



Avaya one-X[®] Client Enablement Services
Service Pack Release 6.2.9
Release Notes

Issue 1.0
September, 2019

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products.

Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on its hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website:

<http://www.avaya.com/support>

Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions thereto.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, <http://support.avaya.com/LicenseInfo/> ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available

to you. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users.

License type(s)

Named User License (NU). You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. "Named User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Avaya - Proprietary. Use pursuant to the terms of your signed agreement or Avaya policy.

DRAFT - November 05, 2012 - 12:05 PM

Third-party components

"Third Party Components" mean certain software programs or portions thereof included in the Software that may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya's website at: <http://support.avaya.com/ThirdPartyLicense/>. You agree to the Third Party Terms for any such Third Party Components.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: <http://www.avaya.com/support>.

Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Providing Telecommunications Security

Telecommunications security (of voice, data, and/or video communications) is the prevention of any type of intrusion to (that is, either unauthorized or malicious access to or use of) your company's telecommunications equipment by some party.

Your company's "telecommunications equipment" includes both this Avaya product and any other voice/data/video equipment that can be accessed by this Avaya product (that is, "networked equipment").

An "outside party" is anyone who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf. Whereas, a "malicious party" is anyone (including someone who might be otherwise authorized) who accesses your telecommunications equipment with either malicious or mischievous intent. Such intrusions might be either to/through synchronous (time-multiplexed and/or circuit-based), or asynchronous (character-, message-, or packet-based) equipment, or interfaces for reasons of:

- Utilization (of capabilities special to the accessed equipment)
- Theft (such as, of intellectual property, financial assets, or toll facility access)
- Eavesdropping (privacy invasions to humans)
- Mischief (troubling, but apparently innocuous, tampering)
- Harm (such as harmful tampering, data loss or alteration, regardless of motive or intent)

Be aware that there might be a risk of unauthorized intrusions associated with your system and/or its networked equipment. Also realize that, if such an intrusion should occur, it might result in a variety of losses to your company (including but not limited to, human/data privacy, intellectual property, material assets, financial resources, labor costs, and/or legal costs).

Responsibility for Your Company's Telecommunications Security

The final responsibility for securing both this system and its networked equipment rests with you — Avaya's customer system administrator, your telecommunications peers, and your managers. Base the fulfillment of your responsibility on acquired knowledge and resources from a variety of sources including but not limited to:

- Installation documents
- System administration documents
- Security documents
- Hardware-/software-based security tools
- Shared information between you and your peers
- Telecommunications security experts

To prevent intrusions to your telecommunications equipment, you and your peers must carefully program and configure:

- Your Avaya-provided telecommunications systems and their interfaces
- Your Avaya-provided software applications, as well as their underlying hardware/software platforms and interfaces
- Any other equipment networked to your Avaya products

TCP/IP Facilities

Customers might experience differences in product performance, reliability and security depending upon network configurations/design and topologies, even when the product performs as warranted.

Standards Compliance

Avaya Inc. is not responsible for any radio or television interference caused by unauthorized modifications of this equipment or the substitution or attachment of connecting cables and equipment other than those specified by Avaya Inc. The correction of interference caused by such unauthorized modifications, substitution or attachment is the responsibility of the user. Pursuant to Part 15 of the Federal Communications Commission (FCC) Rules, the user is cautioned that changes or modifications not expressly approved by Avaya Inc. might void the user's authority to operate this equipment.

Federal Communications Commission Statement

Part 15:

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Canadian Department of Communications (DOC) Interference Information

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment.

European Union Declarations of Conformity



Avaya Inc. declares that the equipment specified in this document bearing the "CE" (Conformité Européenne) mark conforms to the European Union Radio and Telecommunications Terminal Equipment Directive (1999/5/EC), including the Electromagnetic Compatibility Directive (89/336/EEC) and Low Voltage Directive (73/23/EEC).

Copies of these Declarations of Conformity (DoCs) can be obtained by contacting your local sales representative and are available on the Avaya Support website:

<http://www.avaya.com/support>

Trademarks

Avaya, the Avaya logo, Avaya one-X® Client Enablement Services, Communication Manager, Modular Messaging, and Conferencing are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions. All non-Avaya trademarks are the property of their respective owners, and "Linux" is a registered trademark of Linus Torvalds.

Downloading documents

For the most current versions of documentation, see the Avaya Support website:

<http://www.avaya.com/support>

Contact Avaya Support

See the Avaya Support website: <http://support.avaya.com> for product notices and articles, or to report a problem with your Avaya product.

For a list of support telephone numbers and contact addresses, go to the Avaya Support website: <http://support.avaya.com>, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

What's new in Release 6.2.9.....	8
Fixed issues.....	9
Following issues are fixed in Avaya one-X® Client Enablement Services release 6.2.9	9
Avaya one-X® Client Enablement Services Server Fixes	9
Deploying Avaya one-X® Client Enablement Services release 6.2.9.....	10
Obtaining Avaya one-X® Client Enablement Services release 6.2.9.....	10
Installing Avaya one-X® Client Enablement Services release 6.2.9	12
Upgrading Avaya one-X® Client Enablement Services release 6.2.9	12
Troubleshooting – Reverting to the previous release of software after an upgrade	12
Migration process for the presence services from existing PS to PS 7.x.x.....	12
Upgrading Handset Server on Standalone machine from 6.2 build to 6.2.9 build	13
Obtaining Avaya one-X® Client Enablement Services release 6.2 – Clients Software.....	13
Interoperability and requirements	14
Software and firmware compatibility matrix	14
Hardware compatibility	15
Tested Environment.....	15
Unsupported Configurations.....	16
General issues and workarounds.....	16
Known issues and workarounds.....	18
Interoperability Issues	18
Avaya one-X® Client Enablement Services - server issues	20
Avaya one-X® Client Enablement Services - client issues.....	24
Known issues when using CES 6.2.x clients with a CES 6.1.x server	24
Updates in Administering Guide	26
Enterprise Directory domains on page 131 and 152.....	26
System Manager certificate is not imported after installation on page 306.....	26
Running CLI commands on a Linux system on page 179	27
Appendix A: Steps to replace default certificate with SMGR CA on CES 6.2.9 (AC connection fix).....	28
Appendix B: Enabling RC4 cipher suite.....	29

Appendix C: Installing Avaya one-X® Client Enablement Services release 6.2.9 with blocked nsuniqueid on SUN LDAP	30
Appendix D: Steps to replace default ‘Logon Attribute’ to another LDAP attribute (1XC login fix).....	31
Appendix E: Steps to disable the fix for Spectre/Meltdown vulnerability	32
Appendix F: Ports for Client Enablement Services Server (eth0)	33
Appendix G: Acronyms	37

What's new in Release 6.2.9

- IBM WebSphere is upgraded to 8.5.5.15 release
- Apache Tomcat is upgraded to 7.0.94 release
- Avaya one-X® Client Enablement Services 6.2.9 is configured to use TLSv1.2 only
- Added compatibility with RHEL up to release 6.10
- Compatibility with Aura 8.1 (for details please refer to the “Interoperability and requirements” section)

Fixed issues

Following issues are fixed in Avaya one-X® Client Enablement Services release 6.2.9

Avaya one-X® Client Enablement Services Server Fixes

ONEXCESSERVER-10929	Upgrade WebSphere to 8.5.5.15	Fixed
ONEXCESSERVER-10928	Tomcat upgrade to 7.0.94	Fixed
ONEXCESSERVER-10927	CVE-2014-8730 (Medium) - Port 8008	Fixed
ONEXCESSERVER-10932	CFD: CES reverting back to TLS 1.0, causing secure connection to AAM to fail (WestJet)	Fixed
ONEXCESSERVER-10931	Force TLS 1.2 on all CES interfaces	Fixed
ONEXCESSERVER-10930	Allow installation on RHEL 6.10 and verify compatibility	Fixed

Deploying Avaya one-X® Client Enablement Services release 6.2.9

Latest Avaya one-X® Client Enablement Services documents are available at <http://support.avaya.com>

- [Avaya one-X® Client Enablement Services Overview and Specification Guide](#)
- [Implementing Avaya one-X® Client Enablement Services](#)
- [Administering Avaya one-X® Client Enablement Services](#)
- [Troubleshooting Avaya one-X® Client Enablement Services](#)

Refer to known issues for understanding the issues and workarounds before deploying this build.

Obtaining Avaya one-X® Client Enablement Services release 6.2.9

Customers can find the one-X® Client Enablement Services release 6.2.9 files at Avaya PLDS <https://plds.avaya.com>. The download IDs are as following

- Client Enablement Services Release 6.2.9 for RHEL build:
 - 1XCES000197 [Avaya one-X Client Enablement Services R6.2 SP9 RHEL Installer (File 1 of 3) onexces.binaa]
 - 1XCES000198 [Avaya one-X Client Enablement Services R6.2 SP9 RHEL Installer (File 2 of 3) onexces.binab]
 - 1XCES000199 [Avaya one-X Client Enablement Services R6.2 SP9 RHEL Installer (File 3 of 3) onexces.binac]
- Standalone Handset Server installer:
 - 1XCES000200 [Avaya one-X Client Enablement Services R6.2 SP9 Handset Server RHServer.bin]
- Migration utility for deployment on RHEL:
 - 1XCES000201 [Avaya one-X Client Enablement Services R6.2 SP9 Migration Utility onexces_migrator.bin]

Followings are steps to download the files from Avaya PLDS

1. Login with the Avaya handle.
2. Select View Downloads as below screenshot

Home 

Dat NGUYEN ANH, welcome to the Avaya Product Licensing and Delivery System
Please click here for Getting Started documentation and information.

Quick Activation
To begin the activation process, provide the License Activation Code (LAC), then click Activate. The License Host for the activation can also be provided.

*LAC(s): [Add more LACs](#)

License Host:

View Activation Record >>

Asset Mgmt

[Asset Dashboard](#)
[View Entitlements](#)
[View Downloads](#)

Activation Mgmt

[Activation Dashboard](#)
[View Activation Record](#)

Reports

[Reports](#)

Administration

[My Users](#)
[My Company](#)
[Manage Groups](#)
[More...](#)

3. Click Search button as below screenshot

Downloads

 To search for downloads, you must first select a company. Either type the company name in the field below, or use the find icon to search for a

 % Company name:  [Apply Company]

Suggested Downloads

Search by Download

Search by License Host

Download History

4. Enter “avaya” as search string, then click Search Companies as below screenshot

Search Companies 

Use this page to search for and select the company you want to use. You can search for the company based on the name, ID, type, or status. To display additional criteria, click Advanced Search. After providing search criteria, to display a list of companies, click Search Companies. To select the company, click its Select link. [Click here for additional Search Tips.](#)

%Indicates wildcard search

%Name:

ID:

Type:

Status: Active

Search Companies >> Cancel >> [Advanced Search]

5. Click Select on the highlighted item below

Search Companies 

Use this page to search for and select the company you want to use. You can search for the company based on the name, ID, type, or status. To display additional criteria, click Advanced Search. After providing search criteria, to display a list of companies, click Search Companies. To select the company, click its Select link. [Click here for additional Search Tips.](#)

%Indicates wildcard search

%Name:

ID:

Type:

Status: Active

Search Companies >> Cancel >> [Advanced Search]

Showing: 1-30 of 46 | [Next >](#)

Select	ID	Name	Status	HQ Country	HQ City	Type
Select	AVAYA	AVAYA	Active	United States	ALL DOWNLOADS	Avaya
Select	3315289	AVAYA	Active	United States	ORLANDO	Business
Select	4572205	AVAYA	Active	United States	PLANO	Business
Select	4859492	AVAYA	Active	United States	VALRICO	Business
Select	5004493	AVAYA	Active	United States	EDEN PRAIRIE	Business
Select	50051587	AVAYA	Active	United Kingdom	FLEET	Business

6. Fill in the search criteria as in screenshot below, then click Search Downloads

AVAYA -- ALL DOWNLOADS; NJ; United States  [Change Company]

Suggested Downloads Search by Download Search by License Host Download History

ATTENTION: The **Avaya EULA** must be accepted in order to complete this transaction. SOFTWARE DOWNLOADED FROM THIS SITE MUST BE ACTIVATED WITHIN 30 DAYS OF INSTALLATION OR THAT SOFTWARE CERTAIN FEATURES/FUNCTIONALITY MAY BE DISABLED. The terms of the Avaya EULA apply to the Software downloaded from this site ("Downloaded Software"). In addition, your licensing agreement with Avaya or an authorized Avaya channel reseller applies equally to Software previously licensed and to the Downloaded Software. Downloading, activation, and/or use of the Downloaded Software indicates your acceptance of these license terms. Only Authorized Users may obtain Downloaded Software from this site. The term "Authorized Users" is defined as an authorized channel reseller and its designated employee and customers defined as the asset owner(s). To search for available downloads, provide search criteria, then click Search Downloads. Please note that the download function requires that pop-up blocking be turned off. For more information, see [Turning off pop-up blocking](#). [Click here for additional Search Tips.](#)

% indicates wildcard search

Download pub ID:

Group name:

%Download name:

Application:

Download type:

Version:

Search Downloads >> [Advanced search]

7. Click Download to download the one-X Client Enablement Services template, software only package, Migration utility, standalone Handset Server and Mobile Client applications.

8. For software only installation on RHEL 6.5+, merge downloaded files into one using the following command:

```
# cat onexces.binaa onexces.binab onexces.binac > onexces.bin
```


then copy onexces.bin file at /opt on your RHEL machine that hosts the Client Enablement Services server.

Installing Avaya one-X® Client Enablement Services release 6.2.9

Important Notes:

1. Make sure you have NTP server configured, up and running. This is required for Avaya one-X® Client Enablement Services release 6.2.9 deployment.
2. Make sure SMGR SSL certificate is not expired.

Upgrading Avaya one-X® Client Enablement Services release 6.2.9

Important Notes:

1. The Client Enablement Services release 6.2.9 can be upgraded from release 6.2.
2. In LDAP details during the pre-web installation steps, the administrative user name may not be selected automatically from the drop down list (ONEXCESSERVER-9973). An administrative user name needs to be selected manually for successful upgrade.
3. It is not possible to roll back the upgrade on RHEL deployment. As a workaround, we can downgrade the RHEL deployment and install the backed up database. Please see the [Downgrade Avaya one-X® Client Enablement Services to previous 6.2 build on RHEL 6.5+](#) for more details.
4. It is recommended to wait about 15-20 minutes after upgrade is successful before doing any administration or database synchronization.
5. It is assumed that the Aura Setup is upgraded first before upgrading the CES 6.2.9.
6. Follow the process mentioned in “migration process for the presence services from existing PS to PS 7.x.x” to make presence services work if PS 6.x was installed previously.

Troubleshooting – Reverting to the previous release of software after an upgrade

Downgrades of CES from a newer release to an older release are not supported. Avaya recommends that prior to any upgrade you maintain a backup of all software prior to upgrades so that if it is necessary to revert back to the prior release a reinstall and restore can be performed. The following steps define the process to implement this task:

1. When CES upgrade is run, a backup file is taken automatically. This file should be stored somewhere in case a roll back is required later. the backup is created in /opt/avaya/backups/ces/ directory
2. If the result of the upgrade is not satisfactory, CES installation should be uninstalled using “Uninstalling Client Enablement Services on Linux” chapter from the Implementation guide.
3. The old CES version should be installed (the one that was running before the upgrade).
4. When the installation is finished, run the post-installation configuration tool (installation wizard or preweb) and specify the backup file taken at step 1 in the "Install using Migration Archive" window. This will restore the DB backup and installation settings that were used before the upgrade.

Migration process for the presence services from existing PS to PS 7.x.x

Do not use the previous migration script moveToPS70.sh in /opt/avaya/1xp. New script migratePSto7xx.sh /opt/avaya/1xp must be used instead of it.

Procedure

Follow the below mentioned steps to migrate PS from earlier release to PS 7.x.x release:

1. Navigate to /opt/avaya/1xp directory
2. Script is using Admin CLI, so please make sure Admin CLI is extracted on your machine:
tar -xvf 1XP_Admin_CLI_Client.tar (from /opt/avaya/1xp) if Admin CLI is not found script will alert
3. Script is doing following steps:
 - Disable server
 - Migrate server to 7.x.x
 - Update server properties
 - Restart Presence Service

Run the script:

```
./migratePSto7xx.sh -u <username> -p <password> -h <handle>
```

or

```
./migratePSto7xx.sh -u <username> -p <password> -h <handle> -li <(LUS) IP Address> -lp <(LUS) Port> -io <(LUS) IP Address Optional> -po <(LUS) Port>
```

Where:

<username> - the user name of the Client Enablement Services administration application.

<password> - the password of the Client Enablement Services administration application.

<handle> - the handle of Presence Server

4. Once script execution finished – you are done.

Upgrading Handset Server on Standalone machine from 6.2 build to 6.2.9 build

This procedure is only applicable for standalone Handset Server deployment. In co-resident Handset Server deployment, the Handset Server will be upgraded as part of Client Enablement Services server upgrade process. Use following steps to upgrade standalone Handset Server. This process takes few minutes to complete.

1. Copy the Handset Server installable (**RHServer.bin**) to the standalone machine that hosts the Handset Server.
2. Login into the Handset Server machine using SSH
3. Install the 6.2.9 Handset Server (**RHServer.bin**) on a standalone machine. This will automatically replace the existing 6.2 Handset Server. The other Handset Server settings are retained.

Obtaining Avaya one-X® Client Enablement Services release 6.2 – Clients Software

Customers can find Avaya One-X Client Enablement Services release 6.2 – Clients application files at:

1. The Avaya Equinox 3.x for Android client is available for download from the Google Play Market.
2. The Avaya Equinox 3.x for iOS client is available for download from Apple Appstore.

Interoperability and requirements

Software and firmware compatibility matrix

The following table shows the supported systems by Avaya one-X® Client Enablement Services release 6.2.9 (it lists the latest patch / service pack of the component that is tested with Client Enablement Services at the time of release).

Avaya Components	Supported Release
Avaya Aura® System Manager	6.2, 6.3, 6.3.2, 6.3.4, 7.0, 7.1, 8.0, 8.1
Avaya Aura® Communication Manager	5.2.1, 6.2, 6.3, 6.3.2, 6.3.6, 7.0, 7.1, 8.0, 8.1
Avaya Aura® Session Manager	6.2, 6.3, 6.3.2, 6.3.4, 7.0, 7.1, 8.0, 8.1
Avaya Aura® Presence Services	6.1.5, 6.2.1, 6.2.2, 6.2.3, 6.2.4, 6.2.5, 6.2.6, 6.2.7, 7.0, 7.1, 8.0, 8.1
Avaya Modular Messaging	5.2
Avaya Aura Messaging	6.1, 6.2, 6.3, 7.0, 7.1
Avaya Aura® Communication Manager Messaging	6.2, 6.3, 7.0, 7.1
Avaya Meeting Exchange	5.2, 6.2
Avaya Aura Conferencing	6.0, 7.0, 8.0

The following table shows the supported Avaya clients by Avaya one-X® Client Enablement Services release 6.2.9

Avaya Components	Supported Release
Avaya SIP Hard Phones 9620L	2.6.9+
Avaya SIP Hard Phones 9621G	6.3+, 6.4
Avaya SIP Hard Phones 9601	6.1.5+
Avaya H.323 Hard Phones 9620L	3.5.1+
Avaya H.323 Hard Phones 9621G	6.2+
Avaya one-X® Communicator	6.1 SP9, 6.2, 6.2 SP2, 6.2 FP3, 6.2 FP6, 6.2 SP12
Avaya Equinox Client	3.x

The following table shows the supported 3rd party components by Avaya one-X® Client Enablement Services release 6.2.9

3 rd Party Components	Software	Supported Release / Model
CES Server OS	Linux	RHEL 6.5+ 64-bit
Handset Server OS	Linux	RHEL 6.5+
LDAPs	IBM Domino Server	8.5.3, 9.0.1 FP3
	Microsoft Active Directory	2008 R2, 2012 R2, 2016
	Sun Java System Directory Server Enterprise Edition / Oracle Directory Server Enterprise Edition	SDSEE 7.1 / ODSEE 11.1.1.5.0 ODSEE 11.1.7.0
	Novell e-Directory / NetIQ e-Directory	8.8 SP7, 8.8 SP8
	Active Directory Application Mode / Active Directory Lightweight Directory Services	2008 R2
Administration Browser	Microsoft Internet Explorer	11.0
	Mozilla Firefox	53+
	Apple Safari	8.x

Hardware compatibility

The following table shows all supported server hardware with Avaya one-X® Client Enablement Services 6.2.9

Avaya Common Servers	Min. RAM Req.	Platform	One-X CES
HP Proliant DL360 G8 (new install / migration)	32 GB	RHEL 6.5+	6.2.9
HP Proliant DL360 G7 (new install and upgrade / migration)	24 GB	RHEL 6.5+	6.2.9
Dell PowerEdge R610 (new install and upgrade / migration)	24 GB	RHEL 6.5+	6.2.9
S8800 (migration only)	20 GB	RHEL 6.5+	6.2.9
Customer Provided HW (new install only, min spec required)	20 GB	RHEL 6.5+	6.2.9

Tested Environment

The following tables show SV Environment that is used for validating Avaya one-X® Client Enablement Services 6.2.9.

Avaya Components	Supported Release
Avaya Aura® System Manager	7.1.0.0, 8.0.0.0, 8.1.1
Avaya Aura® Communication Manager	7.1.0.0, 8.0.0.1.1, 8.1.1
Avaya Aura® Session Manager	7.1.0.0, 8.0.0, 8.1.1
Avaya Aura® Presence Services	7.1.0.0, 8.0.0, 8.1.0
Avaya Aura Messaging	7.1
Avaya Aura® Communication Manager Messaging	7.0.0.2, 7.1
Avaya Meeting Exchange	6.2 SP5
Avaya one-X® Client Enablement Services	6.2.9
Avaya SIP Hard Phones 9621G	7.0.1.4
Avaya Equinox for Android	3.5, 3.6
Avaya Equinox for iOS	3.5, 3.6
Avaya one-X® Communicator	6.2 FP12

3rd Party Components	Software	Supported Release / Model
CES Server OS	Linux	RHEL 6.5, RHEL 6.10
Handset Server OS	Linux	RHEL 6.5, RHEL 6.10
LDAPs	IBM Domino Server	9.0.1 FP3
	Microsoft Active Directory	2008 R2, 2012 R2
	Oracle Directory Server Enterprise Edition	11.1.1.7.0
	NetIQ (Novell) e-Directory	8.8 SP8
	Active Directory Application Mode / Active Directory Lightweight Directory Services	2008 R2
Administration Browser	Microsoft Internet Explorer	11.0
	Mozilla Firefox	68.0
	Apple Safari	8.x

Unsupported Configurations

The following configurations are NOT supported in this release:

- Presence ACL Access Level = Confirm in User Management in SMGR.

General issues and workarounds

one-X CES ID	Caveat	Workarounds/Notes
Client Enablement Services Server Installation / Upgrade		
ONEXCESSERVER-8825	When installing 1XCES template, lost connection from LDAP server but 1XCES does not show an Error.	Workaround: Need to reinstall the server and make sure the LDAP connection is always up during the installation.
ONEXCESSERVER-9256	1xCES installation fails when RHEL installed using Configuration Mgmt Tool	On the RHEL system, you must be able to administer the users locally
ONEXCESSERVER-9224	Administrator can't access to Scheduler and sub-sequence tabs after fresh install CES 6.2 with multiple Domain (AD2k3 and AD2k8)	The possible cause is the connectivity between CES and LDAP server is lost while installation. Workaround: Re-install and make sure connectivity between CES and LDAP is not lost while installation.
ONEXCESSERVER-10557 / ONEXCESSERVER-9685	Installing CES with blocked nsuniqueid on SUN LDAP will be failed	Please install server according to instruction in Appendix C.
Client Enablement Services Server Administration		
ONEXCESSERVER-9854	No execution permission on 1xpAdmin.sh after extracting 1XP_Admin_CLI_Client.tar	Workaround: manually add execution permission for the file # chmod +x 1xpAdmin.sh
ONEXCESSERVER-9575	CES users are not able to see presence correctly.	The ACL setting must be left as ALLOW for CES users to see Presence correctly of all users.
ONEXCESSERVER-9645	gsk7cmd and ikeyman do not allow creating a CSR in which SAN contains leading digit in hostname	As a workaround, new option "-- nosan" is introduced in CES 6.2.3 script to allow customer to generate a certificate request without SAN. In this case the certificate request would be missing the Subject Alternative Names, but the customer can still request the CA insert these by hand.
NA	Client functionalities would be impaired if same user is configured for both Avaya one-X Mobile server 5.2 and Client Enablement Services.	Do not configure Avaya one-X Mobile server 5.2 and Client Enablement Services for the same user (extension) on Communication Manager.
NA	Client Enablement Services does not support configurations where a managed user is not part of the corporate directory. Furthermore, a unique handle or userid is required for users. Note – the handle or userid should not have any space in it.	All Client Enablement Services users must be part of the corporate LDAP directory. Ensure that userid does not have space in it.
NA	Client Enablement Services does not support multiple direct SIP trunks from the same Client Enablement Services Server to the same Communication Manager server.	Configure only one direct SIP trunk between Client Enablement Services and Communication Manager.
NA	Cannot save Notification server information using Client Enablement Services web admin console if the SMTP server is not reachable (IP and Port)	IP and Port should be reachable while adding SMTP details
ONEXCESSERVER-8087	CES account is not deleted after deleting the user in LDAP and	Full synchronization is required to delete a CES user.

one-X CES ID	Caveat	Workarounds/Notes
	performing incremental synchronization	
<i>Client Enablement Services Client Features</i>		
ONEXCESSERVER-9068	User unable to remove/add contacts to the VIP/FAV and received a voicemail when registration 1XM 6.1.4 (Android) through 1XCES 6.2.	Workaround: Exit 1XM app then re-login. It is highly recommended to upgrade your 1XM to 6.2 SP1 if possible.
ONEXCESSERVER-8247	Call logs: Call durations are not consistent between calling and called parties.	None.
NA	Messaging – VM of length up to 7 minutes supported and could be downloaded and played on mobile client	None.
NA	Messaging – Mobile users can have maximum of 15 voice messages available on their mobile application.	Delete displayed voice messages to see other VMs in the queue.
NA	Call Handling – DTMF Prompt on client sounds like a dial tone	When DTMF is enabled for an end user on the Client Enablement Services, Communication Manager will prompt the user with a dial tone. User to press a key for confirmed answer of inbound or callback calls.
NA	Call Handling – Extend Call button on the Desk Phone only works if the user has the mobile phone set to ring. Call will not be extended to other Ring Also phones.	Set Mobile Phone to ring for Extend Call feature to work from Desk Phone.
NA	Call Handling – Auto-answer set on the user's extension will not work if the extension is controlled by Client Enablement Services.	None.
NA	Call Handling – Send All Calls (SAC) feature on Desk Phone and Block All Calls (BAC) feature on one-X client are not the same and not in sync. Activating / deactivating SAC would not activate / deactivate BAC and vice-versa.	It is recommended that user use Avaya Communicator to activate / deactivate Block All Calls and not use SAC feature on Desk Phone for sending incoming calls to coverage.
ONEXCESSERVER-6415	Callback – In the event of the user being a SIP endpoint, the user has to accept the call at the desk-phone to complete a callback call if the origination point of the call is selected as the desk-phone	Upgrade the firmware on the SIP Hard-Phone that is being used as the desk phone. (Firmware versions 2.6.7.0. and above).
NA	Ring Also / Callback – On-PBX extensions (internal destinations), except own extension, are not supported as Ring Also / Callback origination phones.	None.
NA	Ring Also – Client Enablement Services does not support configurations where two users add the same mobile number as their Ring Also destination.	All users should have unique mobile number as their Ring Also destination.

Known issues and workarounds

Interoperability Issues

Known interoperability issues with Client Enablement Services 6.2.9

Interop Component	Interop Issue ID	Problem	Workaround / Notes
Avaya Aura® Communication Manager 6.3, 6.2, 6.0.1, 5.2.1	defsw103257	No visual or audio alert on the desk phone of a SIP station if it is configured for silent ringing (wi00836407).	This is fixed in CM 6.3 SP4
	defsw111593	Call on Mobile dropped when new number is added in Ring Phones list via the client (wi00879987).	Workaround: Do not edit ring phones while on a call. This would be addressed in future release of Communication Manager.
	ONEXCESSERVER-9835 / defsw140752	Hear both busy tone and ring back tone if Ring My Phone includes Mobile and Mobile is in active call.	This issue happens when CM is connected to PSTN via a SIP signaling with SIP direct media is enabled. Workaround: disable SIP direct media on the SIP signaling group.
	defsw122911	Callback does not work with on-PBX destination	This would be addressed in future release of Communication Manager.
	defsw130872	Enabling AutoExclusion causes call back failure	This would be addressed in future release of Communication Manager.
	defsw130927	calls fail to originate to dest with authcode	This would be addressed in future release of Communication Manager.
	defsw131470 / defsw131637 / defsw131879	CM responds with 403 for SUBSCRIBE from CES	This is fixed in CM 6.3 SP3. Workaround: use direct SIP between CM and CES for earlier versions of CM
	defsw131557	Call drop if user answer callback call on mobile before 4 seconds	This would be addressed in future release of Communication Manager
	ONEXCESSERVER-9770 / ONEXCESSERVER-9784	Two call log entries on 1XCES clients when dialing bridge conference	None.
Presence Services	ONEXCESSERVER-9821	"Away" status is reflected in 1XCES improperly	CES is currently not supporting "away". The "away" is currently mapped to "Unavailable". This will be fixed in future release of CES
Meeting Exchange	ONEXCESSERVER-8967 / wi01105387	When moderator mutes the participant using Bridge UI, the participant is muted but the moderator's Bridge UI is not updated. Then, moderator cannot unmute the participant	This issue happens intermittently. Workaround: participant needs to drop and rejoin the call.
	ONEXCESSERVER-9899	active talker update on Bridge Conferencing UI is not working with MX 6.2	This feature is working for MX 5.2 and AAC 6.0

Interop Component	Interop Issue ID	Problem	Workaround / Notes
Avaya one-X® Mobile SIP	N/A	Call Forward and Call Forward Busy will not function if BAC is activated.	None
	N/A	Call Forward and Call Forward Busy will not function if the call comes in from a non-VIP number.	None
	N/A	If Avaya Communicator has a mobile number configured then EC500 mapping for the same number should not be created on the Avaya Aura® Communication manager. However Avaya Communicator does not have a mobile number configured or the configured mobile number is different from the one that would be used for the SIP iOS client, then the EC500 mapping for the mobile number to be used for Avaya one-X® SIP iOS should be created on the Avaya Aura® Communication manager.	None
	N/A	1. EC500 delay will not work – If Avaya Communicator has a mobile number configured and set to ring, then the user receives two incoming call for every incoming call, one over SIP(VOIP) and the other over GSM. 2. User will not get any incoming call alert on the Avaya one-X® Mobile SIP iOS client, if the deskphone is set for silent ringing.	If the user wants to use both the client for the same user logged in simultaneously then the following configuration should be done on the Avaya one-X® Mobile client – 1. Set Desk Phone Ringer as ON 2. No Also ring number selected to ring whenever the user is logged in with Avaya one-X® Mobile SIP iOS client.
	N/A	Callback call from Avaya Communicator using the deskphone is not supported.	None
Avaya Desktop Video Device	ADVD-4137	Two call entries are getting logged for EC500/Extended calls	None
96x1 SIP	N/A	when the screen saver or the WML Screen saver is displayed on the 96x1 SIP phone, busy/away presence is updated on CES clients	None

Avaya one-X® Client Enablement Services - server issues

Known issues with Client Enablement Services 6.2.9

Issue ID	Problem	Solution/Workaround
Installation / Upgrade		
ONEXCESSERVER-9973	Administrative user name is blank in Preweb LDAP setting when upgrade	Workaround: manually select appropriate administrative user name from dropdown list.
ONEXCESSERVER-9816	Preweb does not check if admin user is in ldap admin security group	Workaround: need to be sure that the admin user is assigned to admin security group in LDAP.
ONEXCESSERVER-9814	Binary Installation Fails if user skips ces admin password	Workaround: make sure you have entered the cesadmin password during the installation process.
ONEXCESSERVER-9640	Enterprise Directory Incremental Synchronization task consumes high CPU resource – Callback and Directory search fails during incremental synchronization.	None.
ONEXCESSERVER-9229	Administrative user does not support non-English name	Workaround: Use English name for administrative user name.
ONEXCESSERVER-9148	Installation fails with Novell Directory on RHEL 6.2 if LDAP security group names are not unique.	Workaround: Security group name must be unique across LDAP tree.
ONEXCESSERVER-9191	Unable access CES admin web if restore database was taken on same release-different build (Take backup database in CES 6.2.0.0.195 build then restore it in CES 6.2.0.0.221 build)	Currently, 1XCES does not support backup/restore database between versions. Backup/restore database must be done via upgrade/migration process.
ONEXCESSERVER-9123	Inaccurate progress bar and time remaining in template installation	None.
ONEXCESSERVER-9823	Mobile clients creates multiple sessions when switching between 3G/EDGE and Wifi	Workaround: The stale connections will automatically be cleared after ~20 minutes.
ONEXCESSERVER-9376	The Corp Dir search results do not get exactly the attributes from LDAP Attribute Mappings.	Workaround: restart 1XCES service then run full directory sync.
ONEXCESSERVER-9160	Can't provision CES users from web admin after fresh install CES 6.2.0.0.219 with AD2k8 on RHEL 6.2	The possible cause is that sync task has not been actually completed. Workaround: After the sync task is reported as completed in Admin web, admin has to sit tight for another 15 minutes and do not do new user provisioning.
ONEXCESSERVER-8178	MM adapter is still shown in connected state when Voice Messaging server is completely stopped.	Workaround: Restarting the MM adapter will get the state reflected correctly.
ONEXCESSERVER-7531	Mobile resource for a user added via admin does not validate the route	Make sure the Mobile number added is routable through CM. Deferred to new release.
ONEXCESSERVER-7110	User part of the Audit group is able to logoff and kill active sessions of a provisioned user.	None.
ONEXCESSERVER-9925	Script to modify port info for LDAP, if customer want to use non-standard port	Workaround: changeLDAP port script is not updating the secure port number in CES admin portal. User need to change port value in Web Admin manually.

Issue ID	Problem	Solution/Workaround
ONEXCESSERVER-10289	Directory search by name does not limit the number of contact attributes to 5 in search result	None.
ONEXCESSERVER-10288	Duplicate enterprise directory contacts will be returned in the search result when using a part of mobile number in 1XM app search criteria	None.
ONEXCESSERVER-10261	Avaya Communicator integrated with CES cannot get presence status after restarting PS server	None.
ONEXCESSERVER-10154	CES server is not presenting "live" voicemail updates for call history after voicemail server had been patched/upgraded.	None
ONEXCESSERVER-10101	After re-run of preweb , configuration values isn't empty	None
ONEXCESSERVER-10417	When changing license configuration no alert shown	None
ONEXCESSERVER-10423	QVMSG00015 is not generated when Incorrect userID/password used for Voice Messaging server	None
ONEXCESSERVER-10363	1XC SIP integrated with CES_Bridge Conference UI displays no active Bridge Conferences screen after moderator uses TUI command to add participant	None
ONEXCESSERVER-10171	Bridge Conference window not update when remove a user who was invited by *1 and *2	None
ONEXCESSERVER-10213	1XC CES mode - when conference is locked, moderator cannot add/invite participants using Conference UI	None
ONEXCESSERVER-10380	Not the full list of history records in 1XC	None
ONEXCESSERVER-10421	Presence status doesn't change at a moment of call if Presence is in "auto-managed" mode	None
ONEXCESSERVER-10099	OneX-C SIP integrated with CES displays 50 calls on the history call after re-login	None
ONEXCESSERVER-10101	After re-run of preweb , configuration values isn't empty	None
ONEXCESSERVER-10398	1XC login issue when CES userid contains special chars	None
ONEXCESSERVER-10105	When audit user tries to change LDAP attributes, wrong message is shown.	None
ONEXCESSERVER-10104	Audit user is able to change search properties	None
ONEXCESSERVER-10421	Presence status doesn't change at a moment of call if Presence is in "auto-managed" mode	None

Issue ID	Problem	Solution/Workaround
ONEXCESSERVER-10294	GRIP: VW Needs SNMPD Agent for discovery	None
ONEXCESSERVER-10276	Admin UI doesn't alert for inactive setting	None
ONEXCESSERVER-10149	1XC SIP CES login automatically changed to previously logged in User	None
ONEXCESSERVER-10179	Blank Call Log displays in 1XC with CES integration after user ends CM conference.	None
ONEXCESSERVER-9994	MDA: Android and OneXC 'Unavailable' status set on Android client - messages delivered on OneXC	None
ONEXCESSERVER-9963	Incorrect mapping of "primaryphone" property.	None
ONEXCESSERVER-10793	Fail to re-enroll SMGR certificate, CES does not re-use existing certificate / keystore.	The certificate was re-enrolled without an issue after password changing.
ONEXCESSERVER-10792	Failed upgrade from 6.2.6.0.21 to 6.2.6.0.25	None
ONEXCESSERVER-10783	Presence note is vanished after PS server upgrade	None
ONEXCESSERVER-10720	Presence still displays the stale status even user has just updated it	Issue does not occur in GSC and SV-Pune lab which uses PS - 7.0.1.0.858.
ONEXCESSERVER-10700	Unable to dial Scopia conference from CES call log history.	Issue was fixed on client side: Carrera 3.0.
ONEXCESSERVER-10693	Duplicate contact is presented at Enterprise search result when user search contact based on partial phone number via CES. Intermittent issue.	None
ONEXCESSERVER-10665	Outgoing call logs generated with incorreccted number when enabling dial rule	Workaround: reconfigure dial plan
ONEXCESSERVER-10631	TE Android 3.0 shows in-correct entry in Call History, when call made to H.323 Extension	None
ONEXCESSERVER-10624	TE iOS 3.0 shows in-correct entry in Call History, when call made to H.323 Extension	None
ONEXCESSERVER-10620	TE iOS 3.0 shows two call log entries for an outgoing call, when call was transferred to another user.	None
ONEXCESSERVER-10595	User CLI import did not retain voicemail passwords.	None
ONEXCESSERVER-10545	1XC SP11-1XC CES Call log shows incorrect call direction for answered call when the user is in call pick up group	None
ONEXCESSERVER-10484	ikeyman utility does not work on Linux install	Solution: Install "xorg-x11-xauth" and "xterm" rpms

Issue ID	Problem	Solution/Workaround
ONEXCESSERVER-10431	CES mobile self-presence is not in sync with desktop client	None
ONEXCESSERVER-10798	presenceIM value is not populated for contacts from additional contact ldap	Populate the same contact in SMGR with some xmpp handles may help to resolve the presentity id of the contact
ONEXCESSERVER-10735	IBM HTTP Server cookie does not have the HTTPOnly and Secure flag set.	These flags have been turned off by default. To enable these flags, go to the opt/avaya/1xp directory and run ./modifyHTTPOnlySecureCookies.sh -e
ONEXCESSERVER-10801	One-X Server Status of station sometimes is set to "trigger" while it should be "normal"	Does not have any impact on the end user, but might increase the traffic between CM and CES
Client features		
ONEXCESSERVER-9889	Unknown/blank call log entry on 1XCES transferee party in unattended call transfer call scenario	None.
ONEXCESSERVER-9766	Call log does not update at end-users if CES SIP Service is failover from SM to CM	None.
ONEXCESSERVER-9475	H.323 CES user has double call logs are generated for a call	Workaround: restart SIP service
ONEXCESSERVER-9380	Priority call does not ring (silent ring) SIP deskphone when called CES user sets "Block All Calls"	None.
ONEXCESSERVER-9214	Callback is not established successfully when deskphone is Other phone mode 1XC	User can set the callback device as other phone instead.
ONEXCESSERVER-10309	Upgrade template does not allow Administrative Account selection	Changing the "objectClass=user" instead of "objectClass=ServiceAccount" resolved the issue
ONEXCESSERVER-10098	Updating extension number in Telephony setting sends incorrect list of device ID's (FA-6043)	None
ONEXCESSERVER-9997	Presence note deleted from AC Android client is not properly updated on AC-Windows client and vice versa.	None
ONEXCESSERVER-10756	Outgoing call log is not shown on Boss when Secretary makes a BLA call for Boss to customer (Equinox 3.1)	Disable CES for BLA if so preferred
ONEXCESSERVER-10910	Error encountered while initializing the page for updating user Telephony resource.	Go back to any other menu option and come back to user view page.

Avaya one-X® Client Enablement Services - client issues

Known issues with one-X® Client Enablement Services release 6.2 – clients SP2 and one-X® Communicator 6.2+

Issue ID	Problem	Solution/Workaround
One-X Communicator		
ONEXC-10020	Many exceptions thrown out in trace.log while logging 1XC (CES mode)	There is no impact in client operation
ONEXC-6667	1xc show login state even when the user is deleted from CES server and the session between CSE and 1xc is gone from the CES server	None.
ONEXC-8593 / ONEXCESSERVER-9384	CES does not return all the matched contacts when doing directory search on 1XC (CES mode)	None.

Known issues when using CES 6.2.x clients with a CES 6.1.x server

The new CES 6.2 clients have features that are not supported by CES 6.1 server. These features are

Features	Descriptions
Call to My Phones / User-selectable BLA handling	Avaya Communicator users can select whether or not to receive their Bridged Line Appearance calls on their mobile client. When a user choses "Primary" in their call settings, then BLA calls will not be sent to their mobile device. Previously, BLA handling was an administrative system-level setting. This feature requires CES 6.2.x server to work. With CES 6.1.x server, changing this setting on Avaya Communicator does nothing.
Jailbroken Device detection and rejection	Avaya Communicator mobile clients look for symptoms typical of jailbroken devices. One-X CES 6.2 can be configured to deny access from devices that fail these tests. CES 6.1.x server will allow access from any device regardless it is jail broken or not.
Device Specific Login	Administrators can now choose an additional factor for authentication by having a user's unique device hardware ID included as part of the authentication process. This Device ID is automatically captured by Avaya Communicator when the user logs in to one-X CES for the first time. Subsequent user login attempts must be made using the registered device, or access will be denied. This feature minimizes the risk of unauthorized network access. CES 6.1.x server does not have ability to store users' Device IDs, and thus allow users to login to their account from any device.
Prevent local storage of contacts info	For security reasons, administrator can now prevent enterprise data, specifically voicemail attachments and corporate contracts, from being downloaded to the mobile device. CES 6.1.x server does not have a setting to prevent contacts info from being downloaded to the mobile device, and thus always allow users to save contacts info in local mobile storage. However, CES 6.1 has a setting to prevent voicemail from being downloaded to the mobile device, but
Flexible LDAP fields	Administrator can now configure CES server to display selective contacts info on mobile device (up to five LDAP attributes). Administrator can also define a "blacklist". For any users added to the corporate directory blacklist, only the entry name will be returned in a corporate directory search. None of contact information will be returned in a corporate directory search. CES 6.1.x server does not have this ability, and thus allow mobile users to see a fixed list of LDAP attributes of every contact.

In addition, there are the following known issues. Avaya recommends upgrading the CES server to the latest version of 6.2 as soon as possible to resolve any incompatibilities with the latest version of the mobile applications.

Issue ID	Problem	Solution/Workaround
<i>Android Clients-</i>		
ONEXCESSERVER-9410	VIP list does not show any VIP contacts after re-launching/re-login to 1XM app	Intermittent
<i>iPhone Clients-</i>		
ONEXCESSERVER-9410	VIP list does not show any VIP contacts after re-launching/re-login to 1XM app	Intermittent

Updates in Administering Guide

Enterprise Directory domains on page 131 and 152

After installing Client Enablement Services since 6.2.4 version, you can modify any information for Enterprise Directory domains (Base DN, Login ID or password). The PSN how to change password in websphere [100172363](#)

Note:

It is not recommended to change the ldap base DN, username, or password, because it requires websphere configuration update. This change will not show up in the pre-web and you will need to re-enter this data on next update. Please contact technical support.

System Manager certificate is not imported after installation on page 306

If the System Manager certificate is not imported after Client Enablement Services installation or if there is any change in the System Manager Host or IP address, CES server may not be able to establish secure connection to Aura servers. In an example, the presence service may be stuck in starting state.

Proposed solution

About this task

Perform the following steps to re-enroll the certificate from System Manager Certificate Authority.

Procedure

1. Ensure that the System Manager host and port details are included in the `/opt/avaya/1xp/config.properties` file.

For example:

```
smgr.host=135.9.2.3  
smgr.port=443
```

2. Reassign the certificate from System Manager.
 - a) In the SSH terminal session on the Client Enablement Services server, log in as root.
 - b) Go to the `/opt/avaya/1xp` directory using the command: `cd /opt/avaya/1xp`
 - c) Renew the certificate using the command: `./run_config_smgr_jython.pl <smgr_enrollment_password>`
 - d) Restart the Client Enablement Services server.
3. Verify whether the System Manager and Presence Services server are reachable by the FQDN. If the servers are not reachable, add entries to `/etc/hosts`.

Running CLI commands on a Linux system on page 179

About this task

Use the command prompt to run the CLI commands. In the command prompt, run the shell script for the CLI commands, and then add the command for the required action. For example, to import users, perform following steps.

Procedure

1. Go to the `/opt/avaya/1xp/1XP_Admin_CLI_Client` directory using the command: `cd /opt/avaya/1xp/1XP_Admin_CLI_Client`
2. In the command prompt, type `./1xpAdmin.sh import users -u /opt/avaya/1xp/<dataexportfilename.csv> -v 6.2`.

In the above command:

- `1xpAdmin.sh` is the shell script for running CLI commands. This script is located in the folder where you have unzipped the `1XP_Admin_CLI_Client.tar` file.
- `/opt/avaya/1xp/<dataexportfilename.csv>` is the location of the file on the server from which you import users.
- `<dataexportfilename.csv>` is the file name of the file that contains user data you want to import.
- `6.2` is the version of the Client Enablement Services system.

3. Press Enter.

The system prompts you to enter your username and password.

4. Enter your `admin_user_name` and the `admin_user_password`.

Enter Login:

Enter Password:

If the operation is successful, the system displays the message: File to import is `/opt/avaya/1xp/<dataexportfilename.csv>`. Operation completed successfully.

If the operation is unsuccessful, the system displays a failure message. Information about the operation is available in the log file `acp_admin_cli.log`.

By default, this log file is created in the

`/opt/IBM/WebSphere/AppServer/profiles/default/logs/acp_admin_cli.log` directory.

Appendix A: Steps to replace default certificate with SMGR CA on CES 6.2.9 (AC connection fix)

Below steps to replace default certificate with SMGR CA on CES 6.2.9 for Avaya Communicator Android and iOS clients to be able to connect:

- 1) Go to directory /opt/avaya/IHS:
./migrate_smgr_ca_key_trust_store_to_ihs.pl
./activate_smgr_ca_certs.pl
- 2) Go to directory /opt/avaya/1xp:
./run_config_httpservers_jython.pl
- 3) Go to directory /opt/avaya/IHS:
./migrate_ihs_keystore_to_handset_server.pl

Once the above-mentioned steps are executed restart 1xp services.
service 1xp restart

Appendix B: Enabling RC4 cipher suite

By default RC4 ciphers are disabled on CES SP9. To enable these ciphers do the following:

- 1) SSH into one-X CES Server from putty.
- 2) Switch to root user. First `craft/craft01` and `su/root01`
- 3) Navigate to `/opt/avaya/1xp`
- 4) Run `./modifyRC4ciphers.sh -e`

Appendix C: Installing Avaya one-X® Client Enablement Services release 6.2.9 with blocked nsuniqueid on SUN LDAP

It is not a default configuration. Installation will be failed. If you want to avoid this issue before installation without executing the script you have to allow admin user to read nsuniqueid field of all users, admins and audits on current LDAP. Otherwise, please use the following instruction to prevent problems with users login:

VSP:

- 1) Start CES VSP installation
- 2) Wait for step "Run post-install plugin if present"
- 3) Login to CES machine via ssh
- 4) Go to /opt/avaya/1xp and start this script (`./force_external_id.sh -id "distinguishedName"`)
- 5) Wait until installation is finished

Appendix D: Steps to replace default 'Logon Attribute' to another LDAP attribute (1XC login fix)

This script is required only after you change your 'Logon Attribute' in CES Web Admin to some other LDAP attribute.

This script is required only when the new 'Logon Attribute' value is not as same as the 'User Id' value or 'e-mail' value. For example, the new 'Logon Attribute' is userPrincipalName = janed@apac.avaya.com, but mail = janed@avaya.com

This script is NOT required for deployments, which do not have 1XC with CES integration.

This script is to add the 'Logon Attribute' to wimconfig.xml file, hence enable 1XC/portal user to login using new 'Logon Attribute'.

Run script in directory /opt/avaya/1xp:

```
./addLoginProperty.sh <LDAP attribute>
```

<LDAP attribute> - LDAP attribute value, which should be used as 'Logon Attribute'

Example of usage: ./addLoginProperty.sh userPrincipalName

Restart the Client Enablement Services server.

```
service 1xp restart
```

Appendix E: Steps to disable the fix for Spectre/Meltdown vulnerability

To disable the fix for Spectre/Meltdown vulnerability, follow these steps:

1. Login on CES via SSH as root
2. Edit `/boot/grub/grub.conf` file.
3. At the end of each line that starts with kernel, add the following flags:
noibrs noibpb nopti
4. Save the file
5. Reboot the CES

Appendix F: Ports for Client Enablement Services Server (eth0)

Source System	Port (Configurable Range)	Destination System	Port (Configurable Range)	Network / Application Protocol	Optionally Enabled / Disabled?	Default port state	Description
CES	Ephemeral	Voice Messaging	25 (C)	TCP/SMTP	Yes	Open	SMTP for sending e-mail and SMS
CES	Ephemeral	Voice Messaging	465 (C)	TCP/SMTP	Yes	Open	SMTP for sending e-mail and SMS
CES	Ephemeral	Voice Messaging	993 (C)	TCPIMAP4	Yes	Open	IMAP for retrieving voicemails and faxes for display, and audio playback for user
CES	Ephemeral	Voice Messaging	389 (C)	TCP/LDAP	Yes	Open	LDAP for Modular Messaging / Avaya Aura® Messaging
CES	Ephemeral	Voice Messaging	636 (C)	TCP/LDAPS	Yes	Open	LDAP for Modular Messaging / Avaya Aura® Messaging
CES	Ephemeral	Conferencing	2000	TCP/BCAPI	Yes	Open	Protocol for communicating with Meeting Exchange
CES	Ephemeral	Conferencing	2002	TCP/BCAPI	Yes	Open	Protocol for communicating with Meeting Exchange
CES	Ephemeral	Conferencing	5040 with auto-increment	TCP/BCAPI	Yes	Open	Protocol for communicating with Meeting Exchange
CES	Ephemeral	Conferencing	5040 with auto-increment	UDP/BCAPI	Yes	Open	Protocol for communicating with Meeting Exchange
CES	Ephemeral	Presence	5061 (C)	TCP/SIPS	Yes	Open	Presence updates for a contact
CES	Ephemeral	Presence	12009 (C)	TCP/RMI	Yes	Open	Presence updates for a contact
CES	Ephemeral	Presence	7000 (C)	TCP/LPS	Yes	Open	Communication between CES PS Lookup Server (LUS).
Presence	Ephemeral	CES	9070 (C)	TCP/LPS	Yes	Open	Presence updates for a contact (LPS Supplier)
Presence	Ephemeral	CES	9072 (C)	TCP/LPS	Yes	Open	Presence updates for a contact (LPS Consumer)
CES	Ephemeral	SMGR	1399	TCP/RMI	Yes	Open	RMI Name Service
CES	Ephemeral	SMGR	1398	TCP/RMI	Yes	Open	JNDI Name Service
CES	Ephemeral	SMGR	3873	TCP/RMI	Yes	Open	EJB3 Remoting Connector
CES	Ephemeral	WebLM	8443 (C)	TCP/HTTPS	Yes	Open	Communication with Avaya Licensing when WebLM on local CDOM
CES	Ephemeral	WebLM	52233 (C)	TCP/HTTPS	Yes	Open	Communication with Avaya Licensing when WebLM SMGR
CES	Ephemeral	Enterprise Directory	389 (C)	TCP / LDAP	No	Open	Enterprise contacts and Authentication/Authorization
CES	Ephemeral	Enterprise Directory	636 (C)	TCP / LDAPS	No	Open	Enterprise contacts and Authentication/Authorization
Admin Web Browse, 1xC, SAL GW	Ephemeral	CES	443	TCP / HTTPS	No	Open	Communication with Administration Client and 1xC soft phone
Web Browser	Ephemeral	CES	9043	TCP/HTTPS	No	Open	WAS's IBM Console
SSH client and SAL GW	Ephemeral	CES	22	TCP / SSH	No	Open	Maintenance
CES	Ephemeral	SAL Gateway and/or NMS	162	UDP/SNMP	Yes	Open	SNMP Traps
CES	Ephemeral	System Manager	443	TCP/SCEP	No	Open	Certificate Trust Management

Source System	Port (Configurable Range)	Destination System	Port (Configurable Range)	Network / Application Protocol	Optionally Enabled / Disabled?	Default port state	Description
Handset Server	Ephemeral	CES	8888 (C)	TCP/TLS	No	Open	1xM binary protocol forwarded from Handset Server
1xMobile devices	Ephemeral	CES	7777 (C)	TCP/TLS	No	Open	1xM binary protocol between public internet and the local Handset Server
SM or CM	Ephemeral	CES	5060 (C)	TCP/SIP	Yes	Open	Communication with Session Manager or Communication Manager
SM or CM	Ephemeral	CES	5061 (C)	TCP/SIPS	Yes	Open	Communication with Session Manager or Communication Manager
CES	Ephemeral	SM or CM	5060 (C)	TCP/SIP	Yes	Open	Communication with Session Manager or Communication Manager
CES	Ephemeral	SM or CM	5061 (C)	TCP/SIPS	Yes	Open	Communication with Session Manager or Communication Manager
Linux command line	Ephemeral	CES	8880	TCP/SOAP	No	Open	SOAP connector port. This interface can be run remotely, but is mostly intra-Client Enablement Services communication (in which case doesn't leave an individual Client Enablement Services – does not have to be configured on external firewall)
NA	Ephemeral	CES	8090 (C)	TCP	No	Open	Intra-Client Enablement Services communication (doesn't leave an individual Client Enablement Services – does not have to be configured on external firewall) WAS connection to internal Audio Transcoding Service
NA	Ephemeral	CES	9443	TCP/HTTPS	No	Open	Intra-Client Enablement Services communication (doesn't leave an individual Client Enablement Services – does not have to be configured on external firewall) HTTPS traffic forwarded from internal IHS to WAS
NA	Ephemeral	CES	523	TCP	No	Open	Intra-Client Enablement Services communication (doesn't leave an individual Client Enablement Services – does not have to be configured on external firewall). DB2 Admin
NA	Ephemeral	CES	50000	TCP	No	Open	Intra-Client Enablement Services communication (doesn't leave an individual Client Enablement Services – does not have to be configured on external firewall). DB2

Source System	Port (Configurable Range)	Destination System	Port (Configurable Range)	Network / Application Protocol	Optionally Enabled / Disabled?	Default port state	Description
NA	Ephemeral	CES	2809	TCP	No	Open	Intra-Client Enablement Services communication (doesn't leave an individual Client Enablement Services – does not have to be configured on external firewall). Bootstrap port
NA	Ephemeral	CES	9402	TCP	No	Open	Intra-Client Enablement Services communication (doesn't leave an individual Client Enablement Services – does not have to be configured on external firewall). CSIV2 client authentication listener port.
NA	Ephemeral	CES	9353	TCP	No	Open	Intra-Client Enablement Services communication (doesn't leave an individual Client Enablement Services – does not have to be configured on external firewall). High availability manager communication port.
NA	Ephemeral	CES	5557	TCP	No	Open	Intra-Client Enablement Services communication (doesn't leave an individual Client Enablement Services – does not have to be configured on external firewall). Internal JMS server port.
NA	Ephemeral	CES	5578	TCP	No	Open	Intra-Client Enablement Services communication (doesn't leave an individual Client Enablement Services – does not have to be configured on external firewall). MQ transport secure port.
NA	Ephemeral	CES	9100	TCP	No	Open	Intra-Client Enablement Services communication (doesn't leave an individual Client Enablement Services – does not have to be configured on external firewall). ORB listener port.
NA	Ephemeral	CES	9401	TCP	No	Open	Intra-Client Enablement Services communication (doesn't leave an individual Client Enablement Services – does not have to be configured on external firewall). SAS SSL SERVERAUTHLISTENER ADDRESS
NA	Ephemeral	CES	7276	TCP	No	Open	Intra-Client Enablement Services communication (doesn't leave an individual Client Enablement Services – does not have to be configured on external firewall). Service integration port.

Source System	Port (Configurable Range)	Destination System	Port (Configurable Range)	Network / Application Protocol	Optionally Enabled / Disabled?	Default port state	Description
NA	Ephemeral	CES	7286	TCP	No	Open	Intra-Client Enablement Services communication (doesn't leave an individual Client Enablement Services – does not have to be configured on external firewall). Service integration secure port.
NA	Ephemeral	CES	8008	TCP/HTTPS	No	Open	Intra-Client Enablement Services communication (doesn't leave an individual Client Enablement Services – does not have to be configured on external firewall). IHS configuration from WAS

Appendix G: Acronyms

HS	Handset Server
1XM	Avaya one-X Mobile client
1XC	Avaya one-X Communicator client
1XP	Avaya one-X Portal client
1XCES/one-X CES	Avaya one-X Client Enablement Services
CM	Avaya Aura Communication Manager
CMM	Avaya Aura Communication Manager Messaging
SMGR	Avaya Aura System Manger
AES	Avaya Application Enablement Server
PS	Avaya Aura Presence Services
SP	Service Pack
AD	Microsoft Active Directory
ADAM	Microsoft Active Directory Application Mode
AD LDS	Microsoft Active Directory Lightweight Directory Services