Avaya one-X® Portal

Release 5.2.2

SP Release Readme

Release 5.2.2
September, 2010

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

© 2009 Avaya Inc. All Rights Reserved.

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document might be incorporated in future releases.

Documentation disclaimer

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree 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 the Customer or End User.

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all the time and we have no control over the availability of the linked pages.

Warranty

Avaya Inc. provides a limited warranty on this product. 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 through the Avaya Support Web site:
http://www.avaya.com/support

License

USE OR INSTALLATION OF THE PRODUCT INDICATES THE END USER'S ACCEPTANCE OF THE TERMS SET FORTH HEREIN AND THE GENERAL LICENSE TERMS AVAILABLE ON THE AVAYA WEB SITE http://support.avaya.com/LicenseInfo/ ("GENERAL LICENSE TERMS"). IF YOU DO NOT WISH TO BE BOUND BY THESE TERMS, YOU MUST RETURN THE PRODUCT(S) TO THE POINT OF PURCHASE WITHIN TEN (10) DAYS OF DELIVERY FOR A REFUND OR CREDIT. Avaya grants End User a license within the scope of the license types described below. 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 End User. "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. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. "Hardware" means the standard hardware Products, originally sold by Avaya and ultimately utilized by End User.

License type(s)

Named User License (NU). Customer 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 Product that permits one user to interface with the Product.

Shrinkwrap License (SR). With respect to Software that contains elements provided by third party suppliers, End User may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickwrap" license accompanying or applicable to the Software ("Shrinkwrap License"). The text of the Shrinkwrap License will be available from Avaya upon End User's request (see "Third-party Components" for more information).

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site:
http://support.avaya.com/ThirdPartyLicense/

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 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 Web site:
http://www.avaya.com/support

Trademarks

Avaya, the Avaya logo, and COMPAS are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions.
All other trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support Website:
http://www.avaya.com/support

Avaya support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Support Web site:
http://www.avaya.com/support

Contents

Obtaining the one-X Portal 5.2 GA release files 5
Installing the GA release of one-X Portal 6
Configuring non-one-X Portal users in the Presence group 6
Upgrading Avaya one-X Portal 7
Post Installation Procedures 11
Stopping and restarting WAS 12
Logging on to Portal Client using HTTPS 12
Acquire one-X Portal Service Pack Software 13
Installing one-X Portal 5.2 Service Pack 2 13
Prerequisites: 13
Installing the update 13
Verifying the update is correctly installed 14
Uninstalling the one-XP 5.2 Service Pack 2 15
Verifying the update is correctly uninstalled 15
Changes delivered with one-X Portal 5.2.2 16
Problems fixed in one-X Portal 5.2, Service Pack 2 16
SP release of the one-X Portal Extensions 17
PDE dependency on MSXML 4.0 17
Functionality not supported for the GA and SP release 18
Functionality not supported in the Administration Application 18
Known Outstanding Issues 18
Pending Issues 18
Known Issues 20
Recreating phone numbers while migrating from 1.1 to 5.2.2 20
Rechecking server field parameters while migrating from 1.1 to 5.2.2 20
Set up Communication Manager to use Universal Call ID (UCID) 20
Synchronizing Avaya one-X Portal and IPS Enterprise Directories 21
WebLM fails to provide licenses when configured for secure https due to certificate error 21
Connection to one-X Portal Server doesn't work if previous version of Portal Desktop Extensions (PDE) was installed 21
Change firewall rules to allow the server to communicate with other servers on port 80 and 443 22
Setting up VNC 22
Interoperability Matrix 26
Port requirements for one-X Portal 26
Server to Server Ports 26
AE Services to Communication Manager Ports 27
Avaya and one-X Portal and administration applications to server ports 27

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

SNMP Ports 28
Required software for the one-X Portal Server 28
Required software for integrating servers with one-X Portal 28
Software for one-X Portal Applications and one-X Portal Extensions 29
Presence States expected behavior 30
Troubleshooting 31
Troubleshooting the one-X Portal installation 31
In an upgrade install, custom log settings removed 32
Troubleshooting one-X Portal servers 33
Postgres database contains 2 entries for the same presentity 33
Troubleshooting one-X Portal administration 34
Need to synchronize the directory to provision a user 34
Database backup through Admin is not working 34
Troubleshooting one-X Portal client 35
Use initial login when changing phone settings 35
Technical Support 36

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

About the Avaya one-X Portal 5.2.2 Service Pack release
An updated version of the current readme document can be found at Avaya Support Site: http://support.avaya.com .

This section includes the following topics:

- Obtaining the one-X Portal 5.2 GA release files
- Installing the GA release of one-X Portal
- Configuring non-one-X Portal users in the Presence group
- Post Installation procedures
- Upgrading Avaya one-X Portal
- GA and SP release of the one-X Portal Extensions
- Functionality not supported for the GA and SP release

Obtaining the one-X Portal 5.2 GA release files

The one-X Portal software and Readme for the GA release of one-X Portal is delivered on a DVD-ROM and via download from Avaya. The installation is packaged in one file that contains the server and optional desktop client software.

The following table describes the contents of the one-X Portal 5.2 DVD-ROM for the GA release.

DVD-ROM directory	**Contents**	**Description**
Root Level	setup.bin	Start file for the installation
	License.html	one-X Portal license file
	1XPGAReadme.pdf	one-X Portal Readme for the GA release
Doc	WhatsNewinOneXP.html	New features of one-X Portal release 5.2
	Implementing_1XP.pdf	Implementation guide for Avaya one-X Portal
	Admin_OLH.pdf	Administration Application Online Help
	WebSphereSecureWebLM.pdf	File describing the steps to configure Websphere to communicate via secure connection to WebLM.
Branding	1XP_Client_Portal_Branding.zip	File used to customize the look and feel of one-X Portal.

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

DVD-ROM directory	Contents	Description
Tools	conftool.zip	Zip archive with files for Environment Validation Tools
One_x_Extensions	One-X.msi	PDE installer

Installing the GA release of one-X Portal

The installer (setup.bin) is located in the root level folder on the DVD-ROM. Copy the setup.bin file to a convenient local directory. Only the root user can install the server software. Run the "**chmod +x setup.bin"** command to ensure the file is executable before you run it.

Before you install:

1. If you are upgrading the one-X Portal server from version 1.1 to 5.2.2, upgrade your Application Enablement Service (AES) server to its highest released version (4.2.2 or greater). You will not be able to login to any of the Portal Clients until the AES server is upgraded to the version 4.2.2 or greater.
2. In a multi AES server environment, all the AES servers must have the same Login ID and Password to support Avaya Intelligent Presence Service integration.

After running the one-X Portal installation, configure one-X Portal. See Implementing Avaya one-X Portal see one-X Portal IPS integration Notes for more one-X Portal configuration information.

Configuring non-one-X Portal users in the Presence group

To be able to see presence for non-one-X Portal users, perform the following steps to configure these users using Presence group:

1. Add the non-one-X Portal user to the LDAP directory server security group that is designated as the security group to be used by the Presence server.
2. Configure the appropriate Communication Manager and AES servers from the Servers tab in the **Administration Web Client** application.
3. Create a **User Import** spreadsheet with the appropriate handles and user names of the non-one-X Portal users and set **Enable Users** to '**n**'. Use the template provided in the /opt/Avaya/1xp/bin directory to ensure the file format is compatible and make sure the users are disabled.

Note:

The spreadsheet contains columns for User Monitor, Enable User, Display Name, User Properties, Group Profile Name, Service Providers, Provider parameters. The Enable User column must be the second column from the left on the spreadsheet.

4. Run a **Full Enterprise Directory Synchronization** from the **Scheduler** tab in the Administration Web Client application.
5. Run the **Import User** script in the **Administration Command Line Client** to import the users.

Upgrading Avaya one-X Portal

Prerequisites

1. one-X Portal version 1.1 or above can only be upgraded.
2. After ensuring you have adequate disk space, perform a database back up from the one-X Portal administration client as described in the one-X Portal troubleshooting guide before you begin upgrading the one-X Portal server. Note the backup directory path where the backup is stored.
3. Create a Presence Users group before the upgrade in the enterprise directory or select ALL ENTERPRISE USERS on the Enterprise directory presence security group screen of the wizard.

To perform an upgrade, you need to either log on to the one-X Portal server machine locally or remotely using VNC (see Setting up VNC on page 13 to install VNC). If you are upgrading from a directory on a network machine, execute **"chmod +x setup.bin"** to add execution rights to setup.bin.

1. Login as root on the server that is hosting one-X Portal.
2. Execute the following command to validate the version of Linux on the server:
   cat /etc/redhat-release

   The following is an example of the response returned by this command: Red Hat Enterprise Linux ES release 4 (Nahant Update 4). one-X Portal release 5.2 supports Red Hat Enterprise ES version 4 Update 4 and greater.

   If one or more of the key items are not correct, do not install one-X Portal. Update the version of Linux to version 4 or 5.
3. If the one-X Portal DVD does not mount automatically, execute the following command:
   mount /dev/cdrom /media/cdrom

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

4. Execute the following commands to change the directory to the cdrom folder and launch the Installation Wizard:
   /media/cdrom/setup.bin
5. Follow the Installation Wizard prompts and enter the required information in the installation wizard screens as described in the substeps below.

   The following buttons are available on all Installation Wizard screens:

Name	Description
Cancel	Cancels the installation of one-X Portal and discards all information entered in the installation Wizard.
Previous	Discards the information entered in the current screen and returns to the previous installer screen.
Next	Saves the information entered in the current screen and moves to the next installer screen.

While upgrading, the installation wizard displays the following screens for:

1. End user license agreement

Name	Description
License Agreement	Records that you have agreed to the terms of the agreement and continues the one-X Portal.
I do not accept the terms of this license agreement	Discards the information entered in the current screen and returns to the previous installer screen.

2. Installation types

Name	Description
Typical	Avaya recommends that you select this installation type. Although this option provides a complete installation, only those components and services that you have configured for integration will function. Installs all the one-X Portal components, including: • Avaya one-X Portal Server • Avaya Administration

	application • Avaya one-X Portal client applications • Avaya one-X Portal application server • Avaya one-X Portal database • Avaya Web License Manager (Optional- you can use a remote WebLM)
Custom	

3. Enterprise Directory configuration
   The Installation Wizard uses this information to configure the connection between one-X Portal and the Enterprise Directory server.

   If the Enterprise Directory has users defined in one domain and security groups defined in another domain, the Installation Wizard presents you with two Enterprise Directory configuration screens. Configure the user domain in the first screen. Configure the resource domain for security group in the second screen.

Name	Example Value	Description
Enterprise Directory IP address	###.###.###.###	IP address of the machine that hosts the Enterprise Directory server.
Enterprise Directory port	389	Port that the one-X Portal machine will use to communicate with the Enterprise Directory server.
Enterprise Directory Domain	users.domain.xyzcorp.com groups.domain.xyzcorp.com	Fully qualified domain name configured on the EnterpriseDirectory server. For a split domain topology, enter the user domain name in the first screen, and the resource domain in the second screen.
Enterprise Directory user	Admin_service_user	Enterprise Directory user

name		that you created for the one-X Portal administrative service account.
Enterprise Directory password	Admin_service_password	Password for the one-X Portal administrative service account.

4. Enterprise Directory presence security group

   The Installation Wizard uses the presence security group to assign permissions to presence for users who want to retrieve presence information on the one-X Portal application.

Note:

Do not use the default security group names, such as Domain Users, for one-X Portal. These default groups do not function correctly with LDAP. For more information, see Microsoft KB 275523.

Name	Example value	Description
Presence Group	CN=1XP Presence,CN=Users, DC=marketing,DC=organization,DC=com	Security group DN for one-X Portal users from whom you want to be able to retrieve presence information. These users are listed as unprovisioned users. They cannot login to one-X Portal and do not consume a license for one-X Portal.

Note:

The selection of the **"Everybody"** option in the installation dialog provides presence information to all the users in the enterprise directory overriding the **"Presence Group DN"** specified in the text box.

5. Restoring database

   The wizard asks for the path where the database back up is stored. Either provide the path or use the Browse button to provide the required database.

6. Summary of one-X Portal installation

   This screen summarizes the selections and configuration information that you entered in the Installation Wizard.

   Review this summary carefully. If you need to change any of the configuration information, click **Previous.** To begin the upgrade, click **Install**.

7. Completing the one-X Portal installation

   Click **Finish** to complete the one-X Portal upgrade.

Note:

At the end of the installation, the installer may continue to display 100% completed for up to twenty minutes. This indicates that the installer is completing the final task in the installation. This screen delay does not indicate that the installer has frozen.

Refer the following topics under Known Issues to perform the relevant checks after the upgrade:

- Post installation procedures
- Recreating phone numbers while migrating from 1.1 to 5.2.2
- Rechecking server field parameters while migrating from 1.1 to 5.2.2
- Stopping and restarting WAS

Post Installation Procedures

After the installation, check to make sure the TSAPI.PRO file still exists in /opt/IBM/Websphere/AppServer/lib (default location). Go to this directory and type **ls -al TSAPI.PRO**. If the file does not exist or does not contain your AES IP address, delete the existing AES server and re-install it in the Administration Web Client application to recreate the file.

Also, you must load the new security certificates for Modular Messaging.

1. In the Administration Web Client, click the **Servers** tab.
2. Select **Voice Messaging** from the left pane.
3. Select each messaging server that is configured.

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

4. In the **SSL Certificate** field, press **Retrieve SSL Certificate**.
5. Verify the message that certificates were properly installed is received.

Stopping and restarting WAS

Follow this procedure to stop and restart WAS, post-upgrade and after you retrieve the SSL certificates from each of the MM servers.

1. Log on to one-X Portal server as root.
2. Go to opt/IBM/WebSphere/AppServer/profiles/default/bin/ using command:

   cd /opt/IBM/WebSphere/AppSerer/profiles/default/bin/

3. Stop WAS with the command:

   ./stopServer.sh server1 –username <admin username> -password <admin password>

   This shows the following confirmation message and the WAS is stopped.
   Server server1 stop completed.

4. To restart WAS, run the command:

   ./startServer.sh server1

   WAS restarts and shows the following confirmation message:
   Server server1 open for e-business

Logging on to Portal Client using HTTPS

In order to protect a user's Enterprise credentials, Avaya one-X Portal client now uses HTTPS to log on to the portal regardless of whether they have chosen HTTP or HTTPS.

The URL:
http://oneXportal_server.domain.com/
used to log on to the portal will now be redirected to:
https://oneXportal_server.domain.com/logon.jsp
where oneXportal_server.domain.com is an IP address or a fully qualified name and domain of the server that hosts one-X Portal. After authentication, the portal will be launched back in HTTP.

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

If you prefer to use HTTPS for the entire one-X Portal client usage, you should use the URL:

https://oneXportal_server.domain.com/

CAUTION:
Use of HTTPS for the entire one-X Portal client usage reduces the client capacity of the portal by up to 10%. Users creating a bookmark/favorites entry of the logon URL must change the URL to http://oneXportal_server.domain.com/ to avoid using HTTPS

Acquire one-X Portal Service Pack Software

To download the Avaya one-X Portal Server software:

1. Open the web browser on your PC, and go to http://www.avaya.com/support.
2. Click **Downloads** under **Resource Library**.
3. Click the letter **A** in the alphabet listing.
4. Click **Avaya one-X™ Portal**.
5. Select **Avaya one-X Portal 5.2 Service Pack 2** from the drop-down menu.
6. Select the appropriate download.

Installing one-X Portal 5.2 Service Pack 2

Prerequisites:

1. 1XP 5.2 GA build should be installed on your system
2. 1xp_update-5.2.2.0.x.tar.gz update file

Installing the update

1. SSH to the 1XP server as root
2. Change directory to 1XP install directory:
   Example: `cd /opt/avaya/1xp`
3. Copy 1xp_update-5.2.2.0.x.tar.gz to /opt/avaya/1xp directory
4. Untar the update using the following command:
   `tar -xzf 1xp_update-5.2.2.0.x.tar.gz`
   The update contents will be extracted to /opt/avaya/1xp/updates/current directory.
   The following files get extracted:

```
upgrade (directory)
earlist.txt
ears.tar.gz
install.sh
jarlist.txt
```

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

```
restore.sh
version.txt
```

5. Install the update using the following command:
   ```
   ./updates/current/install.sh <admin_service_user>
   <admin_service_password> <dbinst_name>
   <dbinst_password> <db_name> <roinst_name>
   ```
   Where <admin_service_user> is the WAS user name and <admin_service_password> is the WAS password.
   ```
   <dbinst_name> is the db2 instance name, default
   "dbinst"
   <dbinst_password> is the password for the instance
   <db_name> is the database name, generally "ACPDB"
   <roinst_name> value would be by default "roinst"
   ```

This completes the service pack installation.

Verifying the update is correctly installed

1. Verify a backup/un-installation location was created by looking for the presence of:
   ```
   /opt/avaya/1xp/updates/5.2.2.0.x/restore.sh
   ```
2. Verify the following applications were properly installed by checking the version at the following URL's:

Application	URL**
1XP_Adapter_APAS.ear	http://*server.domain.com*/adapter-ips/version.jsp
1XP_Adapter_CM.ear	http://*server.domain.com*/adapter-cm/version.jsp
1XP_Adapter_MX.ear	http://*server.domain.com*/adapter-mx/version.jsp
1XP_Client_Admin.ear	http://*server.domain.com*/admin/version.jsp
1XP_Client_Portal.ear	http://*server.domain.com*/version.jsp
1XP_Core.ear	http://*server.domain.com*/core/version.jsp

URL** - server.domain.com should match the FDQN or IP of your 1XP installation.

The Internal Version of each of the Applications should be: **5.2.2.0.1**

3. Verify the installation of the Language Pack for the Portal Client and Portal Client On-Line Help by:
   a. Navigate to URL for Portal client: http://*server.domain.com*/
   b. Logon page for Portal Client should contain Language field
   c. Select desired Language (other than English)
   d. Log onto Portal Client and verify UI appears in selected Language
   e. Select "Online Help" from the Portal Client menu and verify OLH appears in same language as Portal Client.

Uninstalling the one-XP 5.2 Service Pack 2

Follow these steps if you need to uninstall the service pack.

1. SSH to the 1XP server as root
2. Change directory to 1XP install directory :
   Example: `cd /opt/avaya/1xp`
3. Uninstall the update using the following command:
   `./updates/5.2.2.0.x/restore.sh <admin_service_user> <admin_service_password>`
   Where `<admin_service_user>` is the WAS user name and `<admin_service_password>` is the WAS password.

The service pack is now uninstalled.

Verifying the update is correctly uninstalled

1. Verify the following applications were properly installed by checking the version at the following URL's:

Application	URL**
1XP_Adapter_APAS.ear	http://*server.domain.com*/adapter-ips/version.jsp
1XP_Adapter_CM.ear	http://*server.domain.com*/adapter-cm/version.jsp
1XP_Adapter_MX.ear	http://*server.domain.com*/adapter-mx/version.jsp
1XP_Client_Admin.ear	http://*server.domain.com*/admin/version.jsp
1XP_Client_Portal.ear	http://*server.domain.com*/version.jsp
1XP_Core.ear	http://*server.domain.com*/core/version.jsp

URL** - server.domain.com should match the FDQN or IP of your 1XP installation.

The Internal Version of each of these applications depends on what update had been installed prior to installing 5.2.2. The following table outlines the Internal Versions based on prior releases:

Application	5.2.2
1XP_Adapter_APAS.ear	5.2.2.0.4
1XP_Adapter_CM.ear	5.2.2.0.4
1XP_Adapter_MX.ear	5.2.2.0.4
1XP_Client_Admin.ear	5.2.2.0.4
1XP_Client_Portal.ear	5.2.2.0.4
1XP_Core.ear	5.2.2.0.4

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

Changes delivered with one-X Portal 5.2.2

The one-X Portal updates are cumulative. The one-X Portal 5.2, Service Pack 2 release notes includes modifications and enhancements specific to one-X Portal 5.2, Service Pack 2 and from earlier releases. The changes delivered are grouped as follows:

Problems fixed in one-X™ Portal 5.2, Service Pack 2

Problems fixed in one-X Portal 5.2, Service Pack 2

This release includes the following fixes delivered to one-X Portal clients.

Issue ID	Problem
wi00339474	Mute state is not retained after hold and unhold of the call.
wi00387590	When the user logs in with the “this computer” mode and comes out of this mode and tries to login with “Telecommuter” mode. Then 1XP client hangs.
wi00380503	PDE fails to reconnect and function after recovering from network outage.
wi00365819	Anonymous/unknown caller name resolves a different name on the bridge conferencing window.
wi00408166	PDE fails to install on Windows 7 OS.

SP release of the one-X Portal Extensions

The one-X Portal PDE Installation package (one-X.msi) is the installer for the one-X Portal Desktop Extensions. This installer is available for download by users from the settings page of the Portal Client, once the one-X Portal Server has been set up.

Note:

If you are upgrading from one-X Portal 1.1 to one-X Portal 5.2, make sure that all configured conferencing and voice messaging servers are configured with a dial plan. The one-X Portal Administration Application does not enforce this rule, but if dial plans are missing from the server configurations, some of the enhanced functionality will not work.

PDE dependency on MSXML 4.0

PDE requires MSXML 4.0 patch to be installed on the system for users to log on to PDE. MSXML 4.0 comes installed in most Windows systems but it is not a standard in Windows XP. Therefore, most users may not face any problems when they log on to PDE but for systems that do not have the patch installed, users cannot go ahead of the log on window. In such a case, the PDE log on window neither accepts the user credentials nor displays an error message. **Users can download and install MSXML 4.0 from http://www.microsoft.com/downloads/details.aspx?displaylang=en&familyid=3144B72B-B4F2-46DA-B4B6-C5D7485F2B42 and resolve the issue.**

Functionality not supported for the GA and SP release

This section includes the following topics:

- Functionality not supported in the Administration Application

Functionality not supported in the Administration Application

The SES ID, Password and Confirm field on the page to assign a presence resource to a user do not possess any functionality and need to be left blank.

Known Outstanding Issues

Pending Issues

Issue ID	Issue	Suggested Solution
wi00076699 and wi00067657	Once the presence access is permanently blocked for a user, the same user cannot be assigned full access again.	Subscribing User must log out and again log on to one-X Portal.
wi00067660	If you remove a user from your favorites, the user does not get a second confirmation request.	To receive a resubscription request, the user should logout and again log on to the one-X Portal.
wi00109973	The Click to call facility on your Contacts list or Call Log Portlet available from one-X Portal either gives an error or does not work when Skype is running on your machine.	Disable the Skype through browser add-on manager and one-X Portal works as expected.
wi00113669	Disabling one-X Portal user LDAP account does not prevent the same user from logging in again using the	This is an LDAP synchronization issue and resolves once the WAS is restarted. It is however,

Issue ID	Issue	Suggested Solution
	same ID and password.	recommended that administrator should inform all users about the server down time. Approximately 5 minutes of down time is required for the WAS restart. The issue is being worked upon to find a more amicable solution.
wi00112217	Calls cannot be handled through browsers other than internet explorer when one-X Portal is started in “This Computer” mode. Users may experience disturbance or distortion in sound.	Although this is a possibility, users are advised to use IE when using one-X Portal in “This Computer” mode for voice communication. A solution to resolve this issue is being worked on.
wi00118368	If a one-X Portal user has both one-X Portal user window and one-X Portal admin window open using Firefox, losing one of the two one-XP Windows terminates the other.	None.
wi00334914	Upgrade from 1.1 to 5.2 causes log settings to disappear.	All these settings need to be re-done or reapplied after the upgrade.
wi00332632	Upgrade from 1.1 to 5.2 will uncheck the enabled check box and clears backup path.	All these settings need to be re-done or reapplied after the upgrade.
wi00345840	There is no Server Type CM 5.2 in the dropdown list of 1XP Administration configuration. Same issues also happen to Auxiliary Servers (AES), MM, and Conferencing (MX) as well.	When connecting to a CM 5.2, select 4.2 from the dropdown.
wi00305803	The authentication against Directory systems should	None.

Issue ID	Issue	Suggested Solution
	use, by default, a secure LDAP connection in the installer.	
wi00377668	Unable to backup database on some systems with 8GB of RAM or higher.	Please refer to PSN on support website for workaround solution. Formal fix to be incorporated in the upcoming 1XPS 6.1 release.

Known Issues

Recreating phone numbers while migrating from 1.1 to 5.2.2

The phone numbers used for Other Phone, EC500 and forwarding will be lost and need to be recreated when migrating from 1.1 to 5.2.

Rechecking server field parameters while migrating from 1.1 to 5.2.2

The field parameters under the server tab might get changed or lost when you upgrade one-X Portal from lower a version to 5.2.25.2.2. This happens due to the changes taking place in the one-X Portal database structure during the upgrade.

You are strongly advised to recheck all the relevant server field parameters, especially for Auxiliary server, on the Server tab of the administration interference and perform a test for the same. This will ensure smooth functioning of the Communication Manager features.

After the upgrade, retrieve SSL certificates from each of the MM servers for the IMAP 4 connection to work. Subsequently, restart the WAS.

Set up Communication Manager to use Universal Call ID (UCID)

This setup should be performed on every CM that is working with Avaya one-X Portal for the JTAPI changes to work. The setup helps JTAPI to detect the phantom calls with the same CM call ID and delete the call information based on the call ID.

To perform the setup:

1. Run the following command from the Communication Manager system administration console:

   change system-parameters features

2. Configure the following values for the Communication Manger:

   Create Universal Call ID (UCID)? Y (in Universal Call ID section)

   Send UCID to ASAI? Y (in ASAI section)

Synchronizing Avaya one-X Portal and IPS Enterprise Directories

The issue is associated with removing an existing user from AD. Once a user is removed from AD, the Enterprise Directory Synchronization should be performed twice to ensure the user is removed from both one-XP and IPS enterprise directories. If this is not performed, IPS continues to post the related information for the same user to the associated watchers.

WebLM fails to provide licenses when configured for secure https due to certificate error

This issue refers to configuring the Websphere to communicate via secure connection to WebLM. The status of the oneX Portal license server is displayed as “Error Mode” when the server is configured to access https for WebLM. The detailed steps to configure are explained in the document WebSphereSecureWebLM.pdf on the media.

Connection to one-X Portal Server doesn’t work if previous version of Portal Desktop Extensions (PDE) was installed

If a user has been using a prior version of Portal Desktop Extensions (PDE) and uninstalled it. After installing the 5.2.25.2.2, the following steps need to be followed:

a. Open the Settings for the Portal Extension Settings (right-click on the icon in the System Tray...choose Settings).
b. Choose the "Advanced" tab. You may see the old Context Root here (it may also be blank).
c. Clear the "Context Root:" field
d. Click "OK" (do not click “Cancel”)

Now the user should be able to sign in.

Change firewall rules to allow the server to communicate with other servers on port 80 and 443

The one-X Portal server needed to communicate with other servers using HTTP running on port 80 and 443. Due to firewall outgoing rules set for One-X portal, every time http request for remote site resulted into "page not found" error due to redirection to one-X portal. Some environments do not work with this configuration and for that reason some of the rules have been removed from the earlier version. Due to this, one-X admin user logging on one-X Portal server will need to type in complete URL instead of simplified URL.
So, earlier “http://<localhost>/admin” would redirect to “https://<localhost>:9443/admin/logon.jsp”, but now with this change the user has to type-in the complete URL(“https://<localhost>:9443/admin/logon.jsp”) to access the admin pages on the one-X Portal server.

Setting up VNC

Prerequisites: VNC viewer has to be installed on the machine that is used to perform upgrade/installation.

The following procedure describes VNC server setup:

1. To set up VNC Server.
   a. Run command “up2date vnc-server” on a Red Hat Enterprise Linux machine.
   Sample Output:
   adminAddress ['root@localhost']
   1. debug No
   2. disallowConfChange ['noReboot', 'sslCACert', 'useNoSSLForPackages', 'noSSLSe

3. enableProxy No
4. enableProxyAuth No
5. enableRollbacks No
6. fileSkipList []
7. forceInstall No
8. gpgKeyRing /etc/sysconfig/rhn/up2date-keyring.gpg
9. headerCacheSize 40
10. headerFetchCount 10
11. httpProxy
12. isatty Yes
13. keepAfterInstall No
14. networkRetries 5
15. noBootLoader No
16. noReboot No
17. noReplaceConfig Yes
18. noSSLServerURL http://xmlrpc.rhn.redhat.com/XMLRPC
19. pkgSkipList ['kernel*']
20. pkgsToInstallNotUp ['kernel', 'kernel-modules', 'kernel-devel']
21. proxyPassword
22. proxyUser
23. removeSkipList ['kernel*']
24. retrieveOnly No
25. retrieveSource No
26. rhnuuid f1ea8070-1782-11dd-9e79-7198a3bc6f0f
27. serverURL https://xmlrpc.rhn.redhat.com/XMLRPC
28. showAvailablePacka No
29. sslCACert /usr/share/rhn/RHNS-CA-CERT
30. storageDir /var/spool/up2date
31. systemIdPath /etc/sysconfig/rhn/systemid
32. updateUp2date Yes
33. useGPG Yes
34. useNoSSLForPackage No
35. useRhn Yes
36. versionOverride

2. Enter number of item to edit <return to exit, q to quit without saving>:

3. Run the command as root:

   Edit /etc/sysconfig/vncserver

4. Uncomment the line:
   VNCSERVERS=”1:put_the_user_you_will_log_in_as_here”

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

Note:

The server defaults to the resolution of the machine where it is installed. Therefore, if you happen to connect to a desktop with a high resolution monitor from a laptop, you need to uncomment and set the following line also:

VNCSERVERSARGS[1]=”-geomentry 1024x768”

5. Run command:

   chkconfig vncserver on

6. To switch user to the user that you will log on as type:

   su to <user name>

7. To set password, run command:

   vncpasswd <new password> and hit enter
   Sample output:
   [root@onexp]# vncpasswd
   Password:
   Verify:

8. To create initialization files, run:

   [root@onexp]# vncserver

   NOTE: You will require a password to access your desktops.

   Password:
   Verify:

9. Run the command:

   Edit /home/user/.vnc/xstartup

10. Uncomment the following two lines that appear after running the above command to get the normal desktop when you log on.

    unset SESSION_MANAGER
    exec /etc/X11/xinit/xinitrc

11. Run command:

service vncserver start

NOTE: The vncserevr start might fail, as the server is already started, if it is not started then the above command would be required to be executed.

Connect from the remote machine using client VNC viewer by:

servername: <port>

For example:
xpserver:1
where 1 is the port name.

Interoperability Matrix

This section describes the port requirements, product versions and the latest service packs needed for one-X Portal, release 5.2.2

Port requirements for one-X Portal

Server to Server Ports

Server	Protocol	Default Ports		Configurable	Comments
		External Server	one-X Portal		
Modular Messaging	SMTP	25	25	1024-65000	
	IMAP4/SSL	993	993	1024-65000	
	LDAP	389	389	No	MM to LDAP
Meeting Exchange	TCP	20002	20002	No	Meeting Exchange does not support NAT
	TCP	5040 with auto increment	5020	Fixed Rate	
	UDP	5020 with auto increment	5070	Fixed Rate	
Presence		Variable	5070	Yes 1024-65000	
WebLM	HTTP	8443	8443	Remote WebLM: Yes Local WebLM: No	Whether this port is configurable depends on the location of WebLM
Enterprise directory	LDAP	389	389	1-65535	
AE Services	TCP for TSAPI	450	450	No	
	TCP for TSAPI	1050-1065	1050	Yes	

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

	DMCCC/SSL	4721/4722	4721	Yes	By default, this port is disabled. You must enable this port manually.

AE Services to Communication Manager Ports

Protocol	AE Services	Communication Manager
ASAI	Configurable in range 1050-1065	Fixed at 8765
H.323/RAS	Configurable in range 7000-8100	Fixed at 1719
H.323/CCMS	Configurable in range 3000-4100	Fixed at 1720

Avaya and one-X Portal and administration applications to server ports

Application	Protocol	Default port	Configurable
Avaya one-X Portal	HTTP or HTTPS	80 to 443	Yes
Avaya one-X Portal	HTTP or HTTPS	80 to 443	Yes
Administration application	HTTP or HTTPS	80 to 443	Yes
Administration application command line interface	SOAP	8880	Yes

SNMP Ports

Application	Protocol	Default Port	Configurable
SNMP trap daemon	UDP	162	Yes

Required software for the one-X Portal Server

Software	Supported Versions	Location
Operating System	• Red Hat Enterprise Linux ES 4.0 with the following components: Update 4,5 6, 7, 8; 32 bit Red Hat Enterprise Linux ES 5.0 with the following components: • Update 1,2,3,4 32 bit • Daylight Savings Time patch 2006m-3.el4.noarch.rpm • X-Windows only required for installation	Avaya one-X Portal Server machine.
Web Browser	• Mozilla Firefox 2.0, 3.0 • Internet Explorer 6.0 and 7.0	Avaya one-X Portal Server machine computer used by one-X Portal administrator.

Required software for integrating servers with one-X Portal

Software	Supported Versions	Location
Licensing application	Avaya Web License Manager 4.4 and 4.5.5	Optional. You can use the web License Manager installed with one-X Portal
Telephony Switch	Avaya Communications Manager 5.2.1	Avaya one-X Portal Server machine computer used by one-X Portal administrator.
Messaging Application	Avaya Modular Messaging 4.0 and 5.2 all with MSS.	

CTI Application	Avaya enablement service 4.2.2 and 5.2	Uses DMCC and TSAPI connections through Application Enablement Services.
Conferencing Application	• Avaya Meeting Exchange 4.1.2 • Avaya Meeting Exchange 5.2	If the telephone service is not installed at the same time as the Bridge Conference service, one-X Portal users must initiate all bridge conferences from their telephones.
Presence Application	Avaya Intelligent Presence Service 1.0	
Enterprise authentication	• Microsoft active directory service for Windows 2003 Server, SP1. • Microsoft active directory service for Windows 2008. • IBM Domino Server 7.0 • Novell eDirectory 8.8 SP1 • SUN ONE Directory Server 5.2, 6.3	

Software for one-X Portal Applications and one-X Portal Extensions

Software	**Windows XP**	**Windows Vista/7**	**Apple OS X**	**RHEL Desktop**
Operating System	Microsoft Windows XP SP2	Microsoft Windows Vista	Apple OS X V10	Red Hat Enterprise Linux Desktop 4, update 4, 32 bit
Web Browser	• Mozilla Firefox 3.0 • Microsoft Internet Explorer 6.0	• Mozilla Firefox 3.0 • Microsoft Internet Explorer 7.0	• Apple Safari 3.1, 3.2 and 4.0	Mozilla Firefox 3.0

Software	Windows XP	Windows Vista/7	Apple OS X	RHEL Desktop
	SP2, 7.0, 8.0 • Safari 3.2 and 4.0	and 8.0 • Safari 3.2 and 4.0		
Email application	Microsoft Outlook 2003 and 2007	Microsoft Outlook 2004 and 2007	Not supported	Not supported
SMS Application	SMS Client software	SMS Client software	Not supported	Not supported
VoIP (this computer)	Software installed with one-X Portal	Software installed with one-X Portal	Software installer with one-X Portal	Not supported
Avaya one-X Portal Extensions	When installed from one-X Portal or via SMS	When installed from one-X Portal or via SMS	When installed from one-X Portal	Not supported

Presence States expected behavior

Input						Output	
User	**1XP**	**1XM**	**1XC**	**OCS**	**AES**	**Jelly Bean**	**Message**
Available	-					Available	
Busy	-					Busy	
Out of Office	-					Out of Office	
Unavailable	-					Unavailable	
Appear Offline	-					Offline	
Automatic	Away	Away	Away	Away	On-hook	Busy	Away
Automatic	Away	Away	Away	Busy	On-hook	Busy	
Automatic	Away	Away	Away	Do not Disturb	On-hook	Busy	
Automatic	Away	Away	Away	Offline	On-hook	Busy	Away
Automatic	Away	Away	Away	Appear Offline	On-hook	Busy	Away
Automatic		-	-	Away	On-hook	Available	
Automatic		-	-	Busy	On-hook	Busy	
Automatic		-	-	Do not Disturb	On-hook	Busy	
Automatic		-	-	Offline	On-hook	Available	
Automatic		-	-	Appear Offline	On-hook	Available	
Automatic	-		-	Away	On-hook	Available	

Input						Output	
User	**1XP**	**1XM**	**1XC**	**OCS**	**AES**	**Jelly Bean**	**Message**
Automatic	-		-	Busy	On-hook	Busy	
Automatic	-		-	Do not Disturb	On-hook	Busy	
Automatic	-		-	Offline	On-hook	Available	
Automatic	-	-	-	Appear Offline	On-hook	Available	
Automatic	-	-		Away	On-hook	Available	
Automatic	-	-		Busy	On-hook	Busy	
Automatic	-	-		Do not Disturb	On-hook	Busy	
Automatic	-	-		Offline	On-hook	Available	
Automatic	-	-		Appear Offline	On-hook	Available	
Automatic	-	-	-	Away	Off-hook	Busy	On-a-cell
Automatic	-	-	-	Busy	Off-hook	Busy	On-a-cell
Automatic	-	-	-	Do not Disturb	Off-hook	Busy	On-a-cell
Automatic	-	-	-	Offline	Off-hook	Busy	On-a-cell
Automatic	-	-	-	Appear Offline	Off-hook	Busy	On-a-cell

Troubleshooting

This section describes solutions for problems you may encounter while using one-X Portal, organized by component.

- Troubleshooting the one-X Portal installation
- Troubleshooting the one-X Portal servers
- Troubleshooting the one-X Portal administration
- Troubleshooting the one-X Portal client

Troubleshooting the one-X Portal installation

This section describes solutions for the following problems that you might encounter with the one-X Portal installation:

- In an upgrade install custom log settings removed

In an upgrade install, custom log settings removed

Problem: After upgrading one-X Portal from version 1.1 to 5.2.2, the custom log settings that were set prior to the upgrade were removed from the log settings in the Administration Web Client.

Solution: Reset your custom log settings:

1. In the **Administration Web Client**, select the **Services** tab.
2. From the left pane, select **Logging.**
3. The **Logging Configuration** page displays the configuration parameters for logging.
4. Enter the appropriate information and click **Save** to configure your settings.

Note:

For information about the configuration parameters, see the *Administration Application Online Help.*

Troubleshooting one-X Portal servers

This section describes solutions for the following problems that you might encounter with the one-X Portal servers:

- Postgres database contains 2 entries for the same presently

Postgres database contains 2 entries for the same presentity

Problem: Under some conditions, the Postgres database has 2 entries for the same presentity. One of these conditions exists when changes to the user state are taken by the IPS. The Portal Client changes accordingly, but presence for the AES does not contain the <class> element.

Solution: To resolve the issue, run the stop.sh script to clean the database. This script takes down the IPS, so it should be executed after business hours.

1. Start the one-X Portal Administration Application.
2. At the **Servers** tab, select the **Presence** server.
3. Stop the **Presence** server.
4. From the command line go to /opt/IPS/jabber/presence/bin.
5. Execute the stop.sh script.
6. Return to the one-X Portal Administration Application, restart the **Presence** server.

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

Troubleshooting one-X Portal administration

This section describes solutions for the following problems that you might encounter when you are administering one-X Portal:

- Need to synchronize the directory to provision a user
- Database backup through Admin is not working

Need to synchronize the directory to provision a user

Problem: After adding a user to the Enterprise Directory, you must add that user to the Presence group and synchronize the Enterprise Directory before you can provision the user for one-X Portal.

Solution: To synchronize the Enterprise Directory:

1. In the **Administration Web Client,** select the **Scheduler** tab.
2. From the left pane, select **Enterprise Directory Synchronization.**
3. In the **Enterprise Directory Synchronization** window, click **Run Full Sync Now.**
4. In the **Full Backup Schedule Mode** field, select from the schedule parameters.
    a. Daily
    b. Weekly
    c. Monthly
5. In the **Backup File to Location** field, enter the path name of the directory in which to store the database backup.
6. Click **Run Now.**
7. Provision the user for one-X Portal at the **User** tab.

Database backup through Admin is not working

Avaya one-X Portal has the capability of doing a database backup. One of the parameters of the database backup configuration is the directory into which the backup should be saved. If the specified directory is not writable by the “dbinst” user, the backup will fail.

Troubleshooting one-X Portal client

This section describes solutions for the following problems that you might encounter when using the one-X Portal Client:

- Use initial login when changing phone settings

Use initial login when changing phone settings

Problem: When a user changes phone settings, the user should use the original setup and not redo operations (such as logging in) or change Phone Control on one-X Portal. For example, if a user changes the phone settings from This Computer to Other Phone, the user should not log into or change Phone Control on Other Phone if that user is already logged in to This Computer.

Solution: The user can now turn the **Do Not Disturb EC500**, and **Forward** Phone Control settings on or off while logged into a specific phone. The user still cannot change the **Place and receive calls using** setting without causing errors.

The user should not redo operations like logging in.

Note: The troubleshooting issues related to one-X Portal administration described in this readme and in the troubleshooting document are not exhaustive and you need to refer the administration guide to know the other functions.

Technical Support

Support for one-X Portal is available through Avaya Technical Support. If you encounter trouble with one-X Portal:

1. Retry the action. Follow the instructions in written or online documentation carefully.
2. Check the documentation that came with your hardware for maintenance or hardware-related problems.
3. Note the sequence of events that led to the problem and the exact messages displayed. Have the Avaya documentation available.
4. If you continue to have a problem, contact Avaya Technical Support by:
    - Logging on to the Avaya Technical Support Web site http://www.avaya.com/support
    - Calling or faxing Avaya Technical Support at one of the telephone numbers in the Support Directory listings on the Avaya support Web site.

    You may be asked to email one or more files to Technical Support for analysis of your application and its environment.

    Note:

    If you have difficulty reaching Avaya Technical Support through the above URL or email address, please go to http://www.avaya.com for further information.

When you request technical support, provide the following information:

- Configuration settings
- Usage scenario, including all steps required to reproduce the issue.
- Screenshots, if the issue occurs in the Administration Application, end-user web site or Portal clients.
- Copies of all logs related to the issue.
- All other information that you gathered when you attempted to resolve the issue.

Tip:
Avaya Global Services Escalation Management provides the means to escalate urgent service issues. For more information, see the Escalation Contacts listings on the Avaya Web site.

For information about patches and product updates, see the Avaya Technical Support Web site http://www.avaya.com/support.

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