



Installing web.alive in a customer premises

Release 2.5
Issue 1
March 2011

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/](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: Introducing web.alive	9
Introducing this document	9
Scope	9
Limitations	10
Chapter 2: Requirements	11
Software	11
Deployments	11
Hardware	12
Two machine deployment — web.alive	12
Two machine deployment — Big Blue Button	12
Single machine deployment	13
Single machine deployment — System Platform	13
Operating system	14
Licensing	14
Networking	15
Partitions	15
Skills	16
Chapter 3: Installing Big Blue Button from an image	17
The BBB image	17
Bridging	17
Starting VMware	18
Activating your network	19
Activating BBB	21
Verifying BBB	21
Scheduling an automatic restart	22
Configuring Vix	23
Troubleshooting Vix	24
Scheduling the task	24
Chapter 4: Installing Big Blue Button natively	27
A native installation of BBB	27
Installing Ubuntu	28
Activating your network	29
Installing BBB	30
Chapter 5: Installing Web software	33
Installing the Web server and additional framework	33
Installing the Web server	33
Installing the ASP.net framework	35
Ensuring that ports are accessible	36
Chapter 6: Installing web.alive	37
web.alive .zip file	37
Preparing for web.alive	38
About the web.alive set-up script	39
About Windows Powershell	39
Running the set-up script	40

Troubleshooting the web.alive script.....	41
Installing Diamondware.....	41
Installing the interaction server.....	42
Installing the statistics module.....	43
Installing the image service.....	43
Installing the web.alive administration panel.....	44
Installing the file exchange software.....	44
Installing the WAWebService.....	45
Installing web.alive help.....	46
Installing the main web.alive Web pages.....	46
About configuration.....	47
Configuring web.alive.....	47
Troubleshooting configuration.....	48
URLs.....	49
Environments.....	49
Chapter 7: Uninstalling web.alive.....	51
About the uninstall.....	51
Uninstalling web.alive.....	52
Chapter 8: Managing users.....	53
Two options for managing your users.....	53
Local users.....	53
Central users.....	54
Groups.....	54
Setting up central users.....	56
Consequences for a demilitarized zone (DMZ).....	56
Chapter 9: Upgrading web.alive.....	59
About the upgrade.....	59
Restoring configuration settings after an upgrade.....	59
Preparing your server for a fresh installation of web.alive.....	60
Chapter 10: Configuring your firewall.....	61
Firewall changes.....	61
web.alive ports.....	61
Big Blue Button ports.....	62
Tunnelling.....	62
Remote desktop.....	62
Activating the remote desktop feature in the operating system.....	63
Secure shell (SSH).....	63
Chapter 11: Setting up secure sockets layer (SSL).....	65
Secure sockets layer.....	65
About the WAWebService.....	65
Architecture.....	65
Managing your SSL certificate.....	66
Generating a certificate signing request.....	67
Buying a certificate.....	68
Installing the certificate.....	68
Configuring web.alive for SSL.....	70
Configuring web.alive.....	70

Configuring the firewall.....	71
Troubleshooting certificates.....	72
Deleting a certificate signing request.....	73
Chapter 12: Administering web.alive.....	75
Backing up.....	75
Restoring.....	75
Upgrading.....	76
Simplifying the URL.....	76
Reducing the user limit.....	77
Appendix A: PowerShell Scripts.....	79
The set-up script.....	79
Host file.....	79
Partition mapping.....	80
Directories.....	80
Local users.....	80
IIS applications.....	81
Virtual directories.....	81
Upload limits.....	82
Mime types.....	82
Firewall rules.....	83
Registry default.....	83
The remove script.....	84
Appendix B: VMware Player.....	87
Introduction to VMware Player.....	87
VMware Player.....	87
Installing VMware Player.....	87
Using VMware Player.....	88
Starting VMware Player for the first time.....	89
Alternatives.....	89
Appendix C: SSL and trailing slash redirects.....	91
SSL and trailing slash redirects.....	91
Index.....	93

Chapter 1: Introducing web.alive

Introducing this document

Avaya web.alive is a cutting-edge business collaboration tool that combines 3D virtual worlds with state-of-the-art spatial voice interaction. While web.alive has traditionally been available on the internet (<http://www.avayalive.com>), it is also available for installation on a customer's own network and premises as a web.alive Customer Premise Deployment (web.alive CPD). web.alive CPD comes in two deployment styles – CPD Lite and CPD Enterprise. This document deals with CPD Enterprise.



Note:

CPD Lite is an installation of web.alive without extensive IT involvement (for demos and trials). Avaya has created CPD Lite for trials and demos. It is for use by Avaya personnel only. You can request documentation from the web.alive team.

Avaya web.alive CPD Enterprise provides a solution for customers to run a web.alive server inside the customer premise. The goal of this document is to facilitate the installation of web.alive for larger scale deployments or long term deployments with the assistance of an organization's IT department.

CPD Enterprise is a native installation of the web.alive software onto one or two servers. There are two server machines to consider – one for web.alive and one for Big Blue Button (BBB). web.alive uses Big Blue Button for desktop sharing and other collaboration services. You can install these on separate machines or you can install BBB as a virtual appliance on the web.alive server.

This document represents a product in transition. While CPD Enterprise for web.alive 2.5 is a native installation, we anticipate that CPD Enterprise for web.alive 3.0 will be a full virtualization solution, likely based on Avaya Aura® System Platform. As a result, some of this document has an eye to that future.

Scope

This document deals specifically with server installation and configuration. Client installation, either from the Internet or by way of central distribution (for desktops that do not have administrative access or do not have Internet access) is outside the scope of this document.

This document is quite technical in nature. The audience of this document is the personnel doing the installation and any IT staff who are supporting the installation.

Limitations

CPD Enterprise 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. Please see the contact an Avaya Support Representative for more information.
- You can use this solution with a central User Base, but to do so, the web.alive server must be added to a Windows Domain. If the security policy in the customers' organization requires that the server resides in a Demilitarized Zone (DMZ) for Internet access, you must extend the domain into the DMZ.
- Aside from the features on the web.alive administrative panel, you require administrator/installer access on the server in order to configure web.alive.

Chapter 2: Requirements

Software

CPD Enterprise is composed of the following files:

- This document
- web.alive_CPDE_<version>.zip

This file contains all the installers and artifacts that you need to set-up web.alive on a correctly configured machine.

- BBB_<version>.zip

This is a virtual machine (VM) image of a Big Blue Button server running on Ubuntu Server (Linux) 10.04 (32 bit). This file is about 1.5G so please plan for how you are going to get it and move it around. web.alive uses the Big Blue Button for desktop sharing and other collaboration services. You can also install BBB natively, in which case you will not need this file.

Deployments

You can install CPD Enterprise in a variety of deployment styles. These are listed below:

- On two physical machines: One machine for web.alive and one machine for Big Blue Button.
- On two virtual machines: In this case, both virtual machines are provided by the organization's IT department including operating systems, disks, networking, and so on. This deployment style is really no different from two physical machines from the point of view of the installer.
- On one physical machine: In this case, web.alive runs natively on the physical machine and BBB runs as a virtual machine with the physical machine acting as host.
- On one physical machine and the intention is to convert the machine to Avaya Aura® System Platform when web.alive 3.0 is released. While this is really no different from the previous deployment, the use of System Platform will require that the machine satisfy those hardware requirements now. At the time of writing, moving web.alive to System Platform is not a confirmed program.

Hardware

Related topics:

[Two machine deployment — web.alive](#) on page 12

[Two machine deployment — Big Blue Button](#) on page 12

[Single machine deployment](#) on page 13

[Single machine deployment — System Platform](#) on page 13

Two machine deployment — web.alive

Avaya expects that the two required machines will be provided by the organization's IT department (either physical or virtual). The web.alive machine must satisfy the following requirements.

Component	Physical or virtual machine
Processor	Two 64 bit cores; 2.33 GHz
Hard drive <ul style="list-style-type: none">• Operating system partition• web.alive data store partition	See below <ul style="list-style-type: none">• 20G• 10G
Memory	2G
Network	One NIC

Two machine deployment — Big Blue Button

If you are deploying on two machines, the BBB machine must satisfy the following requirements:

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

**Note:**

The BBB web page (www.bigbluebutton.org) does not provide minimum specifications for their product. Avaya has based this table on their own experience and testing.

Single machine deployment

If you are deploying the BBB server as a virtual machine on the web.alive server (single machine deployment), the web.alive server must satisfy the following requirements:


Component	Physical or virtual machine
Processor	One 64 bit; Quad Core; 2.33 GHz
Hard drive	250G (two partitions) <ul style="list-style-type: none"> • Operating system partition • 40G free • web.alive data store partition • 10G
Memory	6G
Network	One NIC

**Note:**

In these tables, 64 bit refers to the processor architecture and not the operating system. The processor must support Virtualization Extensions such as Intel VTx or AMD-V. You must enable these in the Built-In Operating System (BIOS).

Single machine deployment — System Platform

When Avaya releases web.alive 3.0, you may wish to reuse the web.alive machine for System Platform or reuse the System Platform machine for web.alive. If this is the case, this machine must satisfy the following requirements to enable its expanded use in the future:

Component	Physical or virtual machine
Processor	One 64 bit; Quad Core; 2.4 GHz
Hard drive	250G <div>  Note: Avaya recommends a dual Hard Disk Drive (HDD) with Redundant Array of Independent Disks (RAID) 1. </div>
Memory	8G
Network	Two NICs



Note:

The processor must support Virtualization Extensions such as Intel VTx or AMD-V. You must enable these in the Built-In Operating System (BIOS).

Operating system

As there are two machines in the solution, there are two operating system requirements:

- web.alive server: Windows 2008 Standard Edition R2 (64-bit). The requirement for R2 is strict. Avaya does not support R1, either Service Pack 1 or Service Pack 2. Alternatively, Enterprise Edition or Data Center Edition are also acceptable. However, Avaya tests the web.alive software on Windows 2008 Standard Edition.
- BBB server: Ubuntu Server (Linux) 10.04 (32bit or 64bit). BBB also has 64-bit support in version 7 but Avaya has not tested this version.

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

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 web.alive license. The maximum number of regular users is 100. The maximum number of administrator users is five. As a result, the maximum number of CALs is 105.

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

Related topics:

[Reducing the user limit](#) on page 77

Networking

Avaya expects that any machines provided by the organization's IT department will be fully configured for networking. Each machine must have an IP address and a Fully Qualified Domain Name (FQDN) before the installer can work with it.

Every server in web.alive needs a Fully Qualified Domain Name (FQDN) — web.alive clients never reference web.alive by hostname alone. You can easily identify FQDNs as the dot separated names that represent computers, such as `google.com`. FQDNs promote the portability of computers by allowing them to change IP address without changing name. The Domain Name Service (DNS) manages the translation from FQDN to IP address.

Sometimes, you may require a machine to have two FQDNs. Typically, the two FQDNs are the default FQDN, usually based on a hostname, and a public alias. For example, a machine could be called `HT6756s.internal.mycompany.com` but you would rather people use it as `webalive.mycompany.com`. As an example, the web.alive servers in the Amazon cloud all have two FQDNs because the FQDNs that Amazon provides are not user friendly. In a deployment with alias FQDNs, the organization's IT department must perform some configuration tasks before the web.alive installation.

web.alive 2.5 does not support Internet Protocol version 6 (IPv6) at this time. You should disable IPv6 on any web.alive server or BBB server.

Partitions

web.alive uses a two partition model. As usual, the operating system and installed software uses the first drive, the C drive. The web.alive server data uses the second drive, the W drive. This model facilitates easier installation, backup, restore, and upgrade. The organization's IT department, which provides the machine, should 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 for the **Server Manager Tool**.

The quick start icon for the **Server Manager Tool** is toolbox icon at the bottom left of the screen, next to the **Start** Menu.

2. On the tree on the left, select **Disk Manager** under the **Server Manager** and then select **Storage**.
3. In the graphical view of the disk, right-click and select **Shrink Volume**.

4. If it is available, shrink the volume by the desired amount.
5. Use the freed space to create a new partition.

If you have a virtual machine, the organization's IT department must provide both virtual disks. The second partition must satisfy the following rules:

- You must label it *web.alive Data Store*. There are scripts later in the installation that recognize the disk by label. You can change this name from any Explorer window.
- You must assign it to the *w* drive letter or you must ensure that the *w* drive letter is free. The installation scripts will later reassign this drive.
- The drive must also be empty.

Skills

This installation procedure is fairly complex. It is critical that the installation engineer has 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 its associated concepts
- Basic file transfer skills on both Windows and Linux
- Experience with this procedure. Training in a controlled lab environment is an asset.
- Experience with PowerShell scripts. This installation uses PowerShell. A knowledge of how to run PowerShell is an asset.



Tip:

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

Chapter 3: Installing Big Blue Button from an image

The BBB image

Big Blue Button (BBB) provides collaborative Web-based services that web.alive uses. Specifically, web.alive 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. Here are the steps for deploying BBB from an image. The next chapter describes how to deploy BBB as a native install.

While the installation of BBB is technically a pre-requisite for web.alive, you can perform the BBB installation steps in parallel with the installation of IIS and web.alive. Alternatively, you can install BBB later if you are willing to reconfigure a running web.alive server once BBB is available. It is only at the end of the web.alive installation that you have to point it at the BBB server.

If you install BBB as a virtual machine (VM), where the web.alive server acts as the VM host, you can create a full web.alive system on one physical machine. This option is often preferable to consuming two physical machines. BBB runs in its own VM on Ubuntu 10.04 Server (32-bit). The image is in file BBB_<version>.zip. This image is created for VMware Player. You must first install Player on the physical web.alive server.

Related topics:

[Introduction to VMware Player](#) on page 87

[Installing VMware Player](#) on page 87

[Using VMware Player](#) on page 88

Bridging

In a virtual deployment, there is a special networking requirement. 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. This means that a single NIC card can assume multiple identities — one for the

host and one for each virtual machine (VM) running on that host. The VMs and the host share the NIC card as equals. Avaya preconfigures each BBB image with bridging enabled.

Bridging is the only way that VMs can act as servers. If you cannot provide bridging, this deployment of BBB cannot operate successfully. There are a number of reasons why you may not be able to provide bridging:

- The host operating system may be configured to prevent bridging.
- The NIC card may not support bridging, perhaps because it is too old.
- The organization's IT department network policies may prevent bridging. This is more likely to be the case in sensitive deployments such as government-related or military installations. If bridging is blocked, you must run the host in a region of the network that supports virtualized servers.
- Wireless connectivity may prevent bridging. If you are connected wirelessly, you may be unable to provide bridging. Many, though not all, wireless networks do not support bridging.

Starting VMware

VMware is virtualization software. You require this software to control and manage the BBB installation. Your first task, as part of the installation of BBB, is to start the BBB virtual machine and update the default password in the BBB console.

At this point, you require the web.alive image, which you can obtain from Avaya or from your Avaya business partner.

Prerequisites

Obtain the web.alive image from your Avaya customer service representative.

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

-
1. Unzip the BBB image zip file.
The image consists of a root directory and a number of files in that directory
 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 it.
The Player displays the VM specifications with the state **Powered Off**. The left side of the Player dialog displays and retains the location of the VM.

5. Click **Play Virtual Machine**.

The BBB console and the operating system starts. This process may take several minutes.

6. Log in to the BBB console.

The username is `firstuser` and the password is `Default1`. This is a temporary password. You must immediately update the password. The update process involves entering the temporary password and then entering and verifying a new password.

Next steps

Now, you must enable networking for this configuration.

Activating your network

For the web.alive 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 in a VI editor to complete the task.

Prerequisites

Before you activate the network, you must start the BBB virtual machine.

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

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

```
ifconfig
```

This command displays all the networking interfaces. At this stage, the command should only display an interface called `lo`. This is the loopback address. None of the other interfaces are active.

2. Activate networking.

If your deployment uses DHCP:

- a. Enter the following command replacing the variables with the hostname and FQDN of the server. Avaya initializes the BBB hostname with the phrase `nohostname`.

```
./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.

If your deployment uses a static IP:

- a. Enter the following command replacing the variables with the hostname and FQDN of the server.

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

- b. At the resulting command prompt, enter your password.

The script opens a file, into 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
```

The script opens a second file.

- c. Enter the following information:

- IP address of the primary and secondary DNS servers
- The domain name which these DNS servers represent

You must enter this information twice.

- d. Save and close the file.

3. Hit ENTER to restart the server.

4. Restart the BBB virtual machine and verify that networking is activated by entering the following command:

```
ifconfig
```

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

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.

Prerequisites

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

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

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 by restarting several services.
3. Ensure that BBB is accessible by the web.alive clients. To ensure accessibility, you must edit the following file:

```
sudo vi /etc/nginx/sites-enabled/bigbluebutton
```

4. Change the third line of this file, from:

```
server_name <fqdn>;
```

to

```
server_name <ip> alias <fqdn> 127.0.0.1;
```

5. Restart the BBB server by entering the following command:

```
sudo /etc/init.d/nginx restart
```

Next steps

Now, it is a good idea to 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.

Prerequisites

Before you verifying that BB is up and running, you must activate it.

The purpose of this task is to validate the BBB application before you progress any further through the web.alive installation steps.

1. On a Command Prompt dialog, 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 a browser window, verify the BBB URL by entering the following in the **Address** field.

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

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

Scheduling an automatic restart



Note:

This is an optional task.

You are running the BBB application by way of VMware Player. One of the main disadvantages of running an application by way of VMware Player is that the application does not automatically restart each time you restart your host machine. This is a concern because web.alive benefits from periodic restarts. There are a number of ways of ensuring periodic restarts. Avaya recommends creating a scheduled task in the Windows operating system. This method is described in the following sections.

An important aspect of running a server automatically is to run it without a console interface (GUI). Without a GUI, BBB can run automatically upon a restart of the host machine. and there is no longer a necessity to be logged into the BBB machine. To run BBB without a GUI, you require an additional application that operates with VMware Player. This application is called Vix. 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. You may also have to add a mapping to Vix. Lastly, you must schedule the restart task in Windows.

Related topics:

[Configuring Vix](#) on page 23

[Troubleshooting Vix](#) on page 24

[Scheduling the task](#) on page 24

Configuring Vix

VMware produces the Vix application. It is free.

Prerequisites

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

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

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. It is a good idea to omit the `nogui` option until you have verified that the BBB server is accessible by way of an SSH client that allows you to connect from other machines, giving you a terminal window.

3. Verify that the BBB server is running using the steps described in [Verifying BBB](#) on page 21 or by displaying the **Processes** tab of the Task Manager in the host machine and checking the list for a process called `vmware-vmx.exe`.

Note:

Ensure that you do not run two instances of the BBB virtual machines. This error is easy to make.

Next steps

Now, you may have to add a mapping to Vix. This is more likely to be the case if you have a very 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
```

Prerequisites

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

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

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

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

The Vix installation directory contains sub-directories 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. You may have to try several different communication libraries to identify the one which operates with your version of VMware Player.



Tip:

For more information, search the VMware forums or enter the error message or the phrase, `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.

Prerequisites

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

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

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. Enable a task delay and set it 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, browse to 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 none of the options are enabled, with the exception of **Allow task to be run on demand**. 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` executes for a short period of time and it should 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. As a final verification step, reboot the host, wait seven minutes, and verify that the BBB server has also rebooted.

Installing Big Blue Button from an image

Chapter 4: Installing Big Blue Button natively

A native installation of BBB

Big Blue Button (BBB) provides collaborative Web-based services that web.alive uses. Specifically, web.alive 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. Here are the steps for deploying BBB as a native install. The previous chapter describes how to deploy BBB from an image.

While the installation of BBB is technically a pre-requisite for web.alive, you can perform the BBB installation steps in parallel with the installation of IIS and web.alive. Alternatively, you can install BBB later if you are willing to reconfigure a running web.alive server once BBB is available. It is only at the end of the web.alive installation that you have to point it at the BBB server.

Native installation means installing BBB as an application onto an existing machine. The machine can be physical if there is a sufficient machine available. The machine can also be virtual.

Advantages of a native installation on a virtual machine	Disadvantages of a native installation on a virtual or physical machine
You can use a hypervisor or virtual machine monitor of your choice. You are not restricted to VMware.	The installation is complex.
Your instance of web.alive can also be virtual	You require direct Internet access. You cannot perform a native installation by way of a proxy.

One of the main prerequisites for a native installation is that you must have a machine with Ubuntu Server 10.04, 32 or 64 bit. Ubuntu is a Linux operating system. Before you begin the native installation, you must install the Ubuntu server and ensure that it is networked and fully functioning. Avaya does not support Ubuntu 9.04 or any version of Ubuntu desktop for the web.alive native installation.



Important:

It is important to note that you cannot install BBB natively through a proxy server.

Installing Ubuntu

Ubuntu is a Linux operating system.

The purpose of this task is to install the operating system that is required by the BBB native installation.

1. Open an Internet browser and enter <http://releases.ubuntu.com/lucid/> in the **Address** field. Download and install Ubuntu.
2. Watch these videos for information on the installation process for Ubuntu. The Ubuntu forum community creates and posts these videos.

http://www.youtube.com/watch?v=_kSpWCku86M

<http://www.youtube.com/watch?v=Lwc2RCnGF0Q>

These videos describe how to install Ubuntu on a virtual machine. For the purposes of the BBB native installation, there are a number of deviations from the standard procedure. These deviations are described in the following steps.

3. Include the following in the virtual hardware configuration:

Component	Specification
Processor	1
Memory	1G
Single Hard Drive	20G
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 they do in the video.
6. Install OpenSSL.



Note:

Installing Ubuntu on a physical machine is almost identical to installing Ubuntu on a virtual machine:

- Start 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 the BIOS of the physical machine to boot the computer from the CD and continue as for the virtual machine.

Next steps

Now you must ensure that the Ubuntu server can communicate with other machines in your network.

Activating your network

For the web.alive solution to operate effectively, your deployment requires networking. When you install the Ubuntu operating system, it is pre-configured to support DHCP networking, by default. If your deployment uses DHCP networking, you do not need to make any configuration changes. If your deployment uses static IP addresses, you must make some configuration changes. Specifically, you must update two files. These files are:

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

You must know whether your deployment uses DHCP or static IP addresses. If your deployment uses DHCP, you can skip this task and proceed to the installation of BBB. If your deployment uses static IP addresses, you must obtain the IP configuration information from the organization's IT department. This information includes the IP address, netmask, and gateway.

There are several ways to access the configuration files. For example, you can use an SSH client that provides you with a terminal window. Putty is one such application. 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 which share certain characteristics, such as methods of invocation from the operating system command interpreter, and characteristic user interface features.

Prerequisites

Before you enable your network to support static IP addresses, you must contact the organization's IT department to obtain the static IP information.

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.

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

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

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

2. Replace this line:

```
iface eth0 inet dhcp
```

with these lines:

```
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. There is abundant information on the Web about the format and purpose of this file. The Web is the best reference.

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

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

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

4. Replace this line:

```
search myisp.com.
```

with these lines:

```
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.

Installing BBB

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

Avaya recommends visiting this site and reading the explanatory notes and troubleshooting section: <http://bigbluebutton.googlecode.com/svn-history/r4679/wiki/InstallationUbuntu.wiki>.

**Note:**

If your connection to the Internet is slow, this task will take considerably longer.

Prerequisites

Before you install BBB, install the Ubuntu operating system.

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

1. In a terminal window, enter the following:

```
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 may require a password.

2. Enter the following:

```
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 web.alive supports. web.alive does not support later versions.

3. Enter the following:

```
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 the following:

```
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 this command:

```
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 it consists of approximately 50 Linux packages. When 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 see http://en.wikipedia.org/wiki/List_of_country_calling_codes.

6. Enter this command:

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


This command installs BBB. This process takes time to run because it consists of approximately 175 Linux packages. When 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 re-confirm the MySQL database password.

7. Enter this command:

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

These commands restart BBB.

Next steps

Now you must 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 21

Chapter 5: Installing Web software

Installing the Web server and additional framework

For web.alive to operate successfully in your deployment, it requires Internet Information Services (IIS) and ASP.net.

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

At this point you must also ensure that web.alive can use port 443.

In the terminology of Windows 2008, IIS is known as a role. You must add this role using an **Add Roles** wizard. In the terminology of Windows 2008, ASP.net is known as a feature. You must add this feature using an **Add Feature** wizard.

Installing the Web server

The Web server is called IIS.

The purpose of this task is to install the Web server that web.alive requires.

-
1. At the bottom left of the screen, click the **Toolbox** icon to display the Server Manager application.
 2. Select the **Roles** node from the tree on the left of the screen.
 3. Click **Add Roles** in the menu panel on the right of the screen to start the **Add Roles** wizard.
 4. On the **Select Server Roles** dialog, select **Web Server (IIS)** and click **Next**. The application displays a large number of options for this role.
 5. Select these options.
Web Server

- Common HTTP Features (include 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 web.alive components require the ASP.net framework. The version of ASP.net is 3.5.

Prerequisites

Before you perform this task, you must install IIS.

The purpose of this task is to install a supporting framework that web.alive requires.

-
1. At the bottom left of the screen, click the **Toolbox** icon to display the Server Manager application.
 2. Select the **Features** node from the tree on the left of the screen.
 3. Click **Add Features** in the menu panel on the right of the screen to start the **Add Features** wizard.
 4. On the **Select Features** dialog, select **.NET Framework 3.5.1 Features** and click **Next**.
This option has a number of prerequisites.
 5. Accept all prerequisites and complete the wizard to install ASP.net.

Next steps

Now, you must ensure that web.alive can use port 443.

Ensuring that ports are accessible

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

web.alive uses port 443 for two purposes:

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

Since web.alive is using port 443, IIS cannot use it.

- If you install IIS directly from the operating system, as described in [Installing the Web server](#) on page 33, it is unlikely that you will experience any problems because the default installation does not use port 443.
- If you install IIS from a corporate or government image, it is more likely that you will experience a problem because IIS might be configured to use port 443. In this situation, you must make a correction to change the port allocation.

To correct the issue:

1. Open IIS Manager.
2. In the **Connections** pane, expand the **Sites** node and select a site.
3. In the **Actions** pane, click **Bindings** to display the **Site Bindings** dialog.
4. Remove or edit all the site bindings that allocated to port 443.
5. Ensure that the **Require SSL** checkbox is not selected on the **SSL Settings** pane.
6. Restart IIS.

Related topics:

[Architecture](#) on page 65

Chapter 6: Installing web.alive

web.alive .zip file

A file called **web.alive_CPDE_<version>.zip** contains all the files that you require to install web.alive. You must create a directory on your desktop and unzip this file into the new directory.

The installation of web.alive consists of a number of tasks. You must perform each of these tasks in order.

It is a good idea to print out this page and as you perform each task, you can place a check mark in the row to indicate that you have completed that module.

#	Task description	✓
1	Preparing for web.alive on page 38	
2	Running the set-up script on page 40	
3	Installing Diamondware on page 41	
4	Installing the interaction server on page 42	
5	Installing the statistics module on page 43	
6	Installing the image service on page 43	
7	Installing the web.alive administration panel on page 44	
8	Installing the file exchange software on page 44	
9	Installing the WAMWebService on page 45	
10	Installing web.alive help on page 46	
11	Installing the main web.alive Web pages on page 46	
12	Configuring web.alive on page 47	

Preparing for web.alive

Before you begin the web.alive installation process, you must prepare your machine for the installation of web.alive.

Prerequisites

Before you prepare your machine for the installation of web.alive, you must obtain the **web.alive_CPDE_<version>.zip** file and unzip it into a directory on your desktop. You must also install the Web server and ASP.Net.

The purpose of this task is to prepare your machine for the installation of web.alive.

-
1. Create the following directory on your machine: `C:\Scripts`.
 2. Copy these files into the new directory, `C:\Scripts`:
 - `SetupCPDE.ps1`
 - `RemoveCPDE.ps1`
 - `Default.wae`
 3. Copy this file: `C:\Windows\System32\drivers\etc\hosts` to `C:\Scripts` and rename it to `wahosts.template`.
 4. Install Java Runtime Environment (JRE) 1.6, which is also called version 6. If you have Internet access, you can locate the Java installer here: <http://www.oracle.com/technetwork/java/javase/overview/index.html>. Alternatively, Avaya also ships the required Java installer in the web.alive zip file. It is called: `jre-6u22-windows-x64.exe`.

Next steps

Now you can run the web.alive set-up script.

About the web.alive set-up script

The web.alive set-up script is called **SetupCPDE.ps1**. When you run this file, it performs the following actions:

- Defines the FQDN for the machine.
- Adds the FQDN and hostname mapping to the hosts file.
- Moves the data store disk to the `w` drive.

**Note:**

You must ensure that the `w` drive has this label: web.alive Data Store.

- Creates all required directories, moves files, and sets permission where required.
- Creates local users and groups needed for web.alive.
- Creates all required application pools in IIS.
- Creates all additional Web sites in IIS.
- Creates all required Web applications in IIS.
- Creates all required virtual directories in IIS.
- Sets all upload limits in IIS.
- Adds all web.alive MIME types to IIS.
- Adds all web.alive firewall rules.
- Set defaults for the server configuration tool.

Related topics:

[The set-up script](#) on page 79

About Windows Powershell

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

By default, there is a Windows PowerShell quick start icon at the bottom left of the desktop. You can click this icon to start Windows PowerShell. Alternatively, you can launch Windows PowerShell by clicking this file: `C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe`.

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

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. In the unlikely event that the script still does not run, right-click on the file, select **Properties**, and click **Unblock** at the bottom of the **General** tab.

Running the set-up script

The set-up script is called **SetupCPDE.ps1**. You can run it using an application called Windows Powershell.

Prerequisites

Before you run the web.alive set-up script, you must prepare your machine for the installation of web.alive.

The purpose of this task is to run the web.alive set-up script.

-
1. Launch Windows Powershell.
 2. Enter the following commands:

```
cd C:\Scripts
Get-ExecutionPolicy
Set-ExecutionPolicy RemoteSigned
./SetupCPDE.ps1
```

The `Get-ExecutionPolicy` command returns 'Restricted'.

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 web.alive server. The dialog displays the name of the hostname because it is likely that the hostname is related to the FQDN.

3. Enter the FQDN and click **OK**.

Next steps

Now you can run the web.alive voice engine installation. The web.alive voice engine is called DiamondWare.

Related topics:

[Troubleshooting the web.alive script](#) on page 41

Troubleshooting the web.alive script

You can run **SetupCPDE.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.

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. In the unlikely event that the script still does not run, right-click on the file, select **Properties**, and click **Unblock** at the bottom of the **General** tab.

Prerequisites

Attempt to run the **SetupCPDE.ps1** script.

The purpose of this task is to try to fix any issues which arise when you are running the **SetupCPDE.ps1** script.

- Ensure that you have created the `C:\Scripts` directory. Ensure that this directory contains `Default.wae` and `wahosts.template`. Ensure that you have installed IIS and ASP.NET.
- Ensure that you have full administrative access to the machine. Full administrative access includes the ability to create local users and set properties on those users.
- Wait for a period of 10 seconds and re-run the script because:
 - Sometimes, the script fails because the Web server is too slow.
 - On rare occasions, the operating system may fail a request from Windows Powershell.

Installing Diamondware

Diamondware provides the spatial voice engine that web.alive uses. You must install Diamondware. When you install Diamondware, you specify the number of concurrent web.alive users. You can only set this limit at installation time.

Prerequisites

Before you install Diamondware, you must run the web.alive set-up script.

The purpose of this task is to install the voice technology that web.alive requires.

-
1. Run **setup-DWServers_bxxx.exe**.

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

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

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

2. Do not accept the default value of 250. Instead, enter 106.

This figure is calculated using the following metrics:

```
100 regular users + 5 admin users + 1 web.alive server
```

Alternatively, you may want to prepare for some expansion by setting a slightly higher limit. However, it is important to be aware that each channel uses a substantial amount of memory.

Next steps

Now, you can install the web.alive interaction server.

Related topics:

[Reducing the user limit](#) on page 77

Installing the interaction server

The interaction server is the main web.alive server. It contains a component called the Unreal Engine.

Prerequisites

Before you install the interaction server, you must install Diamondware.

The purpose of this task is to install the main web.alive server.

-
1. Run **setup-web.alive-server-<version>_bxxx.exe**.

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

2. Accept all the default options.
The installer displays an option to create a shortcut.
3. Click on the shortcut option to create the shortcut during installation.

Next steps

Now, you can install the statistics module.

Installing the statistics module

The statistics service analyses the server logs and produces analytic Web pages.

Prerequisites

Before you install the statistics module, you must install the interaction server.

The purpose of this task is to install the statistics software.

-
1. Run **setup-web.alive-server-stats-service_bxxx.exe**.

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

2. Accept all the default options.

Next steps

Now, you can install the image service.

Installing the image service

The image service manages the badge pictures that users see in web.alive.

The image service is somewhat optional. Avaya assumes that if you are installing the customer premises solution, you do not want to use the hosted image service. Instead, you require your own image service.

If you have multiple web.alive servers in your deployment, you do not need multiple instances of the image service. Instead, you should install the image service on the first web.alive server and all additional web.alive servers should point to the first one, so that all web.alive servers can share the same image directory.

A limitation of web.alive is that it cannot easily interact with multiple image services. An web.alive client can only upload their photograph to a single image service.

Prerequisites

Before you install the image service, you must install the statistics module.

The purpose of this task is to install the software that manages the badge photographs for web.alive.

-
1. Run **setup-web.alive-image-service-applications_bxxx.exe**.
You may have to right-click on the icon or file and select **Run as Administrator**.
 2. Accept all the default options.
-

Next steps

Now, you can install the web.alive administration panel.

Installing the web.alive administration panel

The web.alive administration panel enables administrators to perform administrative tasks. For more information about the administration panel, see *Administering Avaya web.alive: Customer premises solution*, which is available on support.avaya.com.

Prerequisites

Before you install the web.alive administration panel, you must install the statistics module.

The purpose of this task is to install the administrative GUI.

-
1. Run **setup-web.alive-administration-application_bxxx.exe**.
You may have to right-click on the icon or file and select **Run as Administrator**.
 2. Accept all the default options.
-

Next steps

Now, you can install the file exchange software.

Installing the file exchange software

Two applications manage the process of exchanging and uploading files. These two applications are located in **setup-web.alive-server-applications_bxxx.exe**.

Prerequisites

Before you install the file exchange and upload software, you must install the web.alive administration panel.

The purpose of this task is to install the software necessary for file exchange and upload.

1. Run **setup-web.alive-server-applications_bxxx.exe**.
You may have to right-click on the icon or file and select **Run as Administrator**.
2. Accept all the default options.

Next steps

Now, you can install a utility which provides administrative tools to some web.alive components.

Installing the WAWebService

This component provides services to other tools and web.alive applications. This component installs on to the internal Web site, which is port 8080. This location means that it can be blocked from external access. The access level is significant because this application has the ability to stop the web.alive server.

Prerequisites

Before you install these administrative tools, you must install the file exchange software.

The purpose of this task is to some software that web.alive uses for internal administration.

1. Run **setup-web.alive-server-internal-applications_bxxx.exe**.
You may have to right-click on the icon or file and select **Run as Administrator**.
2. Accept all the default options.

Next steps

Now, you can install the web.alive online help files.

Installing web.alive help

web.alive stores the online help, centrally. There are two main online help projects:

- Online help customized for the administrator role
- Online help customized for the regular user role

Prerequisites

Before you install the online help, you must install some administrative components.

The purpose of this task is to install the help files for administrators and regular users.

-
1. Run **setup-wawebhelp_bxxx.exe**.

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

2. Accept all the default options.

Next steps

Now, you can install main web.alive Web pages.

Installing the main web.alive Web pages

This is the final part of the actual installation and after you install these main web.alive Web pages, the web.alive installer starts up the web.alive Server Configuration Tool.

Prerequisites

Before you install main web.alive Web pages, you must install the online help.

The purpose of this task is to install the main Web pages.

-
1. Run **setup-webpage-content_bxxx.exe**.

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

2. Accept all the default options.

The web.alive installer starts up the web.alive Server Configuration Tool.

Next steps

Now, you can configure web.alive.

About configuration

The final installer, **setup-webpage-content_bxxx.exe**, starts up the web.alive Server Configuration Tool.

The web.alive installers populate all the fields on the Server Configuration Tool with default values. You need to update some of these fields to reflect the properties of your deployment. You need to provide the following information:

- **BBB server FQDN:** By default, this field points to the server running in the cloud. If you do not have a BBB server in your deployment, you can use the BBB server on the Internet. However, if you use the BBB server on the Internet:
 - Your users will be sharing their desktops on the Internet.
 - Your organization's IT security policy may block this form of desktop sharing.

- **Image Service Base URL:** If this is not the first server in your deployment, you must direct this field to use the image service of the first web.alive server.

If you have multiple web.alive servers in your deployment, you do not need multiple instances of the image service. Instead, you should install the image service on the first web.alive server and all additional web.alive servers should point to the first one, so that all web.alive servers can share the same image directory.

- The web.alive administration panel and the statistics module must be able to send e-mails. For example, the password reminder feature sends e-mails to users. Avaya recommends that you enter mail server configuration data in the five Simple Mail Transfer Protocol (SMTP) fields.

By way of terminology clarification, Avaya uses the word server to refer to the machine on which you are running web.alive. Avaya uses the word subscription to refer to a running instance of the web.alive server. This distinction is significant in a hosted environment. However, for the customer premises solution, this distinction is largely irrelevant.

Configuring web.alive

The final installer, **setup-webpage-content_bxxx.exe**, starts up the web.alive Server Configuration Tool.

Prerequisites

Before you configure web.alive, you must complete the web.alive installation. You must also install BBB. .

The purpose of this task is to update the default settings to match the requirements of your network.

1. Enter the fully qualified domain name of the Big Blue Button server in the **BBB Server FQDN** field.
2. Update the **Image Service Base URL** field, if necessary.
3. Scroll down and enter the relevant mail server configuration data in the five SMTP fields.
4. Click **Configure Server**.
web.alive applies these values to your server. This step is very fast.
5. Click **Configure Subscription**. web.alive applies these values to your account instance. This step can take several moments.



Tip:

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

Next steps

Now, you can make a note of the URLs that your users and administrators will require for access.

Related topics:

[Troubleshooting configuration](#) on page 48

Troubleshooting configuration

In a limited number of situations, the configuration may fail. For example:

- The configuration may fail because the web.alive server process, which is called Chainsaw.exe or ChainSawService, is still pending. To fix this issue, open the Task Manager and end the Chainsaw.exe process. Click **Configure Subscription** again.
- The configuration may fail because the IIS fails on a valid request. In the failure log, this form of error may be called a Directory exception. Wait a few moments and try again.

URLs

This is the URL for your regular web.alive users: <http://<web.alive FQDN>/1/html/index.html>.

This is the URL for your web.alive administrators: <http://<web.alive FQDN>/WAAdminPanel/>.

Only people with this special administrator access can use the web.alive administration panel. Avaya has created a default administrator log-in with these credentials:

- User: waadmin
- Password: LP_ko0JI(hu8GY&

Avaya recommends that you update this default log-in when web.alive is up and running.

Related topics:

[Configuring the firewall](#) on page 71

Environments

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 and with items, such as furniture. You can share information in several ways, for example, by projecting presentations on to screen displays within some environments or by depositing documents into drop boxes for other people to access. You can communicate with other people by speaking directly, writing text messages, and by telephoning people who are not currently in the meeting.

Environments have the file extension .wae. In your web.alive installation, Avaya includes an initial .wae file called Default.wae. After installation, you can change this environment by contacting your Avaya Support Representative. Alternatively, customers with accounts on the web.alive store can obtain environments here: <http://avayalive.com/WaStore/Environments>. For more information about updating environments, see *Administering Avaya web.alive: Customer premises solution*, which is available on support.avaya.com.

The URL above replaces the **Find Environment** function of the web.alive administration panel. **Find Environment** is not supported in Customer Premise Deployments.

Chapter 7: Uninstalling web.alive

About the uninstall

It is a simple procedure to uninstall web.alive. You can follow the steps described here.

When you complete the steps described here, you can consider that web.alive has been deleted from your network. However, it is worth noting that a number of components related to web.alive are still present on your network:

- The IIS Web server, which is an operating system role
- ASP.NET, which is an operating system feature
- Java
- All local users and groups created by the web.alive administration panel
- All files on the W: drive

If you want to remove this data, you must remove it manually.

The main uninstall script is called: **RemoveCPDE.ps1**. It is a Powershell script which removes and cleans-up the server. It is very similar to **SetupCPDE.ps1** and performs the opposite function. As with **SetupCPDE.ps1**, you can run **RemoveCPDE.ps1** repeatedly. In summary, **RemoveCPDE.ps1** performs the following:

- Uninstalls the ASP.NET applications
- Uninstalls the web.alive Web pages
- Removes all web server configurations
- Reverses **SetupCPDE.ps1**

For more information on what actions to take if you experience problems with the uninstall script, see [Troubleshooting the web.alive script](#) on page 41.

Related topics:

[The remove script](#) on page 84

Uninstalling web.alive

Prerequisites

Before you uninstall web.alive, it is a good idea to create a back-up of the configuration.

The purpose of this task is to remove web.alive from your network.

1. Navigate to **Start > Administrative Tools > Services** and stop the following services in the following order:
 - a. WStatsService
 - b. ChainSawService
 - c. DWServer

This DWServer also stops the DWMixer.

2. Close the Services Control Panel.
If you do not close this panel, the uninstall may fail.
3. Navigate to **Start > Control Panel > Programs And Features** and uninstall:
 - a. web.alive Statistics Service
 - b. web.alive server
 - c. web.alive DW Voice Services

You may have to change the settings on the Control Panel before you can see the **Programs And Features** option.

4. Start Powershell, navigate to `C:\Scripts` and run this file: **RemoveCPDE.ps1**.

```
.\RemoveCDPE.ps1
```

Next steps

Now, you can use the server for another purpose. Alternatively, you can begin the upgrade process to upgrade to a later edition of web.alive.

Chapter 8: Managing users

Two options for managing your users

web.alive provides you with two options for user management:

- You can configure web.alive to accept the user information that is stored on the web.alive server. Avaya refers to this configuration as a local user base.
- You can configure web.alive to accept the user information that is stored on your organization's centralized directory server. Avaya refers to this configuration as a central user base.

In a single deployment, you can combine a local user base and a central user base. In this combination configuration, web.alive can validate users against a local database or a central database at the same time.

Related topics:

[Local users](#) on page 53

[Central users](#) on page 54

Local users

By default, web.alive is configured to operate with a local user base. This means that web.alive only validates log-ins against the user and groups information that is stored on the local web.alive server. web.alive administrators can manage this data using the web.alive administration panel. The web.alive administration panel only operates with a local user base. Moreover, you must always store the web.alive administrators' log-in details in a local user base. Each new installation of web.alive contains the default `waadmin` log-in in the local user base.

Local users can login using their e-mail address. For e-mail validation to operate successfully, you must create the user using the web.alive administration panel. Similarly, the **Forget Password?** link only operates for local users.

Using a local user base has several disadvantages:

- The user ID only exists on one server and is not shared with other servers.
- The user ID does not match the user ID that the user typically uses to log-in to other applications in the organization.

- You must ensure that you back-up all local user data.
- If a user has direct access to the web.alive server, they could potentially log-in using their local user ID. For this reason, Avaya recommends that you store the web.alive servers in a locked server room with Remote Desktop (RDP) access. Do not give RDP access to non-administrators.

Central users

- Users can login to multiple web.alive servers using the same user ID.
- The user ID matches the user ID that the user typically uses to login to other applications in the organization.
- You do not need to back-up user data as part of the server back-up.
- Access to web.alive is more secure.

However, this configuration also has several disadvantages:

- Users cannot login using their e-mail address.
- web.alive administrators cannot manage this data using the web.alive administration panel.
- You must have a high level of engagement with the organization's IT department. Their involvement in the configuration of a central user base is considerable.

Groups

Users can have varying levels of access to web.alive. When you create a new user, you must allocate access levels to them. You can also edit an existing user to change their access profile. Some environments may not support all access levels. The access levels that are common to all environments are:

- Administrator User
- Laser Pointer User
- Statistics Viewer

Access level	Description
Administrator User	Users with administrator access can attend meetings using the web.alive environment. They can eject other attendees from meetings and they can place other attendees on mute. They can also upload insertions and generally configure the environment. In addition, they have the

Access level	Description
	capabilities of the other user roles; Meeting Room Speaker, Auditorium Speaker, and Statistics Viewer. This access level refers to a user who, within the context of their web.alive environment, can perform administration functions. As a person with access to the administration panel, you also have administrator access in the environment. In addition, you can create a user with administrator access to represent yourself so that you can enter the environment and verify functionality.
Meeting Host	Users with meeting host access activate the web.alive environment when they arrive. Before they arrive, other attendees can enter the environment but cannot move freely around the environment and cannot access many of the web.alive features. Similarly, when the meeting host leaves the environment, web.alive blocks access to many features. This is a special feature and customers must buy a Named Host subscription in order to take advantage of this access level. If you have a Named Host subscription and you access the environment using the Administration Panel preview screen, you have meeting host privileges.
Meeting Room Speaker	Users with meeting room speaker access can speak to an entire meeting room from the podium position. Typically, the meeting organizer or moderator speaks from the podium position.
Auditorium Speaker	Users with auditorium speaker access can speak to an entire auditorium from the podium position. Typically, large meetings or lectures take place in an auditorium.
Laser Pointer User	Users with laser pointer privileges can use their laser pointer in any location in the environment. Users without laser pointer privileges can use a laser pointer but only in the areas where the laser pointer is enabled, such as on the podium of a meeting room.
Statistics Viewer	Users with access to statistics can view the statistics associated with the environment. If you select the Allow anyone to view web.alive statistics checkbox in the Statistics panel, users do not require this privilege.

The GUI recognizes these user groups using the following strings, which are used as local groups or domain groups:

Group	Displayed in the graphic user interface as
Administrator User	ServerAdmin
Auditorium Speaker	AuditoriumPresenter
Meeting Room Speaker	MeetingRoomPresenter
Statistics Viewer	StatisticsViewer
Laser Pointer User	WA_LASERPOINTER

For more information on users and authentication, see *Administering Avaya web.alive: Customer premises solution*, which is available on support.avaya.com.

Setting up central users

To set up a centralized user base, you must add the web.alive server to a Windows domain. Typically, an organization's IT department performs this task. Once the web.alive server is on the Windows domain, you must make web.alive aware of the domain details.

Prerequisites

Before you configure web.alive to operate with a central user base, you must add the web.alive server to a Windows domain.

The purpose of this task is to leverage a central user database for web.alive logins.

-
1. Open a Web browser and enter <http://localhost:8080/WAWebService/WAInterface.aspx?op=WASetDefaultLoginDomains> in the **Address** field.
The **WAInterface Web Service** screen displays.
 2. In the **subscriptionId** field, enter 1.
 3. In the **DefaultLoginDomains** field, enter the name of the domain.
 4. Click **Invoke**.
web.alive restarts and an XML response displays, as follows:
 - If the response is true, the configuration is successful and users can now login 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.
-

Consequences for a demilitarized zone (DMZ)

In a typical deployment, you will require access to web.alive for users within your organization and for users in the general public. So, web.alive must be accessible on the public Internet.

To achieve this configuration, you may wish to place the web.alive server in a demilitarized zone (DMZ).

If you require web.alive to be publicly accessible and if you are using a central user base, you must extend the Windows domain into the DMZ. For this configuration to operate successfully, it is likely that you will have to open several ports on the back firewall of the DMZ. Engage with your organization's IT department for more information.

Chapter 9: Upgrading web.alive

About the upgrade

There are two options available to you when you are updating your version of web.alive. The option you choose depends on whether you wish to retain information, such as:

- Users
- Groups
- Environments
- Uploads
- Certificates

Follow the appropriate sequence of tasks, as follows:

Perform these steps if you require a fresh installation of web.alive, without retaining the information above.	Perform these steps if you wish to retain the information above.
<ol style="list-style-type: none">1. Uninstalling web.alive on page 51.2. Preparing your server for a fresh installation of web.alive on page 60.3. Follow the steps to install web.alive, as described here: Installing web.alive on page 37.4. Restoring configuration settings after an upgrade on page 59.	<ol style="list-style-type: none">1. Uninstalling web.alive on page 51.2. Follow the steps to install web.alive, as described here: Installing web.alive on page 37.3. Restoring configuration settings after an upgrade on page 59.

Restoring configuration settings after an upgrade

After you upgrade your instance of web.alive, you must restore a number of configuration settings, such as security certificate settings.

1. Reset the password for the web.alive administrator (`waadmin`), if necessary.

The web.alive upgrade script does not reset the password for `waadmin`. If you manually delete the `waadmin` account and then recreate web.alive, it allocates the original default password to this role (`LP_ko0JI(hu8GY&)`).

2. If you were using a secure SSL connection in the old system, you must reconfigure the SSL and firewall settings in the new system.

For more information, see [Configuring web.alive for SSL](#) on page 70. The web.alive upgrade script preserves the security certificate.

3. If you were using a secure SSL connection in the old system, you must reconfigure the firewall settings in the new system.

For more information, see [Configuring the firewall](#) on page 71.

4. If the old system had a Web root direct, you need to recreate this setting in the new system. For more information, see [Simplifying the URL](#) on page 76.

Preparing your server for a fresh installation of web.alive

In relation to upgrading web.alive, there are two main options available to you:

- You can upgrade to a new server, with the new server having no resemblance to the old server.
- You can upgrade to a new edition of the software, while retaining all your local user and group information.

The steps here are essential if you wish to upgrade to a new server, with the new server having no resemblance to the old server.

Prerequisites

Before you upgrade web.alive, uninstall the previous version.

The purpose of this task is to 'clean up' the server to delete files relating to users, groups, environments, uploads, certificates, and so on..

If you require an entirely fresh install:

- a. Delete the `W:` drive.
- b. Delete all web.alive local users and groups.
- c. Begin the web.alive installation in the normal way.

Chapter 10: Configuring your firewall

Firewall changes

It is very likely that to successfully deploy web.alive in your network, you will have to make some changes on the firewall — on the Windows 2008 firewall, on the subnet/intranet firewall or both.

Related topics:

[web.alive ports](#) on page 61

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

web.alive ports

web.alive uses these ports:

Port	Protocol	Notes
80	TCP	Web traffic, file upload, file download
443	TCP	Tunnelling port and SSL port
2379	UDP	Spatial voice port
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)

The **SetupCPDE.ps1** script opens all of these ports, with the exception of 3389, on the Windows 2008 firewall. You should 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 may require the engagement of your organization's IT department.

The table includes a port for management. You could open a different, less well known port, for additional security.

Big Blue Button ports

The BBB application uses these 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	SSH (for management)

It is likely that the Ubuntu images do not have a local firewall.

If your firewall has a larger scope, you may require the engagement of your organization's IT department.

The table includes a port for management. You could open a different, less well known port, for additional security.

Tunnelling

web.alive 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, 2379, and 21002 is tunnelled through port 443.

Tunnelling also redirects BBB traffic. All BBB traffic intended for ports 80, 1935, and 9123 is first routed to the web.alive server on port 443. Then the web.alive server redirects the traffic to the BBB server on the BBB ports 80, 1935, and 9123. This means that the web.alive server must have visibility of the BBB server on ports 80, 1935, and 9123.



Note:

Avaya supports this configuration but does not recommend it. In particular, tunnelling through proxies can sometimes adversely impact voice quality due to the time latency.

Remote desktop

In order to enable the remote desktop feature, you must open port 3389. You must also enable the remote desktop feature in the operating system.

Related topics:

[Activating the remote desktop feature in the operating system](#) on page 63

Activating the remote desktop feature in the operating system

In addition to opening port 3389, you must enable the remote desktop feature in the operating system.

Prerequisites

Before you activate the remote desktop feature, you must install web.alive.

The purpose of this task is to activate the remote desktop feature.

-
1. On the web.alive server, navigate to **Start > Control Panel > System and Security > System > Remote Settings**.
 2. At the bottom of the dialog, enable remote desktop.
You can secure the remote desktop feature by client version, by user identity, and/or by client address.
The port in the Windows firewall automatically opens.
 3. Click **OK**.
-

Secure shell (SSH)

All BBB servers should have SSH. When you install BBB from the web.alive image, you receive the OpenSSH package. When you install BBB natively, the instructions provided in this document included installing OpenSSH with the initial OS install.

Related topics:

[Configuring web.alive for SSL](#) on page 70

[SSL and trailing slash redirects](#) on page 91

Chapter 11: Setting up secure sockets layer (SSL)

Secure sockets layer

Typically, when you implement SSL, you secure a Web server. In the web.alive solution, you do not secure a Web server. Instead, you secure the entire web.alive solution, using a single certificate.

There are two main tasks involved in this implementation of SSL:

- [Managing your SSL certificate](#) on page 66
- [Configuring web.alive for SSL](#) on page 70

About the WAWebService

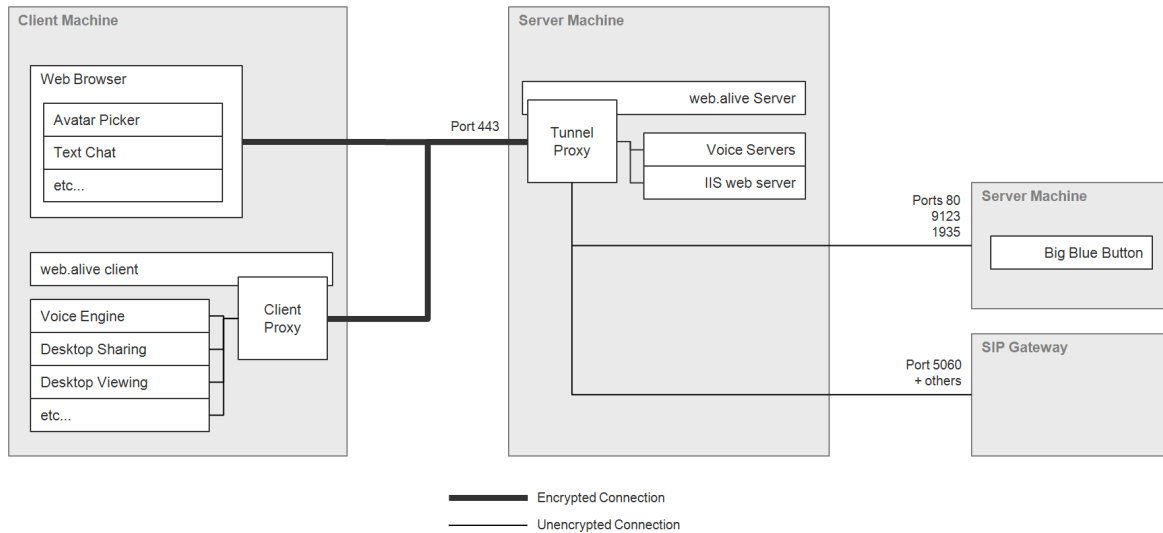
When you install web.alive, you install the WAWebService application. The WAWebService application provides a number of administrative functions for other web.alive applications. It is not available for remote call, but it can be used locally on the server machine. The WAWebService application provides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

Architecture

The web.alive client consists of many components. Some of these components can communicate using SSL and some of the components cannot communicate using SSL. The components that cannot communicate using SSL do not communicate with the web.alive server. Instead, they communicate with a proxy, called the client proxy. The client proxy communicates directly with the web.alive server on their behalf.

The web.alive server also has a proxy, called the tunnel proxy. The tunnel proxy terminates the SSL connections from all sources and routes the communication packets to the appropriate

server-side components of the web.alive solution. The connections behind the web.alive server are not encrypted. Only the web.alive server needs to be SSL-enabled.



Related topics:

[Ensuring that ports are accessible](#) on page 36

Managing your SSL certificate

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

1. Using web.alive, you must generate a request for an SSL certificate. This 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 web.alive, you must install the certificate that you bought.

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

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

web.alive 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 68

[Installing the certificate](#) on page 68

Generating a certificate signing request

Before you approach a CA, you must create a customized request for a certificate. Once you create this request, you can use it to buy a customized certificate.

Prerequisites

Before you generate a certificate signing request (CSR), you must install web.alive.

The purpose of this task is to create a file which you can use to buy a certificate.

-
1. Open a Web browser and enter <http://localhost:8080/WAWebService/WAInterface.aspx?op=CreateCertificateSigningRequest> in the **Address** field. The **WAInterface Web Service** screen displays.
 2. In the **subscriptionId** field, enter 1.
 3. In the **serverFQDN** field, enter the exact FQDN of the server as the client views it.
It must match the information exactly, otherwise there may be errors.
 4. Enter information in all other fields but be aware that the CA will verify your request and may reject it if they are not satisfied with your identity.
Only the **keySize** field is optional. The **keySize** field defaults to 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.
 5. 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.
 6. If the response is true, navigate to `W:\web.alive\1\Certs\CertRequest.csr` to obtain the CSR.
 7. 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. Do not attempt to generate a second CSR at this time.

Next steps

Now you can approach a CA.

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.

Prerequisites

Before you buy a certificate, you must generate a CSR.

The purpose of this task is to create a certificate which you can install on your web.alive server.

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

Next steps

Now, you can install the certificate on the web.alive server.

Installing the certificate

Once you receive the certificate from the CA, you must install it on the web.alive server.

Prerequisites

Before you install the certificate on the web.alive server, you must buy it from a CA.



Note:

Never install certificates on to active servers. Certificate installation results in an disruption in the user experience.

Configuring web.alive for SSL

The process of configuring web.alive for SSL consists of two tasks, which you must complete in sequence:

- Using the web.alive Server Configuration Tool, you must set the HTTPS settings.
- Using the operating system, you must open port 443.

Related topics:

[Secure shell \(SSH\)](#) on page 63

[Configuring web.alive](#) on page 70

[Configuring the firewall](#) on page 71

[SSL and trailing slash redirects](#) on page 91

Configuring web.alive

To configure web.alive, you must open the web.alive 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 web.alive Server Configuration Tool when you installed web.alive and configured your server and subscription.

Prerequisites

Before you configure web.alive, you must obtain and install an SSL certificate.

The purpose of this task is to change many of the web.alive HTTP settings to HTTPS.

-
1. Open the web.alive Server Configuration Tool.
 2. Update the **Web Service Scheme** field to change it from `http` to `https`.
 3. Update the web.alive **Help URL** field to change it from `http` to `https`.
 4. Update the **Image Service Base URL** field to change it 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 of the servers. For more information, see [Installing the image service](#) on page 43.



Note:

Do not update the **WA Web Service URL** and **Proxy Test URL** fields.

5. Click **Configure Server**.
web.alive applies these values to your server. This step is very fast.
6. Click **Configure Subscription**. web.alive applies these values to your account instance. This step can take several moments.

**Tip:**

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

Next steps

Now, you can close all the web.alive ports with the exception of port 443.

Configuring the firewall

The web.alive server is now using SSL. However, you must make some changes to the ports on the firewall to complete the configuration. Specifically, you must close all web.alive ports with the exception of port 443.

Prerequisites

Before you configure the firewall, change the web.alive configuration settings from `http` to `https`.

The purpose of this task is to close all web.alive ports with the exception of a single port — port 443.

-
1. On the web.alive server, navigate to **Start > Administrative Tools > Windows Firewall and Advanced Security**.
 2. Select **Inbound Rules** in the panel on the left.
 3. Set the rules for port 80 to **Blocked**.
There are two active rules for this port.
 4. Set the rules for port 7878 to **Blocked**.
This is the web.alive interaction port and it is particularly important to block this port because it enables the tunnel proxy functionality.
 5. Set the rules for port 2379 to **Blocked**.
This is the voice spatial port.
 6. Set the rules for port 21002 to **Blocked**.

This is the web.alive voice spatial control port.

Next steps

Now, you can make a note of the URLs that your users and administrators will require for access.

This is the URL for your regular web.alive users: <https://<web.alive FQDN>/1/html/index.html>.

This is the URL for your web.alive administrators: <https://<web.alive FQDN>/WAAdminPanel/Login.aspx>.

Related topics:

[URLs](#) on page 49

Troubleshooting certificates

It is important to note that if you use SSL in your web.alive system, you cannot use a Content Distribution Network (CDN) with web.alive. The CDN and the server have different FQDNs and a single certificate cannot secure the solution. To successfully deploy a secure web.alive solution, the server FQDN and the server Web FQDN must be the same.

There are some limitations with regard to the certificate signing request (CSR).

At any given time, you can only have a single CSR in an in-progress state. Do not attempt to generate a second CSR at this time.

However, it is quite common for the CA to fail to verify the CSR. Common causes of a failed validation are:

- 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.

When this happens, you must regenerate the CSR. Before you regenerate the CSR, you must delete the current in-progress CSR.

Related topics:

[Deleting a certificate signing request](#) on page 73

Deleting a certificate signing request

Prerequisites

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

The purpose of this task is to remove the CSR from your server so that you can generate another one.

-
1. Open a Web browser and enter <http://localhost:8080/WAWebService/WAInterface.aspx?op=DeleteCertificateSigningRequest> in the **Address** field. The **WAInterface Web Service** screen displays.
 2. In the **subscriptionId** field, enter 1.
 3. Click **Invoke**.
When the method runs and finishes, the Web page displays an XML response.
 - If the response is true, the CSR has been deleted.
 - If the response is false, the CSR has not been deleted.

Next steps

Now, you can create another CSR, as described in [Generating a certificate signing request](#) on page 67.

Setting up secure sockets layer (SSL)

Chapter 12: Administering web.alive

Backing up

Currently, web.alive does not have an automated back-up procedure. If you wish to back up a web.alive server for later restoration, you must save the following:

- All local groups and users created by the web.alive administration panel, including WAAdmin and WAUploader
- Everything on the `W:` drive

Restoring

Currently, web.alive does not have an automated restore procedure. However, you can restore web.alive using this manual procedure.

Prerequisites

Before you restore your web.alive server, you must back it up first.

The purpose of this task is to reinstall an instance of web.alive.

-
1. Navigate to **Start > Administrative Tools > Services** and stop the following services in the following order:
 - a. WStatsService
 - b. ChainSawService
 - c. DWServer

This DWServer also stops the DWMixer.
 2. Stop the web.alive Web server.
 3. Restore all local users and groups that you have saved in a previous back-up.
 4. Restore the `W` drive that had been saved in a previous back-up.
 5. Restart the web.alive Web server.

6. Start the following services:
 - DWServer
 - DWMixer
7. Open the web.alive Server Configuration Tool and configure the server and the subscription, as described in [Configuring web.alive](#) on page 47



Note:

If you are restoring to a fresh machine, restore the local users, local groups, and **W:** drive first. Then proceed with the installation as normal.

Upgrading

For future releases, Avaya plans to make the upgrade steps available so that you can upgrade from web.alive 2.5 to the next version.

Simplifying the URL

The default web.alive URL includes the subscription ID, <http://<web.alive FQDN>/1/html/index.html>. It is not ideal to provide this information to users. To avoid this situation, you can configure Web root redirects, using your local browser and the WAWebService to replace the full address with the FQDN.

Prerequisites

Before you configure Web root redirects, you must install, configure, and verify your web.alive solution. Only perform this task on a stable system.

The purpose of this task is to replace <http://<web.alive FQDN>/1/html/index.html> with <http://<web.alive FQDN>>.

1. Open a Web browser and enter <http://localhost:8080/WAWebService/WAInterface.aspx?op=WASetupWebRootRedirects> in the **Address** field. The **WAInterface Web Service** screen displays.
2. In the **subscriptionId** field, enter 1.
3. In the **serverWebFQDN** field, enter the FQDN.
4. Click **Invoke**.

web.alive restarts and an XML response displays, as follows:

- If the response is true, the configuration is successful and users can now access web.alive using the FQDN.
- If the response is false, the configuration is unsuccessful and users cannot access web.alive using the FQDN.

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.

6. If the response is true, the new URL for non-SSL solutions is <http://<web.alive FQDN>> and the URL for SSL solutions is <https://<web.alive FQDN>>.

If you switch from an SSL solution to a non-SSL solution or in reverse, you must repeat this task.

Reducing the user limit

In web.alive, the maximum number of users for a server is called Peak Concurrent Users (PCU). By default, Avaya configure each system for 100 users and five administrators. The separate administrator count enables administrators to enter the system even if the system reaches full capacity.

You can reduce the PCU but you cannot increase it without impacting voice quality.

Prerequisites

Before you reduce PCU, you must install, configure, and verify your web.alive solution.

The purpose of this task is to reduce web.alive capacity.

1. Open a Web browser and enter <http://localhost:8080/WAWebService/WAInterface.aspx?op=WAUpdatePCU> in the **Address** field.
The **WAInterface Web Service** screen displays.
2. In the **subscriptionId** field, enter 1.
3. In the **MaxPCU** field, enter the new maximum number of users, such as 80.
4. In the **MaxAdminBuffer** field, enter the new maximum number of administrators.
5. In the **MaxMeetingHosts** field, enter 0.
This field is not supported in the Customer Premises Deployment (CPD).
6. Click **Invoke**.

web.alive restarts and an XML response displays, as follows:

- 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`.

The failure cause is at the bottom.



Note:

Do not perform this task on a system with active users because it requires a server restart. If you use this method to increase the PCU, you are in violation of your Avaya license agreement.

Related topics:

[Licensing](#) on page 14

[Installing Diamondware](#) on page 41

Appendix A: PowerShell Scripts

The set-up script

The PowerShell script, **SetupCPDE.ps1**, performs a number of tasks that automate the configuration of web.alive. This appendix outlines these configuration tasks. Avaya provides this information for your reference and troubleshooting purposes.

Related topics:

[About the web.alive set-up script](#) on page 39

[Host file](#) on page 79

[Partition mapping](#) on page 80

[Directories](#) on page 80

[Local users](#) on page 80

[IIS applications](#) on page 81

[Virtual directories](#) on page 81

[Upload limits](#) on page 82

[Mime types](#) on page 82

[Firewall rules](#) on page 83

[Registry default](#) on page 83

Host file

Avaya has encountered deployments where the FQDN does not map to the IP address of the server on the server itself. This issue causes web.alive to operate incorrectly. To address this issue, Avaya has added the following to the hosts file:

Map from	Map to
"localhost"	127.0.0.1
<hostname>	127.0.0.1
<fqdn>	127.0.0.1

Partition mapping

web.alive requires the second disk to be on the **W** drive. web.alive remaps it as follows:

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

Directories

The **SetupCPDE.ps1** script creates the following directories.

Directory	Notes
C:\WAEFiles	Expected location for the default WAE file. Default.wae is copied 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\WAAAdminPanel	Directory for the administration panel web application.
C:\inetpub\wwwroot\WAFFileExchange	Directory for the File Exchange and Dropbox web application.
C:\inetpub\wwwroot\WAIinsertionUploader	Directory for the web application that uploads files for insertions.
C:\inetpub\wwwroot\WAIImageService	Directory for the Badge web application.
W:\web.alive\avatarBadgePictures	Directory where Badge pictures are stored. The user "Network Service" is given Modify access.
W:\web.alive\WAIImageService	Directory where the Badge web application stores user data. The user "Network Service" is given Modify access.

Local users

The **SetupCPDE.ps1** script creates the following users and groups.

User	In Group	Password	Note
wauploader	IIS_IUSRS (builtin)	<random> 15 characters: At least 2 upper case letters, 2 lower case letters, 2 numbers, and 2 special characters.	IIS Application Pool identity for uploading applications.
waadmin	ServerAdmin	LP_ko0Jl(hu8GY&	Initial identity for accessing the administration panel. Avaya strongly recommends that you update the initial password as soon as web.alive is up and running. In a reinstallation situation where the account already exists, the password is not reset.

When passwords are (re)set, the **SetupCPDE.ps1** script then attempts to set No Password Expiry. If this fails, only a warning is output as this could fail due to policy restrictions.


IIS applications

The **SetupCPDE.ps1** script configures IIS applications, application pools, and Web sites in the following manner. Note the use of a second Web site so that you can place sensitive applications on another port.

Application	Application pools	Identity	Web site	Port
WAAdminPanel	WAAdminPanelAppPool	Local System	Default Web Site	80
WAImageService	WAImageServiceAppPool	Network Service	Default Web Site	80
WAFileExchange	WAUploaderAppPool	wauploader	Default Web Site	80
WAIinsertionUploader	WAUploaderAppPool	wauploader	Default Web Site	80
WAWebService	WAWebServiceAppPool	Local System	Internal	8080

Virtual directories

The following directories are in use.

URL	Mapped to
http://<fqdn>/WAImageService/avatarBadgePictures	W:\web.alive\avatarBadgePictures
http://<fqdn>/<SubscriptionNumber>	W:\web.alive\<SubscriptionNumber>\Web  Note: SetupCPDE.ps1 does not set up this virtual directory. This happens when the subscription is configured.

Upload limits

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

Mime types

The **SetupCPDE.ps1** script adds the following mime Types for web.alive 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
.uz2	application/octet-stream
.lzma	application/octet-stream

Firewall rules

The SetupCPDE.ps1 script adds the following firewall rules to the Windows 2008 firewall. All rules are for incoming ports and 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 Spatial Voice Port	UDP	2379
web.alive Interaction Port	UDP	7878
web.alive Spatial Voice Control Port	TCP	21002

Registry default

As a final step, the **SetupCPDE.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	appshare.avayalive.com
Proxy Test URL	waProxyTestURL	http://www.google.com

The remove script

The PowerShell script, **RemoveCPDE.ps1**, performs a number of tasks that automate the removal of web.alive. You can only run it after you uninstall the web.alive statistics and voice servers. This appendix outlines these configuration tasks. Avaya provides this information for your reference and troubleshooting purposes.

The **RemoveCPDE.ps1** undoes everything that **SetupCPDE.ps1** does with the following clarifying exceptions:

- Not removed: The script does not remove any file from the `W:` drive.
- Not removed: The script does not remove any local users and groups created by the administration panel.
- Not removed: The script does not remove the local users waadmin and wauploader. These users are reflected in the ACLs of files on the `W:` drive.
- Not removed: The script does not remove the local group ServerAdmin.
- Additionally removed: In addition to removing all the Web applications, the script also uninstalls them.
- Additionally removed: The script uninstalls all Web pages installed in the server set-up.
- Additionally removed: The script removes the entities listed in the table below, if they exist.

Type	ID	Created by
Redirect	IIS://localhost/W3SVC/1/Root/index.html In web.alive, the redirect and the redirect file are separate entities that both have to be cleaned. The redirect is held 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

Related topics:

[About the uninstall](#) on page 51

Appendix B: VMware Player

Introduction to VMware Player

For installations in which you are running Big Blue Button (BBB) as a virtual machine on top of a physical web.alive server, Avaya provides the following background material to help you install and use the VMware Player. This material is also applicable to installations in which you are running both the BBB and the web.alive server as virtual machine (VM) images.



Note:

In the following sections, references to a Windows virtual machine always refer to deployments in which both servers are virtual. Avaya often calls this type of installation: Customer Premises Deployment Lite (CPD Lite).

VMware Player

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

Installing VMware Player

For a Windows server; You can easily download and install VMware Player if you have installation rights on your machine. Simply download the executable, double-click it, and complete the installation wizard. You must reboot your machine. You can access VMware Player from the **Programs** menu or from a desktop shortcut.

For a Linux server; The installation is slightly more complex. You must download the bundle file for 64-bit Linux. The following commands are suitable for Ubuntu.

```
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 sudo rights. You do not need to reboot your machine. You can access the VMware Player from **Applications > System Tools > VMware Player**.

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

Using VMware Player

When a virtual machine (VM) is running, VMware Player displays the terminal or windowing 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.

You can enter a Player Console by pressing `Ctrl+G`. You can exit a Player Console by pressing `CTRL+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. If you click into a console, you enter it and if you click outside of a console, you exit 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 `CTRL+Alt` to release.

On Linux Server VMs, you use the keys more frequently. Linux Server has no windowing 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 `CTRL+Alt` to exit and return the mouse.

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

Related topics:

[Starting VMware Player for the first time](#) on page 89

Starting VMware Player for the first time

When you first start the VMware Player, it often displays information messages, such as the following.

Message (paraphrased)	The Avaya 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 it 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?	<ol style="list-style-type: none"> 1. Click Cancel. 2. Open the file system and navigate to the VM files. 3. Delete the *.lck directory. 4. Try again.

Alternatives

The console is convenient but it 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 them. Avaya recommends 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, Avaya recommends an 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 Avaya does not recommend it. The additional resources needed to run the RDP server can adversely impact the VM. By default, RDP is deactivated in the Windows VM.

Appendix C: SSL and trailing slash redirects

SSL and trailing slash redirects

When you use SSL with web.alive, there is a minor issue in which trailing slash redirects do not operate successfully. This issue commonly occurs in the administration panel URL, as follows.

URL	Correct/incorrect
https://<web.alive fqdn>/WAAdminPanel	Incorrect
https://<web.alive fqdn>/WAAdminPanel/	Correct
https://<web.alive fqdn>/WAAdminPanel/Login.aspx	Correct and recommended

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

Avaya has a solution for this issue but has chosen not to include it in the main installation package because Avaya consider the solution to be “larger” than the problem. Stated differently — small problem, big solution.

Avaya includes the following code here for information purposes only. Avaya recommends the URL in the table above.

You can still apply the following to a server in order to enable the redirects to operate successfully.

1. Install the **URL rewrite Module**.

You can download this utility 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>
```

Related topics:

[Secure shell \(SSH\)](#) on page 63

[Configuring web.alive for SSL](#) on page 70

Index

Numerics

443[36](#)

A

activating BBB[21](#)
administration panel[44](#)
architecture[65](#)
ASP.net[35](#)
automatic restart[22](#)

B

backing up[75](#)
BBB[17](#), [21](#), [22](#), [27](#), [31](#)
 activating[21](#)
 automatic restart[22](#)
 native[27](#)
 verifying[22](#)
bridging[17](#)

C

centralized users[54](#)
certificate[68](#)
 installing[68](#)
certificate request[67](#)
clean install[59](#)
concurrent users[77](#)
configuration[47](#), [48](#)
CSR[67](#), [73](#)

D

deployments[11](#)
diamond ware[41](#)
directories[80](#)
DMZ[56](#)

E

environments[49](#)

F

feature[33](#)

file exchange[45](#)
firewall[61](#), [71](#)
firewall rules[83](#)

G

groups[54](#)

H

hardware[12](#)
help[46](#)
host file[79](#)

I

IIS applications[81](#)
image service[43](#)
interaction server[42](#)
introduction[9](#)

L

licensing[14](#)
limitations[10](#)
local users[53](#), [80](#)

M

main pages[46](#)
mime types[82](#)

N

native[31](#)
networking[15](#), [19](#)

O

operating system[14](#)

P

partition mapping[80](#)

partitions	15
PCU	77
ports	36 , 61 , 62
BBB	62
web.alive	61
Powershell	39
preparation steps	38
PuTTY	89

R

registry default	83
remote desktop	62 , 63
remove script	84
restoring	75
role	33

S

scheduled job	25
scope	9
scripts	
remove	84
set-up	79
set up script	39 , 40
set-up script	79
setting up users	56
simple URL	76
single machine deployment	13
skills	16
software	11
SSH	63
SSL	65–68 , 70–72
architecture	65
certificate	66
firewall	71
request	67
troubleshooting	72

Verisign	68
static IP	29
statistics	43

T

trailing slash redirects	91
troubleshooting	48
tunnelling	62
two machine deployment	12

U

Ubuntu	28
uninstall	51 , 52
upgrade	59 , 60
upgrading	76
upload limits	82
URLs	49
user limit	77
users	
centralized	54 , 56
local	53
two options	53

V

verifying BBB	22
Verisign	68
virtual directories	81
Vix	24
VIX	23
vmware	18
VMware Player	87

W

WAWebService	65
Web server	33
web service	45
web.alive	
.zip	37
script	41
Windows Powershell	39