



Avaya Aura® Application Notes: Enabling Zoom Workplace clients with Avaya Aura®

Issue 1.2

Date 27th January 2025

Abstract

This document provides details and information for Avaya Aura® customers with regards to configuration tasks that may be required to register and use Zoom Workplace clients with Avaya Aura®.

CHANGE CONTROL RECORD		
Date (mm/dd/yy)	Issue/Version #	Summary of Changes
01/27/25	1.2	Added Section 8 Device Adaptation
01/15/25	1.1	Updated Zoom provider address Updated instructions for certificate installation Formatting and syntax changes
11/05/24	1.0	Initial revision

Table of Contents

1	Overview	3
2	Prerequisites	3
2.1	Avaya	3
2.2	Zoom	3
2.3	Integrating Avaya Aura® Contacts with Zoom Contacts.....	4
3	Licensing.....	4
4	Avaya Aura® Device Services (AADS) Configuration.....	5
4.1	AADS URL in Zoom Workplace clients.....	5
4.2	OpenID Connect (OIDC) Discovery URL in AADS and Firewall Update	5
4.3	Zoom Configuration	7
5	Session Border Controller (SBC) configuration.....	8
5.1.1	Add SBC User Agent.....	8
5.1.2	Add SBC Endpoint Flow.....	8
5.1.3	SBC Signaling Manipulation script (specific customers only)	9
6	Certificates.....	10
7	Push Notification.....	10
8	Device Adaptation	12
8.1	Regular Expression Adapter configuration	12
8.2	Regular Expression Adapter configuration	14
9	User Provisioning	14
9.1	System Manager (SMGR) configuration	14
9.1.1	User Management – Session Manager Profile screen	14
9.1.2	Session Manager – Communication Profile Editor screen	15
9.1.3	Session Manager – User Registrations screen.....	15
9.2	Zoom User Provisioning.....	16
9.2.1	Add users.....	16
9.2.2	Import users	17
9.2.3	Export users to a CSV file.....	17
9.2.4	Status of the Phone System Integration (PSI) user.....	18

1 Overview

The Zoom-Avaya Aura integration enables users to leverage the benefits of Zoom Workplace while connecting from the Zoom Phone tab to an Avaya Aura system for telephony features.

This integration allows the Zoom Phone tab to become a SIP Softphone that registers to Avaya, using the Avaya Session Manager (SM) and Avaya SBC (ASBCE), if accessed over the Internet. It will also leverage the Avaya Aura Device Services (AADS) for a simplified login from Zoom to the Avaya Aura system. Users will be required to have all of these Avaya components in their environment to support this integration.

2 Prerequisites

Avaya Aura® X for Zoom Workplace license is required for enabling Zoom Workplace.

The customer account must be enabled for the Zoom-Avaya Aura integration during the customer account setup.

2.1 Avaya

Avaya Aura® X for Zoom Workplace is compatible with the following Avaya Aura® Releases:

- 10.1.3.4 Service Pack
(<https://support.avaya.com/css/en/public/documents/101079285>)
- 10.2.0.1 Hot Patch
(<https://support.avaya.com/css/secure/documents/101091757>)
- 10.2.1 or later

2.2 Zoom

- Business Plus, Enterprise, Enterprise Plus, or Enterprise Premium licenses
- Account owner or admin [role](#) for managing users, Phone System integrations, and Zoom Phone
- Zoom Workplace app version 6.2.0 or higher.

2.3 Integrating Avaya Aura® Contacts with Zoom Contacts

Zoom documentation is available at:

https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0077144

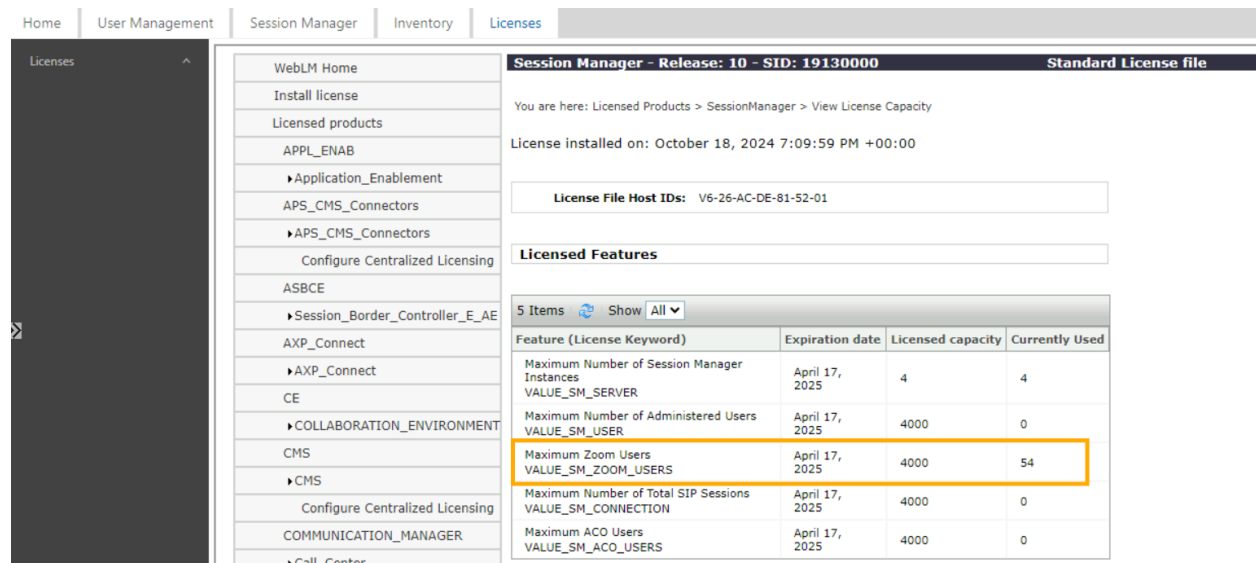
The above Zoom document includes information about how to integrate Avaya Aura® contacts with Zoom contacts - see the “How to manage external contacts” section. External Contacts can be added manually or via CSV and are searchable/callable contacts across the organization.

3 Licensing

Avaya Aura® X for Zoom Workplace license is required for each user which needs to be enabled with Zoom integration. The Session Manager Element Manager enforces that number by means of a **Third-Party Clients** option on the Session Manager Profile. The customer cannot enable Zoom for more users than that licensed maximum.

When a user logs in a Zoom Workplace client, the REGISTER contains a SIP User-Agent header that identifies Zoom, and Session Manager checks to be sure that user is configured to allow Zoom. If not, the registration is rejected.

The following screenshot of the SMGR Licensing page shows 4000 Zoom users licensed, with 54 user having Zoom enabled as a Third-Party Client.



The screenshot displays the Session Manager Licensing page. The left sidebar contains a navigation menu with options like 'WebLM Home', 'Install license', 'Licensed products', and 'APPL_ENAB'. The main content area shows the 'Session Manager - Release: 10 - SID: 19130000' page. It includes a 'License File Host IDs' field with the value 'V6-26-AC-DE-81-52-01'. Below this is a 'Licensed Features' table with 5 items. The table has columns for 'Feature (License Keyword)', 'Expiration date', 'Licensed capacity', and 'Currently Used'. The 'Maximum Zoom Users' row is highlighted with an orange box, showing a capacity of 4000 and 54 currently used.

Feature (License Keyword)	Expiration date	Licensed capacity	Currently Used
Maximum Number of Session Manager Instances VALUE_SM_SERVER	April 17, 2025	4	4
Maximum Number of Administered Users VALUE_SM_USER	April 17, 2025	4000	0
Maximum Zoom Users VALUE_SM_ZOOM_USERS	April 17, 2025	4000	54
Maximum Number of Total SIP Sessions VALUE_SM_CONNECTION	April 17, 2025	4000	0
Maximum ACO Users VALUE_SM_ACO_USERS	April 17, 2025	4000	0

Follow the standard procedure to install the Avaya Aura® X for Zoom Workplace license in Session Manager.

4 Avaya Aura® Device Services (AADS) Configuration

4.1 AADS URL in Zoom Workplace clients

The Avaya Workplace client determines the appropriate AADS URL through a multi-step exchange with the DNS server. In contrast, the Zoom Workplace client does not utilize this mechanism. Instead, the correct **AADS URL** and **Client ID** must be **manually configured** in the Zoom account settings.

4.2 OpenID Connect (OIDC) Discovery URL in AADS and Firewall Update

The correct Zoom OIDC URL must be assigned in AADS, on the screen *Security Settings > Client ID Mapping*. The AADS screenshot below shows the screen on which this is configured.

OIDC Discovery URL needs to be obtained from Zoom account: login to your Zoom web as Admin and navigate to *Account Management > Phone System Integration*. Go to *Settings* and copy Zoom discovery URL:

zoom.us/account/sipphone/sipaccount?amp_device_id=98f04d39-c6a2-4330-ba04-a392fc3ef190#/setting

Avaya Managed Favorites

Search Support 1.888.799.0125 Contact Sales Request

zoom Products Solutions Resources Plans & Pricing Schedule Join Host Web App

Device Management

- Node Management
- Room Management
- Workspaces Management
- Phone System Management
- Account Management**
 - Account Profile
 - Account Settings
 - Alerts & Notifications
 - Location Management
 - Whiteboard Management
 - Notes Management
 - Docs Management **NEW**
 - Recording and Transcript Management
 - Clip Management
 - Summary Management
 - Survey Management
 - Workflow Management **BETA**
- Phone System Integration**
- Reports

Integrated users **Settings**

Zoom discovery URL https://zoom.us/.well-known/avaya/oidc/configuration

Avaya Aura Device Service domains	Client name	AADS domain
aads	aads	aads.engageavaya.ec.avayacloud.com
aaaads09	aaaads09	aads-09.experience.avaya.com

[Manage](#)

Session manager key for Avaya push notification

```
{
  "systemId": "c23d1793-8487-488d-81fb-56508a85667a.experience.avaya.com",
  "description": "Avaya Aura Session Manager",
  "publicKey": "-----BEGIN PUBLIC KEY-----
  VnMFkwEwYHKOZlZjOCAQYIKoZlZjODAQCgAELMPVJlZ0alfYmCSrIVJoMh2RGeU
```

Integrated calling on Zoom mobile

Allow use the integrated phone system to phone call on Zoom mobile client ☒

If this option is turned on and the users are on the list of Phone System Integration, these users can use the 3rd party phone system to place a call.

Create a new client mapping in AADS with *OIDC Discovery URL* set to **Zoom discovery URL** obtained at previous step:

Create new client mapping

Client ID: Zoom

OIDC Discovery URL: aads-poc.frp.zoomappgo.cloud/.well-known/avaya/oidc/configuration_lite

Proxy Address:

Client Secret: NA

Client Name: aads

Enable device Auth: ☐

OK Cancel

Remember to note the *Client Name*, as it will be required for the Zoom configuration later.

Note: AADS will prevent you from submitting the configuration unless the URL is reachable. If the URL is inaccessible, clicking the “OK” button will result in an error. To ensure the above OIDC URL is accessible from AADS the firewall must be configured to allow access. If Proxy server is used ensure its address is specified in the *Proxy Address* field.

4.3 Zoom Configuration

On Zoom web portal navigate to *Account Management > Phone System Integration > Settings* to add AADS domain:

zoom Products Solutions Resources Plans & Pricing Schedule Join Host Web App

Phone System Management

Account Management

Account Profile

Account Settings

Alerts & Notifications

Location Management

Whiteboard Management

Notes Management

Docs Management **NEW**

Recording and Transcript Management

Clip Management

Meeting Summary Management

Survey Management

Workflow Management **BETA**

Phone System Integration

Reports

Integrated users **Settings**

Zoom discovery URL <https://zoom.us/join-unknown/avaya/oidc/configuration>

Avaya Aura Device Service domains	Client name	AADS domain
	aads	aads.engageavaya.ec.avayacloud.com

[Manage](#)

Session manager key for Avaya push notification

Please copy the Key to Export from Session Manager >> Network Configuration >> Push Notification

Integrated calling on Zoom mobile

Allow use the integrated phone system to phone call on Zoom mobile client ☒

If this option is turned on and the users are on the list of Phone System Integration, these users can use the 3rd party phone system to place a call.

If no AADS is previously configured, the **Add** button will be visible; otherwise, the **Manage** button will appear to edit the list of domains. Click the **Add** or **Manage** button as applicable, enter the Client Name from AADS as the client name, and specify the AADS domain.

It is supported to add multiple domains as needed.

Edit AADS domains

Make sure the client names matches the client mapping of the AADS.

Client name	AADS domain
aads	https:// aads.engageavaya.ec.avayacloud.co

[+ Add](#)

[Cancel](#) [Save](#)

5 Session Border Controller (SBC) configuration

5.1.1 Add SBC User Agent

To enable successful registration for remote workers, ensure a **User Agent** is added with the following regular expression: `. *ZoomPbxPhone_.*`

The screenshot shows the 'User Agents' configuration page in the Avaya Session Border Controller for Enterprise. The left sidebar contains a navigation menu with 'User Agents' highlighted. The main area displays a table of existing user agents. A new user agent, 'ZoomPbxPhones', has been added at the bottom, with a regular expression of '. *ZoomPbxPhone_.*'. A red arrow points to the 'Add' button in the top right corner of the table.

Name	Regular Expression	Edit	Delete
Avaya Agent for Desktop	*Avaya Agent.*	Edit	Delete
AvayaCommunicator Equinox	*Avaya Communicator3.*	Edit	Delete
AvayaCommunicator iPhone	*Avaya Communicator for iPhone.*	Edit	Delete
J179	*Avaya J179 IP Phone.*	Edit	Delete
one-X Deskphone	*one-X Deskphone.*	Edit	Delete
J169	*Avaya J169 IP Phone.*	Edit	Delete
Android	*Avaya Communicator Android.*	Edit	Delete
ZoomPbxPhones	*ZoomPbxPhone_.*	Edit	Delete

5.1.2 Add SBC Endpoint Flow

Add a new User Agent (created at previous step) to allowed Network – Endpoint – Subscriber Flows:

The screenshot shows the 'End Point Flows' configuration page in the Avaya Session Border Controller for Enterprise. The left sidebar contains a navigation menu with 'End Point Flows' highlighted. The main area displays a table of existing endpoint flows. A new endpoint flow, 'ZoomPbxPhones', has been added at the bottom, with a priority of 9, flow name 'ZoomPbxPhones', URI Group '*', Source Subnet '*', User Agent 'ZoomPbxPhones', and End Point Policy Group 'RW-EPPG'. A red arrow points to the 'Add' button in the top right corner of the table.

Priority	Flow Name	URI Group	Source Subnet	User Agent	End Point Policy Group
1	one-X Deskphone	*	*	one-X Deskphone	RW-EPPG
2	Avaya Agent for Desktop	*	*	Avaya Agent for Desktop	RW-EPPG
3	Avaya Communicator for...	*	*	AvayaCommunicator iPhone	RW-EPPG
4	Avaya J179 Phone	*	*	J179	RW-EPPG
5	RW-Android	*	*	Android	RW-EPPG
6	Avaya Communicator	*	*	AvayaCommunicator Equinox	RW-EPPG
7	Avaya J169 Phone	*	*	J169	RW-EPPG
8	Sub_WEBRTC_SM	*	*	*	WEBRTC-EPPG
9	ZoomPbxPhones	*	*	ZoomPbxPhones	RW-EPPG

5.1.3 SBC Signaling Manipulation script (specific customers only)

Avaya strongly recommends using **TLS signaling** and **SRTP media** for all soft clients registering through an SBC to ensure optimal security.

If this recommendation is not followed, the installation of the following Signaling Manipulation script is necessary to ensure proper handshake functionality between the Zoom Workplace client and Session Manager.

```
within session "ALL"
{
    act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
    and %METHOD="REGISTER"
    {
        if (exists(%HEADERS["User-Agent"][1])) then
        {
            if (%HEADERS["User-Agent"][1].regex_match("Zoom.*")) then
            {

%HEADERS["To"][1].URI.PARAMS["sc"]=%HEADERS["To"][1].URI.SCHEME;
                %HEADERS["To"][1].URI.PARAMS["ho"]=
%HEADERS["To"][1].URI.HOST;

            }
            if (%HEADERS["User-
Agent"][1].regex_match("AvayaCloudAuraClient.*")) then
            {

%HEADERS["To"][1].URI.PARAMS["sc"]=%HEADERS["To"][1].URI.SCHEME;
                %HEADERS["To"][1].URI.PARAMS["ho"]=
%HEADERS["To"][1].URI.HOST;

            }
        }
        act on message where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING" and %METHOD="REGISTER"
        {
            if (exists(%HEADERS["To"][1].URI.PARAMS["sc"])) then
            {
                %HEADERS["To"][1].URI.SCHEME =
%HEADERS["To"][1].URI.PARAMS["sc"];
                remove(%HEADERS["To"][1].URI.PARAMS["sc"]);
            }
            if (exists(%HEADERS["To"][1].URI.PARAMS["sc"])) then
            {
                %HEADERS["To"][1].URI.HOST = %HEADERS["To"][1].URI.PARAMS["ho"];
                remove(%HEADERS["To"][1].URI.PARAMS["ho"]);
            }
        }
    }
}
```

6 Certificates

To ensure secure communication with Zoom, each Session Manager must have the **DigiCert Global Root G2** certificate installed. This certificate needs to be manually added, as SM does not automatically trust public Certificate Authorities (CAs).

1. In SMGR navigate to **Services > Inventory > Manage Elements** page.
2. For each SM in the list, click the "**More Actions**" dropdown and select "**Manage Trusted Certificates**".
3. Add Trusted certificate:
 - a. Select Store Type to add trusted certificate: **WEBSPPHERE**
 - b. Import **DigiCert Global Root G2** certificate and **Commit**.

Refer to DigiCert web site to download the certificate -

<https://www.digicert.com/kb/digicert-root-certificates.htm#otherroots>

Note: Repeat steps above for each SM.

7 Push Notification

Zoom supports push notifications through its own push entity and does not utilize the Avaya push entity.

Refer to the instructions below and ensure the firewall policy is updated to allow access to the **avayaark.zoom.us** provider address.

1. Navigate to *Session Manager → Network Configuration → Push Notification → Notification Provider* page
2. Add a new entry with the following contents:
 - Provider Name: **Zoom Provider**
 - Provider Address: **avayaark.zoom.us**
 - Provider Port: **443**
 - Company Domain: *<customer's domain>*
3. (optional) **Enable Use Forward Proxy** checkbox if Proxy server is in use.
4. Click **Generate Keys**
 - Key to Export, System Id and Public Key will be created.
5. Copy the content of **Key to Export**
 - This key needs to be added to Zoom Web Admin Portal (refer to step 13).

6. Click **Verify Settings** to ensure the connection is successful.
7. Click **Commit**.
8. Navigate to *Session Manager > Network Configuration > Push Notification > Notification Application Settings* page.
9. Add a new entry with the following contents:
 - Application Name: **Zoom client**
 - Application Id: **us.zoom.videomeetings**
 - Push Notification Provider: **Zoom Provider**

10. Click **Verify Settings** to ensure the connection is successful.
11. Click **Commit**.
12. Navigate to Zoom Web Admin portal > *Account Management > Phone System Integration > Settings*.
13. Copy over the exported Key from Session manager in **“Session Manager key for Avaya push notification”**.

Zoom Products Solutions Resources Plans & Pricing Schedule Join Host Web App

Alerts & Notifications
Location Management
Whiteboard Management
Notes Management
Docs Management **NEW**
Recording and Transcript Management
Clip Management
Meeting Summary Management
Survey Management
Workflow Management **BETA**
Phone System Integration
Reports
Scheduling Tracking Fields
> Advanced

Integrated users **Settings**

Zoom discovery URL <https://zoom.us/well-known/avaya/oidc/configuration>

Avaya Aura Device Service domains	Client name	AADS domain
aads	aads	aads.engageavaya.ec.avayacloud.com
eaaads09	eaaads09	aads-09.experience.avaya.com

[Manage](#)

Session manager key for Avaya push notification

```
{
  "systemId": "c23d1793-8487-488d-81fb-56508a85667a.experience.avaya.com",
  "description": "Avaya Aura Session Manager",
  "publicKey": "-----BEGIN PUBLIC KEY-----
  \nMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAELMPVJfz0alfYmCSrIVjoMh2RGeU
```

Integrated calling on Zoom mobile

Allow use the integrated phone system to phone call on Zoom mobile client ☒

If this option is turned on and the users are on the list of Phone System Integration, these users can use the 3rd party phone system to place a call.

Note: If connectivity verification fails at steps 6 or 10, verify that the certificate is correctly installed (refer to section 6) and check if a firewall update might be required.

8 Device Adaptation

In certain environments the below Device Adaptation configuration may be required in order for Zoom client features to operate properly. For example, if the system is configured to send E.164 numbers for the calling party to the Zoom client, it may not be able to match the number with the corresponding user's extension. In such cases the below Device Adaptation can be configured to translate the calling number information being sent to the client.

Note: If the Communication Manager (CM) is configured to use public numbering format on the trunk group(s) and/or the system is configured to adapt numbers to a format different from the number format recognized by the Zoom client, this Device Adaptation configuration will be required.

8.1 Regular Expression Adapter configuration

1. In SMGR Navigate to *Routing* → *Adaptations* → *Regular Expression Adaptations* page
2. Add a new entry with the following contents on the **Regular Expression Adaptation Details** page:
 - o Name: **Zoom Digit Adaptation**

- State: **enabled**

AVAYA
Aura® System Manager 10.2

Users ▾ Elements ▾ Services ▾ Widgets ▾ Shortcuts ▾

Home Routing

Routing
Domains
Locations
Conditions
Adaptations
Adaptations
Regular Expressions
Device Mappings
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns
Regular Expressions

Regular Expression Adaptation Details [Commit] [Cancel]

General

* Name: Zoom Digit Adaptation
Notes:
State: enabled ▾

Incoming Adaptation Rules

[Add] [Edit] [Duplicate] [Remove]

0 Items [Filter:]

Order	Rule Name	Condition	Notes
-------	-----------	-----------	-------

Outgoing Adaptation Rules

[Add] [Edit] [Duplicate] [Remove]

0 Items [Filter:]

Order	Rule Name	Condition	Notes
-------	-----------	-----------	-------

[Commit] [Cancel]

3. Under **Outgoing Adaptation Rules** click on **Add**
4. Add a new entry with the following contents on the **Regular Expression Adaptation Rule Details** page:
 - Name: **Zoom 10-digit adaptation**
 - Condition: (blank)
 - Direction: **Outgoing**
 - Under **Rule Actions**, configure rules for adapting **P-Asserted-Identity**, **Contact**, and **From** headers as shown below. Enter the **Match Expression** and **Replace / Add Expression** as required for the given Aura configuration.

AVAYA
Aura® System Manager 10.2

Users ▾ Elements ▾ Services ▾ Widgets ▾ Shortcuts ▾

Home Routing

Routing
Domains
Locations
Conditions
Adaptations
Adaptations
Regular Expressions
Device Mappings
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns
Regular Expressions

Regular Expression Adaptation Rule Details [Done] [Cancel]

General

* Rule Name: Zoom 10-digit adaptation
Condition: ▾
* Direction: Outgoing ▾
* Order: 1 ▾
Notes:

Rule Variables

[Add] [Remove]

0 Items [Filter:]

Variable Name	Source Type	Source	Instance	Match Expression	Notes
---------------	-------------	--------	----------	------------------	-------

Rule Actions

[Add] [Remove]

3 Items [Filter:]

Order	Source Type	Source	Instance	Operation	Match Expression	Replace / Add Expression	Notes
1	Header ▾	P-Asserted-Identity	any	modify ▾	\\+1555	555	remove +1 for Zoom
2	Header ▾	Contact	any	modify ▾	\\+1555	555	remove +1 for Zoom
3	Header ▾	From	any	modify ▾	\\+1555	555	remove +1 for Zoom

Select : All, None

Note: The entries shown in the screenshot above only represent an example configuration. The digit adaptations required need to be customized for the specific Aura configuration.

8.2 Regular Expression Adapter configuration

1. Navigate to *Routing* → *Adaptations* → *Device Mappings* page
2. Add a new entry with the following contents on the **Device Mapping Details** page:
 - Name: **Zoom mapping**
 - User Agent: **Zoom.***
 - Origination Dial Pattern Set: (blank)
 - Under **Adaptations**, click on **Add** to add the **Zoom digit adaptation** to the device mapping.

9 User Provisioning

9.1 System Manager (SMGR) configuration

9.1.1 User Management – Session Manager Profile screen

To enable Zoom for a specific user, you must select Zoom from the drop-down list under Third-Party Clients on the Session Manager Profile for that user. See the screen below.

Home

User Management

User Management

Manage Users

Public Contacts

Shared Addresses

System Presence ACLs

Communication Profile ...

Emergency Calling Application Sequences

Emergency Calling Origination Sequence :

Select

Emergency Calling Termination Sequence :

Select

Call Routing Settings

Home Location :

NR1381_RW_NAR1

Conference Factory Set :

Select

Call History Settings

Enable Centralized Call History? :

☒

Third Party Clients

Enable Zoom Client :

☒

9.1.2 Session Manager – Communication Profile Editor screen

You can also enable Zoom for many users at one time using the Communication Profile Editor screen. The Third-Party Client column shows the selected value for that user.

Session Manager

Dashboard

Session Manager Ad...

Global Settings

Communication Profile ...

Network Configuration

Device and Location ...

Communication Profile Editor

This page allows you to edit Session Manager Communication Profiles for users.

Session Manager Communication Profiles

2 Items

Show

All

Filter: Enable

<input type="checkbox"/>	Login Name	Address: Handle	Address: Domain	Secondary Session Manager	Origination Sequence	Block New Registration When Maximum Registrations Active?	Home Location	Enable Centralized Call History?	Third Party Client
<input type="checkbox"/>	a@a.com	5551110500	avaya.com	(None)	(None)	No	Home	No	ZOOM
<input type="checkbox"/>	b@b.com	b	avaya.com	(None)	(None)	No	Home	No	(None)

Select : All, None

9.1.3 Session Manager – User Registrations screen

The screen below was customized to show the SIP User Agent header, showing the Zoom clients that have registered in the column on the right-hand side.

				zoom					
<input type="checkbox"/>	Show	5551110127@engageavaya.ec.avayacloud.com	zoomuser27@cuoncloud.com	Zoom27	User27	NR1381_RW_NAR1	10.16.93.9	ZoomPbxPhone_Windows_Client(6.2.0.45566)	2/3
<input type="checkbox"/>	Show	5551110127@engageavaya.ec.avayacloud.com	zoomuser27@cuoncloud.com	Zoom27	User27	NR1381_RW_NAR1	10.16.93.9	ZoomPbxPhone_IOS_Pad(6.2.0 (17737))	2/3
<input type="checkbox"/>	Show	5551110125@engageavaya.ec.avayacloud.com	zoomuser25@cuoncloud.com	Zoom25	User25	NR1381_RW_NAR1	10.16.93.9	ZoomPbxPhone_IOS_Pad(6.2.0 (14494))	1/3
<input type="checkbox"/>	Show	5551110122@engageavaya.ec.avayacloud.com	zoomuser22@cuoncloud.com	Zoom22	User22	NR1381_RW_NAR1	10.16.93.9	ZoomPbxPhone_Android_Phone(66.6.64722.0907)	1/3
<input type="checkbox"/>	Show	5551110121@engageavaya.ec.avayacloud.com	zoomuser21@cuoncloud.com	Zoom21	User21	NR1381_RW_NAR1	10.16.93.17	Avaya one-X Deskphone 7.1.15.2.1 ccf954a3e1f6	1/3
<input type="checkbox"/>	Show	5551110120@engageavaya.ec.avayacloud.com	zoomuser20@cuoncloud.com	Zoom20	User20	NR1381_RW_NAR1	10.16.93.9	ZoomPbxPhone_MAC_Client(6.2.0.40057)	1/3
<input type="checkbox"/>	Show	5551110107@engageavaya.ec.avayacloud.com	zoomuser07@cuoncloud.com	Zoom07	User07	NR1381_RW_NAR1	10.16.93.17	ZoomPbxPhone_Android_Pad(6.0.2 (20650))	1/3
<input type="checkbox"/>	Show	5551110103@engageavaya.ec.avayacloud.com	zoomuser03@cuoncloud.com	Zoom03	User03	NR1381_RW_NAR1	10.16.93.17	Avaya J179 IP Phone 4.1.5.0.6 c81fea973de3	1/3
<input type="checkbox"/>	Show	5551110100@engageavaya.ec.avayacloud.com	zoomuser00@cuoncloud.com	Zoom00	User00	NR1381_RW_NAR1	10.16.93.17	Avaya J179 IP Phone 4.1.5.0.6 c81fea40568	1/3
<input type="checkbox"/>	Show	---	zoomuser05@cuoncloud.com	Zoom05	User05	NR1381_RW_NAR1	---	---	0/3
<input type="checkbox"/>	Show	---	zoomuser04@cuoncloud.com	Zoom04	User04	NR1381_RW_NAR1	---	---	0/3

Once the configuration above is complete Zoom Admin user can start with user provisioning.

9.2 Zoom User Provisioning

9.2.1 Add users

Navigate to Zoom Web Admin portal > *Account Management* > *Phone System Integration* > *Integrated Users*.

Note: Zoom users should be already added under *User Management* > *Users*.

1. Click “**Add AADS user**” for single user provisioning or choose “Import from CSV” for bulk provisioning.
2. Select user(s) from the list, select AADS domain and click Add button.

Note: You can add a maximum of 50 users.

Add PSI users with AADS

1. Select users

<input type="checkbox"/>	Name	Email Address
<input type="checkbox"/>	CL Teoh	
<input type="checkbox"/>	Avaya_Go_Test Ut955EPg	kaiwang.nie+GO+1725513131@test.z...

Selected(0/50)

Clear all

< > 15/page 2 result(s)

2. Assign AADS domain

aads.engageavaya.ec.avayacloud.com

Cancel Add

The newly added user will initially appear in the **Integrated Users** list with the status **"Syncing."** Refresh the page to update the status. If the user is successfully provisioned, the SIP Station and Domain will be displayed on the screen and Status will be updated accordingly.

<input type="checkbox"/>	Email	User Name	AADS domain	Domain	Last Registration Time	Status	
<input type="checkbox"/>	aadstestzoom@gmail.com	5551112112	aads.engageavaya.ec.avayaclou...	engageavaya...	11/05/2024 03:25:58 AM	Registered	...

9.2.2 Import users

To add users, ensure that the email address matches the email address that was used while creating the Zoom user and the assigned license. Updated users can only be applied to the AADS domain, so do not modify the email address in the existing data. Ensure that the AADS domain matches the domain registered in the **Settings** tab.

Note: The maximum number of users is 10,000.

1. Click the **Integrated Users** tab at the top of the page.
2. At the top of the page, click **Import from CSV**, then choose **Import PSI users with AADS**.
3. In either the **Add users** tab or the **Update users** tab, download and edit the CSV template, then upload the template.

9.2.3 Export users to a CSV file

1. Click the **Integrated Users** tab at the top of the page.
2. At the top of the page, click **Export to CSV file**.
The list of users and their information will be exported to a CSV file.

9.2.4 Status of the Phone System Integration (PSI) user

Status	Description
Idle	The SIP credential has already been synchronized with Zoom, but the user has not yet registered with the Zoom Workplace app.
Syncing	Waiting for Zoom to load SIP credentials, which is dependent on the sync queue workload.
Sync failed	Unable to load SIP credentials from the AADS.
Register failed	The Zoom Workplace app is unable to register with the SIP credential. You can check the error code and detailed errors on the PSI page.
Registered	The Zoom Workplace app has successfully registered with the SIP server.

©2025 Avaya LLC. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya LLC. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya LLC. 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.