



Upgrading to Avaya Aura Experience Portal 7.0.1

Release 7.0.1
April 2015

© 2014 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 may generally make available to users of its products and Hosted Services. 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 Avaya hardware and software. 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://support.avaya.com> or such successor site as designated by Avaya. Please note that if you acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTP://SUPPORT.AVAYA.COM/LICENSEINFO](http://support.avaya.com/licenseinfo) OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. 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 CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The

applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. "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. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

License types

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of 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, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, 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.

Virtualization

Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service 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"). As required, 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 products, Documentation or on Avaya's website at: <http://support.avaya.com/Copyright> or such successor site as designated by Avaya. 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://support.avaya.com> or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

Avaya, the Avaya logo, Avaya Aura® Experience Portal, Avaya Aura® Communication Manager, and Avaya Aura® Orchestration Designer 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. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: <http://support.avaya.com>, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: <http://support.avaya.com> for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: <http://support.avaya.com> (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction	7
Purpose	7
Intended audience	7
Related resources	7
Documentation	7
Viewing Avaya Mentor videos	8
Support	9
Chapter 2: Avaya Aura Experience Portal system upgrade overview	10
System upgrade overview	10
Upgrading a system that uses Avaya Enterprise Linux	11
Upgrading the Primary EPM on Avaya Enterprise Linux	11
Upgrading an Auxiliary EPM on Avaya Enterprise Linux	11
Upgrading a Media Processing Platform (MPP) on Avaya Enterprise Linux	12
Upgrading a single server Experience Portal system on Avaya Enterprise Linux	12
Upgrading a system that uses Red Hat Enterprise Linux Server	13
Upgrading the Primary EPM on Red Hat Enterprise Linux Server	13
Upgrading an Auxiliary EPM on Red Hat Enterprise Linux Server	15
Upgrading a Media Processing Platform (MPP) on Red Hat Enterprise Linux Server	16
Upgrading the single server Experience Portal system on Red Hat Enterprise Linux Server	17
Chapter 3: Upgrading the operating system	19
Operating system upgrade overview	19
Backing up data	20
Preparing to connect to Avaya Enterprise Linux using a crossover Ethernet cable	21
Upgrading Avaya Enterprise Linux using an ISO image file	22
Upgrading Avaya Enterprise Linux from the software installation DVD	25
Upgrading Red Hat Enterprise Linux Server on the dedicated EPM server	29
Upgrading Red Hat Enterprise Linux Server on a dedicated MPP server	31
Upgrading Red Hat Enterprise Linux Server on a single server system	33
Taking an MPP offline using the EPM Web interface	36
Stopping the MPP service	37
Preventing loss of reporting data prior to upgrading MPP	37
Chapter 4: Software upgrade prerequisites	38
Prerequisites overview for upgrading Experience Portal	38
Minimum server hardware requirements	40
Disk space requirements	41
Space requirement for upgrading the primary EPM on Red Hat Enterprise Linux	41
Space requirement for upgrading the primary EPM on Avaya Enterprise Linux	41
License Requirements	42

Verifying the Linux version number.....	43
Installing the Oracle JDBC driver.....	44
Verifying communication between the upgraded Experience Portal servers.....	45
Ensuring that Email messages are processed during upgrades.....	47
Ensuring that SMS messages are processed during upgrades.....	47
Copying and restoring the backup files on Red Hat Enterprise Linux Server.....	48
Checking for stale or hung mount points.....	49
Verifying server time synchronization.....	49
Updating the external database configuration.....	50
Chapter 5: Upgrading the EPM and MPP software on different servers.....	52
Upgrading the Primary EPM server.....	52
EPM software upgrade overview.....	52
Automatically upgrading the Primary EPM software.....	53
Upgrading the Primary EPM software interactively.....	57
Upgrading an Auxiliary EPM server.....	66
Auxiliary EPM software upgrade overview.....	66
Upgrading the Auxiliary Experience Portal software interactively.....	67
Upgrading the MPP software.....	75
MPP software upgrade overview.....	75
Reestablishing the link between the EPM and the upgraded MPP.....	77
Customizing the MPP silent install file for all MPPs.....	78
Upgrading the MPP software silently.....	78
Upgrading the MPP software interactively.....	82
Automatically upgrading the MPP software.....	88
Chapter 6: Upgrading the Experience Portal software on a single server.....	93
Experience Portal software upgrade on a single server overview.....	93
Upgrading the Experience Portal software interactively on a single server.....	94
Reestablishing the link between the EPM and the MPP.....	103
Chapter 7: Optional: Updating the co-resident application server.....	105
Chapter 8: Configuring and testing an upgraded Avaya Aura Experience Portal system.....	108
Avaya Aura® Experience Portal system configuration overview for a system upgraded to 7.0.1 ..	108
Avaya Services access changes between 5.1, 6.0, or 7.0 and 7.0.1 ..	109
Upgrading the Experience Portal license.....	109
Running the sample application.....	110
Configure and run the Application Interface test client.....	111
Configuring Experience Portal for outcall.....	112
Running the Application Interface test client VAppIntfClient.sh ..	112
Testing an individual MPP.....	113
External time sources.....	115
Configuring the Primary EPM server to point to an external time source.....	115
Non-English language support.....	117
Non-English character support on the EPM web pages.....	117

Chapter 9: Troubleshooting upgrade issues	121
Upgrade installation log files	121
Primary EPM root certificate is signed with a weak hashing algorithm warning	123
Fixing Prerequisite Checker failures	123
Prerequisite Checker fails with UnknownHostException:localhost	123
Fixing Prerequisite Installer failures	124
Sample Prerequisite Installer error message	126
Identifying RPM issues	127
Installation Progress Bar stops at 25% completed	128
EPM upgrade finishes with an Axis error	130
Upgrade hangs at Post Installation Summary screen	131
MPP upgrade is hanging	131
MPP or Auxiliary EPM could not import EPM key	132
Changing the Product ID for an existing Experience Portal system	133
Invalid password for database user	134
Time synchronization problems	134
Reloading the Experience Portal environment variables	139
Recovering Avaya Enterprise Linux configuration information after an upgrade	139
Restoring the previous operating system after an upgrade	140
Restore the 5.1, 6.0, or 7.0 software on Avaya Enterprise Linux	140
Restoring the 5.1, 6.0, or 7.0 software on a dedicated Primary EPM server or a single-server EPM system running Red Hat Enterprise Linux Server	144
Restoring the 5.1, 6.0, or 7.0 software on an Auxiliary EPM server running Red Hat Enterprise Linux Server	145
Restoring a dedicated 5.1, 6.0, or 7.0 MPP server on Red Hat Enterprise Linux Server	145
Chapter 10: Preupgrade worksheets	147
Primary EPM server upgrade worksheet	147
Auxiliary EPM server upgrade worksheet	150
MPP server upgrade worksheet	153
Single EPM server upgrade worksheet	155

Chapter 1: Introduction

Purpose

This document describes how to upgrade to Avaya Aura® Experience Portal 7.0.x

Anyone who upgrades and configures the Avaya Aura® Experience Portal system must read and understand the information in this document.

Intended audience

This document is intended for anyone who is involved with installing, configuring, and upgrading Avaya Aura® Experience Portal. The audience includes and is not limited to implementation engineers, field technicians, business partners, solution providers, and customers.

Related resources

Documentation

The following table lists the documents related to Experience Portal. Download the documents from the Avaya Support website at <http://www.avaya.com/support>:

Title	Description	Audience
<i>Implementing Avaya Aura® Experience Portal on multiple servers</i>	Provides procedures to install and configure Avaya Aura® Experience Portal software on two or more dedicated servers.	Implementation engineers
<i>Implementing Avaya Aura® Experience Portal on a single server</i>	Provides procedures to install and configure the Avaya Aura® Experience Portal software on a single server.	Implementation engineers

Table continues...

Title	Description	Audience
<i>Deploying Avaya Aura® Experience Portal in an Avaya Customer Experience Virtualized Environment</i>	Provides procedures for deploying the Experience Portal virtual application in the Avaya Customer Experience Virtualized Environment. This document includes installation, configuration, initial administration, troubleshooting, and basic maintenance checklists and procedures.	Implementation engineers
<i>Troubleshooting Avaya Aura® Experience Portal</i>	Provides general information about troubleshooting and resolving system problems. This document also provides detailed information and procedures for finding and resolving specific problems.	Implementation engineers
<i>Administering Avaya Aura® Experience Portal</i>	Provides general information about and procedures for administering and configuring specific Avaya Aura® Experience Portal functions and features using a web-based interface.	Implementation engineers

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

Procedure

- To find videos on the Avaya Support website, go to support.avaya.com and perform one of the following actions:
 - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
 - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
 - Enter a key word or key words in the Search Channel to search for a specific product or topic.

- Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

 Note:

Videos are not available for all products.

Support

Go to the Avaya Support website at <http://support.avaya.com> for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Chapter 2: Avaya Aura Experience Portal system upgrade overview

System upgrade overview

You can upgrade to Experience Portal 7.0.1 from the following versions:

- Voice Portal 5.1 SP3
- Experience Portal 6.0
- Experience Portal 7.0

For an Experience Portal system that includes multiple zones, Avaya recommends that you upgrade Experience Portal on a zone by zone basis. That is, you upgrade the servers in one zone before upgrading the servers in a different zone. Once the zone is fully upgraded, the zone is fully operational. However, Avaya recommends that once you start upgrading a system, upgrade all zones as soon as possible to avoid any compatibility issues that might occur.

Experience Portal supports upgrades without service interruption and without loss of data. To support an upgrade without service interruption the system must have more than a single MPP. With a single MPP, there will be service interruption but there will not be any loss of data.

Experience Portal supports upgrades from servers that are provided with Voice Portal 5.1 and Experience Portal 6.0; IBM 3550 and HP DL 360 G7 respectively.

 Note:

The upgrade procedure for systems that use Avaya-provided Linux is different from the upgrade procedure for systems that use customer-provided Red Hat Enterprise Linux.

Upgrading a system that uses Avaya Enterprise Linux

Upgrading the Primary EPM on Avaya Enterprise Linux

Before you begin

1. If you use an external database for reports, upgrade the external database schema before upgrading the Experience Portal components. For more information, see [Updating the external database configuration](#) on page 50.
2. Verify that the prerequisites have been met. For more information, see [Software upgrade prerequisites overview for upgrading to Experience Portal](#) on page 38.

About this task

This topic provides information about the tasks that you must perform to upgrade the Primary EPM server.

Procedure

1. Upgrade Avaya Enterprise Linux on the Primary EPM server. For more information, see [Upgrading Avaya Enterprise Linux from the software installation DVD](#) on page 25 or [Upgrading Avaya Enterprise Linux using an ISO image file](#) on page 22.

Upgrading from ISO image file is not supported for upgrades from Voice Portal 5.1 SP3.

2. Upgrade the Primary EPM software to Experience Portal 7.0.1.

For more information, see [Automatically upgrading the Primary EPM software](#) on page 53.

Upgrading an Auxiliary EPM on Avaya Enterprise Linux

Before you begin

Verify that the prerequisites have been met. For more information, see [Software upgrade prerequisites overview for upgrading to Experience Portal](#) on page 38.

About this task

This topic provides information about the tasks that you must perform to upgrade an Auxiliary EPM server.

Procedure

1. Upgrade Avaya Enterprise Linux on the Auxiliary EPM server. For more information, see [Upgrading Avaya Enterprise Linux from the software installation DVD](#) on page 25 or [Upgrading Avaya Enterprise Linux using an ISO image file](#) on page 22.

Upgrading from ISO image file is not supported for upgrades from Voice Portal 5.1 SP3.

2. Upgrade the Auxiliary Experience Portal system to Experience Portal 7.0.1.

For more information, see [Automatically upgrading the Primary EPM software](#) on page 53.

Upgrading a Media Processing Platform (MPP) on Avaya Enterprise Linux

Before you begin

Verify that the prerequisites have been met. For more information, see [Software upgrade prerequisites overview for upgrading to Experience Portal](#) on page 38.

About this task

This topic provides information about the tasks that you must perform to upgrade an MPP server.

Procedure

1. Change the state of the MPP to offline. For more information, see [Taking an MPP offline using the EPM Web interface](#) on page 36.
2. Upgrade Avaya Enterprise Linux on the MPP server. For more information, see [Upgrading Avaya Enterprise Linux from the software installation DVD](#) on page 25 or [Upgrading Avaya Enterprise Linux using an ISO image file](#) on page 22.
3. Upgrade the MPP to Avaya Aura® Experience Portal 7.0.1.
For more information, see [Automatically upgrading the MPP software](#) on page 88.
4. Log on to the EPM Web interface.
5. Navigate to the **MPP Manager** page, and change the mode of the MPP to **Online**.
6. On the **MPP Manager** page, click **Start** to start the MPP server.

Upgrading a single server Experience Portal system on Avaya Enterprise Linux

Before you begin

Verify that the prerequisites have been met. For more information, see [Prerequisites overview for upgrading Experience Portal](#) on page 38.

About this task

This topic provides information about the tasks that you must perform to upgrade a single server Experience Portal system.

Procedure

1. Change the mode of the MPP server to **Offline**. For more information, see [Taking an MPP offline using the EPM Web interface](#) on page 36.
2. Upgrade Avaya Enterprise Linux on the Experience Portal system. For more information, see [Upgrading Avaya Enterprise Linux from the software installation DVD](#) on page 25 or [Upgrading Avaya Enterprise Linux using an ISO image file](#) on page 22.

3. Upgrade the Experience Portal software to Avaya Aura® Experience Portal 7.0.1.
For more information, see [Automatically upgrading the Primary EPM software](#) on page 53.
4. Log on to the EPM Web interface.
5. Navigate to the **MPP Manager** page, and change the mode of the MPP to **Online**.
6. On the **MPP Manager** page, click **Start** to start the MPP.

Upgrading a system that uses Red Hat Enterprise Linux Server

Upgrading the Primary EPM on Red Hat Enterprise Linux Server

Before you begin

Verify that the prerequisites have been met. For more information, see [Prerequisites overview for upgrading Experience Portal](#) on page 38.

About this task

Perform the following steps to upgrade the Primary EPM server that uses the customer-provided Red Hat Enterprise Linux Server.

Procedure

1. Create a backup of the Experience Portal system.
Save the backup folder to an external server that is not part of the Experience Portal system.
For more information, see [Backing up data](#) on page 20.

 Important:

If you upgrade from Experience Portal 7.0 to 7.0.1, database backup is not required for Linux upgrades.

2. If you upgrade to Experience Portal 7.0.1 from versions prior to Experience Portal 7.0, you must do a fresh installation of a supported version of Red Hat Enterprise Linux Server. For more information, see [Upgrading Red Hat Enterprise Linux Server on the dedicated EPM server](#) on page 29.

If you upgrade from Experience Portal 7.0 to 7.0.1, you can select the **Upgrade an Existing Installation** option and follow the upgrade procedure.

 Important:

Ensure that you assign the same host name and IP address to the server that you assigned to the server before the upgrade.

3. Disable the firewall on the Experience Portal server.
4. Disable SELinux on the Experience Portal server.
5. If you upgrade to Experience Portal 7.0.1 from versions prior to Experience Portal 7.0, you must perform the following steps:
 - a. Copy the backup folder to a temporary place on the EPM server.
 - b. Run the `RestoreProps.sh` script to restore the backup files. For more information, see [Copying and restoring the backup files on Red Hat Enterprise Linux Server](#) on page 48.
6. Install the Avaya Aura® Experience Portal 7.0.1 Primary EPM software.

For more information, see [Prerequisites overview for upgrading Experience Portal](#) on page 38 and [Upgrading the Primary EPM software interactively](#) on page 57.

 Important:

Use the interactive upgrade method by running the `installvp` script.

7. Run the `setup_vpms.php` script on each MPP 5.1, 6.0, or 7.0 server to authorize the security certificate, and restart the MPP.
8. Reestablish the communication link between the upgraded EPM and the MPP servers. For more information, see [Reestablishing the link between the EPM and the upgraded MPP](#) on page 77.
9. If the **EPM > Real-time Monitoring > System Monitor** page shows that the MPP needs to be restarted, restart the MPP from the **MPP Manager** page.

 Note:

If your Auxiliary EPM has outcalls in progress, skip the following step.

10. Reestablish the communication link between the upgraded EPM and the Auxiliary EPM servers:
 - a. Log in to Linux on each Auxiliary EPM server.
 - b. Run the `setup_vpms.php` script.
 - c. Log in to the EPM Web interface.
 - d. On the EPM menu, select **EPM Servers**.
 - e. Click the EPM server that you have upgraded.

The system displays the **Change EPM Server** page.
 - f. Select the **Trust new certificate** option.
 - g. Click **Save**.

Upgrading an Auxiliary EPM on Red Hat Enterprise Linux Server

Before you begin

Verify that the prerequisites have been met. For more information, see [Prerequisites overview for upgrading Experience Portal](#) on page 38.

About this task

Perform the following steps to upgrade each Auxiliary EPM system that uses the customer-provided Red Hat Enterprise Linux Server.

Procedure

1. If you upgrade to Experience Portal 7.0.1 from versions prior to Experience Portal 7.0, you must do a fresh installation of a supported version of Red Hat Enterprise Linux Server. For more information, see [Upgrading Red Hat Enterprise Linux Server on the dedicated EPM server](#) on page 29.

If you upgrade from Experience Portal 7.0 to 7.0.1, you can select the **Upgrade an Existing Installation** option and follow the upgrade procedure.

Important:

Ensure that you assign the same host name and IP address to the server that you assigned to the server before the upgrade.

2. Disable the firewall on the Auxiliary Experience Portal server.
3. Disable SELinux on the Auxiliary Experience Portal server.
4. Install the Avaya Aura® Experience Portal 7.0.1 Auxiliary EPM software.

For more information, see [Upgrading the Auxiliary Experience Portal software interactively](#) on page 67.

Important:

You must use the interactive upgrade method by running the `installvp` script. Ensure that when you are prompted for the password to configure the Auxiliary EPM server, enter the same password that you used to upgrade the Primary EPM.

5. Trust the new security certificate for the upgraded Auxiliary EPM by performing the following steps:
 - a. Log in to the EPM Web interface.
 - b. On the EPM menu, select **EPM Servers**.
 - c. Click the Auxiliary EPM server that you upgraded.

The system displays the **Change EPM Server** page.
 - d. Select the **Trust new certificate** option.
 - e. Click **Save**.

6. Restart all the MPPs.

Upgrading a Media Processing Platform (MPP) on Red Hat Enterprise Linux Server

Before you begin

Verify that the prerequisites have been met. For more information, see [Prerequisites overview for upgrading Experience Portal](#) on page 38.

About this task

Perform the following procedure to upgrade each MPP server that uses the customer-provided Linux operating system.

Procedure

1. Log on to the EPM Web interface.
2. **Stop** the MPP from the **MPP Manager** page.
3. Schedule a report data download so that EPM collects all calls records from the MPP server.
For more information, see [Preventing loss of reporting data prior to upgrading MPP](#) on page 37.
4. Take the MPP offline. For more information, see [Taking an MPP offline using the EPM Web interface](#) on page 36.
5. If you upgrade to Experience Portal 7.0.1 from versions prior to Experience Portal 7.0, you must do a fresh installation of a supported version of Red Hat Enterprise Linux Server. For more information, see [Upgrading Red Hat Enterprise Linux Server on the dedicated EPM server](#) on page 29.

If you upgrade from Experience Portal 7.0 to 7.0.1, you can select the **Upgrade an Existing Installation** option and follow the upgrade procedure.

Important:

Assign the same host name and IP address to the server that you assigned to the server before the upgrade.

6. Disable the firewall on the MPP server.
7. Disable SELinux on the MPP server.
8. Install the Experience Portal 7.0.1 MPP software.

For more information, see [Upgrading the MPP software interactively](#) on page 82.

Important:

You must use the interactive upgrade method by running the `installvp` script.

9. Trust the new security certificate for the MPP:
 - a. Log in to the EPM Web interface.
 - b. From the EPM menu, select **MPP Servers**.
 - c. Click the MPP server name that you upgraded.
The system displays the **Change MPP Server** page.
 - d. Select the **Trust new certificate** option.
 - e. Click **Save**.
10. On the EPM Web interface, select the **MPP Manager** menu.
11. Change the mode of the MPP to **Online**.
12. Click **Start** to start the MPP.

Upgrading the single server Experience Portal system on Red Hat Enterprise Linux Server

Before you begin

Verify that the prerequisites have been met. For more information, see [Prerequisites overview for upgrading Experience Portal](#) on page 38.

About this task

Perform the following procedure to upgrade a single server Experience Portal system that uses the customer provided Linux software.

Procedure

1. Log on to the EPM Web interface.
2. On the **MPP Manager** page, click **Stop** to stop the MPP.
3. Schedule a report data download so that EPM collects all calls records from the MPP server.
For more information, see [Preventing loss of reporting data prior to upgrading MPP](#) on page 37.
4. Change the state of the MPP to **Offline**. For more information, see [Taking an MPP offline using the EPM Web interface](#) on page 36.
5. Create a backup of the Experience Portal system.

Ensure that you save the backup folder on an external server that is not a part of the Experience Portal system. For more information, see [Backing up data](#) on page 20.

Important:

If you upgrade from Experience Portal 7.0 to 7.0.1, database backup is not required for Linux upgrades.

6. If you upgrade to Experience Portal 7.0.1 from versions prior to Experience Portal 7.0, you must do a fresh installation of a supported version of Red Hat Enterprise Linux Server. For more information, see [Upgrading Red Hat Enterprise Linux Server on the dedicated EPM server](#) on page 29.

If you upgrade from Experience Portal 7.0 to 7.0.1, you can select the **Upgrade an Existing Installation** option and follow the upgrade procedure.

! Important:

Assign the host name and IP address to the server that you assigned to the server before the upgrade.

7. Disable the firewall on the Experience Portal server.
8. Disable SELinux on the Experience Portal server.
9. If you upgrade to Experience Portal 7.0.1 from versions prior to Experience Portal 7.0, you must perform the following steps:
 - a. Copy the backup folder to a temporary place on the EPM server.
 - b. Run the `RestoreProps.sh` script to restore the backup files. For more information, see [Copying and restoring the backup files on Red Hat Enterprise Linux Server](#) on page 48.
10. Install the Experience Portal 7.0.1 EPM and MPP software.

For more information, see [Upgrading the Experience Portal software interactively on a single server](#) on page 94.

! Important:

You must use the interactive upgrade method by running the `installvp` script.

11. Trust the new security certificate for the MPP:
 - a. Log in to the EPM Web interface.
 - b. From the EPM menu, select **MPP Servers**.
 - c. Click the MPP server name that you upgraded.

The system displays the **Change MPP Server** page.
 - d. Select the **Trust new certificate** option.
 - e. Click **Save**.
12. On the EPM Web interface, select the **MPP Manager** menu.
13. Change the mode of the MPP to **Online**.
14. Click **Start** to start the MPP.

Chapter 3: Upgrading the operating system

Operating system upgrade overview

Important:

If you upgrade from Avaya Aura® Experience Portal 7.0 to 7.0.1:

- Operating system upgrade is optional.
- Avaya recommends that you upgrade the operating system to pick up any security fixes.
- For software-only customers, database backup is not required for Linux upgrades.

To upgrade to Avaya Enterprise Linux 7.0.1:

- Upgrade Avaya Enterprise Linux if you have opted for the Avaya bundled server offer. There are two upgrade methods for Avaya Enterprise Linux:
 - Upgrade using an ISO image file: This upgrade method provides an autoupgrade of Avaya Enterprise Linux.
 - Upgrade with the software installation DVD: This upgrade method provides interactive as well as autoupgrade option to upgrade Avaya Enterprise Linux.

Note:

If you are upgrading a Voice Portal 5.1 system to Experience Portal 7.0.1, use the software installation DVD to upgrade Avaya Enterprise Linux.

- Do a fresh installation of a supported version of Red Hat Enterprise Linux Server if you have opted for the software-only offer and are upgrading from versions prior to Experience Portal 7.0.

If you upgrade from Experience Portal 7.0, you can do an upgrade rather than a fresh install since the Experience Portal 7.0 system is already installed on the 64-bit operating system.

Note:

Red Hat Enterprise Linux Server does not support upgrading from 32-bit to 64-bit versions of Red Hat Enterprise Linux Server.

To save your Experience Portal configuration while doing a fresh installation of a supported version of Red Hat Enterprise Linux Server, ensure that you create a backup of Experience Portal from **System Backup** menu in EPM. Ensure that you save the backup folder on a server that is not part of the Experience Portal system.

For more information about backing up Experience Portal data from the **System Backup** menu in EPM, see the Administering Avaya Aura® Experience Portal guide.

- Upgrade the Primary EPM, Auxiliary EPM, and MPP software after you upgrade the Avaya Enterprise Linux operating system.
- Do a fresh installation of the Primary EPM, Auxiliary EPM, and MPP software after you upgrade the Red Hat Enterprise Linux operating system.

 Important:

- You cannot run an older version of the Experience Portal EPM or MPP software on a server running the upgraded operating system. Therefore, ensure that you upgrade the Primary EPM, Auxiliary EPM, and MPP software to Avaya Aura® Experience Portal 7.0.1.
- Experience Portal 7.0.1 supports outcall using the Axis 2 based Web Service named VPApplntfService. Experience Portal 7.0.1 does not support outcall using the Axis 1.4 based Web Service named ApplntfWS that was supported in prior releases of Experience Portal (6.x and earlier).

Ensure that you upgrade all applications that are using Outcall Axis1.4 based web service named ApplntfWS to instead use Outcall Axis 2 based Web Service named VPApplntfService.

- If your Experience Portal system has Auxiliary EPMs, you can upgrade the Primary EPM while the Auxiliary EPMs continue to process outcalls.

If your Experience Portal system consists of multiple servers, you can upgrade the EPM server operating system and Experience Portal software even while the MPPs are in the running state. In addition, if you have multiple MPPs, you can upgrade an MPP while the other MPPs are in the running state.

Backing up data

About this task

Red Hat Enterprise Linux Server does not support upgrading from 32-bit to 64-bit versions of Red Hat Enterprise Linux Server.

To save your Experience Portal configuration while doing a fresh installation of a supported version of Red Hat Enterprise Linux Server, ensure that you create a backup of Experience Portal.

Procedure

1. Backup the Experience Portal database. For the upgrade procedure, you must use the **System Management > System Backup** menu in the EPM Web interface to create the backup.

For more information on system backup, see *Administering Avaya Aura® Experience Portal*.

2. If you have installed Intelligent Customer Routing (ICR), back up the ICR properties files. For more information, see *Upgrading Intelligent Customer Routing* on the Avaya Support website at <http://support.avaya.com>.
3. If you have manually modified any Voice Portal or Experience Portal properties files, back up those files. You must manually merge the changes after the upgrade is complete.
4. If any Tomcat configuration files in `/opt/Tomcat/tomcat/config` have been manually modified, back up those configurations so that you can manually merge them back after the Experience Portal upgrade is complete.

Preparing to connect to Avaya Enterprise Linux using a crossover Ethernet cable

To install Avaya Enterprise Linux on a server using a crossover connection from a laptop, you must configure the laptop to establish communication between the laptop and the server.

Before you begin

- Install the Avaya provided hardware on the server.
 - Install additional DIMM cards on the server.
 - Ensure that eth1, which is also called port 2, is available for use when you connect to the server using a crossover network cable.
 - Obtain the following equipment for the remote connection:
 - Telnet client and secure shell (SSH) client programs installed on the laptop.
-  **Note:**
- puTTY is a popular, free program that can function as both a Telnet client and as an SSH client.
- A crossover Ethernet or a CAT5 network cable that connects the laptop to the Services port on the server, eth1.

About this task

Use the procedure to prepare the laptop to connect to Avaya Enterprise Linux using a crossover Ethernet cable.

Procedure

1. Connect a crossover Ethernet (or CAT5) network cable from the laptop to the temporary services port eth1.

 Note:

The eth1 port is also called port 2.

2. Configure the laptop with the following settings:

```
ipaddress=192.11.13.5
```

```
netmask=255.255.255.252
```

```
gateway=192.11.13.4
```

3. Verify link connectivity between the system and the server.
 - a. At the command line prompt, enter the `ping 192.11.13.6` command.
 - b. Check the LED on the temporary Services port and the LED on the network card of the laptop.

The LED light flashes green when the link is connected.
 - c. The screen displays the response from the server that shows that the server is operational.
4. Insert the Enterprise Linux Installer software into a DVD drive on the Experience Portal server.
5. Reboot the server so that the server starts from the Avaya Enterprise Linux Installer software.

Next steps

Install or upgrade Avaya Enterprise Linux.

Upgrading Avaya Enterprise Linux using an ISO image file

Before you begin

- The upgrade requires 2GB free space in the /var directory to copy temporary files for the operating system upgrade. This space requirement is in addition to the space that is required for the database upgrade and migration of data, and will be proportional to the pre-upgrade volume of data. If the free space is not available in the /var directory, the installer does not proceed with the operating system installation.
- Note the Fully Qualified Filename (FQFN) of the Avaya Aura® Experience Portal 7.0.1 Linux Installer ISO image. During the installation process, the installer prompts for the FQFN of the ISO image.
- Ensure that no network cable is connected to the maintenance port (eth1) of the server. The installer runs the autoupgrade utility while upgrading Avaya Enterprise Linux without media.
- If you plan to use a direct connection to upgrade Avaya Enterprise Linux, connect a keyboard and monitor to the server.

Warning:

If the upgrade fails, you might require physical access to the server in order to return the server to a working state.

Important:

If you have installed a Tomcat application server on the Experience Portal server, the software on the Application server might get deleted during the operating system upgrade. Back up the

configuration files, data files, Web applications, libraries, and binaries from the directory where the Application server is installed. For more information about the required backup files, contact the application developer.

About this task

Use this procedure to upgrade Avaya Enterprise Linux using an ISO image file. The upgrade is initiated from the Avaya Aura® Experience Portal 7.0.1 Linux Installer ISO image files that you must copy or move to the /var directory during the course of the upgrade process.

! Important:

This upgrade method is supported only for upgrading an Experience Portal 6.0 or 7.0 system to 7.0.1. If you are upgrading a Voice Portal 5.1 system, use the software installation DVD to upgrade Avaya Enterprise Linux.

This upgrade method is non-interactive and provides an automatic upgrade of Avaya Enterprise Linux.

Procedure

1. Log in to Linux on the Experience Portal server.
 - If you upgrade through the console:
 - If you are an Avaya Services representative, log in to the local Linux console as sroot.
 - Or log in to local Linux console as root.
 - If you upgrade through a network connection to eth0:
 - If you are an Avaya Services representative, log in to Linux as craft and change to the user sroot by entering the `su - sroot` command.
 - Or log in to Linux as a non root user, and enter the `su -` command to change to the root user.
2. Copy the Avaya Aura® Experience Portal 7.0.1 Linux Installer ISO image to a folder on the system, and mount the ISO image to the desired directory by entering the mount command.

For example, run the `mount -o loop <aaepInstallerName.iso> /mnt/cdrom` command, where:

- <aaepInstallerName.iso> is the name of the Avaya Aura® Experience Portal 7.0.1 Linux Installer ISO image
 - /mnt/cdrom is the mount point associated with the ISO image
3. Run the `bash /mnt/cdrom/Avaya/vpupgrade.sh` command to run the Pre-upgrade tool.

This tool prepares the system for the upgrade.

4. Type `y` and press `Enter` to confirm that you want to run the tool.

The tool confirms whether you want to upgrade the operating system without media.

5. Type `yes` and press `Enter` to proceed with an autoupgrade without media.

6. If you have performed an upgrade on the system earlier using the ISO image file, the upgrade script prompts if you want to delete the `/var/avlupgrade` directory.
 - If you do not want to delete the `/var/avlupgrade` directory, you will need to exit the upgrade process by performing the following steps:
 - a. Type `no` and press `Enter`.
 - b. At the **Do you want to continue** prompt, type `y` and press `Enter` to exit the installation process.
 - To delete the `/var/avlupgrade` directory and continue with the upgrade, type `yes` and press `Enter`.

The upgrade script prompts for the FQFN of the Avaya Aura® Experience Portal 7.0.1 Linux Installer ISO image.

7. Type the FQFN where:

FQFN is the full filename, including path, to the Avaya Aura® Experience Portal 7.0.1 Linux Installer ISO image, which you have copied to the system at the beginning of the task.

8. Press `Enter`.

The upgrade script prompts you to copy or move the files from the ISO image to `/var`, the static partition.

9. Type `copy` to copy the ISO files or type `move` to move the ISO files, and press `Enter`.

The upgrade script copies/moves the files from the ISO image to the static partition.

10. Type `y` and press `Enter` to confirm that you want the utility to prepare the system for the upgrade.
11. Type `y` and press `Enter` to reboot the server.

The upgrade process starts automatically after the server is rebooted.

12. When the upgrade process is complete and the server responds to ping from a command line, log in to Linux on the Avaya Aura® Experience Portal server.

 Note:

The root login is disabled after you upgrade Avaya Enterprise Linux. If you need the password for the `sroot` or `craft` account, contact Avaya Services.

- If you upgrade through the console, log in to the local Linux console as `sroot`.
 - If you upgrade through a regular network connection to `eth0`, log in to Linux as a non-root user and enter the `su - sroot` command to change to the user `sroot`.
13. For security reasons, change the passwords for the Linux customer-related accounts that the installer creates during the installation procedure.

*** Note:**

If an Avaya Services representative changes the password, you must request the customer to perform either of the following:

- a. Enter the new passwords.
 - b. Enter default passwords and then request the customer to change the passwords immediately.
- a. Enter the `passwd sroot` command.
 - b. Type the password and press `Enter`.
 - c. Confirm the password at the prompt.
 - d. Enter the `passwd cust` command.
 - e. Type the password and press `Enter`.
 - f. Confirm the password at the prompt.
14. If the server is an MPP and you have moved the MPP logs to a new directory or a partition using the `mppMoveLogs.sh` script, add the mount point to the `/etc/fstab` file. For more information, see *Administering Avaya Aura® Experience Portal*.

Next steps

Verify the Network Time Protocol (NTP) as described in [Verify that the NTP service is operating properly](#) on page 135.

After you upgrade Avaya Enterprise Linux, upgrade to Avaya Aura® Experience Portal 7.0.1.

Upgrading Avaya Enterprise Linux from the software installation DVD

Before you begin

If you plan to use a direct connection to upgrade Avaya Enterprise Linux, ensure that you connect a keyboard and monitor to the server.

If you plan to use a Ethernet cross over connection from a laptop, configure the laptop as described in [Preparing to connect to using a crossover Ethernet cable](#) on page 21.

! Important:

If you have installed a Tomcat application server on the Experience Portal server, the software on the Application server might get deleted during the OS upgrade. Back up the configuration files, data files, Web applications, libraries, and binaries from the directory where the Application server is installed. For more information about the required backup files, contact the application developer.

About this task

Use this procedure to upgrade Avaya Enterprise Linux from the Avaya Enterprise Linux software installation DVD. This upgrade method provides both non-interactive as well as automatic upgrade of Avaya Enterprise Linux.

Procedure

1. Log in to Linux on the Experience Portal server.
 - If you upgrade through the console:
 - If you are an Avaya Services representative, log in to the local Linux console as `sroot`.
 - Or log in to local Linux console as `root`.
 - If you upgrade through a network connection to `eth0`:
 - If you are an Avaya Services representative, log in to Linux as `craft` and change to the user `sroot` by entering the `su - sroot` command.
 - Or log in to Linux as a non root user, and enter the `su -` command to change to the root user.
 - If you upgrade through a Ethernet crossover connection to `eth1`:
 - Use a secure shell (SSH) client, such as PuTTY, to open an SSH connection to the IP address 192.11.13.6.
 - If you are an Avaya Services representative, log in to Linux as `craft` and change to the user `sroot` by entering the `su - sroot` command.
 - Or log in to Linux as a non root user, and enter the `su -` command to change to the root user.
2. Insert the Avaya Enterprise Linux software installation DVD in to the server's DVD device.
3. If the DVD device is not automatically mounted, mount the drive by entering the `mount /mnt/cdrom` command.

`/mnt/cdrom` is the mount point associated with the DVD device in the `fstab` file.

If you cannot mount the DVD on Avaya Enterprise Linux, see *Troubleshooting Avaya Aura® Experience Portal* to troubleshoot the issue.
4. Run the `bash /mnt/cdrom/Avaya/vpupgrade.sh` command to run the Pre-upgrade tool.

The tool confirms whether you want to upgrade the OS without media.
5. Type `no` and press `Enter` to confirm that you want to upgrade the OS with media.

The tool prepares the system for the upgrade.
6. Type `y` and press `Enter` to confirm that you want to run the tool.

The tool confirms whether you want to enable the autoupgrade option.
7. Type `n` and press `Enter` to disable autoupgrade, or type `y` and press `Enter` to enable autoupgrade.

! Important:

If you upgrade through a network connection to eth0, ensure that you enable autoupgrade.

8. Press `Enter` to complete the preupgrade tool.

9. Type `Y` and press `Enter` to restart the server.

If you upgrade through a network connection to eth0, and select the autoupgrade option, the system runs the upgrade procedure after the system restarts. Skip to Step 12 for further instructions.

If you upgrade through a console, the system displays the Avaya Enterprise Linux installer Welcome screen after the system restarts.

10. In the Avaya Enterprise Linux installer Welcome screen, type `2` and press `Enter` at the boot prompt to select the **Upgrade** option.

The installer displays the Warning screen.

! Important:

You must enter your selection on the Welcome screen within 60 seconds. Otherwise, the installer searches for an Ethernet crossover connection on the eth1 interface.

If the crossover connection is not detected, the installer continues with autoupgrade if you have selected the autoupgrade option. The installer ejects the DVD and reboots if you have not selected the autoupgrade option.

*** Note:**

Instead of displaying the Warning screen, the Avaya Enterprise Linux installer might display the **No Disks found! /dev/sda missing** error. To resolve the issue, type `n` and press `Enter` at the **Eject CD/DVD before rebooting** prompt.

11. If you upgrade through a crossover Ethernet connection to eth1:
 - a. In the command line, enter the `ping -t 192.11.13.6` command to determine when the server completes the reboot.
 - b. After the server responds to the ping command, type `Ctrl-C` to stop the ping command.
 - c. Open a telnet client, such as PuTTY, and connect to the IP address 192.11.13.6.

! Important:

You must start the telnet session within 5 minutes of the server responding to ping. If you do not start the telnet session, the installer ejects the DVD and reboots the server.

*** Note:**

To use the Windows command telnet as the telnet client:

- a. Enter the `telnet` command.
- b. At the Microsoft Telnet> prompt, enter the `set term vt100` command.
- c. At the Microsoft Telnet> prompt, enter the `open 192.11.13.6` command.

Note: When using telnet connection, the install screen might not display the information clearly.

The installer displays the Warning screen.

- d. Type `u` and press `Enter` at the **Specify your choice** prompt to select the **Upgrade** option.

The installer displays the Warning screen.

12. On the Warning screen, type `yes` and press `Enter` to confirm that you want to upgrade Avaya Enterprise Linux.

*** Note:**

If you upgrade remotely, you do not see the Warning screen, and the installer selects the **Remote Install/Upgrade** option by default.

13. When the installer completes the upgrade procedure, the server ejects the DVD, and the server reboots automatically.

If you upgrade remotely, the upgrade procedure is completed when the server ejects the DVD and the server responds to ping from a command line.

14. Remove the Avaya Enterprise Linux installation DVD from the drive.
15. When the server reboots, log in to Linux on the Avaya Aura® Experience Portal server.

*** Note:**

The root login is disabled after you upgrade Avaya Enterprise Linux. If you need the password for the `sroot` or `craft` account, contact Avaya Services.

- If you upgrade through the console, log in to the local Linux console as `sroot`.
- If you upgrade through a regular network connection to `eth0`, log in to Linux as a non-root user and enter the `su - sroot` command to change to the user `sroot`.
- If you upgrade through a crossover Ethernet connection to `eth1`, you must perform the following:
 - a. Use a secure shell (SSH) client, such as PuTTY, to open an SSH connection to the IP address 192.11.13.6.
 - b. Log in to Linux as a non root user.
 - c. Enter the `su - sroot` command to change to the user `sroot`.

16. For security reasons, change the passwords for the Linux customer-related accounts that the installer creates during the installation procedure.

 Note:

If an Avaya Services representative changes the password, you must request the customer to perform either of the following:

- a. Enter the new passwords.
 - b. Enter default passwords and then request the customer to change the passwords immediately.
- a. Enter the `passwd root` command.
 - b. Type the password and press `Enter`.
 - c. Confirm the password at the prompt.
 - d. Enter the `passwd cust` command.
 - e. Type the password and press `Enter`.
 - f. Confirm the password at the prompt.
17. If the server is an MPP and you have moved the MPP logs to a new directory or partition using the `mppMoveLogs.sh` script, add the mount point to the `/etc/fstab` file. For more information, see *Administering Avaya Aura® Experience Portal*.

Next steps

Verify the Network Time Protocol (NTP) as described in [Verify that the NTP service is operating properly](#) on page 135.

After you upgrade Avaya Enterprise Linux, upgrade to Avaya Aura® Experience Portal 7.0.

Upgrading Red Hat Enterprise Linux Server on the dedicated EPM server

Before you begin

If you upgrade to Experience Portal 7.0.1 from versions prior to Experience Portal 7.0, you must do a fresh installation of a supported version of Red Hat Enterprise Linux Server. In previous releases, Experience Portal supported only 32-bit versions of Red Hat Enterprise Linux Server. Experience Portal 7.0.1 supports only 64-bit versions of Red Hat Enterprise Linux Server. Red Hat does not support upgrading from 32-bit to 64-bit versions of Red Hat Enterprise Linux Server.

If you upgrade from Experience Portal 7.0 to 7.0.1, you can do an upgrade rather than a fresh install since the Experience Portal 7.0 system is already installed on the 64-bit operating system.

- Ensure that you create a backup of the Experience Portal database. For this upgrade procedure, use the **System Management > System Backup** menu in the EPM Web interface to create the backup.

For more information about backing up data from the **System Backup** menu, see *Administering Avaya Aura® Experience Portal*.

*** Note:**

If you upgrade from Experience Portal 7.0 to 7.0.1, database backup is not required for Linux upgrades.

Upd

- Verify that the prerequisites have been met. For more information, see [Software upgrade prerequisites overview for upgrading from 5.1 or 6.0](#) on page 38
- Log in to Linux on the EPM server and turn off the automatic process restart feature for Tomcat by entering the `chkconfig tomcat off` command.

About this task

The following steps are guidelines to install a supported version of Red Hat Enterprise Linux Server, and provide instructions for making selections when the default values are not suitable.

Procedure

1. Reboot the server so that it boots from the media of a supported version of Red Hat Enterprise Linux Server.

The system displays the **Welcome to Red Hat Enterprise Linux** screen.

2. Select the **Install or upgrade an existing system** option.
3. Select **English** as the language to use during the installation process.
4. Select the U.S. English keyboard option.
5. Select **Basic Storage Devices** to install Red Hat Enterprise Linux Server.
6. Select the **Fresh Installation** option.

*** Note:**

If you upgrade from Experience Portal 7.0 to 7.0.1, you can select the **Upgrade an Existing Installation** option and follow the upgrade procedure.

7. Enter a hostname for the system.

*** Note:**

Assign the same IP address to the server that was assigned before the upgrade.

8. To configure the network:
 - a. Ensure that `eth0`, the main Ethernet interface, is enabled.
 - b. Select **Connect automatically** to start the connection automatically when the system boots.
 - c. On the **IPv4 Settings** tab, configure the following settings using the values specified on the installation worksheet:
 - Static IP address
 - Netmask

- Gateway
 - DNS servers
 - Search domains
9. Enter the applicable timezone.
 10. Enter the root password. Ensure that you enter the value that you have specified in the installation worksheet.
 11. Select the **Use All Space** option on the partitioning screen.
 12. Select **Basic Server** as the installation type as **Basic Server** is the recommended option.
 13. **(Optional)** Select the **Customize now** option on the screen to customize the installation.

 Note:

To include Red Hat Enterprise Linux Server languages other than English, press the **Customize now** button and install the languages.

14. Complete the installation and reboot the system.
15. After the system reboots, complete the post-installation configuration procedures.
 - a. Set the system clock.
 - b. Create a non-root account. Ensure that you use the value that you have specified in the installation worksheet.

 Note:

After the Experience Portal software is installed, use a non-root account to log in and then change to `root` account by using the `su` command.

- c. Disable the firewall.
- d. Disable SELinux.

Upgrading Red Hat Enterprise Linux Server on a dedicated MPP server

Before you begin

If you upgrade to Experience Portal 7.0.1 from versions prior to Experience Portal 7.0, you must do a fresh installation of a supported version of Red Hat Enterprise Linux Server. In previous releases, Experience Portal supported only 32-bit versions of Red Hat Enterprise Linux Server. Experience Portal 7.0.1 supports only 64-bit versions of Red Hat Enterprise Linux Server. Red Hat does not support upgrading from 32-bit to 64-bit versions of Red Hat Enterprise Linux Server.

If you upgrade from Experience Portal 7.0 to 7.0.1, you can do an upgrade rather than a fresh install since the Experience Portal 7.0 system is already installed on the 64-bit operating system.

- Verify that the prerequisites have been met. For more information, see [Software upgrade prerequisites overview for upgrading from 5.1 or 6.0](#) on page 38
- Log on to the EPM web interface.
- From the **MPP Manager** page, stop the MPP.
- Take the MPP offline before you upgrade the operating system as described in [Taking an MPP offline using the EPM Web interface](#) on page 36.
- Log in to the Linux server and turn off the automatic process restart feature for the MPP service by entering the `chkconfig mpp off` command.

Procedure

1. Reboot the server so that it boots from the media of a supported version of Red Hat Enterprise Linux Server.

The system displays the **Welcome to Red Hat Enterprise Linux** screen.

2. Select the **Install or upgrade an existing system** option.
3. Select **English** as the language to use during the installation process.
4. Select the U.S. English keyboard option.
5. Select **Basic Storage Devices** to install Red Hat Enterprise Linux Server.
6. Select the **Fresh Installation** option.

Note:

If you upgrade from Experience Portal 7.0 to 7.0.1, you can select the **Upgrade an Existing Installation** option and follow the upgrade procedure.

7. Enter a hostname for the system.

Note:

Assign the same IP address to the server that was assigned before the upgrade.

8. To configure the network:
 - a. Ensure that `eth0`, the main Ethernet interface, is enabled.
 - b. Select **Connect automatically** to start the connection automatically when the system boots.
 - c. On the **IPv4 Settings** tab, configure the following settings using the values specified on the installation worksheet:
 - Static IP address
 - Netmask
 - Gateway
 - DNS servers

- Search domains
9. Enter the applicable timezone.
 10. Enter the root password. Ensure that you enter the value that you have specified in the installation worksheet.
 11. Select the **Use All Space** option on the partitioning screen.
 12. Select **Basic Server** as the installation type as **Basic Server** is the recommended option.
 13. **(Optional)** Select the **Customize now** option on the screen to customize the installation.

 Note:

To include Red Hat Enterprise Linux Server languages other than English, press the **Customize now** button and install the languages.

14. Complete the installation and reboot the system.
15. After the system reboots, complete the post-installation configuration procedures.
 - a. Set the system clock.
 - b. Create a non-root account. Ensure that you use the value that you have specified in the installation worksheet.

 Note:

After the Experience Portal software is installed, use a non-root account to log in and then change to `root` account by using the `su` command.

- c. Disable the firewall.
- d. Disable SELinux.

Upgrading Red Hat Enterprise Linux Server on a single server system

Before you begin

 Important:

If you upgrade to Experience Portal 7.0.1 from versions prior to Experience Portal 7.0, you must do a fresh installation of a supported version of Red Hat Enterprise Linux Server. In Experience Portal 6.0 and prior releases, Experience Portal supported only 32-bit versions of Red Hat Enterprise Linux Server. Experience Portal 7.0.1 supports only 64-bit versions of Red Hat Enterprise Linux Server. Red Hat does not support upgrading from 32-bit to 64-bit versions of Red Hat Enterprise Linux Server.

If you upgrade from Experience Portal 7.0 to 7.0.1, you can do an upgrade rather than a fresh install since the Experience Portal 7.0 system is already installed on the 64-bit operating system.

If you have installed a co-resident Application server on the Experience Portal 6.0 server:

- The co-resident Application server is not preserved when you install the new operating system for the Experience Portal 7.0.1 release.
- Prior to installing the new operating system, manually back up the configuration files, data files, Web applications and components, libraries, and binaries that you want to preserve from the Application server. For more information about the required backup files, contact the application developer.

If you have installed a co-resident Application server on the Experience Portal 7.0 server:

- The co-resident Application server is preserved when you upgrade the operating system, for the Experience Portal 7.0.1 release, in a way that preserves data on the system. Although, it is not mandatory to update the co-resident Application server in such a scenario, it is recommended that you upgrade the application server to pick up the latest Tomcat security fixes.
- The co-resident Application server is not preserved when you upgrade the operating system, for the Experience Portal 7.0.1 release, in a way that does not preserve data on the system. In such a scenario, manually back up any configuration files, data files, Web applications and components, libraries, and binaries that you want to preserve from the Application server prior to upgrading the operating system. For more information about the required backup files, contact the application developer.
- Ensure that you create a backup of the Experience Portal database. For this upgrade procedure, use the **System Management > System Backup** menu in the EPM Web interface to create the backup.

For more information about backing up data from the **System Backup** menu, see *Administering Avaya Aura® Experience Portal*

 Note:

If you upgrade from Experience Portal 7.0 to 7.0.1, database backup is not required for Linux upgrades.

- Verify that the prerequisites have been met. For more information, see [Prerequisites overview for upgrading Experience Portal](#) on page 38.
- Log on to the EPM Web interface.
- From the **MPP Manager** page, stop the MPP.
- Perform the steps described in [Preventing loss of reporting data prior to upgrading MPP](#) on page 37.
- Take the MPP offline before you upgrade the operating system as described in [Taking an MPP offline using the EPM Web interface](#) on page 36.
- Log in to Linux on the Experience Portal server and turn off the automatic process restart feature for the MPP service by entering the `chkconfig mpp off` command.
- Turn off the automatic process restart feature for Tomcat by entering the `chkconfig tomcat off` command.

About this task

This procedure provides instructions on how to install a supported version of Red Hat Enterprise Linux Server.

Procedure

1. Reboot the server so that it boots from the media of a supported version of Red Hat Enterprise Linux Server.

The system displays the **Welcome to Red Hat Enterprise Linux** screen.

2. Select the **Install or upgrade an existing system** option.
3. Select **English** as the language to use during the installation process.
4. Select the U.S. English keyboard option.
5. Select **Basic Storage Devices** to install Red Hat Enterprise Linux Server.
6. Select the **Fresh Installation** option.

 Note:

If you upgrade from Experience Portal 7.0 to 7.0.1, you can select the **Upgrade an Existing Installation** option and follow the upgrade procedure.

7. Enter a hostname for the system.

 Note:

Assign the same IP address to the server that was assigned before the upgrade.

8. To configure the network:
 - a. Ensure that `eth0`, the main Ethernet interface, is enabled.
 - b. Select **Connect automatically** to start the connection automatically when the system boots.
 - c. On the **IPv4 Settings** tab, configure the following settings using the values specified on the installation worksheet:
 - Static IP address
 - Netmask
 - Gateway
 - DNS servers
 - Search domains
9. Enter the applicable timezone.
10. Enter the root password. Ensure that you enter the value that you have specified in the installation worksheet.
11. Select the **Use All Space** option on the partitioning screen.
12. Select **Basic Server** as the installation type as **Basic Server** is the recommended option.
13. **(Optional)** Select the **Customize now** option on the screen to customize the installation.

 Note:

To include Red Hat Enterprise Linux Server languages other than English, press the **Customize now** button and install the languages.

14. Complete the installation and reboot the system.
15. After the system reboots, complete the post-installation configuration procedures.
 - a. Set the system clock.
 - b. Create a non-root account. Ensure that you use the value that you have specified in the installation worksheet.

 Note:

After the Experience Portal software is installed, use a non-root account to log in and then change to `root` account by using the `su` command.

- c. Disable the firewall.
- d. Disable SELinux.

Taking an MPP offline using the EPM Web interface

About this task

This procedure explains how to take an MPP offline from EPM.

Procedure

1. Log in to EPM using an account with the Administration or Operations user role.
2. From the EPM main menu, select **System Management > MPP Manager**.
3. On the MPP Manager page, use the Selection check box in the MPP server table to select the MPP server to take offline.

 Note:

If the MPP is in the stopped state, proceed to step 8.

4. Click **Stop** in the **State Commands** group and confirm your selection.

 Note:

The EPM stops the selected MPP server when the last active call completes or when the grace period expires, whichever condition is met first.

5. Click **Refresh** and verify that the **State** is **Stopped** for the MPP server.
6. If the MPP operational state:
 - Changes to **Stopped**, continue with this procedure.
 - Did *not* change, stop the `mpp` service.

7. Use the Selection check box in the MPP server table to reselect the MPP server to take offline.
8. Click **Offline** in the **Mode Commands** group.
9. Click **Refresh** and verify that the **Mode** is **Offline**.

Stopping the MPP service

You must take the MPP offline using the EPM Web interface. However, if you cannot take the MPP service offline because the EPM is not communicating with the MPP, take the MPP offline by stopping the `mpp` service.

About this task

Use this procedure to take the MPP offline by stopping the `mpp` service.

Procedure

1. Log in to the MPP server.

If you are an Avaya Services representative, and use Avaya Enterprise Linux or if the Avaya Service accounts are installed on this server:

- Log in to the local Linux console as `sroot`.
- Or log in remotely as a non-root user and then change the user to `sroot` by entering the `su - sroot` command.

Otherwise, log in to Linux locally as `root`, or log in remotely as a non-root user and then change the user to `root` by entering the `su -` command.

2. Enter the `/sbin/service mpp stop` command.

Preventing loss of reporting data prior to upgrading MPP

Before you begin

Perform this procedure only if you plan to upgrade a system that is installed on a supported version of Red Hat Enterprise Linux Server.

Procedure

1. Schedule a report data download from the Report Data page of the EPM Web interface.
2. To determine that the report data download is complete, check the Log Viewer for the `Scheduled event completed` message.

Chapter 4: Software upgrade prerequisites

Prerequisites overview for upgrading Experience Portal

Complete these tasks before you upgrade the Avaya Aura® Experience Portal software.

✓	Description	Prerequisite applicable for
	Ensure that you partition the hard drive in order to create the required space for the Experience Portal software installation. For more information on the partition requirements for the hard drive, see <i>Administering Avaya Aura® Experience Portal</i> .	All the Experience Portal components
	Ensure that you can access the Experience Portal site-specific licensing information from Avaya. For more information, see License Requirements on page 42.	Primary EPM
	Check to see if there are Experience Portal patches available on the Avaya online support Web site. If patches are available, download the patches before you begin the software upgrade.	All the Experience Portal components. * Note: Apply the patches after each EP component is upgraded
	Verify that you can access all the target systems using at least one of the following methods: • _____ A computer on the customer's network that has an SSH client to reach the target system. • _____ A keyboard, monitor, and mouse attached directly to the target system. • _____ A crossover cable that connects a second computer that has a keyboard, monitor, mouse, and an SSH client.	All the Experience Portal components
	Verify that the Linux operating system is upgraded. For details, see Verifying the Linux version number on page 43.	All the Experience Portal components

Table continues...

✓	Description	Prerequisite applicable for
		★ Note: Perform this task after the OS Install/ Update
	To connect your Experience Portal system to an external Oracle database, you must install the Oracle JDBC driver. For more information, see Installing Oracle JDBC driver on page 44.	Primary EPM Auxiliary EPM
	Disable the firewall or anti-virus software on the target systems.	All the Experience Portal components ★ Note: Perform this task after the OS Install/ Update
	Disable SELinux on EPM and/or MPP.	EPM MPP
	If you install the EPM software on a dedicated server, verify that the EPM server can communicate with all the MPP servers. For details, see Verifying communication between the upgraded Experience Portal servers on page 45.	Primary EPM
	To ensure that the email messages are processed throughout the upgrade process, configure the email processors in your Experience Portal system as described in Ensuring that Email messages are processed during upgrades on page 47.	Primary EPM Auxiliary EPM
	To ensure that the SMS messages are processed throughout the upgrade process, configure the SMS processors in your Experience Portal system as described in Ensuring that SMS messages are processed during upgrades on page 47.	Primary EPM Auxiliary EPM
	If you are upgrading the Experience Portal software on a Red Hat Linux server, ensure that you copy the back up files to the server as described in Copying and restoring the backup files on Red Hat Enterprise Linux Server on page 48.	Primary EPM ★ Note: Perform this task after the OS Install/ Update
	Ensure that none of the mount points are stale or hung. For details, see Checking for stale or hung mount points on page 49.	All the Experience Portal components ★ Note: Perform this task after the OS Install/ Update

Table continues...

✓	Description	Prerequisite applicable for
	Verify that the time is synchronized between all the Experience Portal servers. For details, see Verifying server time synchronization on page 49. ! Important: If the time is not synchronized between the EPM and MPP servers, the upgrade process might hang.	All the Experience Portal components * Note: Perform this task after the OS Install/Update
	If the Experience Portal system is connected to an external database, verify that the database is configured as described in Updating the external database configuration on page 50.	Primary EPM
	If you have installed a supported version of Red Hat Enterprise Linux Server, verify that the correct RPMs are installed on your system. For more information on how to verify the correct RPMs, see Identifying RPM issues on page 127.	All the Experience Portal components

Minimum server hardware requirements

Customer supplied servers must meet the following minimum specifications in order to run Avaya Aura® Experience Portal:

- Compatibility with a supported version of Red Hat Enterprise Linux Server. For information about hardware compatibility, go to the *Certified Hardware* section of the Red Hat website, <http://www.redhat.com>.
- Dual Quad Core 1.6 GHz Pentium 4 or equivalent processors.
- 4 GB of RAM.
- 120 GB Disk, 7200 RPM.
- One 100/1000 Base-T Ethernet controller that is full duplex (onboard Network Interface Cards (NICs).
- DVD drive.
- Keyboard.
- Monitor.
- Mouse.
- Avaya Secure Access Link (SAL) or Avaya ASG solution. If you purchase a maintenance agreement with Avaya Services, the Experience Portal system requires SAL or Avaya ASG solution so that Avaya Services can remotely access the system for maintenance purposes. Contact Avaya Support to determine the version of SAL and Avaya ASG supported.

Disk space requirements

Space requirement for upgrading the primary EPM on Red Hat Enterprise Linux

While upgrading Experience Portal on Red Hat Enterprise Linux, the Experience Portal database upgrade uses approximately four times the size of the database backup. For example, a system with a backup of 10 GB needs approximately 40 GB of free space to successfully upgrade the database.

To prevent upgrade failure due to space constraints, monitor and estimate hard disk space usage during the upgrade process. The system retains some of the files used in the upgrade process for backup. However, you may either delete these files, or move these files to a different location during or after the upgrade to maximize the available hard disk space. The following table describes some of the database files used during upgrade, their locations, their approximate sizes relative to the database backup, and if you can delete or relocate these files safely. Avaya recommends you to retain these files in a different partition or hard drive, for backup purpose.

Description	Location	Size compared to database backup	When it is safe to delete
Experience Portal backup file	You can select the location	–	You may delete this file after you run the script <code>RestoreProps.sh</code> successfully.
Database export file	<code>/var/lib/pgsql/vp_upgrade.export_vp_<date></code> Where <code><date></code> is the date of installation.	Same as the database backup.	After the Experience Portal prerequisite installer successfully installs the updated PostgreSQL database. Ensure that the PostgreSQL field indicates Success .
Experience Portal database	<code>/var/lib/pgsql/data</code>	The size varies from 10% to 100% larger than the database backup file.	Do not delete this file. Deleting this file causes loss of data.

Space requirement for upgrading the primary EPM on Avaya Enterprise Linux

While upgrading Experience Portal on Avaya Enterprise Linux, the Experience Portal database upgrade uses approximately 3.5 times the size of the database backup. For example, a system with a backup of 10 GB requires approximately 35 GB of free space in the `/var` partition for a successful upgrade.

Enter the command `du -sk /var/lib/pgsql/data/base` to determine the database size. The system displays the size of the database in kilobytes.

To prevent upgrade failure due to space constraints, monitor and estimate hard disk space usage during the upgrade process. The system retains some of the files used in the upgrade process for backup. However, you may either delete these files, or move these files to a different location during or after the upgrade to maximize the available disk space. The following table describes some of the database files used during upgrade, their locations, their approximate sizes relative to the database backup, and if you can delete or relocate these files safely. Avaya recommends you retain these files in a different partition or hard drive, for backup purpose.

Description	Location	Size compared to database	When it is safe to delete
Old Experience Portal database	<code>/var/lib/pgsql/data/base</code>	Approximately same as the database size	After OS upgrade, and before you run the <code>installvp</code> or the <code>autoupgrade</code> command. Ensure that the export file is present at <code>/var/lib/pgsql/vp_upgrade.export</code>.  Caution: Do not move or delete this directory after you run the commands <code>installvp</code> or <code>autoupgrade</code>.
Database export file	<code>/var/lib/pgsql/vp_upgrade.export_vp_<date></code> Where <code><date></code> is the date of installation.	Approximately same as the database size	After the Experience Portal prerequisite installer successfully installs the updated PostgreSQL database. Ensure that the PostgreSQL field indicates Success.

License Requirements

Before you configure Experience Portal, ensure that Avaya provides the following site-specific items:

- **Product ID:** The unique product ID for your site. The numeric identifier that Avaya must provide when the EPM software is installed.
- **The Experience Portal license file:** The file that determines the maximum number of telephony ports available to Experience Portal. The file also determines whether the speech applications in the system can use ASR or TTS resources. You must install the license file on the Avaya WebLM server.

*** Note:**

Before you upgrade the Experience Portal system to a newer version, ensure that you upgrade the license to a newer version. If you upgrade an Experience Portal system to a newer version and do not upgrade the license, the system provides a grace period of 30 days. During the grace period, you must upgrade the license as per the following compatibility matrix, otherwise the license grace period will end and the system will no longer be functional.

The compatible versions of Experience Portal and WebLM licenses are:

Voice Portal/Experience Portal Version	License Version
Voice Portal 5.1	5
Avaya Aura® Experience Portal 6.0	6
Avaya Aura® Experience Portal 7.0	7
Avaya Aura® Experience Portal 7.0.1	7

- If Avaya Services maintains the Experience Portal system, the Avaya Services representative must get the following:
 - The Avaya Service Account authentication file that you can use to create Avaya Service accounts after you install the Experience Portal software.
 - The Listed Directory Number (LDN) in the Avaya Services database for each EPM and MPP server, and each speech server.

Verifying the Linux version number

Procedure

1. On the Experience Portal server, log in to Linux as any user.
2. If you use:
 - Avaya Enterprise Linux Server, enter the `swversion` command to determine the version, and enter the `uname -m` command to determine the architecture.

The result must state the version RH6.5.64-AV01EP7FP1 or later (if the operating system is upgraded) or RH6.4.64-AV13EP7 (if the operating system is not upgraded). If the version is not correct, upgrade the operating system on the server.

- Red Hat Enterprise Linux Server, enter the `cat /etc/issue` command to determine the version, and enter the `uname -m` command to determine the architecture.

The result must state the version is Release 6.4 or later and the architecture is x86_64. If you have an earlier version of Red Hat Enterprise Linux Server, upgrade the operating system on the server.

Or run the `rpm -q redhat-release-server` command to ensure that the Linux build version is correct. The result must state build redhat-release-server-6Server-6.4.0.4.el6.x86_64 or later (if the operating system is upgraded) or redhat-

release-server-6Server-6.4.0.37.el6.i686 or later (if the operating system is not upgraded). If the build is not correct, get the latest build from Red Hat.

+ Tip:

To determine whether the server is running Avaya Enterprise Linux, run the `swversion` command. If the command returns information about your operating system, the server is running Avaya Enterprise Linux.

Installing the Oracle JDBC driver

Before you begin

To connect your Experience Portal system to an external Oracle database, you must first obtain the JDBC driver from Oracle. The Oracle JDBC driver is not shipped with Experience Portal.

Download the Oracle JDBC driver from <http://www.oracle.com/technetwork/database/enterprise-edition/jdbc-112010-090769.html>. From section **Oracle Database 11g Release 2 (11.2.0.3) JDBC Drivers**, download files `ojdbc6.jar` and `orai18n.jar`.

! Important:

Web browsers might change the file extension of the files to `.zip` when the files are downloaded. Rename the files to `ojdbc6.jar` and `orai18n.jar`.

About this task

To have the Oracle JDBC driver installed by the Experience Portal install program, perform the following steps after you install or upgrade Linux. It is recommended that you perform the procedure before you install or upgrade Experience Portal.

The procedure also provides information about how to install the Oracle JDBC driver after you install or upgrade Experience Portal.

Procedure

1. Log in to Linux on the Primary Experience Portal server as a root user.
2. Run the `mkdir ~/OracleJDBC` command to create the `~/OracleJDBC` folder.
3. Copy the `ojdbc6.jar` and `orai18n.jar` driver files to the `~/OracleJDBC` folder.

! Important:

Do not delete the Oracle JDBC driver files from the `~/OracleJDBC` directory after you install or upgrade Experience Portal. You will need the files if you reinstall or upgrade Experience Portal.

4. If you install the Oracle JDBC driver after you install or upgrade the Experience Portal server, you must do the following:
 - a. Run the `/sbin/service vpms stop` command to stop the `vpms` service.

- b. Run the `cd $AVAYA_HOME/Support/Database` command to navigate to the appropriate directory.
- c. Run the `bash InstallOracleJDBC.sh` command to install the JDBC driver.

! Important:

Run the `InstallOracleJDBC.sh` command only after you download the Oracle driver in the `~/OracleJDBC` directory on the server.

- d. Run the `/sbin/service vpms start` command to start the vpms service.
5. Repeat the procedure on each Auxiliary Experience Portal server.

Verifying communication between the upgraded Experience Portal servers

If EPM is running on a dedicated server, ensure that EPM can still communicate with all MPP servers, PBXs, and application servers using their IP addresses. Optionally, verify that the EPM can communicate with the servers using their host names.

Procedure

1. Log in to Linux on the Experience Portal Primary EPM server.
2. Verify the Primary EPM server's IP address and host name:

- a. Enter the `hostname -i` command.

This command must return the server's IP address and not `127.0.0.1`. If this check fails, you must manually map the host names. For more information about the Prerequisite Checker failure with `UnknownHostException:localhost`, see *Implementing Avaya Aura® Experience Portal on multiple servers*.

- b. Enter the `hostname -s` command.

This command must return the server's host name and not `localhost`. If this check fails, you must manually map the host names to connect the Primary EPM with other servers. For more information, see *Implementing Avaya Aura® Experience Portal on multiple servers*.

3. Verify that the Primary EPM server can communicate with all MPP servers:

- a. Enter the `ping -c 4 <mpp_hostname>` command, where:

`<mpp_hostname>` is the hostname of the MPP server you are testing.

- b. Wait for the system to respond with the ping details.
- c. If this check fails, you must manually map the hostnames to connect the Primary EPM with other servers. For more information, see *Implementing Avaya Aura® Experience Portal on multiple servers*.

- d. If your Experience Portal system contains more than one MPP server, repeat this step for each MPP server.
4. If you have an Auxiliary EPM server, verify that the Primary EPM server can communicate with the Auxiliary EPM server:
 - a. Enter the `ping -c 4 <Auxiliary_vpms_hostname>` command, where:
`<Auxiliary_vpms_hostname>` is the hostname of the Auxiliary EPM server.
 - b. Wait for the system to respond with the ping details.
 - c. If the check fails, enter the `ping -c 4 <Auxiliary_vpms_ipaddress>` command, where:
`<Auxiliary_vpms_ipaddress>` is the IP address of the Auxiliary EPM server.
 - d. Wait for the system to respond with the ping details.
 - e. If both the checks fail, you must manually map the host names.
5. Verify that the Primary EPM server can communicate with the external servers by host name or IP address:
 - a. Enter the `ping -c 4 <server_hostname>` command, where:
`<server_hostname>` is the hostname of the one of the following external components attached to your Experience Portal system:
 - A PBX server.
 - An application server.
 - A speech server.
 - Communication Manager.
 - Avaya SIP Enablement Services.
 - b. Wait for the system to respond with the ping details.
 - c. If this check fails, enter the `ping -c 4 <server_ipaddress>` command, where:
`<server_ipaddress>` is the IP address of the server whose hostname you specified in the previous `ping` command.
 - d. Wait for the system to respond with the ping details.
 - e. If either of these checks fail, you must manually map the hostnames to connect the Primary EPM server with the servers. For more information, see *Implementing Avaya Aura® Experience Portal on multiple servers*.
 - f. Repeat this procedure for each external server in your Experience Portal system.

Ensuring that Email messages are processed during upgrades

About this task

This procedure provides information about how to ensure that the email messages are processed during the Primary EPM or Auxiliary EPM upgrade process.

Procedure

1. Ensure that you configure at least two email processors.

 Note:

An Experience Portal system that includes multiple zones, must have more than one processor.

2. From the **Multi-Media Configuration > Email** page in the EPM Web interface, disable the email processor which is handling the email connections.

This will ensure that the Primary EPM automatically assigns any email connections to the other processors.

3. Upgrade the Primary or Auxiliary EPM.
4. After you upgrade the Primary or Auxiliary EPM, enable the email processor that you had disabled in step 2.

Ensuring that SMS messages are processed during upgrades

About this task

This procedure provides information about how to ensure that the SMS messages are processed during the Primary EPM or Auxiliary EPM upgrade process.

Procedure

1. Ensure that you configure at least two SMS processors.

 Note:

An Experience Portal system that includes multiple zones, must have more than one processor.

2. From the **Multi-Media Configuration > SMS** page in the EPM Web interface, manually assign any SMPP connections that are assigned to the processor (that handles the connections) to some other SMS processor.
3. Disable the SMS processor after you assign the SMPP connections to some other SMS processor.

To disable the processor, click on the processor and in the **Change Processor** page, select the **No** option in the **Enable** field

4. Upgrade the Primary or Auxiliary EPM.
5. After you upgrade the Primary or Auxiliary EPM, enable the SMS Processor, and re-assign the SMPP connection back to the SMS processor.

Copying and restoring the backup files on Red Hat Enterprise Linux Server

Before you begin

- Install a supported version of Red Hat Enterprise Linux Server on the server as described in [Operating system upgrade overview](#) on page 19.
- Ensure that you have the location details of the Experience Portal backup files.

* Note:

The procedure is applicable only for the Primary EPM server.

Procedure

1. Log in to the server locally as root, or log in remotely as a non root user and change the user to root by running the `su -` command.
2. Copy the backup package created before the upgrade to a temporary location on the local hard drive.

Note that the folder name of backup packages created by Voice Portal will be `pkgVP<Version>_<XXXXXXXXXXXXXX>` and the folder name for backup packages created by Experience Portal will be `pkgEP<Version>_<XXXXXXXXXXXXXX>` where:

- `<Version>` is the version number of the software that the backup was created with.
- `<XXXXXXXXXXXXXX>` is a 13 digit timestamp that is not in a human readable format.

* Note:

The Experience Portal installation script identifies the Experience Portal version and the configuration information available on the server based on the folder name.

3. Insert the Experience Portal DVD into the DVD drive of the server and mount the DVD.
4. Enter the `cd <MountPoint>/Utilities/EPUpgrade` command, where:

`MountPoint` is the mount point directory.

5. Enter the `./RestoreProps.sh -p <BackupLocation>` command, where:

`BackupLocation` is the location of the Experience Portal backup files.

*** Note:**

To preserve disk space, you can delete the backup directory, which you created in Step 2, after RestoreProps script is run successfully.

Checking for stale or hung mount points

If you have file systems saved on the Experience Portal servers, check if the mounts points are stale or hung. Stale or hung mount points can cause RPM installations to not respond while installing the Experience Portal software.

About this task

Use this procedure to check for stale or hung mount points on the Experience Portal servers.

Procedure

1. On the Experience Portal server, log in to Linux as any user.
2. Enter the `df` command.

If the server:

- Responds to the command, the mount points are working.
- Does not respond to the command, then a mount point is stale or is not responding.

*** Note:**

Run the `umount` command to unmount any stale or hung mount points.

Verifying server time synchronization

After you upgrade the operating systems on all Experience Portal servers, you must ensure that the time on all servers is synchronized.

About this task

Use this procedure to ensure that the time on all servers is synchronized.

*** Note:**

Experience Portal only requires that the EPM and MPP servers are synchronized. However, you can also synchronize the servers that Experience Portal connects to, including the Application server, speech servers, and the PBX. For more information, see [External time sources](#) on page 115.

Procedure

1. On each Experience Portal server, in the same time frame, run the `date` command.

2. Verify that all Experience Portal servers report the time within a few seconds of each server response. If there is a time difference, verify that the planned MPP servers lag behind the planned EPM server.

For example, an MPP server time of 2:10:00 and a EPM server time of 2:10:03 is acceptable.

3. If one or more servers differ by more than a few seconds, set the appropriate date and time by running the `date MMDDhhmmYY.ss` command, where `MMDDhhmmYY.ss` is the two-digit month, day, hour, minute, year, and seconds you want to set based on the 24-hour clock.

For example, to set the date to 2:15:35 p.m. on March 31, 2008, you must enter `date 0331141508.35`.

Updating the external database configuration

If this Experience Portal system is connected to an external database, you must update the external database before you upgrade the EPM software.

About this task

Use this procedure to update the external database configuration.

The .sql files are located in the directory `/Support/ExternalDB/Oracle/UpgradeScripts`.

* Note:

Experience Portal does not refer to the contents of the local or external database, or administration of the system. The administration of the system and contents of the database is a customer responsibility.

Procedure

1. Insert the Experience Portal installation DVD in to the DVD device of the server on which the external database resides.
2. Based on the external database and the upgrade scenario, run the required scripts:
 - a. If you use Oracle:
 - For a 5.1 to 7.0 upgrade scenario, run the scripts in the following order:
 - `Oracle_New_Columns_60.sql`
 - `Oracle_New_Columns_70.sql`
 - For a 6.0 to 7.0 upgrade scenario, run the `Oracle_New_Columns_70.sql` script.
 - b. If you use Postgres:
 - For a 5.1 to 7.0 upgrade scenario, run the scripts in the following order:
 - `New_Columns_60.sql`
 - `New_Columns_70.sql`

For a 6.0 to 7.0 upgrade scenario, run the **NewColumns_70.sql** script.

c. If you use Microsoft SQL:

- For a 5.1 to 7.0 upgrade scenario, run the scripts in the following order:
 - **MSSQL_New_Columns_60.sql**
 - **MSSQL_New_Columns_70.sql**
- For a 6.0 to 7.0 upgrade scenario, run the **MSSQL_New_Columns_70.sql** script.

 Important:

For Microsoft SQL Server, the database user name for Experience Portal must be assigned SELECT, INSERT, UPDATE, DELETE privileges on the newly added VPZones table.

For Postgres, the database user name for Experience Portal must be assigned CONNECT, TEMPORARY ON DATABASE, SELECT, INSERT, UPDATE and DELETE privileges on the newly added VPZones table.

Chapter 5: Upgrading the EPM and MPP software on different servers

Upgrading the Primary EPM server

EPM software upgrade overview

When you install the EPM software, Experience Portal automatically records your answers to basic questions, such as what installation directory you want to use, the name of the EPM server, and what security certificate you want to use. EPM compiles the answers into a file. You can use the file later to upgrade the MPP software using the silent install option. This MPP upgrade option allows you to upgrade with very little user input.

There are two upgrade options for the EPM server.

- Automatic upgrade
- Interactive upgrade

Tip:

In Experience Portal 7.0.1, the certificate generation code is enhanced to use a more secure hashing algorithm. Avaya recommends that you upgrade to Experience Portal 7.0.1 by using the Interactive upgrade option so that you can generate a SHA256 2048 bit server certificate (the new security certificate) to make the systems more secure.

Automatic upgrade

Launch the Experience Portal installation program, and run the auto upgrade utility to upgrade to Experience Portal 7.0.1 on an Avaya Enterprise Linux server. The Experience Portal automatic upgrade utility, `autoupgradevp`, does not prompt for any input. The utility uses the installation options that were chosen during the previous installation.

The automatic upgrade:

- Uses the existing installation directories.
- Specifies the IP address of the server on which you install the EPM software.
- Uses the existing security certificate for the EPM.
- Keeps the existing user accounts.

*** Note:**

If you have deleted all the existing user manager accounts from EPM prior to the upgrade, you need to use the interactive upgrade option.

The system displays error messages, if any, at the end of the upgrade process and all messages are recorded in the installation log files.

*** Note:**

Automatic upgrade is the recommended upgrade option if you want to upgrade to Avaya Aura® Experience Portal 7.0.1 on an Avaya Enterprise Linux server and you do not need changes to the configurations.

Interactive EPM upgrade

On the EPM server, launch the Experience Portal installation program and answer the prompts.

Avaya recommends the Interactive upgrade option if you need to make changes to the configurations during the upgrade.

Automatically upgrading the Primary EPM software**+ Tip:**

In Experience Portal 7.0.1, the certificate generation code is enhanced to use a more secure hashing algorithm. Avaya recommends that you upgrade to Experience Portal 7.0.1 by using the Interactive upgrade option so that you can generate a SHA256 2048 bit server certificate (the new security certificate) to make the systems more secure.

Before you begin

- Ensure that you upgrade the operating system on the server as described in [Operating system upgrade overview](#) on page 19.
- For upgrading the Primary EPM server, complete the [Primary EPM server upgrade worksheet](#) on page 147.
- For upgrading the Auxiliary EPM server, complete the [Auxiliary server upgrade worksheet](#) on page 150.
- Before you upgrade the software, read the Avaya Aura® Experience Portal release notes on the Avaya Aura® Experience Portal installation DVD under *Documentation*. These release notes contain information about the product that is not included in the formal documentation set.
- Download any patches for Avaya Aura® Experience Portal Release 7.0.1 from the Avaya Support Web site at <http://support.avaya.com>.
- Ensure that you complete the software upgrade prerequisites as described in [Prerequisites overview for upgrading Experience Portal](#) on page 38.
- For disk space related information, see [Space requirement for upgrading primary EPM on Red Hat Enterprise Linux](#) on page 41 and [Space requirements for upgrading primary EPM on Avaya Enterprise Linux](#) on page 41.

- If you have installed a managed application, contact the provider of the managed application to check if you need to perform any additional steps as part of the Experience Portal upgrade.

Procedure

1. Log in to the server on which you want to upgrade the Experience Portal software. Ensure that you upgrade using the same Linux account that was used during the previous installation.

If you are an Avaya Services representative, and use Avaya Enterprise Linux or if the Avaya Service accounts are installed on this server:

- Log in to the local Linux console as `sroot`.
- Or log in remotely as a non-root user and then change the user to `sroot` by entering the `su - sroot` command.

Otherwise, log in to Linux locally as `root`, or log in remotely as a non-root user and then change the user to `root` by entering the `su -` command.

* Note:

Ensure that you upgrade using the same Linux account that was used during the prior installation. If you upgrade a Voice Portal or Experience Portal system by using a Linux account that is different than the account used during the previous install or upgrade, the upgrade might fail.

2. Insert the Avaya Aura® Experience Portal 7.0.1 software installation DVD into the DVD drive of the server.

+ Tip:

These instructions assume that you are going to access the Experience Portal installation DVD by mounting the appropriate DVD drive on the target system. If you want to access the installation DVD files from a shared network directory or a local directory, you can copy the files from the Experience Portal installation DVD to that directory. However, that directory must be readable by all users on the system. If the directory is only readable by the `root` or `sroot` user, the installation script will encounter errors and will not complete successfully.

3. Mount the Avaya Aura® Experience Portal 7.0.x software installation DVD. The `mount` command depends on the server's hardware and operating system.

- If you are working with Avaya Enterprise Linux, mount the DVD by entering the `mount /mnt/cdrom` command, where `/mnt/cdrom` is the mount point typically associated with the DVD drive in the `fstab` file.
- If you are working with a supported version of Red Hat Enterprise Linux Server, to mount the DVD:
 - Run the `mkdir /media/cdrom` command.

* Note:

This command is required only if the `/media/cdrom` mount point does not exist.

- Run the `mount /dev/cdrom /media/cdrom` command.

 Warning:

When Red Hat Enterprise Linux Server automatically mounts the DVD, the files on the DVD are not executable. You must manually mount the Experience Portal installation DVD using the commands shown above.

If the `mount` commands shown above do not work, consult your server documentation for the appropriate `mount` command.

4. Change to the mount point directory.
5. Run the `bash autoupgradevp` command to start the upgrade script.

When the upgrade is in progress, the system does not display any prompts.

As the script proceeds, the script displays messages similar to the following:

```
Starting automatic upgrade for Experience Portal software. This
will take several minutes to complete. Please wait...
```

```
-- Initializing install
-- Checking prerequisites
-- Installing prerequisites. Depending on the amount of data being
upgraded, this process could take over an hour. IMPORTANT: DO NOT
ABORT THE INSTALLATION.
-- Gathering install data
-- Starting install. Please be patient and wait for the Post
Installation Summary to be displayed
```

```
The Experience Portal installation has completed. Review the
following information. If there are errors or warnings, then
please review the installation logs.
```

```
Installing Documentation...
...done installing Documentation
```

```
Installing EPM...
...done installing EPM
Installing MPP...
...done installing MPP
```

```
Moving installation logs to: /opt/EP/logs/install_2014-04-01.000
```

 Tip:

You can press `Shift+Page Up` and `Shift+Page Dn` to scroll through the messages.

6. Check the status of the `vpms` service by entering the `service vpms status` command.

If the `vpms` service is running properly, the command displays messages indicating that the `tomcat`, `SL`, and `ActiveMQ` services are all running. The command ends with the message: `Overall Status: VPMS is running.`

7. To unmount and eject the DVD:
 - a. Change the directory to a location that is outside the mount point. For example, enter the `cd /` command to change to the root directory.
 - b. Unmount the DVD as described in the server documentation.
 - c. To eject the Experience Portal installation DVD, press the button on the DVD drive or enter the `eject` command.
8. Load the environment variables created during the installation by logging out of Linux and then logging back in.
 - a. Log out of the Linux system.
 - b. If you are logged in remotely, log back in to Linux by entering a non-root user name and password at the prompts, and log back in as root or `sroot`.
 - On an Avaya Enterprise Linux server, enter the `su - sroot` command.
 - On a Red Hat Enterprise Linux Server, enter the `su -` command.
 - c. If you are logged in directly through a console, log in to the local Linux console as `sroot`.
9. To verify that NTP is operating properly on the server, enter the `/usr/sbin/ntpq -np` command.

A status message similar to the following is displayed:

```

remote      refid      st t when poll reach  delay
offset jitter
=====
*127.127.1.0  73.78.73.84    5 1   4   64  377   0.000
0.000   0.001

```

Ensure that:

- The remote IP address is `*127.127.1.0`.
 - The jitter value is *not* 4000.
10. If you use Avaya Enterprise Linux on a single Experience Portal server that has an application server installed on it, you must start the application server by entering the `/sbin/service appserver start` command.

Next steps

- Verify if the Signature Algorithm displayed on the EPM certificate is SHA256withRSA.
 1. Log in to EPM and navigate to the **System Configuration > EPM Servers** page.
 2. Click on the Primary EPM name to view the details of the Primary EPM server certificate.
 3. If the Signature Algorithm displayed on the EPM certificate is not SHA256withRSA, run the `GenerateServerCertificate` script to generate or the `ImportServerCertificate.sh` script to import a SHA256 2048 bit server certificate. For more information about the `GenerateServerCertificate` and `ImportServerCertificate.sh` scripts, see *Administering Avaya Aura® Experience Portal*.

- Since the root certificate is not modified on any upgrade, you can generate and replace the root certificate from the EPM Web interface. For more information see *Administering Avaya Aura® Experience Portal*.
- For upgrade verification, navigate to `Support/VP-Tools/` and run the `EPInstallationVerifier` script.

*** Note:**

To run the script, enter the `./EPInstallationVerifier <InstallationLogDirectory>` command where `<InstallationLogDirectory>` is located in `/opt/Avaya/ExperiencePortal/logs` and is specified at the end of each upgrade. An example of the command: `./EPInstallationVerifier /opt/Avaya/ExperiencePortal/logs/install_2013-12-01.000`.

- Upgrade the Auxiliary EPM server by repeating this procedure.
- After upgrading the Primary and Auxiliary EPM servers, upgrade the MPPs.
- Install any required patches that you download from the Avaya online support Web site, <http://support.avaya.com>.
- To use an EPM 7.0.1 server with an older version of MPP server, restart the MPP from the **MPP Manager** page in EPM.
- If you wish to change the postgres database password specified by the auto upgrade utility, run the `SetDbPassword.sh` script.

! Important:

If Proactive Outreach Manager is installed on this system, then you must run the script `SetDbPassword.sh` to change the password for the database user postgres. The Experience Portal upgrade program automatically generates a new password for the database user postgres. However, Proactive Outreach Manager is already configured to use the old password. To keep Proactive Outreach Manager working, you must change the password for the database user postgres back to the value that you have configured in Proactive Outreach Manager. For more information about configuring the PostgreSQL database user accounts, see *Administering Avaya Aura® Experience Portal*.

*** Note:**

The auto upgrade utility specifies the postgres database password that was set during the Experience Portal installation. The utility overwrites the post installation password changes, if any.

- Install the Avaya Service Account authentication file. For more information about installing the Avaya Service Account authentication file, see *Troubleshooting Avaya Aura® Experience Portal*.

Upgrading the Primary EPM software interactively

Before you begin

- Ensure that you upgrade the operating system on the server as described in [Operating system upgrade overview](#) on page 19.

! Important:

If you upgrade the Experience Portal software on a Red Hat Linux server, ensure that you have copied the back up files on the server as described in [Copying and restoring the backup files on Red Hat Enterprise Linux Server](#) on page 48.

- Complete the [Primary EPM server upgrade worksheet](#) on page 147 and have it available to help answer the questions raised during the installation.
- Before you upgrade the software, read the Avaya Aura® Experience Portal release notes on the Avaya Aura® Experience Portal installation DVD under *Documentation*. These release notes contain information about the product that is not included in the formal documentation set.
- Download any patches for Avaya Aura® Experience Portal Release 7.0.1 from the Avaya Support Web site at <http://support.avaya.com>.
- Ensure that you have completed the software upgrade prerequisites described in [Prerequisites overview for upgrading Experience Portal](#) on page 38.
- For disk space related information, see [Space requirement for upgrading primary EPM on Red Hat Enterprise Linux](#) on page 41 and [Space requirements for upgrading primary EPM on Avaya Enterprise Linux](#) on page 41.
- If you have installed a managed application, contact the provider of the managed application to check if you need to perform any additional steps as part of the Experience Portal upgrade.

Procedure

1. Log in to the server on which you want to upgrade the Experience Portal software.

If you are an Avaya Services representative, and use Avaya Enterprise Linux or if the Avaya Service accounts are installed on this server:

- Log in to the local Linux console as `sroot`.
- Or log in remotely as a non-root user and then change the user to `sroot` by entering the `su - sroot` command.

Otherwise, log in to Linux locally as `root`, or log in remotely as a non-root user and then change the user to `root` by entering the `su -` command.

*** Note:**

Ensure that you upgrade using the same Linux account that was used during the prior installation. If you upgrade a Voice Portal or Experience Portal system by using a Linux account that is different than the account used during the previous install or upgrade, the upgrade might fail.

2. Insert the Avaya Aura® Experience Portal 7.0.1 software installation DVD into the DVD drive of the server.

+ Tip:

These instructions assume that you are going to access the Experience Portal installation DVD by mounting the appropriate DVD drive on the target system. If you want to access the installation DVD files from a shared network directory or a local

directory, you can copy the files from the Experience Portal installation DVD to that directory. However, that directory must be readable by all users on the system. If the directory is only readable by the root or `sroot` user, the installation script will encounter errors and will not complete successfully.

3. Mount the Avaya Aura® Experience Portal 7.0.x software installation DVD. The `mount` command depends on the server's hardware and operating system.

- If you are working with Avaya Enterprise Linux, mount the DVD by entering the `mount /mnt/cdrom` command, where `/mnt/cdrom` is the mount point typically associated with the DVD drive in the `fstab` file.
- If you are working with a supported version of Red Hat Enterprise Linux Server, to mount the DVD:
 - Run the `mkdir /media/cdrom` command.

 Note:

This command is required only if the `/media/cdrom` mount point does not exist.

- Run the `mount /dev/cdrom /media/cdrom` command.

 Warning:

When Red Hat Enterprise Linux Server automatically mounts the DVD, the files on the DVD are not executable. You must manually mount the Experience Portal installation DVD using the commands shown above.

If the `mount` commands shown above do not work, consult your server documentation for the appropriate `mount` command.

4. Change to the mount point directory.
5. Enter the `bash installvp` command and press `Enter` to start the installation script.

If the 32-bit glibc package is not already installed, the installer displays the message For the Experience Portal installer to run, 32-bit glibc must be installed.

6. If the installer displays the message that you must install 32-bit glibc, type `Y` or press `Enter` to proceed with the 32-bit glibc installation.
7. On the Installation Destination screen, ensure the installation path is the same as the previous installation, and press `Enter`.

 Important:

Do not change the installation directory when upgrading to a new release.

When choosing installation options, wait for the next prompt before pressing a key. The installation stores your key presses in a buffer and enters all the key presses after the current processing completes. For example, if you press the `Enter` key repeatedly while the system is performing its prerequisite checks, you might unintentionally skip options

- you want to change. Use the **Previous** option on any screen to go back and change your earlier choices.
8. Press `Enter` to move to the next screen.
 9. On the Avaya Aura® Experience Portal **Feature Selection** screen:
 - a. Ensure that the **EPM** and **Documentation** options are selected.
 - b. Press `Enter` to confirm your selections.
 10. Press `Enter` to move to the next screen.
 11. On the Version Confirmation screen, verify that:
 - The **Installed Version** column indicates the previous version of Experience Portal that was installed on the server.
 - The **New Version** column indicates that you are upgrading to release 7.0.1.
 - If you upgrade a server that uses Red Hat Enterprise Linux Server, only the feature EPM shows the **Install Type** as **Upgrade**. The feature **Documentation** shows the **Install Type** as **Full Install**.
 - For upgrading an MPP on Red Hat Enterprise Linux Server, the **Installed Version** displays **Not Installed** and the **Install Type** displays **Full Install**.
 - For upgrading an on Avaya Enterprise Linux, the **Install Type** column shows as **Upgrade** for all selected features.
 12. Press `Enter` to move to the next screen.
 13. Read through the end user license agreement.
 14. On the final End User License Agreement page, type `1` and press `Enter` to select option **1 - I accept the terms of the license agreement**.

The screen refreshes with **1 - I accept the terms of the license agreement** as the selected option.
 15. Press `Enter` to accept the agreement.
 16. Press `Enter` to move to the next screen.

Experience Portal automatically starts the Prerequisite Checker, which analyzes your system's hardware and operating system configuration.
 17. After the configuration analysis is complete, the Prerequisite Checker displays a message stating whether all prerequisite checks passed followed by the first Prerequisite Status page. Press `Enter` to view the rest of the Prerequisite Status pages.

If any of the prerequisite installation fails, examine the Prerequisite Status pages carefully to determine which checks failed. You must correct these issues before you can continue with this procedure.
 18. When all prerequisite checks pass, press `Enter` to move to the next screen.

Experience Portal automatically starts the Prerequisite Installer, which attempts to install the required software on the Experience Portal server.

 Important:

The length of time the Prerequisite Installer takes depends on the size of your old Experience Portal database, because this process is also upgrading that database. Do NOT cancel the installation while the Prerequisite Installer is running or you may damage your database.

19. After the Prerequisite Installer completes installing the required software, the installer displays the Installation Status pages. Press `Enter` to view the rest of the Installation Status pages.

If any prerequisite installations fail, examine the Installation Status pages carefully to determine which installations failed. You must correct these issues before you can continue with this procedure.

20. When all prerequisites are successfully installed, press `Enter` to move to the next screen.

21. On the Add/Edit EPM User Manager Account screen, if you want to:

- Create a new **user manager** account or change the password of an existing account:
 - a. Verify that option **1 - Yes** is selected. If it is not selected, type `1` and press `Enter`.
 - b. Press `Enter` twice to confirm the selection and move to the next screen.
 - c. On the EPM Administrator screen, type the new or existing account user name and press `Enter`.

 Note:

If you enter an existing account user name, Experience Portal changes the password for that account. Make sure that any users who log in with that user name know about the new password.

- d. Type the password for this account and press `Enter`.
 - e. Confirm the password by typing it again and pressing `Enter`.
- Retain current account settings:
 - a. Verify that option **2 - No** is selected. If it is not selected, type `2` and press `Enter`.
 - b. Press `Enter` to confirm your selection.

22. Press `Enter` to move to the next screen.

23. You can create a PostgreSQL database user account that can read the report data in the Experience Portal database. If you:

- Want to create the report reader database account:
 - a. Type `1` and press `Enter`.
 - b. Press `Enter` to confirm your selection.

- c. To use the account name in square brackets ([]), press `Enter` at the installation prompt. Otherwise, type a unique user name for the account and press `Enter`.
- d. Type a password for the account and press `Enter`.
- e. Confirm the password by typing the password again and press `Enter`.
- Do not want to create the report reader account:
 - a. Verify that option **2 - No** is selected. If it is not selected, type `2` and press `Enter`.
 - b. Press `Enter` to confirm your selection.

 Note:

This user account can only read those tables in the Experience Portal database that store report data. Speech application developers can use this account to log in to the database to create custom reports using any SQL-enabled report generation tool.

- 24. Press `Enter` to move to the next screen.
- 25. On the Database Login for Auxiliary EPM screen, you can specify whether you want to create a PostgreSQL user account for the optional Auxiliary EPM server. The user account provides the Auxiliary EPM server limited access to the main Experience Portal database, and you require the user account to configure an Auxiliary EPM server.
 - If you want to create the Auxiliary EPM login account:
 - a. Type `1` and press `Enter`.
 - b. Press `Enter` to confirm your selection.
 - c. Type the password for the account and press `Enter`.
 - d. Confirm the password by typing the password again and press `Enter`.
 - If you do not want to create the Auxiliary EPM login account:
 - a. Verify that option **2 - No** is selected. If it is not selected, type `2` and press `Enter`.
 - b. Press `Enter` to confirm your selection.
- 26. Press `Enter` to move to the next screen.
- 27. On the Product ID screen:
 - If you upgrade the software on an Avaya Enterprise Linux server, you can either:
 - a. Use the existing Product ID that was generated with the Automatic Registration Tool (ART) for this installation of Experience Portal, and press `Enter`.
 - b. Or use a new Product ID, type the ID and press `Enter`.
 - If you upgrade the software on a supported version of Red Hat Enterprise Linux Server:
 - a. Enter the Product ID that is generated with the Automatic Registration Tool (ART) for this installation of Experience Portal.
 - b. Press `Enter`.

The notification feature uses the Product ID to generate SNMP traps. SNMP traps are unsolicited notifications of significant events from an SNMP agent to an SNMP manager. The SNMP agent resides on a managed network device.

28. Press `Enter` to move to the next screen.
29. Experience Portal uses the ssl protocol to establish a secure connection between its servers. This connection requires a security certificate that can be created by Experience Portal or purchased from a third-party company. On the Security Certificate screen:

- If you want Experience Portal to create a security certificate:
 - a. Verify that option **1 - Create a new certificate for this server** is selected. If not, type `1` and press `Enter`.
 - b. Press `Enter` to confirm that selection.

 Note:

The Experience Portal installer generates and installs a SHA256 2048 bit server certificate by default. The installer also generates and installs a SHA256 2048 bit EPM Root certificate.

- If you want to import a self-signed or third party certificate, ensure the following:
 - The certificate is in PKCS#12 format. The certificate must be formatted as a PKCS#12 file. A PKCS#12 file always includes a certificate and the corresponding key, and the certificate is encrypted and requires a password. If the certificate is not self-signed then the PKCS#12 file must include the CA certificates.
 - If the “Extended Key Usage” is specified in the X509.V3 certificate extension, specify “Server Authentication” (also called “serverAuth”) and Client Authentication” (also called “clientAuth”), for the usage.
 - The certificate resides on the local server or on an NFS-mounted drive that is locally accessible.

To import a self-signed or third party certificate, do the following:

- a. Verify that option **2 - Import a certificate from a specified location** is selected. If not, type `2` and press `Enter`.
 - b. Press `Enter` to confirm that selection.
 - c. Type the full file path and name of the security certificate and press `Enter`.
The screen displays the location that you entered for your verification.
 - d. Type the password for the security certificate and press `Enter`.
30. Press `Enter` to move to the next screen.
 31. On the Security Certificate Verification screen, verify the security certificate and press `Enter` to move to the next screen.

+ Tip:

When you add the MPP to Experience Portal through the EPM Web interface, the EPM displays the MPP security certificate. You should record the fingerprint information from this security certificate so that you can compare it to the one displayed in the EPM Web interface.

If the imported certificate is a chained certificate, then the final signed certificate (also called the end certificate) of the chained certificate is displayed in the EPM Web interface.

32. On the Pre Installation Summary screen, verify the installation information and press `Enter` to install the Experience Portal software.

Experience Portal displays the Installation Progress screen and begins installing the software. During the install, it displays messages indicating its progress.

The installation process can appear completed or stopped even though it is still processing and installing the software. Wait until Experience Portal displays the Post Installation Summary screen.

33. On the Post Installation Summary screen, verify that the **Installation Progress Bar** has reached 100% and that the message `...done installing feature_name` appears for each feature that you selected on the Experience Portal Feature Selection screen.

*** Note:**

If the **Installation Progress Bar** on the Installation Progress screen stops at 25% and the Post Installation Summary screen states that no summary information could be found, see *Upgrading to Avaya Aura® Experience Portal 7.0.1* on <http://support.avaya.com>.

34. Press `Enter` to end the installation script.

During the installation process, Experience Portal creates several log files that you can use to verify what happened during installation. When the installation process is complete, Experience Portal moves the logs to the standard log directory and displays the exact path on the screen. For more information, see [Upgrade installation log files](#) on page 121.

35. To unmount and eject the DVD:
 - a. Change the directory to a location that is outside the mount point. For example, enter the `cd /` command to change to the root directory.
 - b. Unmount the DVD as described in the server documentation.
 - c. To eject the Experience Portal installation DVD, press the button on the DVD drive or enter the `eject` command.
36. Load the environment variables created during the installation by logging out of Linux and then logging back in.
 - a. Log out of the Linux system.

- b. If you are logged in remotely, log back in to Linux by entering a non-root user name and password at the prompts, and log back in as root or `sroot`.
 - On an Avaya Enterprise Linux server, enter the `su - sroot` command.
 - On a Red Hat Enterprise Linux Server, enter the `su -` command.
 - c. If you are logged in directly through a console, log in to the local Linux console as `sroot`.
37. Check the status of the `vpms` service by entering the `service vpms status` command.

If the `vpms` service is running properly, the command displays messages indicating that the `tomcat`, `SL`, and `ActiveMQ` services are all running. The command ends with the message: Overall Status: VPMS is running.

Next steps

- Verify if the Signature Algorithm displayed on the EPM certificate is SHA256withRSA.
 1. Log in to EPM and navigate to the **System Configuration > EPM Servers** page.
 2. Click on the Primary EPM name to view the details of the Primary EPM server certificate.
 3. If the Signature Algorithm displayed on the EPM certificate is not SHA256withRSA, run the `GenerateServerCertificate` script to generate or the `ImportServerCertificate.sh` script to import a SHA256 2048 bit server certificate. For more information about the `GenerateServerCertificate` and `ImportServerCertificate.sh` scripts, see *Administering Avaya Aura® Experience Portal*.
- Since the root certificate is not modified on any upgrade, you can generate and replace the root certificate from the EPM Web interface. For more information see *Administering Avaya Aura® Experience Portal*.
- For upgrade verification, navigate to `Support/VP-Tools` and run the `EPInstallationVerifier` script.

Note:

To run the script, enter the `./EPInstallationVerifier <InstallationLogDirectory>` command where `<InstallationLogDirectory>` is located in `/opt/Avaya/ExperiencePortal/logs` and is specified at the end of each upgrade. An example of the command: `./EPInstallationVerifier /opt/Avaya/ExperiencePortal/logs/install_2013-12-01.000`.

- Install any required patches that you download from the Avaya online support Web site, <http://support.avaya.com>.
- To use an EPM 7.0.1 server with an older version of MPP server, run the `setup_vpms.php` script on the MPP server to authorize the security certificate, and restart the MPP.
- Reestablish the link between the MPP and the EPM as described in [Reestablishing the link between the EPM and the MPP](#) on page 103.
- Navigate to the **MPP Manager** page in EPM and restart the MPPs
- If the Auxiliary EPM has outcalls in progress, do not run `setup_vpms.php` script on the Auxiliary EPM server.
- Upgrade the Auxiliary EPM. For more information, see [Auxiliary EPM software upgrade overview](#) on page 66.

! Important:

If you are running outcalls during the upgrade, you must upgrade the Auxiliary EPM before upgrading the MPPs.

- If you wish to change the postgres database password specified by the auto upgrade utility, run the SetDbPassword.sh script.

! Important:

If Proactive Outreach Manager is installed on this system, then you must run the script SetDbPassword.sh to change the password for the database user postgres. The Experience Portal upgrade program automatically generates a new password for the database user postgres. However, Proactive Outreach Manager is already configured to use the old password. To keep Proactive Outreach Manager working, you must change the password for the database user postgres back to the value that you have configured in Proactive Outreach Manager. For more information about configuring the PostgreSQL database user accounts, see *Administering Avaya Aura® Experience Portal*.

- The Authentication File System (AFS) tool from Avaya Services generates a new file. For more information about reinstalling the Avaya Service Account authentication file, see *Troubleshooting Avaya Aura® Experience Portal*.

Upgrading an Auxiliary EPM server

Auxiliary EPM software upgrade overview

There are two upgrade options for the Auxiliary EPM server.

- Automatic upgrade: For Avaya Enterprise Linux users only
- Interactive upgrade: For Avaya Enterprise Linux and Red Hat Enterprise Linux Server users

+ Tip:

In Experience Portal 7.0.1, the certificate generation code is enhanced to use a more secure hashing algorithm. Avaya recommends that you upgrade to Experience Portal 7.0.1 by using the Interactive upgrade option so that you can generate a SHA256 2048 bit server certificate (the new security certificate) to make the systems more secure.

Automatic upgrade

Launch the Avaya Aura® Experience Portal installation program and run the auto upgrade utility to upgrade to Avaya Aura® Experience Portal 7.0.1 on an Avaya Enterprise Linux server. The Experience Portal automatic upgrade utility, autoupgradevp, does not prompt for any input. The utility uses the installation options that were chosen during the previous installation.

! Important:

Upgrade the Primary EPM server before the Auxiliary EPM server.

The automatic upgrade utility:

- Uses the existing installation directories.
- Uses the existing security certificate for the Auxiliary EPM.

*** Note:**

You cannot change these default options during the upgrade.

The system displays error messages, if any, at the end of the upgrade process and records all messages in the installation log files.

*** Note:**

Automatic upgrade is the recommended upgrade option if you want to upgrade to Avaya Aura® Experience Portal 7.0.1 on an Avaya Enterprise Linux server and you do not need changes to the configurations.

For more information, see [Automatically upgrading the EPM software](#) on page 53.

Interactive EPM upgrade

On the Auxiliary EPM server, you launch the Experience Portal installation program and answer the prompts as they are displayed.

! Important:

Upgrade the Primary EPM server before the Auxiliary EPM server. While upgrading the Auxiliary EPM server, you are prompted for the following details related to the Primary EPM server:

- IP address of the Primary EPM server so that the system can retrieve the security certificate. To ensure that the system retrieves the updated certificate from the Primary server, upgrade the Primary server first.
- The vpcommon password that was specified during the Primary EPM upgrade. This user account allows the Auxiliary EPM server limited access to the main Experience Portal database.

+ Tip:

If you need to make changes to the configurations during the upgrade, use the Interactive upgrade option.

Upgrading the Auxiliary Experience Portal software interactively

Before you begin

- Upgrade the Primary EPM server before you upgrade the Auxiliary EPM server.
- Complete the [Auxiliary EPM server upgrade worksheet](#) on page 150 and have it available to help answer the questions raised during the upgrade.
- Before you upgrade the software, read the Avaya Aura® Experience Portal release notes on the Avaya Aura® Experience Portal installation DVD under *Documentation*. These release notes contain information about the product that is not included in the formal documentation set.

- Download any patches for Avaya Aura® Experience Portal Release 7.0.1 from the Avaya Support Web site at <http://support.avaya.com>.
- Ensure that you upgrade the server operating system as described in [Operating system upgrade overview](#) on page 19.
- Ensure that you complete the software upgrade prerequisites described in [Prerequisites overview for upgrading Experience Portal](#) on page 38.
- If you have installed a managed application, contact the provider of the managed application to check if you need to perform any additional steps as part of the Experience Portal upgrade.

Procedure

1. Log in to the server on which you want to upgrade the Auxiliary EPM software.

If you are an Avaya Services representative, and use Avaya Enterprise Linux or if the Avaya Service accounts are installed on this server:

- Log in to the local Linux console as `sroot`.
- Or log in remotely as a non-root user and then change the user to `sroot` by entering the `su - sroot` command.

Otherwise, log in to Linux locally as root, or log in remotely as a non-root user and then change the user to root by entering the `su -` command.

Note:

Ensure that you upgrade using the same Linux account that was used during the prior installation. If you upgrade a Voice Portal or Experience Portal system by using a Linux account that is different than the account used during the previous install or upgrade, the upgrade might fail.

2. Insert the Avaya Aura® Experience Portal 7.0.1 software installation DVD into the DVD drive of the server.

Tip:

These instructions assume that you are going to access the Experience Portal installation DVD by mounting the appropriate DVD drive on the target system. If you want to access the installation DVD files from a shared network directory or a local directory, you can copy the files from the Experience Portal installation DVD to that directory. However, that directory must be readable by all users on the system. If the directory is only readable by the root or `sroot` user, the installation script will encounter errors and will not complete successfully.

3. Mount the Avaya Aura® Experience Portal 7.0.x software installation DVD. The `mount` command depends on the server's hardware and operating system.
 - If you are working with Avaya Enterprise Linux, mount the DVD by entering the `mount /mnt/cdrom` command, where `/mnt/cdrom` is the mount point typically associated with the DVD drive in the `fstab` file.

- If you are working with a supported version of Red Hat Enterprise Linux Server, to mount the DVD:

- Run the `mkdir /media/cdrom` command.

 Note:

This command is required only if the `/media/cdrom` mount point does not exist.

- Run the `mount /dev/cdrom /media/cdrom` command.

 Warning:

When Red Hat Enterprise Linux Server automatically mounts the DVD, the files on the DVD are not executable. You must manually mount the Experience Portal installation DVD using the commands shown above.

If the `mount` commands shown above do not work, consult your server documentation for the appropriate `mount` command.

4. Change to the mount point directory.
5. Enter the `bash installvp` command and press `Enter` to start the installation script.

If the 32-bit glibc package is not already installed, the installer displays the message `For the Experience Portal installer to run, 32-bit glibc must be installed.`

6. If the installer displays the message that you must install 32-bit glibc, type `Y` or press `Enter` to proceed with the 32-bit glibc installation.
7. On the Installation Destination screen, press `Enter` to upgrade the software in the same location as the previous release.

 Important:

You must not change the installation directory when upgrading to a new release.

When choosing installation options, wait for the next prompt before pressing a key. The installation stores your key presses in a buffer and enters all the key presses after the current processing completes. For example, if you press the `Enter` key repeatedly while the system is performing its prerequisite checks, you might unintentionally skip options you want to change. Use the **Previous** option on any screen to go back and change your earlier choices.

8. Press `Enter` to move to the next screen.
9. On the Experience Portal Feature Selection screen, press `Enter` to accept the default installation options of **EPM** and **Documentation**.
10. Press `Enter` to move to the next screen.

11. On the Version Confirmation screen:
 - If you are upgrading the Experience Portal software on an Avaya Enterprise Linux server, verify that:
 - The **Install Type** says **Full Install** for all selected features.
 - The **New Version** column indicates the 7.0.1 release .
 - If you are upgrading the Experience Portal software on Red Hat Enterprise Linux Server, verify that the **New Version** column indicates the 7.0.1 release.
12. Press `Enter` to move to the next screen.
13. Read through the end user license agreement.
14. On the final End User License Agreement page, type `1` and press `Enter` to select option **1 - I accept the terms of the license agreement**.

The screen refreshes with **1 - I accept the terms of the license agreement** as the selected option.
15. Press `Enter` to accept the agreement.
16. Press `Enter` to move to the next screen.

Experience Portal automatically starts the Prerequisite Checker, which analyzes your system's hardware and operating system configuration.
17. After the configuration analysis is complete, the Prerequisite Checker displays a message stating whether all prerequisite checks passed followed by the first Prerequisite Status page. Press `Enter` to view the rest of the Prerequisite Status pages.

If any of the prerequisite installation fails, examine the Prerequisite Status pages carefully to determine which checks failed. You must correct these issues before you can continue with this procedure.
18. When all prerequisite checks pass, press `Enter` to move to the next screen.

Experience Portal automatically starts the Prerequisite Installer, which attempts to install the required software on the Experience Portal server.
19. After the Prerequisite Installer completes installing the required software, the installer displays the Installation Status pages. Press `Enter` to view the rest of the Installation Status pages.

If any prerequisite installations fail, examine the Installation Status pages carefully to determine which installations failed. You must correct these issues before you can continue with this procedure.
20. When all prerequisites are successfully installed, press `Enter` to move to the next screen.
21. On the Primary EPM Server Location screen, type the hostname or IP address of the Primary EPM server and press `Enter`.
22. Press `Enter` to move to the next screen.

23. On the Public Key Verification screen, if you recorded the fingerprint information from the EPM security certificate during the Primary EPM software installation. Compare the certificate to the Public Key fingerprint information presented on the screen. The fingerprint information from Public Key must match the fingerprint information from the EPM security certificate.

If the public key is not downloaded, see [MPP or Auxiliary EPM could not import EPM key](#) on page 132.

24. Press `Enter` to move to the next screen.
25. On the **Database Login Check for Auxiliary EPM** screen, type the password for the user `vpcommon` that you specified when you installed the Primary EPM.
26. Press `Enter` to move to the next screen.

Experience Portal makes sure that it can contact the Primary EPM server, and that the password you entered matches the one specified when the Primary EPM server was installed. If the connection can be established and the password is correct, Experience Portal continues to the next screen.

27. You can create a PostgreSQL database user account on the Auxiliary EPM server that can read the report data in the Auxiliary Experience Portal database. If you:

- Want to create the report reader database account:
 - a. Type `1` and press `Enter`.
 - b. Press `Enter` to confirm your selection.
 - c. To use the account name in square brackets (`[ ]`), press `Enter` at the installation prompt. Otherwise, type a unique user name for the account and press `Enter`.
 - d. Type a password for the account and press `Enter`.
 - e. To confirm the password, type the password again and press `Enter`.
- Do not want to create the report reader account:
 - a. Verify that option **2 - No** is selected. If it is not selected, type `2` and press `Enter`.
 - b. Press `Enter` to confirm your selection.

 Note:

This user account can only read those tables in the Experience Portal database that store report data. You should create this account if you plan to set up an external database on this server that is shared by multiple Experience Portal systems and you want to create custom reports for the database using an SQL-enabled report generation tool.

28. Press `Enter` to move to the next screen.
29. You can create a PostgreSQL database user account on the Auxiliary EPM server that can allow external systems to write report data into the Experience Portal database on this server.

You should create this account if you plan to set up an external database on this server that is shared by multiple Experience Portal systems.

- If you want to create the report writer database account:
 - a. Type `1` and press `Enter`.
 - b. Press `Enter` to confirm your selection.
 - c. To use the account name in square brackets (`[ ]`), press `Enter` at the installation prompt. Otherwise, type a unique user name for the account and press `Enter`.
 - d. Type the password for this account and press `Enter`.
 - e. Confirm the password by typing it again and pressing `Enter`.
- If you do not want to create the report writer account, press `Enter`.

 Note:

This user account can only change the data in the tables that store report data in the Experience Portal database on the Auxiliary EPM server.

30. Press `Enter` to move to the next screen.
31. Experience Portal uses the ssl protocol to establish a secure connection between its servers. This connection requires a security certificate that can be created by Experience Portal or purchased from a third-party company. On the Security Certificate screen:
 - If you want Experience Portal to create a security certificate:
 - a. Verify that option **1 - Create a new certificate for this server** is selected. If not, type `1` and press `Enter`.
 - b. Press `Enter` to confirm that selection.

 Note:

The Experience Portal installer generates and installs a SHA256 2048 bit server certificate by default. The installer also generates and installs a SHA256 2048 bit EPM Root certificate.

- If you want to import a self-signed or third party certificate, ensure the following:
 - The certificate is in PKCS12 format. The certificate must be formatted as a PKCS#12 file. A PKCS#12 file always includes a certificate and the corresponding key, and the certificate is encrypted and requires a password. If the certificate is not self-signed then the PKCS#12 file must include the CA certificates.
 - If the “Extended Key Usage” is specified in the X509.V3 certificate extension, specify “Server Authentication” (also called “serverAuth”) and Client Authentication” (also called “clientAuth”), for the usage.
 - The certificate resides on the local server or on an NFS-mounted drive that is locally accessible.

To import a self-signed or third party certificate, do the following:

- a. Verify that option **2 - Import a certificate from a specified location** is selected. If not, type 2 and press `Enter`.
- b. Press `Enter` to confirm that selection.
- c. Type the full file path and name of the security certificate and press `Enter`.

The screen displays the location that you entered for your verification.

- d. Type the password for the security certificate and press `Enter`.
32. Press `Enter` to move to the next screen.
33. On the Security Certificate Verification screen, verify the security certificate and press `Enter` to move to the next screen.

+ Tip:

When you add an Auxiliary EPM to Experience Portal through the EPM Web interface, the EPM displays the Auxiliary EPM's security certificate. You should record the fingerprint information from this security certificate so that you can compare it to the one displayed in the EPM Web interface.

If the imported certificate is a chained certificate, then the final signed certificate (also called the end certificate) of the chained certificate is displayed on the EPM.

34. On the Pre Installation Summary screen, verify the installation information and press `Enter` to install the Experience Portal software.

Experience Portal displays the Installation Progress screen and begins installing the software. During the install, it displays messages indicating its progress.

The installation process can appear completed or stopped even though it is still processing and installing the software. Wait until Experience Portal displays the Post Installation Summary screen.

35. On the Post Installation Summary screen, verify that the **Installation Progress Bar** has reached 100% and that the message `...done installing feature_name` appears for each feature that you selected on the Experience Portal Feature Selection screen.

*** Note:**

If the **Installation Progress Bar** on the Installation Progress screen stops at 25% and the Post Installation Summary screen states that no summary information could be found, see *Upgrading to Avaya Aura® Experience Portal 7.0.1* on <http://support.avaya.com>.

36. Press `Enter` to end the installation script.

During the installation process, Avaya Aura® Experience Portal creates several log files that you can use to verify the installation process. When the installation process is complete, Avaya Aura® Experience Portal moves the logs to the standard log directory and displays the exact path on the screen. For more information, see [Upgrade installation log files](#) on page 121.

37. To unmount and eject the DVD:

- a. Change the directory to a location that is outside the mount point. For example, enter the `cd /` command to change to the root directory.
- b. Unmount the DVD as described in the server documentation.
- c. To eject the Experience Portal installation DVD, press the button on the DVD drive or enter the `eject` command.

38. Load the environment variables created during the installation by logging out of Linux and then logging back in.

- a. Log out of the Linux system.
- b. If you are logged in remotely, log back in to Linux by entering a non-root user name and password at the prompts, and log back in as root or `sroot`.
 - On an Avaya Enterprise Linux server, enter the `su - sroot` command.
 - On a Red Hat Enterprise Linux Server, enter the `su -` command.
- c. If you are logged in directly through a console, log in to the local Linux console as `sroot`.

39. To verify that NTP is operating properly on the server, enter the `/usr/sbin/ntpq -np` command.

A status message similar to the following is displayed:

```

remote          refid          st t when poll reach  delay
offset  jitter
=====
*127.127.1.0    73.78.73.84      5 1   4   64  377   0.000
0.000   0.001

```

Ensure that:

- The remote IP address is `*127.127.1.0`.
- The jitter value is *not* 4000.

40. Check the status of the `vpms` service by entering the `service vpms status` command.

If the `vpms` service is running properly, the command displays messages indicating that the `tomcat`, `SL`, and `ActiveMQ` services are all running. The command ends with the message: Overall Status: VPMS is running.

Next steps

- Verify if the Signature Algorithm displayed on the certificate is SHA256withRSA.
 1. Log in to EPM and navigate to the **System Configuration > EPM Servers** page.
 2. Click on the Auxiliary EPM name to view the details of the Auxiliary EPM server certificate.
 3. If the Signature Algorithm displayed on the EPM certificate is not SHA256withRSA, run the `GenerateServerCertificate` script to generate or the `ImportServerCertificate.sh` script to import a SHA256 2048 bit server certificate. For more information about the

GenerateServerCertificate and ImportServerCertificate.sh scripts, see *Administering Avaya Aura® Experience Portal*.

- For upgrade verification, navigate to `Support/VP-Tools/` and run the EPIInstallationVerifier script.
- Install any required patches that you download from the Avaya online support Web site, <http://support.avaya.com>.
- Reestablish the link between the Primary EPM and the Auxiliary EPM:
 1. Log in to the EPM Web interface using an account with the Administration user role.
 2. From the EPM main menu, select **System Configuration > EPM Servers**.
 3. Click the name of the Auxiliary EPM server.
 4. On the Change EPM Server page, navigate to the **Auxiliary EPM Certificate** section and select the **Trust new certificate** check box if the check box is visible.
 5. Click **Save**.
- Upgrade the MPP software on the MPP servers as described in [Upgrading the MPP software interactively](#) on page 82.

 Note:

If you log in to the upgraded EPM before you upgrade the MPPs, all MPPs in the system might display **Restart Needed** in the **State** column on the System Monitor and MPP Manager pages. EPM automatically updates the state after you upgrade the MPP software and reconnect the upgraded MPP servers with the EPM.

- Install the Avaya Service Account authentication file. For more information about installing the Avaya Service Account authentication file, see *Troubleshooting Avaya Aura® Experience Portal*.

Upgrading the MPP software

MPP software upgrade overview

 Important:

Experience Portal 7.0.1 provides the functionality to use an EPM 7.0.1 server with an MPP 5.1, 6.0, or 7.0 server. If your system is configured to use more than one MPP, you can ensure that while you upgrade an MPP to 7.0.1, the other MPPs (of earlier versions) are functional. To use an EPM 7.0.1 server with an MPP 5.1, 6.0, or 7.0 server, you must run the `setup_vpms.php` script on the MPP 5.1, 6.0, or 7.0 server, trust the new certificate on the **Change MPP** page, and restart the MPP.

After you upgrade the Primary EPM and all Auxiliary EPMS, there are three MPP upgrade options.

+ Tip:

In Experience Portal 7.0.1, the certificate generation code is enhanced to use a more secure hashing algorithm. Avaya recommends that you upgrade to Experience Portal 7.0.1 by using the Interactive upgrade option so that you can generate a SHA256 2048 bit server certificate (the new security certificate) to make the systems more secure.

Automatic upgrade

Automatic upgrade option is for Avaya Enterprise Linux users only. Software only customers who are upgrading from Experience Portal 7.0 can also opt for the automatic upgrade option if:

- The operating system is not upgraded
- The operating system is upgraded in a way that retains the data on the system

Launch the Experience Portal installation program and run the auto upgrade utility. This method does not display prompts when the upgrade is in progress.

+ Tip:

Automatic upgrade is the recommended option if you upgrade the MPP software on Avaya Enterprise Linux and if no changes are required to the installation configuration.

For more information, see [Automatically upgrading the EPM software](#) on page 53.

Interactive MPP upgrade

On each server, launch the Experience Portal installation program and type the responses to the prompts. The procedure is similar to the interactive EPM software upgrade. For details, see [Upgrading the MPP software interactively](#) on page 82.

+ Tip:

Avaya recommends the Interactive upgrade option if you need to make changes to the MPP configurations during the upgrade.

Software upgrade from EPM Web interface

You can upgrade the software version of the MPPs running on your Experience Portal system from the **System Management > Software Upgrade** page in EPM. The **Software Upgrade** page lists only those software versions which have the .iso image set in the `$AVAYA_IA_HOME/download` directory. You can select one or more MPPs for a software upgrade. The MPPs will be taken out of service one at a time during the upgrade process. For more information about the Software Upgrade option, see *Administering Avaya Aura® Experience Portal*.

Silent MPP upgrade

When you upgrade the Primary EPM, Experience Portal automatically records your answers to basic questions, such as the installation directory details, the name of the EPM server, and security certificate information. EPM compiles the answers into a file that is used by the upgrade tool to upgrade the MPP software without further user input.

On each server, copy the installation files to a local directory on the MPP and run the silent install utility. The upgrade tool does not display prompts, but displays error messages at the end of the install process. The tool records all messages in the installation log files. For details, see [Upgrading the MPP software silently](#) on page 78.

 Note:

You can change the options before you run the silent installer. However, ensure that you save the customized install file in case you need to reinstall the software.

Reestablishing the link between the EPM and the upgraded MPP

After you upgrade the MPP software, you need to reestablish the link between the MPP and the EPM by trusting the MPP's security certificate.

Procedure

1. Log in to the EPM Web interface using an account with the Administration user role.
2. From the EPM main menu, select **System Configuration > MPP Servers**.
3. Click the name of the MPP server that is upgraded.
4. On the **Change MPP Server** page, navigate to the MPP Certificate section and select the **Trust new certificate** check box if the check box is visible.
5. Click **Save**.
6. From the EPM main menu, select **System Management > MPP Manager**.
7. If the **Mode** column displays **Offline**, you need to start the MPP. To start the MPP:
 - a. Select the check box next to the name of the MPP.
 - b. In the Mode Commands group, click **Online**.
 - c. Click **Refresh** to verify that the **Mode** column displays **Online** for the MPP.
 - d. Select the check box next to the name of the MPP.
 - e. In the **State Commands** group, click **Start** and confirm your selection when prompted.
 - f. Click **Refresh** to verify that the current state is **Running**.
8. Ensure that the telephony ports are correctly allocated to the MPP server:
 - a. From the EPM main menu, select **Real-time Monitoring > Port Distribution**.
 - b. On the **Port Distribution** page, verify the ports allocated to the MPP in the **Current Allocation** column.
 - c. Ensure that the **Mode** and **State** columns display **Online** and **In Service** status respectively.

Customizing the MPP silent install file for all MPPs

Follow this procedure to change the default options specified in the MPP installation answer file created by the EPM for all MPPs.

About this task

 Tip:

If you want to change the install file for a specific MPP, you should do that after you copy the installation files to the MPP.

Procedure

1. Log in to Linux on the EPM server.
2. Change to the share directory by entering the `cd $AVAYA_HOME/VPMS/share` command, where `$AVAYA_HOME` is the environment variable pointing to the name of the installation directory specified during the EPM software installation. The default variable definition is `/opt/Avaya/ExperiencePortal`.
3. Make a back up copy of the original MPP answer file by entering the `cp mppanswerfile mppanswerfile_original` command.
4. Open `mppanswerfile` in an ASCII editor.
5. Change the information as appropriate. Verify that you read the instructions in the file carefully before you change any of the information or the installation will not run properly.
6. Save and close the file.

Upgrading the MPP software silently

Before you begin

- If you want to change any of the default upgrade options for all MPPs, edit the default MPP answer file as described in [Customizing the MPP silent install file for all MPPs](#) on page 78.
- Make sure you have upgraded the server operating system as described in [Operating system upgrade overview](#) on page 19.
- Make sure the MPP server is offline.
- Make sure you have upgraded the EPM software on the Primary EPM server as described in [EPM software upgrade overview](#) on page 52.
- Ensure that you have upgraded the Auxiliary EPM software on the Auxiliary EPM server as described in [Auxiliary EPM software upgrade overview](#) on page 66.
- Download any patches for Avaya Aura® Experience Portal Release 7.0.1 from the Avaya Support Web site at <http://support.avaya.com>.
- Verify that the prerequisites have been met. For more information, see [Software upgrade prerequisites overview for upgrading from 5.1 or 6.0](#) on page 38.

About this task

* Note:

To upgrade the MPP software silently, you need to copy the installation files to the MPP or any other accessible file server. If you are using Red Hat Enterprise Linux Server, you can share the appropriate directory on the EPM server with your MPP servers instead of copying the files. This option does not work with Avaya Enterprise Linux, however, because network shares cannot be created with that operating system.

In order to work with all operating systems, these instructions assume that you are copying the files directly to the MPP. If you are sharing the EPM directory or using a file server, make the necessary adjustments to this procedure.

Procedure

1. Log in to Linux on the Experience Portal MPP server.

If you are an Avaya Services representative, and use Avaya Enterprise Linux or if the Avaya Service accounts are installed on this server:

- Log in to the local Linux console as `sroot`.
- Or log in remotely as a non-root user and then change the user to `sroot` by entering the `su - sroot` command.

Otherwise, log in to Linux locally as root, or log in remotely as a non-root user and then change the user to root by entering the `su -` command.

2. Make sure that the local directory into which you want to copy the files already exists. If not, create it.

You can create a directory using the following command: `mkdir /opt/<directory_name>`.

* Note:

Ensure that the directory name does not contain spaces. If there are spaces in the directory name, the installation script will encounter errors and will not complete successfully.

3. Copy the Experience Portal software .iso file from the EPM server to the MPP with a utility such as `scp`.

If you are using `scp`, enter the `scp -rp <NON_ROOT_USER>@<EPM_HOSTNAME>:/opt/Avaya/InstallAgent/download/<ISO_Name>.iso /opt/<directory_name>` command, where:

- `<NON_ROOT_USER>` is the name of a non-root user account on the EPM server
- `<EPM_HOSTNAME>` is the hostname or IP address of the EPM server
- `/opt/Avaya/InstallAgent/download/` is the directory in which the EPM software is installed.
- `<ISO_NAME>.iso` is the name of the ISO file to be transferred.
- `<directory_name>` is the name of the local directory that you have created.

For example, `scp -rp NonRoot@EPM_HOSTNAME:/opt/Avaya/InstallAgent/download/7.0.1.0.1305.iso /opt/<directory_name>`

The message for authenticity of host and the RSA key fingerprint is displayed if you are using scp with this host for the first time.

For example:

The authenticity of host '`<host_IP_address>` (`<host_IP_address>`)' can't be established. RSA key fingerprint is `b9:de:40:81:62:7d:ba:ba:13:a1:e6:fa:69:8c:72:f1`.

4. Select **Yes** to continue connecting. The following message is displayed:

Warning: Permanently added 'host IP address' (RSA) to the list of known hosts.

5. Enter the non root user password.
6. Copy the mppanswerfile from the EPM server to the MPP. You can use a utility such as scp.

For example: `scp <Non_Root_USER>@<EPM_HOSTNAME>:/opt/Avaya/ExperiencePortal/VPMS/share/mppanswerfile /opt/mppanswerfile`

7. Enter the non root user password.
8. Mount the installation iso file.
For example, enter the `cd /opt/<directory_name>` command.
9. Change to the mount point directory.
10. Enter the `mount -o loop <ImageFileName> <MountPoint>` command to mount the ISO image. For example, enter the `mount -o loop 7.0.1.0.1305.iso /mnt/cdrom` command.
11. Enter the `bash silentinstallmpp /opt/mppanswerfile` command to start the installation script.

As the script proceeds, it produces messages similar to the following:

Starting silent install for Avaya Aura Experience Portal MPP. This will take several minutes to complete. Please wait...

The Avaya Aura Experience Portal installation has completed. Review the following information. If there are errors or warnings, then please review the installation logs.

Installing Documentation...

...done installing Documentation

Installing MPP...

...done installing MPP

Moving installation logs to: `/opt/Avaya/ExperiencePortal/logs/<install_log_directory>`

12. Enter the `/sbin/service mpp status` command to verify that the MPP system manager is running.

The MPP server returns the message `mppsismgr (pid <pid>) is running`, where `<pid>` is the process id.

13. Load the environment variables created during the installation by logging out of Linux and then logging back in.
 - a. Log out of the Linux system.
 - b. If you are logged in remotely, log back in to Linux by entering a non-root user name and password at the prompts, and log back in as root or `sroot`.
 - On an Avaya Enterprise Linux server, enter the `su - sroot` command.
 - On a Red Hat Enterprise Linux Server, enter the `su -` command.
 - c. If you are logged in directly through a console, log in to the local Linux console as `sroot`.

14. To verify that NTP is operating properly on the MPP enter the `/usr/sbin/ntpq -np` command.

The system displays a status message similar to the following:

```
remote refid st t when poll reach delay offset jitter
=====
123.123.123.123 127.127.1.0 6 u 23 64 1 0.354 0.361 0.004
```

Ensure that:

- The remote IP address points to the Primary EPM server.
 - The jitter value is *not* 4000.
15. After the installation has completed, you can either delete the local directory into which you copied the installation files or leave those files on the server in case you need to reinstall the MPP.
 16. If this is the last MPP server in the Experience Portal system, you can delete the files in the `$AVAYA_HOME/EPM/share` directory on the EPM server, especially if you have saved the relevant installation files to the MPP server.

Important:

If you leave the files on the EPM or MPP servers and you have included secure information such as the password for a third-party certificate in the MPP answer file, verify that you secure the local installation directory so that only root or `sroot` users have access to those files.

Next steps

- Install any required patches that you download from the Avaya online support Web site, <http://support.avaya.com>.
- If desired, upgrade the MPP software on another server machine by repeating this procedure on that machine.

- Reestablish the connection between the upgraded MPP and the EPM server as described in [Reestablishing the link between the EPM and the upgraded MPP](#) on page 77.
- If required, upgrade the MPP software on another server machine by repeating this procedure on that machine.
- Configure and test the Experience Portal system. For more information, see [Avaya Aura Experience Portal system configuration overview for a system upgraded to 7.0.1](#) on page 108.

Upgrading the MPP software interactively

Before you begin

- Ensure that you have upgraded the EPM software on the Primary EPM server as described in [EPM software upgrade overview](#) on page 52.
- Ensure that you have upgraded the Auxiliary EPM software on the Auxiliary EPM server as described in [Auxiliary EPM software upgrade overview](#) on page 66.
- Download any patches for Avaya Aura® Experience Portal Release 7.0.1 from the Avaya Support Web site at <http://support.avaya.com>.
- Complete the [MPP server upgrade worksheet](#) on page 153 and have it available to help answer the questions raised during the installation.
- Ensure that the MPP server is offline.
- Ensure that you have upgraded the server operating system as described in [Operating system upgrade overview](#) on page 19.
- Prior to running the upgrade for an MPP, EPM, verify that the prerequisites have been met. For more information, see [Software upgrade prerequisites overview for upgrading from 5.1 or 6.0](#) on page 38.

Procedure

1. Log into the server on which you want to upgrade the MPP software.

If you are an Avaya Services representative, and use Avaya Enterprise Linux or if the Avaya Service accounts are installed on this server:

- Log in to the local Linux console as `sroot`.
- Or log in remotely as a non-root user and then change the user to `sroot` by entering the `su - sroot` command.

Otherwise, log in to Linux locally as `root`, or log in remotely as a non-root user and then change the user to `root` by entering the `su -` command.

2. Insert the Avaya Aura® Experience Portal 7.0.1 software installation DVD into the DVD drive of the server.

Tip:

These instructions assume that you are going to access the Experience Portal installation DVD by mounting the appropriate DVD drive on the target system. If you

want to access the installation DVD files from a shared network directory or a local directory, you can copy the files from the Experience Portal installation DVD to that directory. However, that directory needs to be readable by all users on the system because the Experience Portal installation script changes users during the install procedure. If the directory is only readable by the root or sroot user, the installation script encounters errors and does not complete successfully. You must ensure that the directory name does not contain spaces. If there are spaces in the directory name, the installation script encounters errors and does not complete successfully.

3. Mount the Avaya Aura® Experience Portal 7.0.x software installation DVD. The `mount` command depends on the server's hardware and operating system.

- If you are working with Avaya Enterprise Linux, mount the DVD by entering the `mount /mnt/cdrom` command, where `/mnt/cdrom` is the mount point typically associated with the DVD drive in the `fstab` file.
- If you are working with a supported version of Red Hat Enterprise Linux Server, to mount the DVD:
 - Run the `mkdir /media/cdrom` command.

 Note:

This command is required only if the `/media/cdrom` mount point does not exist.

- Run the `mount /dev/cdrom /media/cdrom` command.

 Warning:

When Red Hat Enterprise Linux Server automatically mounts the DVD, the files on the DVD are not executable. You must manually mount the Experience Portal installation DVD using the commands shown above.

If the `mount` commands shown above do not work, consult your server documentation for the appropriate `mount` command.

4. Change to the mount point directory.
5. Enter the `bash installvp` command and press `Enter` to start the installation script.

If the 32-bit glibc package is not already installed, the installer displays the message `For the Experience Portal installer to run, 32-bit glibc must be installed.`

6. If the installer displays the message that you must install 32-bit glibc, type `Y` or press `Enter` to proceed with the 32-bit glibc installation.
7. On the Installation Destination screen, ensure the installation path is the same as the previous installation, and press `Enter`.

 Important:

Do not change the installation directory when upgrading to a new release.

When choosing installation options, wait for the next prompt before pressing a key. The installation stores your key presses in a buffer and enters all the key presses after the current processing completes. For example, if you press the `Enter` key repeatedly while the system is performing its prerequisite checks, you might unintentionally skip options you want to change. Use the **Previous** option on any screen to go back and change your earlier choices.

8. Press `Enter` to move to the next screen.
9. On the Experience Portal Feature Selection screen:
 - a. Type `1` and press `Enter` to clear **EPM**.

The screen refreshes with only **Documentation** selected.
 - b. Type `2` and press `Enter` to select **MPP**.

The screen refreshes with both **MPP** and **Documentation** selected.
 - c. Press `Enter` to confirm your selections.
10. Press `Enter` to move to the next screen.
11. On the Version Confirmation screen:
 - a. If you are upgrading the MPP software on an Avaya Enterprise Linux server, verify that the **New Version** column indicates upgrade to release 7.0.1 of the MPP software.
 - b. If you are upgrading the MPP software on a Red Hat Enterprise Linux Server, verify that the **New Version** column indicates install release 7.0.1 of the MPP software.
12. Press `Enter` to move to the next screen.
13. Read through the end user license agreement.
14. On the final End User License Agreement page, type `1` and press `Enter` to select option **1 - I accept the terms of the license agreement**.

The screen refreshes with **1 - I accept the terms of the license agreement** as the selected option.
15. Press `Enter` to accept the agreement.
16. Press `Enter` to move to the next screen.

Experience Portal automatically starts the Prerequisite Checker, which analyzes your system's hardware and operating system configuration.
17. After the configuration analysis is complete, the Prerequisite Checker displays a message stating whether all prerequisite checks passed followed by the first Prerequisite Status page. Press `Enter` to view the rest of the Prerequisite Status pages.

If any of the prerequisite installation fails, examine the Prerequisite Status pages carefully to determine which checks failed. You must correct these issues before you can continue with this procedure.
18. When all prerequisite checks pass, press `Enter` to move to the next screen.

Experience Portal automatically starts the Prerequisite Installer, which attempts to install the required software on the Experience Portal server.

19. After the Prerequisite Installer completes installing the required software, the installer displays the Installation Status pages. Press `Enter` to view the rest of the Installation Status pages.

If any prerequisite installations fail, examine the Installation Status pages carefully to determine which installations failed. You must correct these issues before you can continue with this procedure.

20. When all prerequisites are successfully installed, press `Enter` to move to the next screen.
21. Press `Enter` to move to the next screen.
22. On the Primary EPM Server Location screen, specify the server name or IP address of the EPM server. If you want to:
 - Use the existing EPM server that is displayed in square brackets [] after the installation prompt, press `Enter`.

 Important:

This option is available only if you are upgrading the MPP software on an Avaya Enterprise Linux server.

- If no existing EPM location exists or you want to change the location of the EPM server, type the server name or IP address where the EPM software is installed. Press `Enter` to submit the new address.

For example, to specify the machine with the server name `EPM_Server` on the default port, type `EPM_Server`. To specify the same server on port 86, type `EPM_Server:86`.

The MPP installation uses the information to retrieve the public key from the EPM. The public key provides authentication between the EPM and MPP servers to help secure your Experience Portal system.

23. Press `Enter` to move to the next screen.
24. On the Public Key Verification screen, if you recorded the fingerprint information from the EPM security certificate during the Primary EPM software installation, compare the information to the Public Key fingerprint information. The fingerprint information from Public Key must match the fingerprint information on the EPM security certificate.

If the public key is not downloaded, see [MPP or Auxiliary EPM could not import EPM key](#) on page 132.
25. Press `Enter` to move to the next screen.

26. Experience Portal uses the ssl protocol to establish a secure connection between its servers. This connection requires a security certificate that can be created by Experience Portal or purchased from a third-party company. On the Security Certificate screen:

- If you want Experience Portal to create a security certificate:
 - a. Verify that option **1 - Create a new certificate for this server** is selected. If not, type `1` and press `Enter`.
 - b. Press `Enter` to confirm that selection.

*** Note:**

The Experience Portal installer generates and installs a SHA256 2048 bit server certificate by default. The installer also generates and installs a SHA256 2048 bit EPM Root certificate.

- If you want to import a self-signed or third party certificate, ensure the following:
 - The certificate is in PKCS12 format. The certificate must be formatted as a PKCS#12 file. A PKCS#12 file always includes a certificate and the corresponding key, and the certificate is encrypted and requires a password. If the certificate is not self-signed then the PKCS#12 file must include the CA certificates.
 - If the "Extended Key Usage" is specified in the X509.V3 certificate extension, specify "Server Authentication" (also called "serverAuth") and Client Authentication" (also called "clientAuth"), for the usage.
 - The certificate resides on the local server or on an NFS-mounted drive that is locally accessible.

To import a self-signed or third party certificate, do the following:

- a. Verify that option **2 - Import a certificate from a specified location** is selected. If not, type `2` and press `Enter`.
- b. Press `Enter` to confirm that selection.
- c. Type the full file path and name of the security certificate and press `Enter`.
The screen displays the location that you entered for your verification.
- d. Type the password for the security certificate and press `Enter`.

27. Press `Enter` to move to the next screen.

28. On the Security Certificate Verification screen, verify the security certificate and press `Enter` to move to the next screen.

+ Tip:

When you add the MPP to Experience Portal through the EPM Web interface, the EPM displays the MPP security certificate. You should record the fingerprint information from this security certificate so that you can compare it to the one displayed in the EPM Web interface.

If the imported certificate is a chained certificate, then the final signed certificate (also called the end certificate) of the chained certificate is displayed in the EPM Web interface.

29. On the Pre Installation Summary screen, verify the installation information and press `Enter` to install the Experience Portal software.

Experience Portal displays the Installation Progress screen and begins installing the software. During the install, it displays messages indicating its progress.

The installation process can appear completed or stopped even though it is still processing and installing the software. Wait until Experience Portal displays the Post Installation Summary screen.

30. On the Post Installation Summary screen, verify that the **Installation Progress Bar** has reached 100% and that the message `...done installing feature_name` appears for each feature that you selected on the Experience Portal Feature Selection screen.

 Note:

If the **Installation Progress Bar** on the Installation Progress screen stops at 25% and the Post Installation Summary screen states that no summary information could be found, see *Upgrading to Avaya Aura® Experience Portal 7.0.1* on <http://support.avaya.com>.

31. Press `Enter` to end the installation script.

During the installation process, Experience Portal creates several log files that you can use to verify the installation. When the installation process is complete, Experience Portal moves the logs to the standard log directory and displays the exact path on the screen. For more information, see [Upgrade installation log files](#) on page 121.

32. Enter the `/sbin/service mpp status` command to verify that the MPP system manager is running.

The MPP server returns the message `mppsismgr (pid <pid>) is running`, where `<pid>` is the process id.

33. To unmount and eject the DVD:

- a. Change the directory to a location that is outside the mount point. For example, enter the `cd /` command to change to the root directory.
- b. Unmount the DVD as described in the server documentation.
- c. To eject the Experience Portal installation DVD, press the button on the DVD drive or enter the `eject` command.

34. Load the environment variables created during the installation by logging out of Linux and then logging back in.
 - a. Log out of the Linux system.

- b. If you are logged in remotely, log back in to Linux by entering a non-root user name and password at the prompts, and log back in as root or `sroot`.
 - On an Avaya Enterprise Linux server, enter the `su - sroot` command.
 - On a Red Hat Enterprise Linux Server, enter the `su -` command.
 - c. If you are logged in directly through a console, log in to the local Linux console as `sroot`.
35. To verify that NTP is operating properly on the MPP enter the `/usr/sbin/ntpq -np` command.

The system displays a status message similar to the following:

```
remote  refid  st  t  when  poll reach  delay  offset  jitter
=====
123.123.123.123  127.127.1.0  6  u  23   64  1  0.354  0.361  0.004
```

Ensure that:

- The remote IP address points to the Primary EPM server.
- The jitter value is *not* 4000.

Next steps

- Install any required patches that you download from the Avaya online support Web site, <http://support.avaya.com>.
- Upgrade the MPP software on another server machine by repeating the procedure.
- Reestablish the connection between the upgraded MPP and the EPM server as described in [Reestablishing the link between the EPM and the upgraded MPP](#) on page 77.
- If required, upgrade the MPP software on another server machine by repeating this procedure on that machine.
- Configure and test the Experience Portal system. For more information, see [Avaya Aura Experience Portal system configuration overview for a system upgraded to 7.0.1](#) on page 108.

Automatically upgrading the MPP software

Before you begin

! Important:

Automatic upgrade is not supported if you are upgrading Voice Portal 5.1 software to Avaya Aura® Experience Portal 7.0.1 on a supported version of Red Hat Enterprise Linux Server. Since the upgrade information required is not retained on RHEL, automatic upgrade is not possible.

+ Tip:

In Experience Portal 7.0.1, the certificate generation code is enhanced to use a more secure hashing algorithm. Avaya recommends that you upgrade to Experience Portal 7.0.1 by using the

Interactive upgrade option so that you can generate a SHA256 2048 bit server certificate (the new security certificate) to make the systems more secure.

- Ensure that you have upgraded the EPM software on the Primary EPM server as described in [EPM software upgrade overview](#) on page 52.
- Ensure that you have upgraded the Auxiliary EPM software on the Auxiliary EPM server as described in [Auxiliary EPM software upgrade overview](#) on page 66.
- Download any patches for Avaya Aura® Experience Portal Release 7.0.1 from the Avaya Support Web site at <http://support.avaya.com>.
- Complete the [MPP server upgrade worksheet](#) on page 153 and have it available to help answer the questions raised during the installation.
- Ensure that the MPP server is offline.
- Ensure that you have upgraded the server operating system as described in [Operating system upgrade overview](#) on page 19.
- Prior to running the upgrade for an MPP, EPM, verify that the prerequisites have been met. For more information, see [Software upgrade prerequisites overview for upgrading from 5.1 or 6.0](#) on page 38.

Procedure

1. Log into the server on which you want to upgrade the MPP software.

If you are an Avaya Services representative, and use Avaya Enterprise Linux or if the Avaya Service accounts are installed on this server:

- Log in to the local Linux console as sroot.
- Or log in remotely as a non-root user and then change the user to sroot by entering the `su - sroot` command.

Otherwise, log in to Linux locally as root, or log in remotely as a non-root user and then change the user to root by entering the `su -` command.

2. Insert the Avaya Aura® Experience Portal 7.0.1 software installation DVD into the DVD drive of the server.

Tip:

These instructions assume that you are going to access the Experience Portal installation DVD by mounting the appropriate DVD drive on the target system. If you want to access the installation DVD files from a shared network directory or a local directory, you can copy the files from the Experience Portal installation DVD to that directory. However, that directory needs to be readable by all users on the system because the Experience Portal installation script changes users during execution. If the directory is only readable by the root or sroot user, the installation script will encounter errors and will not complete successfully. You also need to ensure the directory name does not contain spaces. If there are spaces in the directory name, the installation script will encounter errors and will not complete successfully.

3. Mount the Avaya Aura® Experience Portal 7.0.x software installation DVD. The **mount** command depends on the server's hardware and operating system.

- If you are working with Avaya Enterprise Linux, mount the DVD by entering the `mount /mnt/cdrom` command, where `/mnt/cdrom` is the mount point typically associated with the DVD drive in the `fstab` file.
- If you are working with a supported version of Red Hat Enterprise Linux Server, to mount the DVD:
 - Run the `mkdir /media/cdrom` command.

 Note:

This command is required only if the `/media/cdrom` mount point does not exist.

- Run the `mount /dev/cdrom /media/cdrom` command.

 Warning:

When Red Hat Enterprise Linux Server automatically mounts the DVD, the files on the DVD are not executable. You must manually mount the Experience Portal installation DVD using the commands shown above.

If the **mount** commands shown above do not work, consult your server documentation for the appropriate **mount** command.

4. Change to the mount point directory.
5. Enter the `bash autoupgradevp` command to start the upgrade script. No prompts are displayed when the upgrade is in progress.

As the script proceeds, it produces messages similar to the following:

```
Starting automatic upgrade for MPP software. This will take several
minutes to complete. Please wait...
```

```
The MPP installation has completed. Review the following
information. If there are errors or warnings, then please review
the installation logs.
```

```
Installing Documentation...
```

```
...done installing Documentation
```

```
Installing MPP...
```

```
...done installing MPP
```

```
Moving installation logs to: /opt/Avaya/ExperiencePortal/logs/
install_2013-12-12.000
```

6. Enter the `/sbin/service mpp status` command to verify that the MPP system manager is running.

The MPP server returns the message `mppsismgr (pid <pid>) is running`, where `<pid>` is the process id.

7. To unmount and eject the DVD:
 - a. Change the directory to a location that is outside the mount point. For example, enter the `cd /` command to change to the root directory.
 - b. Unmount the DVD as described in the server documentation.
 - c. To eject the Experience Portal installation DVD, press the button on the DVD drive or enter the `eject` command.
8. Load the environment variables created during the installation by logging out of Linux and then logging back in.
 - a. Log out of the Linux system.
 - b. If you are logged in remotely, log back in to Linux by entering a non-root user name and password at the prompts, and log back in as root or `sroot`.
 - On an Avaya Enterprise Linux server, enter the `su - sroot` command.
 - On a Red Hat Enterprise Linux Server, enter the `su -` command.
 - c. If you are logged in directly through a console, log in to the local Linux console as `sroot`.
9. To verify that NTP is operating properly on the MPP enter the `/usr/sbin/ntpq -np` command.

The system displays a status message similar to the following:

```
remote refid st t when poll reach delay offset jitter
=====
123.123.123.123 127.127.1.0 6 u 23 64 1 0.354 0.361 0.004
```

Ensure that:

- The remote IP address points to the Primary EPM server.
- The jitter value is *not* 4000.

Next steps

- Verify if the Signature Algorithm displayed on the certificate is SHA256withRSA.
 1. Log in to EPM and navigate to the **System Configuration > MPP Servers** page.
 2. Click on the MPP name to view the details of the MPP server certificate.
 3. If the Signature Algorithm displayed on the EPM certificate is not SHA256withRSA, run the `GenerateServerCertificate` script to generate or the `ImportServerCertificate.sh` script to import a SHA256 2048 bit server certificate. For more information about the `GenerateServerCertificate` and `ImportServerCertificate.sh` scripts, see *Administering Avaya Aura® Experience Portal*.
- Install any required patches that you download from the Avaya online support Web site, <http://support.avaya.com>.
- Put the MPP in online Mode.
- Start the MPP.

- If required, upgrade the MPP software on another server machine by repeating this procedure on that machine.
- Configure and test the Experience Portal system. For more information, see [Avaya Aura Experience Portal system configuration overview for a system upgraded to 7.0.1](#) on page 108.

Chapter 6: Upgrading the Experience Portal software on a single server

Experience Portal software upgrade on a single server overview

When you install the EPM software, Avaya Aura® Experience Portal automatically records your answers to basic questions, such as installation directory details, the name of the EPM server, and security certificate information. EPM compiles the answers into a file. You can use the file to upgrade the EPM software on a server without further user input.

After you install the Experience Portal software, you have two EPM upgrade options:

- Automatic upgrade: For Avaya Enterprise Linux users only
- Interactive upgrade: For Avaya Enterprise Linux and Red Hat Enterprise Linux Server users

Tip:

In Experience Portal 7.0.1, the certificate generation code is enhanced to use a more secure hashing algorithm. Avaya recommends that you upgrade to Experience Portal 7.0.1 by using the Interactive upgrade option so that you can generate a SHA256 2048 bit server certificate (the new security certificate) to make the systems more secure.

Automatic upgrade

Launch the Experience Portal installation program, and run the auto upgrade utility to upgrade to Avaya Aura® Experience Portal 7.0.1 on an Avaya Enterprise Linux server.

By default, the automatic upgrade:

- Uses the default installation directories.
- Specifies the IP address of the server on which you install the EPM software.
- Uses the existing security certificate for the EPM.
- Keeps the existing user accounts. If you have deleted all the existing user manager accounts from EPM prior to the upgrade, you need to use the console EPM upgrade option to create a new user manager account.

If you have deleted your last user manager account and need to create a new local user manager, you can perform a reinstall of the latest version. During installation, you can select the option of creating a new EPM user manager account.

If the username you specify refers to an existing local user, the system updates the password and creates a new user manager account.

The system displays the error messages at the end of the upgrade process, and all messages are recorded in the installation log files.

 Note:

Avaya recommends the automatic upgrade option if you want to upgrade to Avaya Aura® Experience Portal 7.0.1 on an Avaya Enterprise Linux server and you do not need changes to the configurations.

For more information, see [Automatically upgrading the EPM software](#) on page 53.

Interactive EPM upgrade

On the EPM server, launch the Experience Portal installation program and answer the prompts.

 Tip:

Avaya recommends the Interactive upgrade option if you need to make changes to the configurations during the upgrade.

Upgrading the Experience Portal software interactively on a single server

Before you begin

- Ensure that you upgrade the operating system on the server as described in [Operating system upgrade overview](#) on page 19.

 Important:

If you upgrade the Experience Portal software on a Red Hat Linux Server, ensure that you have copied the back up files on the server as described in [Copying and restoring the backup files on Red Hat Enterprise Linux Server](#) on page 48.

- Complete the [Single EPM server upgrade worksheet](#) on page 155 and have it available to help answer the questions raised during the installation.
- Before you upgrade the software, read the Avaya Aura® Experience Portal release notes on the Avaya Aura® Experience Portal installation DVD under *Documentation*. These release notes contain information about the product that is not included in the formal documentation set.
- Download any patches for Avaya Aura® Experience Portal Release 7.0.1 from the Avaya Support Web site at <http://support.avaya.com>.
- Ensure that you have completed the software upgrade prerequisites described in [Prerequisites overview for upgrading Experience Portal](#) on page 38.
- For disk space related information, see [Space requirement for upgrading primary EPM on Red Hat Enterprise Linux](#) on page 41 and [Space requirements for upgrading primary EPM on Avaya Enterprise Linux](#) on page 41.
- If you have installed a managed application, contact the provider of the managed application to check if you need to perform any additional steps as part of the Experience Portal upgrade.

Procedure

1. Log into the server on which you want to upgrade the Experience Portal software.

If you are an Avaya Services representative, and use Avaya Enterprise Linux or if the Avaya Service accounts are installed on this server:

- Log in to the local Linux console as `sroot`.
- Or log in remotely as a non-root user and then change the user to `sroot` by entering the `su - sroot` command.

Otherwise, log in to Linux locally as root, or log in remotely as a non-root user and then change the user to root by entering the `su -` command.

*** Note:**

Ensure that you upgrade using the same Linux account that was used during the prior installation. If you upgrade a Voice Portal or Experience Portal system by using a Linux account that is different than the account used during the previous install or upgrade, the upgrade might fail.

2. Insert the Avaya Aura® Experience Portal 7.0.1 software installation DVD into the DVD drive of the server.

+ Tip:

These instructions assume that you are going to access the Experience Portal installation DVD by mounting the appropriate DVD drive on the target system. If you want to access the installation DVD files from a shared network directory or a local directory, you can copy the files from the Experience Portal installation DVD to that directory. However, that directory must be readable by all users on the system. If the directory is only readable by the root or `sroot` user, the installation script will encounter errors and will not complete successfully.

3. Mount the Avaya Aura® Experience Portal 7.0.x software installation DVD. The `mount` command depends on the server's hardware and operating system.

- If you are working with Avaya Enterprise Linux, mount the DVD by entering the `mount /mnt/cdrom` command, where `/mnt/cdrom` is the mount point typically associated with the DVD drive in the `fstab` file.
- If you are working with a supported version of Red Hat Enterprise Linux Server, to mount the DVD:
 - Run the `mkdir /media/cdrom` command.

*** Note:**

This command is required only if the `/media/cdrom` mount point does not exist.

- Run the `mount /dev/cdrom /media/cdrom` command.

 Warning:

When Red Hat Enterprise Linux Server automatically mounts the DVD, the files on the DVD are not executable. You must manually mount the Experience Portal installation DVD using the commands shown above.

If the `mount` commands shown above do not work, consult your server documentation for the appropriate `mount` command.

4. Change to the mount point directory.
5. Enter the `bash installvp` command and press `Enter` to start the installation script.

If the 32-bit `glibc` package is not already installed, the installer displays the message `For the Experience Portal installer to run, 32-bit glibc must be installed.`

6. If the installer displays the message that you must install 32-bit `glibc`, type `Y` or press `Enter` to proceed with the 32-bit `glibc` installation.
7. On the Installation Destination screen, press `Enter` to upgrade the software in the same location as the previous release.

 Important:

You must not change the installation directory when upgrading to a new release.

When choosing installation options, wait for the next prompt before pressing a key. The installation stores your key presses in a buffer and enters all the key presses after the current processing completes. For example, if you press the `Enter` key repeatedly while the system is performing its prerequisite checks, you might unintentionally skip options you want to change. Use the **Previous** option on any screen to go back and change your earlier choices.

8. Press `Enter` to move to the next screen.
9. On the Experience Portal Feature Selection screen:
 - a. Type `2` and press `Enter` to select **MPP**.
The screen refreshes with **EPM**, **MPP**, and **Documentation** selected.
 - b. Press `Enter` to confirm your selections.
10. Press `Enter` to move to the next screen.
11. On the Version Confirmation screen, verify that:
 - The **Installed Version** column indicates the previous version of Experience Portal that was installed on the server.
 - The **New Version** column indicates that you are upgrading to release 7.0.1.
 - If you upgrade a server that uses Red Hat Enterprise Linux Server, only the feature **EPM** shows the **Install Type** as **Upgrade**. The feature **Documentation** shows the **Install Type** as **Full Install**.

- For upgrading an MPP on Red Hat Enterprise Linux Server, the **Installed Version** displays **Not Installed** and the **Install Type** displays **Full Install**.
- For upgrading an on Avaya Enterprise Linux, the **Install Type** column shows as **Upgrade** for all selected features.

12. Press `Enter` to move to the next screen.
13. Read through the end user license agreement.
14. On the final End User License Agreement page, type `1` and press `Enter` to select option **1 - I accept the terms of the license agreement**.

The screen refreshes with **1 - I accept the terms of the license agreement** as the selected option.

15. Press `Enter` to accept the agreement.
16. Press `Enter` to move to the next screen.

Experience Portal automatically starts the Prerequisite Checker, which analyzes your system's hardware and operating system configuration.

17. After the configuration analysis is complete, the Prerequisite Checker displays a message stating whether all prerequisite checks passed followed by the first Prerequisite Status page. Press `Enter` to view the rest of the Prerequisite Status pages.

If any of the prerequisite installation fails, examine the Prerequisite Status pages carefully to determine which checks failed. You must correct these issues before you can continue with this procedure.

18. When all prerequisite checks pass, press `Enter` to move to the next screen.

Experience Portal automatically starts the Prerequisite Installer, which attempts to install the required software on the Experience Portal server.

 Important:

The length of time the Prerequisite Installer takes depends on the size of your old Experience Portal database, because this process is also upgrading that database. Do NOT cancel the installation while the Prerequisite Installer is running or you may damage your database.

19. After the Prerequisite Installer completes installing the required software, the installer displays the Installation Status pages. Press `Enter` to view the rest of the Installation Status pages.

If any prerequisite installations fail, examine the Installation Status pages carefully to determine which installations failed. You must correct these issues before you can continue with this procedure.

20. When all prerequisites are successfully installed, press `Enter` to move to the next screen.

21. On the Add/Edit EPM User Manager Account screen, if you want to:

- Create a new **user manager** account or change the password of an existing account:
 - a. Verify that option **1 - Yes** is selected. If it is not selected, type **1** and press `Enter`.
 - b. Press `Enter` twice to confirm the selection and move to the next screen.
 - c. On the EPM Administrator screen, type the new or existing account user name and press `Enter`.

 Note:

If you enter an existing account user name, Experience Portal changes the password for that account. Make sure that any users who log in with that user name know about the new password.

- d. Type the password for this account and press `Enter`.
 - e. Confirm the password by typing it again and pressing `Enter`.
- Retain current account settings:
 - a. Verify that option **2 - No** is selected. If it is not selected, type **2** and press `Enter`.
 - b. Press `Enter` to confirm your selection.

22. Press `Enter` to move to the next screen.

23. You can create a PostgreSQL database user account that can read the report data in the Experience Portal database. If you:

- Want to create the report reader database account:
 - a. Type **1** and press `Enter`.
 - b. Press `Enter` to confirm your selection.
 - c. To use the account name in square brackets ([]), press `Enter` at the installation prompt. Otherwise, type a unique user name for the account and press `Enter`.
 - d. Type a password for the account and press `Enter`.
 - e. Confirm the password by typing the password again and press `Enter`.
- Do not want to create the report reader account:
 - a. Verify that option **2 - No** is selected. If it is not selected, type **2** and press `Enter`.
 - b. Press `Enter` to confirm your selection.

 Note:

This user account can only read those tables in the Experience Portal database that store report data. Speech application developers can use this account to log in to the database to create custom reports using any SQL-enabled report generation tool.

24. Press `Enter` to move to the next screen.

25. On the Database Login for Auxiliary EPM screen, you can specify whether you want to create a PostgreSQL user account for the optional Auxiliary EPM server.

This account allows each Auxiliary EPM server limited access to the main Experience Portal database, and it is required if you plan to configure an Auxiliary EPM server.

- If you want to create the Auxiliary EPM login account:
 - a. Type `1` and press `Enter`.
 - b. Press `Enter` to confirm your selection.
 - c. Type the password for this account and press `Enter`.
 - d. Confirm the password by typing it again and pressing `Enter`.
- If you do not want to create the Auxiliary EPM account:
 - a. Verify that option **2 - No** is selected. If it is not selected, type `2` and press `Enter`.
 - b. Press `Enter` to confirm your selection.

26. Press `Enter` to move to the next screen.

27. On the Product ID screen:

- If you are upgrading the Voice Portal software on Avaya Enterprise Linux, you can either:
 - a. Use the existing Product ID that is generated with the Automatic Registration Tool (ART) for this installation of Experience Portal, and press `Enter`.
 - b. Use a new Product ID, type the ID and press `Enter`.
- If you are upgrading the Voice Portal software on Red Hat Enterprise Linux Server:
 - a. Enter the Product ID that is generated with the Automatic Registration Tool (ART) for this installation of Experience Portal, and press `Enter`.

The notification feature uses the Product ID to generate SNMP traps. SNMP traps are unsolicited notifications of significant events from an SNMP agent to an SNMP manager. The SNMP agent resides on a managed network device.

28. Press `Enter` to move to the next screen.

29. Experience Portal uses the ssl protocol to establish a secure connection between its servers. This connection requires a security certificate that can be created by Experience Portal or purchased from a third-party company. On the Security Certificate screen:

- If you want Experience Portal to create a security certificate:
 - a. Verify that option **1 - Create a new certificate for this server** is selected. If not, type `1` and press `Enter`.
 - b. Press `Enter` to confirm that selection.

*** Note:**

The Experience Portal installer generates and installs a SHA256 2048 bit server certificate by default. The installer also generates and installs a SHA256 2048 bit EPM Root certificate.

- If you want to import a self-signed or third party certificate, ensure the following:
 - The certificate is in PKCS#12 format. The certificate must be formatted as a PKCS#12 file. A PKCS#12 file always includes a certificate and the corresponding key, and the certificate is encrypted and requires a password. If the certificate is not self-signed then the PKCS#12 file must include the CA certificates.
 - If the “Extended Key Usage” is specified in the X509.V3 certificate extension, specify “Server Authentication” (also called “serverAuth”) and Client Authentication” (also called “clientAuth”), for the usage.
 - The certificate resides on the local server or on an NFS-mounted drive that is locally accessible.

To import a self-signed or third party certificate, do the following:

- a. Verify that option **2 - Import a certificate from a specified location** is selected. If not, type `2` and press `Enter`.
- b. Press `Enter` to confirm that selection.
- c. Type the full file path and name of the security certificate and press `Enter`.
The screen displays the location that you entered for your verification.
- d. Type the password for the security certificate and press `Enter`.

30. Press `Enter` to move to the next screen.

31. On the Security Certificate Verification screen, verify the security certificate and press `Enter` to move to the next screen.

+ Tip:

When you add the MPP to Experience Portal through the EPM Web interface, the EPM displays the MPP security certificate. You should record the fingerprint information from this security certificate so that you can compare it to the one displayed in the EPM Web interface.

If the imported certificate is a chained certificate, then the final signed certificate (also called the end certificate) of the chained certificate is displayed in the EPM Web interface.

32. On the Pre Installation Summary screen, verify the installation information and press `Enter` to install the Experience Portal software.

Experience Portal displays the Installation Progress screen and begins installing the software. During the install, it displays messages indicating its progress.

The installation process can appear completed or stopped even though it is still processing and installing the software. Wait until Experience Portal displays the Post Installation Summary screen.

33. On the Post Installation Summary screen, verify that the **Installation Progress Bar** has reached 100% and that the message `...done installing feature_name` appears for each feature that you selected on the Experience Portal Feature Selection screen.

*** Note:**

If the **Installation Progress Bar** on the Installation Progress screen stops at 25% and the Post Installation Summary screen states that no summary information could be found, see *Upgrading to Avaya Aura® Experience Portal 7.0.1* on <http://support.avaya.com>.

34. Press `Enter` to end the installation script.

During the installation process, Experience Portal creates several log files that you can use to verify what happened during installation. When the installation process is complete, Experience Portal moves those logs to the standard log directory and displays the exact path on the screen. For more information, see [Upgrade installation log files](#) on page 121.

35. Enter the `/sbin/service mpp status` command to verify that the MPP system manager is running.

The MPP server returns the message `mppsismgr (pid <pid>) is running`, where `<pid>` is the process id.

36. Check the status of the `vpms` service by entering the `service vpms status` command.

If the `vpms` service is running properly, the command displays messages indicating that the `tomcat`, `SL`, and `ActiveMQ` services are all running. The command ends with the message: `Overall Status: VPMS is running`.

37. To verify that NTP is operating properly on the server, enter the `/usr/sbin/ntpq -np` command.

A status message similar to the following is displayed:

```

remote      refid      st t when poll reach  delay
offset jitter
=====
*127.127.1.0 73.78.73.84  5 1   4   64  377   0.000
0.000   0.001
```

Ensure that:

- The remote IP address is `*127.127.1.0`.
- The jitter value is *not* 4000.

38. To unmount and eject the DVD:

- a. Change the directory to a location that is outside the mount point. For example, enter the `cd /` command to change to the root directory.

- b. Unmount the DVD as described in the server documentation.
 - c. To eject the Experience Portal installation DVD, press the button on the DVD drive or enter the `eject` command.
39. Load the environment variables created during the installation by logging out of Linux and then logging back in.
 - a. Log out of the Linux system.
 - b. If you are logged in remotely, log back in to Linux by entering a non-root user name and password at the prompts, and log back in as root or `sroot`.
 - On an Avaya Enterprise Linux server, enter the `su - sroot` command.
 - On a Red Hat Enterprise Linux Server, enter the `su -` command.
 - c. If you are logged in directly through a console, log in to the local Linux console as `sroot`.
40. If you use Avaya Enterprise Linux and if you install an application server on this server, you need to start the application server by entering the `/sbin/service appserver start` command.

Next steps

- Verify if the Signature Algorithm displayed on the EPM certificate is SHA256withRSA.
 1. Log in to EPM and navigate to the **System Configuration > EPM Servers** page.
 2. Click on the Primary EPM name to view the details of the Primary EPM server certificate.
 3. If the Signature Algorithm displayed on the EPM certificate is not SHA256withRSA, run the `GenerateServerCertificate` script to generate or the `ImportServerCertificate.sh` script to import a SHA256 2048 bit server certificate. For more information about the `GenerateServerCertificate` and `ImportServerCertificate.sh` scripts, see *Administering Avaya Aura® Experience Portal*.
- Since the root certificate is not modified on any upgrade, you can generate and replace the root certificate from the EPM Web interface. For more information see *Administering Avaya Aura® Experience Portal*.
- For upgrade verification, navigate to `Support/VP-Tools` and run the `EPInstallationVerifier` script.

Note:

To run the script, enter the `./EPInstallationVerifier <InstallationLogDirectory>` command where `<InstallationLogDirectory>` is located in `/opt/Avaya/ExperiencePortal/logs` and is specified at the end of each upgrade. An example of the command: `./EPInstallationVerifier /opt/Avaya/ExperiencePortal/logs/install_2013-12-01.000`.

- Install any required patches that you download from the Avaya online support Web site, <http://support.avaya.com>.
- Reestablish the link between the MPP and the EPM as described in [Reestablishing the link between the EPM and the MPP](#) on page 103.
- If you wish to change the postgres database password specified by the auto upgrade utility, run the `SetDbPassword.sh` script.

! Important:

If Proactive Outreach Manager is installed on this system, then you must run the script `SetDbPassword.sh` to change the password for the database user `postgres`. The Experience Portal upgrade program automatically generates a new password for the database user `postgres`. However, Proactive Outreach Manager is already configured to use the old password. To keep Proactive Outreach Manager working, you must change the password for the database user `postgres` back to the value that you have configured in Proactive Outreach Manager. For more information about configuring the PostgreSQL database user accounts, see *Administering Avaya Aura® Experience Portal*.

- Install the Avaya Service Account authentication file. For more information about installing the Avaya Service Account authentication file, see *Troubleshooting Avaya Aura® Experience Portal*.
- Upgrade the coresident application server. For more information, see [Optional: Updating the co-resident application server](#) on page 105.

Reestablishing the link between the EPM and the MPP

After you upgrade the Experience Portal software, you need to reestablish the link between the MPP and the EPM by trusting the MPP's security certificate.

Procedure

1. Log in to the EPM web interface using an account with the Administration user role.
2. From the EPM main menu, select **System Configuration > MPP Servers**.
3. Click the name of the MPP server.
4. On the **Change MPP Server** page, navigate to the MPP Certificate section and select the **Trust new certificate** check box if the check box is visible.
5. Click **Save**.
6. From the EPM main menu, select **System Management> MPP Manager**.
7. If the **Mode** column displays **Offline**, you need to start the MPP. To start the MPP:
 - a. Select the check box next to the name of the MPP.
 - b. In the Mode Commands group, click **Online**.
 - c. Click **Refresh** to verify that the **Mode** column displays **Online** for the MPP.
 - d. Select the check box next to the name of the MPP.
 - e. In the **State Commands** group, click **Start** and confirm your selection when prompted.
 - f. Click **Refresh** to verify that the current state is **Running**.

 Note:

Check the **System Monitor** page. If the **Last Poll** date and time details displays **never**, restart the *vpms* service.

8. Ensure that the telephony ports are correctly allocated to the MPP server:
 - a. From the EPM main menu, select **Real-Time Monitoring > Port Distribution**.
 - b. On the **Port Distribution** page, verify the ports allocated to the MPP in the **Current Allocation** column.
 - c. Ensure that the **Mode** and **State** columns display **Online** and **In Service** status respectively.

Next steps

Configure the upgraded system as described in [Avaya Aura Experience Portal system configuration overview for a system upgraded to 7.0.1](#) on page 108.

Chapter 7: Optional: Updating the co-resident application server

If you have installed a Tomcat application server on the Avaya Aura® Experience Portal server, you can choose to update the version of the application server, but it is not required.

Before you begin

- From the EPM main menu, select **Real-time Monitoring > Active Calls** and ensure that the applications hosted by the co-resident application server are not handling any active calls.
- Back up the required configuration files, data files, web applications and associated components, libraries and binaries from the directory where the application server is installed. For more information on the required backup files, contact the application developer.

Procedure

1. Log in to Linux on the Experience Portal server.

If you are an Avaya Services representative, and use Avaya Enterprise Linux or if the Avaya Service accounts are installed on this server:

- Log in to the local Linux console as `sroot`.
- Or log in remotely as a non-root user and then change the user to `sroot` by entering the `su - sroot` command.

Otherwise, log in to Linux locally as `root`, or log in remotely as a non-root user and then change the user to `root` by entering the `su -` command.

2. If you use Avaya Enterprise Linux, enter the `/sbin/service appserver stop` command to stop the application server.
3. Navigate to the `Support/AppServer` directory under the Avaya Aura® Experience Portal installation directory by entering the `cd $AVAYA_HOME/Support/AppServer` command.

`$AVAYA_HOME` is the environment variable pointing to the name of the installation directory specified during the EPM software installation.

Tip:

This script is also available in the `Support/AppServer` directory of the Experience Portal installation DVD.

4. Run the installation script by entering the `bash InstallAppServer.sh install_dir` command, where `install_dir` is the name of the directory in which you have installed the existing application server.

For example, to install the application server in the `/opt/AppServer` directory, you would enter `bash InstallAppServer.sh /opt/AppServer`.

5. Follow the prompts displayed by the script.

When the script has completed, the system displays the message `Application Server Installation complete`.

*** Note:**

The installation script also registers the application server as a Linux service so that it will be restarted whenever the server restarts.

6. Start the application server by entering the `/sbin/service appserver start` command.
7. Give the server time to start, and then check the server status by entering the following command:

```
/sbin/service appserver status.
```

The server should respond that the `tomcat` service is running.

8. If you want to administer the tomcat server from the Tomcat Manager Web interface, you need to add a tomcat user as specified in the *Adding Tomcat user accounts* section in the *Implementing Avaya Aura® Experience Portal on a single server* guide.

If you use the Avaya provided application installation script, the script creates the user accounts automatically.

*** Note:**

You can access the Tomcat Manager Web Interface from the System Management > Application Server menu in the EPM web interface with the tomcat user account.

9. If you want to administer the server, open a web browser and go to `http://EP-server:7080/manager/html`, where *EP-server* is the hostname or IP address of the Experience Portal server.

Next steps

After you install the application server:

- Deploy the speech applications to the application server as described in your application server documentation.
- You can delete the previous directory structure of the application server. If the new application server is installed in the same root directory as the old application server, make sure that you do not delete the new application server or the symbolic link named *tomcat*, which points to the new application server.

For example, if you update Tomcat-5.5.26 to Tomcat-6.0.37 in the `/opt/AppServer` directory, where `/opt/AppServer` is the root location of the old application server, you will see the following directory structure:

- `/opt/AppServer/apache-tomcat-5.5.26`
- `/opt/AppServer/apache-tomcat-6.0.37`

- /opt/AppServer/tomcat

You should only delete /opt/AppServer/apache-tomcat-5.5.26.

 Note:

The new version does not overwrite the existing directory structure of the application server. Instead, it creates a sub directory for the new version within the directory.

Chapter 8: Configuring and testing an upgraded Avaya Aura Experience Portal system

Avaya Aura[®] Experience Portal system configuration overview for a system upgraded to 7.0.1

Step	Description
1	If the WebLM server does <i>not</i> reside on the Experience Portal EPM server, you can upgrade the WebLM software to version 6.3 as described in the file <code>Support/WebLM/Licensing Installation Instructions.pdf</code> that is available on the Experience Portal server.
2	Upgrade the 5.1, 6.0, or 7.0 license as described in Upgrading the Experience Portal license on page 109.
3	Reconfigure the Avaya Service accounts as described in Avaya Services access changes between 5.1, 6.0, or 7.0 and 7.0.1 on page 109.
4	Test an existing Experience Portal test application.
5	Test the basic system by placing a call to a custom speech application or to the sample application. For more information about the sample application, see Running the sample application on page 110.
6	Test each MPP server individually as described in Testing an individual MPP on page 113.
7	Connect the EPM server to an external time source so that all servers in the Experience Portal system stay properly synchronized as described in External time sources on page 115.
8	The EPM can accept input in non-English languages if desired. If you are using Red Hat Enterprise Linux Server, the languages need to be installed with the operating system. If you are using Avaya Enterprise Linux, you can configure it to accept input in Chinese, Japanese, or Korean as described in: • Configuring Chinese on Avaya Enterprise Linux on page 117 • Configuring Japanese on Avaya Enterprise Linux on page 118 • Configuring Korean on Avaya Enterprise Linux on page 119
9	If you use Dialog Designer, you can upgrade to the Orchestration Designer software as well. Your applications must be at Dialog Designer release 5.1 or later for compatibility with Experience Portal 7.0.1.

Avaya Services access changes between 5.1, 6.0, or 7.0 and 7.0.1

The way an Avaya Services representative maintains the `MPPmap.data` file has changed. For details, see the *Avaya Services MPPmap.data file* topic in *Administering Avaya Aura® Experience Portal*.

Upgrading the Experience Portal license

Before you begin

If the WebLM server does *not* reside on the Experience Portal EPM server, you can upgrade the WebLM software to version 6.3 as described in the file `Support/WebLM/Licensing Installation Instructions.pdf` that is available on the Experience Portal server.

About this task

* Note:

If you do not receive a license file from Avaya, contact your Avaya representative or Avaya Partner representative.

Experience Portal provides an initial 30 day grace period for all features.

Procedure

1. Open the email that contains the Experience Portal license file.
2. Detach the license file from the email and store the license file locally on either the WebLM server or on a computer that is accessible to the Experience Portal servers from a network connection.

For example, you can install the license file on any server from which you can access the EPM Web interface.

3. Log in to the EPM Web interface using an account with the Administration user role.
4. From the EPM main menu, select **Security > Licensing**.

The Licensing page displays the license information and the location of the License server.

5. If the **License Server URL** field is blank or if the location of WebLM has changed, type the location of the license server in the **Location** field.

The URL must be in the format `https://WebLM-machine:port_num/WebLM/LicenseServer`, where *WebLM-machine* is the hostname or IP address of the WebLM server and *:port_num* is an optional parameter that consists of a colon followed by the port number for the WebLM server. If WebLM uses the default configuration, specify: 8443 or 52233. If no port number is specified, Experience Portal sets the default to 8443 for a coresident WebLM server and 52233 for a standalone WebLM.

6. Click **Verify**.

The browser opens a separate window and displays the Avaya WebLM page, which contains a **License Administration** link.

7. Click **License Administration**.

The system displays the Web License Manager Logon page.

8. If you have done a fresh installation of the WebLM server, you have to do the following:

- a. Enter the default user name `admin`.
- b. Enter the default password `weblmadmin`.
- c. Press `Enter` or click the arrow button to log in.
- d. Enter the details on the Change Password page. Make sure that you type `weblmadmin` in the **Current Password** field.
- e. Click **Submit**.
- f. On the Logon page, log in with your new password.

9. If you have an existing WebLM server, you have to do the following:

- a. Type the user name.
- b. Type the password.
- c. Click **Continue**.

10. On the Install License page, click **Browse** to locate the Experience Portal license file.

11. Select the license file, and click **Install**.

WebLM uploads the license file from your computer to the WebLM server and displays the message `License file installed successfully`.

12. Log out of the Web License Manager and close the Web License Manager page.

13. On the EPM Licensing page, click **Apply**.

14. Click **OK** to confirm the change.

15. Verify that the new licensing information is correct.

Running the sample application

Procedure

1. Call the test application number.

The test application number is the number that you specify when you add the test application to the Experience Portal system.

2. If you run the test application as a VoiceXML application, press:

- 1 for Automatic Speech Recognition (ASR)

- 2 for Text-to-Speech (TTS)
 - 3 for Bridge Transfer
 - 4 for Blind Transfer
 - 5 for Consultative Transfer
 - 6 for Audio test
 - 7 to Exit
3. If you run the test application as a CCXML application, press:
- 1 for Automatic Speech Recognition (ASR)
 - 2 for Text-to-Speech (TTS)
 - 3 for Bridge Transfer
 - 4 for Blind Transfer
 - 5 for Consultative Transfer
 - 6 for Audio test
 - 7 to test Conferencing
 - 8 to test Merge
 - 9 to test Call Classification
 - 0 to Exit

Next steps

After you run the application, you can create reports to verify the application's performance and, if you have enabled transcriptions, view the transcription data.

Configure and run the Application Interface test client

Use the Application Interface test client to validate the Application Interface web service and the Experience Portal outcall functionality. The Application Interface test client is available in `$AVAYA_HOME/Support/OutCallTest/VPAppIntfClient`.

Related Links

[Configuring Experience Portal for outcall](#) on page 112

[Running the Application Interface test client VPAppIntfClient.sh](#) on page 112

Configuring Experience Portal for outcall

About this task

Important:

This configuration is required only if you use Experience Portal to perform outcalls or the Application Interface web service to launch VXML and CCXML applications.

Procedure

1. Ensure that at least one of the ports in the system is configured to allow outbound calls. For more information on configuring ports, see *Administering Avaya Aura® Experience Portal*.
2. The VAppIntfService Web service version authenticates users that are configured as Experience Portal users. The user must have the Web Services role.

Related Links

[Configure and run the Application Interface test client](#) on page 111

Running the Application Interface test client VAppIntfClient.sh

Before you begin

Ensure that you configure Experience Portal for the Application Interface test client as described in [Configuring Experience Portal for outcall](#) on page 112.

Procedure

1. Log in to Linux locally as sroot, or log in remotely as a non-root user and change the user to root by entering the `su - sroot` command.
2. Navigate to the Application Interface test client directory by entering the `cd $AVAYA_HOME/Support/OutCallTest/VAppIntfClient` command.
3. Enter the `./VAppIntfClient.sh -n <outcall-username> -p <outcall password>` command to request the number of available outbound ports.
 - <outcall-username> is an Experience Portal user configured from EPM Web interface.
 - <outcall password> is the password for <outcall-username> that is configured from the EPM Web interface .

Note:

The user must have the Web Services user role.

4. Verify that the Application Interface test client displays a response that shows the total ports and unused ports available for outcalls.

For example:

Mon Jun 03 16:55:26 PDT 2013:VPAppIntfServiceClient: queryResources succeeded, Total Resources = 0, Unused H323 = 0, Unused SIP = 0

Mon Jun 03 16:55:26 PDT 2013: VPAppIntfServiceClient: exiting

5. Enter the `./VPAppIntfClient.sh -R 1 -A <application-name> -T <number-to-dial> -n <outcall-username> -p <outcall password>` command to initiate an outcall and launch a VoiceXML application.
 - <application-name> is the name of the application that you specify on the application page.
 - <number-to-dial> is the phone number to place the outcall to.
 - <outcall-username> is the Experience Portal username configured with the Web Services role in the EPM .
 - <outcall password> is the password assigned to the outcall-username above that was configured on the **EPM -> Users** page.
6. Verify that the dialed phone number rings.
7. Answer the phone and verify that the specified application handles the call.

 Note:

The application handles the call in the same way as when an actual user calls into the system.

8. Verify that the Application Interface test client displays the following:
 - A response that shows the result of the LaunchVXML operation.
 - The total ports and the unused ports available for outcalls.

For example:

Mon Jun 03 17:00:31 PDT 2013: VPAppIntfServiceClient: launchVXML succeeded, SessionID = scaaep134-2013155001030-5, TotalRes = 100, UnusedH323 = 0, UnusedSIP = 99

Mon Jun 03 17:00:31 PDT 2013: VPAppIntfServiceClient: exiting

Related Links

[Configure and run the Application Interface test client](#) on page 111

Testing an individual MPP

If your system consists of multiple MPP servers, you can test each one individually to make sure they are all running as expected.

Before you begin

Configure the system as described in [Avaya Aura Experience Portal system configuration overview for a system upgraded to 7.0.1](#) on page 108.

Procedure

1. From the EPM main menu, select **System Management > MPP Manager**.
2. In the MPP server table on the MPP Manager page, click the Selection check box next to all MPP servers *except* the one you want to test.
3. Click the **Stop** button in the **State Commands** group and confirm your selection when prompted.

Experience Portal stops the selected the MPP servers. This process can take several minutes depending on how many servers there are in your system.
4. After a few minutes, click **Refresh** and verify that the **State** is **Stopped** for all MPP servers except the one you want to test.
5. Call the number you associated with the test application when adding the Experience Portal test application and use that application to verify the selected MPP. For more information about adding the test application, see *Implementing Avaya Aura® Experience Portal on multiple servers*.
6. When you are satisfied that the MPP works correctly, in the MPP server table on the MPP Manager page, click the Selection check box next to the MPP server you just tested.
7. Click the **Stop** button in the **State Commands** group and confirm your selection when prompted.
8. In the MPP server table, click the Selection check box next to the new MPP server that you want to test.
9. Click the **Start** button in the **State Commands** group and confirm your selection when prompted.
10. After a few minutes, click **Refresh** and verify that the **State** is **Stopped** for all MPP servers except the one you want to test.
11. Call the number you associated with the test application when adding the Experience Portal test application and use that application to verify the selected MPP. For more information, see *Adding the Avaya Aura® Experience Portal test application* topic in the *Implementing Avaya Aura® Experience Portal on multiple servers* guide.
12. Repeat steps 6-11 until each MPP server has been tested.
13. When you are finished testing the servers:
 - a. Click the Selection check box next to any MPP server whose state is **Stopped**.
 - b. Click the **Start** button in the **State Commands** group and confirm your selection when prompted.
 - c. After a few minutes, click **Refresh** and verify that the **State** is **Running** for all MPP servers.

Once the MPP servers start successfully, the basic Experience Portal system is now available.

External time sources

To make sure that the reporting and logging activities across all servers in your network are synchronized to the same time, use the same external time source for the following:

- The server running the Primary EPM software
- Any application servers running on dedicated machines
- All available speech servers
- All PBX switches
- All email servers

You can use a corporate or a public time server as the external time source.

Note:

Avaya only provides guidelines for public time servers. Ensure that the servers you choose are accessible through your corporate firewall. Some public time servers either limit the amount of access a particular site has or charge for their services. If you select a public time server, make sure that the time server meets all requirements before you change the `ntp.conf` file on the Primary EPM server.

Related Links

[Configuring the Primary EPM server to point to an external time source](#) on page 115

Configuring the Primary EPM server to point to an external time source

Before you begin

Make sure you have the server names or IP addresses of one or two appropriate external time sources. For more information, see [External time sources](#) on page 115.

Procedure

1. Log in to Linux on the Experience Portal Primary EPM server.

If you are an Avaya Services representative, and use Avaya Enterprise Linux or if the Avaya Service accounts are installed on this server:

- Log in to the local Linux console as `sroot`.
- Or log in remotely as a non-root user and then change the user to `sroot` by entering the `su - sroot` command.

Otherwise, log in to Linux locally as root, or log in remotely as a non-root user and then change the user to root by entering the `su -` command.

2. Open the `/etc/ntp.conf` file in an ASCII text editor.

3. Edit the `/etc/ntp.conf` file to add the server you want to use as the primary external time source and an explicit declaration to set the local clock. If desired, you can also add a server to use as the secondary time source if the primary source cannot be found. The format is:

```
server xxxx           // primary external time server
server yyyy           // optional secondary external time server
server 127.127.1.0     // set local clock to time received from external server
fudge 127.127.1.0 stratum 10
driftfile /var/lib/ntp/drift
authenticate no
```

Where `xxxx` and `yyyy` are either server names or IP addresses of the external time servers you want to use.

*** Note:**

The typical settings for `driftfile` and `authenticate` are shown above. If the `ntp.conf` file at your site has different settings, check with your system administrator before you change them.

The following uses the external time sources `clock.sjc.he.net` and `ntp-1.cede.psu.edu`:

```
server clock.sjc.he.net // primary external time server
restrict clock.sjc.he.net nomodify
server ntp-1.cede.psu.edu // secondary time server
restrict ntp-1.cede.psu.edu nomodify
server 127.127.1.0       // set local clock
fudge 127.127.1.0 stratum 10
driftfile /var/lib/ntp/drift
authenticate no
```

4. Save and close the file.
5. Using a text editor of your choice, open the `/etc/ntp/step-tickers` file.
This file is used for initial time setup on the EPM.
6. Add a line in the file to specify the time source server names or IP addresses.

For example, if you are using the servers `clock.sjc.he.net` and `ntp-1.cede.psu.edu`, you would add the following lines:

```
clock.sjc.he.net
ntp-1.cede.psu.edu
```

7. Save and close the file.
8. Restart the `ntpd` daemon by entering the `/sbin/service ntpd restart` command.

The system returns:

```
Shutting down ntpd: [OK]
Synchronizing with time server [OK]
Starting ntpd: [OK]
```

Related Links

[External time sources](#) on page 115

Non-English language support

Non-English character support on the EPM web pages

While the EPM You can use non-English characters when entering field values if you have the appropriate languages installed on the EPM server. Avaya Enterprise Linux, Avaya provides font files for Chinese, Japanese, and Korean.

Related Links

[Configuring Chinese on Avaya Enterprise Linux](#) on page 117

[Configuring Japanese on Avaya Enterprise Linux](#) on page 118

[Configuring Korean on Avaya Enterprise Linux](#) on page 119

Configuring Chinese on Avaya Enterprise Linux Procedure

1. Log in to Linux on the Experience Portal Primary EPM server.

If you are an Avaya Services representative, and use Avaya Enterprise Linux or if the Avaya Service accounts are installed on this server:

- Log in to the local Linux console as `sroot`.
- Or log in remotely as a non-root user and then change the user to `sroot` by entering the `su - sroot` command.

Otherwise, log in to Linux locally as root, or log in remotely as a non-root user and then change the user to root by entering the `su -` command.

2. Navigate to the Linux font directory by entering the `cd /usr/share/fonts` command.

Note:

If the font directory does not already exist, create the directory by entering the `mkdir /usr/share/fonts` command, then navigate to the directory you just created.

3. Copy the Chinese font file to the font directory by entering the `cp $AVAYA_HOME/Support/fonts/zh_CN/TTzh_CN.tar .` command.

Important:

Make sure you include the `.` (period) at the end of the `cp` command to indicate that you want Linux to copy the files to the current directory.

4. Extract the font file by entering the `tar -xvf TTzh_CN.tar` command.
5. Copy the system language file to the Linux system configuration directory by entering the `cp $AVAYA_HOME/Support/fonts/zh_CN/il8n /etc/sysconfig/` command.
6. Navigate to the Java fonts directory by entering the `cd $JAVA_HOME/jre/lib/fonts` command.

7. Create the fallback directory by entering the `mkdir fallback` command.
8. Navigate to the fallback directory by entering the `cd fallback` command.
9. Copy the Chinese font files to the fallback directory by entering the `cp /usr/share/fonts/zh_CN/TrueType/*.ttf .` command.

! Important:

Make sure you include the `.` (period) at the end of the `cp` command to indicate that you want Linux to copy the files to the current directory.

10. Reboot the EPM server machine by entering the `reboot` command.

Related Links

[Non-English character support on the EPM web pages](#) on page 117

Configuring Japanese on Avaya Enterprise Linux Procedure

1. Log in to Linux on the Experience Portal Primary EPM server.

If you are an Avaya Services representative, and use Avaya Enterprise Linux or if the Avaya Service accounts are installed on this server:

- Log in to the local Linux console as `sroot`.
- Or log in remotely as a non-root user and then change the user to `sroot` by entering the `su - sroot` command.

Otherwise, log in to Linux locally as `root`, or log in remotely as a non-root user and then change the user to `root` by entering the `su -` command.

2. Navigate to the Linux font directory by entering the `cd /usr/share/fonts` command.

*** Note:**

If the font directory does not already exist, create the directory by entering the `mkdir /usr/share/fonts` command, then navigate to the directory you just created.

3. Copy the Japanese font file to the font directory by entering the `cp $AVAYA_HOME/Support/fonts/ja/TTja.tar .` command.

! Important:

Make sure you include the `.` (period) at the end of the `cp` command to indicate that you want Linux to copy the files to the current directory.

4. Extract the font file by entering the `tar -xvf TTja.tar` command.
5. Copy the system language file to the Linux system configuration directory by entering the `cp $AVAYA_HOME/Support/fonts/ja/i18n/etc/sysconfig/` command.
6. Navigate to the Java fonts directory by entering the `cd $JAVA_HOME/jre/lib/fonts` command.

7. Create the fallback directory by entering the `mkdir fallback` command.
8. Navigate to the fallback directory by entering the `cd fallback` command.
9. Copy the Japanese font files to the fallback directory by entering the `cp /usr/share/fonts/ja/TrueType/*.ttf .` command.

! Important:

Make sure you include the `.` (period) at the end of the `cp` command to indicate that you want Linux to copy the files to the current directory.

10. Reboot the EPM server machine by entering the `reboot` command.

Related Links

[Non-English character support on the EPM web pages](#) on page 117

Configuring Korean on Avaya Enterprise Linux Procedure

1. Log in to Linux on the Experience Portal Primary EPM server.

If you are an Avaya Services representative, and use Avaya Enterprise Linux or if the Avaya Service accounts are installed on this server:

- Log in to the local Linux console as `sroot`.
- Or log in remotely as a non-root user and then change the user to `sroot` by entering the `su - sroot` command.

Otherwise, log in to Linux locally as `root`, or log in remotely as a non-root user and then change the user to `root` by entering the `su -` command.

2. Navigate to the Linux font directory by entering the `cd /usr/share/fonts` command.

*** Note:**

If the font directory does not already exist, create the directory by entering the `mkdir /usr/share/fonts` command, then navigate to the directory you just created.

3. Copy the Korean font file to the font directory by entering the `cp $AVAYA_HOME/Support/fonts/ko/TTko.tar .` command.

! Important:

Make sure you include the `.` (period) at the end of the `cp` command to indicate that you want Linux to copy the files to the current directory.

4. Extract the font file by entering the `tar -xvf TTko.tar` command.
5. Copy the system language file to the Linux system configuration directory by entering the following command:

`cp $AVAYA_HOME/Support/fonts/ko/i18n /etc/sysconfig/` command.

6. Navigate to the Java fonts directory by entering the `cd $JAVA_HOME/jre/lib/fonts` command.
7. Create the fallback directory by entering the `mkdir fallback` command.
8. Navigate to the fallback directory by entering the `cd fallback` command.
9. Copy the Korean font files to the fallback directory by entering the `cp /usr/share/fonts/ko/TrueType/*.ttf .` command.

! Important:

Make sure you include the . (period) at the end of the `cp` command to indicate that you want Linux to copy the files to the current directory.

10. Reboot the EPM server machine by entering the `reboot` command.

Related Links

[Non-English character support on the EPM web pages](#) on page 117

Chapter 9: Troubleshooting upgrade issues

Upgrade installation log files

The upgrade installation log files contain detailed information about the upgrade installation process.

Avaya Aura® Experience Portal creates several log files during the upgrade process. If the upgrade process:

- Completes successfully, Experience Portal copies the log files to `$AVAYA_HOME/logs/install_date`, where `$AVAYA_HOME` is the environment variable pointing to the installation path you specified on the Installation Destination installation screen and `date` is the date the installation process was run. The default installation directory is `/opt/Avaya/ExperiencePortal`.
- Does not complete successfully, Experience Portal leaves the log files in `/opt/_Avaya_Voice-Portal_temp`.

General installation log files

Log filename	Description
VP_Install.log	Main log containing output from all EPM and MPP installation processes. This is the first log file you should consult if you need to troubleshoot an installation issue.  Note: This file contains detailed log messages which might appear to be warnings or errors, but can safely be ignored, particularly if those warnings do not appear in the installation summary (ISSummary.log).
ISSummary.log	Summary of the Experience Portal installation, including any warning or error messages encountered during the installation.
ISOpt.log	InstallShield generated log containing internal data.
installSequence.log	Subset of ISOpt.log
prereqchecker.log	Detailed information from the Prerequisite Checker.
prereqchecker.out.log	Results from the Prerequisite Checker.
prereqchecker.err.log	Any internal errors encountered by the Prerequisite Checker.
prereqinstaller.log	Detailed information from the Prerequisite Installer.
prereqinstaller.out.log	Results from the Prerequisite Installer.

Table continues...

Log filename	Description
prereqinstaller.err.log	Any internal errors encountered by the Prerequisite Installer.
SetIAVersion<component>.log	Version history of the Experience Portal components installed. The <component> can be VPMS, MPP, or Docs.
ExtensionsPersistFiles.log	A directory containing files used to preserve properties during EPM upgrades.
installStatus.log	Log file generated for use by auto upgrade to log and track major steps during the installation
GetIAVersionVPMS.err.log	Log file containing any warning messages generated while trying to retrieve version information as part of an upgrade. The presence of a warning in this log file does not necessarily indicate an error.

MPP-specific installation log files

Log filename	Description
av-mpp-<buildnumber>-Install-<date>.log	mppinstall.sh script output.
av-mpp-<buildnumber>-Install-rpm-<date>.log	Output from the Red Hat Package Manager (RPM) during the MPP software installation.
mpp.cert.gen.out.log	Results from the security certificate generation process.
mpp.cert.gen.err.log	Any internal errors generated from the certificate generation process.
mpp.cert.imp.out.log	Results from the security certificate import process.
mpp.cert.imp.err.log	Any internal errors generated from the certificate import process.
mpp.key.import.out.log	Results from the public key import process from the EPM.
mpp.key.import.err.log	Any internal errors generated from the public key import process from the EPM.
mpp.key.log	Summary and fingerprint information about the public key imported by the MPP from the Primary EPM.

EPM-specific installation log files

Log filename	Description
vpms.cert.gen.out.log	Results from the security certificate generation process.
vpms.cert.gen.err.log	Any internal errors generated from the certificate generation process.
vpms.cert.imp.out.log	Results from the security certificate import process.
vpms.cert.imp.err.log	Any internal errors generated from the certificate import process.
vpms.cert.log	Summary and fingerprint information about the certificate generated during EPM installation that is used for communication with the MPP and any Auxiliary EPMs.

Primary EPM root certificate is signed with a weak hashing algorithm warning

The Experience Portal installer might display a warning message if the existing EPM Root certificate is signed with a weak hashing algorithm. Avaya recommends that you generate a new SHA256 2048 bit root certificate from the **Root Certificate** tab of the **Security > Certificate** page in EPM.

You must export the new root certificate and install it on applications such as speech servers, telephone, and LDAP servers to which the Experience Portal needs to make an SSL connection.

Fixing Prerequisite Checker failures

Solution

Procedure

1. Examine the Prerequisite Checker pages to determine exactly what problems were encountered.

 Tip:

If the error is `UnknownHostException: localhost`, see [Prerequisite Checker fails with UnknownHostException:localhost](#) on page 123.

2. Upgrade your system to meet the minimum hardware and operating system requirements for Experience Portal

Next steps

If you aborted the installation, enter `installvp/autoupgradevp` to start the installation.

After you upgrade your system, you can resume the Experience Portal installation script at the current point as long as you did *not* exit the installation script or restart your Experience Portal server. If you want to:

- Resume the script, type `2` and press `Enter` until you go past the first Prerequisite Status page. Experience Portal reruns the Prerequisite Checker and you can then continue with the installation instructions.
- Quit the installation script, type `3` and press `Enter`, then type `1` and press `Enter` to confirm.

Prerequisite Checker fails with UnknownHostException:localhost

If you receive an error during the prerequisite check for the `localhost`, or a `faultString` reporting `UnknownHostException:localhost` during Experience Portal installation or upgrade,

it is likely that the `/etc/hosts` file of the server is not properly set up. As a result, the installation script cannot deploy certain Experience Portal components correctly.

The `/etc/hosts` file is a simple text file that associates IP addresses with one or more hostnames. The format is one line per IP address, with the associated hostnames separated by white space (spaces or tabs).

Solution

Procedure

1. Log into Linux on the EPM server.

If you are an Avaya Services representative, and use Avaya Enterprise Linux or if the Avaya Service accounts are installed on this server:

- Log in to the local Linux console as `sroot`.
- Or log in remotely as a non-root user and then change the user to `sroot` by entering the `su - sroot` command.

Otherwise, log in to Linux locally as root, or log in remotely as a non-root user and then change the user to root by entering the `su -` command.

2. Back up the original file prior to editing it by entering the `cp /etc/hosts /etc/hosts.bak` command.
3. With the ASCII text editor of your choice, open the `/etc/hosts` file.
4. Verify that:
 - The first line contains `127.0.0.1 localhost localhost.localdomain`, with the IP address and hostnames separated by spaces or tabs
 - If the file has other entries, each entry must be in the form `IP_address hostname1 hostname2...`, where `IP_address` is the IP address of a server in the Experience Portal system and `hostname1 hostname2...` is one or more hostnames, separated by tabs or spaces, to associate with the IP address.

Example

The following shows a properly-formatted `/etc/hosts` file with two MPP servers:

<code>127.0.0.1</code>	<code>localhost</code>	<code>localhost.localdomain</code>	<code>#Required first line</code>
<code>123.123.123.122</code>	<code>epm_server_hostname</code>		<code>#Primary EPM server IP address and hostname</code>
<code>123.123.123.123</code>	<code>first_mpp.domainname.com</code>	<code>first_MPP</code>	<code>#First MPP server</code>
<code>123.123.123.123</code>	<code>second_mpp.domainname.com</code>	<code>second_MPP</code>	<code>#Second MPP server</code>

Fixing Prerequisite Installer failures

The Prerequisite Installer installs additional software required for Experience Portal such as the Apache Web Server, Tomcat, and php. The majority of this software comes from RPMs installed by the Prerequisite Installer.

Installer failures are generally the result of installing Experience Portal on a server running a:

- More recent supported version of Red Hat Enterprise Linux Server. Although Experience Portal does support updates to Red Hat Enterprise Linux Server, some system RPMs in the newer updates can conflict with some of the RPMs that Experience Portal is attempting to install.
- Customized Red Hat Enterprise Linux Server installation that is missing an RPM required by one of the Experience Portal prerequisite RPMs.

Solution

Procedure

1. Examine the Prerequisite Installer report to determine exactly what problems were encountered and what log file, if any, is available for more information.

For an example of one such error, see [Sample Prerequisite Installer error message](#) on page 126.

2. If you are using a supported version of Red Hat Enterprise Linux Server and the Prerequisite Installer fails for any of the php RPMs, install the following RPMs from your Red Hat Enterprise Linux Server installation DVD or the Red Hat support website:

- `php-common.x86_64`
- `php-cli.x86_64`
- `php.x86_64`
- `php-soap.x86_64`
- `php-xml.x86_64`
- `php-pgsql.x86_64`
- `php-process.x86_64`

3. If that does not solve the problem, see [Identifying RPM issues](#) on page 127 for more information.

Next steps

If you aborted the installation, enter `installvp/autoupgradevp` to start the installation.

After you fix any prerequisite software issues, you can resume the Avaya Aura® Experience Portal installation script at the current point as long as you did *not* exit the installation script or restart your Avaya Aura® Experience Portal server. If you want to:

- Resume the script, type `2` and press `Enter` until you go past the first Installation Status page. Avaya Aura® Experience Portal reruns the Prerequisite Installer and you can then continue with the installation instructions.
- Quit the installation script, type `3` and press `Enter`, then type `1` and press `Enter` to confirm.

Sample Prerequisite Installer error message

The following is an example of the error messages produced by the Prerequisite Installer when the installer encounters a more recent version of the JDK than Experience Portal was about to install. You can use this example as a guideline for solving any Prerequisite Installer issues you encounter.

```
=====
=====
Installation Status
=====
=====
- Third-Party
Software=====
| - Semange Libraries-----Success
| - ActiveMQ-----Success
| - GCC and C++ Shared Libraries -----Success
| - Java(TM) 2 SDK Standard Edition-----Failed
```

The following line indicates the start of the error information:

```
| |      Error:  RPM Installation failed with the following detail.
| |      =====
| |      jdk-1.7.0_45-fcs.x86_64.rpm install
| |      - original directory='/mnt/cdrom/external'
| |      - RPM install directory='/mnt/cdrom/external/J2SDK'
| |      - RPM name ='jdk-1.7.0_45-fcs.x86_64.rpm'
| |      - LOG file = '/tmp/Avaya/install-rpm.log'
| |      -----
| |      >>>>>Starting RPM installation: 'rpm -U --replacepks
jdk-1.7.0_45-fcs.x86_64.rpm'
```

The following two lines show the installed JDK version and why it does not match the version Experience Portal needs to install:

```
| |      package jdk-1.7.0_48-fcs (which is newer than jdk-1.7.0_45-fcs)
is
| |      Already Completed
| |      >>>>>RPM Installation failed: Exit Code: 2
| |      =====
```

The following three lines restate the error that the version found was not the version expected:

```
| |      RPM installation check: Expecting 'Found' = 'Expected'.
| |      Expected: jdk-1.7.0_45-fcs.x86_64.rpm
| |      Found:      jdk-1.7.0_45-fcs          Out of Date
| |      Non-compliant Java SDK found.  Enter "rpm -e j2sdk" in the
command line
| |      to uninstall the SDK, then run the prerequisite installer
again.
```

```
=====
=====
Install aborted due to installation failure.
```

=====

=====

To resolve this issue:

1. If you want to verify that this version is actually installed, enter the `rpm -q jdk` command.
2. Before you remove the more recent RPM version that you have installed, check the Avaya online support Web site, <http://support.avaya.com>, to make sure that a solution to this issue has not been posted. If no solution is available:
 - a. Look at the `RPM installation check` line, which is the third highlighted line in the example. In this case, the Prerequisite Installer expected that the version it found installed on the system would be identical to the version it was installing. The solution is to remove the more recent version and let the Prerequisite Installer install the JDK version Experience Portal requires.
 - b. To remove the installed JDK version, enter the `rpm -e jdk` command.
 - c. Once the JDK has been removed, return to the Experience Portal installation script and resume the installation.

Identifying RPM issues

If you have installed a supported version of Red Hat Enterprise Linux Server, you should also verify that the correct RPMs are installed on your system. If you are registered with Red Hat to automatically receive updates, there might be a conflict with one or more of the updated RPMs.

The Experience Portal installation included a file that lists the RPMs and version numbers in the supported version of Red Hat Enterprise Linux Server. This file is installed in `$AVAYA_HOME/Support/RedHat-RPM-Lists` and on the Experience Portal installation DVD under `Support/RedHat-RPM-Lists`.

You can generate a listing of the RPMs that are currently installed on your system and then compare the RPMs you have installed against what has been verified. Other versions than the ones verified might cause your Experience Portal system not to operate.

Note:

If the list of RPMs installed on your system does not exactly match the list of RPMs in the `RedHat-RPM-Lists` file that is located in the Support directory of the Experience Portal installation DVD, it does not necessarily mean there is a problem. However, if you are still experiencing problems after you have reviewed the installation log files and initial configuration settings, you might bring your system in line with the verified list of RPMs to see if that solves the problem.

Solution

Procedure

1. Log in to Linux on the Experience Portal Primary EPM server.

If you are an Avaya Services representative, and use Avaya Enterprise Linux or if the Avaya Service accounts are installed on this server:

- Log in to the local Linux console as `sroot`.
- Or log in remotely as a non-root user and then change the user to `sroot` by entering the `su - sroot` command.

Otherwise, log in to Linux locally as `root`, or log in remotely as a non-root user and then change the user to `root` by entering the `su -` command.

2. Enter the `cat /etc/issue` command.
3. Verify that the version is Release 6.5 64 bit or later.
4. To get a list of the RPMs installed on your system and redirect the list to a file, enter the `rpm -qa | sort > /tmp/rpmlist.txt` command.

When the system has finished generating `rpmlist.txt`, it stores the file in the `/tmp` directory.

5. To find any differences between the RPMs currently installed and the RPMs that are required for Experience Portal, enter the `diff /tmp/rpmlist.txt $AVAYA_HOME/Support/RedHat-RPM-Lists/RHEL6.4.txt` command.
6. Review the reported differences and bring the installed RPMs in line with the RPMs listed in the `Support > RedHat-RPM-Lists` directory of the Experience Portal installation DVD.
7. If you need the correct version of an RPM, download it from Red Hat website, <http://www.redhat.com>.
8. Once you have identified the problems and downloaded any required RPMs:
 - To upgrade an RPM to a different version, enter the `rpm -U <path>/rpmname` command, where `<path>` is the complete path and `rpmname` is the filename of the RPM you are updating.
 - To install an RPM, enter the `rpm -i path/rpmname` command, where `path/rpmname` is the complete filename and path of the RPM you are installing.
 - To remove an RPM, enter the `rpm -e rpmname` command, where `rpmname` is the name of the RPM you are removing.

 Important:

Do not specify a file path when you remove an RPM.

Installation Progress Bar stops at 25% completed

If the **Installation Progress Bar** does not advance beyond 25% completed and the Post Installation Summary screen states that no summary information could be found, then InstallShield has encountered an internal error and the Experience Portal installation or upgrade was not successful.

This error condition is shown in the following example:

```

Installation Progress
Note: The last portion of the install might take several minutes to
complete.
Please be patient and wait for the Post Installation Summary to be
displayed.
Installing Avaya Aura Experience Portal. Please wait...
|-----|-----|-----|-----|
0%          25%          50%          75%          100%
|||||||
-----
-----
Post Installation Summary
The Avaya Aura Experience Portal
  installation has completed. Review the following information.
If there are errors or warnings, then please review the installation
logs.
No summary information could be found; please check the log files for
more
information
Press 3 to Finish or 5 to Redisplay [3]
java.io.IOException: java.io.IOException: /opt/_Avaya_Voice-Portal_temp/
MoveLogFiles: not found
    at java.lang.UNIXProcess.<init>(UNIXProcess.java:143)
    at java.lang.Runtime.execInternal(Native Method)
    at java.lang.Runtime.exec(Runtime.java:566)
    at com.installshield.util.Java2ProcessExec.processExec(Unknown
Source)
    at com.installshield.util.ProcessExec.executeProcess(Unknown
Source)
    at
com.installshield.wizardx.actions.ExecWizardAction.executeProcess(Unknown
Source)
    at com.installshield.wizardx.actions.ExecWizardAction.run(Unknown
Source)
    at java.lang.Thread.run(Thread.java:534)

```

In this case, no Experience Portal software was actually installed or upgraded.

Solution

Procedure

1. Type 3 to finish the aborted installation or upgrade process.
2. Return to the beginning of the installation or upgrade procedure you were following and rerun the Experience Portal installation script `installvp` or `autoupgradevp`.

EPM upgrade finishes with an Axis error

A known issue with Axis sometimes affects the EPM software upgrade. If this problem occurs, the EPM software installer displays either `Exception: AxisFault` or `Warning: Axis may not be accepting new applications properly`, as shown in the following Post Installation Summary screens.

First sample Post Installation Summary screen:

```
Installing EPM...
Possible Error during operation: Register vpappLog with Axis
- Start error description -
Exception: AxisFault
faultCode: {http://schemas.xmlsoap.org/soap/
envelope/}Server.generalException
  faultSubcode:
    faultString: Couldn't find an appropriate operation for XML QName
{http://xml.apache.org/axis/wsdd/}deployment
    faultActor:
    faultNode:
    faultDetail:
    {http://xml.apache.org/axis/}hostname:takuma.avaya.com

- End error description -
Possible Error during operation: Deploy Core Services (Part 2/2)
- Start error description -
Error: Could not deploy network log server: 255
Error: Could not deploy alarm server: 255
- End error description -
```

Second sample Post Installation Summary screen showing the `Warning: Axis may not be accepting new applications properly` message:

```
Installing Documentation...
...done installing Documentation
Installing EPM...
Possible Error during operation: Start Tomcat
- Start error description -
Warning: Axis may not be accepting new applications properly
- End error description -
...done installing EPM
Installing MPP...
...done installing MPP
```

Solution

Procedure

1. Type 3 to finish the incomplete installation process.
2. Return to the beginning of the installation procedure you were following and rerun the Experience Portal installation script `installvp` or `autoupgradevp`.

Upgrade hangs at Post Installation Summary screen

A known InstallShield issue sometimes causes the software upgrade to hang, especially if there is a long delay between steps.

The Post Installation Summary screen displays messages similar to the following:

```
Post Installation Summary

The Avaya Aura Experience Portal installation has completed. Review the following
information. If there are errors or warnings, then please review the
installation logs.

Installing Documentation...
Press 3 to Finish or 5 to Redisplay [3]
```

Solution

Procedure

Restart the installation script from the beginning, making sure that you do not pause too long between steps.

The Post Installation Summary screen should display messages similar to the following:

```
Post Installation Summary

The Experience Portal installation has completed. Review the following
information. If there are errors or warnings, then please review the
installation logs.

Installing Documentation...
...done installing Documentation

Installing EPM...
...done installing EPM

Press 3 to Finish or 5 to Redisplay [3] 3
Moving installation logs to: /opt/Avaya/ExperiencePortal/logs/install_2013-12-12.000

[sroot@vpms-server cdrom]# reboot
```

MPP upgrade is hanging

Any hung or stale NFS mount points can cause RPM installations to hang while upgrading the Experience Portal software.

Solution

Procedure

1. On the MPP server, enter the `df` command.
2. If the server:
 - Responds to this command, then all NFS mount points are operational. Make sure that the EPM and MPP clocks are properly synchronized .
 - Does not respond to the command, continue with this procedure.
3. Enter the `umount -l` command to unmount any file systems.
4. If not already done, exit the Experience Portal installation script.
5. If the automount feature is enabled, disable it by commenting out the appropriate lines in the server's `/etc/fstab` file.
6. Reboot the server.
7. Restart the installation script from the beginning.

MPP or Auxiliary EPM could not import EPM key

The Primary EPM upgrades correctly but the MPP or Auxiliary EPM upgrade fails. The error happens after the user is asked to enter the Primary EPM server location during the MPP or aux interview. The following is an example of an error message that is displayed. Since the text includes the name and the IP address of Primary EPM, the text varies from one system to another:

```
Public Key Verification
```

```
Please verify the following Public Key. Proceed to the next dialog if you wish
to install this key on this system, or return to the previous dialog to modify
your selection or correct any errors below
```

```
Error: Specified host does not appear to be a valid primary EPM: <IP address>
```

```
Press 2 for Previous, 3 to Cancel or 5 to Redisplay [2]
```

The most common cause of this error is that the *iptables* firewall is enabled on the MPP server. If this is the case, disable it as described below. If not, contact Avaya technical support.

Solution

Procedure

1. Log in to Linux on the Experience Portal Primary EPM server.

If you are an Avaya Services representative, and use Avaya Enterprise Linux or if the Avaya Service accounts are installed on this server:

- Log in to the local Linux console as `sroot`.
- Or log in remotely as a non-root user and then change the user to `sroot` by entering the `su - sroot` command.

Otherwise, log in to Linux locally as root, or log in remotely as a non-root user and then change the user to root by entering the `su -` command.

2. Determine whether the `iptables` firewall is active by entering the `service iptables status` command.
3. If the firewall is:
 - Running, disable it by entering the `chkconfig --del iptables` command and proceed to Step 4.
 - Not running, try to manually download the certificate by entering the `curl http://EPM-server/cert.pem` command, where *EPM-server* is the domain name or IP address of the system where the Primary EPM software is installed.

If the command displays the lines `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----`, regardless of what information is displayed between those lines, continue with this procedure. Otherwise, contact your Avaya Services representative.

4. Restart the `vpms` service by entering the `/sbin/service vpms restart` command.

You will see a series of messages as the command starts to shut down EPM components. When the command has successfully stopped all relevant components, the system displays the message: `VPMS Shutdown Status: [ OK ]`.

The command immediately starts the relevant components. When the command is run successfully, the system displays the message: `VPMS Start Status: [ OK ]`.

5. Verify that you can log in to the EPM Web interface as described in the *Logging in to the Avaya Aura® Experience Portal web interface* topic in the *Administering Avaya Aura® Experience Portal* guide.
6. Return to the MPP server and either continue the current installation or restart the installation process.

Changing the Product ID for an existing Experience Portal system

Before you begin

If you have just installed or upgraded the Experience Portal software and are still logged into the server, verify that you reloaded the environment variables as described in [Reloading the Experience Portal environment variables](#) on page 139.

Procedure

1. Log in to Linux on the Experience Portal Primary EPM server.

If you are an Avaya Services representative, and use Avaya Enterprise Linux or if the Avaya Service accounts are installed on this server:

- Log in to the local Linux console as sroot.
- Or log in remotely as a non-root user and then change the user to sroot by entering the `su - sroot` command.

Otherwise, log in to Linux locally as root, or log in remotely as a non-root user and then change the user to root by entering the `su -` command.

2. Navigate to the Support/VP-Tools directory by entering the `cd /opt/Avaya/ExperiencePortal/Support/VP-Tools` command.
3. Stop `vpms` service by entering the `service vpms stop` command.
4. To run the script:

On Linux: Enter the `bash ResetProductID New_ProductID` command where `New_ProductID` is the product ID that you want to use.

5. Restart `vpms` service by entering the `service vpms restart` command.
6. Restart all MPPs by entering the `service mpp restart`
7. Follow any on-screen instructions displayed by the script.

Invalid password for database user

The EPM auto upgrade fails with the invalid password error.

The most common cause of this error is that the password could not be loaded from configuration or the password validation failed.

Solution

1. Reboot the server
2. Restart the upgrade script by selecting the Interactive EPM upgrade option. The interactive upgrade allows you to create a new user account and password to access the database.

Time synchronization problems

Experience Portal uses Network Time Protocol (NTP) to control and synchronize the clocks when the EPM and MPP software is running on different servers. The dedicated MPP servers and the optional auxiliary EPM server point to the primary EPM server as the reference clock.

To troubleshoot synchronization errors, perform the following procedures in the order given, advancing to the next procedure only if the problem continues to persist.

Determining whether the servers are synchronized

Procedure

1. Simultaneously log in to Linux on the EPM server, each MPP server, and, if configured, the optional auxiliary EPM server.
2. On each server, during the same time enter the `date` command.
3. Verify that each MPP server and the optional auxiliary EPM server are synchronized with the primary EPM server.
4. If you find one or more unsynchronized servers, follow the procedure [Verify that the NTP service is operating properly](#) on page 135 below.

Verify that the NTP service is operating properly

Procedure

1. If necessary, log in to Linux on each unsynchronized MPP or auxiliary EPM server.

If you are an Avaya Services representative, and use Avaya Enterprise Linux or if the Avaya Service accounts are installed on this server:

- Log in to the local Linux console as `sroot`.
- Or log in remotely as a non-root user and then change the user to `sroot` by entering the `su - sroot` command.

Otherwise, log in to Linux locally as root, or log in remotely as a non-root user and then change the user to root by entering the `su -` command.

2. Enter the `/sbin/service ntpd status` command.

If the server returns a message stating that the NTP service is running, continue with this procedure. Otherwise, go to [Synchronizing the MPP or auxiliary EPM clock with the primary EPM](#) on page 136.

3. To verify that the NTP service is operating properly, enter the `/usr/sbin/ntpq -np` command.
4. A status message similar to the following appears:

```

remote      refid      st    t   when  poll  reach  delay
offset  jitter
=====
=====
123.123.123.123  LOCAL(0)   6     u   23    64     1     0.354
0.361      0.004

```

If the `jitter` value displayed is 4000, go to [Synchronizing the MPP or auxiliary EPM clock with the primary EPM](#) on page 136.

 Note:

The remote IP address displayed should point to the primary EPM server.

Synchronizing the MPP or auxiliary EPM clock with the primary EPM

Procedure

1. If you are working with an MPP server and the MPP software is running, stop it using the EPM Web interface:
 - a. Log in to the EPM Web interface using an account with the Administration or Operations user role.
 - b. From the EPM main menu, select **System Management > MPP Manager**.
 - c. On the MPP Manager page, click the selection box associated with the MPP that you want to stop, then click **Stop** in the **State Commands** group.
 - d. Confirm the action when requested.
 - e. Wait until the operational state changes to Stopped.
To check this, click **Refresh** and look at the **State** field.

 Note:

The operational state changes when the last active call completes or the operational grace period expires, whichever comes first.

2. If necessary, log in to Linux on the server.
If you are an Avaya Services representative, and use Avaya Enterprise Linux or if the Avaya Service accounts are installed on this server:
 - Log in to the local Linux console as sroot.
 - Or log in remotely as a non-root user and then change the user to sroot by entering the `su - sroot` command.Otherwise, log in to Linux locally as root, or log in remotely as a non-root user and then change the user to root by entering the `su -` command.
3. If you are working with:
 - An MPP server, stop the `mpp` process by entering the `/sbin/service mpp stop` command.
 - The auxiliary EPM server, stop the `vpms` service by entering the `/sbin/service vpms stop` command.
4. Restart the NTP process by entering the `/sbin/service ntpd restart` command.

The system returns:

```
Shutting down ntpd: [OK]
Synchronizing with time server [OK]
Starting ntpd: [OK]
```

*** Note:**

After you restart the NTP process, wait up to 10 minutes for the server to synchronize with the EPM.

5. After you give the servers enough time to synchronize themselves, verify that the process worked by entering the `/usr/sbin/ntpq -np` command.

A status message similar to the following appears:

```
remote          refid      st    t   when  poll   reach   delay
offset jitter
=====
=====
123.123.123.123  LOCAL(0)   6     u   23    64     1      0.354
0.361  0.004
```

*** Note:**

The remote IP address displayed should point to the primary EPM server.

6. If the `jitter` value is still set to 4000, go to [Advanced time synchronization troubleshooting](#) on page 137 below. Otherwise continue with this procedure.
7. If you are working with:
 - An MPP server, start the `mpp` process by entering the `/sbin/service mpp start` command.
 - The auxiliary EPM server, start the `vpms` service by entering the `/sbin/service vpms start` command.
8. Verify the service has started by entering the `/sbin/service mpp status` or `/sbin/service vpms status` command.

Advanced time synchronization troubleshooting

Procedure

1. If necessary, log in to Linux on the MPP or auxiliary EPM server.

If you are an Avaya Services representative, and use Avaya Enterprise Linux or if the Avaya Service accounts are installed on this server:

- Log in to the local Linux console as `sroot`.
- Or log in remotely as a non-root user and then change the user to `sroot` by entering the `su - sroot` command.

Otherwise, log in to Linux locally as root, or log in remotely as a non-root user and then change the user to root by entering the `su -` command.

2. Using an ASCII text editor, open the following files on the server and ensure that the hostname or the IP address of the primary EPM server is correct:
 - `/etc/ntp.conf`
 - `/etc/ntp/step-tickers`
3. If the IP address or hostname is incorrect in either of the above files, fix it then save and close the files. Otherwise simply close the files.
4. If the primary EPM server is synchronized with an external clock, verify that the `/etc/ntp.conf` file on the primary EPM server is properly set up.
5. If you made any changes to the files:
 - a. Stop the appropriate service by entering the `service mpp stop` or `/sbin/service vpms stop` command.
 - b. Restart the NTP process by entering the `/sbin/service ntpd restart` command.

The system returns:

```
Shutting down ntpd: [OK]
Synchronizing with time server [OK]
Starting ntpd: [OK]
```

*** Note:**

After you restart the NTP process, wait up to 10 minutes for the server to synchronize with the EPM.

- c. After you give the servers enough time to synchronize themselves, verify that the process worked by entering the `/usr/sbin/ntpq -np` command.

A status message similar to the following appears:

```
remote          refid      st   t   when  poll  reach
delay  offset jitter
=====
=====
123.123.123.123  LOCAL(0)   6    u   23    64    1
0.354    0.361  0.004
```

*** Note:**

The remote IP address displayed should point to the primary EPM server.

6. If the `jitter` value is still set to 4000:
 - a. Reboot the server.
 - b. Enter the `/usr/sbin/ntpq -np` command.
 - c. If the `jitter` value is still set to 4000, reinstall the MPP or auxiliary EPM software.

Time Synchronization between external database and EPM servers

If you connect a Experience Portal system to an external database, you may want to make sure that you synchronize the time so that it is same across all servers. While Experience Portal only requires that the EPM and MPP server time be synchronized, you can also synchronize all the servers that Experience Portal connects to. For more information, see the *External time sources* topic in the *Implementing Avaya Aura® Experience Portal on multiple servers* guide.

Reloading the Experience Portal environment variables

After you install or upgrade an Experience Portal server, you need to load the new environment variables.

Procedure

1. Log completely out of the Linux system.
2. If you are on the console and are working with:
 - Avaya Enterprise Linux, enter the `su - sroot` command.
 - Red Hat Enterprise Linux Server, enter the `su -` command.

 Note:

If you are a remote user, log in to Linux by entering a non-root user name and password at the prompts.

Recovering Avaya Enterprise Linux configuration information after an upgrade

You can still access configuration information from any text files stored on your 5.1, 6.0, or 7.0 Avaya Enterprise Linux system even after you upgrade the operating system.

Procedure

1. Log in to Linux on the Experience Portal server.

If you are an Avaya Services representative, and use Avaya Enterprise Linux or if the Avaya Service accounts are installed on this server:

- Log in to the local Linux console as sroot.
- Or log in remotely as a non-root user and then change the user to sroot by entering the `su - sroot` command.

Otherwise, log in to Linux locally as root, or log in remotely as a non-root user and then change the user to root by entering the `su -` command.

2. Change to the `/root2` directory to access the 5.1, 6.0, or 7.0 partition by entering the `cd /root2` command.

The files from the previous installation are available.

Restoring the previous operating system after an upgrade

Restore the 5.1, 6.0, or 7.0 software on Avaya Enterprise Linux

If you want to revert an upgraded Experience Portal system running on Avaya Enterprise Linux back to 5.1, 6.0, or 7.0, you must perform the steps mentioned in the following table:

Step	Description	✓
1	Restore the previous version of Avaya Enterprise Linux on all Experience Portal servers as described in Restoring the Avaya Enterprise Linux 5.1, 6.0, or 7.0 operating system on page 140.	
2	Restore the 5.1, 6.0, or 7.0 Primary EPM server as described in Restoring the 5.1, 6.0, or 7.0 software on the Primary EPM server or a single-server Experience Portal system running Avaya Enterprise Linux on page 141.	
3	Restore the 5.1, 6.0, or 7.0 software on the Auxiliary EPM server as described in Restoring OS on Auxiliary EPM server on page 142.	
4	Restore the 5.1, 6.0, or 7.0 MPP servers as described in Restoring the 5.1, 6.0, or 7.0 MPP software on a server running Avaya Enterprise Linux on page 143.	

Related Links

[Restoring the Avaya Enterprise Linux 5.1, 6.0, or 7.0 operating system](#) on page 140

[Restoring the 5.1, 6.0, or 7.0 software on the Primary EPM server or a single-server Experience Portal system running Avaya Enterprise Linux](#) on page 141

[Restoring the 5.1, 6.0, or 7.0 software on the Auxiliary EPM server running Avaya Enterprise Linux](#) on page 142

[Restoring the 5.1, 6.0, or 7.0 MPP software on a server running Avaya Enterprise Linux](#) on page 143

Restoring the Avaya Enterprise Linux 5.1, 6.0, or 7.0 operating system

Before you begin

If you are working with an MPP server, take the MPP offline.

Procedure

1. Log in to Linux on the Experience Portal server.

If you are an Avaya Services representative, and use Avaya Enterprise Linux or if the Avaya Service accounts are installed on this server:

- Log in to the local Linux console as `sroot`.
- Or log in remotely as a non-root user and then change the user to `sroot` by entering the `su - sroot` command.

Otherwise, log in to Linux locally as root, or log in remotely as a non-root user and then change the user to root by entering the `su -` command.

2. Verify which partition is the boot partition by entering the `/opt/Avaya/LinuxInstaller/bin/cpartition` command.
3. If the boot partition is not equal to the standby partition (which contains your previous Avaya Enterprise Linux version), revert to the previous boot partition by entering the `/opt/Avaya/LinuxInstaller/bin/cpartition -c` command.

Note:

The `-o` and `-p` options are not used with the current **cpartition** version. The `-c` option changes the boot partition from Standby to Active, and makes it permanent.

4. Reboot the server.

Related Links

[Restore the 5.1, 6.0, or 7.0 software on Avaya Enterprise Linux](#) on page 140

Restoring the 5.1, 6.0, or 7.0 software on the Primary EPM server or a single-server Experience Portal system running Avaya Enterprise Linux

Before you begin

Make sure you have restored the operating system as described in [Restoring the Avaya Enterprise Linux 5.1, 6.0, or 7.0 operating system](#) on page 140.

Procedure

1. Log in to Linux on the Experience Portal Primary EPM server.

If you are an Avaya Services representative, and use Avaya Enterprise Linux or if the Avaya Service accounts are installed on this server:

- Log in to the local Linux console as `sroot`.
- Or log in remotely as a non-root user and then change the user to `sroot` by entering the `su - sroot` command.

Otherwise, log in to Linux locally as root, or log in remotely as a non-root user and then change the user to root by entering the `su -` command.

2. Stop the `vpms` service by entering the `/sbin/service vpms stop` command.

You will see a series of messages as the command starts to shut down the EPM components. When the command has successfully stopped all relevant components, the system displays the message: `VPMS Shutdown Status: [ OK ]`.

3. Check the status of the `postgres` service by entering the `/sbin/service postgresql status` command.
4. If the `postgres` service is running, stop it by entering the `/sbin/service postgresql stop` command.
5. Navigate to the `pgsql` directory by entering the `cd /var/lib/pgsql` command.
6. Rename the current data directory that contains the 7.0 data by entering the `mv data data_OLD` command.
7. In the `pgsql` directory, locate the backup directory that Experience Portal created when you installed the new version. The file name has the format `data_vp_<backup_date>_<backup_time>`.
8. Copy this backup directory into the main data directory by entering the `cp -rp data_vp_<backup_date>_<backup_time> data` command.
9. Start the `postgresql` service by entering the `/sbin/service postgresql start` command.
10. Wait for a few seconds for the database to start, then verify that it is running by entering the `/sbin/service postgresql status` command.
11. Start the `vpms` service by entering the `/sbin/service vpms start` command.

You will see a series of messages as the command starts several EPM components. When the command has successfully started all relevant components, the system displays the message: `VPMS Start Status: [ OK ]`.

Related Links

[Restore the 5.1, 6.0, or 7.0 software on Avaya Enterprise Linux](#) on page 140

Restoring the 5.1, 6.0, or 7.0 software on the Auxiliary EPM server running Avaya Enterprise Linux

Before you begin

Make sure you have restored the operating system as described in [Restoring the Avaya Enterprise Linux 5.1, 6.0, or 7.0 operating system](#) on page 140.

Procedure

1. Log in to Linux on the Auxiliary EPM server

If you are an Avaya Services representative, and use Avaya Enterprise Linux or if the Avaya Service accounts are installed on this server:

- Log in to the local Linux console as `sroot`.

- Or log in remotely as a non-root user and then change the user to root by entering the `su - sroot` command.

Otherwise, log in to Linux locally as root, or log in remotely as a non-root user and then change the user to root by entering the `su -` command.

2. Stop the `vpms` service by entering the `/sbin/service vpms stop` command.

You will see a series of messages as the command starts to shut down the EPM components. When the command has successfully stopped all relevant components, the system displays the message: `VPMS Shutdown Status: [ OK ]`.

3. Check the status of the `postgres` service by entering the `/sbin/service postgresql status` command.
4. If the `postgres` service is running, stop it by entering the `/sbin/service postgresql stop` command.
5. Navigate to the `pgsql` directory by entering the `cd /var/lib/pgsql` command.
6. Rename the current data directory that contains the 7.0 data by entering the `mv data data_OLD` command.
7. In the `pgsql` directory, locate the backup directory that Experience Portal created when you installed the new version. The file name has the format `data_vp_<backup_date>_<backup_time>`.
8. Copy this backup directory into the main data directory by entering the `cp -rp data_vp_<backup_date>_<backup_time> data` command.
9. Start the `postgresql` service by entering the `/sbin/service postgresql start` command.
10. Wait for a few seconds for the database to start, then verify that it is running by entering the `/sbin/service postgresql status` command.
11. Start the `vpms` service by entering the `/sbin/service vpms start` command.

You will see a series of messages as the command starts several EPM components. When the command has successfully started all relevant components, the system displays the message: `VPMS Start Status: [ OK ]`.

Related Links

[Restore the 5.1, 6.0, or 7.0 software on Avaya Enterprise Linux](#) on page 140

Restoring the 5.1, 6.0, or 7.0 MPP software on a server running Avaya Enterprise Linux

Before you begin

- Make sure you have restored the operating system as described in [Restoring the Avaya Enterprise Linux 5.1, 6.0, or 7.0 operating system](#) on page 140.
- Make sure you have restored the Primary EPM server.

Procedure

1. Restore the log files.
2. If the server is an MPP and you have moved the MPP logs to a new directory or a partition using the `mppMoveLogs.sh` script, add the appropriate mount point to the `/etc/fstab` file. For more information, see *Administering Avaya Aura® Experience Portal*.

Next steps

At this point, you can:

- Restore another MPP server.
- Start the restored MPP as described in *Administering Avaya Aura® Experience Portal*.
- Start multiple restored MPP servers as described in *Administering Avaya Aura® Experience Portal*.

Related Links

[Restore the 5.1, 6.0, or 7.0 software on Avaya Enterprise Linux](#) on page 140

Restoring the 5.1, 6.0, or 7.0 software on a dedicated Primary EPM server or a single-server EPM system running Red Hat Enterprise Linux Server

Before you begin

Ensure that you have access to the backup files taken before the upgrade. For more information about backing up the existing 5.1, 6.0, or 7.0 data, see *Upgrading to Avaya Aura® Experience Portal 7.0.1*.

About this task

Note:

If your installation uses a dedicated Primary EPM server, you should always restore the Primary EPM server first and then you can restore each Auxiliary EPM and MPP server separately.

Procedure

1. Install the previous version of Red Hat Enterprise Linux Server using the Red Hat Enterprise Server installation CD-ROM and the exact options you used for the 5.1, 6.0, or 7.0 software installation.
2. Reinstall the EPM software from your 5.1, 6.0, or 7.0 software installation DVD.
Ensure that you select the same options that you selected during the first install.
3. Restore your Experience Portal database from the backup as described in the document *Upgrading to Avaya Aura® Experience Portal 7.0.1*.
4. If you have changed the default log and alarm retention periods, reset those values as described in *Administering Avaya Aura® Experience Portal*.

Restoring the 5.1, 6.0, or 7.0 software on an Auxiliary EPM server running Red Hat Enterprise Linux Server

Before you begin

If your installation uses a dedicated Primary EPM server, you should always restore the Primary EPM server first and then restore each Auxiliary EPM.

Procedure

1. Install the previous version of Red Hat Enterprise Linux Server using the Red Hat Enterprise Server installation CD-ROM and the exact options you used for the 5.1, 6.0, or 7.0 software installation.
2. Reinstall the EPM software from your 5.1, 6.0, or 7.0 software installation DVD.
Ensure that you select the same options that you selected during the first install.
3. Reestablish the link between the MPP and the Auxiliary EPM as described in [Reestablishing the link between the EPM and the MPP](#) on page 103.

Restoring a dedicated 5.1, 6.0, or 7.0 MPP server on Red Hat Enterprise Linux Server

To restore 5.1, 6.0, or 7.0, you need to reinstall the operating system and then reinstall the Experience Portal software.

Before you begin

Make sure you have already restored your Primary EPM server.

Procedure

1. Take the MPP offline.

 Note:

If you cannot stop the MPP through the EPM, log onto the MPP server and stop the process by entering the `/sbin/service mpp stop` command.

2. Install Red Hat Enterprise Linux Server using the Red Hat Enterprise Linux Server installation CD-ROM and the exact options you used for Avaya Voice Portal 5.1, Experience Portal 6.0, or 7.0.
3. Reinstall the MPP software from your Experience Portal installation DVD. Verify that you select the same options that you selected during the first install.
4. Restore the MPP log files.
5. If you changed the AVB configuration files, restore the customized files.

6. If all MPP servers have been restored, reestablish the link between the restored EPM server and the restored MPP servers.

Next steps

- Restore another MPP by following this procedure on that MPP.

Chapter 10: Preupgrade worksheets

Primary EPM server upgrade worksheet

Complete this worksheet if you are installing the EPM server on a dedicated Avaya Aura® Experience Portal server.

Requirement/ Information Needed	Your value	Notes
Ensure that the hardware meets the minimum requirements. For more information on minimum server machine hardware requirements, see <i>Avaya Aura® Experience Portal Overview and Specification</i> on http://support.avaya.com .		For minimum hardware requirements, see Minimum (Linux) server machine hardware requirements on page 40.
What access method are you going to use?	☐ Local keyboard, mouse, and monitor ☐ Remote access via SSH client or modem	
Server information	IP address _____ Host name _____	The host name cannot contain spaces or periods.
Avaya Enterprise Linux network configuration information	Subnet mask on Corporate LAN _____ Default gateway _____ Primary DNS Server _____	For more information about the Avaya-provided server installation, see <i>Implementing Avaya Aura® Experience Portal on multiple servers</i> .

Table continues...

Requirement/ Information Needed	Your value	Notes
	_____ DNS domain name _____ Time zone _____	
For customer-provided hardware, is Release 6.5 64 bit or later installed?	_____ Yes _____ No	If No, install Release 6.5 64 bit or later.
Is the default language for Linux set to English?	_____ Yes _____ No	If No, set the default language to English. You can change the default language after Experience Portal is installed.
Can all planned Experience Portal servers communicate with one another?	_____ Yes _____ No	For more information about verifying server communication, see <i>Implementing Avaya Aura® Experience Portal on multiple servers</i> on http://support.avaya.com .
For Avaya Enterprise Linux, user account passwords	cust account password: _____ root account password: _____	
For Red Hat Enterprise Linux Server, user accounts and passwords	root account password: _____ Non-root account name: _____ Non-root account password: _____	
Can you log in to the Experience Portal server with the non-root account name and password?	_____ Yes _____ No	The upgrade tool deletes all existing root accounts. Therefore, after the upgrade, the administrator uses the non-root account name and password to log in and: • Install a new Authentication File System (AFS) file. • Activate the Avaya service accounts.
Installation directory, if different from default	_____	Default directory: /opt/Avaya/ExperiencePortal Specify an absolute directory path containing only standard English

Table continues...

Requirement/ Information Needed	Your value	Notes
		alphanumeric characters and the symbols / (forward slash), _ (underscore), - (hyphen), ~ (tilde), or . (period).
EPM Web interface administration user name and password	User name: _____ Password: _____	The Experience Portal administrator uses this account to log in to the EPM Web interface to administer the Experience Portal system. The account is assigned the Administration user role as well as the Auditor and User Manager user roles. For details about User Roles, see <i>Administering Avaya Aura® Experience Portal</i> on http://support.avaya.com .
Do you want to create a database account that can access the report information in the database?	_____ Yes _____ No If Yes, account user name, if different from the default: _____ Password: _____	Default user name is: report This user account can only read those tables in the Experience Portal database that store report data. Speech application developers can use this account to log in to the database to create custom reports using any SQL-enabled report generation tool. * Note: The report user name cannot be the same as any of the EPM Web interface administration user account names or the report writer user account name.
Third-party SSL certificate information.	Third-party SSL certificate information. The location of the existing certificate: _____ The existing certificate's password: _____	
Will Avaya Services maintain this server?	_____ Yes _____ No If Yes, what is the Listed Directory Number (LDN) for this server? _____ Where is the Avaya Service Account authentication file located? _____	For more information on configuring Avaya service accounts, see <i>Implementing Avaya Aura® Experience Portal on multiple servers</i> .

Table continues...

Requirement/ Information Needed	Your value	Notes
WebLM information	License server URL, if not located on the EPM server: WebLM password: 	
The external time sources that the EPM server should be synchronize with, if desired	The name or IP address of primary time source: The name or IP address of secondary time source: 	

Auxiliary EPM server upgrade worksheet

Complete this worksheet if you are installing the EPM server on an Auxiliary Experience Portal server.

Requirement/ Information Needed	Your value	Notes
Ensure that the hardware meets the minimum requirements. For more information on minimum server machine hardware requirements, see <i>Avaya Aura® Experience Portal Overview and Specification</i> on http://support.avaya.com .		For minimum hardware requirements, see Minimum (Linux) server machine hardware requirements on page 40.
What access method are you going to use?	_____ Local keyboard, mouse, and monitor _____ Remote access via SSH client or modem	
Server information	IP address 	The host name cannot contain spaces or periods.

Table continues...

Requirement/ Information Needed	Your value	Notes
	Host name _____	
Avaya Enterprise Linux network configuration information	Subnet mask on Corporate LAN _____ Default gateway _____ Primary DNS Server _____ DNS domain name _____ Time zone _____	For more information about the Avaya-provided server installation, see <i>Implementing Avaya Aura® Experience Portal on multiple servers</i> .
For customer-provided hardware, is Release 6.5 64 bit or later installed?	_____ Yes _____ No	
Is the default language for Linux set to English?	_____ Yes _____ No	If No, set the default language to English. You can change the default language after Experience Portal is installed.
Can all planned Experience Portal servers communicate with one another?	_____ Yes _____ No	For more information about verifying server communication, see <i>Implementing Avaya Aura® Experience Portal on multiple servers</i> on http://support.avaya.com .
For Avaya Enterprise Linux, user account passwords	cust account password: _____ root account password: _____	
For Red Hat Enterprise Linux Server, user accounts and passwords	root account password: _____ Non-root account name: _____ Non-root account password: _____	
Can you log in to the Experience Portal server with the non-	_____ Yes _____ No	The upgrade tool deletes all existing root accounts. Therefore, after the upgrade, the administrator can use the non-root

Table continues...

Requirement/ Information Needed	Your value	Notes
root account name and password?		account name and password to log in and: • Install a new Authentication File System (AFS) file. • Activate the Avaya service accounts.
Installation directory, if different from default	_____	Default directory: /opt/Avaya/ExperiencePortal Specify an absolute directory path containing only standard English alphanumeric characters and the symbols / (forward slash), _ (underscore), - (hyphen), ~ (tilde), or . (period).
Auxiliary EPM database password	_____	For more information about the Primary EPM server installation worksheet, see <i>Implementing Avaya Aura® Experience Portal on multiple servers</i> .
Do you want to create a database account that can access the report information in the database?	_____ Yes _____ No If Yes, account user name, if different from the default: _____ Password: _____	Default user name is: report This user account can only read those tables in the Experience Portal database that store report data. Speech application developers can use this account to log in to the database to create custom reports using any SQL-enabled report generation tool.  Note: The report user name cannot be the same as any of the EPM Web interface administration user account names or the report writer user account name.
Do you want to create a report writer database account that allows external Experience Portal servers to write report data into the Experience Portal database on this server.	_____ Yes _____ No If Yes, account username: _____ If Yes, account password: _____	

Table continues...

Requirement/ Information Needed	Your value	Notes
Third-party SSL certificate information.	Third-party SSL certificate information. The location of the existing certificate: _____ The existing certificate's password: _____	
Will Avaya Services maintain this server?	_____ Yes _____ No If Yes, what is the Listed Directory Number (LDN) for this server? _____ Where is the Avaya Service Account authentication file located? _____	

MPP server upgrade worksheet

Complete the following worksheet for each planned Media Processing Platform (MPP) server on this Experience Portal system.

Requirement or information needed	Your value	Notes
Ensure that the hardware meets the minimum requirements. For more information on minimum server machine hardware requirements, see <i>Avaya Aura® Experience Portal Overview and Specification</i> on http://support.avaya.com .		For minimum hardware requirements, see Minimum (Linux) server machine hardware requirements on page 40.
What access method are you going to use?	_____ Local keyboard, mouse, and monitor _____ Remote access via SSH client or modem	

Table continues...

Requirement or information needed	Your value	Notes
Corporate LAN IP address	_____	
PBX LAN IP address, if different from the corporate LAN	_____	
Avaya Enterprise Linux network configuration information	Subnet mask on Corporate LAN _____ Subnet mask on PBX LAN, if different from Corporate LAN _____ Default gateway _____ Primary DNS Server _____ DNS domain name _____ Time zone _____	
For Avaya Enterprise Linux, user account passwords	cust account password: _____ root account password: _____	
For Red Hat Enterprise Linux Server, user accounts and passwords	root account password: _____ Non-root account name: _____ Non-root account password: _____	
Is the default language for Linux set to English?	_____ Yes _____ No	If No, set the default language to English. You can change the default language after Experience Portal is installed.
Maximum simultaneous calls	_____	The maximum number of calls that this MPP can handle at any one time. It is equivalent to the maximum number of ports that Experience Portal will allocate to this MPP.

Table continues...

Requirement or information needed	Your value	Notes
		For assistance in sizing your MPP server capacity and setting the correct value for the Maximum Simultaneous Calls parameter for each MPP server, contact your Avaya Services representative or Avaya Business Partner.
Installation directory, if different from default	_____	
Third-party SSL certificate information.	Third-party SSL certificate information. The location of the existing certificate: _____ The existing certificate's password: _____	
Will Avaya Services maintain this server?	_____ Yes _____ No If Yes, what is the Listed Directory Number (LDN) for this server? _____	

Single EPM server upgrade worksheet

Complete this worksheet if you are installing the EPM server on a dedicated Avaya Aura® Experience Portal server.

Requirement/Information Needed	Your value	Notes
Ensure that the hardware meets the minimum requirements. For more information on minimum server machine hardware requirements, see <i>Avaya Aura® Experience Portal Overview and Specification</i> on http://support.avaya.com .		For minimum hardware requirements, see Minimum (Linux) server machine hardware requirements on page 40.

Table continues...

Requirement/ Information Needed	Your value	Notes
What access method are you going to use?	☐ Local keyboard, mouse, and monitor ☐ Remote access via SSH client or modem	
PBX LAN IP address, if different from the corporate LAN	_____	
Server information	IP address _____ Host name _____	The host name cannot contain spaces or periods.
Avaya Enterprise Linux network configuration information	Subnet mask on Corporate LAN _____ Default gateway _____ Primary DNS Server _____ DNS domain name _____ Time zone _____	For more information about the Avaya-provided server installation, see <i>Implementing Avaya Aura® Experience Portal on multiple servers</i> .
For customer-provided hardware, is Release 6.5 64 bit or later installed?	☐ Yes ☐ No	If No, install Release 6.5 64 bit or later.
Is the default language for Linux set to English?	☐ Yes ☐ No	If No, set the default language to English. You can change the default language after Experience Portal is installed.
Maximum simultaneous calls	_____	The maximum number of calls that this MPP can handle at any one time. It is equivalent to the maximum number of ports that Experience Portal will allocate to this MPP. For assistance in sizing your MPP server capacity and setting the correct value for the Maximum Simultaneous Calls parameter for each MPP server, contact

Table continues...

Requirement/ Information Needed	Your value	Notes
		your Avaya Services representative or Avaya Business Partner.
Can all planned Experience Portal servers communicate with one another?	☐ Yes ☐ No	For more information about verifying server communication, see <i>Implementing Avaya Aura® Experience Portal on multiple servers</i> on http://support.avaya.com .
For Avaya Enterprise Linux, user account passwords	cust account password: _____ root account password: _____	
For Red Hat Enterprise Linux Server, user accounts and passwords	root account password: _____ Non-root account name: _____ Non-root account password: _____	
Can you log in to the Experience Portal server with the non-root account name and password?	☐ Yes ☐ No	The upgrade tool deletes all existing root accounts. Therefore, after the upgrade, the administrator uses the non-root account name and password to log in and: • Install a new Authentication File System (AFS) file. • Activate the Avaya service accounts.
Installation directory, if different from default	_____	Default directory: /opt/Avaya/ExperiencePortal Specify an absolute directory path containing only standard English alphanumeric characters and the symbols / (forward slash), _ (underscore), - (hyphen), ~ (tilde), or . (period).
EPM Web interface administration user name and password	User name: _____ Password: _____	The Experience Portal administrator uses this account to log in to the EPM Web interface to administer the Experience Portal system. The account is assigned the Administration user role as well as the Auditor and User Manager user roles. For details about User Roles, see <i>Administering Avaya Aura® Experience Portal</i> on http://support.avaya.com .

Table continues...

Requirement/ Information Needed	Your value	Notes
Do you want to create a database account that can access the report information in the database?	_____ Yes _____ No If Yes, account user name, if different from the default: _____ Password: _____	Default user name is: report This user account can only read those tables in the Experience Portal database that store report data. Speech application developers can use this account to log in to the database to create custom reports using any SQL-enabled report generation tool.  Note: The report user name cannot be the same as any of the EPM Web interface administration user account names or the report writer user account name.
Third-party SSL certificate information.	Third-party SSL certificate information. The location of the existing certificate: _____ The existing certificate's password: _____	
Will Avaya Services maintain this server?	_____ Yes _____ No If Yes, what is the Listed Directory Number (LDN) for this server? _____ Where is the Avaya Service Account authentication file located? _____	For more information on configuring Avaya service accounts, see <i>Implementing Avaya Aura® Experience Portal on multiple servers</i>.
WebLM information	License server URL, if not located on the EPM server: _____ WebLM password: _____	
The external time sources that the EPM server should be synchronize with, if desired	The name or IP address of primary time source: _____ The name or IP address of secondary time source: _____	

Index

A

Application Interface	111
Application Interface test client	111
applications	
testing	110
ASR servers	
testing	110
audience	7
Avaya Aura Experience Portal	
configuring	108
hardware requirements	40
installing license file	109
installing on multiple servers	78
license requirements	42
synchronize all of the servers	139
upgrade log files	121
upgrading on multiple servers	77
Avaya Aura Experience Portal servers	
verifying and setting time	49
verifying communication	45
Avaya Enterprise Linux	
configuring for Chinese input	117
configuring for Japanese input	118
configuring for Korean input	119
recovering configuration information	139
restoring 4.0.x	140
restoring previous version	140
upgrade overview	11
upgrading	
Auxiliary VPMS overview	11
Avaya Enterprise Linux	22, 25
EPM overview	11
Avaya Services	
access changes	109
AxisFault exception	130
Axis installation error	130

C

Chinese, configuring on Avaya Enterprise Linux	117
communication between servers	
verifying	45
configuring Avaya Aura Experience Portal	108

D

database	
external	139

E

email	
upgrade	47
email processor	47
Enterprise Linux Installer	
preparing to install	21
environment variables, reloading	139
EPM	
configuring for non-English input	117
synchronizing time with MPPs	49
synchronizing with external time source	115
upgrade finishes with an Axis error	130
upgrade log files	121
upgrading Red Hat Linux on	29
worksheet for auxiliary	150
worksheet for primary	147
worksheet for single server	155
etc/hosts file	
verifying	45
external database	139
verifying before upgrade	50
external time source	
setting for EPM	115

F

Fixing Prerequisite Checker failures	123
Fixing Prerequisite Installer failures	124
sample messages	126

H

hardware requirements	40
hung or stale mount points, checking for	49

I

Identifying RPM issues	127
import key error during MPP install	132
install	
JDBC driver	44
process hangs	131
installation	
testing	110
worksheets	
Auxiliary EPM server	150
MPP server	153
primary EPM server	147
single EPM server	155
installation progress bar stops at 25% completed	128
installing	

error messages (*continued*)

Avaya Aura Experience Portal on multiple servers	78
error messages	
no summary information found	128
unknown HostException localhost	123
import key error	132
installation hangs	128
license file	109
intended audience	7
Invalid Password	134
iptables Tomcat service	132

J

Japanese, configuring on Avaya Enterprise Linux	118
JDBC driver, install	44

K

Korean, configuring on Avaya Enterprise Linux	119
---	---------------------

L

legal notices	
License compatibility matrix	42
license file, installing	109
license requirements	42
localhost exception error	123
logs	
upgrade	121
loss of reporting data	
preventing	37

M

mount point	
checking status	49
MPP could not import EPM key	132
MPPs	
checking	
time synchronization with EPM	49
import key error during install	132
reconnecting after upgrade	77 , 103
testing after initial installation	113
troubleshooting	
time synchronization	134
upgrade hangs	131
upgrade log files	121
upgrading	77
upgrading Red Hat Linux on	31
worksheet for	153
MPP upgrade	
upgrade overview	12
MPP upgrade is hanging	131

N

notices, legal	
NTP	
external time source	115
synchronizing time with	134

O

Oracle	
JDBC driver	44
OS version number, verifying	43
outcall test application	112
overview	10
Avaya Aura Experience Portal configuration	108
single server	12

P

Password	
Invalid password	134
preparing	
Avaya Enterprise Linux Installer	21
Prerequisite Checker fails with UnknownHostException:	
localhost	123
Product ID	
changing	133

R

Red Hat Enterprise Linux	
check version number	43
identifying RPM issues	127
overview	
Auxiliary VPMS overview	15
MPP upgrade	16
Single server upgrade	17
VPMS overview	13
restoring 4.1 or 5.0 MPP server	144
restoring 5.1 or 6.0 Auxiliary server	145
upgrade overview	13 , 15–17
upgrading	
Red Hat Linux on EPM	29
Red Hat Linux on MPP	31
Red Hat Linux on single server	33
upgrading EPM	29
upgrading MPP	31
upgrading single server	33
related documents	7
reloading environment variables	139
requirements	
hardware	40
license	42
ResetProductID script	133
restoring	
4.0.x Avaya Enterprise Linux	140

restoring (<i>continued</i>)	
4.0.x Red Hat MPP server	144
5.1 or 6.0 software with Avaya Enterprise Linux	140
6.0 Red Hat MPP server	145
root certificate	123
RPMs	
identifying issues	127
running Application Interface test client	112
S	
space requirement	
upgrading primary EPM on Avaya Enterprise Linux	41
upgrading primary EPM on RHEL	41
speech servers	
testing	110
stale or hung mount points, checking for	49
status of	
mount points	49
summary information, not found after install	128
support	9
T	
testing	
Avaya Aura Experience Portal configuration	110
time, synchronizing between servers	49
timestamps, not synchronized	134
time synchronization	139
Time synchronization problems	134
Tomcat	
iptables service	132
troubleshooting	
hashing algorithm warning	123
incorrect timestamps	134
TTS servers	
testing	110
U	
unknown host exception error	123
upgrade	47
software prerequisites	38
verifying external database	50
Upgrade	7
upgrade overview	10
upgrading	
Avaya Aura Experience Portal on multiple servers	77
EPM	
upgrade options	52 , 93
EPM options	52 , 93
error messages	
AxisFault exception	130
no summary information found	128
log files	121
MPP install hangs	131

MPPs	
upgrade options	75
MPP silently	78
MPP software	77
options	75
reconnecting MPP	103
reconnecting MPPs	77
restoring 4.0.x Avaya Enterprise Linux	140
restoring 4.1 or 5.0 Red Hat MPP server	144
restoring 5.1 or 6.0 software	140
restoring 5.1 Red Hat MPP server	145
stopping mpp service	37
taking MPP offline with 4.x	36
upgrading Auxiliary	
EPM	
Auxiliary upgrade options	66
EPM options	66
upgrading primary EMP on RHEL	41
upgrading primary EPM on Avaya Enterprise Linux	41
V	
verifying	
communication between Avaya Aura Experience Portal	
servers	45
OS version number	43
stale or hung mount points	49
time between Avaya Aura Experience Portal servers ..	49
videos	8
W	
WebLM server	
installing license file for	109
worksheets	
auxiliary EPM server install	150
MPP server	153
primary EPM server install	147
single EPM server install	155
software upgrade prerequisites	38