



Avaya Solution & Interoperability Test Lab

Application Notes for ION Networks Netgard Privileged Gateway with Avaya Aura® Suite, Avaya Session Border Controller for Enterprise, Avaya Messaging, Avaya Breeze, and Avaya IP Office - Issue 1.0

Abstract

These Application Notes describe the configuration steps required to enable ION Networks Netgard Privileged Gateway to provide secure access to Avaya Aura® Suite, Avaya Session Border Controller for Enterprise, Avaya Messaging, Avaya Breeze, and Avaya IP Office. The Avaya Aura® Suite included Avaya Aura® Communication Manager, Avaya Aura® Media Server, Avaya Aura® System Manager, Avaya Aura® Session Manager, and Avaya Aura® Application Enablement Services. ION Networks Netgard Privileged Gateway is a secure, remote access gateway that allows enterprises to manage privileged user access to critical voice and data services. In this compliance test, ION Networks Netgard Privileged Gateway provided secure access to the aforementioned Avaya endpoints using SSH, web access via HTTPS, Remote Desktop (RDP), and thick clients.

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

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

1. Introduction

These Application Notes describe the configuration steps required to configure ION Networks Netgard Privileged Gateway (NPG) to provide secure access to Avaya Aura® Suite, Avaya Session Border Controller for Enterprise, Avaya Messaging, Avaya Breeze, and Avaya IP Office. The Avaya Aura® Suite included Avaya Aura® Communication Manager, Avaya Aura® Media Server, Avaya Aura® System Manager, Avaya Aura® Session Manager, and Avaya Aura® Application Enablement Services (AES). ION Networks Netgard Privileged Gateway is a secure, remote access gateway that allows enterprises to manage privileged user access to critical voice and data services. In this compliance test, ION Networks Netgard Privileged Gateway provided secure access to the aforementioned Avaya endpoints using SSH, web access via HTTPS, SFTP, Remote Desktop (RDP), and thick clients.

Users log into NPG and establish a connection to one or more Avaya endpoints. The connection is “tunneled” through NPG from the user’s PC to the Avaya endpoint(s). NPG assigns an IP address, from a pre-configured pool of IP addresses, to the Avaya endpoint to mask the actual IP address of the Avaya endpoint.

The connection is made using a specific protocol handler, such as SSH, SFTP, or HTTPS, or a “generic” protocol handler. In addition to the protocol handler, a port(s) must also be specified for the connection. When a specific protocol handler is used for the connection, NPG provides a hyperlink that could be clicked to open the appropriate access application. For example, for the HTTPS protocol handler, NPG could open a web browser, which would be set as the default application for HTTPS on the user’s PC. A “generic” protocol handler is used when the application used to access an endpoint is proprietary or requires multiple ports; for example, a thick client such as IP Office Manager. In this case, the user would manually open the thick client, such as IP Office Manager. The user can then use the assigned IP address to open an application, such as a thick client, to access the Avaya endpoint. The user would then log in with their user credentials. Once the user no longer requires the connection, the user would close the NPG connection.

Additional features provided by NPG include administrator approval for connections and recording connection activity and playback.

2. General Test Approach and Test Results

The interoperability compliance test included feature and serviceability testing. The feature testing focused on establishing connections through NPG to provide access to Avaya endpoints using SSH, SFTP, HTTPS, RDP, and thick clients and closing connections.

The serviceability testing focused on verifying that the NPG server come back into service after a reboot or re-connecting the Ethernet cable.

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 this DevConnect Application Note 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 Netgard Privileged Gateway used SFTP, SSH, and HTTPS to some Avaya systems.

2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- Establishing connections through NPG to Avaya endpoints.
- Closing connections to Avaya endpoints.
- Accessing Avaya endpoints using SSH, SFTP, HTTPS, RDP, and thick clients using connections established through NPG.
- Establishing multiple connections to the same and different Avaya endpoints via a single user.
- Establishing multiple connections to the same and different Avaya endpoints across different users.
- Administrator approval/rejection of connection requests.
- Recording a playing back connection activity. This requires the ION Networks Desktop Agent software.
- Proper system recovery after rebooting and re-establishing IP connectivity to NPG.

2.2. Test Results

All test cases passed with the following observations:

- When a connection is made, NPG assigns an IP address from a pool of IP addresses to Avaya endpoints to hide the actual IP address regardless how the "Use Real Addresses" toggle is configured. For the compliance test, the "Use Real Addresses" option was disabled as shown in **Section 6.7**.
- When the SFTP protocol handler is used for a connection, the user should manually open the SFTP application to avoid a problem opening the application using the hyperlink provided by NPG. Alternatively, the "generic" protocol handler may be used with the

SFTP port to prevent a hyperlink from being provided by NPG. This issue has been addressed in all builds subsequent to 1.0.6-11.

2.3. Support

For technical support of ION Networks Netgard Privileged Gateway, contact ION Networks Technical Support via phone, web, or email.

- Phone: +1 (800) 722-8986 (US)
- Web: <https://www.apitech.com/brands/secure-systems-information-assurance/ion/>
- Email: ion.networks.support@apitech.com

3. Reference Configuration

Figure 1 illustrates a sample configuration that supports connections established through NPG from a user PC to Avaya endpoints using SSH, SFTP, HTTPS, Remote Desktop (RDP), and thick clients, such as IP Office Manager, Monitor, and System Status. ION Networks Desktop Agent was also installed on the user PC to support the recording of connection activity.

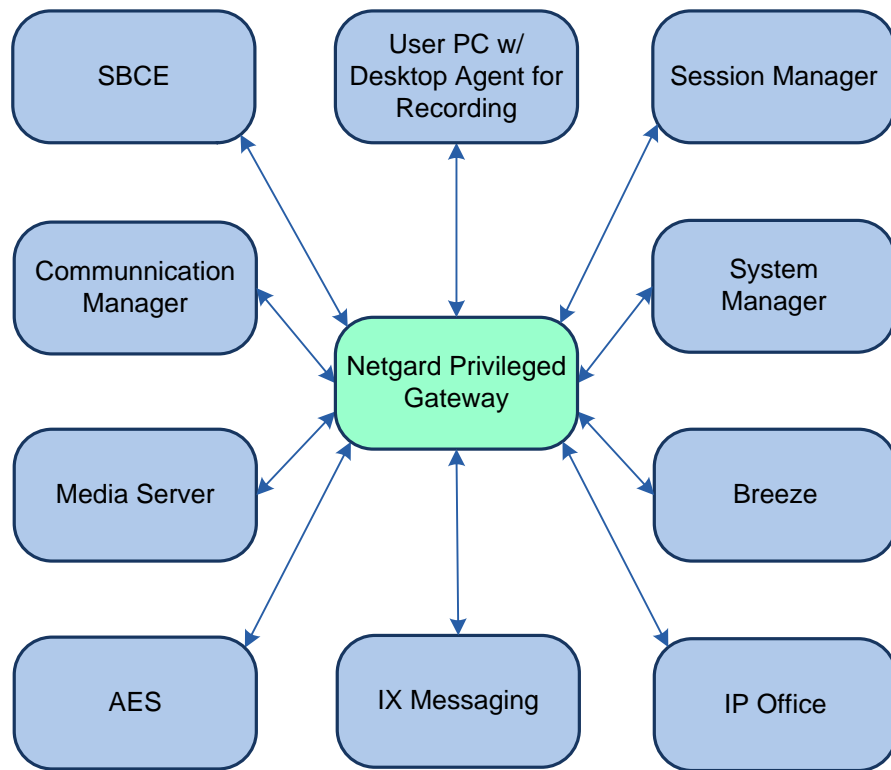


Figure 1: ION Networks Netgard Privileged Gateway with Avaya Endpoints

The table below lists the access methods used for each Avaya endpoint.

Avaya Endpoint	Access Method(s)
Aura® Communication Manager	HTTPS, SSH (including SAT)
Aura® System Manager	HTTPS, SSH
Aura® Session Manager	SSH, SFTP
Aura® Media Server	HTTPS, SSH
Aura® Application Enablement Services	HTTPS, SSH
Session Border Controller for Enterprise <ul style="list-style-type: none">▪ Element Management System (EMS)▪ SBCE	HTTPS SSH, SFTP
Messaging	HTTPS, RDP, Web
Breeze	HTTPS via System Manager, SSH
IP Office Server Edition	HTTPS, SSH, Manager, System Status, and Monitor Applications

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	8.1.3.2.0-FP3SP2
Avaya Aura® Media Server	v.8.0.2.138
Avaya Aura® System Manager	8.1.3.1 Build No. – 8.1.0.0.733078 Software Update Revision No: 8.1.3.1.1012493 Service Pack 1
Avaya Aura® Session Manager	8.1.3.1.813113
Avaya Aura® Application Enablement Services	8.1.3.0.0.25-0
Avaya Session Border Controller for Enterprise	8.1.2.0-31-19809
Avaya Messaging	10.8 SP1 SU3
Avaya Breeze	3.6.0.2.360201
IP Office*	11.1.1.0.0 build 209
ION Networks Netgard Privileged Gateway	1.0.4-20_enc
ION Networks Desktop Agent (required for connection recordings)	1.1.0.10529

** Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500 v2 and also when deployed with IP Office Server Edition in all configurations.*

5. Configure Avaya Endpoints

The login credentials for the Avaya products were established during the software installation. However, additional user accounts may be added as necessary. The references in **Section 9** provide additional information about the ports that may be opened to each Avaya product. No additional configuration is required to allow access to the Avaya products.

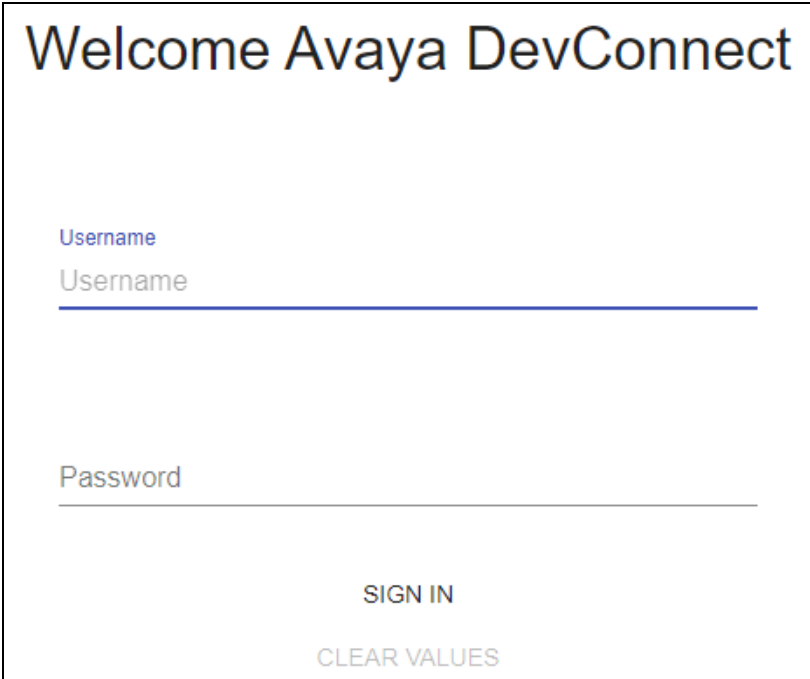
6. Configure ION Networks Netgard Privileged Gateway

This section provides the procedure for configuring Netgard Privileged Gateway (NPG), including IP address pool, users, endpoints, and access control. Configuration of NPG is performed via NPG Web Interface. This section covers the following areas:

- Launch NPG Web Interface
- Administer Networking
- Administer System Setup
- Administer Access Control
- Administer Permissions
- Administer Users
- Administer Endpoints

6.1. Launch NPG Web Interface

Access the NPG Web Interface by using the URL **Error! Hyperlink reference not valid.** in an Internet browser, where *<ip-address>* is the NPG server IP address. Log in with the appropriate credentials.



Welcome Avaya DevConnect

Username

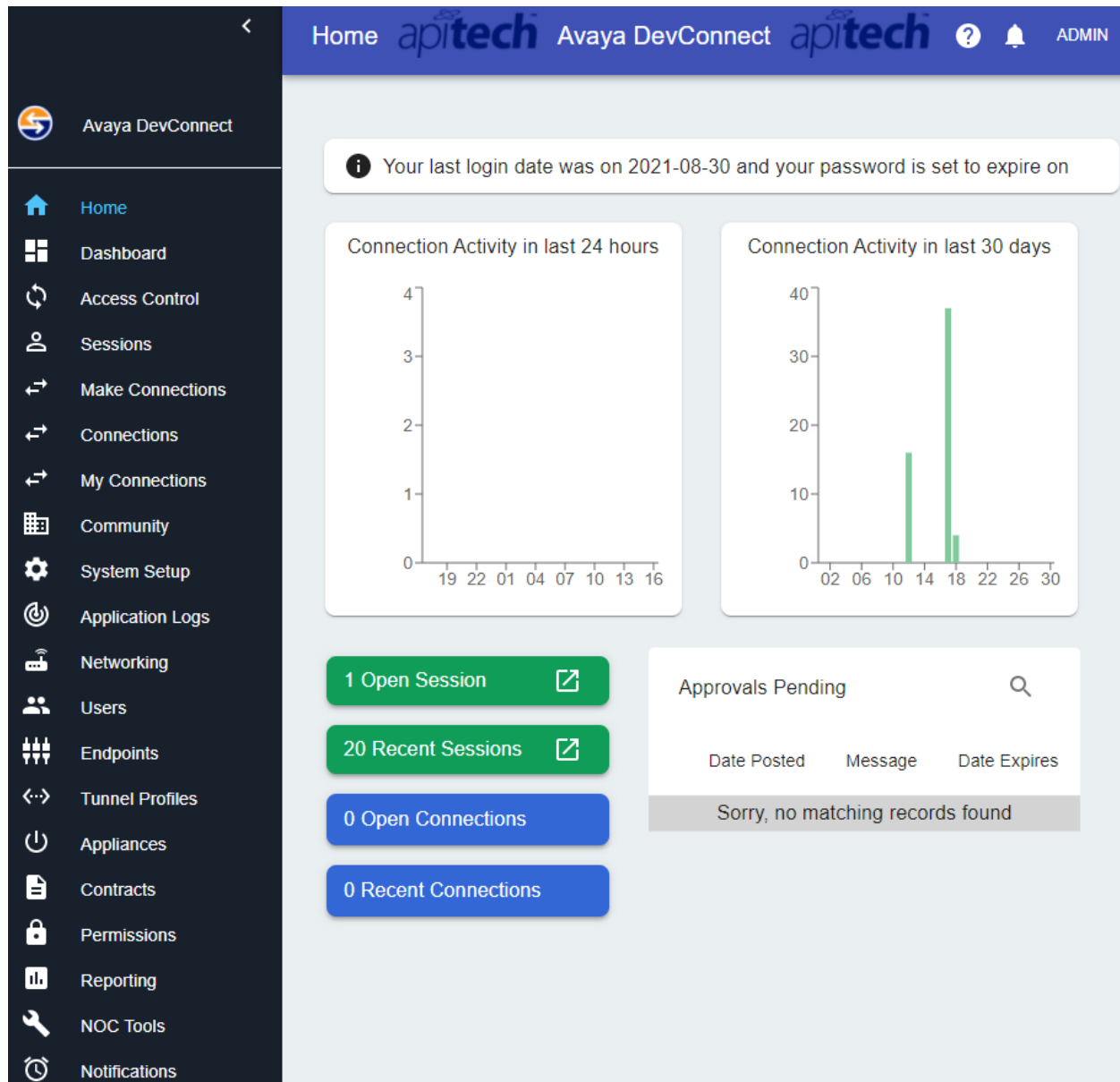
Username

Password

SIGN IN

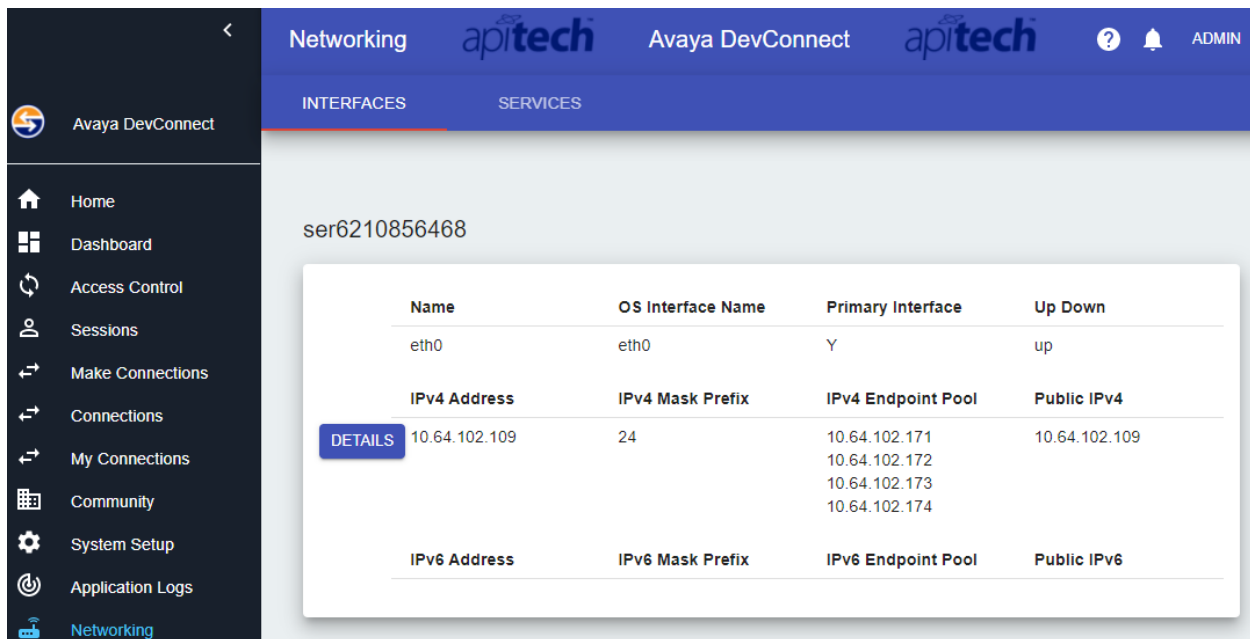
CLEAR VALUES

Once logged in, the following screen is displayed in the NPG Web Interface. The user interface includes administration options in the left pane as shown below.



6.2. Administer Networking

Navigate to **Networking** and select the **Interfaces** tab to configure the **IPv4 Endpoint Pool**. When a connection is made to an Avaya endpoint, an IP address from the endpoint pool is assigned to the endpoint to hide the actual IP address. In the following example, four IP addresses were added to the endpoint pool. The assigned IP address can then be used to access the Avaya endpoint.



The screenshot displays the Avaya DevConnect interface for configuring Networking. The left sidebar contains navigation links: Home, Dashboard, Access Control, Sessions, Make Connections, Connections, My Connections, Community, System Setup, Application Logs, and Networking (selected). The top navigation bar shows 'Networking' and 'Interfaces' (selected). The main content area displays the 'ser6210856468' configuration page. A table lists the interface details:

Name	OS Interface Name	Primary Interface	Up Down
eth0	eth0	Y	up
IPv4 Address	IPv4 Mask Prefix	IPv4 Endpoint Pool	Public IPv4
10.64.102.109	24	10.64.102.171 10.64.102.172 10.64.102.173 10.64.102.174	10.64.102.109
IPv6 Address	IPv6 Mask Prefix	IPv6 Endpoint Pool	Public IPv6

6.3. Administer System Setup

Navigate to **System Setup** and select the **Attributes** tab to add **Models** under **Endpoint Attributes**. In the **Endpoint Attributes** section, click on the **Model** edit icon.


The screenshot displays the Avaya DevConnect System Setup interface. The top navigation bar includes 'System Setup', 'apitech', 'Avaya DevConnect', 'apitech', a help icon, a notification bell, and an 'ADMIN' link. Below this is a secondary navigation bar with 'PROPERTIES', 'LICENSING', 'ATTRIBUTES' (selected), and 'CERTIFICATES'. The left sidebar contains a list of navigation items: Home, Dashboard, Access Control, Sessions, Make Connections, Connections, My Connections, Community, System Setup (highlighted), Application Logs, Networking, Users, Endpoints, Tunnel Profiles, Appliances, Contracts, Permissions, and Reporting. The main content area is divided into two panels: 'User Attributes' and 'Endpoint Attributes'. Each panel has a blue '+' icon in the top right corner. The 'User Attributes' panel lists 11 attributes: 1 Community Id, 2 User, 3 Department, 4 Name, 5 Location, 6 NPG Access Class, 7 Recorded, 8 Technical Role, 9 Phone Number, 10 LoginStatus, and 11 LastLogin. The 'Endpoint Attributes' panel lists 8 attributes: 1 Community Id, 2 Endpoint, 3 Name, 4 Equipment Type, 5 Location, 6 Manufacturer, 7 Model, and 8 Recorded. Each attribute row includes a checkbox, an edit icon (pencil), and a delete icon (trash). At the bottom of each panel, there are radio buttons for 'Summary' (selected) and 'Detail', and an 'Update' button.

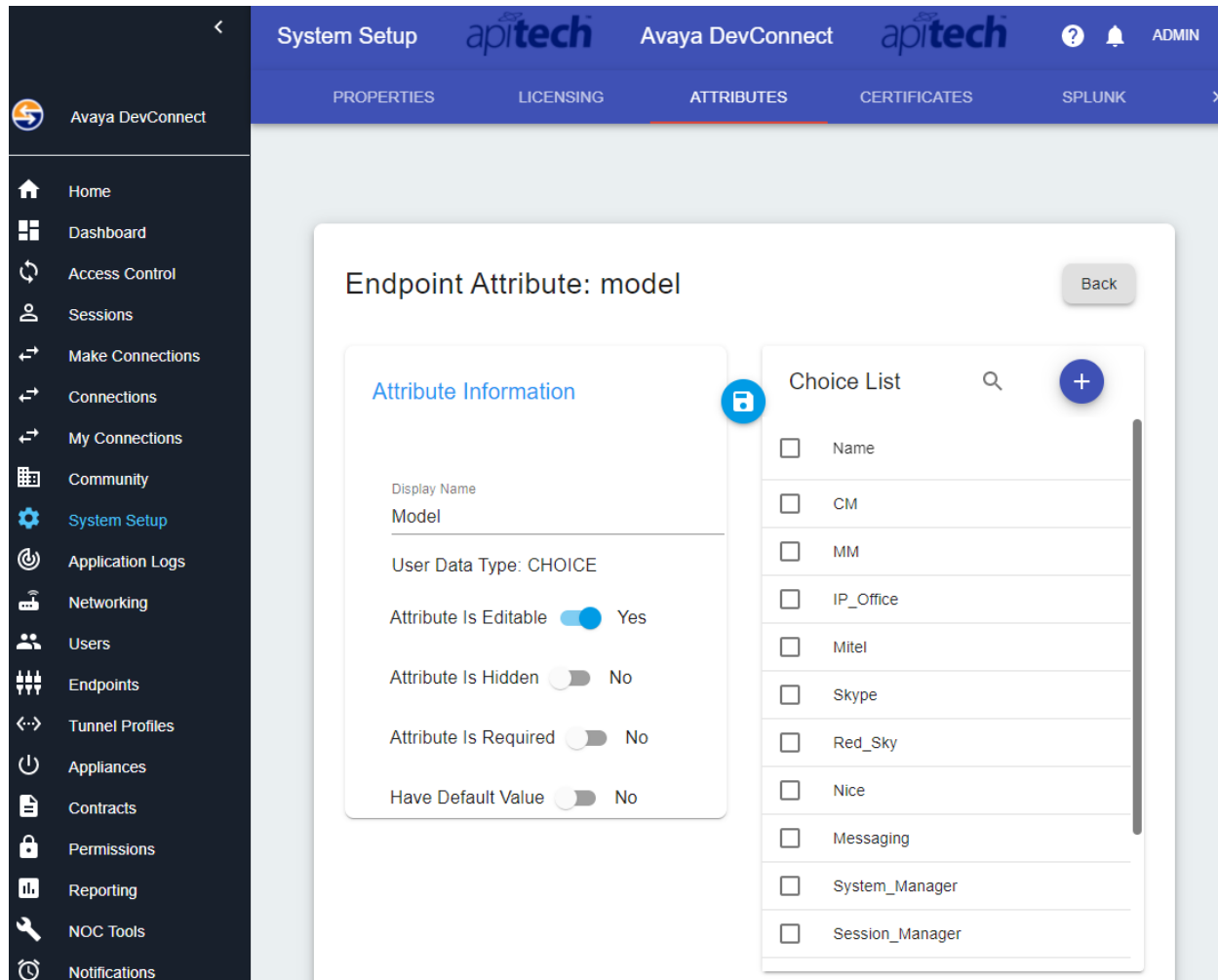
Attribute ID	Attribute Name	Checkbox	Edit Icon	Delete Icon
1	Community Id	<input type="checkbox"/>		
2	User	<input type="checkbox"/>		
3	Department	<input checked="" type="checkbox"/>		
4	Name	<input checked="" type="checkbox"/>		
5	Location	<input checked="" type="checkbox"/>		
6	NPG Access Class	<input checked="" type="checkbox"/>		
7	Recorded	<input checked="" type="checkbox"/>		
8	Technical Role	<input checked="" type="checkbox"/>		
9	Phone Number	<input checked="" type="checkbox"/>		
10	LoginStatus	<input type="checkbox"/>		
11	LastLogin	<input type="checkbox"/>		

☒ Summary ☐ Detail

Attribute ID	Attribute Name	Checkbox	Edit Icon	Delete Icon
1	Community Id	<input type="checkbox"/>		
2	Endpoint	<input type="checkbox"/>		
3	Name	<input checked="" type="checkbox"/>		
4	Equipment Type	<input checked="" type="checkbox"/>		
5	Location	<input checked="" type="checkbox"/>		
6	Manufacturer	<input checked="" type="checkbox"/>		
7	Model	<input checked="" type="checkbox"/>		
8	Recorded	<input checked="" type="checkbox"/>		

☒ Summary ☐ Detail

In the **Choice List** section, click on  to add a model name for an Avaya endpoint. In the example below, a model was added for *CM*, *Media_Server*, *System_Manager*, *Session_Manager*, *Application_Enablement_Services*, *Messaging*, *SBCE*, *Breeze*, and *IP_Office* (not all models are shown below). These model choices will be used in **Section 6.7** when administering **Endpoints**.



System Setup apitech Avaya DevConnect apitech ? ADMIN

PROPERTIES LICENSING ATTRIBUTES CERTIFICATES SPLUNK

Endpoint Attribute: model

Back

Attribute Information

Display Name
Model

User Data Type: CHOICE

Attribute Is Editable ☒ Yes

Attribute Is Hidden ☐ No

Attribute Is Required ☐ No

Have Default Value ☐ No

Choice List

- ☐ Name
- ☐ CM
- ☐ MM
- ☐ IP_Office
- ☐ Mitel
- ☐ Skype
- ☐ Red_Sky
- ☐ Nice
- ☐ Messaging
- ☐ System_Manager
- ☐ Session_Manager

6.4. Administer Access Control

Navigate to **Access Control**, which provides four default Access Control rules to allow Local Login, Endpoint Access, When to Record, and When to Require Connection Approvals as shown below. Each Access Control rule was configured as shown below. Note that local login and endpoint access was always allowed and recording connections and connection approvals were only required on weekends per the configuration below.

The screenshot displays the Avaya DevConnect web interface for Access Control. The left sidebar contains navigation links: Home, Dashboard, Access Control (highlighted), Sessions, Make Connections, Connections, My Connections, Community, System Setup, Application Logs, Networking, Users, Endpoints, Tunnel Profiles, Appliances, and Contracts. The main content area is titled 'Access Control' and features a 'RULES' tab and a 'CREATE' button. Below this, four default rules are listed, each with a 'DETAILS' button and a configuration summary:

- Endpoint Access by Local User**: DETAILS button. System Default: Allow all users access to All local endpoints at all times. Always.
- When to Record Connection**: DETAILS button. Recording. Weekends.
- When to Require Approval**: DETAILS button. System Default: Require Approval On Weekend Connections. Weekends.
- Local Login**: DETAILS button. System Default: Allow all users to login at all times. Always.

6.5. Administer Permissions

Navigate to **Permissions** to specify the permissions allowed per role. For example, an **Administrator** has access to everything whereas a Technician is only allowed to **Make Connections**.

Permissions		Avaya DevConnect					ADMIN	
Avaya DevConnect		Roles						
Rule Sets		Administrator	Auditor	Factory-Admin	NPG Admin	Technician	User Admin	
	Access Control Mgmt	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
	Appliance Mgmt	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	Attribute Mgmt	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
	Certificate Mgmt	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	Certificate View	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	Community Mgmt	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	Community View	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	Connection Mgmt	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	Connection View	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	Console	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	Contract Mgmt	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	Contract View	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	Endpoint Mgmt	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	Endpoint View	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	Log View	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	Make Connections	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	Network Mgmt	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	NOC Mgmt	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

6.6. Administer Users

Navigate to **Users** and select the **Create** tab to add a user. In the following example, a Technician user account is created. Configure the following fields in the **Account Settings** section:

- **User Name:** Specify a user name (e.g., *tech1*).
- **Email:** Specify the user email (e.g., *tech1@devcon.com*).
- **Is Account Enabled:** Enable the account.
- **Account Valid From Date:** Specify a valid date.
- **Account Valid Until Date:** Specify an expiration date for the account.
- **Password Expiration Date:** Specify an expiration date for the password.
- **Password:** Specify a valid password that adheres to the password creation rules.

The screenshot displays the Avaya DevConnect interface. On the left is a dark sidebar with navigation icons and labels: Home, Dashboard, Access Control, Sessions, Make Connections, Connections, My Connections, Community, System Setup, Application Logs, Networking, Users (highlighted), Endpoints, Tunnel Profiles, Appliances, Contracts, Permissions, Reporting, NOC Tools, and Notifications. The main header is blue with 'Users', 'apitech', 'Avaya DevConnect', and 'apitech' logos, along with a help icon, a bell, and 'ADMIN'. Below the header are 'LIST' and 'CREATE' tabs. The 'CREATE' tab is active, showing an 'Account Settings' form. The form contains the following fields and values:

Field	Value
User Name	tech1
Email	tech1@devcon.com
Ldap Cn	
Auth Type	disabled
User Tunnel Common Name	
Is Account Enabled	Yes
Account Valid From Date	08/30/2021
Account Valid Until Date	12/30/2021
Is Password Change Required	Yes
Does Password Expire	Yes
Password Expiration Date	12/31/2021
Num Sessions Remaining	-1
Token Key	
Mobile Phone	
Password

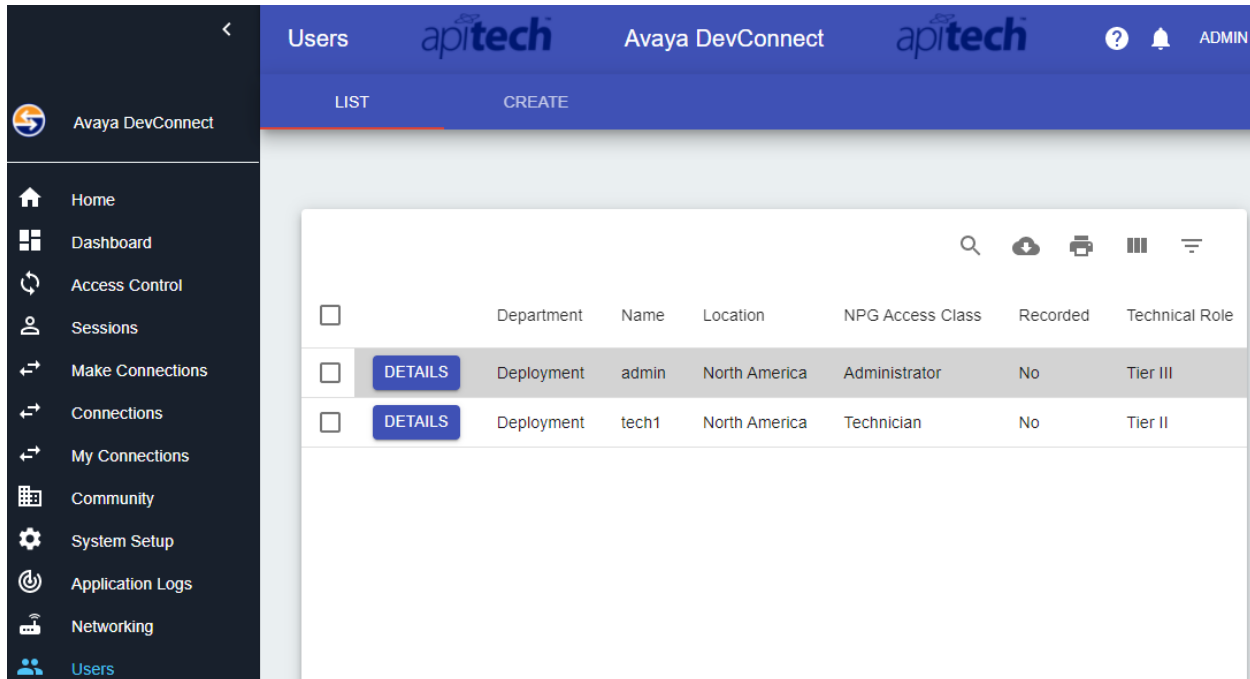
In the User Attributes section, configure the following fields:

- **Display Name:** Specify name displayed on the web interface for the user.
- **NPG Access Class:** Specify the role for the user described in **Section 6.5**.
- **Department:** Specify the user's department.
- **Location:** Specify the user's location.
- **Technical Role:** Specify the user's technical role.

User Attributes

Display Name	NPG Access Class
tech1	Technician
Department	Location
Deployment	North America
Technical Role	Recorded <input checked="" type="checkbox"/> No
Tier II	
Phone Number	

The **List** tab provides a list of configured users. In this example, an Administration and Technician account has been created.

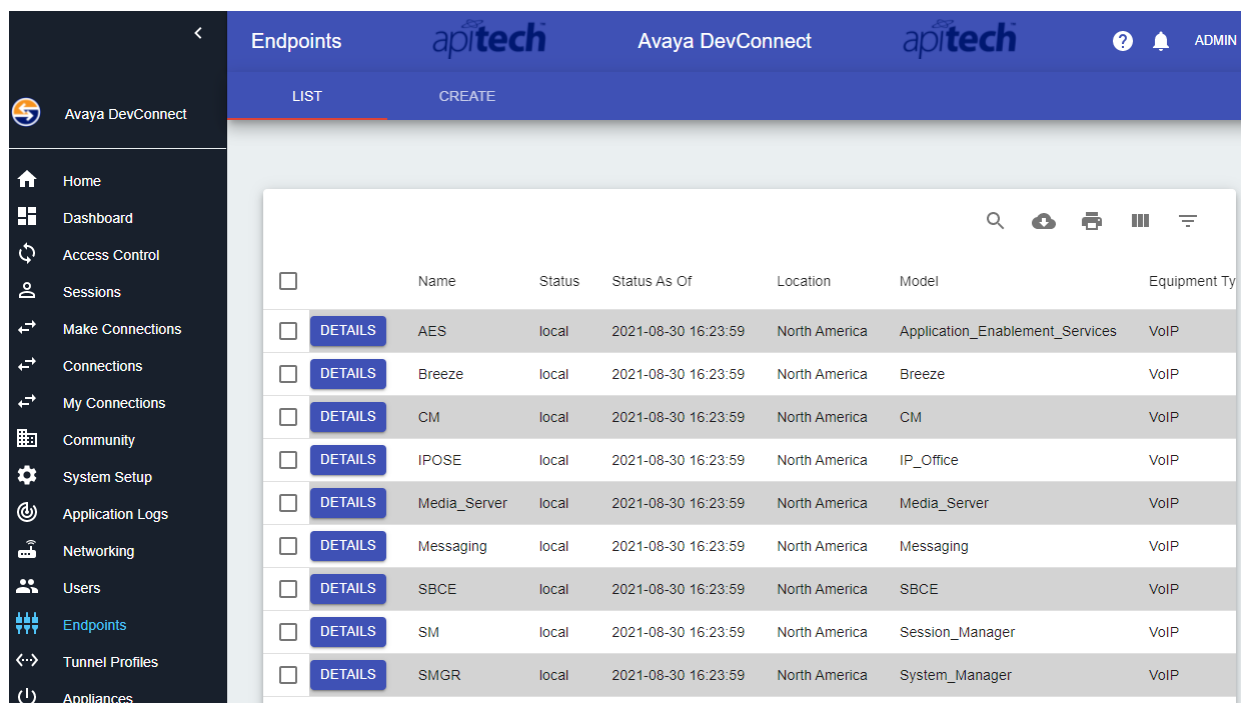


The screenshot displays the Avaya DevConnect web interface. On the left is a dark sidebar with navigation links: Home, Dashboard, Access Control, Sessions, Make Connections, Connections, My Connections, Community, System Setup, Application Logs, Networking, and Users (highlighted). The top header bar is blue and contains the 'Users' tab, 'apitech' logo, 'Avaya DevConnect' text, another 'apitech' logo, and user controls (help, notifications, ADMIN). Below the header, there are 'LIST' and 'CREATE' tabs. The main content area shows a table of users with columns: Department, Name, Location, NPG Access Class, Recorded, and Technical Role. Two users are listed: 'admin' (Administrator, Tier III) and 'tech1' (Technician, Tier II). Each row has a checkbox and a 'DETAILS' button.

	Department	Name	Location	NPG Access Class	Recorded	Technical Role
<input type="checkbox"/>	Deployment	admin	North America	Administrator	No	Tier III
<input type="checkbox"/>	Deployment	tech1	North America	Technician	No	Tier II

6.7. Administer Endpoints

Navigate to **Endpoints** to view the list of available Avaya endpoints to which a user may connect. For the compliance test, the following Avaya endpoints were added as shown below and listed in **Section 3**. The following sections will provide the endpoint configuration for each Avaya endpoints, including the protocol handler and port. As mentioned in the **Introduction** in **Section 1**, a specific protocol handler, such as SSH or HTTPS, will allow the appropriate application to open using the specified port when the endpoint name link is clicked. For example, for HTTPS, an Internet browser will be opened. Alternatively, the user may open the Internet browser manually, or any other application, and access the Avaya endpoint using the endpoint pool address provided. A “generic” protocol handler doesn’t provide an endpoint name link so the user would manually open the application to access the Avaya endpoint, such as IP Office Manager.



The screenshot displays the Avaya DevConnect web interface. The left sidebar contains navigation links: Home, Dashboard, Access Control, Sessions, Make Connections, Connections, My Connections, Community, System Setup, Application Logs, Networking, Users, Endpoints (highlighted), Tunnel Profiles, and Appliances. The main content area is titled 'Endpoints' and includes a 'LIST' tab and a 'CREATE' button. Below this is a table of endpoints with columns for Name, Status, Status As Of, Location, Model, and Equipment Ty. Each row has a 'DETAILS' button next to the Name column.

	Name	Status	Status As Of	Location	Model	Equipment Ty
<input type="checkbox"/>	DETAILS AES	local	2021-08-30 16:23:59	North America	Application_Enablement_Services	VoIP
<input type="checkbox"/>	DETAILS Breeze	local	2021-08-30 16:23:59	North America	Breeze	VoIP
<input type="checkbox"/>	DETAILS CM	local	2021-08-30 16:23:59	North America	CM	VoIP
<input type="checkbox"/>	DETAILS IPOSE	local	2021-08-30 16:23:59	North America	IP_Office	VoIP
<input type="checkbox"/>	DETAILS Media_Server	local	2021-08-30 16:23:59	North America	Media_Server	VoIP
<input type="checkbox"/>	DETAILS Messaging	local	2021-08-30 16:23:59	North America	Messaging	VoIP
<input type="checkbox"/>	DETAILS SBCE	local	2021-08-30 16:23:59	North America	SBCE	VoIP
<input type="checkbox"/>	DETAILS SM	local	2021-08-30 16:23:59	North America	Session_Manager	VoIP
<input type="checkbox"/>	DETAILS SMGR	local	2021-08-30 16:23:59	North America	System_Manager	VoIP

6.7.1. Avaya Aura® Communication Manager

Navigate to **Endpoints** and select the **Create** tab to add an Endpoint for Communication Manager. In the **Configuration** section, configure the following fields:

- **Real IP:** Specify the endpoint's IP address.
- **Use Real Addresses:** Disable this option.
- **Interface:** Specify the endpoint's network interface.

The screenshot displays the Avaya DevConnect web interface. On the left is a dark sidebar with navigation icons and labels: Home, Dashboard, Access Control, Sessions, Make Connections, Connections, My Connections, Community, System Setup, Application Logs, Networking, Users, and Endpoints (highlighted in blue). The main content area has a blue header with 'Endpoints', 'apitech', 'Avaya DevConnect', 'apitech', a help icon, a bell icon, and 'ADMIN'. Below the header are 'LIST' and 'CREATE' tabs. The 'CREATE' tab is active, showing a 'CM' configuration window. The window has a title bar with a blue save icon, a red delete icon, and a grey close icon. The configuration form is titled 'Configuration' and contains the following fields:

Real Ip	Virtual Ip: N/A
10.64.102.115	
Interface	Use Real Addresses <input type="checkbox"/> No
eth0	
Connect Via	Connect Via Openvpn Commonname
local	
Last Online Status: N/A	Is Online: No
Last Updated: 2021-08-06 15:26:50	

In the **Attributes** section, configure the following fields:

- **Name:** Specify the endpoint's name (e.g., *CM*).
- **Location:** Specify the endpoint's location.
- **Equipment Type:** Set to *VoIP*.
- **Manufacturer:** Set to *Avaya*.
- **Model:** Select the model name from **Section 6.3**.








Attributes

Name	Location
CM	North America
Equipment Type	Manufacturer
VoIP	Avaya
Model	Recorded <input type="checkbox"/> No
CM	

In the **Ports** section, specify *HTTPS* protocol handler and port *443* for the Communication Manager System Management Interface and *SSH* protocol handler and port *22* for SSH. The SSH port allows access to the System Access Terminal (SAT). Additional ports may be opened using the “generic” protocol handler. Refer to [1] for a list of ports used by Communication Manager.

Ports

New Port

		Name	Tcp Ports	Udp Ports	User Access Query	Protocol Handler
		CM_Web	443		()	https
		CM_SSH	22		()	ssh
		CM- Generic	21, 22, 23, 5022, 5023, 80, 443, 8443, 52233, 389, 636, 3389	162	()	generic

6.7.2. Avaya Aura® Media Server

Navigate to **Endpoints** and select the **Create** tab to add an Endpoint for Media Server. In the **Configuration** section, configure the following fields:

- **Real IP:** Specify the endpoint's IP address.
- **Use Real Addresses:** Disable this option.
- **Interface:** Specify the endpoint's network interface.

The screenshot displays the Avaya DevConnect web interface. On the left is a dark sidebar with navigation icons and labels: Home, Dashboard, Access Control, Sessions, Make Connections, Connections, My Connections, Community, System Setup, Application Logs, Networking, Users, and Endpoints (highlighted in blue). The main content area has a blue header with 'Endpoints', 'apitech', 'Avaya DevConnect', 'apitech', a help icon, a notification bell, and 'ADMIN'. Below the header are 'LIST' and 'CREATE' tabs. The 'CREATE' tab is active, showing a 'Media_Server' endpoint configuration form. The form includes a title bar with save, delete, and close icons. The configuration fields are as follows:

Configuration	
Real Ip 10.64.102.118	Virtual Ip: N/A
Interface eth0	Use Real Addresses <input type="checkbox"/> No
Connect Via local	Connect Via Openvpn Commonname
Last Online Status: N/A	Is Online: No
Last Updated: 2021-08-17 15:31:05	

In the **Attributes** section, configure the following fields:

- **Name:** Specify the endpoint's name (e.g., *Media_Server*).
- **Location:** Specify the endpoint's location.
- **Equipment Type:** Set to *VoIP*.
- **Manufacturer:** Set to *Avaya*.
- **Model:** Select the model name from **Section 6.3**.





Attributes

Name	Location
Media_Server	North America
Equipment Type	Manufacturer
VoIP	Avaya
Model	Recorded <input type="checkbox"/> No
Media_Server	

In the **Ports** section, specify *HTTPS* protocol handler and port *8443* for the EM Web-based Administration Tool and *SSH* protocol handler and port *22* for SSH.

Ports

New Port

	Name	Tcp Ports	Udp Ports	User Access Query	Protocol Hand
	 AMS_SSH	22		()	ssh
	 AMS_Web	8443		()	https

6.7.3. Avaya Aura® System Manager

Navigate to **Endpoints** and select the **Create** tab to add an Endpoint for System Manager. In the **Configuration** section, configure the following fields:

- **Real IP:** Specify the endpoint's IP address.
- **Use Real Addresses:** Disable this option.
- **Interface:** Specify the endpoint's network interface.

The screenshot shows the Avaya DevConnect System Manager (SMGR) interface. On the left is a dark sidebar with navigation icons and labels: Home, Dashboard, Access Control, Sessions, Make Connections, Connections, My Connections, Community, System Setup, Application Logs, Networking, Users, and Endpoints (highlighted in blue). The main content area has a blue header with 'Endpoints', 'apitech', 'Avaya DevConnect', 'apitech', a help icon, a bell icon, and 'ADMIN'. Below the header are 'LIST' and 'CREATE' tabs. The 'CREATE' tab is active, showing a 'Configuration' modal window. The modal has a title bar with a save icon (blue), a delete icon (red), and a close icon (grey). The configuration fields are as follows:

Configuration	
Real Ip	Virtual Ip: N/A
10.64.102.120	
Interface	Use Real Addresses <input type="checkbox"/> No
eth0	
Connect Via	Connect Via Openvpn Commonname
local	
Last Online Status: N/A	Is Online: No
Last Updated: 2021-08-17 14:30:03	

In the **Attributes** section, configure the following fields:

- **Name:** Specify the endpoint's name (e.g., *SMGR*).
- **Location:** Specify the endpoint's location.
- **Equipment Type:** Set to *VoIP*.
- **Manufacturer:** Set to *Avaya*.
- **Model:** Select the model name from **Section 6.3**.







Attributes

Name	Location
SMGR	North America
Equipment Type	Manufacturer
VoIP	Avaya
Model	Recorded <input type="checkbox"/> No
System_Manager	

In the **Ports** section, specify *HTTPS* protocol handler and port *443* for the System Manager Web Interface, *SSH* protocol handler and port *22* for SSH, and *HTTPS* protocol handler and port *52233* for WebLM License Server.

Ports

New Port

	Name	Tcp Ports	Udp Ports	User Access Query	Protocol
 	SMGR_SSH	22		()	ssh
 	SMGR_Web	443		()	https
 	SMGR_WebLM	52233		()	https

6.7.4. Avaya Aura® Session Manager

Navigate to **Endpoints** and select the **Create** tab to add an Endpoint for Session Manager. In the **Configuration** section, configure the following fields:

- **Real IP:** Specify the Session Manager management IP address.
- **Use Real Addresses:** Disable this option.
- **Interface:** Specify the endpoint's network interface.

The screenshot displays the Avaya DevConnect web interface. On the left is a dark sidebar with navigation links: Home, Dashboard, Access Control, Sessions, Make Connections, Connections, My Connections, Community, System Setup, Application Logs, Networking, Users, and Endpoints (highlighted). The main content area has a blue header with 'Endpoints', 'apitech', 'Avaya DevConnect', and 'apitech' logos, along with a help icon, a bell, and an 'ADMIN' link. Below the header are 'LIST' and 'CREATE' tabs. The 'CREATE' tab is active, showing a configuration form for a Session Manager (SM) endpoint. The form includes fields for 'Real Ip' (10.64.102.116), 'Interface' (eth0), 'Connect Via' (local), 'Virtual Ip' (N/A), 'Use Real Addresses' (disabled), 'Connect Via Openvpn Commonname', 'Last Online Status' (N/A), 'Is Online' (No), and 'Last Updated' (2021-08-17 16:26:37). There are also icons for save, delete, and close at the top right of the form.

Configuration	
Real Ip	Virtual Ip: N/A
10.64.102.116	
Interface	Use Real Addresses <input type="checkbox"/> No
eth0	
Connect Via	Connect Via Openvpn Commonname
local	
Last Online Status: N/A	Is Online: No
Last Updated: 2021-08-17 16:26:37	

In the **Attributes** section, configure the following fields:

- **Name:** Specify the endpoint's name (e.g., *SM*).
- **Location:** Specify the endpoint's location.
- **Equipment Type:** Set to *VoIP*.
- **Manufacturer:** Set to *Avaya*.
- **Model:** Select the model name from **Section 6.3**.

Attributes

Name	Location
SM	North America
Equipment Type	Manufacturer
VoIP	Avaya
Model	Recorded
Session_Manager	<input type="checkbox"/> No

In the **Ports** section, specify *SSH* protocol handler and port 22 for SSH and *Generic* protocol handler and port 22 for SFTP. The SSH session may be used to access the *traceSM* utility tool.

Ports New Port

	Name	Tcp Ports	Udp Ports	User Access Query	Protocol Handler
	SM_Generic	22		()	generic
	SM_SSH	22		()	ssh

6.7.5. Avaya Aura® Application Enablement Services

Navigate to **Endpoints** and select the **Create** tab to add an Endpoint for Application Enablement Services. In the **Configuration** section, configure the following fields:

- **Real IP:** Specify the endpoint's IP address.
- **Use Real Addresses:** Disable this option.
- **Interface:** Specify the endpoint's network interface.

The screenshot displays the Avaya DevConnect web interface. On the left is a dark sidebar with navigation icons and labels: Home, Dashboard, Access Control, Sessions, Make Connections, Connections, My Connections, Community, System Setup, Application Logs, Networking, Users, and Endpoints (highlighted in blue). The main content area has a blue header with 'Endpoints', 'apitech' logo, 'Avaya DevConnect', another 'apitech' logo, and icons for help, notifications, and 'ADMIN'. Below the header are 'LIST' and 'CREATE' tabs. The 'CREATE' tab is active, showing a configuration form for an endpoint named 'AES'. The form includes a title bar with save, delete, and close icons. The configuration fields are as follows:

Configuration	
Real Ip	Virtual Ip: N/A
10.64.102.119	
Interface	Use Real Addresses <input type="checkbox"/> No
eth0	
Connect Via	Connect Via Openvpn Commonname
local	
Last Online Status: N/A	Is Online: No
Last Updated: 2021-08-17 17:01:25	

In the **Attributes** section, configure the following fields:

- **Name:** Specify the endpoint's name (e.g., *AES*).
- **Location:** Specify the endpoint's location.
- **Equipment Type:** Set to *VoIP*.
- **Manufacturer:** Set to *Avaya*.
- **Model:** Select the model name from **Section 6.3**.





Attributes

Name	Location
AES	North America
Equipment Type	Manufacturer
VoIP	Avaya
Model	Recorded <input type="checkbox"/> No
Application_Enablement_Services	

In the **Ports** section, specify *HTTPS* protocol handler and port *443* for the AES Management Console and *SSH* protocol handler and port *22* for SSH.

Ports

New Port

	Name	Tcp Ports	Udp Ports	User Access Query	Protocol Handler
 	AES_Web	443		()	https
 	AES_SSH	22		()	ssh

6.7.6. Avaya Session Border Controller for Enterprise

Navigate to **Endpoints** and select the **Create** tab to add an Endpoint for Session Border Controller for Enterprise (SBCE). For the compliance test, the EMS and SBCE were deployed on the same server. In the **Configuration** section, configure the following fields:

- **Real IP:** Specify the endpoint's IP address.
- **Use Real Addresses:** Disable this option.
- **Interface:** Specify the endpoint's network interface.

The screenshot displays the Avaya DevConnect web interface. On the left is a dark sidebar with navigation links: Home, Dashboard, Access Control, Sessions, Make Connections, Connections, My Connections, Community, System Setup, Application Logs, Networking, Users, and Endpoints (highlighted in blue). The main content area has a blue header with 'Endpoints', 'apitech', 'Avaya DevConnect', and 'apitech' logos, along with a help icon, a bell icon, and an 'ADMIN' link. Below the header are 'LIST' and 'CREATE' tabs. The 'CREATE' tab is active, showing a form for a new SBCE endpoint. The form is titled 'SBCE' and includes a 'Configuration' section with the following fields: 'Real Ip' (10.64.102.105), 'Virtual Ip' (N/A), 'Interface' (eth0), 'Use Real Addresses' (disabled toggle), 'Connect Via' (local), 'Connect Via Openvpn Commonname' (empty), 'Last Online Status' (N/A), 'Is Online' (No), and 'Last Updated' (2021-08-17 18:19:09). There are also icons for saving, deleting, and closing the form.

Configuration	
Real Ip	Virtual Ip: N/A
10.64.102.105	
Interface	Use Real Addresses <input type="checkbox"/> No
eth0	
Connect Via	Connect Via Openvpn Commonname
local	
Last Online Status: N/A	Is Online: No
Last Updated: 2021-08-17 18:19:09	

In the **Attributes** section, configure the following fields:

- **Name:** Specify the endpoint's name (e.g., *SBCE*).
- **Location:** Specify the endpoint's location.
- **Equipment Type:** Set to *VoIP*.
- **Manufacturer:** Set to *Avaya*.
- **Model:** Select the model name from **Section 6.3**.

Attributes

Name	Location
SBCE	North America
Equipment Type	Manufacturer
VoIP	Avaya
Model	Recorded <input type="checkbox"/> No
SBCE	

In the **Ports** section, specify *HTTPS* protocol handler and port *443* for the EMS Web Interface, *SSH* protocol handler and port *22* for SSH, and *Generic* protocol handler and port *22* for SFTP. The SSH session may be used to access the *tracesbc* utility tool.

Ports

New Port

	Name	Tcp Ports	Udp Ports	User Access Query	Protocol H
	SBCE_SSH	22		()	ssh
	SBCE_Web	443		()	https
	SBCE_Generic	22		()	generic

6.7.7. Avaya Messaging

Navigate to **Endpoints** and select the **Create** tab to add an Endpoint for Messaging. In the **Configuration** section, configure the following fields:

- **Real IP:** Specify the endpoint's IP address.
- **Use Real Addresses:** Disable this option.
- **Interface:** Specify the endpoint's network interface.

The screenshot shows the Avaya DevConnect web interface. The left sidebar contains navigation links: Home, Dashboard, Access Control, Sessions, Make Connections, Connections, My Connections, Community, System Setup, Application Logs, Networking, Users, and Endpoints. The main content area is titled 'Endpoints' and has a 'CREATE' button. Below this, the 'Messaging' configuration form is shown. The form includes the following fields:

Configuration	
Real Ip	Virtual Ip: N/A
10.64.102.107	
Interface	Use Real Addresses <input type="checkbox"/> No
eth0	
Connect Via	Connect Via Openvpn Commonname
local	
Last Online Status: N/A	Is Online: No
Last Updated: 2021-08-12 18:20:57	

In the **Attributes** section, configure the following fields:

- **Name:** Specify the endpoint's name (e.g., *Messaging*).
- **Location:** Specify the endpoint's location.
- **Equipment Type:** Set to *VoIP*.
- **Manufacturer:** Set to *Avaya*.
- **Model:** Select the model name from **Section 6.3**.

The screenshot shows the 'Attributes' configuration page. It contains several input fields and a toggle switch. The 'Name' field is set to 'Messaging'. The 'Location' dropdown is set to 'North America'. The 'Equipment Type' dropdown is set to 'VoIP'. The 'Manufacturer' dropdown is set to 'Avaya'. The 'Model' dropdown is set to 'Messaging'. There is a 'Recorded' toggle switch which is currently turned off, with the text 'No' next to it.





Name	Location
Messaging	North America

Equipment Type	Manufacturer
VoIP	Avaya

Model	Recorded
Messaging	<input type="checkbox"/> No

In the **Ports** section, specify *HTTPS* protocol handler and port *443* for Messaging Web Access and *Generic* protocol handler and port *3389* for Remote Desktop (RDP). The RDP session may be used to access the *Messaging Admin* and *SIP Configurator* applications.

The screenshot shows the 'Ports' configuration page. It has a 'New Port' button in the top right corner. Below it is a table with columns: Name, Tcp Ports, Udp Ports, User Access Query, and Protocol. There are two rows of data. The first row is for 'Messaging_Generic' with Tcp Ports '3389', Udp Ports '()', User Access Query '()', and Protocol 'gene'. The second row is for 'Messaging_Web' with Tcp Ports '443', Udp Ports '()', User Access Query '()', and Protocol 'https'. Each row has a trash icon and a pencil icon to its left.

	Name	Tcp Ports	Udp Ports	User Access Query	Protocol
 	Messaging_Generic	3389	()	()	gene
 	Messaging_Web	443	()	()	https

6.7.8. Avaya Breeze

Navigate to **Endpoints** and select the **Create** tab to add an Endpoint for Breeze. In the **Configuration** section, configure the following fields:

- **Real IP:** Specify the endpoint's IP address.
- **Use Real Addresses:** Disable this option.
- **Interface:** Specify the endpoint's network interface.

The screenshot displays the Avaya DevConnect web interface. On the left is a dark sidebar with navigation links: Home, Dashboard, Access Control, Sessions, Make Connections, Connections, My Connections, Community, System Setup, Application Logs, Networking, Users, and Endpoints (highlighted). The main content area has a blue header with 'Endpoints', 'apitech', 'Avaya DevConnect', and 'apitech' logos, along with a help icon, a bell icon, and an 'ADMIN' link. Below the header are 'LIST' and 'CREATE' tabs. The 'CREATE' tab is active, showing a configuration form for an endpoint named 'Breeze'. The form includes fields for 'Real Ip' (10.64.110.218), 'Interface' (eth0), 'Connect Via' (local), 'Virtual Ip' (N/A), 'Use Real Addresses' (toggle set to No), 'Connect Via Openvpn Commonname', 'Last Online Status' (N/A), and 'Is Online' (No). The 'Last Updated' timestamp is 2021-08-17 18:31:34. Action buttons (save, delete, close) are visible at the top right of the configuration panel.

Configuration	
Real Ip	Virtual Ip: N/A
10.64.110.218	
Interface	Use Real Addresses <input type="checkbox"/> No
eth0	
Connect Via	Connect Via Openvpn Commonname
local	
Last Online Status: N/A	Is Online: No
Last Updated: 2021-08-17 18:31:34	

In the **Attributes** section, configure the following fields:



- **Name:** Specify the endpoint's name (e.g., *Breeze*).
- **Location:** Specify the endpoint's location.
- **Equipment Type:** Set to *VoIP*.
- **Manufacturer:** Set to *Avaya*.
- **Model:** Select the model name from **Section 6.3**.

The screenshot shows the 'Attributes' configuration page. It contains several input fields and a toggle switch. The 'Name' field is set to 'Breeze'. The 'Location' dropdown is set to 'North America'. The 'Equipment Type' dropdown is set to 'VoIP'. The 'Manufacturer' dropdown is set to 'Avaya'. The 'Model' dropdown is set to 'Breeze'. There is a 'Recorded' toggle switch set to 'No'.

Field	Value
Name	Breeze
Location	North America
Equipment Type	VoIP
Manufacturer	Avaya
Model	Breeze
Recorded	No

In the **Ports** section, specify *SSH* protocol handler and port 22 for SSH. Note that Breeze is configured through System Manager, which is an endpoint configured in **Section 6.7.3**.

The screenshot shows the 'Ports' configuration page. It features a 'New Port' button and a table with columns: Name, Tcp Ports, Udp Ports, User Access Query, and Protocol Handler. The table contains one entry: 'Breeze_SSH' with '22' in the 'Tcp Ports' column and 'ssh' in the 'Protocol Handler' column. There are also icons for deleting and editing the entry.

	Name	Tcp Ports	Udp Ports	User Access Query	Protocol Handler
 	Breeze_SSH	22		()	ssh

6.7.9. Avaya IP Office Server Edition

Navigate to **Endpoints** and select the **Create** tab to add an Endpoint for IP Office Server Edition. In the **Configuration** section, configure the following fields:

- **Real IP:** Specify the endpoint's IP address.
- **Use Real Addresses:** Disable this option.
- **Interface:** Specify the endpoint's network interface.

The screenshot displays the Avaya DevConnect web interface. On the left is a dark sidebar with navigation icons and labels: Home, Dashboard, Access Control, Sessions, Make Connections, Connections, My Connections, Community, System Setup, Application Logs, Networking, Users, and Endpoints (highlighted). The main content area has a blue header with 'Endpoints', 'apitech', 'Avaya DevConnect', and 'apitech' logos, along with a help icon, a bell icon, and an 'ADMIN' link. Below the header are 'LIST' and 'CREATE' tabs. The 'CREATE' tab is active, showing a configuration form for an endpoint named 'IPOSE'. The form has a title 'Configuration' and includes the following fields: 'Real Ip' (10.64.102.90), 'Interface' (eth0), 'Connect Via' (local), 'Virtual Ip: N/A', 'Use Real Addresses' (toggle set to 'No'), 'Connect Via Openvpn Commonname', 'Last Online Status: N/A', and 'Is Online: No'. At the bottom, it shows 'Last Updated: 2021-08-06 15:25:16'. There are also icons for saving, deleting, and closing the form.

Configuration	
Real Ip	Virtual Ip: N/A
10.64.102.90	
Interface	Use Real Addresses <input type="checkbox"/> No
eth0	
Connect Via	Connect Via Openvpn Commonname
local	
Last Online Status: N/A	Is Online: No
Last Updated: 2021-08-06 15:25:16	

In the **Attributes** section, configure the following fields:

- **Name:** Specify the endpoint's name (e.g., *IPOSE*).
- **Location:** Specify the endpoint's location.
- **Equipment Type:** Set to *VoIP*.
- **Manufacturer:** Set to *Avaya*.
- **Model:** Select the model name from **Section 6.3**.

Attributes

Name
IPOSE

Location
North America

Equipment Type
VoIP

Manufacturer
Avaya







Model
IP_Office

Recorded ☐ No

In the **Ports** section, specify *HTTPS* protocol handler and port *7071* or *7070* for the IP Office Web Manager, *SSH* protocol handler and port *22* for SSH, and *Generic* protocol handler and the ports shown below for access to IP Office Manager, Monitor, and System Status applications. Refer to [7] for the ports that should be opened for the IP Office applications.

Ports

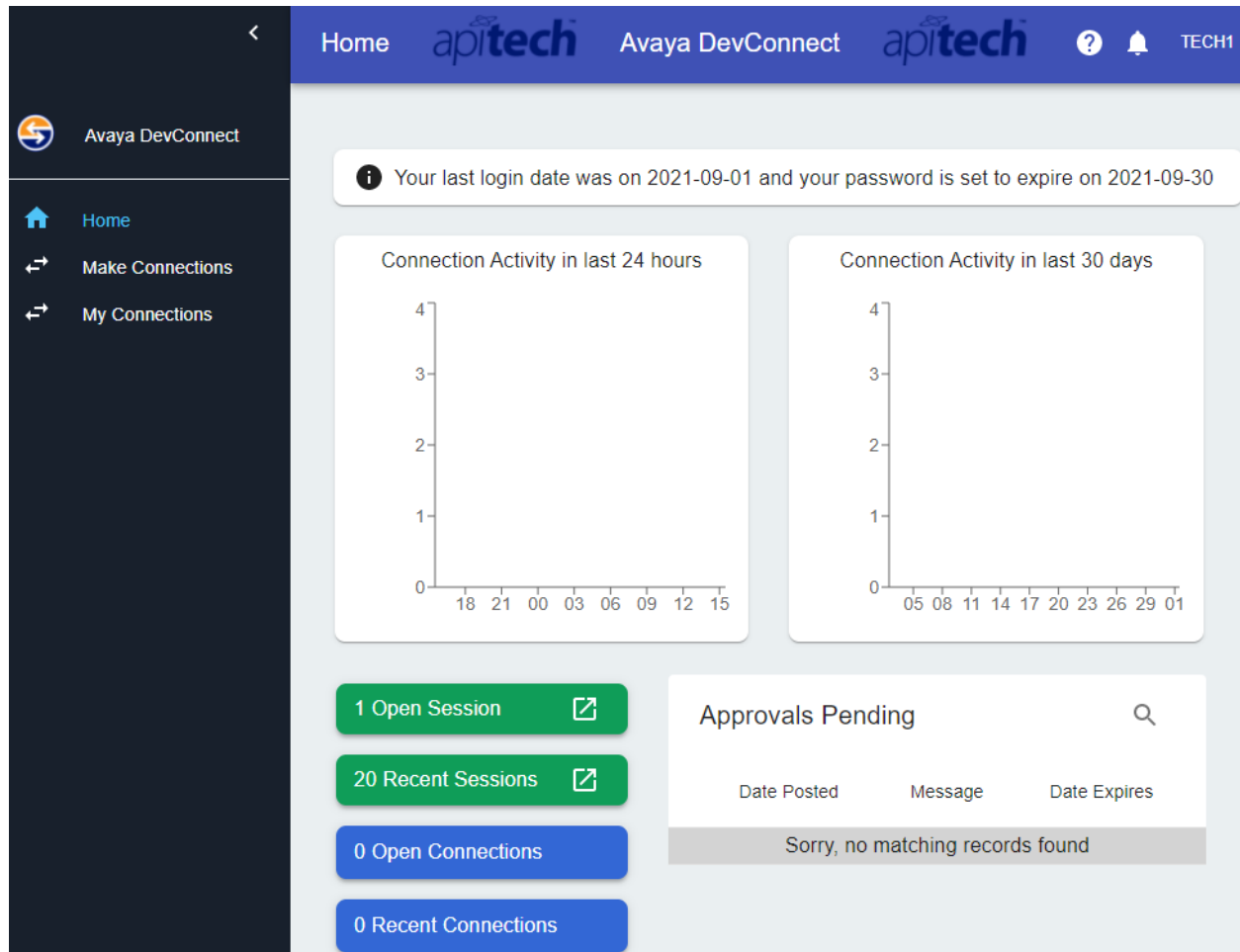
New Port

	Name	Tcp Ports	Udp Ports	User Access Query	Protocol Handler
 	IPO_Web	7071		()	https
 	IPO- Generic	50813, 50812, 50809, 50808, 50805, 50804, 50802, 50794, 69, 50814, 50791, 53248, 53251, 48620, 48621, 48622, 48623, 5032, 5033, 5034, 5035, 53252, 53253, 53254, 53255, 48624, 48625, 48626, 48627, 5036, 5037, 5038, 5039, 3389, 80, 443, 8080, 8443, 7070, 7071, 22, 8444, 9443	162, 50794	()	generic
 	IPO_SSH	22		()	ssh

7. Verification Steps

This section provides the tests that can be performed to verify proper configuration of ION Networks Netgard Privileged Gateway with a few Avaya endpoints using SSH, Web/HTTPS, RDP, and IPO Manager.

1. Log into the NPG Web Interface using a “technician” account. Verify the following screen is displayed with the **Make Connections** option in the left pane.



- Click on the **Make Connections** option to display a list of endpoints available to the technician. Click on **CONNECT** associated with an SSH connection (e.g., *CM_SSH*).

	Name	Port Name	Status	Status As Of	
<input type="checkbox"/>	CONNECT	AES	AES_SSH	local	2021-09-01 15:10:43
<input type="checkbox"/>	CONNECT	AES	AES_Web	local	2021-09-01 15:10:43
<input type="checkbox"/>	CONNECT	Breeze	Breeze_SSH	local	2021-09-01 15:10:43
<input type="checkbox"/>	CONNECT	CM	CM-Generic	local	2021-09-01 15:10:43
<input type="checkbox"/>	CONNECT	CM	CM_SSH	local	2021-09-01 15:10:43
<input type="checkbox"/>	CONNECT	CM	CM_Web	local	2021-09-01 15:10:43

- Verify the connection is established successfully as shown below. Click on the **Endpoint Port Name** (e.g., *CM_SSH*) to open the default SSH application and log into Communication Manager with the appropriate credentials. When done, click on **Close Connection** to terminate the connection.

Connection Successful

[Close Dialog](#) ✕

Endpoint Name	CM
Endpoint Pool Address	10.64.102.171
Endpoint Port Name	CM_SSH
TCP Ports	22
UDP Ports	
Protocol Handler	ssh
Result	

[Close Connection](#) 🗑

- Click on the **Make Connections** option to display a list of endpoints available to the technician. Click on **CONNECT** associated with an Web/HTTPS connection (e.g., *AES_Web*).

Avaya DevConnect

Home

Make Connections

My Connections

Make Connections

apitech


Avaya DevConnect

apitech


TECH1

		Name	Port Name	Status	Status As Of
<input type="checkbox"/>	CONNECT	AES	AES_SSH	local	2021-09-01 15:10:43
<input type="checkbox"/>	CONNECT	AES	AES_Web	local	2021-09-01 15:10:43
<input type="checkbox"/>	CONNECT	Breeze	Breeze_SSH	local	2021-09-01 15:10:43
<input type="checkbox"/>	CONNECT	CM	CM-Generic	local	2021-09-01 15:10:43

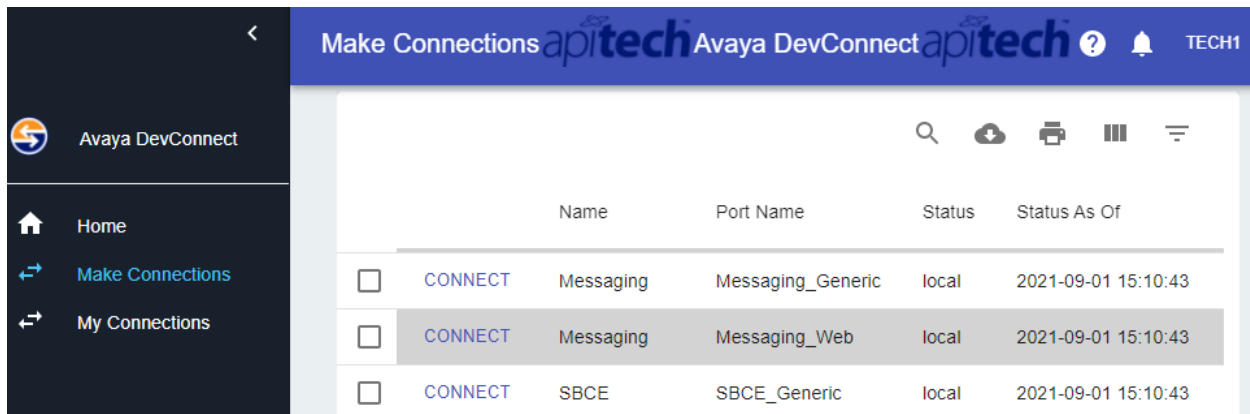
- Verify the connection is established successfully as shown below. Click on the **Endpoint Port Name** (e.g., *AES_Web*) to open an Internet browser and log into AES with the appropriate credentials. When done, click on **Close Connection** to terminate the connection.

Connection Successful [Close Dialog](#) 

Endpoint Name	AES
Endpoint Pool Address	10.64.102.171
Endpoint Port Name	AES_Web
TCP Ports	443
UDP Ports	

[Close Connection](#) 

6. Click on the **Make Connections** option to display a list of endpoints available to the technician. Click on **CONNECT** associated with a Generic connection using port 3389 for Remote Desktop (e.g., *Messaging_Generic*).



	Name	Port Name	Status	Status As Of	
<input type="checkbox"/>	CONNECT	Messaging	Messaging_Generic	local	2021-09-01 15:10:43
<input type="checkbox"/>	CONNECT	Messaging	Messaging_Web	local	2021-09-01 15:10:43
<input type="checkbox"/>	CONNECT	SBCE	SBCE_Generic	local	2021-09-01 15:10:43

7. Verify the connection is established successfully as shown below. Note that when the “generic” protocol handler is used, no **Endpoint Port Name** is provided. The technician should use the **Endpoint Pool Address** (e.g., *10.64.102.171*) to enter in Remote Desktop. Log in with the appropriate credentials. When done, click on **Close Connection** to terminate the connection.

Connection Successful

[Close Dialog](#) 

Endpoint Name	Messaging
Endpoint Pool Address	10.64.102.171
Endpoint Port Name	Messaging_Generic
TCP Ports	3389
UDP Ports	

[Close Connection](#) 

8. Click on the **Make Connections** option to display a list of endpoints available to the technician. Click on **CONNECT** associated with a Generic connection using IP Office Server Edition ports for IP Office Manager (e.g., *IPO_Generic*).

Avaya DevConnect

Home

Make Connections

My Connections

Make Connections

apitech

Avaya DevConnect

apitech

TECH1

<input type="checkbox"/>	CONNECT	IPOSE	IPO-Generic	local	2021-09-01 15:10:43
<input type="checkbox"/>	CONNECT	IPOSE	IPO_SSH	local	2021-09-01 15:10:43
<input type="checkbox"/>	CONNECT	IPOSE	IPO_Web	local	2021-09-01 15:10:43
<input type="checkbox"/>	CONNECT	Media_Server	AMS_SSH	local	2021-09-01 15:10:43
<input type="checkbox"/>	CONNECT	Media_Server	AMS_Web	local	2021-09-01 15:10:43

9. Verify the connection is established successfully as shown below. Note that when the “generic” protocol handler is used, no **Endpoint Port Name** is provided. The technician should use the **Endpoint Pool Name** (e.g., *10.64.102.171*) to open IP Office Manager, Monitor, or System Status. Log in with the appropriate credentials. When done, click on **Close Connection** to terminate the connection.

Connection Successful

Close Dialog X

Endpoint Name	IPOSE
Endpoint Pool Address	10.64.102.171
Endpoint Port Name	IPO-Generic
TCP Ports	50813,50812,50809,50808,50805,50804,50802,50794,69,50814,50791
UDP Ports	162,50794
Protocol Handler	generic

Close Connection

8. Conclusion

These Application Notes describe the configuration steps required to enable ION Networks Netgard Privileged Gateway to provide secure access to Avaya Aura® Suite, Avaya Session Border Controller for Enterprise, Avaya Messaging, Avaya Breeze, and Avaya IP Office. System access to the Avaya endpoints successfully used SSH, SFTP, HTTPS, RDP, and thick clients. All test cases passed with observations noted in **Section 2.2**.

9. References

This section references the Avaya documentation relevant to these Application Notes available at <http://support.avaya.com>.

- [1] *Avaya Port Matrix: Avaya Aura® Communication Manager 8.1.3*, Issue 1.1, March 10, 2021.
- [2] *Avaya Port Matrix: Avaya Aura® System Manager 8.1*, Issue 4.0, March 16, 2021.
- [3] *Avaya Port Matrix: Avaya Aura® Session Manager 8.1.12*, Issue 1.0, June 12, 2021, DocID 193457.
- [4] *Avaya Port Matrix: Avaya Aura® Application Enablement Services 8.1.11*, Issue 1.0, March 2021.
- [5] *Avaya Port Matrix: Avaya Aura® Presence Services 8.1.4*, Issue 1.0, April 5, 2021.
- [6] *Avaya Port Matrix: Avaya Session Border Controller for Enterprise (SBCE)*, Release 8.x, Issue 1, December 2020.
- [7] *Avaya Port Matrix: Avaya IP Office 11.1.1.0*, Issue 12.4, January 28, 2021.

©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 DevConnect Program at devconnect@avaya.com.