



## Avaya Solution & Interoperability Test Lab

---

# Application Notes for Dizzion DaaS Complete with Avaya Workplace Client for Windows – Issue 1.0

### Abstract

These Application Notes describe the configuration steps required for Dizzion DaaS Complete to interoperate with Avaya Workplace Client for Windows. Dizzion DaaS Complete is a virtual desktop infrastructure solution that can be used by remote workers for contact centers.

In the compliance testing, remote workers on the internet used Dizzion DaaS Complete virtual desktops running Avaya Workplace Client for Windows. The remote workers registered and logged in as SIP agents to Avaya Aura® Session Manager and Avaya Aura® Communication Manager and handled ACD calls via the public interface of 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

These Application Notes describe the configuration steps required for Dizzion DaaS Complete (DaaS) with Avaya Workplace Client for Windows (Workplace). DaaS is a Virtual Desktop Infrastructure (VDI) solution that can be used by remote workers for contact centers.

In the compliance testing, remote workers on the internet used DaaS with Workplace running on each virtual desktop. The remote workers registered and logged in as SIP agents to Avaya Aura® Session Manager and Avaya Aura® Communication Manager and handled ACD calls via the public interface of Avaya Session Border Controller for Enterprise (SBCE).

Avaya support for VDI solutions requires that the audio stream be outside the VDI path. If a customer implements a solution where the audio is delivered through the VDI path and encounters issues including audio degradation, it is the responsibility of the customer and the VDI vendor to troubleshoot and resolve the issue. Avaya will only accept support tickets when the issue can be reproduced in a supported environment outside of the VDI.

## 2. General Test Approach and Test Results

The feature test cases were performed manually. Incoming ACD calls were placed from the PSTN and answered by remote workers logged in as agents via Workplace on DaaS. All call control actions were initiated via Workplace.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to the agent's home PC.

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 this Application Note, the interface between Avaya systems and DaaS used encrypted connections.

## 2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following for Workplace on DaaS with all traffic flowed through the SBCE:

- Use of HTTPS to obtain Workplace settings file from file server.
- Use of HTTPS to obtain Workplace license from license server.
- Use of HTTPS, TLS, and SRTP to download PPM data, register, and control calls with Session Manager.
- Call scenarios including login/logout, change work modes, pending aux work, inbound, outbound, internal, external, ACD, non-ACD, screen pop, drop, hold/resume, blind/attended transfer, attended conference, multiple agents, multiple calls, long duration, RONA, q-stats, supervisor assist, and service observing.
- Subjective assessment on audio quality with generation and monitor of Workplace Call Statistics of an active call.

The serviceability test cases were performed by disconnecting/reconnecting the Ethernet connection to the agent's home PC and disconnecting/reconnecting the remote connection to DaaS for various durations to verify user Workplace configuration data persistence.

## 2.2. Test Results

All test cases were executed, and the following is an observation on DaaS:

- A User Profile Management policy is required on DaaS for user Workplace configuration data to persist. Without such policy, agents will need to enter his/her station and agent credentials upon each access, even when the next access is five minutes later with credentials configured to be memorized. The policy requirement can be specified on the Dizzion order form with the user AppData settings needing to persist.
- An audio degradation was experienced during a call with an agent having multiple active and content heavy web pages, but the issue was not reproducible at will.

## 2.3. Support

Technical support on DaaS can be obtained through the following:

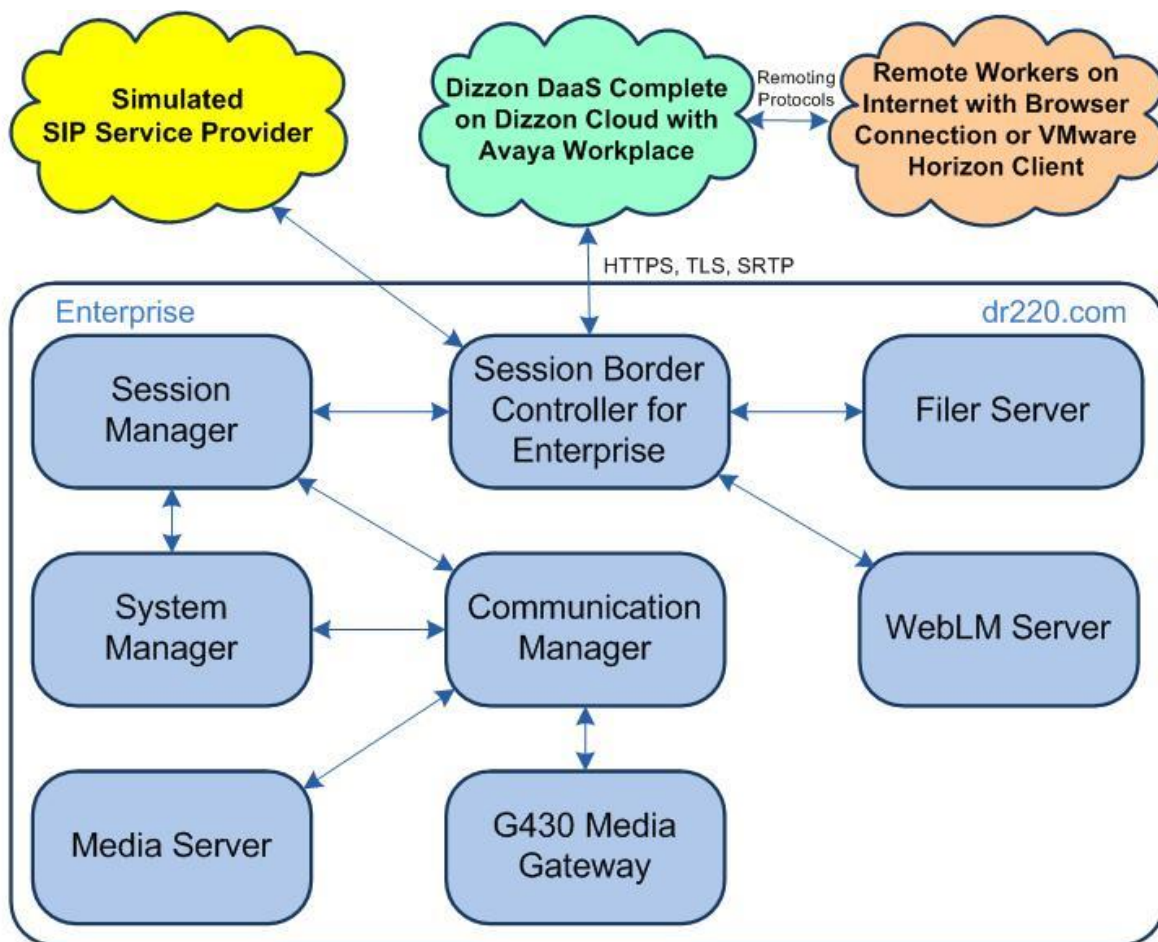
- **Phone:** (888) 225-2974, option 2
- **Email:** [support@dizzion.com](mailto:support@dizzion.com)
- **Web :** <https://mysupport.dizzion.com>

### 3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**. The administration of basic configuration and routing between Communication Manager, Session Manager, SBCE, and of contact center devices are not the focus of these Application Notes and will not be described.

These Application Notes assume agents using Workplace with encrypted connections are already configured and working from within the enterprise, and that the focus is on the additional configuration needed to allow agents to use Workplace on DaaS to connect via SBCE as remote workers. The compliance testing used two agents and one supervisor shown in table below.

Device Type	Extension/Password
Supervisor Station	66006/123456
Agent Station	66008 /234567, 66009/345678
Agent ID	65888/65888, 65889/65889



**Figure 1: Compliance Testing Configuration**

## 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager in Virtual Environment	8.1.3.4 (8.1.3.4.0.890.27348)
Avaya G430 Media Gateway	41.34.4
Avaya Aura® Media Server in Virtual Environment	8.0.2.218
Avaya Aura® Application Enablement Services in Virtual Environment	8.1.3.4 (8.1.3.4.0.2-0)
Avaya Aura® Session Manager in Virtual Environment	8.1.3.4 (8.1.3.4.813401)
Avaya Aura® System Manager in Virtual Environment	8.1.3.4 (8.1.3.4.1014355)
Avaya Session Border Controller for Enterprise in Virtual Environment	8.1.3.1 (8.1.3.1-38-21632)
Agent Home PC with Windows 10 <ul style="list-style-type: none"><li>VMware Horizon Client</li></ul>	Pro 8.6.0.29364
Virtual Desktop with Windows 10 Enterprise on Dizzion CaaS Complete <ul style="list-style-type: none"><li>Avaya Workplace Client for Windows</li></ul>	NA NA 3.29.0.54

## 5. Configure Avaya Session Border Controller for Enterprise

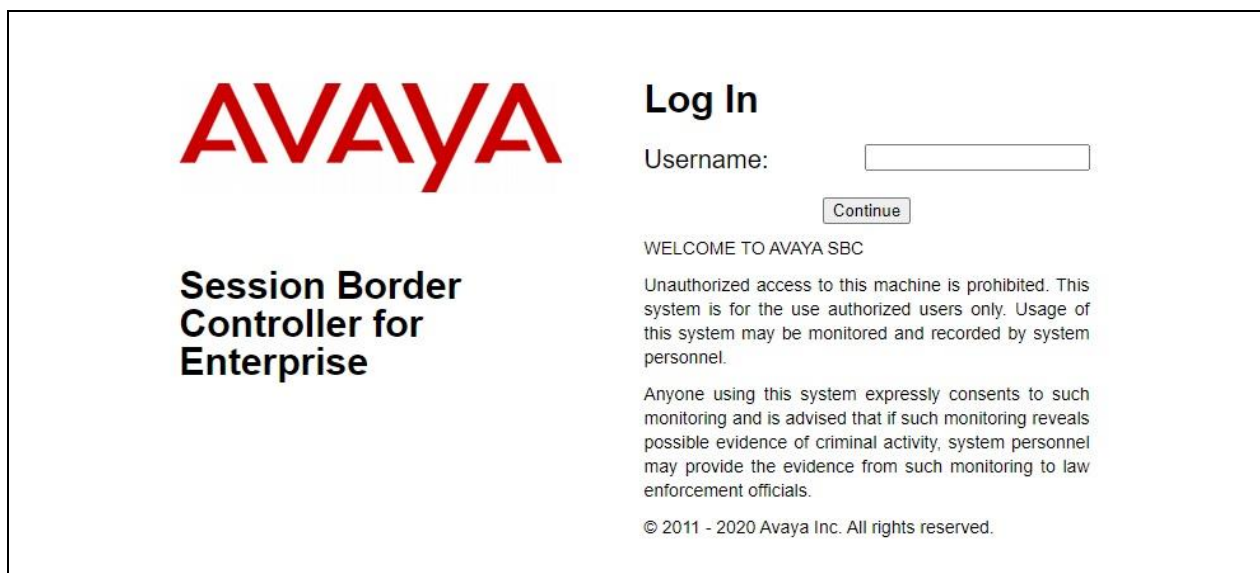
This section provides the procedures for configuring SBCE to allow connection from remote workers. The procedures include the following areas:

- Launch web interface
- Administer network management
- Generate certificate signing requests
- Install certificates
- Administer client profiles
- Administer server profiles
- Administer media rule
- Administer end point policy groups
- Administer media interface
- Administer signaling interface
- Administer user agents
- Administer subscriber flows
- Administer server flows
- Administer PPM mapping
- Administer reverse proxy

These Application Notes assume that connectivity between SBCE and Session Manager is already in place with use of TLS for encrypted connection.

### 5.1. Launch Web Interface

Access the SBCE web interface by using the URL **https://ip-address/sbc** in an Internet browser window, where **ip-address** is the IP address of the SBCE management interface. The screen below is displayed. Log in using the appropriate credentials.



The image shows the login page of the Avaya Session Border Controller for Enterprise. On the left, there is a large red 'AVAYA' logo and the text 'Session Border Controller for Enterprise' in black. On the right, under the heading 'Log In', there is a 'Username:' label followed by a text input field. Below the input field is a 'Continue' button. Further down, there is a 'WELCOME TO AVAYA SBC' message, followed by a disclaimer: '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.' Below this is a consent statement: '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.' At the bottom, it says '© 2011 - 2020 Avaya Inc. All rights reserved.'

## 5.2. Administer Network Management

In the subsequent screen, select **Device** → **SBCE** from the top menu, followed by **Backup/Restore** → **Network & Flows** → **Network Management** from the left pane to display the **Network Management** screen. Select the **Networks** tab and determine the interfaces to use for remote worker. Enable new interface and/or add new IP address to an existing interface as necessary.

In the compliance testing, two interfaces below are used for remote worker traffic.

- **10.64.101.222**: IP address of private **A1** interface for remote worker traffic.
- **50.50.50.50**: Masked IP address of public **B2** interface for remote worker traffic.

Note that the remote worker traffic included the following in the compliance testing:

- TLS and SRTP for SIP registration and calls with Session Manager.
- HTTPS for file transfer with file server.
- HTTPS for Personal Profile Manager (PPM) download with Session Manager.
- HTTPS for license obtainment with WebLM server.

The screenshot shows the Avaya Session Border Controller for Enterprise (SBCE) Network Management interface. The top navigation bar includes 'Device: SBCE', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The left sidebar lists various management options, with 'Network & Flows' and 'Network Management' highlighted. The main content area displays the 'Networks' tab, which contains a table of network configurations. The table has columns for Name, Gateway, Subnet Mask / Prefix Length, Interface, and IP Address. Three networks are listed: Private-A1, Public-B1, and Public-B2. The IP addresses for Private-A1 (10.64.101.222) and Public-B2 (50.50.50.50) are highlighted with red boxes. Each row also includes 'Edit' and 'Delete' buttons.

Name	Gateway	Subnet Mask / Prefix Length	Interface	IP Address	
Private-A1	10.64.101.1	255.255.255.0	A1	10.64.101.222	Edit Delete
Public-B1	10.64.102.1	255.255.255.0	B1	10.64.102.221, 10.64.102.222	Edit Delete
Public-B2	50.50.50.1	255.255.255.0	B2	50.50.50.50	Edit Delete



### 5.3. Generate Certificate Signing Requests

Select **Backup/Restore** → **TLS Management** → **Certificates** from the left pane to display existing certificates. Click **Generate CSR** to add a certificate signing request for each remote worker interface from **Section 5.2**.

The **Generate CSR** pop-up screen is displayed. Enter pertinent values for **Country Name**, **State/Province Name**, **Locality Name**, **Organization Name**, **Organization Unit**, **Contact Name**, and **Contact E-Mail**.

Enter desired values for **Common Name**, **Passphrase**, and **Confirm Passphrase** for the private interface for remote worker traffic.

For **Subject Alt Name**, enter the IP addresses and DNS name for the private interface used for remote worker. In the compliance testing, **IP:10.64.101.221,IP:10.64.101.222,DNS:dr220.com** was used. Note that all IP addresses associated with the interface need to be included.

Select **Generate CSR** followed by **Download** (not shown) in the subsequent screen to download the certificate signing request.

The screenshot shows the 'Generate CSR' pop-up screen in the Avaya Session Border Controller interface. The background shows the 'Session Border Controller' dashboard with a left-hand navigation menu. The 'Generate CSR' pop-up is a modal window with the following fields and values:

Field	Value
Country Name	US
State/Province Name	NJ
Locality Name	Morristown
Organization Name	Avaya
Organizational Unit	DevConnect
Common Name	sbceA1
Algorithm	SHA256
Key Size (Modulus Length)	2048 bits
Key Usage Extension(s)	<input checked="" type="checkbox"/> Key Encipherment <input checked="" type="checkbox"/> Non-Repudiation <input checked="" type="checkbox"/> Digital Signature
Extended Key Usage	<input checked="" type="checkbox"/> Server Authentication <input checked="" type="checkbox"/> Client Authentication
Subject Alt Name	IP:10.64.101.221,IP:10.64.101.222,DNS:dr220.com
Passphrase	*****
Confirm Passphrase	*****
Contact Name	tit
Contact E-Mail	tit@dr220.com

At the bottom of the pop-up, there is a 'Generate CSR' button.



Repeat the procedure to add a certificate signing request for the public interface for remote worker traffic.

For **Subject Alt Name**, enter the IP addresses and DNS name for the public interface used for remote worker. In the compliance testing, **IP:50.50.50.50,DNS:dr220.com** was used.

The screenshot shows the 'Generate CSR' dialog box in the Avaya Session Border Controller (SBCE) configuration interface. The dialog is titled 'Generate CSR' and has a close button (X) in the top right corner. The background shows the SBCE configuration page with a sidebar menu on the left and a main content area on the right. The sidebar menu includes options like EMS Dashboard, Software Management, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management, Certificates, Client Profiles, Server Profiles, SNI Group, Network & Flows, DMZ Services, and Monitoring & Logging. The main content area shows the 'Generate CSR' dialog box with the following fields and values:

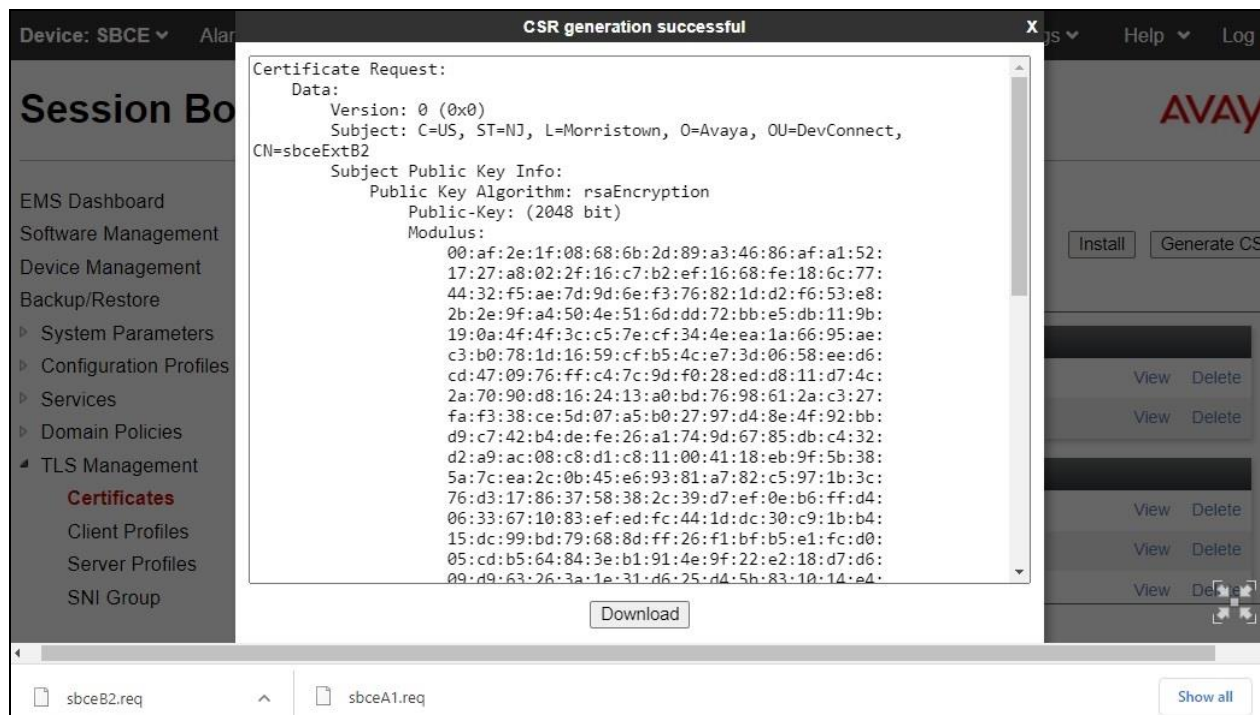
- Country Name: US
- State/Province Name: NJ
- Locality Name: Morristown
- Organization Name: Avaya
- Organizational Unit: DevConnect
- Common Name: sbceB2
- Algorithm: SHA256
- Key Size (Modulus Length): 2048 bits
- Key Usage Extension(s): Key Encipherment, Non-Repudiation, Digital Signature
- Extended Key Usage: Server Authentication, Client Authentication
- Subject Alt Name: IP:50.50.50.50,DNS:dr220.com
- Passphrase: \*\*\*\*\*
- Confirm Passphrase: \*\*\*\*\*
- Contact Name: tlt
- Contact E-Mail: tlt@dr220.com

A 'Generate CSR' button is located at the bottom right of the dialog box.

The **CSR generation successful** pop-up screen is displayed next. Click **Download** to download the certificate signing request.

Send the two downloaded certificate signing requests **sbceA1.req** and **sbceB2.req** shown below to the Certificate Authority (CA) for signing.

In the compliance testing, the System Manager was used as the CA and see **Section 6** for sample generation of signed identity certificates and obtainment of CA certificate.



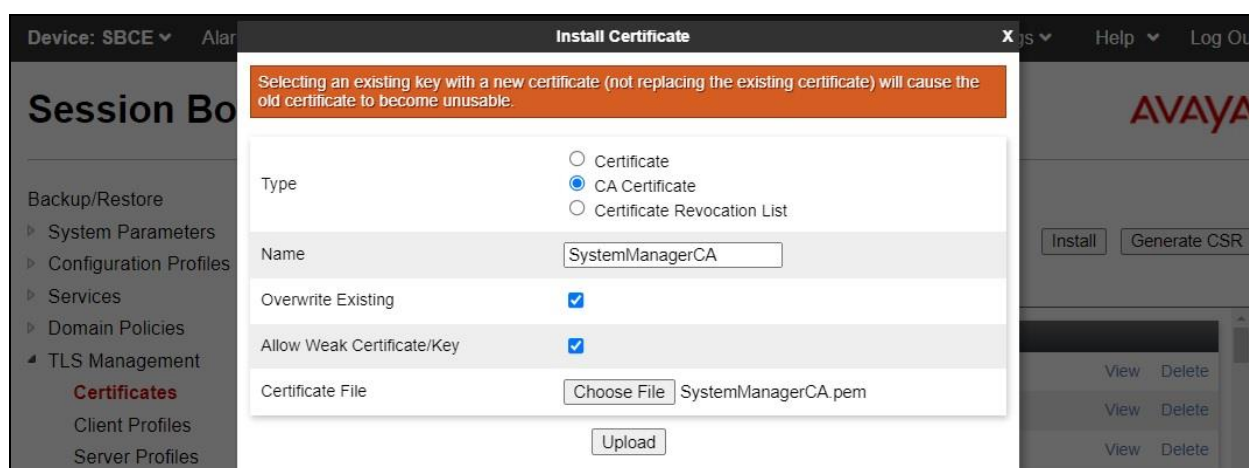
## 5.4. Install Certificates

After obtainment of CA certificate and identity certificates for the private and public SBCE interfaces from **Section 6**, proceed with this section to install the certificates.

Select **Backup/Restore** → **TLS Management** → **Certificates** from the left pane followed by **Install** to display the **Install Certificate** pop-up screen.

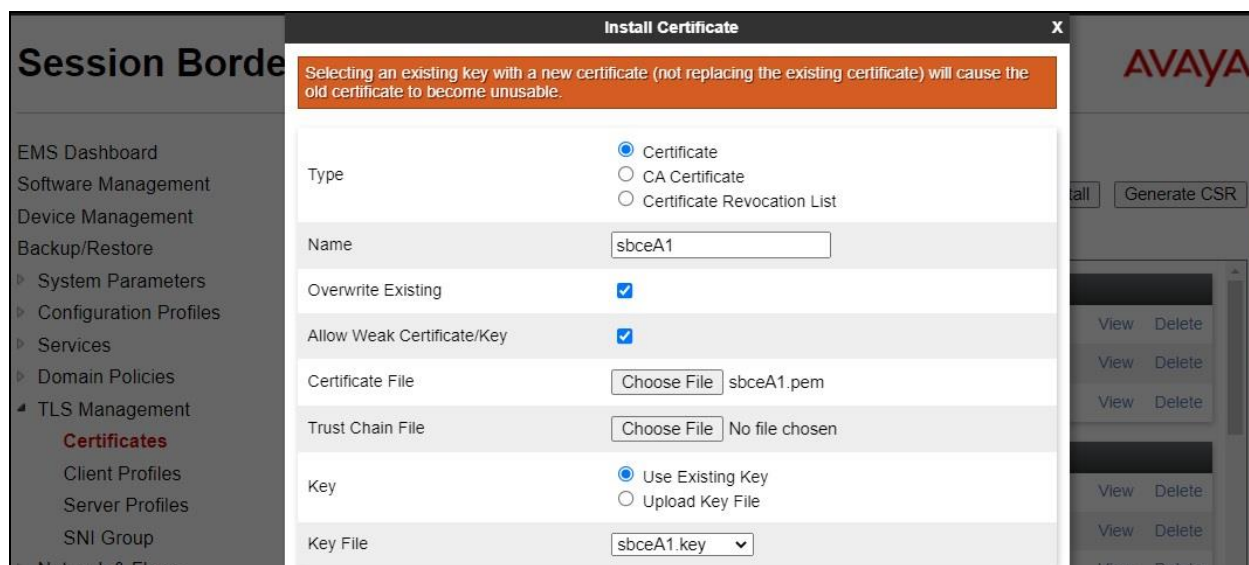
Set the parameters as shown below where **SystemManagerCA** is the desired name for the CA certificate and **SystemManagerCA.pem** is the downloaded CA certificate file from **Section 6.4**.

Click **Upload** followed by **Install** (not shown) in the subsequent screen to install the certificate.



The screenshot shows the 'Install Certificate' dialog box. At the top, a warning message states: 'Selecting an existing key with a new certificate (not replacing the existing certificate) will cause the old certificate to become unusable.' The 'Type' is set to 'CA Certificate'. The 'Name' field contains 'SystemManagerCA'. The 'Overwrite Existing' checkbox is checked. The 'Allow Weak Certificate/Key' checkbox is checked. The 'Certificate File' field shows 'SystemManagerCA.pem' with a 'Choose File' button. An 'Upload' button is at the bottom.

Repeat the procedure to install the identity certificate for the SBCE private interface as shown below where **sbceA1** is desired name for the certificate, **sbceA1.pem** is the associated certificate file from **Section 6.3**, and **sbceA1.key** is the auto generated key associated with the interface.



The screenshot shows the 'Install Certificate' dialog box. At the top, a warning message states: 'Selecting an existing key with a new certificate (not replacing the existing certificate) will cause the old certificate to become unusable.' The 'Type' is set to 'Certificate'. The 'Name' field contains 'sbceA1'. The 'Overwrite Existing' checkbox is checked. The 'Allow Weak Certificate/Key' checkbox is checked. The 'Certificate File' field shows 'sbceA1.pem' with a 'Choose File' button. The 'Trust Chain File' field shows 'No file chosen' with a 'Choose File' button. The 'Key' is set to 'Use Existing Key'. The 'Key File' field shows 'sbceA1.key' with a dropdown arrow.

Repeat the procedure to install the identity certificate for the SBCE public interface where **sbceB2** is desired name for the certificate, **sbceB2.pem** is the associated certificate file from **Section 6.3**, and **sbceB2.key** is the auto generated key associated with the interface.

The screenshot displays the Avaya Session Border Controller (SBCE) web interface. The top navigation bar includes links for Device: SBCE, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The left sidebar shows a menu with categories like EMS Dashboard, Software Management, Device Management, Backup/Restore, System Parameters, Configuration Profiles, Services, Domain Policies, TLS Management, Certificates, Client Profiles, Server Profiles, SNI Group, Network & Flows, DMZ Services, and Monitoring & Logging. The main content area is titled 'Install Certificate' and features a warning message: 'Selecting an existing key with a new certificate (not replacing the existing certificate) will cause the old certificate to become unusable.' Below the warning, the form includes fields for Type (Certificate selected), Name (sbceB2), Overwrite Existing (checked), Allow Weak Certificate/Key (checked), Certificate File (sbceB2.pem), Trust Chain File (No file chosen), Key (Use Existing Key selected), and Key File (sbceB2.key). An 'Upload' button is at the bottom of the form. The background shows a list of certificates with 'View' and 'Delete' actions.

Type	Name	Overwrite Existing	Allow Weak Certificate/Key	Certificate File	Trust Chain File	Key	Key File
<input checked="" type="radio"/> Certificate <input type="radio"/> CA Certificate <input type="radio"/> Certificate Revocation List	sbceB2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Choose File sbceB2.pem	Choose File No file chosen	<input checked="" type="radio"/> Use Existing Key <input type="radio"/> Upload Key File	sbceB2.key

Upload

## 5.5. Administer Client Profiles

Select **Backup/Restore** → **TLS Management** → **Client Profiles** from the left pane followed by **Add** (not shown) to add a new client profile for each identity certificate from **Section 6.3**.

Enter a desired **Profile Name** for the private interface. For **Certificate**, select the pertinent certificate associated with the SBCE private interface, in this case **sbceA1.pem**.

For **Peer Certificate Authorities**, select the pertinent CA certificate. Set **Verification Depth** to **1** as shown below. Retain the default value in the remaining fields.

**Device:** SBCE **Alarms** **New Profile** **Settings** **Help** **Log Out**

**Session Board**

EMS Dashboard  
Software Management  
Device Management  
Backup/Restore  
‣ System Parameters  
‣ Configuration Profiles  
‣ Services  
‣ Domain Policies  
‣ TLS Management  
‣ Certificates  
‣ **Client Profiles**  
‣ Server Profiles  
‣ SNI Group  
‣ Network & Flows  
‣ DMZ Services  
‣ Monitoring & Logging

**WARNING:** Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as at least one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems.

**TLS Profile**

Profile Name: sbceA1-client

Certificate: sbceA1.pem

SNI: ☐ Enabled

**Certificate Verification**

Peer Verification: Required

Peer Certificate Authorities: AvayaDeviceEnrollmentCAchain.crt, avayaitrootca2.pem, entrust\_g2\_ca.cer, SystemManagerCA.pem

Peer Certificate Revocation Lists:

Verification Depth: 1

Extended Hostname Verification: ☐

Server Hostname:

**Next**

Repeat the procedure to add a client profile for the SBCE public interface as shown below.

The screenshot shows the Avaya EMS Dashboard with the 'New Profile' dialog open. The dialog has a warning banner at the top: 'WARNING: Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as at least one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems.'

The dialog is divided into two main sections: 'TLS Profile' and 'Certificate Verification'.

**TLS Profile Section:**

- Profile Name: sbceB2-client
- Certificate: sbceB2.pem
- SNI: ☐ Enabled

**Certificate Verification Section:**

- Peer Verification: Required
- Peer Certificate Authorities: A list box containing 'AvayaDeviceEnrollmentCAchain.crt', 'avayaitrootca2.pem', 'entrust\_g2\_ca.cer', and 'SystemManagerCA.pem'.
- Peer Certificate Revocation Lists: An empty list box.
- Verification Depth: 1
- Extended Hostname Verification: ☐
- Server Hostname: An empty text field.

A 'Next' button is located at the bottom right of the dialog. The background shows the Avaya EMS Dashboard with a sidebar menu including 'Session Board', 'EMS Dashboard', 'Software Management', 'Device Management', 'Backup/Restore', 'System Parameters', 'Configuration Profiles', 'Services', 'Domain Policies', 'TLS Management', 'Certificates', 'Client Profiles' (highlighted), 'Server Profiles', 'SNI Group', 'Network & Flows', 'DMZ Services', and 'Monitoring & Logging'.



## 5.6. Administer Server Profiles

Select **Backup/Restore** → **TLS Management** → **Server Profiles** from the left pane followed by **Add** (not shown) to add a new server profile for each identity certificate from **Section 6.3**.

Enter a desired **Profile Name** for the private interface. For **Certificate**, select the pertinent certificate associated with the SBCE private interface, in this case **sbceA1.pem**.

Retain the default value in the remaining fields.

The screenshot shows the Avaya EMS Dashboard with the 'New Profile' dialog open. The dialog is titled 'New Profile' and has a close button (X) in the top right corner. A warning message is displayed at the top: 'WARNING: Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as at least one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems.' The dialog is divided into two main sections: 'TLS Profile' and 'Certificate Verification'. In the 'TLS Profile' section, the 'Profile Name' field is set to 'sbceA1-server', the 'Certificate' dropdown is set to 'sbceA1.pem', 'SNI Options' is set to 'None', and 'SNI Group' is set to 'None'. In the 'Certificate Verification' section, 'Peer Verification' is set to 'None', 'Peer Certificate Authorities' is a list containing 'AvayaDeviceEnrollmentCAchain.crt', 'avayaitrootca2.pem', 'entrust\_g2\_ca.cer', and 'SystemManagerCA.pem', 'Peer Certificate Revocation Lists' is empty, and 'Verification Depth' is set to 'None'. A 'Next' button is located at the bottom right of the dialog. The background shows the Avaya EMS Dashboard with the left sidebar containing navigation links like 'EMS Dashboard', 'Software Management', 'Device Management', 'Backup/Restore', 'System Parameters', 'Configuration Profiles', 'Services', 'Domain Policies', 'TLS Management', 'Certificates', 'Client Profiles', 'Server Profiles', 'SNI Group', 'Network & Flows', 'DMZ Services', and 'Monitoring & Logging'. The top bar shows 'Device: SBCE' and various menu items like 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'.



Repeat the procedure to add a server profile for the SBCE public interface as shown below.

The screenshot shows the 'New Profile' dialog box in the Avaya EMSD interface. The dialog is titled 'New Profile' and has a close button (X) in the top right corner. It contains a warning message at the top, followed by two main sections: 'TLS Profile' and 'Certificate Verification'. The 'TLS Profile' section includes fields for 'Profile Name' (sbceB2-server), 'Certificate' (sbceB2.pem), 'SNI Options' (None), and 'SNI Group' (None). The 'Certificate Verification' section includes a 'Peer Verification' dropdown (None), a list of 'Peer Certificate Authorities' (AvayaDeviceEnrollmentCAchain.crt, avayaitrootca2.pem, entrust\_g2\_ca.cer, SystemManagerCA.pem), an empty 'Peer Certificate Revocation Lists' field, and a 'Verification Depth' field. A 'Next' button is located at the bottom right of the dialog. The background shows the Avaya EMSD interface with a sidebar menu and a top navigation bar.

Device: SBCE Alarms Settings Help Log Out

**Session Board**

EMS Dashboard  
Software Management  
Device Management  
Backup/Restore  
System Parameters  
Configuration Profiles  
Services  
Domain Policies  
TLS Management  
Certificates  
Client Profiles  
**Server Profiles**  
SNI Group  
Network & Flows  
DMZ Services  
Monitoring & Logging

**WARNING:** Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as at least one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems.

**TLS Profile**

Profile Name sbceB2-server

Certificate sbceB2.pem

SNI Options None

SNI Group None

**Certificate Verification**

Peer Verification None

Peer Certificate Authorities  
AvayaDeviceEnrollmentCAchain.crt  
avayaitrootca2.pem  
entrust\_g2\_ca.cer  
SystemManagerCA.pem

Peer Certificate Revocation Lists

Verification Depth

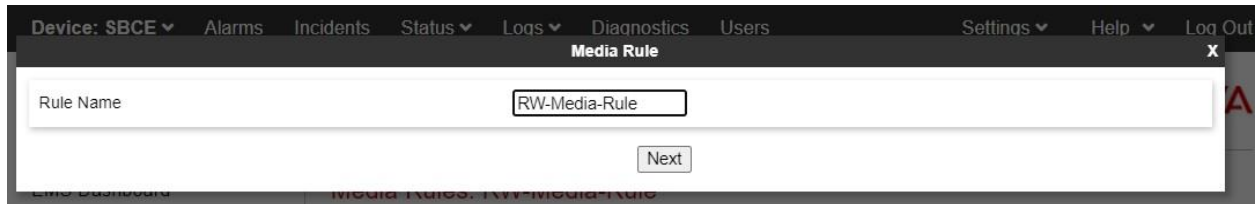
Next

AVAYA

Delete

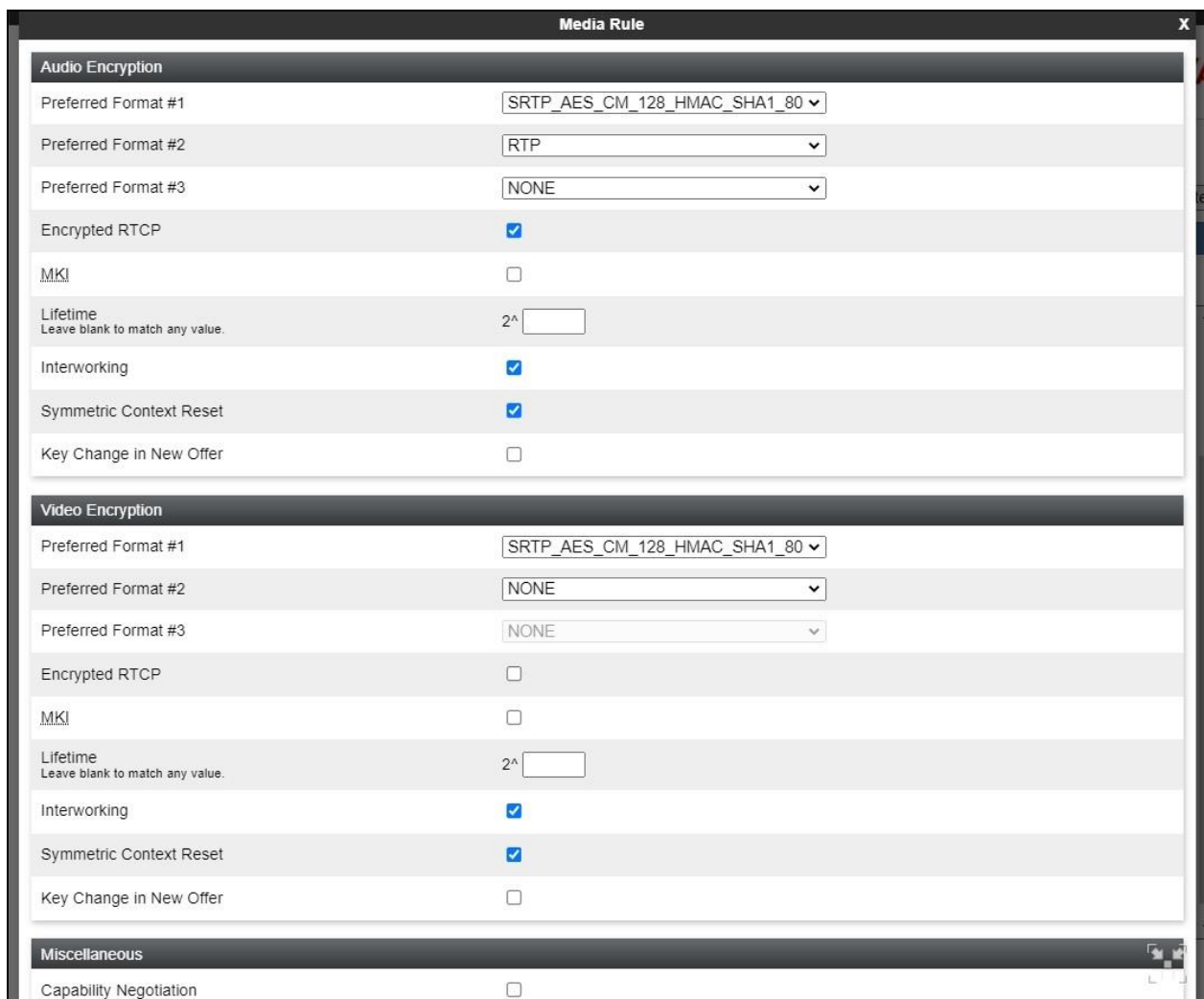
## 5.7. Administer Media Rule

Select **Backup/Restore** → **Domain Policies** → **Media Rule** (not shown) from the left pane followed by **Add** (not shown) to add a media interface for the SBCE private interface for support of remote workers. The **Media Rule** pop-up screen is displayed. Enter a desired **Rule Name**.



The screenshot shows the 'Media Rule' configuration window. At the top, there is a navigation bar with links: Device: SBCE, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. Below this, the title 'Media Rule' is centered. The main area contains a text input field labeled 'Rule Name' with the value 'RW-Media-Rule' entered. To the right of the input field is a 'Next' button.

In the next screen, select the desired encryption methods for **Preferred Format**, check **Interworking**, and retain the default values in the remaining fields.

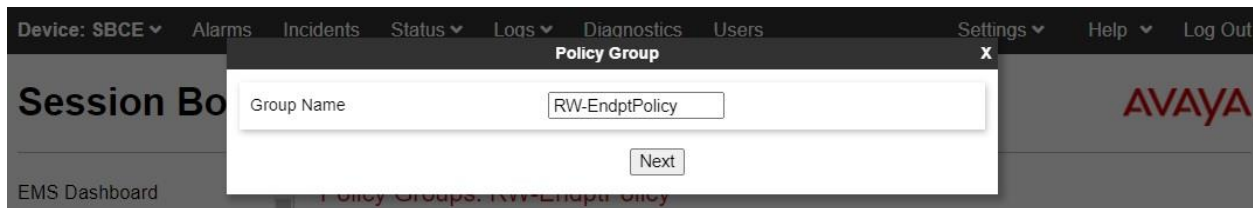


The screenshot shows the 'Media Rule' configuration window with the 'Audio Encryption' and 'Video Encryption' sections expanded. The 'Audio Encryption' section has the following settings: Preferred Format #1 (SRTP\_AES\_CM\_128\_HMAC\_SHA1\_80), Preferred Format #2 (RTP), Preferred Format #3 (NONE), Encrypted RTCP (checked), MKI (unchecked), Lifetime (2^16), Interworking (checked), Symmetric Context Reset (checked), and Key Change in New Offer (unchecked). The 'Video Encryption' section has the following settings: Preferred Format #1 (SRTP\_AES\_CM\_128\_HMAC\_SHA1\_80), Preferred Format #2 (NONE), Preferred Format #3 (NONE), Encrypted RTCP (unchecked), MKI (unchecked), Lifetime (2^16), Interworking (checked), Symmetric Context Reset (checked), and Key Change in New Offer (unchecked). The 'Miscellaneous' section at the bottom has the following settings: Capability Negotiation (unchecked).

## 5.8. Administer End Point Policy Groups

Select **Backup/Restore** → **Domain Policies** → **End Point Policy Groups** (not shown) followed by **Add** to add a policy group for remote workers.

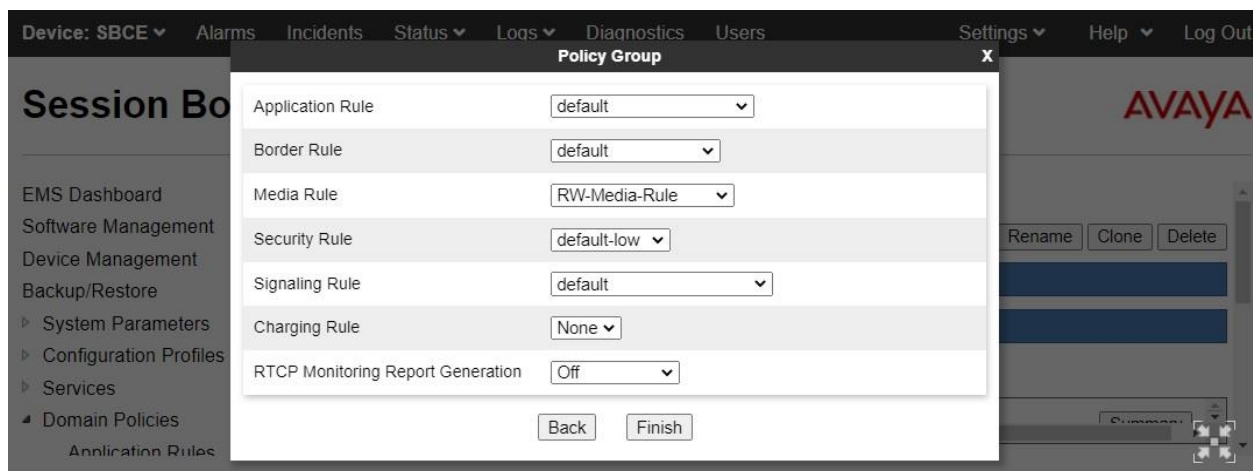
The **Policy Group** pop-up screen is displayed. Enter a desired **Group Name**.



The screenshot shows the 'Policy Group' pop-up window. The 'Group Name' field is populated with 'RW-EndptPolicy'. A 'Next' button is visible at the bottom right of the form. The background shows the Avaya EMS Dashboard with the 'Session Board' and 'Policy Groups' tabs.

The **Policy Group** pop-up screen is updated as shown below. For **Media Rule**, select the media rule for remote workers from **Section 5.7**.

Retain the default values for the remaining fields.



The screenshot shows the 'Policy Group' pop-up window with the following settings:

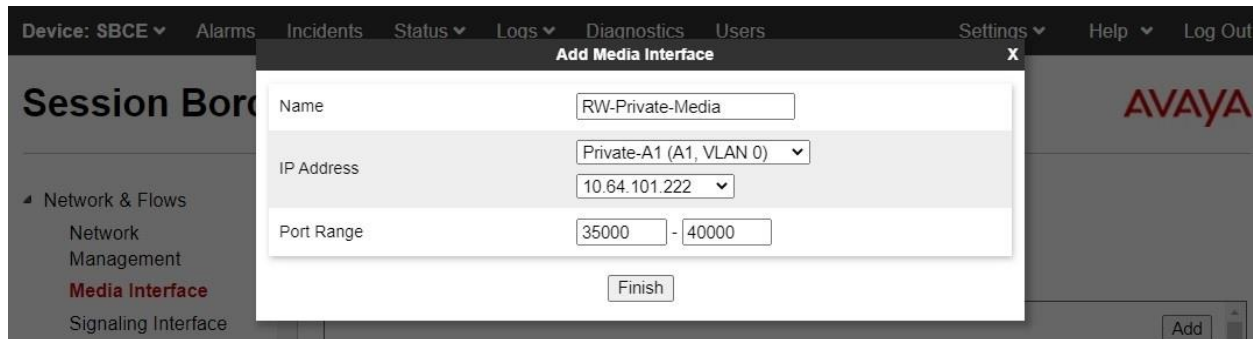
Field	Value
Application Rule	default
Border Rule	default
Media Rule	RW-Media-Rule
Security Rule	default-low
Signaling Rule	default
Charging Rule	None
RTCP Monitoring Report Generation	Off

Buttons: Back, Finish

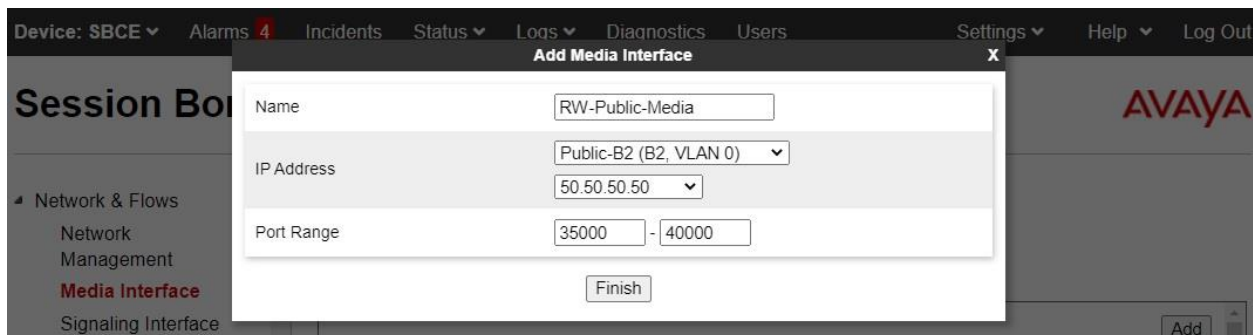
## 5.9. Administer Media Interface

Select **Backup/Restore** → **Network & Flows** → **Media Interface** from the left pane followed by **Add** (not shown) to add a media interface for the SBCE private interface for support of remote workers.

Enter a desired **Name**. For **IP Address**, select pertinent entries associated with SBCE private interface for support of remote workers from **Section 5.2**. Retain the default values for the remaining fields as shown below.



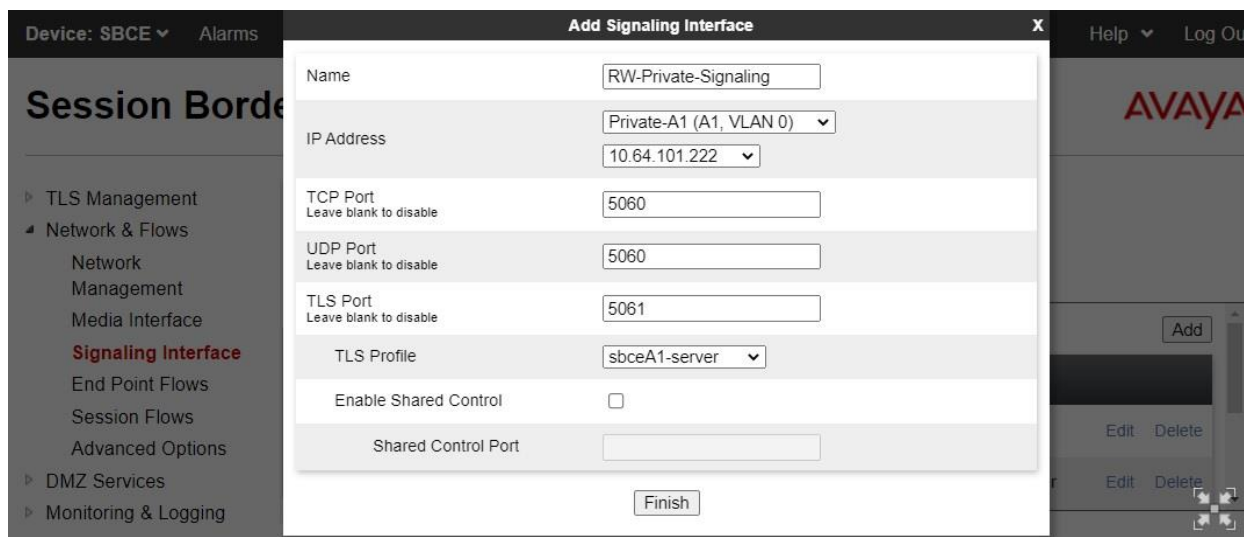
Repeat the procedure to add a media interface for the SBCE public interface for support of remote workers as shown below.



## 5.10. Administer Signaling Interface

Select **Backup/Restore → Network & Flows → Signaling Interface** from the left pane followed by **Add** (not shown) to add a signaling interface for the SBCE private interface for support of remote workers.

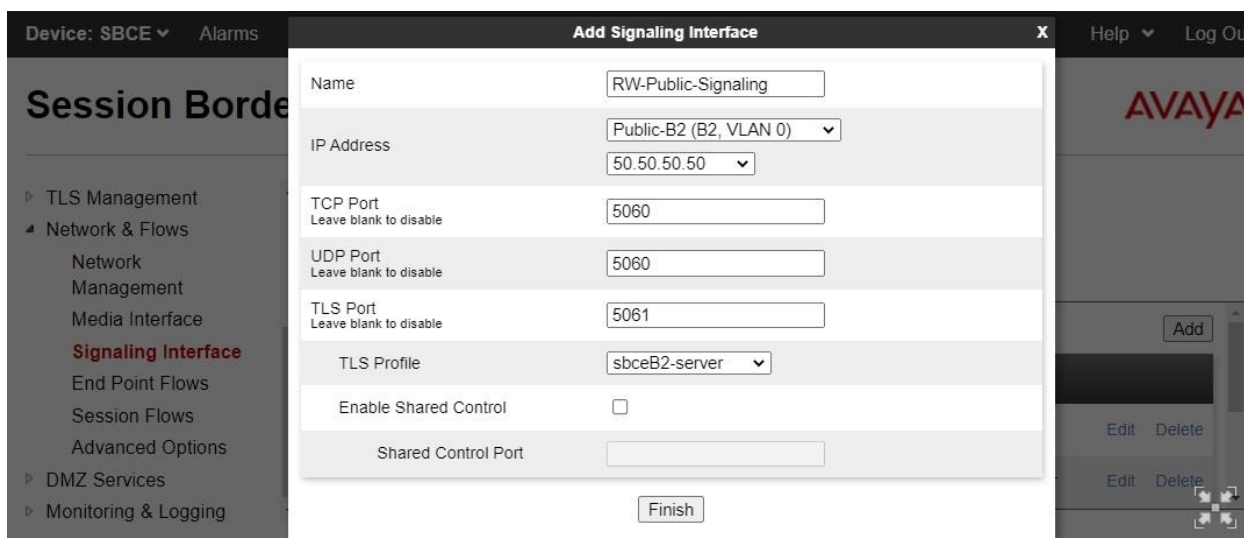
Enter a desired **Name**. For **IP Address**, select pertinent entries associated with SBCE private interface for support of remote workers from **Section 5.2**. Enter 5061 for TLS Port and select the pertinent server profile for the private interface from **Section 5.6**.



The screenshot shows the 'Add Signaling Interface' dialog box in the Avaya Session Border Controller (SBCE) configuration interface. The left pane shows the navigation menu with 'Signaling Interface' selected under 'Network & Flows'. The dialog box contains the following fields:

- Name: RW-Private-Signaling
- IP Address: Private-A1 (A1, VLAN 0) (dropdown menu)
- IP Address: 10.64.101.222
- TCP Port: 5060 (Leave blank to disable)
- UDP Port: 5060 (Leave blank to disable)
- TLS Port: 5061 (Leave blank to disable)
- TLS Profile: sbceA1-server (dropdown menu)
- Enable Shared Control: ☐
- Shared Control Port: (empty field)
- Finish button

Repeat the procedure to add a signaling interface for the SBCE public interface for support of remote workers.



The screenshot shows the 'Add Signaling Interface' dialog box in the Avaya Session Border Controller (SBCE) configuration interface for the public interface. The left pane shows the navigation menu with 'Signaling Interface' selected under 'Network & Flows'. The dialog box contains the following fields:

- Name: RW-Public-Signaling
- IP Address: Public-B2 (B2, VLAN 0) (dropdown menu)
- IP Address: 50.50.50.50
- TCP Port: 5060 (Leave blank to disable)
- UDP Port: 5060 (Leave blank to disable)
- TLS Port: 5061 (Leave blank to disable)
- TLS Profile: sbceB2-server (dropdown menu)
- Enable Shared Control: ☐
- Shared Control Port: (empty field)
- Finish button

## 5.11. Administer User Agents

Select **Backup/Restore** → **System Parameters** → **User Agents** from the left pane followed by **Add** to add a user agent for support of remote workers.

Enter a desired **Name**. For **Regular Expression**, enter the expression to match the User-Agent header value in the SIP message. In the compliance testing, the expression **Avaya.\*** was used, which will match to all Avaya endpoints.

The screenshot shows the 'Add User Agent' dialog box in the Avaya EMS interface. The dialog has a title bar with 'Add User Agent' and a close button. A warning message states: 'WARNING: Invalid or incorrectly entered regular expressions may cause unexpected results. Note: This regular expression is case-sensitive.' Below the warning, an example 'Ex:' is provided: 'Avaya one-X Deskphone', 'Aastra.\*', 'Cisco-CP7970G[0-9]{3}', and 'RTC/1.1RTC/1.2'. The form contains two input fields: 'Name' with the value 'RW-User-Agents' and 'Regular Expression' with the value 'Avaya.\*'. A 'Finish' button is at the bottom right of the form. The background shows the 'Session Board' menu with 'User Agents' selected.

## 5.12. Administer Subscriber Flows

Select **Backup/Restore** → **Network & Flows** → **End Point Flows** from the left pane. Select the **Subscriber Flows** (not shown) tab and click **Add** to add a subscriber flow for remote workers.

The **Add Flow** pop-up screen is displayed. Enter a desired **Flow Name**.

For **User Agent**, select the user agent from **Section 5.11**. For **Signaling Interface**, select the public signaling interface for remote workers from **Section 5.10** as shown below. Click **Next**.

The screenshot shows the 'Add Flow' dialog box in the Avaya EMS interface. The dialog has a title bar with 'Add Flow' and a close button. The 'Criteria' section contains several fields: 'Flow Name' with the value 'RW-Subsc-Flow', 'URI Group' with a dropdown showing '\*', 'User Agent' with a dropdown showing 'RW-User-Agents', 'Source Subnet' with a text field containing '\*' and an example 'Ex: 192.168.0.1/24', 'Via Host' with a text field containing '\*' and an example 'Ex: domain.com, 192.168.0.1/24', 'Contact Host' with a text field containing '\*' and an example 'Ex: domain.com, 192.168.0.1/24', and 'Signaling Interface' with a dropdown showing 'RW-Public-Signaling'. A 'Next' button is at the bottom right of the form. The background shows the 'Session Board' menu with 'End Point Flows' selected.

The **Add Flow** pop-up screen is updated as shown below. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Media Interface:** Select the public media for remote workers from **Section 5.9**.
- **End Point Policy Group:** Select the endpoint policy group from **Section 5.8**.
- **Routing Profile:** Select the existing routing profile for Session Manager.
- **TLS Client Profile:** Select the client profile for public interface from **Section 5.5**.

**Add Flow**

**Profile**

Source: ☒ Subscriber ☐ Click To Call

Methods Allowed Before REGISTER: INFO, MESSAGE, NOTIFY, OPTIONS

Media Interface: RW-Public-Media

Secondary Media Interface: None

Received Interface: None

End Point Policy Group: RW-EndptPolicy

Routing Profile: SM-Route

FQDN Support: ☐

FQDN:

**Optional Settings**

TLS Client Profile: sbceB2-client

Signaling Manipulation Script: None

Presence Server Address:   
Ex: domain.com, 192.168.0.101

Back Finish



## 5.13. Administer Server Flows

Select **Backup/Restore → Network & Flows → End Point Flows** from the left pane. Select the **Server Flows** (not shown) tab and click **Add** to add a server flow for remote workers.

The **Add Flow** pop-up screen is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Flow Name:** A descriptive name.
- **SIP Server Profile:** Select the existing server profile for Session Manager.
- **Received Interface:** Remote worker public signaling interface from **Section 5.10**.
- **Signaling Interface:** Remote worker private signaling interface from **Section 5.10**.
- **Media Interface:** Remote worker private media interface from **Section 5.9**.
- **End Point Policy Group:** Remote worker end point policy group from **Section 5.8**.

The screenshot displays the 'Add Flow' pop-up screen in the Avaya Session Border Controller (SBC) configuration interface. The left pane shows the navigation menu with 'End Point Flows' selected. The right pane shows the 'Add' button and 'Clone', 'Edit', 'Delete' options. The form fields are as follows:

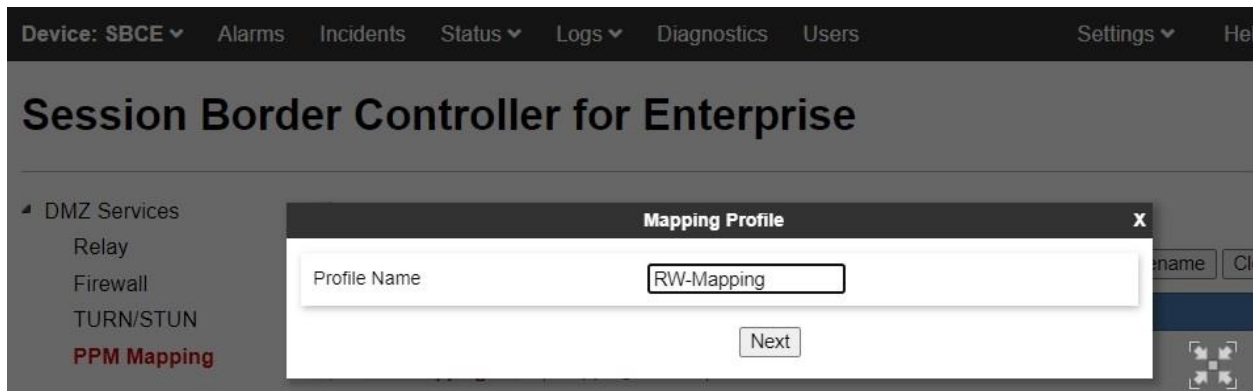
Field	Value
Flow Name	RW-Flow
SIP Server Profile	SM-Server
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	RW-Public-Signaling
Signaling Interface	RW-Private-Signaling
Media Interface	RW-Private-Media
Secondary Media Interface	None
End Point Policy Group	RW-EndptPolicy
Routing Profile	default
Topology Hiding Profile	None
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	<input type="checkbox"/>
FQDN Support	<input type="checkbox"/>
FQDN	

Buttons: Finish, Clone, Edit, Delete.

## 5.14. Administer PPM Mapping

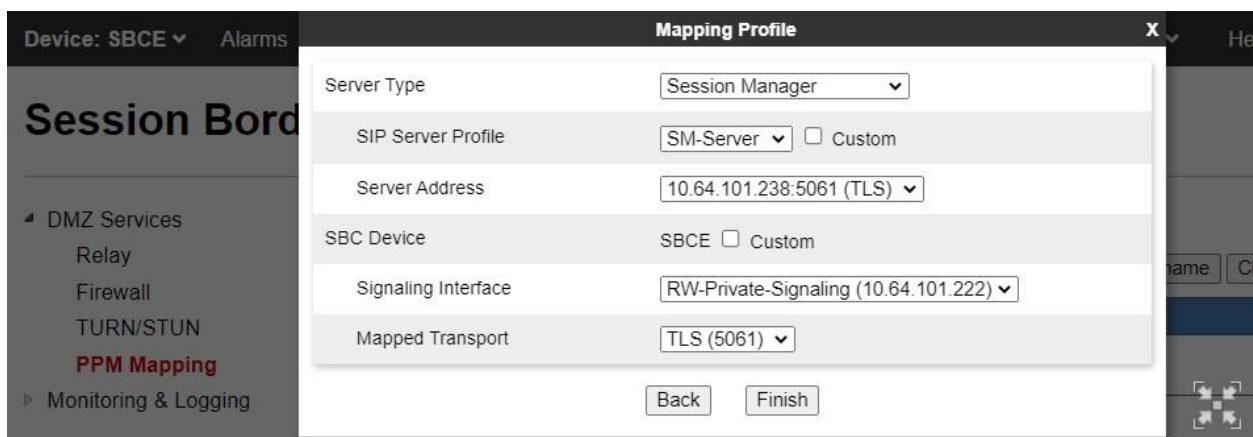
Select **Backup/Restore** → **DMZ Services** → **PPM Mapping** from the left pane followed by **Add** (not shown) to add a PPM mapping profile for PPM data download from Session Manager.

The **Mapping Profile** pop-up screen is displayed. Enter a desired **Profile Name**.



The **Mapping Profile** pop-up screen is updated as shown below. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Server Type:** “Session Manager”
- **SIP Server Profile:** Select the existing server profile for Session Manager.
- **Server Address:** Select the TLS address for Session Manager.
- **Signaling Interface:** The remote worker private signaling interface from **Section 5.10**.
- **Mapped Transport:** Select TLS transport.



## 5.15. Administer Reverse Proxy

Select **Backup/Restore** → **DMZ Services** → **Relay** from the left pane, followed by the **Reverse Proxy** (not shown) tab, followed by **Add** (not shown) to add a reverse proxy for obtainment of PPM data from Session Manager for remote workers.

The **Add Flow** pop-up screen is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Service Name:** A descriptive name.
- **Listen IP:** Select the pertinent public interface and IP from **Section 5.2**.
- **Listen Protocol:** “HTTPS”
- **Server Protocol:** “HTTPS”
- **PPM Mapping Profile:** The PPM mapping profile from **Section 5.14**.
- **Enabled:** Check this field.
- **Listen Port:** “443”
- **Listen TLS Profile:** The TLS server profile for the public interface from **Section 5.6**.
- **Connect IP:** Select the pertinent private interface and IP from **Section 5.2**.
- **Server TLS Profile:** The TLS client profile for the private interface from **Section 5.5**.
- **Server Addresses:** IP address of Session Manager and port “443”.

The screenshot shows the 'Add Reverse Proxy Profile' configuration window. The left pane has 'Relay' selected under 'DMZ Services'. The configuration fields are as follows:

Field	Value
Service Name	RW-PPM
Enabled	<input checked="" type="checkbox"/>
Listen IP	Public-B2 (B2, VLAN 0) 50.50.50.50
Listen Port	443
Listen Protocol	HTTPS
Listen TLS Profile (TLS Server Profile)	sbceB2-server
Listen Domain (Optional)	
Connect IP	Private-A1 (A1, VLAN 0) 10.64.101.222
Server Protocol	HTTPS
Server TLS Profile (TLS Client Profile)	sbceA1-client
Load Balancing Algorithm	None
PPM Mapping Profile	RW-Mapping
Reverse Proxy Policy Profile	default
Whitelisted IPs (Max of 5 comma-separated IPs)	

At the bottom, there is a table for 'Server Addresses':

Server Addresses	Received Server Host	Whitelisted URL	URL Replace
40.64.101.238:443	Any	/	

Buttons: Add, Edit, Delete, Finish.

Repeat the procedure to add a reverse proxy for HTTPS file transfer from file server for remote workers, including obtainment of the remote worker settings file.

Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Service Name:** A descriptive name.
- **Listen IP:** Select the pertinent public interface and IP from **Section 5.2**.
- **Listen Protocol:** “HTTPS”
- **Server Protocol:** “HTTPS”
- **Enabled:** Check this field.
- **Listen Port:** An available port, in this case “8443” with “443” already in use.
- **Listen TLS Profile:** The TLS server profile for the public interface from **Section 5.6**.
- **Connect IP:** Select the pertinent private interface and IP from **Section 5.2**.
- **Server TLS Profile:** The TLS client profile for the private interface from **Section 5.5**.
- **Server Addresses:** IP address of file server and port “443”.

**Device: SBCE** **Add Reverse Proxy Profile**

Service Name: RW-FileXfer Enabled: ☒

Listen IP: Public-B2 (B2, VLAN 0) 50.50.50.50 Listen Port: 8443

Listen Protocol: HTTPS Listen TLS Profile (TLS Server Profile): sbceB2-server

Listen Domain (Optional): Connect IP: Private-A1 (A1, VLAN 0) 10.64.101.222

Server Protocol: HTTPS Server TLS Profile (TLS Client Profile): sbceA1-client

Rewrite URL: ☐ Load Balancing Algorithm: None

PPM Mapping Profile: None Reverse Proxy Policy Profile: default

Whitelisted IPs (Max of 5 comma-separated IPs):

Server Addresses	Received Server Host	Whitelisted URL	URL Replace	Delete
10.64.101.230:443	Any	/		<input type="button" value="Delete"/>

Repeat the procedure to add a reverse proxy for HTTPS license obtainment from WebLM server for remote workers.

Enter the following values for the specified fields and retain the default values for the remaining fields.

- **Service Name:** A descriptive name.
- **Listen IP:** Select the pertinent public interface and IP from **Section 5.2**.
- **Listen Protocol:** “HTTPS”
- **Server Protocol:** “HTTPS”
- **Enabled:** Check this field.
- **Listen Port:** “52233”
- **Listen TLS Profile:** The TLS server profile for the public interface from **Section 5.6**.
- **Connect IP:** Select the pertinent private interface and IP from **Section 5.2**.
- **Server TLS Profile:** The TLS client profile for the private interface from **Section 5.5**.
- **Server Addresses:** IP address of WebLM server and port “52233”.

Device: SBCE

Add Reverse Proxy Profile

Service Name

RW-WebLM

Enabled

☒

Listen IP

Public-B2 (B2, VLAN 0)  
50.50.50.50

Listen Port

52233

Listen Protocol

HTTPS

Listen TLS Profile (TLS Server Profile)

sbceB2-server

Listen Domain (Optional)

Connect IP

Private-A1 (A1, VLAN 0)  
10.64.101.222

Server Protocol

HTTPS

Server TLS Profile (TLS Client Profile)

sbceA1-client

Rewrite URL

☐

Load Balancing Algorithm

None

PPM Mapping Profile

None

Reverse Proxy Policy Profile

default

Whitelisted IPs  
Max of 5 comma-separated IPs.

Add

Server Addresses	Received Server Host	Whitelisted URL	URL Replace	
10.64.101.235:52233	Any	/		Delete

Finish

## 6. Configure Avaya Aura® System Manager

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

- Launch System Manager
- Administer end entity
- Create certificate from CSR
- Fetch CA certificate

### 6.1. Launch System Manager

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

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons.

User ID:

Password:



## 6.2. Administer End Entity

In the subsequent screen (not shown), select **Services** → **Security** → **Certificates** → **Authority** from the top menu, followed by **RA Functions** → **Add End Entity** to display the **Add End Entity** screen. Create an end entity for the SBCE private interface for remote worker traffic.

For **End Entity Profile**, select **EXTERNAL\_CSR\_PROFILE**. Enter desired values for **Username**, **Password**, and same password value in **Confirm Password**.

Set **Certificate Profile**, **CA**, and **Token** as shown below. Set the remaining parameters to match values in the certificate signing request from **Section 5.3** for the SBCE private interface.

**AVAYA** Aura® System Manager 8.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾ Search 🔍

Home Security

S...

**CA Functions**

- CA Activation
- CA Structure & CRLs
- Certificate Profiles
- Certification Authorities
- Crypto Tokens
- Publishers

**RA Functions**

- Add End Entity
- End Entity Profiles
- Search End Entities
- User Data Sources

**Supervision Functions**

- Approve Actions
- View Log

**System Functions**

- Administrator Roles
- Internal Key Bindings
- Services

**System Configuration**

- CMP Configuration
- SCEP Configuration
- System Configuration

**My Preferences**

### Add End Entity

End Entity Profile: EXTERNAL\_CSR\_PROFILE ▾ Required

Username: sbceA1 ✓

Password (or Enrollment Code): ..... ✓

Confirm Password: ..... ✓

E-mail address: tlt @ dr220.com

**Subject DN Attributes**

CN, Common name: sbceA1 ✓

CN, Common name:

O, Organization: AVAYA

C, Country (ISO 3166): US

OU, Organizational Unit: DevConnect

L, Locality: Morristown

ST, State or Province: NJ

**Other subject attributes**

**Subject Alternative Name**

DNS Name: dr220.com

DNS Name:

IP Address: 10.64.101.221

IP Address: 10.64.101.222

**Main certificate data**

Certificate Profile: ID\_CLIENT\_SERVER ▾ ✓

CA: tmdefaultca ▾ ✓

Token: User Generated ▾ ✓

Add Reset

Made by PrimeKey Solutions AB, 2002–2014.



Repeat the procedure to create an end entity for the SBCE public interface for remote worker traffic, as shown below.

**AVAYA**  
Aura® System Manager 8.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾ Search 🔍 🔔 ☰

Home Security

S...

### Add End Entity

End Entity Profile: **EXTERNAL\_CSR\_PROFILE** ▾ Required

**Username** sbceB2 ☒

Password (or Enrollment Code) \*\*\*\*\* ☒

Confirm Password \*\*\*\*\*

E-mail address: tlr @ dr220.com ☐

**Subject DN Attributes**

CN, Common name: sbceB2 ☒

CN, Common name: ☐

O, Organization: AVAYA ☐

C, Country (ISO 3166): US ☐

OU, Organizational Unit: DevConnect ☐

L, Locality: Morristown ☐

ST, State or Province: NJ ☐

**Other subject attributes**

**Subject Alternative Name**

DNS Name: dr220.com ☐

DNS Name: ☐

IP Address: 50.50.50.50 ☐

IP Address: ☐

**Main certificate data**

Certificate Profile: **ID\_CLIENT\_SERVER** ▾ ☒

CA: tmdefaultca ▾ ☒

Token: User Generated ▾ ☒

Add Reset

Made by PrimeKey Solutions AB, 2002–2014.

**CA Functions**

- CA Activation
- CA Structure & CRLs
- Certificate Profiles
- Certification Authorities
- Crypto Tokens
- Publishers

**RA Functions**

- Add End Entity
- End Entity Profiles
- Search End Entities
- User Data Sources

**Supervision Functions**

- Approve Actions
- View Log

**System Functions**

- Administrator Roles
- Internal Key Bindings
- Services

**System Configuration**

- CMP Configuration
- SCEP Configuration
- System Configuration

**My Preferences**

**Public Web**

### 6.3. Create Certificate From CSR

Select **Public Web** (not shown below) followed by **Enroll → Create Certificate from CSR** in the subsequent screen to display the **Certificate enrollment from a CSR** screen.

For **Username** and **Enrollment code**, enter the username and password values associated with the end entity for the SBCE private interface from **Section 6.2**.

For **Request file**, select **Choose File** and navigate to the certificate signing request associated with the SBCE private interface from **Section 5.3** as shown below.

Retain the default value for **Result type** and click **OK**.

The screenshot displays the EJBCA PKI BY PRIMEKEY web interface. On the left is a navigation menu with sections: **Enroll** (containing 'Create Browser Certificate', 'Create Certificate from CSR', 'Create Keystore', 'Create CV certificate'), **Register** (containing 'Request Registration'), **Retrieve** (containing 'Fetch CA Certificates', 'Fetch CA CRLs', 'List User's Certificates', 'Fetch User's Latest Certificate'), **Inspect** (containing 'Inspect certificate/CSR', 'Check Certificate Status'), and **Miscellaneous** (containing 'Administration', 'Documentation'). The main content area is titled 'Certificate enrollment from a CSR' in red. It contains instructions: 'Please give your username and enrollment code, select a PEM- or DER-formatted certification request file (CSR) for upload, or paste a PEM-formatted request into the field below and click OK to fetch your certificate.' Below this, it states: 'A PEM-formatted request is a BASE64 encoded certificate request starting with -----BEGIN CERTIFICATE REQUEST----- and ending with -----END CERTIFICATE REQUEST-----'. The 'Enroll' form includes fields for 'Username' (filled with 'sbceA1') and 'Enrollment code' (filled with '\*\*\*\*\*'). The 'Request file' section has a 'Choose File' button and the text 'sbceA1.req'. Below this is a large text area labeled 'or pasted request'. At the bottom, the 'Result type' dropdown is set to 'PEM - certificate only', and there is an 'OK' button.

The **Certificate Created** screen is displayed next with the identity certificate **sbceA1.pem** auto downloaded as shown below.



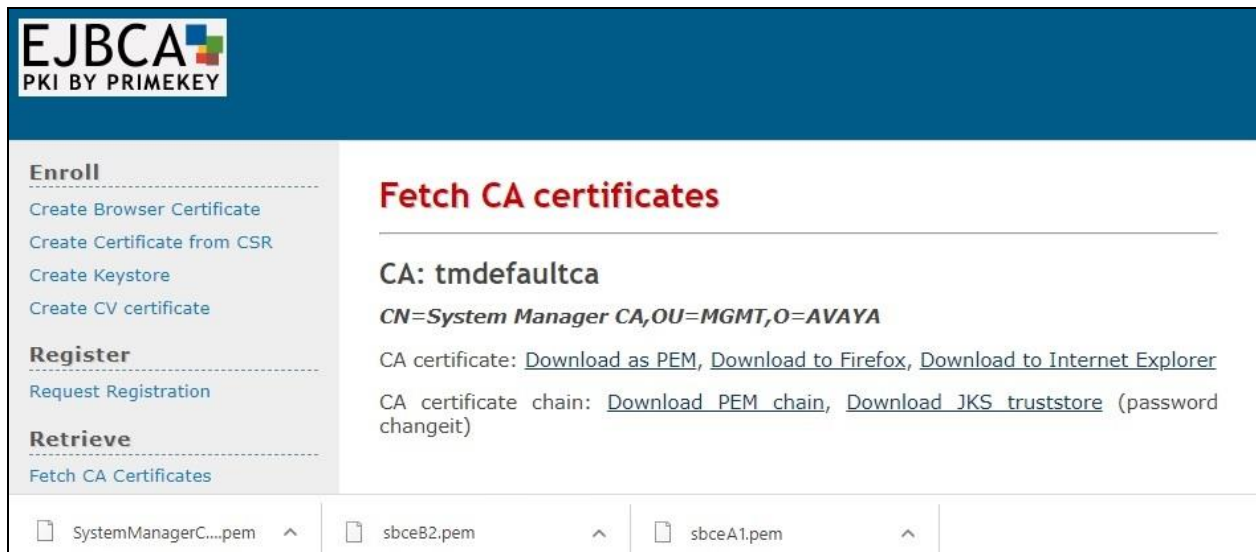
Repeat the procedure to create and download the certificate for the SBCE public interface, in this case **sbceB2.pem** as shown below.



## 6.4. Fetch CA Certificate

Select **Retrieve** → **Fetch CA Certificates** from the left pane to display the Fetch CA certificates screen.

Select **Download as PEM** to download the CA certificate in this case **SystemManagerCA.pem** is downloaded as shown below.



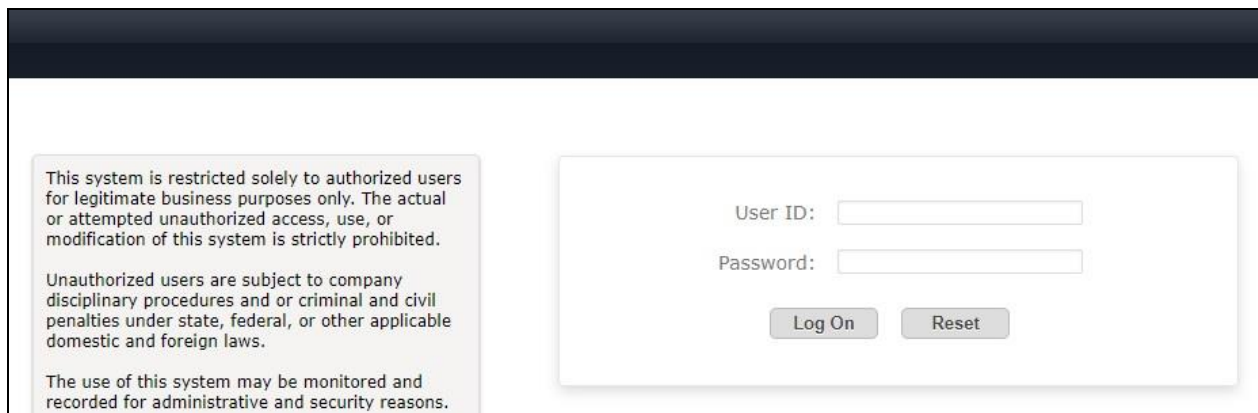
## 7. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager, which is performed via the web interface of System Manager. The procedures include the following areas:

- Launch System Manager
- Administer remote access
- Administer SIP firewall
- Administer PPM limiting

### 7.1. Launch System Manager

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



This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons.

User ID:

Password:

## 7.2. Administer Remote Access

In the subsequent screen (not shown), select **Elements** → **Session Manager** → **Network Configuration** → **Remote Access** from the top menu followed by **New** (not shown) to create a new remote access configuration for remote workers.

The **Remote Access Configuration** screen is displayed. Enter a descriptive **Name**.

In the **SIP Proxy Mapping Table** sub-section, click **New** to add an entry. For **SIP Proxy Public Address**, enter the IP address associated with the SBCE public interface for remote workers from **Section 5.2**. For **Session Manager**, select the pertinent Session Manager.

In the **SIP Proxy Private IP Addresses** sub-section, click **New** to add an entry. For **SIP Private Address**, enter the IP address associated with the SBCE private interface for remote workers from **Section 5.2**.

Retain the default values in the remaining fields.

Aura® System Manager 8.1

Users
Elements
Services
Widgets
Shortcuts

Home
Session Manager

Remote Access Configuration

Add
Cancel

Name:
SM Remote Workers

Note:

Click to open Remote Access Reference Map

SIP Proxy Mapping

SIP Proxy Mapping Table

New
Delete

	SIP Proxy Public Address (Reference A)	Session Manager (Reference C)	IP Address Family (Reference C)
<input type="checkbox"/>	50.50.50.50	DR-SM	IPv4

Select : All, None

SIP Proxy Private IP Addresses

New
Delete

	SIP Private Address (Reference B)	SBC Type	Securable	Note
<input type="checkbox"/>	10.64.101.222	Avaya SBC	<input type="checkbox"/>	

Select : All, None

### 7.3. Administer SIP Firewall

In the subsequent screen (not shown), select **Session Manager** → **Network Configuration** → **SIP Firewall** from the left menu followed by **New** (not shown) to create a new SIP firewall rule set for remote workers.

The **Rule Set** screen is displayed. Enter a descriptive **Name**.

Select the **Whitelist** tab, followed by **New** to create a new entry. For **Value**, enter the IP address associated with the SBCE private interface for remote workers from **Section 5.2**. Enter the pertinent **Mask** value and retain the default values in the remaining fields.

The screenshot displays the Avaya Aura System Manager 8.1 interface. The left sidebar shows the navigation menu with 'SIP Firewall' selected. The main content area is titled 'Rule Set' and includes a 'Commit' button and a 'Cancel' button. Below the title, there is a description: 'Edit or view SIP Firewall Rule Set whitelist, blacklist, and rules.' The form contains the following fields:

- \*Name:** Firewall-Rule-SBCE
- Description:** (empty)
- \*SM Type:** SM

Below these fields, there are tabs for 'Rules', 'Blacklist', and 'Whitelist'. The 'Whitelist' tab is active. Under the 'Whitelist' tab, there is an 'Enabled' checkbox which is checked. Below this, there are 'New' and 'Delete' buttons. A table with the following columns is shown:

	Key	Value	Mask
<input type="checkbox"/>	Remote IP Address	10.64.101.222	255.255.255.255

At the bottom of the table, there is a 'Select' dropdown menu with options 'All' and 'None'.



## 7.4. Administer PPM Limiting

Select **Session Manager** → **Session Manager Administration** from the left pane to display the **Session Manager Administration** screen.

Select the pertinent Session Manager entry and click **Edit**.

**Session Manager Administration**

This page allows you to administer Session Manager instances and configure their global settings.

**Session Manager Instances** | **Branch Session Manager Instances**

**Session Manager Instances**

New View Edit Delete

1 Item Filter:

Name	License Mode	Primary Communication Profiles	Secondary Communication Profiles	Maximum Active Communication Profiles	Des
DR-SM	Normal	12	0	12	SM

In the subsequent screen, scroll down to the **Personal Profile Manager (PPM) – Connection Settings** sub-section, uncheck **Limited PPM Client Connection** and **PPM Packet Rate Limiting** as shown below.

**Personal Profile Manager (PPM) - Connection Settings**

Include User to User Calls ☒

Include Incomplete Calls ☒

Limited PPM Client Connection ☐

\*Maximum Connection per PPM Client

PPM Packet Rate Limiting ☐

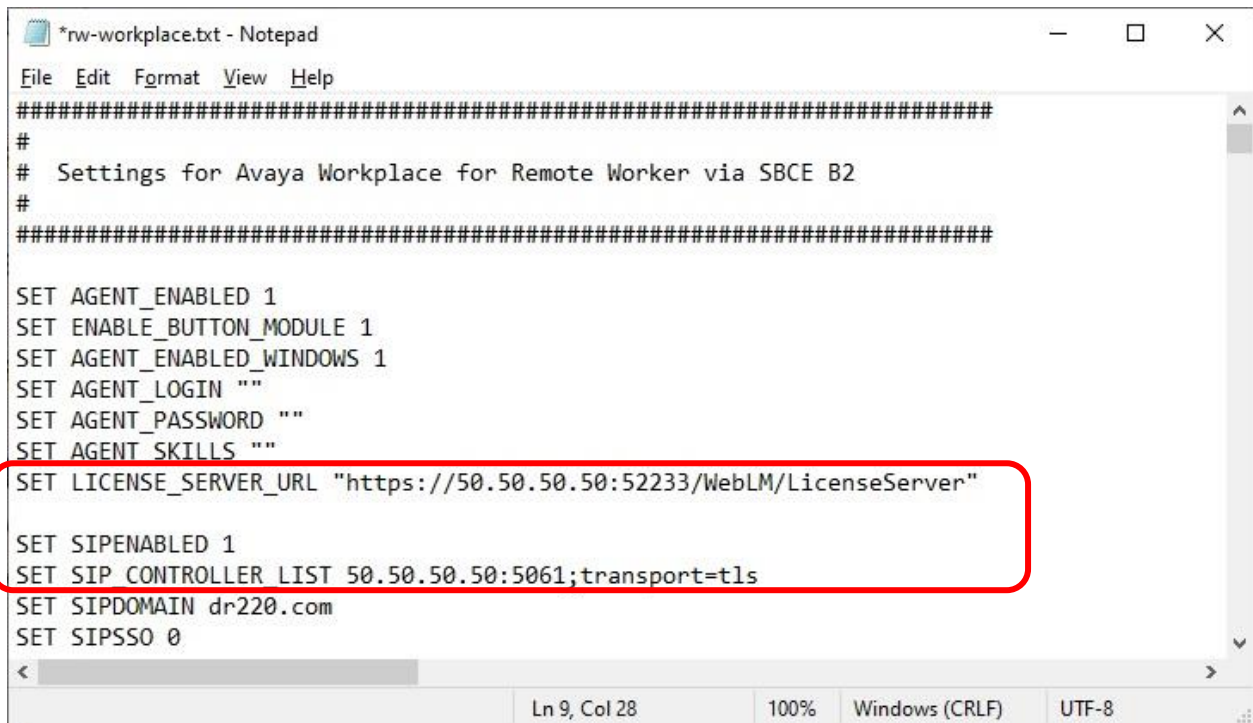
\*PPM Packet Rate Limiting Threshold

## 8. Configure File Server

The deployment and configuration of settings needed for agents to use Workplace from within the enterprise is assumed to be in place and outside the scope of these Application Notes.

In the compliance testing, the automatic configuration method via use of file server address was used. A new settings file **rw-workplace.txt** was replicated from the existing Workplace settings file with update of two parameters and deployed to the file server for agents to use when connecting as remote worker via DaaS with SBCE.

The parameters **LICENSE\_SERVER\_URL** and **SIP\_CONTROLLER\_LIST** was updated to point to the SBCE public interface from **Section 5.2** for remote workers, rather than to the local WebLM server and Session Manager, as shown below.



```
*rw-workplace.txt - Notepad
File Edit Format View Help
#####
#
# Settings for Avaya Workplace for Remote Worker via SBCE B2
#
#####

SET AGENT_ENABLED 1
SET ENABLE_BUTTON_MODULE 1
SET AGENT_ENABLED_WINDOWS 1
SET AGENT_LOGIN ""
SET AGENT_PASSWORD ""
SET AGENT_SKILLS ""
SET LICENSE_SERVER_URL "https://50.50.50.50:52233/WebLM/LicenseServer"
SET SIPENABLED 1
SET SIP_CONTROLLER_LIST 50.50.50.50:5061;transport=tls
SET SIPDOMAIN dr220.com
SET SIPSSO 0

Ln 9, Col 28    100%    Windows (CRLF)    UTF-8
```

## 9. Configure Dizzion DaaS Complete

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

- Prepare order form
- Prepare golden image

### 9.1. Prepare Order Form

Prior to integration, customer needs to fill out an order form from Dizzion with pertinent requirements for the virtual desktops, such as operating system, capacity, network services, multi-factor authentication, applications, graphics, etc.

Below is a sample of the **Desktop Services**, **Telephony**, and **Endpoint Devices** sections of the form for the compliance testing.

<b>Desktop Services</b>	
<input checked="" type="checkbox"/> New Desktop Pool(s) <input checked="" type="checkbox"/> New Golden Image(s)	
Desktop Pool #1	<ul style="list-style-type: none"><li>– OS Version: Windows 10</li><li>– OS Licensing (<i>Dizzion/Customer</i>)*: Dizzion</li><li>– vCPU / RAM: 2x4</li><li>– Pool Name: Devconnect</li><li>– Pool Type (<i>Dedicated/Floating</i>): Dedicated</li><li>– # of Desktops: 3</li><li>– Profile Mgmt. (<i>Yes/No – list items to persist</i>): No</li><li>– 3D/GPU Requirements: no</li><li>– Apps to be installed: Avaya Workplace</li><li>– Graphically intensive apps: N/A</li></ul>
*Note: If OS licensing is provided by the customer, a KMS server is required.	
<b>Telephony</b>	
Softphone/SIP Telephony Integration?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Voice type / application	Avaya Workplace
<b>Endpoint Devices</b>	
Endpoint Device Type ( <i>Choose all that apply</i> )	<input checked="" type="checkbox"/> Windows <input type="checkbox"/> MacOS <input type="checkbox"/> Chrome OS <input type="checkbox"/> Android <input type="checkbox"/> iOS <input type="checkbox"/> zLink BYOD <input type="checkbox"/> zLink (conversion software) <input type="checkbox"/> 3rd Party Thin Client/Zero Client – ( <i>model?</i> ) <input type="checkbox"/> Other:
Peripherals	<input checked="" type="checkbox"/> USB Headset <input type="checkbox"/> WebCam <input type="checkbox"/> Scanner <input type="checkbox"/> Printer <input type="checkbox"/> Other ( <i>describe</i> ):
End User Location(s)	CO, NJ

## 9.2. Prepare Golden Image

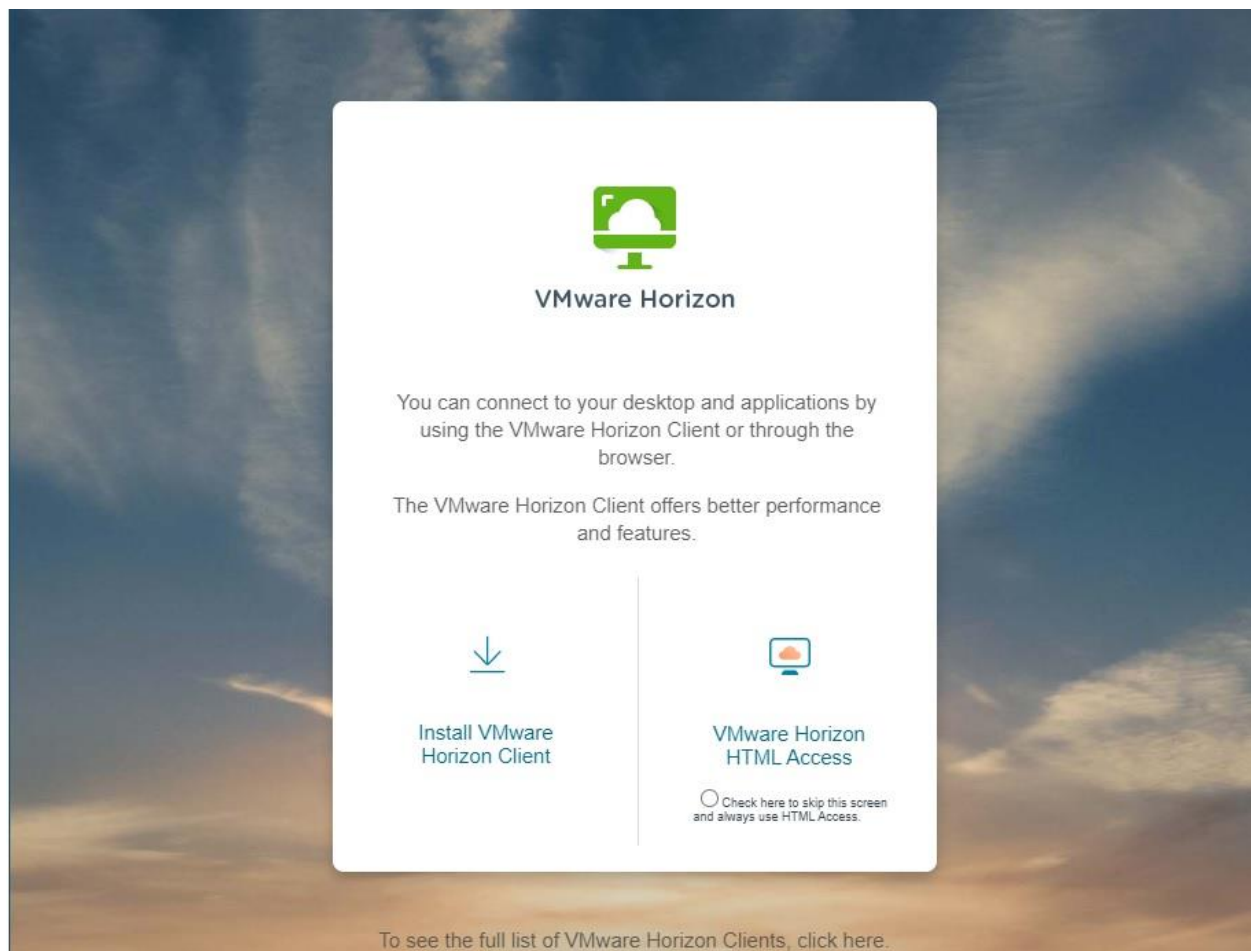
Custom golden images are built by Dizzion based on requirements from the order form in **Section 9.1**. Once available, the access information for the golden images is provided by Dizzion to customer for installation of needed common applications before the image is replicated for creation of virtual desktops for User Acceptance Testing (UAT).

For best practices on Workplace deployments, refer to [2]. In the compliance testing, one golden image was built and accessed for installation of Workplace and CA certificate for encrypted connection with SBCE. The completed golden image was then replicated to create three virtual desktops for UAT that were used in the compliance test.

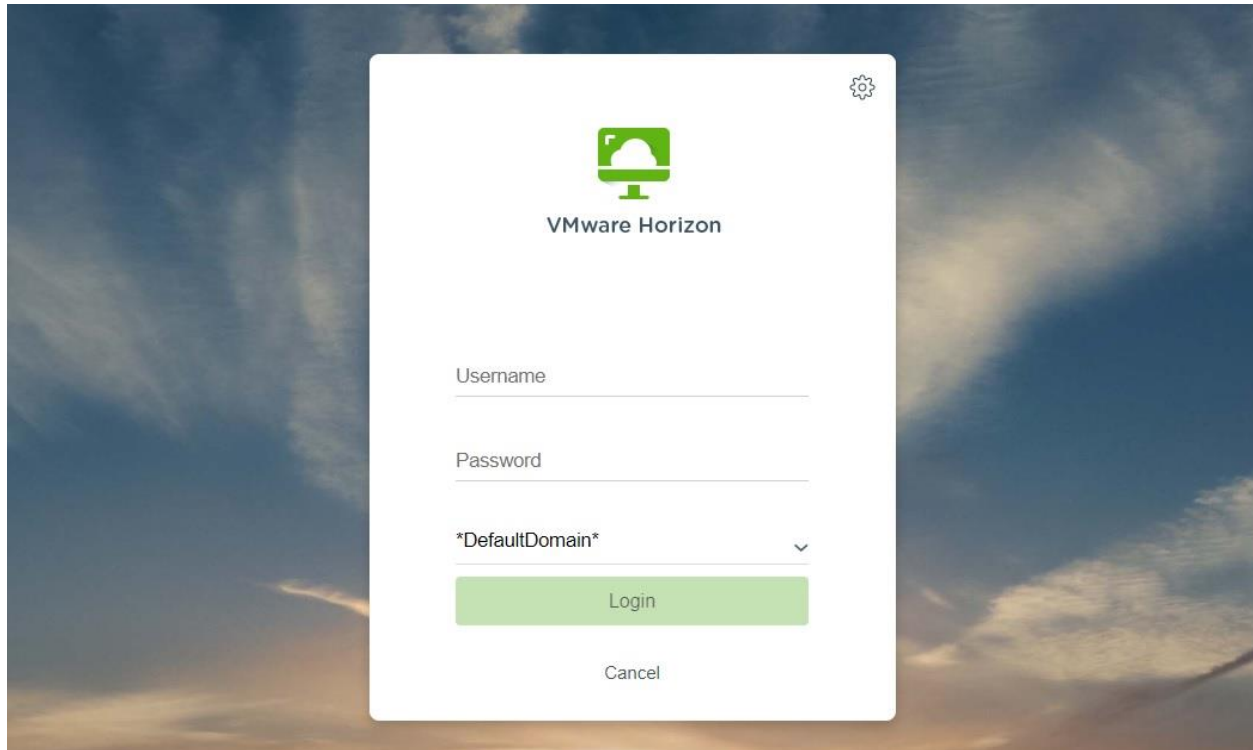
### 9.2.1. Access Image

From the administrator PC, access the customer specific portal in an Internet browser window by using the URL provided by Dizzion. The **VMware Horizon** screen below is displayed.

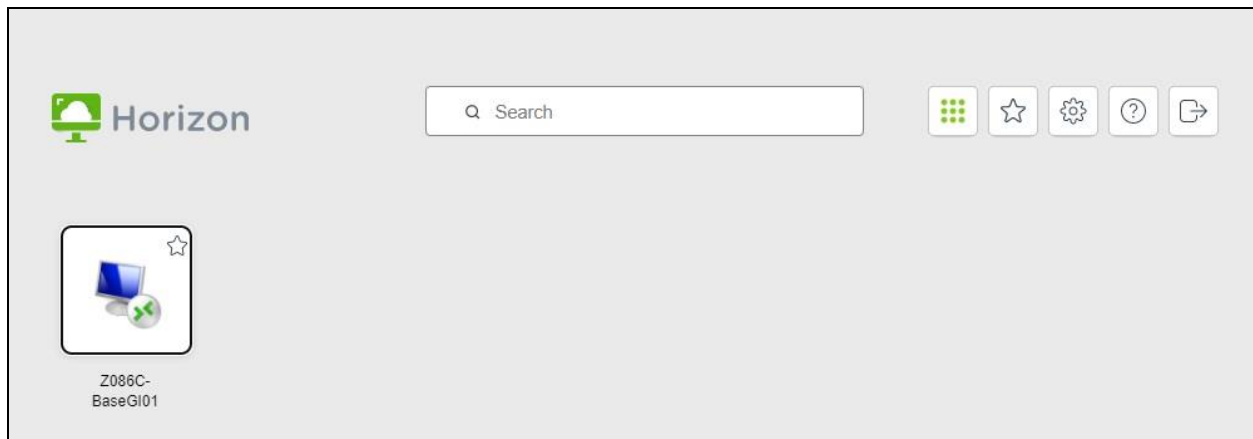
Select the desired connection method. In the compliance testing, the **VMware Horizon HTML Access** method was used.



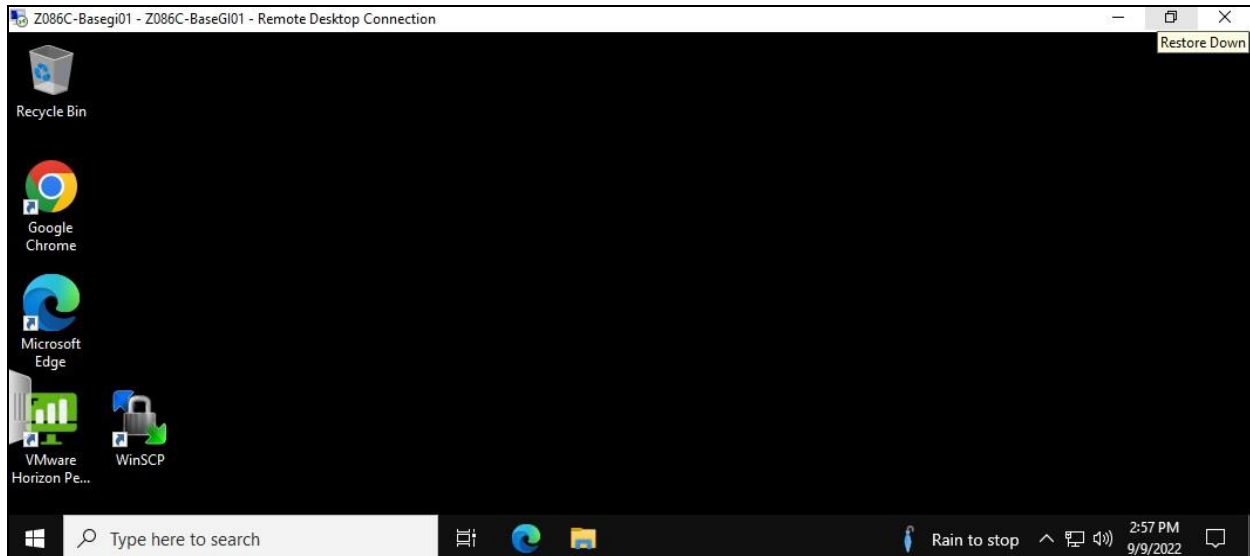
The screen below is displayed next. Log in with the credentials provided by Dizzion.



The **Horizon** screen below is displayed with other non-relevant golden images removed for security reasons. Double click on the pertinent golden image, in this case **Z086C-BaseGI01**.



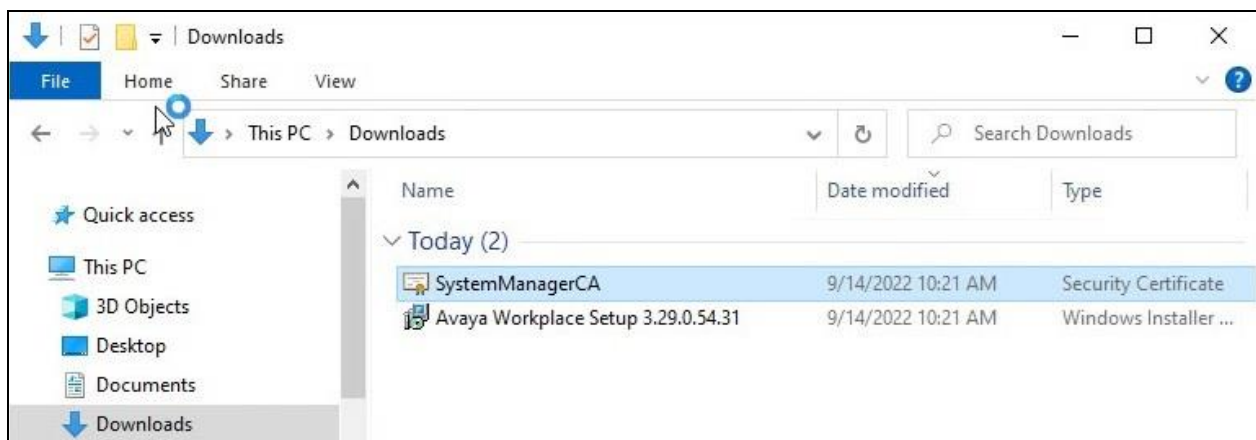
The **Windows Security** (not shown) pop-up screen is displayed. Enter the credentials provided by Dizzion. The **Remote Desktop Connection** screen below is displayed next. Note that the pre-installed browsers and applications shown on the desktop are defaults for all golden images, and that any non-needed application can be removed when the solution goes into production.



### 9.2.2. Copy Workplace and CA Certificate

Typically there is a VPN tunnel between the customer network and Dizzion for remote desktop connection for administrators. The VPN tunnel is used by customer administrators to access golden images with ability to share local drives. The needed application and certificate files on local drives of the administrator local PCs can then be copied to the golden images.

In the compliance testing, an alternate method using Dropbox cloud storage was used in place of VPN tunnel. The pertinent Workplace window installer file and the CA certificate from **Section 6.4** were uploaded to Dropbox from the DevConnect test engineer local PC, and then manually downloaded to the golden image via an Internet browser connection with Dropbox. The screenshot below shows the downloaded files in the **Downloads** folder of the golden image.



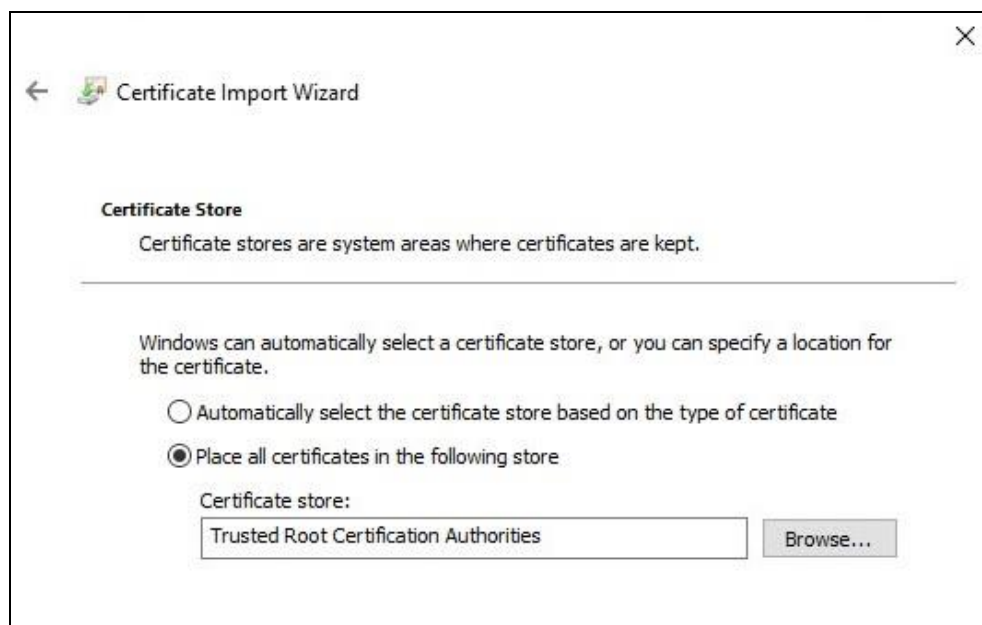


### 9.2.3. Install CA Certificate

Right click on the CA certificate from **Section 9.2.2** and select **Install Certificate**. The **Welcome to the Certificate Import Wizard** screen is displayed. For **Store Location**, select **Local Machine**, which is an important setting for the certificate to apply to all users.



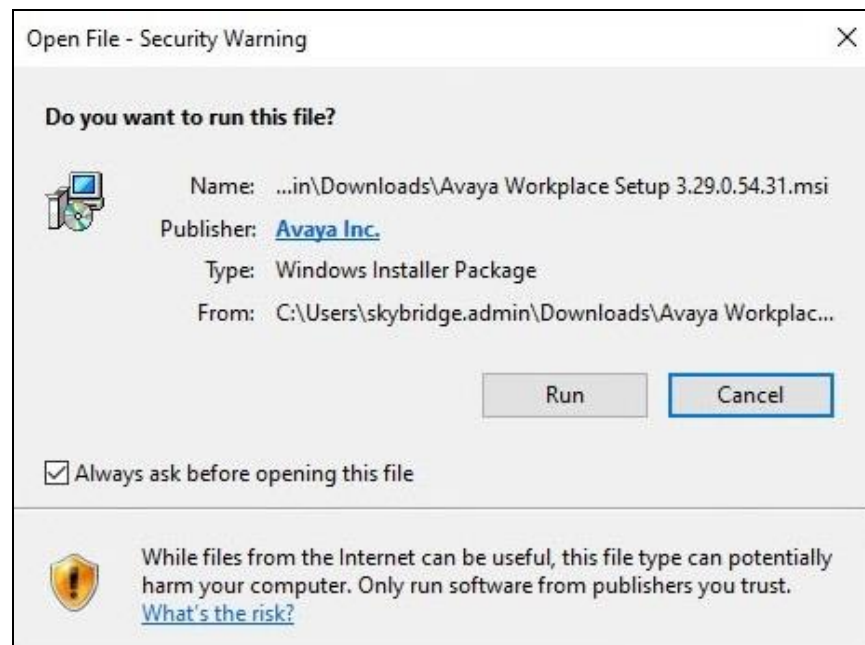
In the next **Certificate Store** screen, place the certificate in the **Trusted Root Certification Authorities** store as shown below. Proceed to complete the certificate installation.



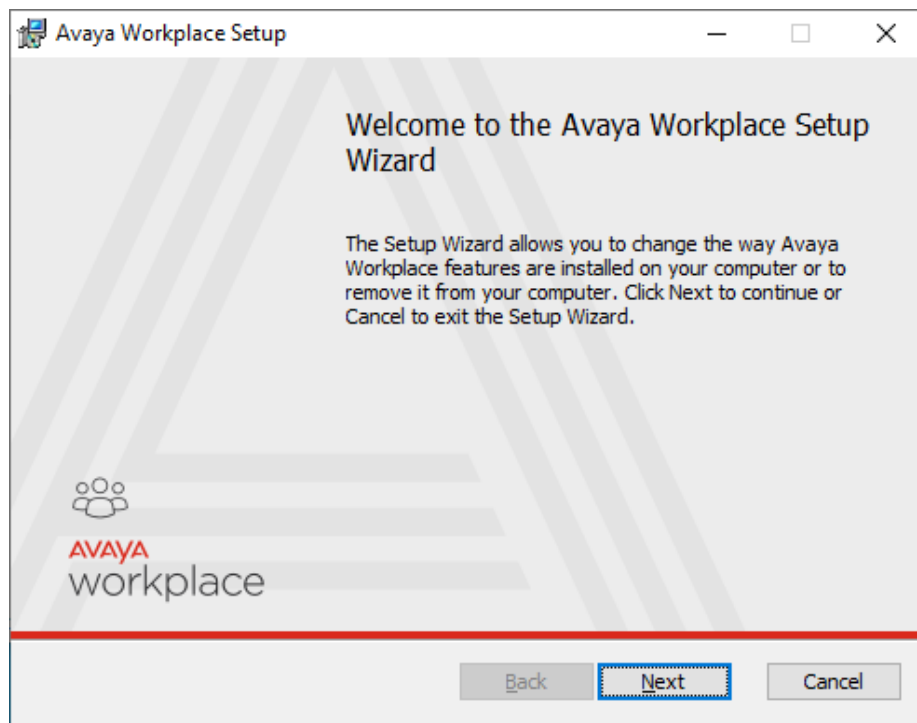


### 9.2.4. Install Workplace

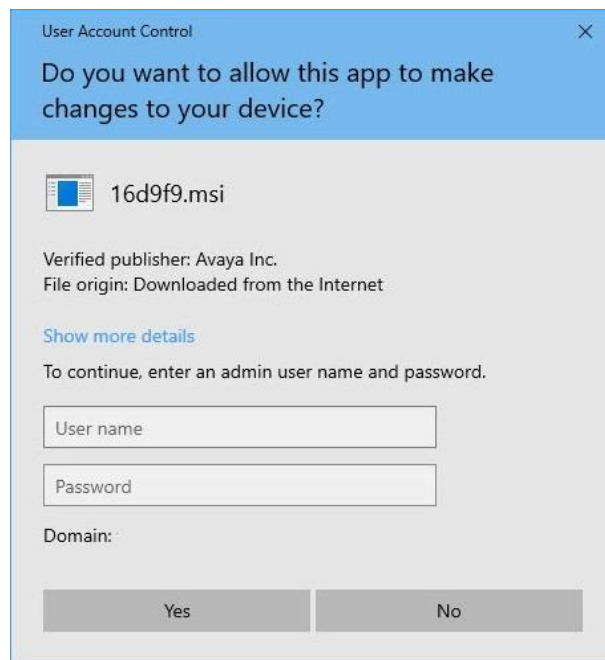
Right click on the Workplace windows installer file from **Section 9.2.2** and select **Install** (not shown). The **Open File – Security Warning** screen is displayed, click **Run**.



The **Avaya Workplace Setup** screen is displayed next. Continue the installation with acceptance of License Agreement and use of default values in the remaining screens.



Toward the end of installation, the **User Account Control** screen below is displayed. Note that the displayed domain information is removed from the screenshot for security reasons. Enter the pertinent administrator credentials from Dizzion to complete the installation.

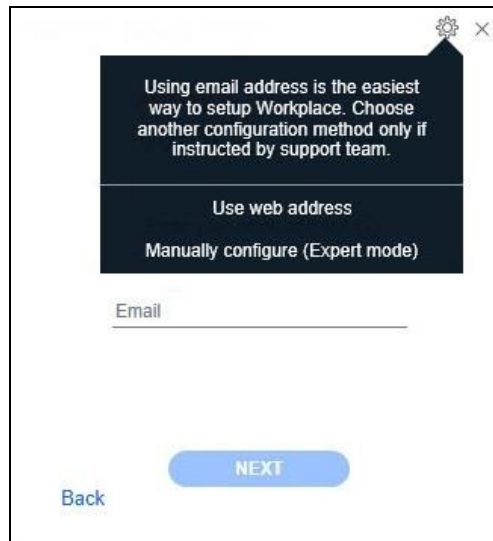


### 9.2.5. Administer Workplace

Upon completion of Workplace installation, the application is auto launched as shown below. Select **Configure my account**.



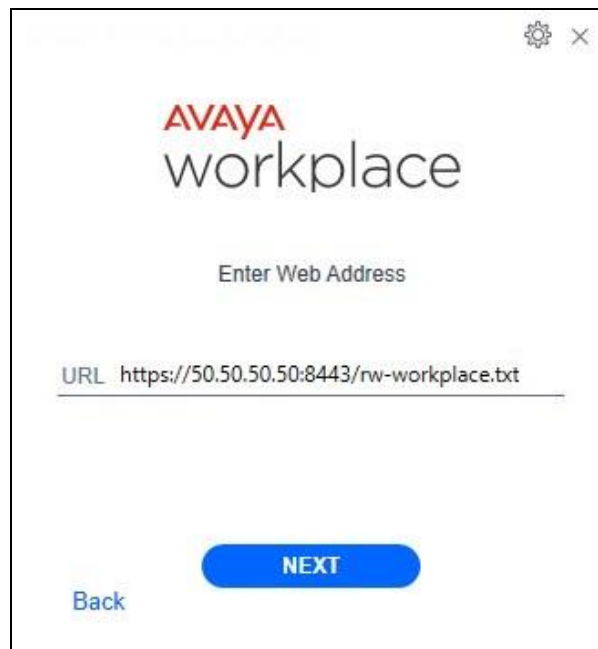
In the updated screen, select the **Options and Settings** icon in the upper right corner followed by **Use web address** from the drop-down list.



The screenshot shows a configuration window for Avaya Workplace. At the top right, there is a settings gear icon and a close 'X' icon. A dark blue message box contains the text: "Using email address is the easiest way to setup Workplace. Choose another configuration method only if instructed by support team." Below this, there are two options: "Use web address" and "Manually configure (Expert mode)". Under "Use web address", there is an "Email" input field. At the bottom, there is a "Back" link and a blue "NEXT" button.

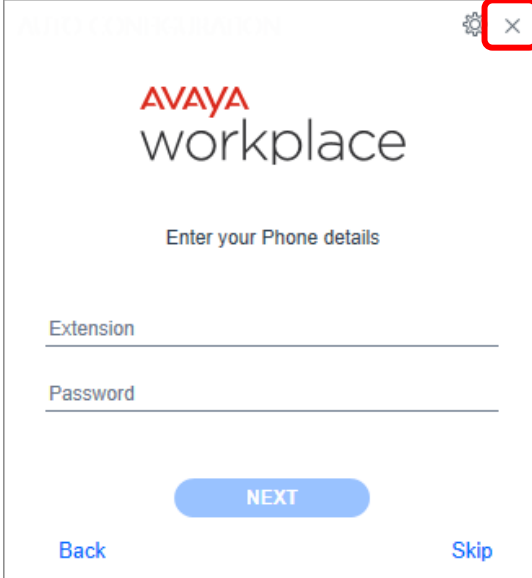
In the updated screen below, enter the URL **https://50.50.50.50:8443/rw-workplace.txt**, where **50.50.50.50** is the IP address of the SBCE public interface for remote workers from **Section 5.2**, and **8443** is the HTTPS file transfer port for remote workers from **Section 5.15**, and **rw-workplace.txt** is the Workplace settings file for remote workers from **Section 8**.

Verify that the URL can be accepted without problems, indicating successful connection with SBCE and obtainment of file.



The screenshot shows the Avaya Workplace setup screen. At the top, the "AVAYA workplace" logo is displayed. Below the logo, the text "Enter Web Address" is shown. There is a "URL" input field containing the text "https://50.50.50.50:8443/rw-workplace.txt". At the bottom, there is a "Back" link and a blue "NEXT" button.

The screen below is displayed next, click on the **Close Window** icon on the upper right to close the application.

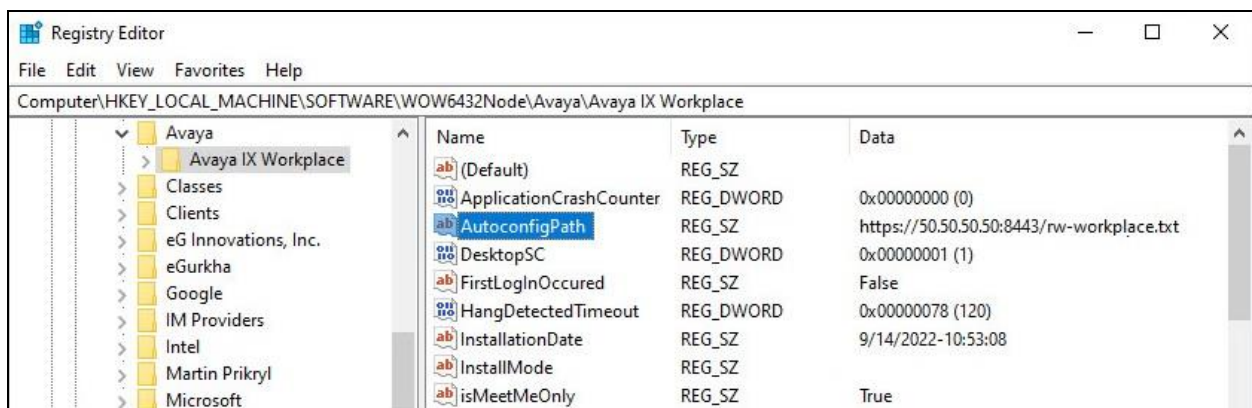


The image shows the Avaya workplace login window. It has a title bar with a gear icon and a close button (X) which is highlighted with a red square. The main content area has the 'AVAYA workplace' logo, the text 'Enter your Phone details', and two input fields labeled 'Extension' and 'Password'. At the bottom, there are three buttons: 'Back', 'NEXT' (highlighted in blue), and 'Skip'.

### 9.2.6. Administer Registry

In the Windows search bar, enter **regedit** to display the **Registry Editor** screen. Navigate to the **Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\Avaya\Avaya IX Workplace** directory as shown below.

Select **Avaya IX Workplace** in the left pane to display a list of associated registry parameters. Double click on the **AutoconfigPath** parameter and set the value to the same URL in **Section 9.2.5**. This registry setting allows for the settings file to be auto discovered upon launch of Workplace.



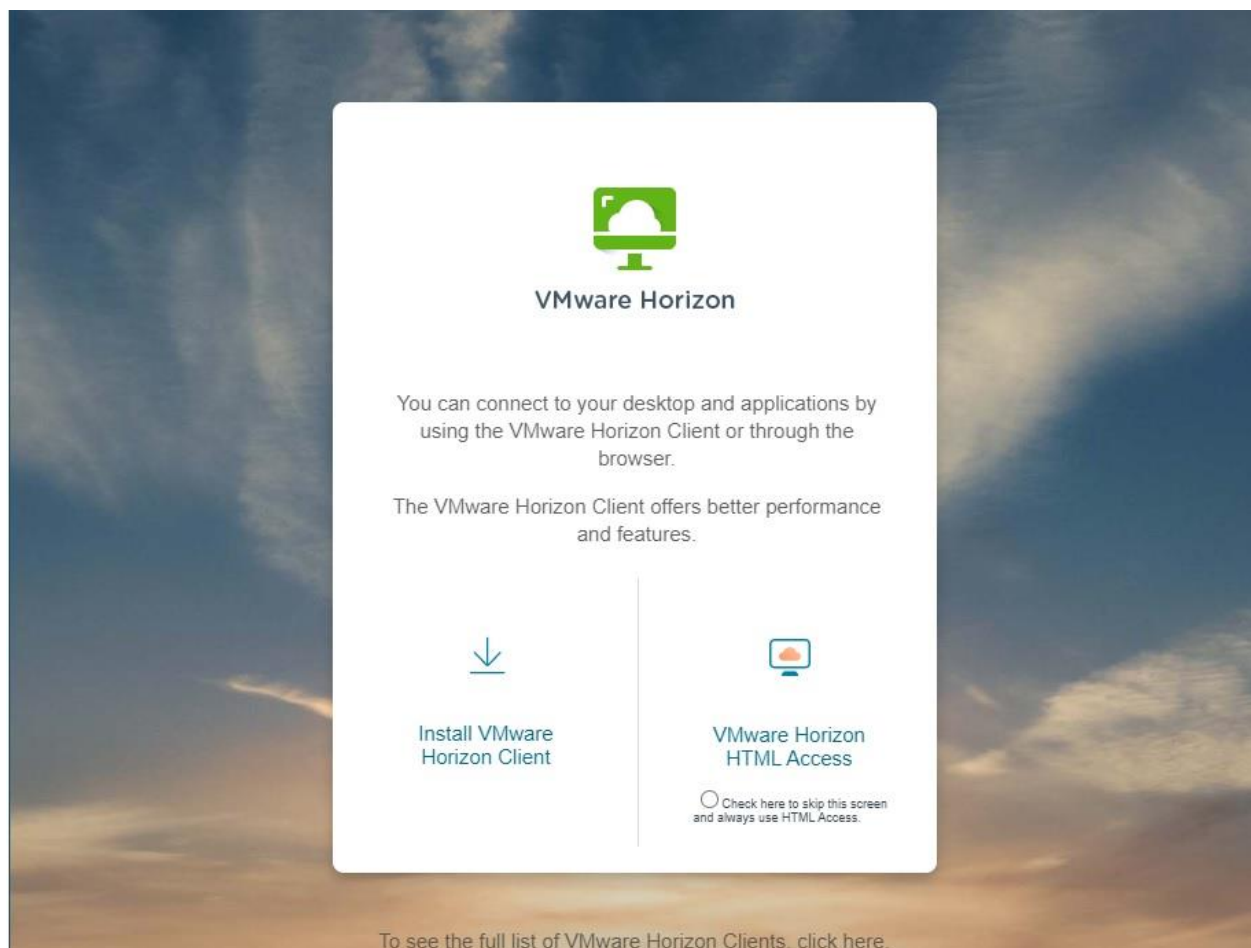
## 10. Verification Steps

This section provides the tests that can be performed to verify proper configuration of SBCE, System Manager, Session Manager, and Workplace on DaaS.

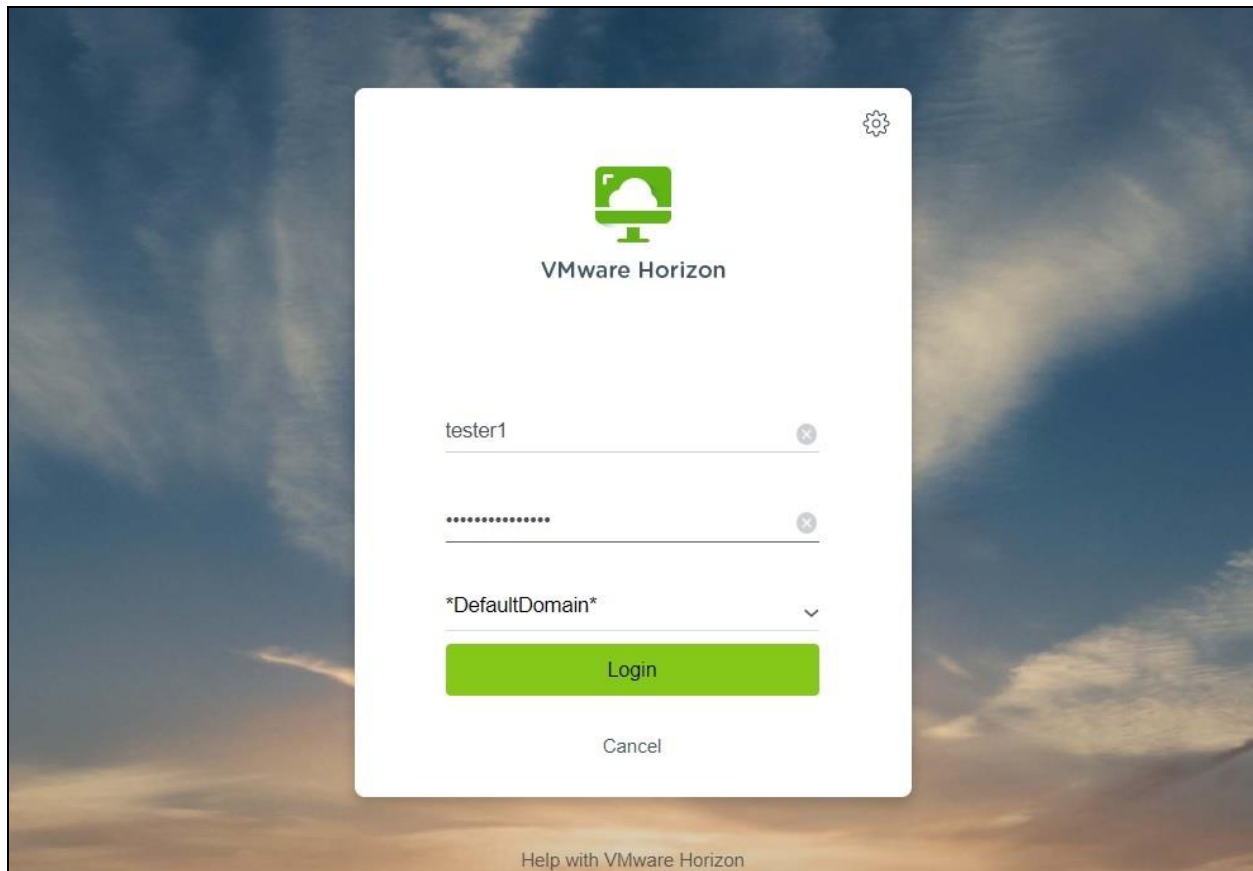
### 10.1. Verify Avaya Workplace on Dizzion DaaS Complete

From an agent user's home PC on the internet, access the customer specific portal in an Internet browser window by using the URL provided by Dizzion. The **VMware Horizon** screen below is displayed.

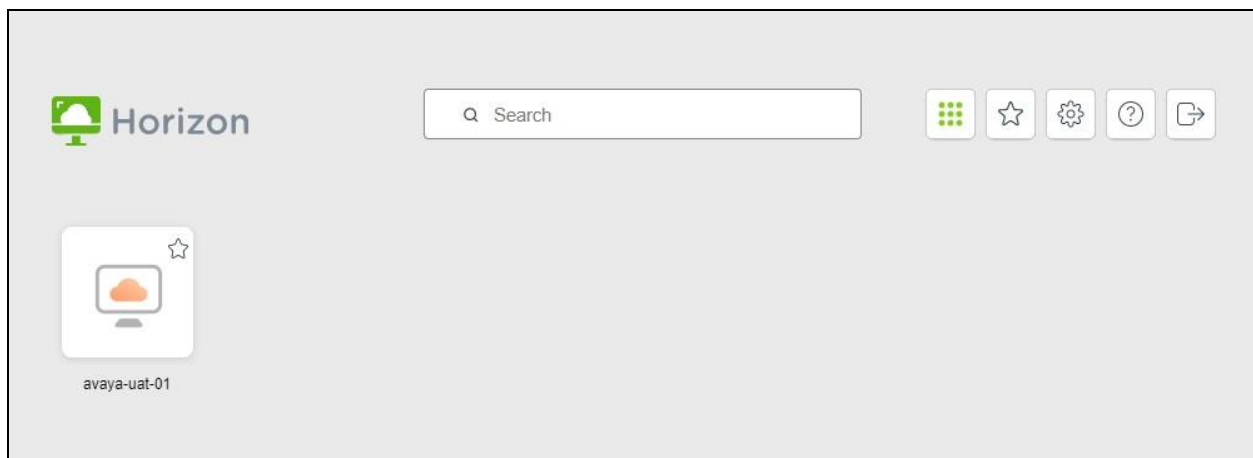
Select the desired connection method. Note that local drive sharing is only supported by the **VMware Horizon Client** method. Both methods were used in the compliance testing, and screenshots captured below are from the **VMware Horizon HTML Access** method.



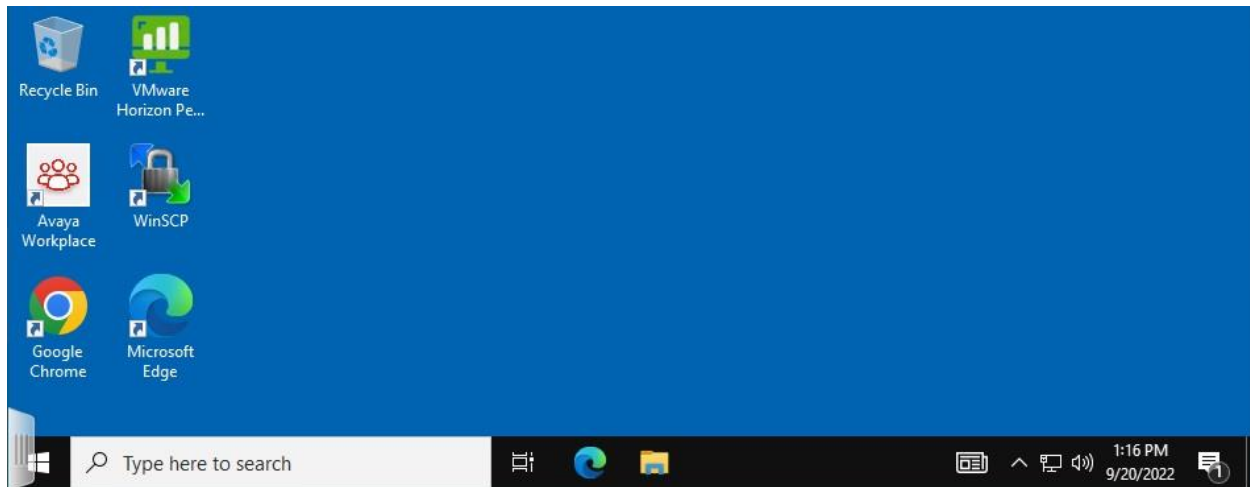
The screen below is displayed. Log in with user credentials provided by the customer administrator.



The **Horizon** screen below is displayed with the dedicated UAT assigned to this user. Note that Dizzion can support dedicated or floating virtual desktops, and the dedicated method was used in the compliance testing. Select the dedicated UAT, in this case **avaya-uat-01**.



Double click on the **Avaya Workplace** icon from the virtual desktop to launch the application.

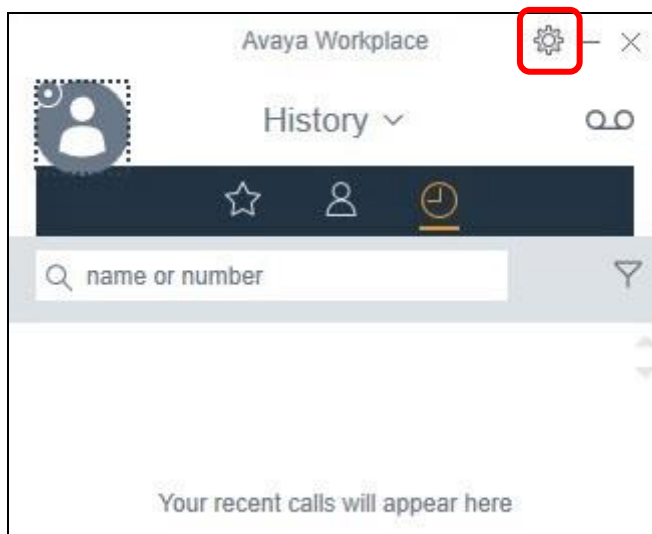


The screen below is displayed upon initial access. Enter the pertinent agent station extension and password from **Section 3**.

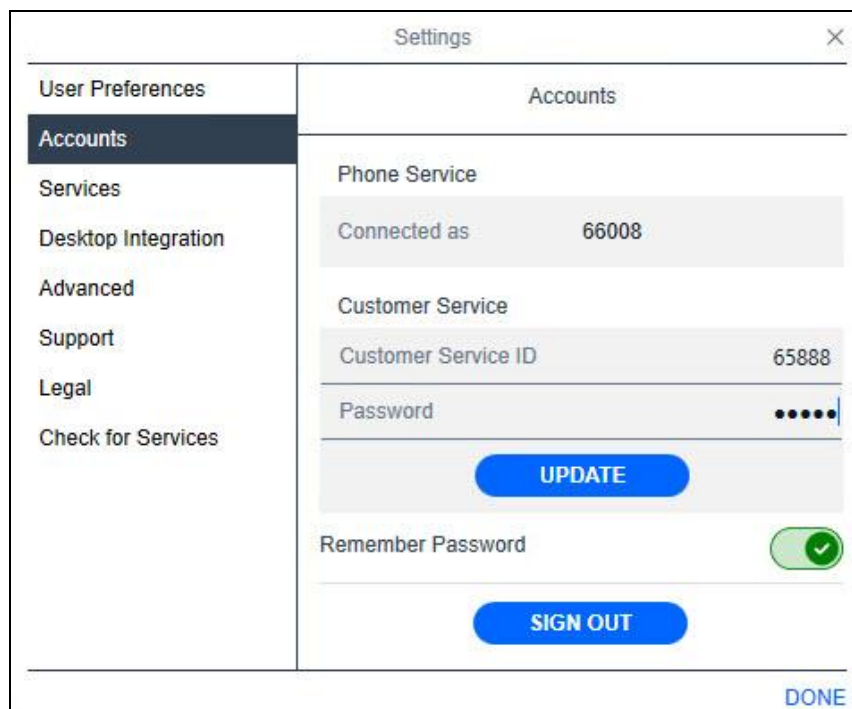


The **Welcome to Avaya Workplace!** (not shown) screen may be displayed next, depending on the settings file, and can be browsed through or skipped if already familiar with the application.

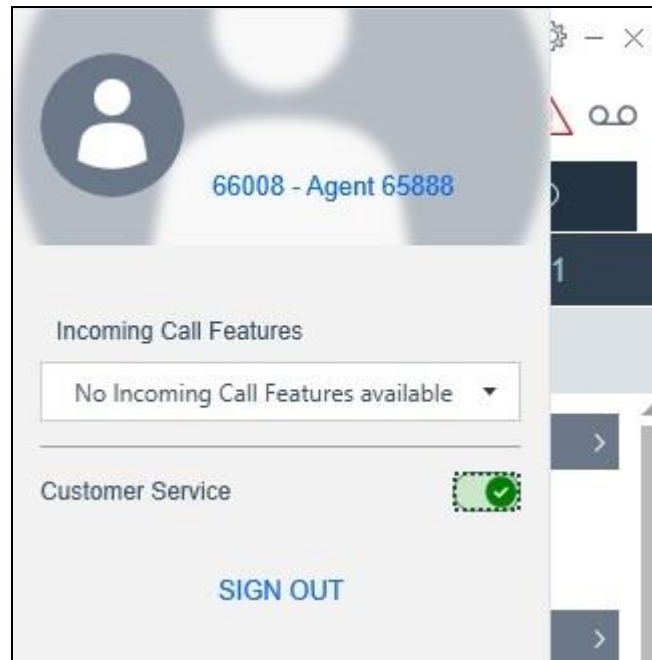
In the compliance testing, the **Avaya Workplace** screen below is displayed. Note that features displayed in the lower portion of screen are determined by the Workplace settings file and can therefore vary. Select the **Options and Settings** icon in the upper right corner.



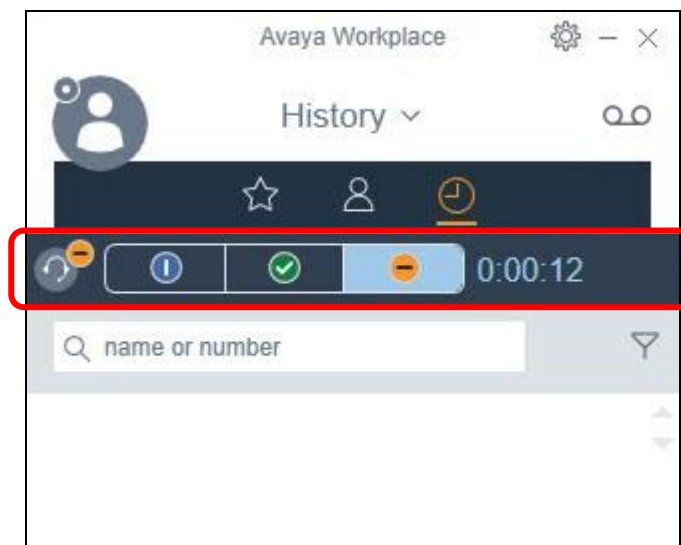
The **Settings** screen is displayed. Select **Accounts** in the left pane to display the **Accounts** screen. Under **Customer Service**, enter the assigned agent ID and password for the agent from **Section 3**, as shown below. Select **UPDATE** followed by **DONE**.



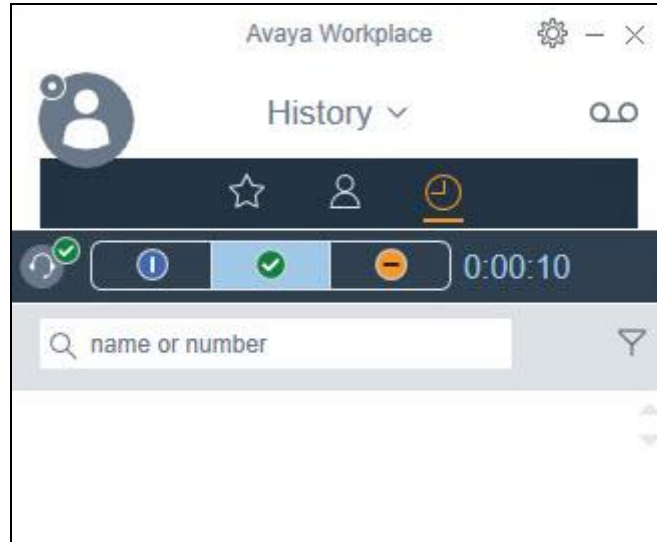
From the main Workplace screen below, click on the avatar icon and enable **Customer Service** from the drop-down as shown below.



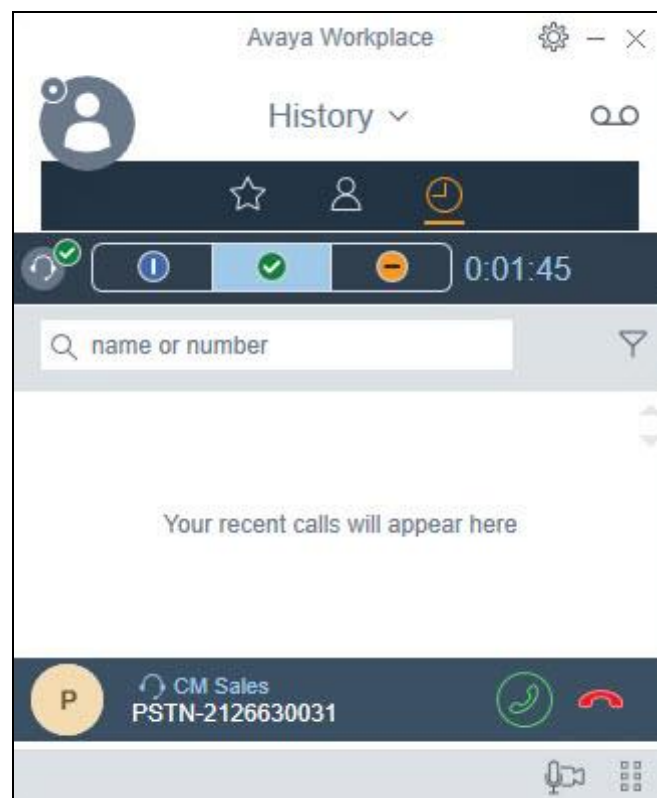
The **Avaya Workplace** screen is updated with an Agent bar as shown below. Verify that the Agent bar reflects agent in the amber **Not Ready (AUX)** state. Select the green **Ready** icon.



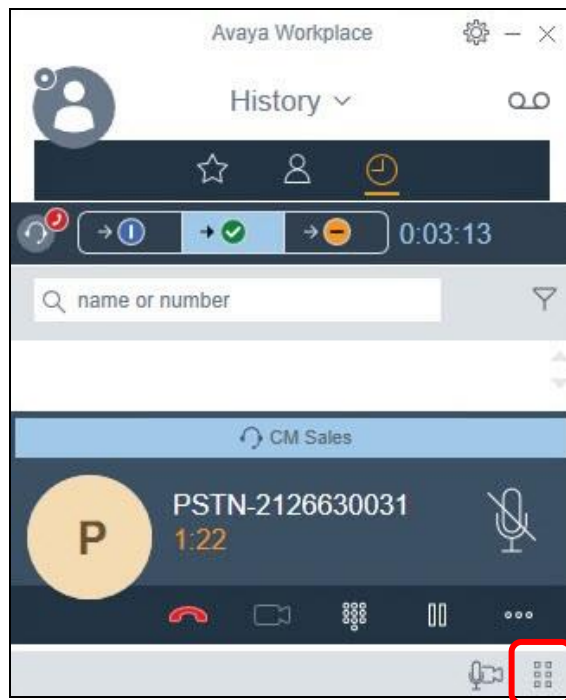
Verify that the Agent bar is updated reflecting agent in the green **Ready** state.



Place an incoming ACD call from the PSTN. Verify that the available agent hears alerting via the virtual desktop to his/her USB headset connected to the local PC, and that the call is reflected in the bottom of the **Avaya Workplace** screen. Click on the green handset icon in the bottom of screen.



Verify that the agent is connected to the PSTN caller with two-way talk paths. Click on the **More options** icon in bottom right of screen and select **Call Statistics** from the drop-down.

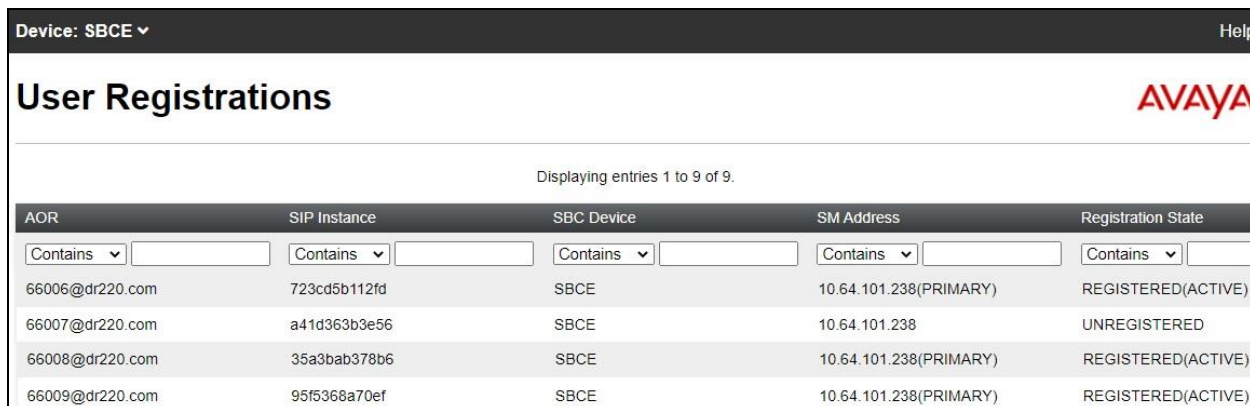


Verify that the **CALL STATISTICS** screen is displayed with acceptable values for audio quality related parameters such as **Round Trip delay** and **Jitter Local / Remote**, as shown below.

CALL STATISTICS			×
Audio statistics			
Video statistics			
Collaboration			
Codec	PCMU		
Encryption	AES 128 / SHA 1 HMAC 80		
Packetization	20 ms		
Round Trip delay	44 ms		
Packets Sent / Received	3165 / 3155		
Bytes Sent / Received	538050 / 504800		
Loss Local / Remote	0 % / 0 %		
Jitter Local / Remote	1 ms / 9 ms		
Buffer Current / Pref	21 ms / 20 ms		
Packet lost	0 %		
Discard Rate	0 %		

## 10.2. Verify Avaya Session Border Controller for Enterprise

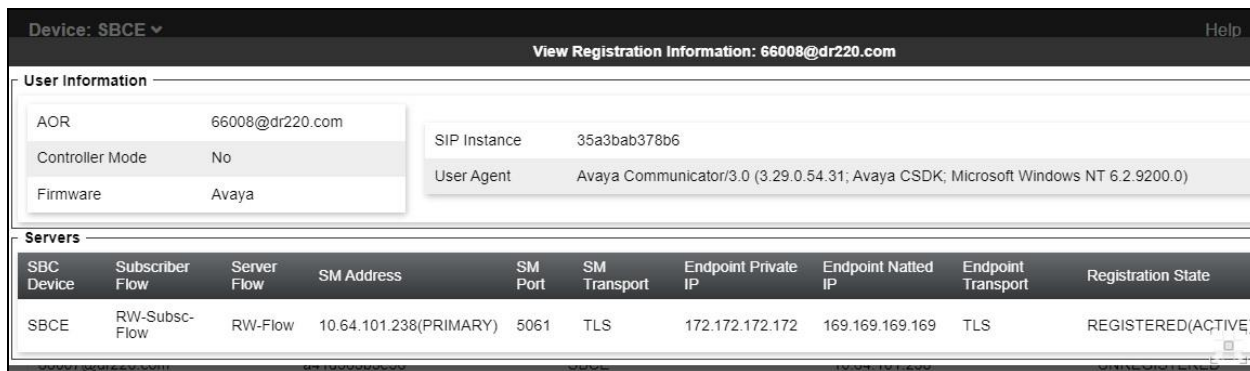
From the SBCE web-based interface, select **Status** → **User Registrations** (not shown) from the top menu to display the **User Registrations** screen. Verify that the listing includes the logged in supervisor and agents from **Section 3** with **Registration State** of **REGISTERED (ACTIVE)** as shown below.



AOR	SIP Instance	SBC Device	SM Address	Registration State
66006@dr220.com	723cd5b112fd	SBCE	10.64.101.238(PRIMARY)	REGISTERED(ACTIVE)
66007@dr220.com	a41d363b3e56	SBCE	10.64.101.238	UNREGISTERED
66008@dr220.com	35a3bab378b6	SBCE	10.64.101.238(PRIMARY)	REGISTERED(ACTIVE)
66009@dr220.com	95f5368a70ef	SBCE	10.64.101.238(PRIMARY)	REGISTERED(ACTIVE)

Scroll the screen to the right as necessary to locate and select **Details** (not shown) associated with a registered user, in this case **66008@dr220.com**.

Verify that the screen below is displayed, reflecting encrypted **TLS** connection with the public IP address of DaaS in **Endpoint Natted IP**. Note that the IP addresses are masked in the screenshot below for security reasons.



SBC Device	Subscriber Flow	Server Flow	SM Address	SM Port	SM Transport	Endpoint Private IP	Endpoint Natted IP	Endpoint Transport	Registration State
SBCE	RW-Subsc-Flow	RW-Flow	10.64.101.238(PRIMARY)	5061	TLS	172.172.172.172	169.169.169.169	TLS	REGISTERED(ACTIVE)

### 10.3. Verify Avaya Aura® Session Manager

From the System Manager web-based interface, select **Elements** → **Session Manager** → **System Status** → **User Registrations** from the top menu to display the **User Registrations** screen.

Verify that supervisor and agent users from **Section 3** are registered, as shown below with a check in the **Remote Office**, **AST Device**, and **Registered Prim** columns.

AVAYA

Users

Elements

Services

Widgets

Shortcuts

Aura® System Manager 8.1

Search

admin

Home

Session Manager

S...

Help ?

User Registrations

Select rows to send notifications to devices. Click on Details column for complete registration status.

View

Default

Export

Force Unregister

AST Device Notifications:

Reboot

Reload

Failback

As of 2:38 PM

Advanced Search

9 Items

Show

All

Filter: Enable

	Details	Address	First Name	Last Name	Actual Location	IP Address	Remote Office	Shared Control	Simult. Devices	AST Device	Registered			
											Prim	Sec	Surv	Visiting
<input type="checkbox"/>	<a href="#">Show</a>	66006@dr220.com	SIPRW 6	Avaya	DR-Loc	10.64.101.222	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<a href="#">Show</a>	---	SIPRW 7	Avaya	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<a href="#">Show</a>	66008@dr220.com	SIPRW 8	Avaya	DR-Loc	10.64.101.222	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<a href="#">Show</a>	66009@dr220.com	SIPRW 9	Avaya	DR-Loc	10.64.101.222	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<a href="#">Show</a>	---	Vantage	Avaya	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Select : All, None

## 11. Conclusion

These Application Notes describe the configuration steps required for Dizzion DaaS Complete to successfully interoperate with Avaya Workplace Client for Windows. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

## 12. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 13, June 2022, available at <http://support.avaya.com>.
2. *Administering Avaya Aura® Session Manager*, Release 8.1.x, Issue 12, June 2022, available at <http://support.avaya.com>.
3. *Administering Avaya Session Border Controller for Enterprise*, Release 8.1.x, Issue 12, June 2022, available at <http://support.avaya.com>.
4. *Planning for and Administering Avaya Workplace Client for Android, IOS, Mac, and Windows*, September 20, 2022, available at <http://support.avaya.com>.
5. *Using Avaya Workplace Client for Android, IOS, Mac, and Windows*, September 20, 2022, available at <http://support.avaya.com>.
6. *Cloud Delivered Desktops for Contact Centers Data Sheet*, available at <https://dizzion.com>.



---

**©2023 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](mailto:devconnect@avaya.com).