1 >				

The information about the Real-Time Scan is displayed in a tabular format. In addition to the **Application** and **SBC ID**, the screen shows the **Scan ID** (real-time scan in progress), **When** (the date when the initial scan was initiated), **Risk Score** (real-time risk score) and **Detailed Report**, with the **View** button to see the Detailed Report. Click the link shown under **Scan ID**.

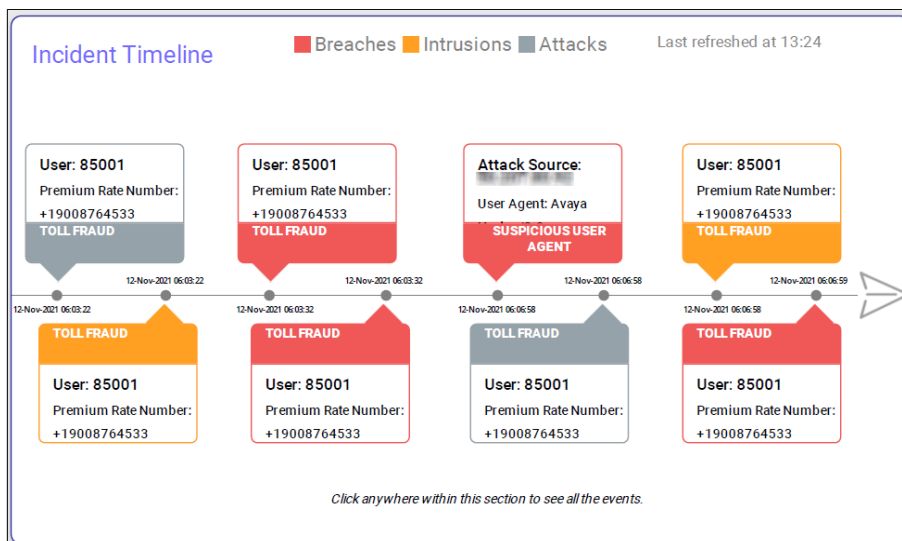
Application	SBC ID	Scan ID	When	Risk Score	Detailed Report
Avaya Session Border Controller Enterprise	SBCE8-90_10.64.90.90	scan-mkrgz2nh	15-Nov-2021	79	View

The Summary Report opens and the scan results are displayed.

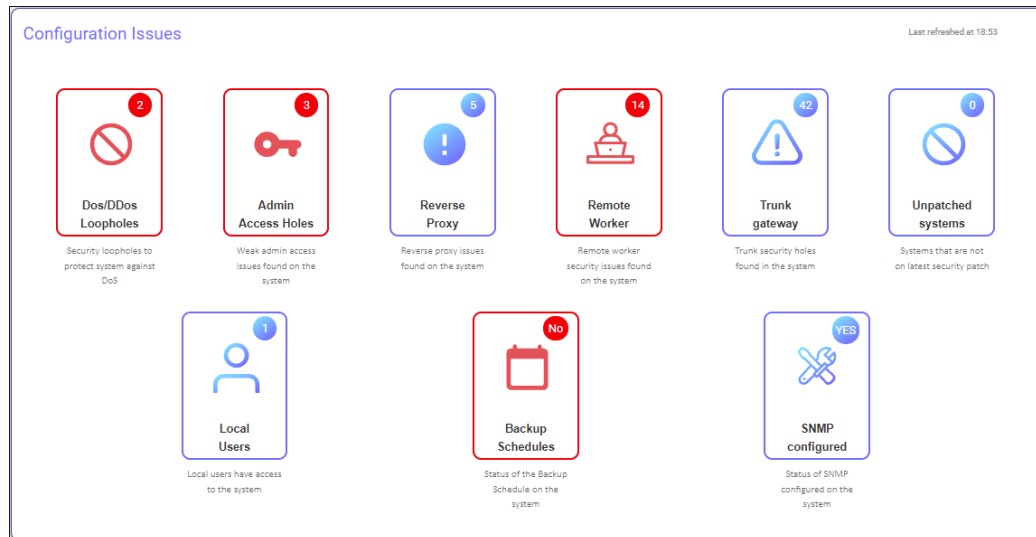
The Executive Summary at the top states the current status of the SBC. The SBC Risk Profile shows the current risk score and the criticality band. It shows the score that can be achieved after remediation measures are taken. The number of Breaches, Toll Fraud calls, Intrusions and Intruders detected are displayed. The number of configuration issues found on the system are listed.



The Incident Timeline shows the most recent occurrences of breaches, attacks or suspicious activities found on the Avaya SBCE.



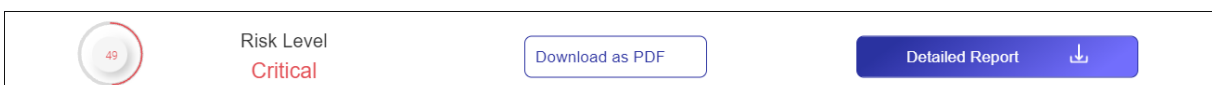
Configuration Issues found on the Avaya SBCE are listed.



Other sections of the Summary Report include:

- **Threat Origination**: shows the geographical locations from where the Breaches or Attacks have originated.
- **Cloud Posture**: shows the state of the public interfaces that are exposed to the Public Network.
- **User Scan Details**: shows the details of the scan, device that was scanned and the user who performed the scan.

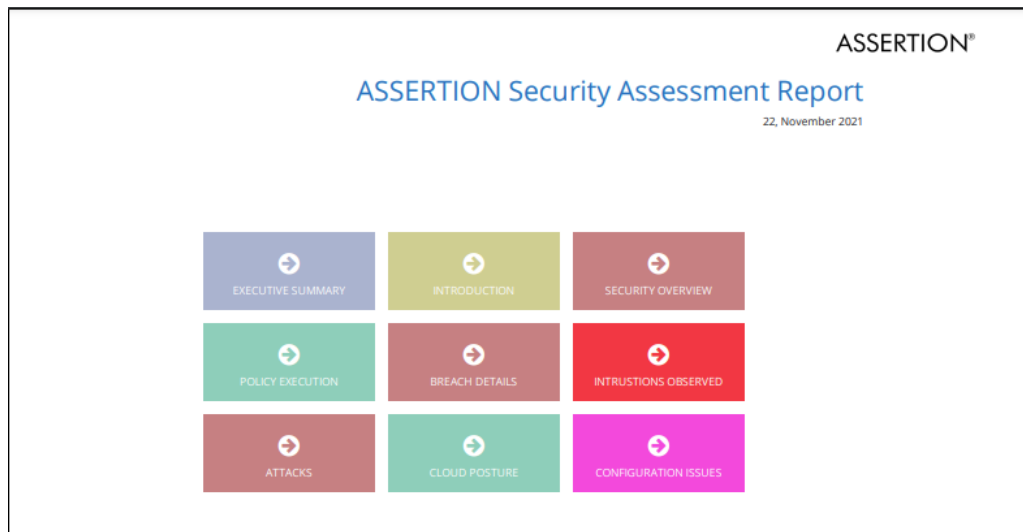
The taskbar at the bottom of the screen allows to download the report as a pdf document. It also contains a link to the Detailed Report.



6.5. Detailed Report

The Report can be obtained by clicking the Detailed Report link on the taskbar at the bottom of the Summary Report.

The Detailed Report contains all the findings for Breaches, Attacks, Potential Attacks, Cloud Posture and Configuration Issues that were found. It provides specific information regarding the origin and nature of the threats, file locations with evidence, as well as specific configuration recommendations to improve the SBC security posture. Click the links shown on the screen to navigate to a specific section of the report.



The screen below shows one of the examples in the report on the **Breach Details** section. Some of the details include IP address of the suspicious source, specific log file with the evidence, etc.

Check : Detect Breach by successful registration from suspected IP address Threat level : High				
Remote User	Suspicious SourceIP	Instance	Date & Time	Evidence
50235	[REDACTED]	29	11-06-2021 06:34:51	tracesbc_sip_1636200893_1636204467_1.gz
50237	[REDACTED]	3	10-05-2021 06:14:42	tracesbc_sip_1633432557_1633436147_1.gz
50287	[REDACTED]	2	10-06-2021 13:23:23	tracesbc_sip_1633547769_1633551349_1.gz
685678	[REDACTED]	481	11-22-2021 08:36:06	tracesbc_sip_1637594139_1637595617.gz
85001	[REDACTED]	485	11-19-2021 07:22:13	tracesbc_sip_1637331334_1637331916.gz
85004	[REDACTED]	2	10-07-2021 09:19:18	tracesbc_sip_1633619771_1633623350_1.gz
89324	[REDACTED]	461	11-09-2021 10:18:57	tracesbc_sip_1636478096_1636481680_1.gz
89327	[REDACTED]	951	11-05-2021 13:59:24	tracesbc_sip_1636139693_1636143256_1.gz
Risk category: Remote Worker Security			Security Policy: Registrations from Known Suspicious Subnets	
Impact / Fallout: User impersonation leading to enterprise fraud			Violation : Restrict registration from unknown network	
Description : Detect successful registrations from suspicious activity sources				

The **Configuration Issues** section (not shown) contains **Security Configuration Holes** detected, with specific recommendations for changes in the Avaya SBCE for remediation of these vulnerabilities.

Note: Data collection for the Avaya SBCE configuration occurs once every 24 hours, usually late in the evening. Changes made to the configuration are reflected on the Detailed Report and the SBC Risk Profile only after the next configuration data is collected.

7. Verification Steps

This section provides verification steps that may be performed in the field to verify that the solution is configured properly.

7.1. Assertion® Scanner Log Data Collection Verification

Verify the Avaya SBCE log data is being collected by the Assertion® Scanner.

- Login to the scanner. Navigate to the `/home/assertion/assertion-scanner/log-collector/logs` folder.

A folder should have been automatically created here during the “add.device” installation script process, with the IP-address of the added device. (**10.64.90.90** in the reference configuration).

- Navigate to folder `<SBCE-IP>/tar`. In the example below, this is `cd /10.64.90.90/tar`.
- Enter `ls -ltr`.

```
[assertion@rhel 10.64.90.90]$ cd /home/assertion/assertion-scanner/log-collector/logs
[assertion@rhel logs]$ ls -ltr
total 0
drwxr-xr-x. 8 assertion assertion 114 Nov 15 06:50 10.64.90.90
[assertion@rhel logs]$ cd 10.64.90.90/tar
[assertion@rhel tar]$ ls -ltr
total 92
-rw-r--r--. 1 assertion assertion 46428 Nov 22 07:20 lastRolledOverTarFile.tar.gz
-rw-r--r--. 1 assertion assertion 33427 Nov 22 07:55 currentTarFile.tar.gz
[assertion@rhel tar]$
```

The **currentTarFile.tar.gz** log file is present. Note that if the Avaya SBCE has rolled over files, then **lastRolledOverTarFile.tar.gz** is also present.

Enter the command below to look at the most recent messages captured by the scanner.

- `zcat currentTarFile.tar.gz |more` or

Note: The scanner polls the Avaya SBCE logs and updates the file with new data every 5 minutes.

SSH into the Avaya SBCE. Navigate to the folder `/archive/log/tracesbc/tracesbc_sip`. Use the command `ls -ltr` to check the latest live file. In the example below corresponding to the reference configuration, that file is **tracesbc_sip_1637590539**.

```

ipcs@SBCE8-90:/archive/log/tracesbc/tracesbc_sip
-rw-rw----+ 1 sbcd sbcd 44227 Nov 21 16:15 tracesbc_sip_1637532938_1637536515_1.gz
-rw-rw----+ 1 sbcd sbcd 48999 Nov 21 17:15 tracesbc_sip_1637536538_1637540137_1.gz
-rw-rw----+ 1 sbcd sbcd 50805 Nov 21 18:15 tracesbc_sip_1637540138_1637543737_1.gz
-rw-rw----+ 1 sbcd sbcd 51057 Nov 21 19:15 tracesbc_sip_1637543738_1637547325_1.gz
-rw-rw----+ 1 sbcd sbcd 49915 Nov 21 20:15 tracesbc_sip_1637547338_1637550924_1.gz
-rw-rw----+ 1 sbcd sbcd 44015 Nov 22 00:15 tracesbc_sip_1637561739_1637565337_1.gz
-rw-rw----+ 1 sbcd sbcd 44140 Nov 22 01:15 tracesbc_sip_1637565339_1637568916_1.gz
-rw-rw----+ 1 sbcd sbcd 44384 Nov 22 02:15 tracesbc_sip_1637568939_1637572516_1.gz
-rw-rw----+ 1 sbcd sbcd 44417 Nov 22 03:15 tracesbc_sip_1637572539_1637576116_1.gz
-rw-rw----+ 1 sbcd sbcd 44353 Nov 22 04:15 tracesbc_sip_1637576139_1637579716_1.gz
-rw-rw----+ 1 sbcd sbcd 44252 Nov 22 05:15 tracesbc_sip_1637579739_1637583317_1.gz
-rw-rw----+ 1 sbcd sbcd 46354 Nov 22 06:15 tracesbc_sip_1637583339_1637586920_1.gz
-rw-rw----+ 1 sbcd sbcd 50911 Nov 22 07:15 tracesbc_sip_1637586939_1637590528_1.gz
-rwx-----+ 1 sbcd sbcd 20480 Nov 22 08:01 tracesbc_sip_pl_active_clients_2
-rwx-----+ 1 sbcd sbcd 9375744 Nov 22 08:01 tracesbc_sip_l5_513
-rw-rw----+ 1 sbcd sbcd 472625 Nov 22 08:01 tracesbc_sip_1637590539
[ipcs@SBCE8-90 tracesbc_sip]$

```

Enter the command **tracesbc** <tracesbc_sip_xxxxxxxx> using the appropriate file name for the system.

Verify that the same messages are present in the “tracesbc_sip_...” file on the Avaya SBCE and on the “currentTarFile.tar.gz” in the Assertion® Scanner. The same messages should be present on both the devices. Note that there may be a lag of 2 to 5 minutes for the scanner to show the same message.

7.2. Assertion® Scanner Configuration Data Collection Verification

The Avaya SBCE configuration data is collected by the Assertion® Scanner every 24 hours after the initial scan. Navigate to the `/home/assertion/assertion-scanner/DataCollector` folder and verify the zip files with the SBCE name and address are being captured daily.

```

Last login: Mon Nov 22 08:14:23 2021 from 192.168.120.29
[assertion@rhel ~]$ cd /home/assertion/assertion-scanner/DataCollector
[assertion@rhel DataCollector]$ ls -ltr
total 166164
-rwxr-xr-x. 1 assertion assertion 124649693 Nov 9 03:40 DataCollector-1.0.1.jar
drwxrwxr-x. 7 assertion assertion 4096 Nov 15 06:21 chrome-linux
-rw-rw-r--. 1 assertion assertion 44894832 Nov 15 06:46 SBCE8-90_10.64.90.90_1636978912413.zip
drwxrwxr-x. 2 assertion assertion 70 Nov 15 06:46 jobs-ds
-rw-r--r--. 1 assertion assertion 64736 Nov 15 23:24 SBCE8-90_10.64.90.90_1637038804792.zip
-rw-r--r--. 1 assertion assertion 65792 Nov 16 23:25 SBCE8-90_10.64.90.90_1637125205575.zip
-rw-r--r--. 1 assertion assertion 65520 Nov 17 23:25 SBCE8-90_10.64.90.90_1637211604362.zip
-rw-r--r--. 1 assertion assertion 65696 Nov 18 23:25 SBCE8-90_10.64.90.90_1637298003958.zip
drwxrwxr-x. 2 assertion assertion 133 Nov 18 23:25 config
-rw-r--r--. 1 assertion assertion 65696 Nov 19 23:25 SBCE8-90_10.64.90.90_1637384404637.zip
-rw-r--r--. 1 assertion assertion 65664 Nov 20 23:25 SBCE8-90_10.64.90.90_1637470804778.zip
drwxrwxr-x. 2 assertion assertion 4096 Nov 21 23:00 logs
-rw-rw-r--. 1 assertion assertion 151 Nov 21 23:00 stderr.out
-rw-rw-r--. 1 assertion assertion 103005 Nov 21 23:25 CollectedData.json
drwxrwxr-x. 2 assertion assertion 4096 Nov 21 23:25 backups
-rw-r--r--. 1 assertion assertion 65872 Nov 21 23:25 SBCE8-90_10.64.90.90_1637557204769.zip
drwxrwxr-x. 2 assertion assertion 6 Nov 21 23:26 Driver
[assertion@rhel DataCollector]$

```

7.3. Verify Connectivity to Assertion® Cloud

Verify that the Assertion® Scanner is able to resolve the IP address of the Assertion® SBC Security Cloud service, and it can reach the service using port 443 over the public Internet.

The command below can be run on the RHEL server where Assertion® Scanner is installed. This is useful when trying to validate local networking and firewall configuration.

- **curl -v telnet://scan.assertion.cloud:443**

The command should return a line stating that the server is connected, with the IP address and port used, as show on the screen below:

```
login as: assertion
assertion@10.64.90.65's password:
Activate the web console with: systemctl enable --now cockpit.socket

This system is not registered to Red Hat Insights. See https://cloud.redhat.com/
To register this system, run: insights-client --register

Last login: Mon Nov 22 07:42:00 2021 from 192.168.120.29
[assertion@rhel ~]$ curl -v telnet://scan.assertion.cloud:443
* Rebuilt URL to: telnet://scan.assertion.cloud:443/
* Trying 10.64.90.125...
* TCP_NODELAY set
* Connected to scan.assertion.cloud (10.64.90.125) port 443 (#0)
```

Press **Ctrl+C** to cancel the command.

8. Conclusion

The sample configuration presented in these Application Notes describe the procedures necessary for Assertion® SBC Security to interoperate with Avaya Session Border Controller for Enterprise 8.1.3.

Testing was performed to verify the functionality described in **Section 0**. All test cases completed successfully.

9. Additional References

Avaya product documents can be obtained from <https://support.avaya.com/>:

- [1] *Administering Avaya Session Border Controller for Enterprise*, Release 8.1.x, August 2021
- [2] *Maintaining and Troubleshooting Avaya Session Border Controller for Enterprise*, Release 8.1.x., December 2020
- [3] *Avaya SBCE 8.1 Security Configuration and Best Practices Guide*, Release 8.1, February 2020

Assertion:

- [4] <https://assertion.cloud/sbc/>
- [5] <https://assertion.cloud/sbc/attacks/>
- [6] <https://assertion.cloud/blog/>

©2021 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 Solution & Interoperability Test Lab at interopnotesdl@avaya.com