Avaya one-X® Client Enablement Services
Service Pack Release 6.2.4
Release Notes

Issue 1.0
19th August, 2015

© 2015 Avaya Inc. All Rights Reserved.

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 ANAUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA R ESELLER. 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 OTHERSTO 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.

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

CE

Avaya Inc. declares that the equipment specified in this document bearing the "CE" (Conformité Europeénne) 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 8

- PS 7.x Configuration Details:- 8

Fixed issues 10

Following issues are fixed in Avaya one-X® Client Enablement Services release 6.2.4 10

Avaya one-X® Client Enablement Services Server Fixes 10

Deploying Avaya one-X® Client Enablement Services release 6.2.4 14

Obtaining Avaya one-X® Client Enablement Services release 6.2.4 14

Installing Avaya one-X® Client Enablement Services release 6.2.4 17

Installing Avaya one-X® Client Enablement Services release 6.2.4 on System Platform 17

Installing Avaya one-X® Client Enablement Services release 6.2.4 on RHEL 17

Upgrading Avaya one-X® Client Enablement Services release 6.2.4 18

Upgrading Avaya Aura System Platform from 6.0 (6.0.3.9.3) to 6.2 (6.2.2.09001.0) 18

Upgrading Avaya one-X® Client Enablement Services from 6.2 (build 6.2.0.0.237) to 6.2.4 (build 6.2.4.0.97) on System Platform 19

Upgrading Avaya one-X® Client Enablement Services from 6.2.x to 6.2.4 on System Platform 6.2.2.09001.0 19

Upgrading Avaya one-X® Client Enablement Services from 6.2.x to 6.2.4 on RHEL 6.2+ 19

Troubleshooting – Reverting to the previous release of software after an upgrade 20

Migrating Avaya one-X® Client Enablement Services from 6.2.x on System Platform 6.2.2.09001 to 6.2.4 on RHEL 6.2+ 20

Migration process for the presence services from existing PS to PS 7.0 21

Upgrading Handset Server on Standalone machine from 6.1 SP3 build to 6.2.4 build 21

Upgrading Handset Server on Standalone machine from 6.2 build to 6.2.4 build 22

Obtaining Avaya one-X® Client Enablement Services release 6.2 – Clients Software 23

Interoperability and requirements 23

Software and firmware compatibility matrix 23

Hardware compatibility 24

Tested Environment 24

Unsupported Configurations 26

General issues and workarounds 26

Known issues and workarounds 29

Interoperability Issues 29
Avaya one-X® Client Enablement Services - server issues 32
Avaya one-X® Client Enablement Services - client issues 36
Known issues when using CES 6.2.x clients with a CES 6.1.x server 37
Appendix A: Steps to replace default certificate with SMGR CA on CES 6.2.4 (AC connection fix) 38
Appendix B: The following can be done on the CES Server to disable the RC4 cipher suite: 39
Appendix C: Acronyms 40

What's new in Release 6.2

- Support various RHEL versions from version 6.2 up to version 6.5.
- Update to WAS 8.5.5.4, DB2 9.7.0.9 and IHS 8.5.5.4.
- Support multiple LPS versions which mean support various versions of Presence Services. 6.1.5 | 6.2.0 | 6.2.1 | 6.2.2 | 6.2.3 | 6.2.4 | 6.2.6 |7.0.0.
- Support modifying Enterprise Directory information without reinstalling the server. This is in conjunction with PSN003998u.
- LDAP attribute mapping includes new Presence IM Address field, blank by default. One-X Communicator next release is required to work with this.



- This release contains a number of fixes including a fix against POODLE (Padding Oracle On Downgraded Legacy Encryption CVE-2014-3566) vulnerability for IBM WebSphere, which by default disables vulnerable protocol SSL v3.0. All secure connections with CES now are using TLS protocol, which is not affected by this vulnerability. No ports or security settings are needed to be changed here. **Thus, it is necessary to make sure that all third-party servers, which connect to CES (e.g. LDAP), support TLS (minimum required version - 1.0).** This will **not disable SSL v3.0 on other servers, so protecting them from POODLE vulnerability remains server owner responsibility.**

- **PS 7.x Configuration Details:-**

Name	Description
Type	The type of server configured on the system. For the Presence Services, the system displays *ps*.
Version	The version of the server configured on the system.
Handle	The unique name assigned to the server by the administrator.
Description	A short description of the server that uniquely identifies the presence server.
Enabled	If selected, enables the presence server.
PS Data Grid Lookup Server (LUS) IP Address Optional	Optional IP address for the second instance of PS Lookup Server (LUS). PS datagrid LUS configuration can have maximum two locator's services. Leave optional configuration empty if you have only one LUS server.
PS Data Grid Lookup Server (LUS) Port Optional	Communication port between Client Enablement Services and second instance of PS Lookup Server (LUS). 7000 is the default port.
PS Data Grid Lookup Server (LUS) IP Address	The network host address of PS Lookup Server (LUS). It can be defined either as FQDN (fully qualified domain name), or as an IP address. Find out LUS information of PS on SMGR EM (Collaboration Environment→Cluster Administration→Show→<*Server Name*>→Management Network Interface→FQDN or IP Address).
PS Data Grid Lookup Server (LUS) Port	Communication port between Client Enablement Services and PS Lookup Server (LUS).

	7000 is the default port.
OK or Save	OK used on Add/Create pages saves the new resource. Save used on Modify pages saves updates to the resource.
Reset	On Modify/Update pages, restores the form values back to the last successful save. On Add/Create pages, restores the form back to the default or blank values.
Cancel	Exits the page without making any additions or changes.
Delete	Removes the server from Client Enablement Services.

Fixed issues

Following issues are fixed in Avaya one-X® Client Enablement Services release 6.2.4

Avaya one-X® Client Enablement Services Server Fixes

Issue ID	Issue Description	Notes\Comments
ONEXCESSERVER-10390	WAS application version info is invalid in CES Admin (System-<General tab)	Fixed
ONEXCESSERVER-10387	Procedure to change presence server details to Aura 7.0 PS is not acceptable	Fixed \ Executing backup script removes all provisioned users and for (4k) it takes approximately 5 hours. Executing restore script provision all users and for (4k) and it takes approximately 1 hour.
ONEXCESSERVER-10371	Port 443 issue after updating CES default certificate with SMGR CA cert	Fixed
ONEXCESSERVER-10359	One-X Communicator not able to login to One-X CES server	Fixed
ONEXCESSERVER-10329	Scripts referring to gsk7cmd command stop working in CES 6.2.4	Fixed
ONEXCESSERVER-10293	VW needs MIBs for SNMP	Fixed
ONEXCESSERVER-10259	1XM user not able to login after update LDAP attribute mapping	Fixed
ONEXCESSERVER-10215	VM adapter not working properly due to new mail.jar in WAS 8.5.5	Fixed
ONEXCESSERVER-10208	Can't change or see presence status	Fixed
ONEXCESSERVER-10156	Offline activity PS publish format changed	Fixed
ONEXCESSERVER-10068	Admin CLI: Import users, creating/updating resource failed.	Fixed
ONEXCESSERVER-10030	Proper DNS does not get highlighted in resolv.conf after installation	Fixed
ONEXCESSERVER-10018	When user trying to make call from 1XM it gets an error as “Mobile resource not enabled for the user"	Fixed
ONEXCESSERVER-10017	Duplicate call records in all clients for every call	Fixed
ONEXCESSERVER-10016	Internal API exception when updating ldap fields in Web Admin(IBM Domino)	Fixed
ONEXCESSERVER-10011	Shellshock Bash Security Flaw Fix in CES SP template	Fixed

ONEXCESSERVER-9972	Allow user to modify the ldap referral setting during CES upgrade	Fixed
ONEXCESSERVER-9951	Update preweb for AD case to bind user name as it is done for other LDAP types	Fixed
ONEXCESSERVER-9946	Websphere 8.5	Fixed
ONEXCESSERVER-9896	run_config_firewall.pl does not allow required port for MX and PS integration	Fixed
ONEXCESSERVER-9837	Upgrade script failed with /tmp directory mount with "noexec" flag	Fixed
ONEXCESSERVER-9834	Device ID should not be updated while Lost and Stolen is still enabled	Fixed
ONEXCESSERVER-9822	After DB restore 75% of Provisioned user are disabled but shows enabled on admin page	Fixed
ONEXCESSERVER-9819	Customer should be able to modify any information for Enterprise Directory in Web Admin and Upgrade pre-web	Fixed
ONEXCESSERVER-9790	Stop Exposing IBM Console to customer	Fixed
ONEXCESSERVER-9709	CES allows adding non-routable mobile number on Admin Screen	Fixed
ONEXCESSERVER-9691	Warn user when modifying ldap base dn, username, or password	Fixed
ONEXCESSERVER-9683	Allow installer to specify "follow referral" during ldap configuration	Fixed
ONEXCESSERVER-9170	TLS connection succeeds even if SIP Local Server is configured for TCP	Fixed
ONEXCESSERVER-9911	Call log updates incorrectly on 1xM when user makes conference call for three participants(A,B,C) using Avaya desk phones.	Fixed
ONEXCESSERVER-9908	CES performance is poor with admin GUI and ldap searches	Fixed

ONEXCESSERVER-10369	AC connection issue to CES	Fixed
ONEXCESSERVER-10266	Corp Dir Searches from 1XC takes over 2 minutes to display	Fixed
ONEXCESSERVER-10265	1XM on iPhone - Some or all Favorites are sometimes gone	Fixed
ONEXCESSERVER-10257	Call duration shows blank on 1XM app for conference	Fixed
ONEXCESSERVER-10182	Can't import user list as relayed in 1XCES 6.2.3 Administrative guide	Fixed
ONEXCESSERVER-10143	Users are unable to do a search in oneX-mobile using a contacts full name	
ONEXCESSERVER-10142	Users are unable to do a search in oneX-communicator using a contacts full name	
ONEXCESSERVER-10138	Disable SSLv3 to guard against POODLE vulnerability	
ONEXCESSERVER-10037	Support for APS 7.0 on CE	
ONEXCESSERVER-10006	Update Blackduck	
ONEXCESSERVER-9962	ADAM issue: Issue with applying LDAP configuration while installing CES 6.2.3 template	
ONEXCESSERVER-9961	Split domain issue: WebSphere services not working properly after upgrade from 6.2.0.0.237 to 6.2 SP3	
ONEXCESSERVER-9957	"No Voicemail resource administered for this user" messages pop up comes way too many times on the mobile app	

ONEXCESSERVER-9907	Voicemail from internal extensions are showing up as "Unknown" in OneXMobile	
ONEXCESSERVER-9101	FAV/VIP and History do not display the Address value in contact details	
ONEXCESSERVER-9585	New-Years Security Escalation (2048-bit keys and SHA-256 digest) - Verify connections to other Aura products that present 2048-bit/SHA-256 certificates work properly	
Security		
ONEXCESSERVER-10180	Poodle fix - Fix Handset Services module to accept TLS connections	Fixed
ONEXCESSERVER-10010	Fix for Shellshock Bash Security Flaw	Fixed
ONEXCESSERVER-9998	PSST : [RHSA-2014:1306-01] Critical: bash security and bug fix update	Fixed
ONEXCESSERVER-10271	PSST :[RHSA-2015:0707-01] Moderate: qpid security and bug fix update	Fixed
ONEXCESSERVER-10270	PSST :[RHSA-2015:0700-01] Moderate: unzip security update	Fixed
ONEXCESSERVER-10269	PSST :[RHSA-2015:0696-01] Important: freetype security update	Fixed
ONEXCESSERVER-10251	PSST :[RHSA-2015:0674-01] Important: kernel security and bug fix update	Fixed
ONEXCESSERVER-10250	PSST :[RHSA-2015:0672-01] Moderate: bind security update	Fixed
ONEXCESSERVER-10249	PSST :openssl security update (CVE-2014-3570, CVE-2014-3571, CVE-2014-8275, CVE-2015-0204)	Fixed

Deploying Avaya one-X® Client Enablement Services release 6.2.4

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.
Important points for Fresh install on SP-

1. Take existing template backup from CDOM of current system and store it remotely. This is to be used in case the new configuration / user migration fails or has issues.
2. Backup 1xCES database and store remotely.
3. Backup IHS and HSS keystores which contain third party (ie: VeriSign) certificates and store remotely.
4. Take screen shots of CES web admin configuration for reference when re-configuring post fresh install.
5. Export users accounts (with Mobile, VM Extension and Conferencing data) from CES using the steps mentioned in Admin guide.
6. Export Dial Plan.
7. Export Avaya System Configuration (CM, Messaging, Conferencing, Presence).
8. Remove the current template from CDOM.
9. Restart the system from SP CDOM.
10. Copy the new build files on system.
11. Start **fresh install** from SP CDOM.
12. Run Enterprise Sync on the CES web admin.
13. Configure the CES system exactly the way it was on the old system – make sure the handles of the servers (adapters) match exactly the way it was before. Use screen shots taken above. Reconfigure Avaya System components (CM, Messaging, Conferencing, Presence)
14. Restore the keystores.
15. Import dial plan.
16. Import the user Accounts (Mobile, VM Extension, Conferencing) once CES is installed using the steps mentioned in Admin guide.

Obtaining Avaya one-X® Client Enablement Services release 6.2.4

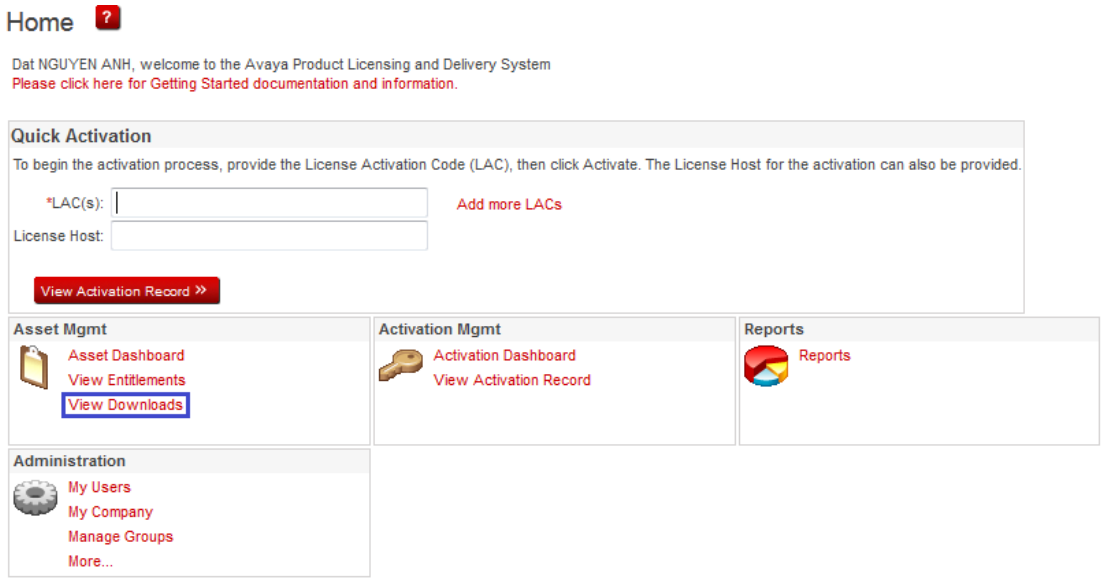
Customers can find the one-X® Client Enablement Services release 6.2.4 files at Avaya PLDS https://plds.avaya.com. The download IDs are as following

- The Client Enablement Services Release 6.2.4 template:
    1. 1XCES000142 [Avaya one-X Client Enablement Services R6.2.4 (file 1 of 4) oneXCES_6231.taraa]
    2. 1XCES000143 [Avaya one-X Client Enablement Services R6.2.4 (file 2 of 4) oneXCES_6231.tarab]
    3. 1XCES000144 [Avaya one-X Client Enablement Services R6.2.4 (file 3 of 4) oneXCES_6231.tarac]
    4. 1XCES000145 [Avaya one-X Client Enablement Services R6.2.4 (file 4 of 4) oneXCES_6231.tarad]
- Client Enablement Services Release 6.2.4 for RHEL build: 1XCES000140 [Avaya one-X Client Enablement Services R6.2.4 RHEL Installer onexces.bin]

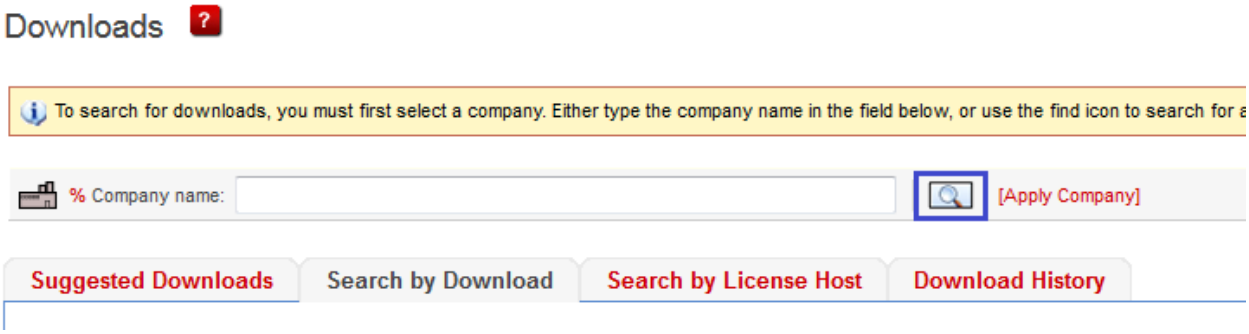
- Standalone Handset Server installer: 1XCES000141 [Avaya one-X Client Enablement Services R6.2.4 Handset Server RHServer.bin]
- Migration utility for deployment on RHEL: 1XCES000146 [Avaya one-X Client Enablement Services R6.2.4 Migration Utility onexces_migrator.bin]

Followings are steps to download the files from Avaya PLDS

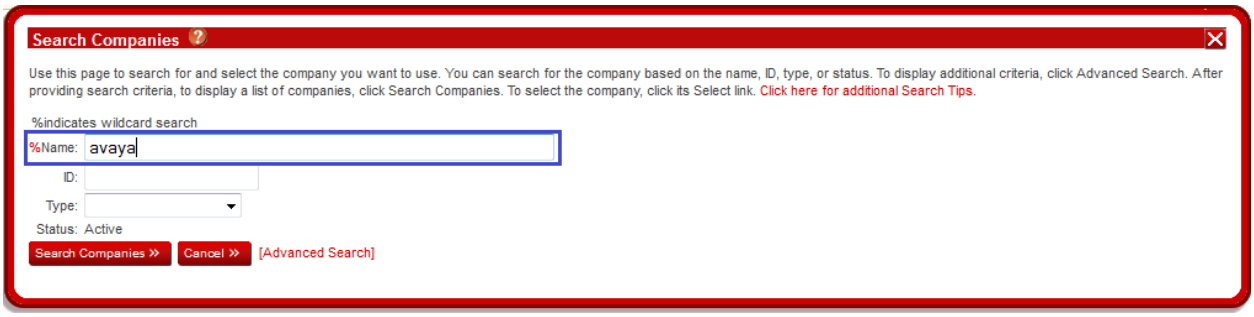
1. Login with the Avaya handle.
2. Select View Downloads as below screenshot



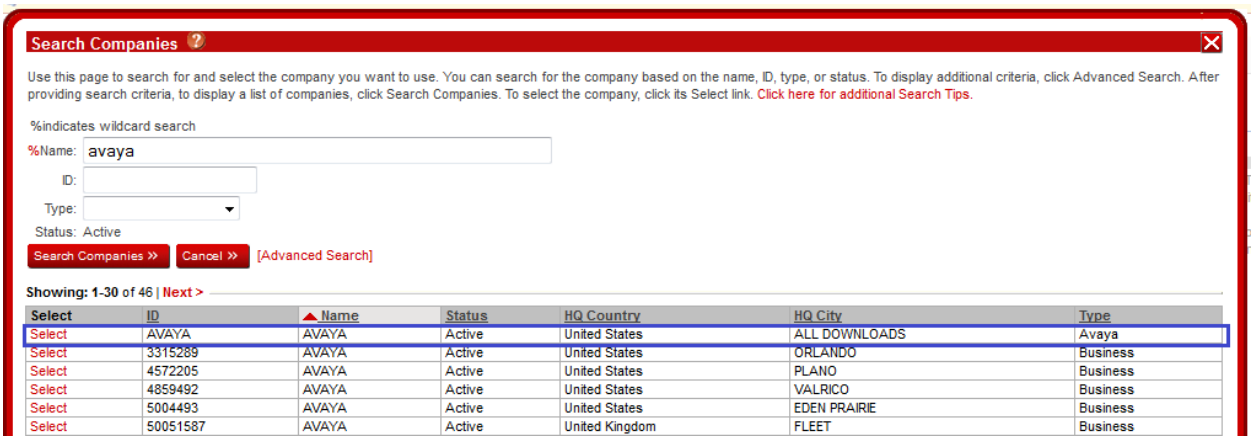
3. Click Search button as below screenshot



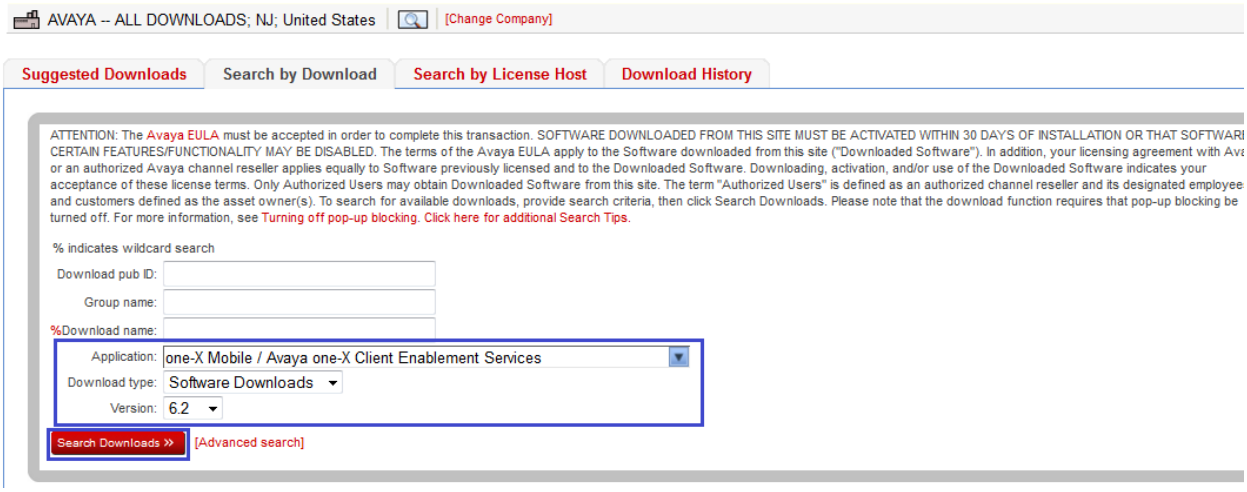
4. Enter “avaya” as search string, then click Search Companies as below screenshot



5. Click Select on the highlighted item below



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



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 SP template installation
   - Copy the <downloaded> .tar files at location /vsp-template/ of CDOM on your System Platform machine that hosts the Client Enablement Services server.
   - Log in the SSH terminal of CDOM and make sure adequate (more than 16GB) disk space is available on mount **/vsp-template**. Use the **df -h** command to check space availability. You can delete the tar files and extracted files of previous build to regain disk space.
   - Extract or untar the template files of 6.2.4 from the location /vsp-template/ using the command:
     # cat oneXCES_624.tara* | (tar x)
   - This creates the following files into a directory labeled with the version that you have downloaded, example: /vsp-template/6.2.4
     - backup_onexps.sh
     - onexps_template.mf
     - restore_onexps.sh
     - lv_rhel.img.gz
     - patchplugin_onexps.sh
     - versioninfo_onexps.sh
     - onexps_template_16GB.ovf
     - post_install.sh
     - onexps_template_24GB.ovf

        - preweb.war
    - The .tar files can be deleted to free up the disk space.

9. For software only installation on RHEL 6.2+, copy the downloaded onexces.bin file at /opt on your RHEL machine that hosts the Client Enablement Services server.

Installing Avaya one-X® Client Enablement Services release 6.2.4

Important Notes:

1. Make sure you have NTP server configured, up and running. This is required for Avaya one-X® Client Enablement Services release 6.2.4 deployment.
2. Make sure CDOM has enough disk space of at least 10GB before start installing 1xCES.
3. Make sure SMGR SSL certificate is not expired.

Installing Avaya one-X® Client Enablement Services release 6.2.4 on System Platform

Avaya one-X® Client Enablement Services Release 6.2.4 can be directly installed on a new system platform version 6.2.2.09001.0 or 6.3.1.08002.0 or 6.3.7. It does not need any prior release of Avaya one-X® Client Enablement Services 6.X to be present. This installation takes around 75-90 minutes to complete.

Follow the *Implementing Avaya one-X® Client Enablement Services* guide at https://downloads.avaya.com/css/P8/documents/100173256 for detailed instructions on installing the Client Enablement Services Server.

Note: It is recommended to wait about 15-20 minutes after installation is successful before doing any administration or database synchronization.

Installing Avaya one-X® Client Enablement Services release 6.2.4 on RHEL

Avaya one-X® Client Enablement Services Release 6.2.4 can be installed on RHEL 6.2+. This installation takes around 40-50 minutes to complete.

Follow the “Implementing Avaya one-X® Client Enablement Services guide at https://downloads.avaya.com/css/P8/documents/100173256 for detailed instructions on installing the Client Enablement Services Server.

Notes:

- After the CES installation and a subsequent mandatory host reboot, the ‘root’ user will no longer be able to login to the host via SSH
- It is recommended to wait about 15-20 minutes after installation is successful before doing any administration or database synchronization.

Upgrading Avaya one-X® Client Enablement Services release 6.2.4

Important Notes:

- *The Client Enablement Services release 6.2.4 can be upgraded from release 6.2.*
- *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.*
- *It is possible to roll back the upgrade on System Platform deployment, but it is not 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 6.2+*** for more details.
- *After upgrading System Platform 6.0.3 to System Platform 6.2.1.0.9, vsp-patch 6.2.2.09001 must be installed.*
- *It is recommended to wait about 15-20 minutes after upgrade is successful before doing any administration or database synchronization.*
- *It is assumed that the Aura Setup is upgraded first before upgrading the CES 6.2.4.*
- *With the upgraded Aura setup the CES should work fine except for presence services.*
- *Follow the process mentioned in "migration process for the presence services from existing PS to PS 7.0" to make presence services work.*

Upgrading Avaya Aura System Platform from 6.0 (6.0.3.9.3) to 6.2 (6.2.2.09001.0)

Follow the procedure below to upgrade the System Platform on Avaya Common Server R1 (Dell PE R610 or HP DL360 G7). This upgrade takes around 30–40 minutes to complete.

Note:

- It is possible to roll back the upgrade before committing the upgrade.
- You can also enable SVM during the System Platform upgrade.
- Once SVM 1.0 is enabled on System Platform 6.2, you can also upgrade SVM 1.0 to SVM 2.0.

Steps

1. From the web console of the CDOM go to: Server Management > Backup / Restore > Backup and Select the Backup Now option.
2. Select the Backup Now button.
3. From the web console of the CDOM go to: Server Management > Platform Upgrade.
4. Select location where your System Platform 6.2.1.0.9 release located then click Upgrade.
5. Select the appropriate .ovf file.
6. Click OK when prompted to confirm that the template has been qualified for the platform version to which you are upgrading.
7. Click OK when prompted to confirm the upgrade.
8. Click Commit to finalize the upgrade process.
9. From the web console of the CDOM go to: Server Management > Patch Management > Download/Upload.
10. Upload and Install System Platform patch vsp-patch-6.2.2.09001.0.noarch.rpm
11. The server will be automatically restarted.

Upgrading Avaya one-X® Client Enablement Services from 6.2 (build 6.2.0.0.237) to 6.2.4 (build 6.2.4.0.97) on System Platform

If the 6.2 release of the Client Enablement Services is pre-installed on the system, it can be upgraded to release 6.2.4. Before upgrading Avaya one-X® Client Enablement Services from 6.2(build 6.2.0.0.237) to 6.2.4 (build 6.2.4.0.97), you must upgrade Avaya Aura System Platform from 6.0 to 6.2. This upgrade will take around 60–75 minutes to complete. Follow the *Implementing Avaya one-X® Client Enablement Services* guide at https://downloads.avaya.com/css/P8/documents/100173256 for detailed instructions on upgrading the Client Enablement Services Server.

Upgrading Avaya one-X® Client Enablement Services from 6.2.x to 6.2.4 on System Platform 6.2.2.09001.0

If the previous build of 6.2 releases of Client Enablement Services is pre-installed on the system, it can be upgraded to latest load of release 6.2.4. Follow the same procedure in ***Upgrading Avaya one-X® Client Enablement Services from 6.2 (build 6.2.0.0.237) to 6.2.4 (build 6.2.4.0.97) on System Platform*** to upgrade the Client Enablement Services server. This upgrade will take 60–75 minutes to complete.

Upgrading Avaya one-X® Client Enablement Services from 6.2.x to 6.2.4 on RHEL 6.2+

If the previous build of 6.2 releases of Client Enablement Services is pre-installed on the system, it can be upgraded to latest load of release 6.2.4. Follow the *Implementing Avaya one-X® Client Enablement Services* guide at https://downloads.avaya.com/css/P8/documents/100173256 for detailed instructions on upgrading the Client Enablement Services Server.

Important Notes:

- It is not possible to rollback the upgrade with RHEL 6.2+ deployment if something goes wrong. Please refer to ***Downgrade Avaya one-X® Client Enablement Services to previous 6.2 build on RHEL 6.2+*** for procedure to downgrade Client Enablement Services to the version that you were using before the upgrade.
- If you have third party certificate(s) installed in IBM HTTP Server and Handset Services, you must backup the keystores and put the keystores in safe place before upgrading the server.
  The files you need to backup (and then restore post upgrade) are
  - /opt/IBM/HTTPServer/ihsserverkey.kdb
  - /opt/IBM/HTTPServer/ihsserverkey.rdb
  - /opt/IBM/HTTPServer/ihsserverkey.sth
  - /opt/IBM/WebSphere/AppServer/lib/ext/keystore.jks
- After restoring the keystore files, you will need to activate the IBM HTTP Server certificate using script "/opt/avaya/IHS/activate_3rdparty_certs.pl", re-import the IHS certificate in 1XCES WebSphere server using script "/opt/avaya/1xp/run_config_httpservers_jython.pl" and restart 1XCES using "service 1xp restart"

```
# cd /opt/avaya/IHS/
# ./activate_3rdparty_certs.pl
# cd /opt/avaya/1xp
# ./run_config_httpservers_jython.pl
# service 1xp restart
```

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.

Migrating Avaya one-X® Client Enablement Services from 6.2.x on System Platform 6.2.2.09001 to 6.2.4 on RHEL 6.2+

If the 6.2 release of Client Enablement Services is pre-installed on a System Platform 6.2 system, there will be an option to migrate the Client Enablement Services release 6.2 databases on System Platform 6.2 to Client Enablement Services release 6.2.4 on RHEL 6.2+.

Follow the *Implementing Avaya one-X® Client Enablement Services* guide at https://downloads.avaya.com/css/P8/documents/100173256 for

- Procedure to install the migration utility on CES 6.2 server.
- Procedure to backup the CES 6.2 data using migration utility.
- Procedure to install backup database during ***Installing Avaya one-X® Client Enablement Services release 6.2.4 on RHEL***

Migration process for the presence services from existing PS to PS 7.0

Follow the below mentioned steps to migrate PS from earlier release to PS 7.0 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) Run the script using "-backup" option. Script execution takes some time... Script is doing user export. Stopping IHS and Handset Service. Disabling and Unprovisioning all users. And start stopped services back. Stop of services required to kill all user sessions.
    ./moveToPS70.sh –u <CESADMIN> -p <PASSWORD> -backup
4) When script execution finished Stop Presence Service manually from Web Admin>Monitoring>Presence
5) From Web Admin>Servers>Presence
    a.Check the name (handle) of presence adapter created. Save it somewhere.
    b.Delete old presence adapter.
    c.Create new one of version 7.0.0 with the same handle!
    d.Check adapter is able to connect PS 7.0
6) Run the script again using "-restore" option. Script execution takes less time… Script is doing user import from backup file.
    ./moveToPS70.sh –u <CESADMIN> -p <PASSWORD> -restore
7) Once script execution finished – you are done. Check that users are in provisioned list and have presence resource as before you start.

Notes:-
Executing the script with backup option, removes all provisioned users and it takes approximately 5 hours for 4k users.
Executing the script with restore option, provision all users and it took 1 hour for 4k users.
This instruction can also be applied for 6.2.0.-6.2.5 adapters i.e. if you upgraded CES but still using PS 6.2.2, you will need to follow same procedure to configure correct PS adapter.

Upgrading Handset Server on Standalone machine from 6.1 SP3 build to 6.2.4 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. If you have installed any 3rd party certificates like VeriSign, ensure that you back up the IHS keystores first. The key stores are located at **/opt/IBM/HTTPServer**. The keystore at location **/opt/avaya/HandsetServer** should also be backed up. This will be needed when you upgrade/migrate Client Enablement Services server.

4. Stop the currently installed Handset Server using "**service handset_server stop"**

5. Install the 6.2.4 Handset Server (**RHServer.bin**) on a standalone machine. This will automatically remove the existing 6.1 SP3 Handset Server. You may need to re-enter the Handset Server IP address. The other Handset Server settings are retained.

Upgrading Handset Server on Standalone machine from 6.2 build to 6.2.4 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 6.2.4 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 Communicator 2.1.1 for Android client is available for download from the Google Play Market.
2. The Avaya Communicator 2.1 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 6.2.4 (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 Platform	6.2 Build 6.2.1.0.9 Patch 6.2.2.09001 6.3 Build 6.3.0.0.18002 Patch 6.3.1.08002.0 6.3.7.0.05001
Avaya Aura® System Manager	6.2, 6.3, 6.3.2, 6.3.4, 6.3.8,7.0
Avaya Aura® Communication Manager	5.2.1, 6.2, 6.3.0, 6.3.2, 6.3.3, 6.3.6,7.0
Avaya Aura® Session Manager	6.2, 6.3, 6.3.2, 6.3.4, 6.3.8,7.0
Avaya Aura® Presence Services	6.1 SP2, 6.1 SP5, 6.2, 6.2 SP1, 6.2 SP2, 6.2 SP4,6.2 SP6,7.0
Avaya Modular Messaging	5.2
Avaya Aura Messaging	6.1, 6.2,7.0
Avaya Aura® Communication Manager Messaging	6.2, 6.3
Avaya Meeting Exchange	5.2, 6.2, 6.2 SP1
Avaya Aura Conferencing	6.0 SP1
Avaya one-X® Client Enablement Services	6.1 SP3, 6.2, 6.2 SP1, 6.2 SP2, 6.2.3 SP1,6.2 SP4

The following table shows the supported Avaya clients by Avaya one-X® Client Enablement Services release 6.2.4

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® Mobile Client for Android*	6.1.4, 6.2, 6.2 SP1, 6.2 SP2,6.2 SP4
Avaya one-X® Mobile Client for iPhone*	6.1.4, 6.2, 6.2 SP1, 6.2 SP2,6.2 SP5
Avaya Communicator for Android	2.1.1
Avaya Communicator for iOS	2.1
Avaya one-X® Communicator	6.1 SP9, 6.2, 6.2 SP2, 6.2 FP3,6.2 FP6

*One-X Mobile clients (CES versions) will not be available after Sept 2015. They have been replaced by Avaya Communicator mobile clients who offer improved functionality, performance and quality. Avaya Communicator mobile clients can connect to your CES server. Please see PSNs on this topic for additional information.

The following table shows the supported 3rd party components by Avaya one-X® Client Enablement Services release 6.2.4

3rd Party Components	Software	Supported Release / Model
CES Server OS	Linux	RHEL 6.2+ 64-bit
Handset Server OS	Linux	RHEL 6.2+
LDAPs	IBM Domino Server	8.5.3
	Microsoft Active Directory	2008 R2
	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	8.0, 9.0
	Mozilla Firefox	11.x
	Apple Safari	5.x

Hardware compatibility

The following table shows all supported server hardware with Avaya one-X® Client Enablement Services 6.2.4

Avaya Common Servers	Min. RAM Req.	Platform	One-X CES
HP Proliant DL360 G8 (new install / migration)	32 GB	SP 6.3.1 / RHEL 6.2+	6.2.x
HP Proliant DL360 G7 (new install and upgrade / migration)	24 GB	SP 6.3.1 / SP 6.2.2 / RHEL 6.2+	6.2.x
Dell PowerEdge R610 (new install and upgrade / migration)	24 GB	SP 6.2.2 / RHEL 6.2+	6.2.x
S8800 (migration only)	16 GB	RHEL 6.2+	6.2.x
Customer Provided HW (new install only, min spec required)	16 GB	RHEL 6.2+	6.2.x

Tested Environment

The following tables show SV Environment that is used for validating Avaya one-X® Client Enablement Services 6.2.4.

Avaya Components	Supported Release
Avaya Aura® System Platform	6.3 Build 6.3.0.0.18002 Patch 6.3.5.01003.0 6.3.7.0.05001
Avaya Aura® System Manager	6.3.7, 6.3.12,7.0
Avaya Aura® Communication Manager	6.3.5, 6.3.6, 6.3.10,7.0
Avaya Aura® Session Manager	6.3.7, 6.3.8, 6.3.12,7.0
Avaya Aura® Presence Services	6.2 SP4, 6.2.3 Patch 7, 6.2.6 Patch 1,7.0
Avaya Modular Messaging	5.2 SP16
Avaya Aura Messaging	6.2.5, 6.3.2
Avaya Aura® Communication Manager Messaging	6.2, 6.3
Avaya Meeting Exchange	6.2.2.05
Avaya Aura Conferencing	6.0 SP1 (Bridge 6.0.1.12.1)
Avaya one-X® Client Enablement Services	6.2.4
Avaya SIP Hard Phones 9620L	2.6.9+
Avaya SIP Hard Phones 9621G	6.5
Avaya SIP Hard Phones 9601	6.1.5+
Avaya H.323 Hard Phones 9620L	3.5.1+
Avaya H.323 Hard Phones 9621G	6.4
Avaya one-X® Mobile Client for Android*	6.2 SP4
Avaya one-X® Mobile Client for iPhone*	6.2 SP5
Avaya Communicator for Android	2.1.1
Avaya Communicator for iOS	2.1
Avaya one-X® Communicator	6.2 FP6

*One-X Mobile clients (CES versions) will not be available after Sept 2015. They have been replaced by Avaya Communicator mobile clients who offer improved functionality, performance and quality. Avaya Communicator mobile clients can connect to your CES server. Please see PSNs on this topic for additional information.

*

3rd Party Components	Software	Supported Release / Model
CES Server OS	Linux	RHEL 6.5
Handset Server OS	Linux	RHEL 6.5
LDAPs	IBM Domino Server	9.0.1 FP3
	Microsoft Active Directory	2008 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	36.0
	Apple Safari	5.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-8256	SIP Local Port and Secure option is not retained after upgrading from CES 6.1 SP2 to 6.1 SP3	Workaround: Administrator can change SIP Local Port setting after upgrade in Web Admin
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-9510 / ONEXCESSERVER-9812	Unable to provision new CES users when using mail attribute as userID to deploy 1XCES 6.2.3.0.117 build integration with Novell	Currently, 1XCES does not support using mail attribute as userID for Novell directory.
Client Enablement Services Server Administration		
ONEXCESSERVER-9871	Local WebLM server isn't accessible via https://< IP_address_of_Client_Enablement_Services_server >/WebLM/LicenseServer	Workaround: Using the below instead https://< IP_address_of_Client_Enablement_Services_server >/weblm-server-4.7.1/LicenseServer
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-8784	TLS 1.2 is currently disabled (not supported)	This is to avoid TLS 1.2 handshake failure between 1XCES clients and 1XCES server when server certificate does not support TLS 1.2

one-X CES ID	Caveat	Workarounds/Notes
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 performing incremental synchronization	Full synchronization is required to delete a CES user.
Client Enablement Services Client Features		
ONEXCESSERVER-9304 / ONEXCESSERVER-9582	CES is using the Avaya SIP CA certificate on the IHS, and custom self-signed certificate on HSS. New mobile clients and 1XC clients may fail to login due to this untrusted certificate.	Workaround: To populate the SMGR CA signed certificate on the IHS/HSS, the following steps need to be invoked. # cd /opt/avaya/IHS # ./migrate_smgr_ca_key_trust_store_to_ihs.pl # ./activate_smgr_ca_certs.pl # ./migrate_ihs_keystore_to_handset_server.pl # service 1xp restart
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

one-X CES ID	Caveat	Workarounds/Notes
		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 6.2.4

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-9181 / PRES-2537	Web admin page response is slow, System menu page is not loaded and Monitors has page error for Handset and Other Services	In some circumstances it's possible that the Presence adapter will fail to stop properly and will hang in the stopping state. This is due to a bug in the Presence library (3rd party to CES), so the fix for this issue can't be provided by CES. Workaround: if PS adapter hangs in the stopping state for too long (5 minutes or more), then PS server should be restarted: on the PS server, execute scripts /opt/Avaya/Presence/presence/bin/stop.sh ; /opt/Avaya/Presence/presence/bin/start.sh.

	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
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 6.2.4

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-9510	Administrator can't access to Scheduler and sub-sequence tabs after fresh install CES 6.2.1.0.20 build with Novell eDirectory/Sun Directory using "mail" attribute as userID	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-9035	New voicemails do not get downloaded on Avaya Communicator after upgrading 1XCES from 6.1.3.0.12 to 6.2.0.0.195 with single AD on System Platform 6.2.2.09001.0.	Intermittent issue. Workaround: Restart 1XCES service after the upgrade is committed.
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-9277	After changing LDAP login attribute from "sAMAccountName" to "userPrincipalName" on CES web admin, only 1XM can login using new login attribute.	Workaround: Login 1XCES Web Admin, IBM Web Console and 1XC using "sAMAccountName" only. Recommendation: Login attribute should be set at CES installation.

Issue ID	Problem	Solution/Workaround
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.
ONEXCESSERVER-10309	Upgrade template does not allow Administrative Account selection	Workaround: on changing the “objectClass=user” instead of “objectClass=ServiceAccount” for service account in the customer’s LDAP resolved the issue
ONEXCESSERVER-10400	CES server is intermittently (about 80-90 %) failing to shut down during the weekly system platform backup.	None.
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-10258	Avaya Communicator integrated with CES cannot receive incoming call when Calls to My Phones is set Only Primary	None.
ONEXCESSERVER-10388	Admin CLI do not allow to manage PS 7.0.0 adapter	None
ONEXCESSERVER-10154	CES server is not presenting "live" voicemail updates for call history after voicemail server had been patched/upgraded.	None
ONEXCESSERVER-10120	Incomplete corporate favorites list returned on full refresh immediately after login	None
ONEXCESSERVER-10101	After re-run of preweb , configuration values isn't empty	None

Issue ID	Problem	Solution/Workaround
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
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

Issue ID	Problem	Solution/Workaround
ONEXCESSERVER-9380	Priority call does not ring (silent ring) SIP deskphone when called CES user sets “Block All Calls”	None.
ONEXCESSERVER-9232	1xM Login takes 25 seconds	Once the client is logged in successfully and the password is cached (for an hour), the login will be successful very fast. Consult the IT LDAP team. This can be due to slow LDAP access. Also could be due to enabled LDAP referrals
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-9101 / ONEXMOBILE-1928	FAV/VIP and History do not display the Address value in contact details	None.
ONEXCESSERVER-10357	1xCES build 6.2.4.0.92 enabling few protocol traffic logs generates lots of SystemErr.log and SystemOut.log	Issue is observed only when PS adapter 7.0.0
ONEXCESSERVER-10309	Upgrade template does not allow Administrative Account selection	
ONEXCESSERVER-10002	Customer want to know why they getting bulk of errors in system logs related to ClosedChannelExceptionjava.nio.channels.ClosedChannelException	None
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-9956	1XM on iPhone - Some or all Favorites are sometimes gone	None
ONEXCESSERVER-9955	After Upgrade to CES SP3 the Administration page no longer displays	None
ONEXCESSERVER-9914	No name for visual voice mail on 1xC and 1xM when the caller (with a CES account) let a message with its deskphone	None
ONEXCESSERVER-9913	IPhone 5 does not show presence status	None
ONEXCESSERVER-9912	CES not extending calls to mobile	None
ONEXCESSERVER-9891	Inconsistent presence status message updation	None
ONEXCESSERVER-9828	Need to run full sync twice every time whenever a new user is added on AD. First full sync does not show users in unprovision list	None
ONEXCESSERVER-9101	FAV/VIP and History do not display the Address value in contact details	None

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 6.1 SP9 or 6.2 SP2 or 6.2 FP3

Issue ID	Problem	Solution/Workaround
One-X Communicator		
ONEXC-10020	Many exceptions thrown out in trace.log while logging 1XC (CES mode)	There is on 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
Android Clients-		
ONEXCESSERVER-9410	VIP list does not show any VIP contacts after re-launching/re-login to 1XM app	Intermittent
iPhone Clients-		
ONEXCESSERVER-9410	VIP list does not show any VIP contacts after re-launching/re-login to 1XM app	Intermittent

Appendix A: Steps to replace default certificate with SMGR CA on CES 6.2.4 (AC connection fix)

Below are steps to replace default certificate with SMGR CA on CES 6.2.4 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: The following can be done on the CES Server to disable the RC4 cipher suite:

1) SSH into one-X CES Server from putty.
2) Switch to root user. First craft/craft01 and su/root01
3) Run the following command, to stop IHS :
    a. /sbin/service ihs stop
4) Edit the file /opt/IBM/HTTPServer/conf/httpd.conf using vi editor.
5) Remove the following lines and replace with the new ones:
    a. Lines to remove :
        i. SSLCipherSpec 3A
        ii. SSLCipherSpec 35
        iii. SSLCipherSpec 2F
        iv. SSLCipherSpec 35b
    b. Replace with the following lines, which disable RC4 suite:
        i. SSLCipherSpec TLS_RSA_WITH_AES_128_CBC_SHA
        ii. SSLCipherSpec TLS_RSA_WITH_AES_256_CBC_SHA
        iii. SSLCipherSpec SSL_RSA_WITH_3DES_EDE_CBC_SHA
6) The final set of lines between SSLEnable and SSLDisable should read as:
    a. SSLEnable
    b. SSLCipherSpec TLS_RSA_WITH_AES_128_CBC_SHA
    c. SSLCipherSpec TLS_RSA_WITH_AES_256_CBC_SHA
    d. SSLCipherSpec SSL_RSA_WITH_3DES_EDE_CBC_SHA
    e. SSLProtocolDisable SSLv2 SSLv3
    f. </VirtualHost>
    g. KeyFile /opt/IBM/HTTPServer/ihsserverkey_default.kdb
    h. SSLDisable
7) Start the IHS
    a. /sbin/service ihs start

Appendix C: 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 / System Platform
AD	Microsoft Active Directory
ADAM	Microsoft Active Directory Application Mode
AD LDS	Microsoft Active Directory Lightweight Directory Services