Installing AvayaLive™ Engage: On-Premise Solution

Release 3.0
Issue 1
September 2012

Notice

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

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

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

Warranty

Avaya provides a limited warranty on its Hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support Web site: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

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

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Software” means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. “Hardware” means the standard hardware originally sold by Avaya and ultimately utilized by End User.

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.

CPU License (CP). End User may install and use each copy of the Software on a number of Servers up to the number indicated by Avaya provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

Copyright

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

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Product (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

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 Web site: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support Web site: http://support.avaya.com.

Contact Avaya Support

Self-service support is available at http://www.avayalive.com.

To create a support request, go to the Avaya Support Web site: http://www.avaya.com/support

Contents

Chapter 1: Introduction to AvayaLive™ Engage

Overview

AvayaLive™ Engage provides a cutting-edge, business-collaboration tool that combines the 3D virtual worlds with state-of-the-art spatial voice interaction. While AvayaLive™ Engage has traditionally been available on the Internet at http://www.avayalive.com, it is also available for installation on the network and premises of a partner or customer as AvayaLive™ Engage On-Premise Solution (OPS). This document deals with the installation of OPS. AvayaLive™ Engage OPS provides a solution for customers to run an AvayaLive™ Engage server system in the customer premises. You can install AvayaLive™ Engage for large-scale deployments or long-term deployments with the assistance of the IT department of your organization. OPS is the native installation of the AvayaLive™ Engage software onto one or two servers. You can install a server for AvayaLive™ Engage and a server for Big Blue Button (BBB) on separate machines or install BBB as a virtual server on the AvayaLive™ Engage server.

AvayaLive™ Engage uses the BBB server for desktop sharing and other collaborative services.

Purpose of the document

This document deals with the installation and configuration of the AvayaLive™ Engage server. This document does not deal with client installation, either from the Internet or through central distribution for desktops that do not have administrative access or Internet access.

Intended audience

The audience of this document are the following:

- the personnel installing AvayaLive™ Engage
- the IT staff supporting the installation

Limitations

AvayaLive™ Engage OPS has the following limitations:

- Avaya has designed and configured this solution for 100 peak concurrent users. While modification of this limit is not a problem, Avaya does not have any engineering information about how the system behaves above this level. For more information about increasing users, contact an Avaya support representative.
- This solution can be used with a central user base through the Windows domain. For this, the AvayaLive™ Engage server must be added to the Windows domain. If the server must be placed in Demilitarized Zone (DMZ) for Internet access, the domain must also be in DMZ.
- The administrator, or installer must log into the servers directly to configure features other than the features on the AvayaLive™ Engage administration panel.

Chapter 2: Requirements

Software

The AvayaLive™ Engage OPS software comprises the following files:

- The *Installing AvayaLive™ Engage : On-Premise Solution* guide
- AvayaLive_Engage_OPS_<version>.zip

  This file contains the installers and artifacts that you require to set up AvayaLive™ Engage on the configured machine.
- BBB_<version>.zip

  This is a virtual machine (VM) image of a Big Blue Button server running on 32 bit Linux based Ubuntu Server. As this file is about 1.5 GB, plan how to download and save the file. AvayaLive™ Engage uses the Big Blue Button for desktop sharing and other collaboration services. You can also install BBB using native installation, in which case you do not need this file.

Deployments

You can install AvayaLive™ Engage in one of the following deployment styles:

- On two physical machines: One machine for AvayaLive™ Engage and one machine for Big Blue Button.
- On two virtual machines: In this case, the IT department of your organization provides the virtual machines including operating systems, disks, networking, and other equipment. This installation is similar to the installation on the physical machines.
- On one physical machine: In this case, AvayaLive™ Engage runs natively on the physical machine and BBB runs as a virtual machine with the physical machine functioning as the host.

Hardware

Related topics:

[Two machine deployment for AvayaLive Engage](#) on page 12
[Two machine deployment for Big Blue Button](#) on page 13
[Single machine deployment](#) on page 13

Two machine deployment for AvayaLive™ Engage

The IT department of your organization must provide the two machines, either physical or virtual. The AvayaLive™ Engage machine must meet the following requirements for the two machine deployment:

Component	Physical or virtual machine
Processor	Two 64 bit cores and 2.33 GHz **Note:** This is a minimum requirement and unchanged since AvayaLive™ Engage 2.5. With the inclusion of video services in AvayaLive™ Engage 3.0, use a quad core.
Hard drive • Operating system partition • AvayaLive™ Engage Data Store Partition	• 20 GB • 10 GB **Note:** If you expect extensive use of video services in AvayaLive™ Engage 3.0, you would require a larger AvayaLive™ Engage Data Store Partition as per your requirement.
Memory	2 GB
Network	One NIC

Two machine deployment for Big Blue Button

If you are deploying AvayaLive™ Engage on two machines, the BBB machine must meet the following requirements:

Component	Physical or virtual machine
Processor	One core
Hard drive	20 GB
Memory	1 GB
Network	One NIC

Note:

The BBB web page, www.bigbluebutton.org, does not provide minimum specifications for their product. Avaya has estimated this information based on the experience of working with BBB in the cloud.

Single machine deployment

If you deploy the BBB server as a virtual machine on the AvayaLive™ Engage server as a single machine deployment, ensure that the AvayaLive™ Engage server meets the following requirements:

Component	Physical or virtual machine
Processor	One 64 bit and Quad Core and 2.33 GHz **Note:** • 64 bit refers to the processor architecture, and not the operating system. • This processor must support Virtualization Extensions, such as Intel VTx or AMD-V. The processor must be enabled in the BIOS.
Hard drive • Operating system partition • AvayaLive™ Engage Data Store Partition	250 GB (two partitions) • 40 GB free • 10 GB

Component	Physical or virtual machine
	Note: If you use video services in AvayaLive™ Engage 3.0 extensively, you require a larger AvayaLive™ Engage Data Store Partition according to the requirement.
Memory	6 GB
Network	One NIC

Operating system

The machines provided by the IT department of your organization must have the operating systems already installed. If you deploy the virtualization of BBB, Avaya provides an image with an installed operating system. You must have full administrative access to both the operating systems, including the ability to create local users and set properties for those users. The machines must be installed with virus scanning software. Your IT department is responsible for updating this software.

As the solution includes two machines, the two sets of operating system requirements are as follows:

- AvayaLive™ Engage server: Windows 2008 Standard Edition R2 (64 bit).

  Note:

  The requirement for R2 is mandatory. AvayaLive™ Engage does not support R1, either Service Pack 1 or Service Pack 2. Alternatively, you can use Enterprise Edition or Data Center Edition. However, Avaya tests the AvayaLive™ Engage software on Windows 2008 Standard Edition.

- BBB server: Ubuntu server (Linux) 10.04 (32 bit or 64 bit)

  Note:

  BBB also has 64-bit support in version 7 but Avaya has not tested this version.

Licensing

The IT department is responsible for licensing the Windows operating system. The license must include any Customer Access License (CALs). You must buy one CAL from Microsoft for each Peak Concurrent User (PCU) in your AvayaLive™ Engage license. As the maximum

number of regular users is 100 and the maximum number of administrator users is five, the maximum number of CALs is 105.

The Ubuntu operating system is free under the open-source license.

Networking

The machines that the IT department of your organization provides must be fully configured for networking. Each machine must have an IP address and Fully Qualified Domain Name (FQDN) before you start working with the machine.

Every server in AvayaLive™ Engage needs FQDN as AvayaLive™ Engage clients are not referenced only by the host name. You can identify FQDNs as the dot separated names that represent computers, such as `google.com`. FQDNs promote the portability of computers as the IP address can be changed without changing the name. Domain Name Service (DNS) manages the translation from FQDN to the IP address.

Sometimes, you might require a machine to have two FQDNs: the default FQDN, usually based on a host name, and a public alias. For example, a machine could be called `HT6756s.internal.mycompany.com` but you would prefer the machine being referred to as `webalive.mycompany.com`. As an example, the AvayaLive™ Engage servers in the Amazon cloud have two FQDNs because the FQDNs that Amazon provides are not user friendly. In a deployment with alias FQDNs, the IT department of your organization must perform some configuration tasks before installing AvayaLive™ Engage.

AvayaLive™ Engage 3.0 does not support Internet Protocol version 6 (IPv6). You must disable IPv6 on any AvayaLive™ Engageserver or BBB server.

Partitions

AvayaLive™ Engage uses a two-partition model. The operating system and installed software use the first drive, the C drive. The AvayaLive™ Engage server uses the second drive, the `W` drive for data. This model facilitates easier installation, backup, restore, and upgrade. The IT department of your organization must handle the creation of the partitions.

If you have a physical machine, you can split an existing partition using the tools in Windows 2008:

1. Click the quick start icon of the **Server Manager Tool** next to the **Start** menu.
2. On the tree on the left, click **Server Manager** > **Storage** > **Disk Management**.
3. In the graphical view of the disk, right-click and select **Shrink Volume**.

4. Shrink the volume by the desired amount.
5. Use the freed space to create a new partition.

If you have a virtual machine, the IT department of your organization must provide both virtual drives. The drive must meet the following rules:

- You must label the drive as *web.alive Data Store*. The later scripts in the installation recognize the disk by label. You can change the script name from any Internet Explorer window.
- You must assign the drive the `W` drive letter or you must ensure that the `W` drive letter is free. The installation scripts reassign this drive later.
- The drive must be empty.

Skills

As this installation procedure is fairly complex, the installation engineer must have the following skills:

- Familiarity with the Windows operating systems, specifically Windows 2008 R2
- Familiarity with Linux
- Familiarity with the with Internet Information Services (IIS) 7.0 Web Server and the associated concepts
- Basic editing skills on Windows and Linux.
- Basic file transfer skills on Windows and Linux
- Experience with this procedure. Training in a controlled lab environment is an asset.
- Experience with PowerShell scripts as this installation uses PowerShell. A knowledge of how to run PowerShell is an asset.

Tip:

Ensure that an engineer from the IT department of your organization also reads this documentation in advance.

Chapter 3: Installing Big Blue Button from an image

Big Blue Button image

Big Blue Button (BBB) provides collaborative Web-based services that AvayaLive™ Engage uses. AvayaLive™ Engage uses BBB for desktop sharing and other services.

You can deploy BBB in two ways: as a virtual machine from the provided image, or as a native installation on a provided machine.

This chapter describes how to deploy BBB from an image. The next chapter describes how to deploy BBB as a native install.

While the installation of BBB is technically a prerequisite for AvayaLive™ Engage, you can perform the BBB installation steps in parallel with the installation of IIS and AvayaLive™ Engage. Alternatively, you can install BBB later if you are willing to reconfigure a running AvayaLive™ Engage server after BBB is available. It is only at the end of the AvayaLive™ Engage installation that you have to point the AvayaLive™ Engage server at the BBB server.

If you install BBB as a virtual machine (VM), where the AvayaLive™ Engage server functions as the VM host, you can create a full AvayaLive™ Engage system on one physical machine. Use this option instead of using two physical machines.

BBB runs on the VM assigned to the BBB server. The image is in the `BBB_<version>.zip` file, and is created for VMware Player. You must first install Player on the physical AvayaLive™ Engage server.

Bridging

In virtual deployment, the physical machine and the network on which the machine resides must support bridging. Bridging is a virtualization technique whereby a single NIC card handles multiple MAC addresses and multiple IP addresses. A single NIC card can function as an NIC card for the host and for each virtual machine (VM) running on that host. The VMs and the host share the same NIC card. Avaya preconfigures each BBB image with bridging enabled.

Bridging is the only way that VMs can function as servers. If you cannot provide bridging, you cannot deploy BBB successfully. You might not be able to provide bridging for the following reasons:

- The host operating system might be configured to prevent bridging.
- The NIC card might not support bridging as the card is too old.
- The network policies of the IT department within your organization might prevent bridging. Such blocking might occur in sensitive deployments such as government or military installations. If bridging is blocked, you must run the host in a region of the network that supports virtualized servers.
- Wireless connectivity might prevent bridging. If you are connected wirelessly, you might be unable to provide bridging as many though not all wireless networks do not support bridging.

Starting VMware

VMware is a virtualization software. You require this software to control and manage the BBB installation. To install BBB, start the BBB virtual machine and update the default password in the BBB console.

At this point, you require the AvayaLive™ Engage image, which you can obtain from Avaya or from yourAvaya business partner.

Before you begin

Obtain the AvayaLive™ Engage image from your Avaya customer service representative or business partner.

About this task

The purpose of this task is to start the VMware and update the default password.

Procedure

1. Unzip the BBB image zip file.

   The image consists of a root directory and files in that directory, but not subdirectories.

2. Start the VMware Player.
3. Click **Open a Virtual Machine** and navigate to the directory into which you unzipped the BBB image zip file.

   The directory contains a single `.vmx` file.

4. Select the `.vmx` file and open.

   The Player displays the VM specifications with the **Powered Off** state. The left side of the Player dialog box displays and retains the location of the VM.

5. Click **Play Virtual Machine**.
   The BBB console and the operating system starts. This process might take several minutes.
6. Log in to the BBB console with the following credentials:
   - User name: `firstuser`
   - Password: `Default1`

   Note:

   The password is temporary. You will be prompted to change the password.

   You are now logged in and the system displays the command prompt.

Next steps

Now, you must enable networking for this configuration.

Activating your network

For the AvayaLive™ Engage solution to operate effectively, you must enable networking. When the BBB virtual machine first starts, networking is disabled. The process of enabling networking in deployments with Dynamic Host Configuration Protocol (DHCP) is not the same as the process of enabling networking in deployments that use a static IP address. You must know whether your deployment uses DHCP or static IP addresses.

If your deployment uses a static IP, Avaya provides a script to guide you through the process but you must be proficient with VI editor to complete the task.

Before you begin

- Before you activate the network, you must start the BBB virtual machine.
- For a deployment using static IP, obtain the IP address, Netmask and Gateway from the IT department of your organization.

About this task

The purpose of this task is to enable networking in your configuration with DHCP.

Procedure

1. At the command prompt in the BBB VM console, enter the following:
   ```
   ifconfig
   ```
   This command displays all the networking interfaces. But, the command must display only an interface called `lo`, which is the loopback address. This is the loopback address. None of the other interfaces are active.

2. To activate networking:

   If your deployment uses DHCP:

   a. Enter the following command replacing the variables with the host name and FQDN of the server. Avaya initializes the BBB hostname with the phrase `nohostname` for Linux images.

      ```
      ./.setup_dhcp.sh <hostname> <FQDN>
      ```

      If your deployment has automatic DNS enrollment, use a command similar to the following:

      ```
      ./.setup_dhcp.sh myhost123 myhost123.mycompany.com
      ```

      If your deployment does not use automatic DNS enrollment, use a command similar to the following:

      ```
      ./.setup_dhcp.sh myhost123 bbbhost1.mycompany.com
      ```

   b. At the resulting command prompt, enter your password.
   c. Press **Enter** to start powering down the VM.
   d. Restart the server.
      The VM shuts down.
   e. Use Player to start the VM again.
   f. Relog in and use `ifconfig` to check that networking is enabled.

      You should see the `eth0` interface, and the `lo` interface. The IP address is at the `inet addr` field.

      Note:

      The`ifconfig` command might not show the IP address for the following reasons:

      - Restart the hyperviser. Quit the guest OS, and restart Player. If the `ifconfig` command does not show the IP address, restart the host.
      - DHCP is not available in this network.
      - Bridging is not allowed or supported in this network.

   If your deployment uses a static IP:

   a. Enter the following command replacing the variables with the host name and FQDN of the server:

      ```
      ./.setup_static.sh <hostname> <FQDN>
      ```

   b. At the resulting command prompt, enter your password.
      The script opens a file, in which you must enter the following information:

      - IP address
      - Netmask
      - Gateway

Note:

You can edit this file again later, using this command:

```
sudo vi /etc/network/interfaces
```

c. Save the file.
The script opens a second file.

d. Enter the following information:

- IP address of the primary and secondary DNS servers
- The domain name that these DNS servers represent. You have to enter this information twice.

Important:

The domain names in this file must end with a period (.).

e. Save and close the file.

3. Press Enter to shut down the virtual machine.
4. Use Player to restart the BBB virtual machine and verify that networking is activated by entering the following command:

```
ifconfig
```

Next steps

Now, you must activate the BBB application.

Activating BBB

After you set up networking, you must activate the Big Blue Button (BBB) application.

Before you begin

Before you activate BBB, ensure that you enable networking in your deployment.

About this task

The purpose of this task is to activate the BBB application.

Procedure

1. At the command prompt in the BBB console, enter the following:

```
bbb-conf --setip <FQDN>
```

2. At the resulting command prompt, enter your password.
The BBB application begins the configuration and restarts several services.

3. Ensure that BBB is accessible by the AvayaLive™ Engage clients. To ensure accessibility, you must edit the following file:
   ```
   sudo vi /etc/nginx/sites-enabled/bigbluebutton
   ```
4. Change line 3, the server_name line, of this file, from:
   ```
   server_name <FQDN>;
   ```
   to
   ```
   server_name <ip> alias <FQDN> 127.0.0.1;
   ```
5. Restart the Web server by entering the following command:
   ```
   sudo /etc/init.d/nginx restart
   ```

Example

The following shows an example of a modified file (top part):

```
server {      listen 80;      server_name 135.9.172.219 alias gsslab-
bbb2.avayalive.com 127.0.0.1;     access_log /var/log/nginx/
bigbluebutton.access.log;         # Handle RTMPT (RTMP Tunneling). Forwards
requests         # to Red5 on port 8088.       location ~ (/open/|/close/|/idle/|/
send/) {      …
```

Next steps

Verify that the BBB application is operating successfully.

Verifying BBB

You can verify that the BBB application is up and running by *pinging* the machine from another physical machine.

Before you begin

Before you verify that BBB is running, you must activate BBB.

About this task

The purpose of this task is to validate the BBB application before you proceed with the AvayaLive™ Engage installation.

Procedure

1. In the Command Prompt dialog box, enter the following commands to verify the networking. Replace the variables with information that applies to your deployment.
   ```
   ping <ipaddress>
   ping <bbb FQDN>
   ```

2. In the browser window, verify the BBB URL by entering the following in the **Address** field.

```
http://<BBB FQDN>/
http://<BBB ipaddress>
```

   The browser must display a **Welcome** screen.

Scheduling an automatic restart

Note:

This is an optional task.

If you run the BBB application through VMware Player, the application does not automatically restart each time you restart the host machine. This is a concern because AvayaLive™ Engage benefits from periodic restarts. You can ensure periodic restarts through many ways. Create a scheduled task in the Windows operating system. This method is described in the following sections.

If you run a server automatically, run the server without a console interface, that is, GUI. Without a GUI, BBB can run automatically on the restart of the host machine, and you do not need to log in to the BBB machine. To run BBB without a GUI, you require an additional application, called Vix, that works with VMware Player. Vix is a command line tool that operates with most VMware products.

To schedule an automatic restart of the BBB application, you must perform several short tasks. You must install and configure Vix, might have to add a mapping to Vix, and schedule the restart task in Windows.

Related topics:

Configuring Vix on page 23
Troubleshooting Vix on page 24
Scheduling the task on page 25

Configuring Vix

VMware produces the Vix application, which is free.

Before you begin

Before you configure Vix, you must unzip the BBB image zip file and remember the location of the unzipped directory.

About this task

The purpose of this task is to set up Vix to operate with BBB.

Procedure

1. Open an Internet browser and enter http://www.vmware.com/support/developer/vix-api/ in the **Address** field. Download and install Vix.
2. Open a DOS Command prompt, and enter the following command:

   ```
   vmrun –T player start <path to .vmx file> nogui
   ```

   The .vmx file for BBB is located in the directory to which you unzipped the BBB image zip file. The following is an example of this command:

   ```
   "C:\Program Files (x86)\VMware\VMware VIX\vmrun.exe" -T player start "C:
   \Users\Smith\Documents\Virtual Machines\BBB_Native70\BBB_Native70.vmx"
   nogui
   ```

   The `nogui` option ensures that VMware runs without a user interface. Do not use the `nogui` option until you verify that the BBB server is accessible through the SSH client, using which you can connect from other machines through a terminal window. Omit the `nogui` option until you have verified that the BBB server is accessible through an SSH client that allows you to connect from other machines, giving you a terminal window.
3. To verify that the BBB server is running, perform the steps described in Verifying BBB on page 22. Or, check the **Processes** tab of Task Manager in the host machine and check the list for the `vmware-vmx.exe` process.

   Note:

   Ensure that you do not run two instances of the BBB virtual machines.

Next steps

You might have to add a mapping to Vix if you have a new version of VMware Player.

Troubleshooting Vix

Vix operates by mapping your instance of VMware Player to a special communication library. If this mapping is missing, you may see the following error:

```
Unable to connect to host.
Error: The specified version was not found
```

Before you begin

Before you address any issues with Vix, ensure that you have downloaded the latest version of Vix.

About this task

The purpose of this task is to add a mapping to a Vix file to ensure that the mapping can connect to the BBB server.

Procedure

1. From the Vix installation directory, open the `vixwrapper-config.txt` file.
2. Add a line, such as:

   ```
   player   9  vmdb  3.1.1 Workstation-7.0.0
   ```

   The Vix installation directory contains subdirectories of communication libraries. The field `Workstation-7.0.0` is the directory of the communication libraries in the Vix installation directory. The field `3.1.1` is the version of VMware Player. Check different communication libraries to identify the library which operates with the version of VMware Player.

   Tip:

   For more information about the directories, search the VMware forums or enter the error message or, `vixwrapper-config.txt`, in a www.google.com search.
3. Save the file and close it.

Next steps

Now, you can create the scheduled task in Windows.

Scheduling the task

You must create a scheduled task that restarts BBB when the host machine restarts.

Before you begin

Before you schedule the restart task, ensure that the command line accessibility operates successfully.

About this task

The purpose of this task is to create a scheduled task to ensure that the BBB server restarts each time the host machine restarts.

Procedure

1. On the host machine, navigate to **Start** > **Administrative Tools** > **Task Scheduler**.
2. From the **Actions** menu, select **Create Task...** to display the task wizard.

3. In the **General** tab, enter a name for the task.
4. Set the user.
   Ensure that the user has admin elevation privileges, and set **Run** with the highest privileges. Alternatively, run the task as the **System** user.
5. Set **Run whether user is logged in or not**.
6. In the **Triggers** tab, click **New** and begin the task **At startup**.
7. Set task delay for five minutes.
8. Click **OK**.
9. In the **Actions** tab, click **New** and the action, **Start a program**.
10. In the **Program/Script** field, run the `vmrun.exe` file.
11. In the **Add Arguments** field, enter:
    ```
    -T player start “<.vmx file>” nogui
    ```
12. Click **OK**.
13. In the **Settings** tab, ensure that only the **Allow task to be run on demand** is enabled. Ensure that this option is enabled.
14. Click **OK** to complete the task.
    Windows displays the task in the **Task Scheduler Library** on the left of the screen. You can right-click it to display a menu.
15. From the right-click menu, select **Run** to verify that the script runs successfully.
    If the script runs successfully, vmrun must run for a short period of time and display the **Last Run Result** as `0x0`.

    There are many other failure codes, such as `0xFFFFFFFF`. This code suggests that the task does not have enough privileges.
16. Reboot the host, wait seven minutes, and verify that the BBB server is also rebooted.

Chapter 4: Installing Big Blue Button natively

A native installation of BBB

Big Blue Button (BBB) provides collaborative Web-based services that AvayaLive™ Engage uses. AvayaLive™ Engage uses BBB for desktop sharing and other services.

You can deploy BBB in two ways — either as a virtual machine from the provided image or as a native install on a provided machine.

While the installation of BBB is technically a prerequisite for AvayaLive™ Engage, you can perform the BBB installation steps in parallel with the installation of IIS and AvayaLive™ Engage. Alternatively, you can install BBB later if you are willing to reconfigure a running AvayaLive™ Engage server after BBB is available. It is only at the end of the AvayaLive™ Engage installation that you have to point the AvayaLive™ Engage server at the BBB server.

This chapter deals with deploying BBB as a native install.

Native installation is an installation of BBB as an application onto an existing machine. The machine can be physical if sufficient disk space is available, or can be virtual.

The following are the advantages of a native installation on a virtual machine:

- You can use a hypervisor or virtual machine monitor of your choice and need not use VMware only.
- The installation of AvayaLive™ Engage can also be virtual

The following are the disadvantages of a native installation on a virtual or physical machine:

- The installation is complex.
- You require direct Internet access. BBB is an open-source product that you can install from public repositories. You cannot perform a native installation using a proxy server.

Installing Ubuntu

Ubuntu is a Linux operating system.

Before you begin

- For native installation, you must have a machine with Ubuntu server of 10.04, 32, or 64-bit. Before you begin the native installation, you must install the Ubuntu server and ensure that the server is networked and fully functioning. Avaya does not support Ubuntu 9.04 or any version of Ubuntu desktop for the AvayaLive™ Engage native installation.
- The Ubuntu community creates and posts videos describing the process of installation into a new Virtual Machine on YouTube. The links to some videos are as follows:
  - http://www.youtube.com/watch?v=_kSpWCku86M
  - http://www.youtube.com/watch?v=Lwc2RCnGF0Q

About this task

The following procedure describes the deviations from the procedures shown on YouTube:

Procedure

1. Open an Internet browser and enter http://releases.ubuntu.com/lucid/ in the **Address** field.
2. Download and install Ubuntu.
3. Include the following in the virtual hardware configuration:

Component	Specification
Processor	1
Memory	1 GB
Single Hard Drive	20 GB
Network Adapter	Bridged

4. Call the initial user `firstuser`. This user has sudo rights.
5. At the end of the installation, do not install LAMP as shown in the video as LAMP installs Apache. Installing Apache interferes with the Web server that BBB uses, nginx.
6. Install OpenSSL.

   OpenSSL provides remote access to the machine from any free SSL client.

Note:

The procedure for installing Ubuntu on a physical machine and a virtual machine is similar:

- Start the installation with the ISO file and create a CD with the software. To create a CD, you require a software package, such as Infra Recorder. Alternatively, you could save the ISO file to a flash drive, such as Universal USB Installer. For more information, see http://www.ubuntu.com/business/get-ubuntu/download.

- Use BIOS of the physical machine to boot the computer from the CD and continue with the steps that you perform for installing the virtual machine.

Next steps

Ensure that the Ubuntu server communicates with other machines in your network.

Activating the Ubuntu network

For the AvayaLive™ Engage solution to operate effectively, your deployment requires networking. When you install the Ubuntu operating system, Ubuntu supports DHCP networking by default. If your deployment uses DHCP networking, you do not need to make any configuration changes. You can skip this task and proceed to the installation of BBB. However, if the deployment uses static IP addresses, you must make some configuration changes and update the following two files:

- `/etc/network/interfaces`
- `/etc/resolv.conf`

Before you begin

You must obtain the IP configuration information, such as IP address, netmask, and gateway, from the IT department of your organization.

You can gain access to the configuration files in several ways. You can use an SSH client, for example, Putty, that provides you with a terminal window. You can download Putty from http://www.chiark.greenend.org.uk/ ~sgtatham/putty/ download.html.

You can edit the files using an application called vi. vi is a family of screen-oriented text editors that share certain characteristics, such as methods of invocation from the operating system command interpreter and characteristic user interface features.

About this task

The purpose of this task is to enable the Ubuntu operating system to support static IP addresses. You can skip this task if your deployment uses DHCP networking.

Procedure

1. Open the `/etc/network/interfaces` file.

   For example, enter the following command in a terminal window:

   ```
   sudo vi /etc/network/interfaces
   ```

2. Replace:

   ```
   iface eth0 inet dhcp
   ```

   with:

   ```
   iface eth0 inet static
   address XXX.XX.XXX.XX
   ```

```
netmask XXX.XX.XXX.XX
gateway XXX.XX.XXX.XX
```

Replace `XXX.XX.XXX.XX` with the appropriate information from your deployment. For more information about the format and purpose of this file, browse the Internet.

3. Open the `/etc/resolv.conf` file.

   For example, enter the following command in a terminal window:

   ```
   sudo vi /etc/resolv.conf
   ```

4. Replace:

   ```
   search myisp.com.
   ```

   with:

   ```
   domain myisp.com.
   nameserver XXX.XX.XXX.XX
   nameserver XXX.XX.XXX.XX
   nameserver XXX.XX.XXX.XX
   ```

   Replace `XXX.XX.XXX.XX` with the appropriate information from your deployment. There is abundant information on the Web about the format and purpose of this file. The Web is the best reference.

5. Reboot the server and verify that networking operates effectively.

Next steps

Now, you can install the BBB application.

Proxy support

Avaya intends to offer proxy support for the native BBB installation. Currently, the BBB native installation requires direct access to the Internet. If you install BBB natively using a proxy server, the installation fails.

The Ubuntu operating system uses a proxy URL that takes the following form:

```
http://[[user][:pass]@]host[:port]/
```

The following is an example of a proxy that does not require authentication:

```
http://my.proxy.server:8000/
```

The following is an example of a proxy that requires authentication:

```
http://asmith:ASmith1@my.proxy.server:8000/
```

When you install the Ubuntu operating system, the installer requests for this information. You must enter it and complete the installation of the Ubuntu operating system. When Ubuntu is running, you must log in and configure this information globally in the following file:

```
/etc/environment
```

You can gain access to the configuration files in several ways. You can use an SSH client, for example, Putty, that provides you with a terminal window. You can download Putty from http://www.chiark.greenend.org.uk/ ~sgtatham/putty/ download.html.

You can edit the files using an application called vi. vi is a family of screen-oriented text editors that share certain characteristics, such as methods of invocation from the operating system command interpreter and characteristic user interface features.

For example, enter the following command in a terminal window:

```
sudo vi /etc/environment
```

Add the following two lines to this file:

```
http_proxy="<proxy URL>"
ftp_proxy="<proxy URL>"
```

Save and close the file and then reboot the BBB server.

During native installation, you must perform this configuration task after the installation of Ubuntu and before the installation of BBB.

Note:

The proxy information is included here for completeness only. Avaya does not currently support this configuration.

Installing BBB

After you have installed the Ubuntu operating system and enabled networking, you can install the BBB application.

For more information on troubleshooting and to read explanatory notes, go to http://bigbluebutton.googlecode.com/svn-history/r4679/wiki/InstallationUbuntu.wiki.

Before you begin

Before you install BBB, install the Ubuntu operating system.

About this task

The purpose of this task is to install the BBB application.

Procedure

1. In a terminal window, enter

```
> wget http://archive.bigbluebutton.org/bigbluebutton.asc
> sudo apt-key add bigbluebutton.asc
```

   These commands add the package key for the BBB application.

   If you do not have Internet access, the `wget` command fails.

   The `apt-key` command might require a password.

2. Enter

```
> echo "deb http://archive.bigbluebutton.org/lucid bigbluebutton-lucid
main" | sudo tee /etc/apt/sources.list.d/bigbluebutton.list
```

   This command adds the software archive for BBB version .70 for Ubuntu 10.04. This is the version that AvayaLive™ Engage supports. AvayaLive™ Engage does not support later versions.

3. Enter

```
> echo "deb http://us.archive.ubuntu.com/ubuntu/ lucid multiverse" | sudo
tee -a /etc/apt/sources.list
```

   This command adds the main Ubuntu software archive for Ubuntu 10.04.

4. Enter

```
> sudo apt-get update
```

   This command updates anything that needs to be updated before you start the installation. Usually this command runs very quickly.

5. Enter

```
> sudo apt-get install asterisk
```

   This command installs Asterisk which is a prerequisite for BBB. Asterisk is an open-source telephony product. This command takes time to run because approximately 50 Linux packages are downloaded and installed. After you enter this command, the installer prompts you to confirm the package list and installation. Enter `Y`.

   During the installation, the installer prompts you for the ITU-T Telephone Code for your location. The code for Canada and the US is `1`. For a full list of codes, go tohttp://en.wikipedia.org/wiki/List_of_country_calling_codes.

6. Enter

```
> sudo apt-get install bigbluebutton
```

   This command installs BBB. This process takes time to run because approximately 175 Linux packages are downloaded and installed. After you enter this command, the installer prompts you to confirm the package list and installation. Enter `Y`.

   During the installation, the installer prompts you to set and confirm the MySQL database password. Make a note of this information.

   During the installation, the BBB software prompts you to re-enter and reconfirm the MySQL database password.

If your Internet connection is slow, this task takes a longer time to complete.

7. Enter

```
> sudo bbb-conf --restart
> sudo bbb-conf --check
```

These commands restart BBB.

Next steps

Perform two final tasks to configure the BBB application. Customers who install BBB from an image also perform these two tasks. The two tasks are:

- Activating BBB on page 21
- Verifying BBB on page 22

Chapter 5: Setting up IIS and APS.NET

Installing IIS and ASP.NET

To operate successfully in the deployment, AvayaLive™ Engage requires Internet Information Services (IIS) and ASP.NET.

- IIS is a Web server application and set of feature extension modules that Microsoft has created.
- ASP.NET is a Web application framework that Microsoft has developed and marketed.

Ensure that AvayaLive™ Engage can use port 443.

In Windows 2008, IIS is known as a role and ASP.NET is known as a feature.

The following topics deal with installing IIS and ASP.NET. This chapter also deals with the port 443 used for AvayaLive™ Engage.

Installing IIS

AvayaLive™ Engage uses IIS, the Web server. IIS is not installed by default with the Windows 2008 installation. IIS provides a reliable, manageable, and scalable Web application infrastructure.

About this task

The purpose of this task is to install IIS that AvayaLive™ Engage requires.

Procedure

1. At the bottom left of the screen, click the toolbox icon.
   The system displays the Server Manager application.
2. Click the **Roles** node in the **Server Manager** tree on the left of the screen.
3. Click **Add Roles** in the menu panel on the right of the screen.
   The system displays the Add Roles Wizard.
4. In the **Select Server Roles** dialog box, select **Web Server (IIS)**, and click **Next**.
   The application displays many options for this role.

5. Select the following options that are used for the AvayaLive™ Engage IIS installation:.

   Web Server

   • Common HTTP Features including all child options

      - Static Content
      - Default Document
      - Directory Browsing
      - HTTP Errors
      - HTTP Redirection
      - WebDAV Publishing

   • Application Development (include all child options)

      - ASP.NET
      - NET Extensibility
      - ASP
      - CGI
      - ISAPI Extensions
      - ISAPI Filters
      - Server Side Includes

   • Health and Diagnostics

      - HTTP Logging
      - Request Monitor

   • Security (include all child options)

      - Basic Authentication
      - Windows Authentication
      - Digest Authentication
      - Client Certificate Mapping Authentication
      - IIS Client Certificate Mapping Authentication
      - URL Authorization
      - Request Filtering
      - IP and Domain Restrictions

   • Performance

      - Static Content Compression

- Management Tools
  - IIS Management Console
  - IIS Management Scripts and Tools
  - IIS 6 Management Compatibility
    - IIS 6 Metabase Compatibility
    - IIS 6 WMI Compatibility
    - IIS 6 Scripting Tools

6. Complete the wizard to install IIS.

Next steps

Now, you must install ASP.NET.

Installing the ASP.NET framework

Several server components in AvayaLive™ Engage require the ASP.NET version 3.5 framework.

Before you begin

Before you perform this task, you must install IIS.

About this task

The purpose of this task is to install a supporting framework that AvayaLive™ Engage requires.

Procedure

1. At the bottom left of the screen, click the toolbox icon to display the Server Manager application.
2. Click the **Features** node in the **Server Manager** tree on the left of the screen.
3. Click **Add Features** in the menu panel on the right of the screen.
   The system displays the Add Features Wizard.
4. In the **Select Features** dialog box, select **.NET Framework 3.5.1 Features** and click **Next**.
   This option has many prerequisites.
5. Accept all prerequisites and complete the wizard to install ASP.NET.

Next steps

Now, you must ensure that AvayaLive™ Engage can use port 443.

Using port 443

Servers commonly use port 443 for Hypertext Transfer Protocol (HTTP) communications over Secure Socket Layer (SSL) (HTTPS).

AvayaLive™ Engage server uses port 443 for two purposes:

- For non-SSL servers, AvayaLive™ Engage uses port 443 for tunnelling so that client applications can traverse firewalls to reach servers.
- For SSL servers, AvayaLive™ Engage uses port 443 for SSL and for tunnelling.

AsAvayaLive™ Engage uses port 443, IIS cannot use the same port.

- If you install IIS directly from the operating system, as described in Installing IIS on page 35, the default installation does not use port 443.
- If you install IIS from a corporate or government image, IIS is often preconfigured to use port 443. In this situation, you must make a correction to change the port allocation.

About this task

Use the following procedure to change the port allocation for IIS:

Procedure

1. Click **Start** > **Administrative Tools** > **IIS Manager**.
2. In the **Connections** pane, expand the **Sites** node.
3. Click **Default Web Sites**.
4. In the **Actions** pane, click **Bindings**.
   The system displays the **Site Bindings** dialog box.
5. Remove or edit all the site bindings that are allocated to port 443.
6. Double click SSL Settings in the central pane.
7. Clear the **Require SSL** check box to turn off SSL on the Web server.
8. Restart IIS by clicking the host name in the left pane and **Restart** in the right pane.

Chapter 6: Installing AvayaLive™ Engage

Preparing to install AvayaLive™ Engage

All the files that you require to install AvayaLive™ Engage are in a `AvayaLive_Engage_OPS_<version>.zip` file. This file contains installers and artifacts needed to install AvayaLive™ Engage.

Before you begin

- Create a directory on the desktop and unzip the `AvayaLive_Engage_OPS_<version>.zip` file.
- You must also install IIS and ASP.Net.

About this task

The purpose of this task is to prepare your machine to install AvayaLive™ Engage.

Procedure

1. Create the following directory on your machine: `C:\Scripts`.
2. Copy the following files into the `C:\Scripts` directory:
   - `Setup.ps1`
   - `Remove.ps1`
   - `Default.wae`
3. Copy `C:\Windows\System32\drivers\etc\hosts` to `C:\Scripts\wahosts.template`.
4. Install Java Runtime Environment (JRE) 1.6, which is also called version 6.

   Note:

   The required Java installers are found in the zipped file bundle, namely:

   - `jre-6u31-windows-i586.exe`
   - `jre-6u31-windows-x64.exe`

   Install 32-bit and 64-bit versions of Java.

About the AvayaLive™ Engage set-up script

The **Setup.ps1** file is a Windows PowerShell script. Use this file to prepare the machine to perform the following tasks:

- Define FQDN for the machine.
- Augment the hosts file with the FQDN mapping and the Hostname mapping. However, in some cases, if the FQDN of a machine does not map directly to the machine in DNS, override the host file.
- Move the data store disk to the `W` drive. The drive must be labelled `web.alive Data Store`.
- Create all required directories, move files, and set permission wherever required.
- Create local users and groups needed for AvayaLive™ Engage.
- Create all the required application pools in IIS.
- Create all the additional Web sites in IIS.
- Create all the required Web applications in IIS.
- Create all the required Virtual Directories in IIS.
- Set all upload limits in IIS.
- Add all AvayaLive™ Engage MIME Types to IIS.
- Add all AvayaLive™ Engage firewall rules.
- Set defaults for the Server Configuration Tool.

Running the set-up script

The set-up script called **Setup.ps1**, runs within an application called Windows PowerShell. Windows PowerShell is a Microsoft task automation framework, consisting of a command-line shell. When you start Windows PowerShell, it displays a DOS-like window.

Click the Windows PowerShell quick-start icon at the bottom left of the desktop to start Windows PowerShell.

Note:

You can also start Windows PowerShell by clicking the `C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe` file. If you are not running this file as Administrator but have administrator access, then right-click the icon or file and select **Run as Administrator**

Before you begin

- Before you run the AvayaLive™ Engage set-up script, you must prepare your machine for the installation of AvayaLive™ Engage as described in Preparing to install AvayaLive Engage on page 39.
- If you do not use the Administrator account but have administrator access, ensure that the PowerShell windows are running as administrators. If the title of your PowerShell window is not titled Administrator then type `powershell` into the search area of the **Start** menu. Right-click on the result and click **Run as Administrator** to execute Powershell at the correct elevation. The same applies to any individual installer you want to run.

About this task

Use the following procedure to run the AvayaLive™ Engage set-up script:

Procedure

1. Start Windows Powershell.
2. Enter the following commands:

   ```
   cd C:\Scripts
   Get-ExecutionPolicy
   ```

   The current execution policy is displayed as `Restricted`.

   ```
   Set-ExecutionPolicy RemoteSigned
   ```

   The system prompts you to confirm.

   ```
   .\Setup.ps1
   ```

   Note:

   The execution policy for PowerShell may have been set by your system administrator. In that case, return to the original setting as output from the `Get-ExecutionPolicy` command after the installation is complete.

   If you cannot set an execution policy of `RemoteSigned`, retry the step replacing `RemoteSigned` with `AllSigned`.

   Windows Powershell prompts you for the FQDN of the AvayaLive™ Engage server. The dialog box displays the host name because the host name might be related to FQDN.

3. Enter FQDN and click **OK**.
   Windows PowerShell runs the script.

   Note:

   - During upgrades, the dialog box shows FQDN that existed in the old system. This FQDN cannot be changed on upgrade.
   - For security reasons, the Windows PowerShell scripts are securely signed. The script may not run until you confirm that your computer trusts the

signature of the signer, such as Verisign. You must confirm by pressing Y on your keyboard.

If the script still does not run , right-click the file, click **Properties**, and click **Unblock** at the bottom of the **General** tab.

Related topics:

[About passwords](#) on page 42
[Troubleshooting the Setup.ps1 script](#) on page 42
[About application pools and security](#) on page 43

About passwords

The `Setup.ps1` script sets up local accounts for AvayaLive™ Engage. Provide passwords for the local accounts if:

- `Setup.ps1` has detected that the required account is not present and must be created.
- `Setup.ps1` has detected that the IIS application pool is missing and the account associated with the application pool needs a password reset.

Ensure that the password complies with the password policy of your system. If you cancel the **password** dialog box, the script stops from running further. If you have the `waadmin` account, remember the password for later use.

Troubleshooting the Setup.ps1 script

You can run `Setup.ps1` again and again. In the unlikely event that your first attempt to run the file fails, try some of the steps listed here in order to fix the issue.

The common reasons for the script to fail are as follows:

- For security reasons, the Windows PowerShell scripts are securely signed. The script may not run until you confirm that your computer trusts the signature of the signer, such as Verisign. You can confirm by pressing Y on your keyboard. If the script still does not run, right-click the file, select **Properties**, and click **Unblock** at the bottom of the **General** tab.
- The preconditions to run the script are not met.

  Ensure that you have created the `C:\Scripts` directory and that this directory contains `Default.wae` and `wahosts.template`. Install IIS and ASP.NET.
- Permissions on an operation fail in the script.

Ensure that you have full administrative access to the machine. Full administrative access includes permission to create local users and set properties for those users. Obtain all permissions and run the script again.

- The Web server is too slow to satisfy requests of the script.

  This often happens for Application Pool operations. Wait for 10 seconds and rerun the script.

- The operating system might fail a request from Windows Powershell.

  Wait for 10 seconds and rerun the script.

- If you have done a restore earlier, this script might fail to update file and directory permissions due to ownership issues. This script failure takes place with directories `W:\web.alive\avatarBadgePictures` and `W:\web.alive\WAImageService`. To rectify this issue, do the following:

  - Open **Properties** of the file or directory involved. Select the **Security** tab of the file, or the directory.
  - Open **Advanced** and select the **Owner** tab.
  - Open **Edit** and select the administration account you are using to install with.
  - Click **Apply** and then click **OK** to accept all the open dialog boxes.
  - Repeat the above steps with all the other files or directories, or rerun `Setup.ps1`

About application pools and security

Application pools

One of the tasks of `Setup.ps1` is to create and configure all the IIS application pools that are required for AvayaLive™ Engage. Application pools provide the process framework for Web applications to run inside IIS. The following are two application pools with high security requirements:

- WAWebServiceAppPool: This pool contains the WAWebService application. WAWebServiceAppPool runs as a LocalSystem user so that it can manipulate the AvayaLive™ Engage processes and services. WAWebServiceAppPool runs on port 8080. As port 8080 is closed on the firewall, WAWebServiceAppPool is not available remotely.
- WAAdminPanelAppPool: This pool contains the Admin Panel application which is used to perform many administrative operations on the AvayaLive™ Engage server. WAAdminPanelAppPool runs as a LocalSystem user so that the Admin Panel can create local users, delete local users, back up, restore, and gain access to certain files. The Admin Panel provide remote access but contains application level authentication and can only be run by administrators.

Security

Sometimes, a security scanning software identifies WAWebServiceAppPool and WAAdminPanelAppPool as application pools that do not conform to the security requirements.

These application pools cannot be run as different identities without impacting their functionality. Both contain application level security to prevent misuse.

Running the installer

You can run `RunInstallers.ps1` repeatedly. You can reinstall most installers on top of a partial install. In some cases, you might have to uninstall a component before rerunning `RunInstallers.ps1`. All the installers run in sequence and no user input is required, except for the first installer. For the list of installers, see The RunInstallers.ps1 script on page 88

Diamondware is the first installer that the set-up script runs. Diamondware provides the spatial voice engine that AvayaLive™ Engage uses. While running the installer, specify the number of concurrent users. You can set this limit only at the time of installation.

About this task

The purpose of this task is to run the `RunInstallers.ps1` script.

Procedure

1. Open a new PowerShell window.
2. Run `.\RunInstallers.ps1`.

   You may have to right-click on the icon or file and select **Run as Administrator**.

   When the installation is complete, the installer prompts you for the number of voice channels that you require.

   ```
   Enter number of maximum users[250]:
   ```

3. Do not accept the default value of `250`. Instead, enter `116`.

   This value is calculated using the following metrics:

   ```
   100 regular users + 5 admin users + 10 telephone calls + 1 AvayaLive™
   Engage server (the control channel)
   ```

   You can set this limit only at installation by entering the maximum number of users who might use the server. You might also set a higher limit for an expansion in the future. However, remember that voice channels use a lot of memory in the DiamondWare servers and excess capacity is wasteful.

4. Press any key to continue.
   Then `.\RunInstallers.ps1` installer runs the remaining 11 installers. No user input is required.

Related topics:

Configuring AvayaLive Engage on page 45

Configuring AvayaLive™ Engage

After `RunInstallers.ps1` is complete, the script detects if requirements to install AvayaLive™ Engage are met. The script then automatically starts the Server Configuration Tool.

Note:

The Server Configuration Tool is also available as a shortcut on your desktop when running the `RunInstallers.ps1` script is complete.

Before you begin

- Before you configure AvayaLive™ Engage, you must complete the AvayaLive™ Engage installation.
- Install the BBB server at this point. However, you can also add the BBB server later, if required.

About this task

All the fields have default values for this installation. Use the following procedure to update the default settings to match the requirements of your network.

Procedure

1. Enter the fully qualified domain name of the Big Blue Button server in the **BBB Server FQDN** field.

   Note:

   If you do not have a BBB server, you might use the one at appshare.avayalive.com but the option is risky as users might share desktops on the internet. If your organization has blocked desktop sharing, open ports. After you enter FQDN, click another field to register the change with the tool.

2. Update the **Image Service Base URL** field, and change the FQDN part of the URL to point to the original server.

   Note:

   If this is not the first server set up for your organization, direct this server to use Image Service of the first server. Image Services for badges are shared among related servers. The Image Service is installed on all machines, but use only one machine.

3. Scroll down and enter the relevant mail server configuration data in the five SMTP fields to allow AvayaLive™ Engage to gain access to a mail server.

4. Click **Configure Server**.
   AvayaLive™ Engage applies these values to your server quickly.

5. Click **Configure Subscription**. AvayaLive™ Engage applies these values to your account. This step can take several moments.

Tip:

Ensure that you do not click **Configure Subscription** without first clicking **Configure Server**.

Related topics:

Troubleshooting subscription configuration on page 46

Troubleshooting subscription configuration

The subscription configuration might fail in some situations due to the following reasons:

- TheAvayaLive™ Engage server process, called `webalive.exe` or `webaliveService-1` is *pending*. This happens when the Windows Services Manager starts AvayaLive™ Engage prematurely. To fix this issue, open the Task Manager and end the `webalive.exe` process. Click **Configure Subscription** again.
- The IIS fails to process a valid request. In the failure log, this form of error might be recorded as Directory exception. Wait a few moments and try again.
- The application pools created by `Setup.ps1` used the .NET 4.0 setting instead of the .NET 2.0 setting. Make sure the .NET setting is .NET 2.0 using IIS Configuration Manager.

URLs

You need the following URLs to use the system:

- To open the client application, use http://<engage FQDN>/1/html/index.html.
- To open the server, use http://<engage FQDN>/WAAdminPanel/.

Only people with this special administrator access can use the AvayaLive™ Engage administration panel. The `Setup.ps1` script creates the initial user to gain access to the administration panel. The initial user has the following credentials:

- User: `waadmin`
- Password: `<password you provided>`

Environments

In AvayaLive™ Engage, the environment is the location where meetings take place. A typical environment has rooms and open spaces. You can navigate through the environment to attend meetings. In the environment, you can interact with other people or move items, such as furniture. You can share information in several ways, for example, by projecting presentations on to a screen in some environments. You can also deposit documents in drop boxes for other people. You can communicate with other people by speaking directly, writing text messages, or using the telephone to contact people who are not currently in the meeting.

The 3D world that exists in an AvayaLive™ Engage server is called a Web Alive Environment or WAE, pronounced as way. These environments have the `.wae` file extension . In your AvayaLive™ Engage installation, the OPS bundle includes an initial `.wae` file called `Default.wae`. After installation, you can change this environment by contacting the Avaya Support Representative. Alternatively, customers with accounts on the AvayaLive™ Engage store can obtain environments from http:/avayalive.com/WaStore/Environments. For more information about updating environments, see *Administering AvayaLive™ Engage: On-Premise Solution*, at http://support.avaya.com.

The OPS customers might want to develop `.wae` files in 3D environment content development. The customers can develop a new environment, or modify one of the public environment if the license permits such modifications. If a server administrator has a new `.wae` file, you can load the file on the server easily. Using the administration panel, click **Upload Environment**.

Chapter 7: Removing and upgrading AvayaLive™ Engage

Uninstalling AvayaLive™ Engage

Before you begin

Before you uninstall AvayaLive™ Engage, create a back up of the configuration.

About this task

The purpose of this task is to remove AvayaLive™ Engage from the server.

Procedure

1. Click **Start** > **Control Panel** > **Programs And Features**, and remove the following applications in the following order:
   a. AvayaLive™ Engage Media Applications
   b. AvayaLive™ Engage Statistics Service
   c. AvayaLive™ Engage server <version>
   d. AvayaLive™ Engage DW Voice Services

   You may have to change the settings on the Control Panel before you can see the **Programs And Features** option.
2. Start Powershell, navigate to `C:\Scripts`, and run this file: **Remove.ps1**.
   The system displays two options: **Upgrade**, and **Remove**.
3. Select the option related to the task you want the script to perform, and click **OK**.

   Note:

   With some exceptions, the `Remove.ps1` script removes all the configurations and installations that the `Setup.ps1` script performs. The `Remove.ps1` script performs the following:

   - Uninstalls all the ASP.NET applications
   - Uninstalls all the AvayaLive™ Engage Web pages
   - Uninstalls all the AvayaLive™ Engage client loads on the server
   - Removes all the Web server configurations that were done by **Configure Subscription**

Note:

The `Remove.ps1` script removes the Web server configurations only if you select the **Remove** option when running the `Remove.ps1` script. The `Remove.ps1` scrip does not remove the Web server configurations if you select **Upgrade**.

After running the `Remove.ps1` script, the following installations and configurations are present on the server:

- The Web server (operation system role)
- ASP.NET (operating system feature)
- Java
- All local users and groups created using the administration panel. This includes `waadmin` and `wauploader` that are present in the `W` drive. These configurations cannot be removed.
- Everything on the `W` drive
- If you perform an Upgrade task, most of the AvayaLive™ Engage data in the registry, file system, and Web server are left intact.

RemovingAvayaLive™ Engage completely

About this task

Use the following procedure to completely remove AvayaLive™ Engage from a machine so that you can perform a new installation of the application or if you plan to use the machine for something else:

Procedure

1. Run the `Remove.ps1` script from `C:\Scripts`.
2. Click **Remove**.
3. Delete the `W` drive.

   Once the `W` drive is deleted, you cannot recover the drive.
4. Click the toolkit icon next to the **Start** menu to run the Server Manager application.
5. Click **Configuration** > **Local Users and Groups** > **Users**.
6. Delete accounts `waadmin` and `wauploader`.

Note:

The uninstaller can remove the infrastructure components, such as Java, ASP.NET Framework 3.5.1 Feature, and Web Server (IIS) Role.

Upgrading web.alive 2.5 to AvayaLive™ Engage 3.0

Before you begin

Tip:

Back up of the `W` drive.

About this task

Use the following procedure to upgrade the AvayaLive™ Engage server version 2.5 to 3.0.

Procedure

1. Copy `nocache_web.config` from the bundle into `W:\web.alive\1\Web\html`.
2. Rename the file as `web.config`.

   Wait for 24 hours for the caches to clear as several AvayaLive™ Engage version 2.5 Web resources are cached increasing the upgrade time.
3. Copy `Remove.ps1` from the bundle to `C:\Scripts`.

   Note:

   You must use the remove script for version 3.0 to remove version 2.5.
4. Run the `Remove.ps1` script.

   Note:

   Run the `Remove.ps1` script instead of the `RemoveCPDE.ps1` script.
5. Click the **Upgrade** option.
6. Uninstall Java as AvayaLive™ Engage version 2.5 was installed with only 64-bit Java. To do this, click **Start** > **Control Panel** > **Programs And Features**.
7. Install Java that is provided with the 3.0 bundle. Install 32-bit and 64-bit Java.
8. To install AvayaLive™ Engage 3.0, perform the following:

   a. Copy `Setup.ps1` and `Default.wae` from the bundle into `C:\Scripts`

b. Run `Setup.ps1`.

Note:

During upgrades, the previous server FQDN is already provided and cannot be changed, so the field is disabled. To change the FQDN, you must first run the `Remove.ps1` script with the **Remove** option.

c. Run `RunInstallers.ps1`.

Note:

During the upgrade, the values in Server Configuration Tool do not change.

d. Configure **Server** and **Subscription** in the Server Configuration Tool.

Result

After the upgrade, the server runs the existing 2.5 `.wae` file.

Next steps

To gain access to the newer AvayaLive™ Engage version 3.0 features like live video wall and room triggers, you need to upload the 3.0 `.wae` file using the administration panel.

Upgrading AvayaLive™ Engage 3.0 to 3.0

Before you begin

Tip:

Back up the `W:` drive.

About this task

You can upgrade the AvayaLive™ Engage server version 3.0 to a later version of 3.0. For example, you can upgrade from the 3.0 Beta version to the 3.0 GA version. To perform this, use the following procedure:

Procedure

1. Uninstall AvayaLive™ Engage.
2. Run the `Remove.ps1` script.
3. Click the **Upgrade** option.
4. Copy `Setup.ps1`, `Remove.ps1`, and `Default.wae` from the bundle into `C:\Scripts`.
5. Run the `Setup.ps1` script.

Note:

During upgrades, the previous server FQDN is already provided and cannot be changed, so the field is disabled. In order to change the FQDN, you must first run the `Remove.ps1` script with the **Remove** option.

6. Run the `RunInstallers.ps1` script.

Note:

During the upgrade, the values in the Server Configuration Tool remain the same.

7. Configure **Server** and **Subscription** in Server Configuration Tool.

Chapter 8: Managing users

User base

AvayaLive™ Engage requires a user base to support authenticated access by clients. AvayaLive™ Engage works on three types of user bases:

- Local user base
- Central user base via a Windows domain
- Web authentication

Local user base

By default, AvayaLive™ Engage is configured to operate with a local user base. This means that the system uses users and groups on the local server machine as the user base for the clients of that server.

This administrator administers the user base using the **User Admin** tab on the Admin Panel. The administrator can also create users and give permissions to the users.

The Admin Panel deals only with local users. All functions that the Admin Panel provides to users work only with Local Users.

Using a local user base has the following advantages:

- You can only log in to the Admin Panel with a local user. The system creates the `waadmin` default user during installation.
- Only local users can log in using their email addresses. Enter the email address when you create a user in the Admin Panel.
- The Login dialog box displays a **Forget Password?** link. This link is an Admin Panel function and works only for local users.
- The Admin Panel displays a **Change Password** link. This link works only for local users.
- The Admin Panel provides authenticated access to statistics. This feature works only for local users.

Using a local user base has the following disadvantages:

- A user ID on one server is not shared with multiple servers.
- The local user ID does not match the user ID that the user typically uses in an Enterprise system.
- The administrator must back up the local users and groups as part of the server data.
- If a user can get direct access to a server machine, then the user can log in with the local user account. Hence, ensure that AvayaLive™ Engage servers are in locked server rooms with only RDP access as AvayaLive™ Engage users cannot access a server using RDP.

Central users

AvayaLive™ Engage also supports a central user base via the Windows domain. This configuration has several advantages over the local user base:

- Users can log in to multiple AvayaLive™ Engage servers using the same user ID.
- The user ID matches the domain user ID that the user is already using in the organization.
- You do not need to back up the user data as part of the server backup process.
- Access to AvayaLive™ Engage server is more secure.

However, this configuration also has several disadvantages:

- Users cannot log in using their email address.
- AvayaLive™ Engage administrators cannot manage this data using the AvayaLive™ Engage administration panel. To use the Admin Panel, use a local user account that is part of the local ServerAdmin account.
- AvayaLive™ Engage administrators cannot use the **Forgot Password** link, the **Change Password** link, and the authenticated access to Statistics on the AvayaLive™ Engage administration panel.
- Administrators must rely on the IT department of the organization for the configuration of a central user base.

Related topics:

Setting up central users on page 56
Domain groups on page 57

Setting up central users

To set up a centralized user base, you must add the AvayaLive™ Engage server to a Windows domain. Typically, the IT department of an organization performs this task. After the

AvayaLive™ Engage server is on the Windows domain, you must process the domain details of AvayaLive™ Engage.

Before you begin

Before you configure AvayaLive™ Engage to operate with a central user base, you must add the AvayaLive™ Engage server to a Windows domain.

Procedure

1. Open a Web browser and enter http://localhost:8080/WAWebService/WAInterface.asmx?op=WASetDefaultLoginDomains in the **Address** field.
   The system displays the **WAInterface Web Service** screen.
2. In the **subscriptionId** field, enter `1`.
3. In the **DefaultLoginDomains** field, enter the name of the domain.
4. Click **Invoke**.
   AvayaLive™ Engage restarts and displays the following XML response:
   - If the response is true, the configuration is successful and users can now log in using their domain credentials.
   - If the response is false, the configuration is unsuccessful and you must investigate the reasons.
5. If the response is false, navigate to `W:\web.alive\Logs` for the most recent `WAWebService_<datetime>.log`.
   The failure cause is at the bottom.

Domain groups

Users can have varying levels of access in the AvayaLive™ Engage environment. When you create a new user, you must allocate access levels to the user. You can also edit an existing user profile to change the access level. Some environments might not support all access levels. The access levels that are common to all environments are:

- Administrator User
- Laser Pointer User
- Statistics Viewer

The environment GUI recognizes these user groups using strings, which are used as local groups or domain groups. The following table displays the group name, the string name in the GUI, and the purpose of the group name.

Group	Displayed in the graphic user interface as	Purpose
Administrator User	ServerAdmin	This group is for server administrators. In the environment, this group provides access to all the administrative functions in the main background and avatar menus. This group also usually provides upload rights in general areas.
Auditorium Speaker	AuditoriumPresenter	This group provides access to restricted areas in large rooms and also upload rights in those areas. Users in this group also have laser-pointer rights in those areas.
Meeting Room Speaker	MeetingRoomPresenter	This group provides access to restricted areas in small rooms and also upload rights in those areas. Users in this group also have laser-pointer rights in those areas.
Statistics Viewer	StatisticsViewer	This group is provided for completeness. Since the Admin Panel provides authenticated access to statistics, the administrator can only add local users to this group to gain access to Statistics. The administrator cannot add Domain users to this group.
Laser Pointer User	WA_LASERPOINTER	This group provides its users with laser-pointer rights anywhere.

For more information on users and authentication, see *Administering AvayaLive™ Engage: On-Premise Solution* at http://support.avaya.com.

Web authentication

The most flexible method of connecting AvayaLive™ Engage to a user base is through web authentication. When you set up a connection through Web authentication, AvayaLive™ Engage clients can authenticate using Web cookies that might be already in the running browser. The actual authentication is through a web call. Since clients that authenticate in this manner do not use the AvayaLive™ Engage login dialog box, this method creates Single Sign On (SSO).

For more details on Web authentication, see *Administering AvayaLive™ Engage: On-Premise Solution* at http://support.avaya.com

Related topics:

Configuring web authentication on page 59

Configuring web authentication

Before you begin

To configure web authentication, you require the following:

- An enterprise authentication server

  Note:

  Avaya has tested this server using WebSEAL.

- A web application that integrates the AvayaLive™ Engage calls with the authentication server

About this task

To configure Web authentication using the administration panel.

Procedure

1. Log in to the administration panel, and select the **Advanced** tab.
2. Click on the *instructions* link to gain access to online help.
3. Click on the *help* link to know more about user bases.

Combined user base

The use of domain users and groups does not preclude the use of local users and groups at the same time. The administration panel still functions, as expected, to create local users and groups while a domain is in use. The same can be said for Web authentication. If Web authentication fails, or the required cookies are not present, the user can still log in using the domain user or local user.

Consequences of a demilitarized zone (DMZ)

In a typical deployment, you will require access to AvayaLive™ Engage for users within your organization and for users in the general public, that is, on the public Internet. To achieve this configuration, you have to place the AvayaLive™ Engage server in a demilitarized zone (DMZ).

If you require AvayaLive™ Engage to be publicly accessible and if you are using a central user base, you must extend the Windows domain into the DMZ, as the AvayaLive™ Engage server

needs to communicate with the domain controller. For successful configuration, you must open several ports on the firewall at the rear of the DMZ. Similarly, for web authentication, the AvayaLive™ Engage server in the DMZ must be able to make the authentication request across the back firewall to the enterprise authentication server. For more information, contact the IT department of your organization.

Chapter 9: Setting up the firewall

Firewall changes

To successfully deploy AvayaLive™ Engage in your network, you must make some changes to the firewall. Make the changes to the Windows 2008 firewall and the subnet or the intranet firewall, or both.

Related topics:

[AvayaLive Engage ports](#) on page 61
[Big Blue Button ports](#) on page 62

AvayaLive™ Engage ports

AvayaLive™ Engage uses the following ports:

Port	Protocol	Notes
80	TCP	Web traffic, file upload, file download
443	TCP	Tunnelling port and SSL port
1935	TCP	Media Server port
2379	UDP	Spatial voice port for voice channel
7878	UDP	Unreal interaction port for synchronization of data between the client and the server
21002	TCP	Spatial voice control port
3389	TCP	Remote desktop for management

Note:

- Use the `Setup.ps1` script to opens all of these ports, with the exception of 3389, on the Windows 2008 firewall. You do not need to modify the local firewall unless another process closes the ports at a later point in time. If your firewall has a larger scope, you might require to contact the IT department of your organization.
- Open Port 3389 for management of a remote desktop on the AvayaLive™ Engage server. You can run these services on different ports. It is possible to run these services

on different ports to gain an additional level of security so that both services are provided on lesser known ports.

Big Blue Button ports

The BBB server uses the following ports:

Port	Protocol	Notes
80	TCP	Web traffic
9123	TCP	Desktop sharing used by the desktop sharer
1935	TCP	Flash Media Server port used by desktop viewers
22	TCP	Secure Shell (SSH) used for management

Note:

- The Ubuntu images might not have a local firewall. If your firewall has a larger scope, you might require to contact the IT department in your organization.
- Open port 22 for SSH on the BBB server for management. It is possible to run these services on different ports to gain an additional level of security so that both services are provided on lesser known ports.

Tunnelling

AvayaLive™ Engage supports tunnelling to enable clients to contact servers through firewalls. If the client cannot contact the server on port 7878, then all traffic usually intended for 7878, 1935, 2379, and 21002 is tunnelled through port 443.

Note:

AvayaLive™ Engage supports tunnelling through port 443 for convenience, but avoid this tunnelling, if possible.

Tunnelling also redirects BBB traffic. All BBB traffic intended for ports 80, 1935, and 9123 is first routed to the AvayaLive™ Engage server on port 443. Then, the AvayaLive™ Engage server redirects the traffic to the BBB server on the BBB ports 80, 1935, and 9123. For redirection, ensure that the BBB server is visible to the AvayaLive™ Engage server on ports 80, 1935, and 9123.

Note:

- Set up servers to accept all ports, and let the client perform tunnelling for firewalls.
- Voice traffic is especially sensitive to the time lag that occurs in tunnels. The time lag gets worse if the tunnelling is done through proxies.

Remote desktop

You must open port 3389 to enable the remote desktop feature. You must also enable the Remote Desktop feature in the operating system.

Before you begin

Before you activate the remote desktop feature, you must install AvayaLive™ Engage.

About this task

Activate the Remote Desktop feature in your operating system.

Procedure

1. On the AvayaLive™ Engage server, navigate to **Start** > **Control Panel** > **System and Security** > **System** > **Remote**.
2. At the bottom of the dialog, enable remote desktop.
3. Click **OK**.

Note:

- You can secure the remote desktop feature by one or all of the following: the client version, the user identity, and the client address.
- Enabling the remote desktop in Windows automatically opens the port in the Windows firewall.

Secure shell (SSH)

All BBB servers must have SSH. The OpenSSH package is included in the AvayaLive™ Engage image when you install BBB. When you install BBB natively, refer to the instructions provided in Chapter 4 *Installing Big Blue Button* in this document and also install the OpenSSH package while installing the OS.

Chapter 10: Setting up secure sockets layer (SSL)

Secure sockets layer

Traffic between the client machine and the server machine, which also roughly maps to the ports that AvayaLive™ Engage uses, falls into the following four categories:

- 3D interaction traffic (UDP)
- Voice traffic (UPD with some TCP)
- HTTP traffic (TCP). This traffic includes all communications with Web servers.
- Media traffic (TCP). This traffic includes video, Web cameras, and application sharing.

With these traffic types, AvayaLive™ Engage: OPS supports the following modes, or levels of traffic security:

- No traffic encrypted. The default mode when you first install OPS.
- Only HTTP traffic encrypted using SSL and voice traffic encrypted using SRTP. The other traffic types remain unencrypted. This option is the default in AvayaLive™ Engage Hosted Solution deployment. The option is also the default when you upgrade the AvayaLive™ Engage 2.5 SSL-enabled server to version 3.0.
- All traffic encrypted via a shared SSL tunnel.

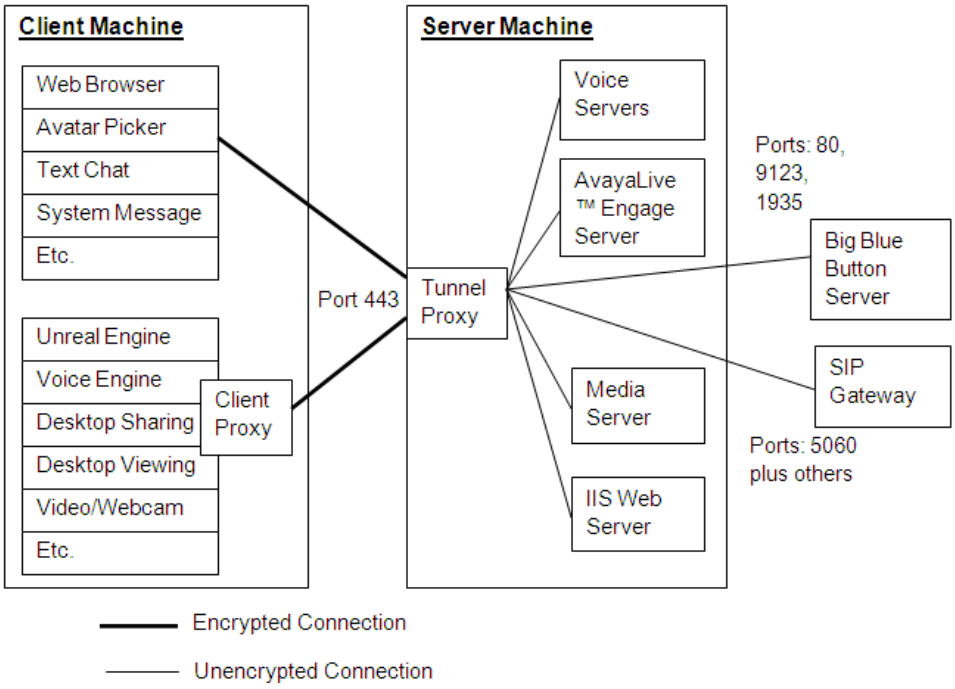
About WAWebService

When you install AvayaLive™ Engage, you install the WAWebService application. The WAWebService application provides a number of administrative functions for other AvayaLive™ Engage applications. The WAWebService application is not available for remote call, but the application can be used locally on the server machine. The WAWebService application provides the certificate management that AvayaLive™ Engage requires for the SSL solution.

Architecture

The AvayaLive™ Engage client consists of many components. Not all the components can communicate using SSL. The components that cannot communicate using SSL do not communicate with the AvayaLive™ Engage server. Such components communicate with a proxy called the client proxy that communicates directly with the AvayaLive™ Engage server on behalf of the components.

The AvayaLive™ Engage server also has a proxy, called the tunnel proxy, which runs as a Windows service in version 3.0. The tunnel proxy terminates the SSL connections from all sources and routes the communication packets to the appropriate server-side components of the AvayaLive™ Engage solution. The connections behind the AvayaLive™ Engage server are not encrypted. Enable only the AvayaLive™ Engage server for SSL.



Related topics:

Port 443 on page 66

Port 443

The AvayaLive™ Engage solution uses port 443 for secure communications in the form of HTTPS.

- For non-SSL servers, AvayaLive™ Engage uses port 443 for tunnelling so that clients can traverse firewalls to reach servers.
- For SSL servers, AvayaLive™ Engage uses port 443 for SSL and for tunnelling.

Since AvayaLive™ Engage is using port 443, this means that other servers, including the IIS Web server, cannot use port 443.

Managing your SSL certificate

The process of managing your SSL certificate consists of three tasks, which you must complete in sequence:

1. Using AvayaLive™ Engage, you must generate a request for an SSL certificate. This task is called a certificate signing request (CSR).
2. Using the CSR, you must engage with an SSL Certificate Authority (CA) vendor, such as Verisign, to buy a certificate.
3. Using AvayaLive™ Engage, you must install the certificate that you bought.

Additional actions, such as importing, exporting, and backing-up

You can import certificates into AvayaLive™ Engage that you have exported from other systems. However, a description of this process is beyond the scope of this document.

AvayaLive™ Engage does not currently support certificate export.

You must back up the `W:` drive as soon as you install the certificate. You cannot replace certificates that are lost due to failure. In the event of a failure, you must purchase a new certificate.

Related topics:

Generating a certificate signing request on page 67
Buying a certificate on page 69
Deleting a certificate signing request on page 69
Installing the certificate on page 70
Intermediate CA certificates on page 71

Generating a certificate signing request

Before you approach a CA, you must create a customized request for a certificate. After you create this request, you can use this requested file to buy a customized certificate.

Before you begin

Before you generate a certificate signing request (CSR), you must install AvayaLive™ Engage.

About this task

Create a file which you can use to buy a certificate.

Procedure

1. Open a Web browser and enter http://localhost:8080/WAWebService/WAInterface.asmx?op=CreateCertificateSigningRequest in the **Address** field.
   The system displays the **WAInterface Web Service** screen.
2. Enter the **serverFQDN**.

   Note:

   The **serverFQDN** must match exactly the FQDN of the server as the clients will see the server FQDN displayed on the screen. The system generates errors in case of a mismatch.
3. Enter accurate information in all other fields.

   Note:

   The CA will verify your request and might reject the request if the CA is not satisfied with your identity.

   Only the **keySize** field is optional. The default **keySize** field is 2048. Valid values are 512, 1024, and 2048, with larger numbers being more secure. The CA must support the keysize, otherwise the request will fail OR the issued certificate will be invalid.
4. Click **Invoke**.
   When the method runs and finishes, the Web page displays an XML response.
   - If the response is true, the request has been generated.
   - If the response is false, the request has not been generated.
5. If the response is true, navigate to `W:\web.alive\Certs\CertRequest.csr` to obtain the CSR.
6. If the response is false, navigate to `W:\web.alive\Logs` for the most recent `WAWebService_<datetime>.log`.

   The failure cause is at the bottom.

   Note:

   At any given time, you can only have a single CSR in an in-progress state. Generating the CSR for a second time fails because the CA provides a private

key that is associated with the CSR waiting to be mated with the certificate. Generating a second CSR invalidates the first.

Buying a certificate

The process of buying an SSL certificate varies from vendor to vendor. In a typical scenario, you navigate through a wizard, provide your CSR details, and receive a customized certificate upon completion of the wizard.

Before you begin

Before you buy a certificate, you must generate a CSR and remember the following:

- Ensure that you obtain an SSL certificate. Other types are not applicable.
- If the CA requires a format for the certificate, select an option such as Apache (Verisign calls this Apache format) or OpenSSL, or Base-64 Encoded X.509. The certificate format is critical.

Note:

To operate successfully in the deployment, AvayaLive™ Engage requires Internet Information Services (IIS) and ASP.NET.

Deleting a certificate signing request

Before you begin

Before you delete a CSR, the CA must fail to validate your CSR.

About this task

The purpose of this task is to remove the CSR from your server so that you can generate another one. This method deletes the original private key and invalidates the original CSR.

Procedure

1. Open a Web browser and enter http://localhost:8080/WAWebService/WAInterface.asmx?op=DeleteCertificateSigningRequest in the **Address** field. The system displays the **WAInterface Web Service** screen.
2. Click **Invoke**.
   The Web page displays one of the following XML responses:
   - If the response is true, the CSR is deleted.

- If the response is false, the CSR is not deleted.

Installing the certificate

After you receive the certificate from the CA, you must install the certificate on the AvayaLive™ Engage server.

Before you begin

Before you install the certificate on the AvayaLive™ Engage server, you must buy the certificate from a CA.

⚠ Warning:

The following procedure restarts the tunnel proxy. Users on the server might be disrupted. Do not install certificates on active servers.

About this task

The purpose of this task is to install a customized SSL certificate on your network to enable AvayaLive™ Engage to provide secure communications between the client and the server.

Procedure

1. Copy the certificate that you bought in Buying a certificate on page 69 into `W:\web.alive\Certs\NewCert.cer`.

   An example certificate to show the format:

```
-----BEGIN CERTIFICATE-----
MIIF3zCCBMegAwIBAgIQVm9ieh3hLeRmgUBU27wTyzANBgkqhkiG9w0BAQUFADCB
yzELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMTAwLgYDVQQL
EydGb3IgVGVzdCBQdXJwb3NlcyBPbmx5LiAgTm8gYXNzdXJhbmNlcy4xQjBABgNV
BAsTOVRlcm1zIG9mIHVzZSBhdCBodHRwczovL3d3dy52ZXJpc2lnbi5jb20vY3Bz
L3Rlc3RjYSAoYykwOTEtMCsGA1UEAxMkVmVyaVNpZ24gVHJpYWwgU2VjdXJlIFNl
cnZlciBDQSAtIEcyMB4XDTEwMTExOTAwMDAwMFoXDTEwMTIwMzIzNTk1OVowgbMx
CzAJBgNVBAYTAkNBMRAwDgYDVQQIEwdPbnRhcmlvMQ8wDQYDVQQHFAZPdHRhd2Ex
DjAMBgNVBAoUBUF2YXlhMRIwEAYDVQQLFAl3ZWIuYWxpdmUxOjA4BgNVBAsUMVRl
cm1zIG9mIHVzZSBhdCB3d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EgKGMpMDUx
ITAfBgNVBAMUGGdzc2xhYi13YTIuYXZheWFsaXZlLmNvbTCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBALQ4NFmnRs0i71lOBUE0QMaMi5FEKSB3KjkcKU5R
KIOzzX2gceciR64reUpB/qjugBb+3qzGnv8/mkDr19kdtXa/PCFPO4mAN4k937ft
kozgzvbLhqm88htGzNDuQif1Oa5Cca4O8sAk1WzjuF8G7Fs+9iLZGFJWjX7yOcOs
kozgzvbLhqm88htGzNDuQif1Oa5Cca4O8sAk1WzjuF8G7Fs+9iLZGFJWjX7yOcOs
36bHC00l2mESFbT/yW7bI4CXuO/y9mZGyP0MNg8W+YGvtOl8z5ztwMiLiOq4j+vS
yjVRQwZS2MkzZwx+zHbDPcFy4yk7hUdAEo2G4mf3G/2HvPNRPRrFpzyQod67+Z+B
XwKdNKyd0TmjcyZKtSGfa+qEEMVd+N1qBTgXSymFwdo+50cCAwEAAaOCAdMwggHP
MAkGA1UdEwQCMAAwCwYDVR0PBAQDAgWgMEMGA1UdHwQ8MDowOKA2oDSGMmh0dHA6
Ly9TVlJUcmlhbC1HMi1jcmwudmVyaXNpZ24uY29tL1NWUlRyaWFsRzIuY3JsMEoG
A1UdIARDMEEwPwYKYIZIAYb4RQEHFTAxMC8GCCsGAQUFBwIBFiNodHRwczovL3d3
dy52ZXJpc2lnbi5jb20vY3BzL3Rlc3RjYTAdBgNVHSUEFjAUBggrBgEFBQcDAQYI
KwYBBQUHAwIwHwYDVR0jBBgwFoAUKBcTir3WorXcBiy3to7aEGZgbuUwdAYIKwYB
BQUHAQEEaDBmMCQGCCsGAQUFBzABhhhodHRwOi8vb2NzcC52ZXJpc2lnbi5jb20w
PgYIKwYBBQUHMAKGMmh0dHA6Ly9TVlJUcmlhbC1HMi1haWEudmVyaXNpZ24uY29t
L1NWUlRyaWFsRzIuY2VyMG4GCCsGAQUFBwEMBGIwYKFeoFwwWjBYMFYWCWltYWdl
L2dpZjAhMB8wBwYFKw4DAhoEFEtruSiWBgy70FI4mymsSweLIQUYMCYWJGh0dHA6
Ly9sb2dvLnZlcmlzaWduLmNvbS92c2xvZ28xLmdpZjANBgkqhkiG9w0BAQUFAAOC
```

```
AQEAsOEcBByYNF8q4/48yGHvF4KOzRlBSJ5etaAtWSVUcxRpsD/g0P7Q7M9AoI66
sbASlYqPLMB+P+pV2T1eRit3YjfMd2sZKm7kzJD7y6BqIzGDTzJpl02Q1eaybJu1
4sWY4oioMYhRH9OpfhDjgqCCaXhWaku9ltiv+nY2YsURZCIbZkO9o3Bt6P2pJPkX
4uBPV/4T6WTkNDJ6hJNcPbYhv8LN03GQ/T5aw4lxSDGaIM5pCmrA+DhExPkdbKCZ
Yehgir40rOEmuTQGS7TuxVDjiFLFLDxtelBRNv2IOb440HyCXon0tQOn5+zWxgE8
GnPbNVmsapw0fjQpGZpe3rcFHw==
-----END CERTIFICATE-----
```

2. Open a Web browser and enter http://localhost:8080/WAWebService/WAInterface.asmx?op=InstallCertificate in the **Address** field.
   The system displays the **WAInterface Web Service** screen.
3. Click **Invoke**.
   The AvayaLive™ Engage server restarts.
   The Web page displays one of the following XML responses:
   - If the response is true, the CSR is installed.
   - If the response is false, the CSR is not installed.

Intermediate CA certificates

Modern Certificate Authorities often do not issue certificates that are connected directly to their root certificate. Instead, one or more intermediate certificates connect the certificate the authorities issue to you to their root certificate, thus forming a chain. The website of the CA contains detailed information about the intermediate certificates they use and provide the ability to download them. Intermediate certificates must be installed into the trusted database of the server. In certain cases, if an SSL server end point expresses a certificate without its chain, the client may consider that invalid, even if the intermediate certificates are trusted on the client.

About this task

The Engage Tunnel Proxy uses the trusted database of the Windows operating system to build chains. Therefore, you need to only install the intermediate certificates into the operating system. Use the following procedure for each intermediate certificate you need to install.

⚠ Warning:

This procedure restarts the Tunnel Proxy server. Hence, you must not perform this procedure on active servers as users on the server may be disrupted.

Procedure

1. Download the intermediate certificate from the website of the CA and place it on the file system of the server.
2. Double-click the certificate.
   The certificate opens in a dialog box.

3. Click **Install Certificate**.
4. In the Certification Import Wizard, click **Next**.
5. Select **Place all certifications in the following store** and click **Browse**.
6. Click **Show physical stores** and select **Intermediate Certification Authorities** > **Local Computer** in the presented tree.
7. Click **OK**.
8. Click **Next** and then click **Finish**.
9. Once all the intermediate certificates are installed, you must restart the Tunnel Proxy server as follows:
   a. Open the Services Control panel using **Start** > **Administrative Tools** > **Services**.
   b. Scroll to **WATunnelProxyService** and click **Restart** from the right-click menu.

Configuring AvayaLive™ Engage for SSL

The process of configuring AvayaLive™ Engage for SSL consists of two tasks, which you must complete in sequence:

- Using the AvayaLive™ Engage Server Configuration Tool, set the HTTPS settings.
- Using the operating system, open port 443.

Note:

You can encrypt all user traffic using the administration panel.

Related topics:

Changing the HTTP setting on page 72
Managing traffic on page 73
URLs on page 74

Changing the HTTP setting

To configure AvayaLive™ Engage, you must open the AvayaLive™ Engage Server Configuration Tool and change the Hypertext Transfer Protocol (HTTP) settings to HTTPS. HTTPS is the secure form of HTTP communications.

Recall that you last used the AvayaLive™ Engage Server Configuration Tool when you installed AvayaLive™ Engage and configured your server and subscription.

Before you begin

Before you configure AvayaLive™ Engage, you must obtain and install an SSL certificate.

About this task

The purpose of this task is to change many of the AvayaLive™ Engage HTTP settings to HTTPS.

Procedure

1. Open the AvayaLive™ Engage Server Configuration Tool.
2. Change the **Web Server Scheme** field from `http` to `https`.
3. Change the **web.alive Help URL** field from `http` to `https`.
4. Change the **Image Service Base URL** field change from `http` to `https`. If your deployment consists of several servers sharing an image service, ensure that you coordinate the details of this field on each server. For more information, see Configuring AvayaLive Engage on page 45.

   Note:

   Do not update the **WA Web Service URL** and **Proxy Test URL** fields.
5. Click **Configure Server**.
   AvayaLive™ Engage applies these values to your server quickly.
6. Click **Configure Subscription**. AvayaLive™ Engage applies these values to your account. This step can take several moments.

   Tip:

   Ensure that you do not click **Configure Subscription** without first clicking **Configure Server**.

Managing traffic

Fully encrypted traffic is more secure but lowers traffic performance. Voice traffic is especially sensitive to lag and jitter when the switch is from UDP to a TCP SSL tunnel. Unless network conditions are ideal, this switch often causes a reduction of voice quality. At this point, all HTTP traffic is over SSL and all voice traffic is over SRTP, while the other traffic types are not encrypted. If this is the desired traffic, then no further action is required.

About this task

Use the following procedure to switch to all traffic types over SSL:

Warning:

This procedure disrupts active users accessing the server. Hence, change this value only when no one is using the server.

Procedure

1. Log in to the administration panel using your administrator credentials.
2. In the **Settings** section, under the **Main** tab, click the **Encrypt all user traffic** check box.
3. Click **Apply**.

URLs

The URL for your regular AvayaLive™ Engage users is https://<engage FQDN>/1/html/index.html.

The URLs for your AvayaLive™ Engage administrators are as follows:

- https://<engage FQDN>/WAAdminPanel/Login.aspx. Use this URL when using AvayaLive™ Engage for SSL.
- https://<engage FQDN>/WAAdminPanel/.

Troubleshooting certificates

If you use SSL in your AvayaLive™ Engage system, you cannot use a Content Distribution Network (CDN) with AvayaLive™ Engage. The CDN and the server have different FQDNs, and a single certificate cannot secure the solution. To successfully deploy a secure AvayaLive™ Engage solution, the server FQDN and the server Web FQDN must be the same.

However, the CA frequently fails to verify the CSR. The following are common causes of a failed validation:

- You have made a typographical error.
- You did not provide the official company name. The official company name can often be different from the commonly used company name.
- You did not provide the official company address. The CA may have different address details for your company in their records.
- You, or your company do not own the domain that you are trying to get a certificate for.

When a validation fails, regenerate the CSR. Before you regenerate the CSR, you must delete the current in-progress CSR. To delete a CSR, see Deleting a certificate signing request on page 69.

Chapter 11: Administering AvayaLive™ Engage

Backing up

The administration panel has a backup utility. Use the backup utility to back up the AvayaLive™ Engage data on the W: drive of the server. The utility does not back up local users and groups created by the administration panel. To back up user accounts, use another utility.

About this task

Use the following procedure to back up the AvayaLive™ Engage data.

Note:

The backup process does not back up the following:

- Operating system and any software installed on the server.
- AvayaLive™ Engage software. Only the subscription data is backed up.
- Local users and groups created by the administrator.
- Accounts created by the AvayaLive™ Engage server installation.
- File permissions of backed-up files.

Procedure

1. Log in to the administration panel.
2. Click the **Advanced** tab.
3. Click **Backup**.
   The backup may take a while depending on how much data is on the server.

   When the backup completes, the Web page displays a link to the back-up file.
4. Click on the link to download the back-up file and save the file in a safe location.

Restoring

To restore AvayaLive™ Engage, the server must be functional. The restore function is available on the administration panel.

Before you begin

- Before you restore your AvayaLive™ Engage server, you must first create the backup file.
- Place the backup file on the server in the `w:\web.alive\backups` directory before beginning the restore.

About this task

Use the following procedure to reinstall AvayaLive™ Engage.

Note:

You can only restore AvayaLive™ Engage to the same FQDN that was used to create the backup. Therefore, use a back-up file for restoration only if you:

- Lost data on an existing machine and want to restore that machine using a back up.
- Want to restore a broken machine. The replacement must have the same FQDN as the original.

Procedure

1. Log in to the administration panel.
2. Click the **Advanced** tab.
3. Click **Restore**.
   The system displays a confirmation dialog box warning of a server restart.
4. Click **OK** to start the restore.
   The system restarts the AvayaLive™ Engage server, the tunnel proxy, and the AvayaLive™ Engage statistics.

   The system displays a message to inform you that the restore process is complete.

Simplifying the URL

The default AvayaLive™ Engage URL includes the subscription ID, http://<engage FQDN>/1/html/index.html. To prevent users from gaining access to the subscription ID, configure Web

root redirects using your local browser and the WAWebService to replace the full address with the FQDN.

Before you begin

- Install, configure, and verify your AvayaLive™ Engagesolution.
- Ensure that the system is functional and stable, and Subscription Configuration is complete. Perform this task only on a stable system.

About this task

To simplify the URL before distributing to the users, use the following procedure.

Procedure

1. Open a Web browser and enter http://localhost:8080/WAWebService/WAInterface.asmx?op=WASetupWebRootRedirects in the **Address** field.
   The system displays the **WAInterface Web Service** screen.
2. In the **subscriptionId** field, enter 1.
3. In the **serverWebFQDN** field, enter the FQDN.
4. Click **Invoke**.
   AvayaLive™ Engage restarts, and an XML response displays the following:
   - If the response is true, the configuration is successful and users can now access AvayaLive™ Engage using the FQDN.
   - If the response is false, the configuration is unsuccessful and users cannot access AvayaLive™ Engage using the FQDN.
5. If the response is false, navigate to `W:\web.alive\Logs` for the most recent `WAWebService_<datetime>.log` file.
   The system displays the cause of the failure at the bottom of the file.
6. If the response is true, the new URL for a non-SSL solutions is http://<engage FQDN>/ , and the URL for an SSL solutions is //<engage FQDN>/.
   If you switch from an SSL solution to a non-SSL solution or vice versa, you must repeat this task.

Reducing the user limit

In AvayaLive™ Engage, the maximum number of users for a server is called Peak Concurrent Users (PCU). By default, each system is set up for 100 users and five administrators. The separate administrator count enables administrators to enter the system and to remove users if required, even if the system reaches full capacity.

You can reduce the PCU, but you cannot increase PCU without affecting voice quality.

Before you begin

Before you reduce PCU, you must install, configure, and verify your AvayaLive™ Engage solution.

Note:

This method restarts the AvayaLive™ Engage server. Users on the server will be disrupted. Hence, do not change the PCU limits on active servers.

About this task

Use the following procedure to reduce the PCU in AvayaLive™ Engage.

Procedure

1. Open a Web browser and enter http://localhost:8080/WAWebService/WAInterface.asmx?op=WAUpdatePCU in the **Address** field.
   The system displays the **WAInterface Web Service** screen.
2. In the **subscriptionId** field, enter `1`.
3. In the **MaxPCU** field, enter the new maximum number of users.
4. In the **MaxAdminBuffer** field, enter the new maximum number of administrators who can access the server.
5. In the **MaxMeetingHosts** field, enter `0`.

   On-Premise Solution (OPS) does not support this field.
6. Click **Invoke**.
   The system restarts AvayaLive™ Engage and also displays the following XML response:
   - If the response is true, the configuration is successful and the new limits are set.
   - If the response is false, the configuration is unsuccessful and the new limits are not set.
7. If the response is false, navigate to `W:\web.alive\Logs` for the most recent `WAWebService_<datetime>.log` file.

   The system displays the cause of the failure at the bottom.

   Note:

   If you use this method to increase the PCU, you are in violation of your Avaya license agreement.

Appendix A: PowerShell Scripts

The Setup.ps1 script

The `Setup.ps1` script performs a number of tasks that automate the configuration of AvayaLive™ Engage.

Related topics:

Host file

In deployments where the FQDN does not map to the IP address of the server, AvayaLive™ Engage operates incorrectly. To address this issue, Avaya has added the following to the host file:

Map from	Map to
localhost	127.0.0.1
<hostname>	127.0.0.1
<FQDN>	127.0.0.1

Partition mapping

To ensure that the second disk is on the W: drive, AvayaLive™ Engage Engage remaps the system as follows:

Drive name	From	To
web.alive Data Store	Any drive letter	`W:`

Directories

Using the `Setup.ps1` script, you can create the following directories:

Directory	Notes
`C:\WAEFiles`	Expected location for the default `.WAE` file. The `Setup.ps1` script copies the `Default.wae` file into this directory after creation.
`C:\inetpub\Internal`	Directory for the Internal Web site.
`C:\inetpub\Internal \WAWebService`	Directory for the `WAWebService` Web application.
`C:\inetpub\wwwroot \WAAdminPanel`	Directory for the administration panel Web application.
`C:\inetpub\wwwroot \WAFileExchange`	Directory for the File Exchange and Dropbox Web application.
`C:\inetpub\wwwroot \WAInsertionUploader`	Directory for the Web application that uploads files for insertions.
`C:\inetpub\wwwroot \WAImageService`	Directory for the Badge Web application.
`C:\inetpub\wwwroot \ServerStats`	Directory for the Server Stats Web application.
`W:\web.alive\INIs`	Directory for server-wide INI files.
`W:\web.alive \avatarBadgePictures`	Directory to store Badges. The `Setup.ps1` script gives the Modify permission to the `Network Service` user.
`W:\web.alive\WAImageService`	Directory where the Badge Web application stores user data. The `Setup.ps1` script

Directory	Notes
	gives the Modify permission to the `Network Service` user.

Local users and groups

Create the following local users and groups using the `Setup.ps1` script :

User	In Group	Password	Notes
wauploader	IIS_IUSRS (built in)	<Installer Provided>	IIS Application Pool identity for uploading applications.
waadmin	ServerAdmin	<Installer Provided>	Initial identity for gaining access to the administration panel.

When passwords are set or reset, the `Setup.ps1` script attempts to set **No Password Expiry**. If the attempt fails, only a warning message is displayed, as the attempt could fail due to policy restrictions.

IIS applications

The `Setup.ps1` script configures IIS applications, application pools, and websites in the following manner. You can use the second Web site to place sensitive applications on another port.

Application	Application pools	Identity	Website	Port
WAAdminPanel	WAAdminPanelAppPool	Local system	Default Web site	80
WAImageService	WAImageServiceAppPool	Network service	Default Web site	80
WAFileExchange	WAUploaderAppPool	wauploader	Default Web site	80
WAInsertionUploader	WAUploaderAppPool	wauploader	Default Web site	80
WAServerStats	WAServerStatsAppPool	Network service	Default Web site	80
WAWebService	WAWebServiceAppPool	Local system	Internal	8080

Note:

- WAAdminPanelAppPool runs as a LocalSystem user so that the Admin Panel can create users, delete users, back up, restore, and access certain files. The Admin Panel application contains application level authentication and can only be run by administrators to protect the application pool from exploitation.
- WAWebServiceAppPool runs as a LocalSystem user so that WAWebService can process the services and processes of AvayaLive™ Engage. WAWebServiceAppPool runs on port 8080 which is closed on the firewall to protect the application pool from exploitation.

Virtual directories

The `Setup.ps1` script uses the following virtual directories:

URL	Mapped to
http://<fqdn>/WAImageService/avatarBadgePictures	`W:\web.alive\avatarBadgePictures`
http://<fqdn>/<SubscriptionNumber>	`W:\web.alive\<SubscriptionNumber>\Web` **Note:** Configuring the subscription creates this virtual directory. `Setup.ps1` does not set up this virtual directory.

Upload limits

The upload limit for both the default website and the internal website is changed from 30M to 200M. This upload limit is the limit for the website as a whole. Individual applications that perform an uploading function maintain their own limits.

Mime types

The `Setup.ps1` script adds the following mime types for the AvayaLive™ Engage file types:

File extension	Mime type
.bik	application/octet-stream
.csm	application/octet-stream
.dae	application/octet-stream
.uax	application/octet-stream
.ukx	application/octet-stream
.umx	application/octet-stream
.usx	application/octet-stream
.lzma	application/octet-stream
.sign	application/octet-stream
.json	application/json;charset=UTF-8

Firewall rules

The `Setup.ps1` script adds the following firewall rules to the Windows 2008 firewall. All rules are for incoming ports and are added for all scopes. Duplicate rules for port 80 do not cause the firewall any harm.

Rule name	Protocol	Port
web.alive Web Port	TCP	80
web.alive Tunnelling Port	TCP	443
web.alive Media Port	TCP	1935
web.alive Spatial Voice Port	UDP	2379
web.alive Interaction Port	UDP	7878
web.alive Spatial Voice Control Port	TCP	21002

Registry default

The `Setup.ps1` script adds default values for the Server Configuration Tool so that you do not have to enter them manually. The values exist in the registry at `HKCR\web.aliveServer\waServerConfiguration`.

Field in Server Configuration Tool	Registry key	Registry value
Installation Type	installationType	Production - Customer premises
Customer ID	customerID	0
Subscription ID	subscriptionID	1
Server FQDN	serverFQDN	<FQDN>
Server Web FQDN	serverWebFQDN	<FQDN>
web.alive Help URL	waHelpBaseURL	http://<fqdn>/WAWebHelp
Image Service Base URL	imageServiceBaseURL	http://<fqdn>/WAImageService
WA WebService URL	waWebServiceURL	http://localhost:8080/WAWebService/WAInterface.asmx
BBB Server FQDN	appSharingProviderFQDN	http://appshare.avayalive.com/
Proxy Test URL	waProxyTestURL	http://www.google.com

Upgrade related

The `Setup.ps1` script performs the following actions related to the upgrade tasks:

Action	Notes
`Delete C:\Windows\SysWOW64\config\systemprofile\AppData\Roaming\Diamondware\DWServer`	Deletes the DiamondWare databases
`Delete C:\Windows\SysWOW64\config\systemprofile\AppData\Roaming\web.alive\voice`	Deletes the voice INIs for DiamondWare
`Delete W:\web.alive\1\INIs\Voice.ini`	Deletes the voice INIs for DiamondWare
`Move W:\web.alive\1\Certs to W:\web.alive\Certs`	Moves the SSL data from the subscription to the server
`Move W:\web.alive\1\Cache to W:\web.alive\Cache`	Moves the SSL data from the subscription to the server
`Create W:\web.alive\Certs\Cert.ini`	New SSL configuration for 3.0

The Remove.ps1 script

The PowerShell script, `Remove.ps1`, performs a number of tasks that automate the removal of AvayaLive™ Engage. You can only run it after you uninstall the AvayaLive™ Engage statistics, media, and voice servers.

The `Remove.ps1` script with the **Remove** option undoes everything that the `Setup.ps1` script does with the following exceptions:

- The script does not remove any file from the `W:` drive.
- The script does not remove any local users and groups created by the administration panel.
- The script does not remove the `waadmin` and `wauploader` local users. These users are reflected in the ACLs of files on the `W:` drive.
- The script does not remove the ServerAdmin local group.
- In addition to removing all the Web applications, the script also uninstalls them.
- The script uninstalls all Web pages installed in the server setup.
- With the script, you can remove the following entities, if the entities exist:

Type	ID	Created by
Redirect	IIS://localhost/W3SVC/1/Root/index.html In AvayaLive™ Engage, redirect and the redirect file are separate entities and you must clean both. Redirect rests in an active directory node that is generally invisible.	WASetupWebRootRedirects
Redirect	IIS://localhost/W3SVC/1/Root/indexAuth.html	WASetupWebRootRedirects
Redirect	IIS://localhost/W3SVC/1/Root/indexNoPrompt.html	WASetupWebRootRedirects
Application	http://<FQDN>/<SubscriptionNumber>/stats	Subscription Configuration
Virtual Directory	http://<FQDN>/<SubscriptionNumber>	Subscription Configuration
File	C:\inetpub\wwwroot\index.html	WASetupWebRootRedirects
File	C:\inetpub\wwwroot\indexAuth.html	WASetupWebRootRedirects

File	C:\inetpub\wwwroot\indexNoPrompt.html	WASetupWebRootRedirects

The `Remove.ps1` script with the **Upgrade** option only removes software and leaves all configuration data intact. It also does the following actions:

- The script stops all the AvayaLive™ Engage application pools.
- The script uninstalls all the AvayaLive™ Engage Web applications.
- The script uninstalls all the AvayaLive™ Engage Web pages.
- The script uninstalls all the AvayaLive™ Engage client loads.
- The script deletes all the DiamondWare and Voice databases.
- The script starts all the AvayaLive™ Engage applications pools.

The RunInstallers.ps1 script

This script runs the installers outlined in the table below:

Note:

The Reinstallable column indicates if the software of the installer can be installed directly on top of itself. This is particularly useful for the recovery of the script. Installers make installation a transactional operation but that is not always possible. If the script fails in a partial fashion on an installer that cannot be reinstalled, the uninstaller for that component must be run before running the script again.

Installer	File	Type	Reinstallable
DiamondWare Voice Services	`setup-DWServers_*.exe`	Service	No
web.alive Interaction Server	`setup-web.alive-server-[1-9]*.exe`	Service	No
Red5 Media Server	`setup-web.alive-media-applications_*.exe`	Service	No
Stats	`setup-web.alive-server-stats-service_*.exe`	Service	No
PC Client Load	`setup-web.alive-pcii-client-*.exe`	Client Load	Yes
MAC Client Load	`setup-web.alive-macii-client-*.exe`	Client Load	Yes

Administration Panel	`setup-web.alive-administration-application_*.exe`	ASP.NET	Yes
Image Service (Badges)	`setup-web.alive-image-service-applications_*.exe`	ASP.NET	Yes
Insertion Upload and File Exchange	`setup-web.alive-server-applications_*.exe`	ASP.NET	Yes
WAWebService	`setup-web.alive-server-internal-applications_*.exe`	ASP.NET	Yes
Help	`setup-wawebhelp_*.exe`	Web Pages	Yes
Main Web Page Content	`setup-webpage-content_*.exe`	Web Pages	Yes

Appendix B: VMware Player

Introduction to VMware Player

For installations where you are run Big Blue Button (BBB) as a virtual machine on top of a physical AvayaLive™ Engage server, the following background material helps you install and use the VMware Player. This material is also applicable to installations in which you are running both the BBB server and the AvayaLive™ Engage server as virtual machine (VM) images.

Note:

In the following sections, references to a Windows virtual machine is not applicable to the On-Premise Solution deployment.

VMware Player

The AvayaLive™ Engage solution uses VMware Player as the hypervisor. For more information, see http://www.vmware.com/products/player/. You can download VMware Player for free from http://downloads.vmware.com/d/info/desktop_downloads/vmware_player/3_0. The AvayaLive™ Engage solution runs on version 3.1.0 or later of VMware Player. If you have a license, you can also run the AvayaLive™ Engage solution on VMware Workstation 7.1 or later. Workstation is useful for development and the license cost is very low.

Installing VMware Player

The VMware Player runs on all Windows operating systems. The Linux operating system is more restrictive. Issues might arise on newer instances of the Linux operating system.

On a Windows server: Use the following procedure to download and install VMware Player if you have installation rights on your machine:

1. Download the `.exe` file.
2. Double click the file, and complete the installation wizard.
3. Reboot your machine.

You can access VMware Player from the **Programs** menu or from a shortcut on your desktop.

On a Linux server: The installation is slightly more complex. Use the following procedure to download and install VMware Player:

1. Download the bundle file for 64-bit Linux.
2. Run the following commands on the Ubuntu server:

```
cd <directory where the .bundle file is
chmod +x ./VMware-Player*.bundle
gksudo bash ./VMware-Player*.bundle>
```

The installer prompts you for a password. The installation account requires pseudo rights. You do not need to reboot your machine. You can access the VMware Player from **Applications** > **System Tools** > **VMware Player**.

Using the VMware Player

When a virtual machine (VM) is running, VMware Player displays the terminal or window of the VM inside a host window. This terminal window is called the Player Console.

You must ensure that the control, or focus, of the Player Console is explicit. The VMware Player attempts to hide the window.

By default, you can enter a Player Console by pressing `Control+G`. To exit a Player Console press `Control+Alt`. An information message at the bottom of the console displays the current mode.

On Windows VMs, you rarely have to use the control keys. To enter the console, click within the console area, and to exit, click outside the console. Sometimes, you have to double-click the console to enter it because you have to return focus to the window first. The only exception to this rule is if the Windows VM is busy. Sometimes when busy, it does not release the mouse. In this case, use `Control+Alt` to release.

On Linux Server VMs, you must use the keys more frequently. Linux Server has no windows system because it is just a terminal. To enter the Player Console, you must click on the console until the mouse disappears. Since there is no mouse, you use `Control+Alt` to exit and return the mouse.

If you do not use the Player Console for a long period of time, the player gets deactivated. A deactivated console displays as all black. To reactivate the player on the Windows operating system, simply click on the player. To reactivate the player on the Linux operating system, click on the player until your mouse disappears and then press `Esc`.

Related topics:

Starting the VMware Player for the first time on page 93

Starting the VMware Player for the first time

When you first start the VMware Player, the player often displays the following information messages:

Message (paraphrased)	Suggested response
A newer version VMware Tools is available. Do you want to install?	Remind me later
Hardware X on the host is available to the VM if you like.	Ignore
More than one VM is running on this host. Certain hardware like disk drives can only be attached to one at a time.	Ignore
Feature X in the host OS has been disabled but VMs will run faster if feature X is enabled. Do you want it enabled?	Yes
Has this VM been moved or copied?	Copied
The VM appears to be in use. Do you want VMware to attempt to run the VM anyway and risk damage?	1. Click **Cancel**. 2. Open the file system and navigate to the VM files. 3. Delete the `*.lck` directory. 4. Try again.

Alternative to using the VMPlayer console

The console is convenient but the console also has limitations. There are alternatives. Both Linux images have Secure Shell (SSH) servers enabled. You can download any free SSH client from the Web and connect to the servers. Download the PuTTY utility from http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html.

If you are doing a lot of work while logged into a Linux Server VM, use the SSH client. The console for Windows VMs is better than the Linux version but you can use Remote Desktop (RDP) as an alternative. RDP is adequate but the additional resources needed to run the RDP server can adversely impact the VM. By default, RDP is deactivated for Windows.

Appendix C: SSL and trailing slash redirects

SSL and trailing slash redirects

When you use SSL with AvayaLive™ Engage, a minor issue occurs in which trailing slash redirects do not operate successfully. This issue commonly occurs in the administration panel URL shown in the following table:

URL	Correct/Incorrect
https://<engage FQDN>/WAAdminPanel	Incorrect
https://<engage FQDN>/WAAdminPanel/	Correct
https://<engage FQDN>/WAAdminPanel/Login.aspx	Correct and should be used

The issue is that when the Web server issues a trailing slash redirect, the server redirects to `http` which is a closed port.

The main installation package does not include the solution to this issue.

The following code is for information purposes only. Use the URL mentioned in the earlier table. You might also apply the following to a server to get the redirects to work:

1. Install the **URL rewrite Module** from http://www.iis.net/download/URLRewrite and run the 64-bit installer.
2. Add the following code to the `web.config` file in the `wwwroot` directory, as a peer of `<security/>` and `<staticContent/>`.

```
<rewrite>
<rules>
<rule name="AddTrailingSlash" stopProcessing="true">
<match url="^WAAdminPanel$" ignoreCase="true"./>
<action type="Redirect" url="https://{HTTP_HOST}{REQUEST_URI}/"
redirectType="Permanent"./>
</rule>
</rules>
</rewrite>
```

or the following alternative:

```
<rewrite>
<rules>
<rule name="AddTrailingSlash" stopProcessing="true">
<match url="(.*)" ignoreCase="true" />
<action type=action type="Redirect" redirectType="Found" url="https://
{HTTP_HOST}{REQUEST_URI}/">
```

```
<add input="{URL}" pattern="/WAAdminPanel$" />
</conditions>
</rule>
</rules>
</rewrite>
```

Index

W