one-X™ Portal 1.1.4

Release Notes

one-X Portal 1.1, Service Pack #4
Issue 1
July 29, 2009

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 gents, 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 Website: 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 Web site:
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

Getting Started

Avaya one-X Portal Service Pack is a maintenance release that includes customer found defect fixes, language support, and/or roll-up of patches. Delivered updates are cumulative, meaning they include all fixes up to the current version as well. This means that prior Service Packs to the release need not be installed before installing this most recent version. Installing this Service Pack brings your one-X Portal installation to the latest release of the software.

Please review this release notes prior to installing one-X Portal Server Service Pack software. The pre-installation and post-installation notes are grouped as follows:

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 1.1 Service Pack 4** from the drop-down menu.
6. Select the appropriate download.

Installing one-X Portal 1.1, Service Pack 4

Prerequisites:

1. 1XP 1.1 GA build should be installed on your system
2. 1xp_update-1.1.4.0.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-1.1.4.0.x.tar.gz to /opt/avaya/1xp directory
4. Untar the update using the following command:
   `tar -xzf 1xp_update-1.1.4.0.x.tar.gz`
   The update contents will be extracted to /opt/avaya/1xp/updates/current directory.
   The following files get extracted:
   `upgrade (directory)`
   `acp-l10n.jar`
   `earlist.txt`

```
ears.tar.gz
install.sh
jarlist.txt
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/1.1.4.0.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_1_1.ear	http://*server.domain.com*/1xp/adapter-presence/version.jsp
1XP_Adapter_CM_1_1.ear	http://*server.domain.com*/1xp/adapter-cm/version.jsp
1XP_Adapter_MX_1_1.ear	http://*server.domain.com*/1xp/adapter-mx/version.jsp
1XP_Admin_Client_1_1.ear	http://*server.domain.com*/1xp/admin/version.jsp
1XP_Portal_Client_1_1.ear	http://*server.domain.com*/1xp/portalclient/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: **1.1.4.0.6**

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*/1xp/portalclient
   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 Clilent.

Uninstalling the update

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/1.1.4.0.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_1_1.ear	http://*server.domain.com*/1xp/adapter-presence/version.jsp
1XP_Adapter_CM_1_1.ear	http://*server.domain.com*/1xp/adapter-cm/version.jsp
1XP_Adapter_MX_1_1.ear	http://*server.domain.com*/1xp/adapter-mx/version.jsp
1XP_Admin_Client_1_1.ear	http://*server.domain.com*/1xp/admin/version.jsp
1XP_Portal_Client_1_1.ear	http://*server.domain.com*/1xp/portalclient/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 1.1.4. The following table outlines the Internal Versions based on prior releases:

Application	1.1 GA	1.1.1	1.1.2	1.1.3
1XP_Adapter_APAS_1_1.ear	1.1.0.0.159	1.1.1.0.10	1.1.2.0.1	1.1.3.0.9
1XP_Adapter_CM_1_1.ear	1.1.0.0.159	1.1.1.0.10	1.1.2.0.1	1.1.3.0.9
1XP_Adapter_MX_1_1.ear	1.1.0.0.159	1.1.1.0.10	1.1.2.0.1	1.1.3.0.9
1XP_Admin_Client_1_1.ear	1.1.0.0.159	1.1.1.0.10	1.1.2.0.1	1.1.3.0.9
1XP_Portal_Client_1_1.ear	1.1.0.0.159	1.1.1.0.10	1.1.2.0.1	1.1.3.0.9

WebSphere security adjustments relative to one-X Portal 1.1

This section addresses the two issues which may arise during one-X Portal 1.1 deployments. This information was first delivered with one-X Portal 1.1.1, so may not be new to your installation. If you have already taken care of issues outlined in this section due to installation of a prior update, you can skip this section now.

1. Creating new WebSphere certificate after upgrade from one-XP 1.0 to one-XP 1.1
   - In this scenario, WebSphere is upgraded from 6.0 to 6.1, which means original WebSphere certificates are preserved
   - WebSphere 6.0 certificates are set with CN=jserver, which does not match machine's FQDN and causes browser to constantly advise about "invalid" certificate. Even if "jserver" certificate is loaded to browser's certificate store, depending on the browser the warning will continue to display the next time a connection is attempted to 1XP.
     The solution is to replace the "jserver" certificate with a self-signed certificate.

   Note: on fresh installs WebSphere 6.1 creates a certificate with appropriate CN
2. Replacing WebSphere 6.1 certificate
   - Some customers do want to create their own certificate, or periodically replace the self-signed certificate which comes with WebSphere. One might create a new certificate in WebSphere, but it needs to be made active in WebSphere.

The subsequent sections are broken down in sequence of steps required to fulfill the above requirement.

Creating a new certificate

On a fresh one-X Portal 1.1 installation, this is already done during WebSphere installation. This procedure is recommended when you upgrade from one-X Portal 1.0 to 1.1 or higher.

1. Login as Administrator to WebSphere console
2. Go to **Security** > **SSL Certificate and Key Management**
3. Go to **Key Stores and Certificate**
   a. Click **NodeDefaultKeyStore**
   b. Click **Personal Certificates**
   c. Press **Create a Self-signed Certificate**
   d. Enter certificate alias (suggestion "default")
   e. Enter FQDN for this machine
   f. Enter Organization name
   g. Enter other optional values
   h. Click **OK**
   i. Save configuration
4. Reference section **Extract a Certificate** and extract the certificate just created
5. Reference section **Add a Certificate** and add the certificate above to NodeDefaultTrustStore
6. Reference section **Activate a Certificate** and follow the steps described in Extracting a certificate.

Extracting a certificate

One can extract a certificate from key or trust stores. This procedure is constructed using NodeDefaultKeyStore as the starting point.

1. Login as Administrator to WebSphere console
2. Go to **Security** > **SSL Certificate and Key Management**
3. Click **Key Stores and Certificates**
4. Click **NodeDefaultKeyStore**
5. Click **Personal Certificates**
6. Select the certificate to extract
7. Press **Extract**
    a. Enter file name (suggestion: “\tmp\default.pem”)
    b. Click **OK**

Adding a certificate

In order for a certificate to be used as a default WebSphere certificate, it needs to exist in key (Personal) and trust (Signer) stores. The procedure is created using NodeDefaultTrustStore, as starting point:

1. Login as Administrator to WebSphere console
2. Go to **Security** > **SSL Certificate and Key Management**
3. Click **Key Stores and Certificates**
4. Click **NodeDefaultTrustStore**
    a. Click **Signer Certificates**
    b. Click **Add**
    c. Enter alias for this certificate
    d. Enter file name where certificate is located
    e. Click **OK**
    f. Save configuration

Activating a certificate

1. Log on as Administrator to WebSphere console
2. Go to **Security** > **SSL Certificate and Key Management**
3. Go to **SSL Configurations**
4. Click **NodeDefaultSSLSettings**
5. Press **Get Certificate Aliases**
6. Select default server and client aliases
7. Click **OK**
8. Save configuration
9. Restart WebSphere

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.

Changes delivered with one-X Portal 1.1.4

Avaya one-X Portal 1.1, Service Pack 4 Release Notes

The one-X Portal updates are cumulative. The one-X Portal 1.1, Service Pack 4 release notes includes modifications and enhancements specific to one-X Portal 1.1, Service Pack 4 and from earlier releases. The changes delivered are grouped as follows:

Enhancements

This Service Pack contains additional support for the following languages: Spanish, Italian, Korean, Dutch, Portuguese, Russian, French, German, Japanese, and Chinese (Simplified). This language support was added to Portal Client, Portal Client On-Line Help, and the Portal Extensions.

Problems fixed in one-X Portal 1.1, Service Pack 4

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

Issue ID	Problem
wi00313342	T-Mobile setParticipantName() causing overload on MX
wi00304127	Participant name not changed after renaming it for MX 5.1 and MX 5.0
wi00307761	ACPResourceUnavailableException errors when requesting setControlMode
wi00329054	Change the case of the "milpitasdev" switch to match the AES configuration

Problems fixed in updates prior to one-X Portal 1.1.4 that are included

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

Issue ID	Problem
wi00110806	Bridge number is not being updated through CLI.
wi00288767	Contact Service is not filling in the primary phone when AcpContact.getContactByUserId is used
wi00302086	I18n: When Legal Disclaimer link is long and wraps it overlaps box...just need to make box a bit bigger.
wi00302080	I18n: Label on the Call Details window is getting cut off.
wi00301776	When a Bridge Conference Starts when the Bridge Conference Window is

	open it can cause 1XP to hang
wi00301400	Need for 1.1.3 - The fix put in to not do unconstrained Searches has broken 1XC's fetch of Personal Contacts
wi00300958	Client Side changes: Specifying another phone number to be the caller ID on emergency calls is not working using voip
wi00299743	Placeholder shown in tooltip on welcome screen
wi00299742	The buttons to the right of the Start Bridge Conference window are cut off a little
wi00299741	Names of service states appearing in Status Bar messages are not Internationalized
wi00296334	Continuous call logs stop working after a server down and the user is using 1XC
wi00292398	Phantom Call appearance on CM adaptor restart (SP1)
wi00246247	No incoming and outgoing call appearance after CMAdaptor restart.
wi00052928	Settings Font Size needs to have supported range limit
wi00300045	Specifying another phone number to be the caller ID on emergency calls is not working using voip
wi00298418	Conference participants that are resolved, but not logged into 1XP do not get their userid passed up appropriately
wi00296446	Extension numbers encoded as SIP end point cause MX to fail participant identification
wi00295618	QQ 142961 Contact Domain configuration doesn't allow import of contacts from the defined contact domain
wi00293748	We need to ensure the Admin CLI can deal with MBCS users, handles, etc...
wi00293425	Contact Service should not import empty phone numbers
wi00293422	Contact Service should return empty set immediatly if search criteria is empty or null
wi00278877	WI for delivering the Localized files for 1.1 Language Patch for Portal Client
wi00304284	Client Portal Side - Need to update the certificate of that is associated with our ActiveX controls
wi00288648	Repackage WebLM with latest version
wi00307018	MX 5.1 jars report memory leak with OOM < 1 day
wi00306500	Some times the normal client login throws error "The service that supports your telephone has now recovered..." and finally GUI become inactive/unfriendly for any 1XP activity
wi00305527	Admin and Portal Clients need to be tweaked to allow Apple SSO solution to work
wi00280092	WI for resolving Internationalization issues in Portal Client for 1.1 Language Patch
wi00292809	Notes in Japanese are not propagated from client to client

wi00116281	External callers to a conf bridge are showing up as one user name
wi00282835	Incorporate DND reporting to Presence Adapter
wi00284484	Re-assess publication expiration timeouts for extended absence periods of time
wi00284771	Large amounts of JTAPI threads are creating a native out of memory crash - 1X code changes
wi00284772	Large amounts of JTAPI threads are creating a native out of memory crash - Upgrade CMAPI libraries
wi00285137	Incorporate latest LPS to 1X
wi00284773	Large amounts of JTAPI threads are creating a native out of memory crash - Change the version of AES Supported
wi00247812	Cannot Login into the client in first attempt using THIS computer Mode
wi00283371	Show on call when in dialing state
wi00289502	1XP1.1 does not integrate with MX5.1

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.