



Deploying IP Office Server Edition and Application Servers

Release 12.0
Issue 31
April 2024

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 in varying media which may include product information, subscription or service descriptions, operating instructions and performance specifications that are generally made available to users of 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 or on the express behalf of Avaya. End user agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End user.

Link disclaimer

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

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Please refer to your agreement with Avaya to establish the terms of the limited warranty. In addition, Avaya's standard warranty language as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: <https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010> under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if the product(s) was purchased from an authorized Avaya channel partner outside of the United States and Canada, the warranty is provided by said Avaya Channel Partner and not by Avaya.

"Hosted Service" means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE). THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, [HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO](https://support.avaya.com/licenseinfo) UNDER THE LINK "Avaya Terms of Use for Hosted Services" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE

TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

The Global Software License Terms ("Software License Terms") are available on the following website <https://www.avaya.com/en/legal-license-terms/> or any successor site as designated by Avaya. These Software License Terms are applicable to anyone who installs, downloads, and/or uses Software and/or Documentation. By installing, downloading or using the Software, or authorizing others to do so, the end user agrees that the Software License Terms create a binding contract between them and Avaya. In case the end user is accepting these Software License Terms on behalf of a company or other legal entity, the end user represents that it has the authority to bind such entity to these Software License Terms.

Copyright

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

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Unless otherwise stated, each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpegla.com).

Service Provider

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE H.264 CODEC OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpegla.com).

Compliance with Laws

You acknowledge and agree that it is Your responsibility to comply with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

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, please contact your Avaya Sales Representative.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of <https://support.avaya.com/security>.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (<https://support.avaya.com/css/P8/documents/100161515>).

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, 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, Hosted Service(s) 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 LLC.

All non-Avaya trademarks are the property of their respective owners.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

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

Contact Avaya Support

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

Contents

Part 1: Introduction	9
Chapter 1: Purpose	10
Deploying an IP Office Server Edition Solution	11
Licenses and Subscriptions	11
Licenses	12
Subscriptions	12
Default parameters	13
Server Types and Roles	14
Virtual IP Office Servers	15
Server Edition Network	15
Small Community Network Support	16
Additional Documentation	17
Chapter 2: Subscriptions	18
Ordering Subscriptions	18
Trial Mode	19
User Subscriptions	19
Application Subscriptions	20
Customer Operations Manager (COM)	21
Subscription Connection Operation	22
Subscription Network Requirements	23
Subscription Mode Ports	24
Migrating Existing IP Office Systems to Subscription Mode	25
Part 2: Server Software Installation	26
Chapter 3: Server Software Installation	27
Adding and Configuring Additional Hard Disks	27
Downloading the Software	28
Creating a bootable USB key	29
Downloading the Avaya USB Creator Tool	29
Creating a USB Drive using the Avaya USB Creator	29
Creating a USB Drive using Rufus	30
Creating a bootable DVD	31
Installing the software manually (DVD/USB)	32
Installing the software manually (USB)	34
Igniting the server	35
Part 3: Primary Server Installation	39
Chapter 4: Primary Server Installation and Initial Configuration	40
Primary server initial configuration using Web Manager	40
Primary server initial configuration using IP Office Manager	42

Chapter 5: The Setup Wizard/Initial Configuration	45
Setup Wizard: Panels Summary.....	46
Setup Wizard: System Panel (Initial Configuration Utility).....	47
Setup Wizard: VoIP.....	51
Setup Wizard: Voicemail.....	55
Setup Wizard: Subscription.....	57
Setup Wizard: Licensing.....	58
Setup Wizard: User.....	58
Setup Wizard: Groups.....	58
Setup Wizard: Lines.....	58
Setup Wizard: Incoming Call Routes.....	59
Setup Wizard: Outgoing Call Routes.....	60
Chapter 6: Subscription and COM Support Setup	61
Checking the System Subscriptions.....	61
Enabling COM Support on Server Edition Systems.....	62
Enabling Additional COM Support Settings.....	63
Setting All Servers to Subscription Mode.....	64
Chapter 7: Server PLDS Licensing	65
Adding the PLDS License File.....	65
Assigning PLDS licenses.....	66
Part 4: Secondary Server Installation	68
Chapter 8: Secondary Server Installation and Initial Configuration	69
Adding a Secondary server using Web Manager.....	69
Adding a Secondary server using Manager.....	71
Enabling COM Support on Server Edition Systems.....	74
Assigning PLDS licenses.....	74
Part 5: Expansion Server Installation	76
Chapter 9: Expansion Server (Linux) Installation and Initial Configuration	77
Adding an Expansion Server Using Web Manager.....	77
Adding an Expansion Server Using Manager.....	79
Enabling COM Support on Server Edition Systems.....	82
Assigning PLDS licenses.....	82
Chapter 10: Expansion Server (IP500 V2) Initial Configuration	84
Initial IP500 V2 Configuration using Web Manager.....	84
Initial IP500 V2 Configuration using Manager.....	86
Adding an IP500 V2 Expansion using Web Manager.....	88
Adding an IP500 V2 Expansion using Manager.....	89
Enabling COM Support on Server Edition Systems.....	90
Assigning PLDS licenses.....	91
Part 6: Application Server Installation	92
Chapter 11: Application Server Installation	93

Service User Configuration for COM Support.....	93
Application Server Initial Configuration.....	94
Chapter 12: Application Server configuration in a Server Edition network.....	96
Disabling the local portal service.....	96
Entering the address of the remote portal service.....	97
Adding the application server to the network.....	97
Chapter 13: Application Server Configuration for IP500 V2 Support.....	99
Part 7: Application Configuration.....	100
Chapter 14: Voicemail Server Configuration	101
Configuring Voicemail Pro.....	101
Adding TTS Languages.....	102
Downloading and installing the Voicemail Pro client.....	103
Enabling Voicemail Pro client connection.....	103
Logging into Voicemail Pro server.....	104
Backing up and restoring voicemail.....	105
Backing up Voicemail Pro.....	105
Restoring Voicemail Pro stored on IP Office Server Edition server.....	105
Migrating Voicemail Pro to IP Office Server Edition.....	106
Chapter 15: one-X Portal Configuration.....	110
one-X Portal Service Initial Configuration.....	110
Configuring portal users.....	112
Administering a standalone portal server.....	112
If the Portal Server Status Remains Yellow.....	113
Chapter 16: Avaya one-X Portal WebRTC Configuration.....	115
Enabling the WebRTC Service.....	115
Enable SIP Support.....	116
Configuring the WebRTC Gateway.....	116
Testing and Logging WebRTC.....	118
Setting the Server's Logging Level.....	119
Downloading Server Log Files.....	119
Viewing WebRTC Log Messages.....	119
Running the WebRTC Test Application.....	120
WebRTC External Client Access.....	120
Part 8: Backup/Restore.....	122
Chapter 17: Backup and Restore.....	123
Backup and restore policy.....	124
Backup and restore protocols.....	125
Enabling HTTP backup support.....	125
Disk space required for backups.....	126
Checking the backup server's backup quota.....	127
Backup data sets.....	127
Creating a remote server connection.....	129

Backing up a server/servers.....	129
Restoring from the backup server.....	130
Restoring a failed server.....	131
Part 9: Upgrading Servers.....	133
Chapter 18: Server Upgrades.....	134
Upgrade methods.....	134
Upgrade policy.....	135
Server Edition downgrade policy.....	137
Chapter 19: Upgrading systems using an ISO file transfer.....	139
Transferring the ISO File.....	139
Transferring an ISO file from a remote file server.....	139
Transferring an ISO file using a browser.....	140
Transferring an ISO file via SSH.....	141
Transferring an ISO file from a DVD.....	142
Transferring an ISO file from a USB Key.....	142
Upgrading using a transferred ISO file.....	143
Chapter 20: Upgrading the system using a bootable DVD.....	145
Chapter 21: Upgrading using a USB key.....	147
Part 10: Server Maintenance.....	148
Chapter 22: Configuration.....	149
Administration tools.....	149
Starting Web Manager.....	149
Accessing the Server's Web Control Menus.....	150
Starting IP Office Manager.....	150
Setting a login warning banner.....	151
Chapter 23: General Maintenance.....	153
Changing the Server Date and Time Settings.....	153
Checking the Services.....	154
Rerunning the Initial Configuration Menu.....	156
Chapter 24: Changing Server Password.....	157
Synchronizing the system service users and passwords.....	157
Changing the Administrator password using Web Manager.....	158
Changing the root user password.....	158
Changing the common Administrator passwords using IP Office Manager.....	159
Chapter 25: Log Files.....	160
Viewing the Debug log files.....	160
Configuring syslog files.....	160
Viewing the syslog records.....	161
Configuring the age of the log files.....	162
Downloading the log files.....	162
Chapter 26: Shutting Down/Restarting Servers.....	164

Shutting down an IP500 V2 Expansion.....	164
Shutting Down a Linux Server Using Web Manager.....	165
Shutting down a server using Web Control.....	165
Removing a Secondary server.....	166
Removing an expansion system.....	166
Chapter 27: Changing Server Addresses.....	167
Changing the IP Address of the Primary Server.....	167
Changing the IP Address of a Secondary or Expansion Server.....	168
Chapter 28: Hardware Replacement	170
Replacing IP500 V2 system.....	170
Replacing System SD Card.....	171
Replacing an IP 500 V2 Field Replacable Unit.....	171
Replacing a Linux server.....	172
Chapter 29: Troubleshooting.....	174
Warning message.....	174
“IP Office is under Server Edition Manager Administration”.....	175
Resetting a server's security settings.....	175
All systems online in Web Manager but unable save configurations from Manager.....	177
All systems online in Manager but offline in Web Manager/Web Control.....	177
Debugging steps.....	177
Logging in as a root user.....	178
Checking memory usage.....	179
IP Office Server Edition certificates.....	181
Identity certificates.....	181
After failback, the H323 phones do not automatically register back to the original server.....	182
Unable to export template.....	182
Expansion users disconnected from portal when the system registers SIP phones.....	183
Part 11: Appendix.....	184
Chapter 30: IP Office LAN support.....	185
IP Office LAN differences.....	185
IP Office LAN features.....	185
Part 12: Further Help.....	189
Chapter 31: Additional Help and Documentation.....	190
Additional Manuals and User Guides.....	190
Getting Help.....	190
Finding an Avaya Business Partner.....	191
Additional IP Office resources.....	191
Training.....	192

Part 1: Introduction

Chapter 1: Purpose

This document covers the processes for installing and maintaining Linux-based IP Office servers. That is:

- Primary, secondary and non-expansion IP500 V2 servers in an IP Office Server Edition or Select network.
- An IP Office Application server to support a IP500 V2 system.

This document covers installation of a pre-built server supplied by Avaya or installation onto a physical server. For installation of IP Office as a virtualized servers, refer also to the "[Deploying Avaya IP Office Servers as Virtual Machines](#)" document.

Related links

[Deploying an IP Office Server Edition Solution](#) on page 11

[Licenses and Subscriptions](#) on page 11

[Default parameters](#) on page 13

[Server Types and Roles](#) on page 14

[Virtual IP Office Servers](#) on page 15

[Server Edition Network](#) on page 15

[Small Community Network Support](#) on page 16

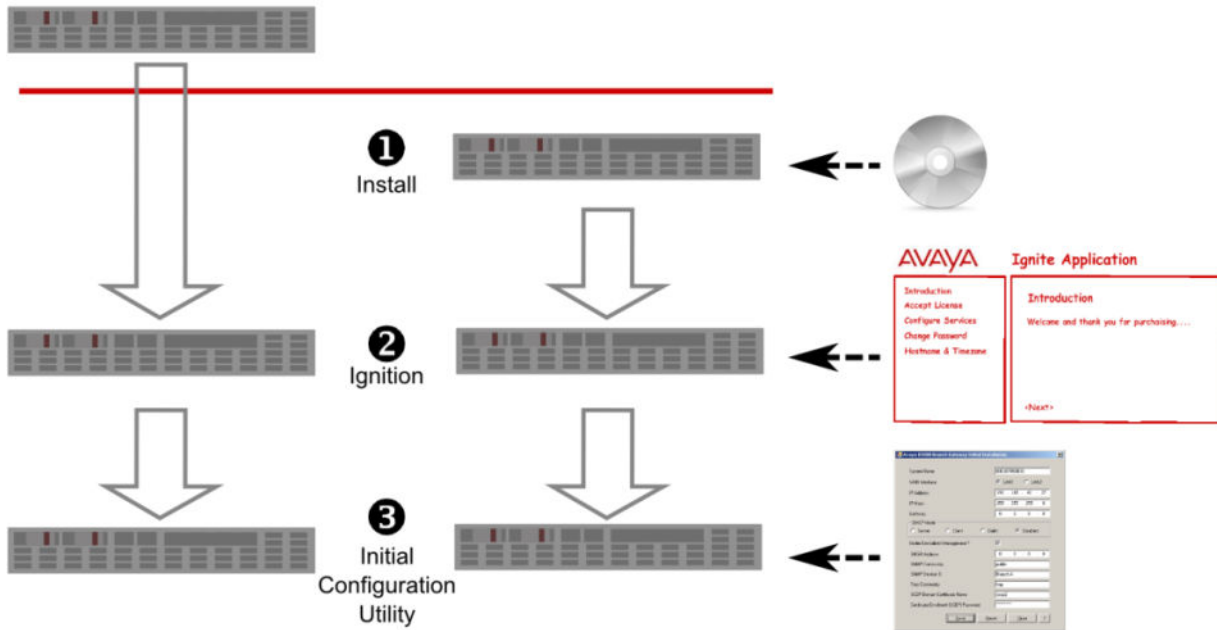
[Additional Documentation](#) on page 17

Deploying an IP Office Server Edition Solution

About this task

AVAYA Supplied Hardware

Non-Avaya Supplied Hardware
(Controlled introduction only)



You can install the software for an IP Office Server Edition Solution only on the servers that Avaya supports. Avaya does not provide support for Server Edition software that you install on any other servers. For more information, about the servers that Avaya supports, see *IP Office Server Edition Reference Configuration*.

Related links

[Purpose](#) on page 10

Licenses and Subscriptions

The entitlements necessary to run specific features on the primary server are provided through the installation of licenses or subscriptions. For a primary server in a network, those entitlements are shared with other servers within the network.

The two method of granting these entitlements are:

- **PLDS Licenses**

These entitlements are supplied in an XML file which is uploaded to the primary server. Though the server configuration of each server in the network, you can then allocate particular numbers of licenses to each server. See [Licenses](#) on page 12.

- **Subscriptions**

Purpose

Subscriptions are entitlements requested from an Avaya subscription server. They are per-month and per-user entitlements, purchased for a set period such as 6-months or 1-year. See [Subscriptions](#) on page 12.

In both cases, the licenses or subscriptions are validated against a value unique to the particular primary server. Depending on the method being used, either its **WebLM ID** or its **PLDS ID**.

- For servers supplied by Avaya, those values are printed on the server packaging and the server itself.
- For non-Avaya servers, the values are shown on the ignition login menu following software installation and should be noted.

The above means that the stage at which licenses or subscriptions for a particular primary server can be obtained varies:

- For Avaya servers, licenses or subscriptions can be requested before installation.
- For non-Avaya servers, licenses or subscriptions can only be requested once server ignition has been performed.

Related links

[Purpose](#) on page 10

[Licenses](#) on page 12

[Subscriptions](#) on page 12

Licenses

These entitlements are supplied in an XML file which is uploaded to the primary server. Though the server configuration of each server in the network, you can then allocate particular numbers of licenses to each server.

The license file is normally valid for a particular release of IP Office software and its service/feature packs. However, more major upgrades required a new license file.

Related links

[Licenses and Subscriptions](#) on page 11

Subscriptions

Subscriptions are entitlements requested from an Avaya subscription server. They are per-month and per-user entitlements, purchased for a set period such as 6-months or 1-year.

Subscriptions can be divided into two main groups; user subscriptions and application subscriptions for selected applications. The user subscriptions are allocated through the individual user configurations.

Ordering Subscriptions

Subscription for an **Server Edition – Subscription** mode system are ordered from the Avaya Channel Marketplace, using the primary server's **PLDS ID**.

After ordering the subscriptions, details of the customer number and address of the subscription server are supplied in an email. Those details are required during the initial system configuration.

Subscription Operation

In order to use subscriptions, the system must have:

- An internet connection.
- An accurate SNTP source (the default used is `time.google.com`).
- An IP route to the customer network's default gateway for external internet traffic.
- The IP address of the customer network's DNS server.

During operation:

- If connection to the subscription server is lost, the system continues running with the existing subscription entitlements it has received for 30-days.
- If when connected, any subscriptions expire, the feature or features associated with the expired subscriptions cease operation immediately.
 - The person responsible for the subscriptions must ensure that they are aware of all subscription expiry dates and that they renew subscriptions in a timely manner, including allowing time for any renewal orders to be processed.

Related links

[Licenses and Subscriptions](#) on page 11

Default parameters

They are as number of scenarios where the server has a set of default parameters applied:

- Pre-built servers supplied by Avaya
- Servers installed from an automatic installation USB key
- Servers installed from a virtual server OVA file

The default parameters server settings are:

Parameter	Value
Language for installation	US English
Keyboard for the system	US English
Hostname	MAC_HOSTNAME: : 00:AE:EF:00:00:00
System eth0	<ul style="list-style-type: none"> • Connection name: eth0 • IP address: 192.168.42.1 • Netmask: 255.255.255.0 • Gateway: 0.0.0.0

Table continues...

Purpose

Parameter	Value
System eth1	<ul style="list-style-type: none">• Connection name: eth1• IP address: 192.168.43.1• Netmask: 255.255.255.0• Gateway: 0.0.0.0
Root Password	Administrator

Related links

[Purpose](#) on page 10

Server Types and Roles

The IP Office software installed using the processes in this documentation can perform a number of different IP Office server roles. The particular role is selected during the installation process. The following is a general summary of the different IP Office servers.

Server	Descriptions	Services
Primary Server	This Linux-based IP Office server is the mandatory component of any Server Edition network. It performs licensing/subscription control for all other servers in the network and is the host for most application services.	IP Office Avaya one-X Portal Voicemail Pro Media Manager Collaboration Server
Secondary Server	This Linux-based IP Office server is similar to the primary and for a range of resilience scenarios it can temporarily take over many of the functions of the primary server.	IP Office Avaya one-X Portal Voicemail Pro
Expansion Server (L)	This Linux-based server is used to support additional IP telephony connections with a Server Edition Network. For example, to provide local IP telephony support at different location than the existing primary and secondary server. This helps network performance and resilience.	IP Office
Expansion Server (V2)	This is the Avaya proprietary hardware based version of IP Office, called IP Office IP500 V2. When used as an expansion server in an Server Edition network, it allows the connection of non-IP based trunks and telephones to that network. Its installation is not covered by this document, other than how to connect the server to a Server Edition network.	IP Office

Table continues...

Server	Descriptions	Services
IP Office Application Server	<p>The Linux-based IP Office server is used to provide support to the IP Office telephony service running on another server.</p> <ul style="list-style-type: none"> • When used to support a standalone or SCN networked IP Office, it can support all the services indicated. • When used to support a Server Edition primary or secondary, only one-X Portal is supported. 	<p>Avaya one-X Portal</p> <p>Voicemail Pro</p> <p>Media Manager</p> <p>Collaboration Server</p>

Related links

[Purpose](#) on page 10

Virtual IP Office Servers

The software installation sections of this document cover the installation of IP Office software onto physical server PCs. That being done using the ISO file provided by Avaya.

IP Office software can also be installed onto virtual server PCs running on various different virtual server platforms. For example; VMware, Microsoft Hyper-V, Azure, and Amazon Web Services (AWS). However, this is not done using the ISO file. Instead different installation packages are provided for each different type of virtual server platform.

For details, refer to [Deploying Avaya IP Office Servers as Virtual Machines](#).

Related links

[Purpose](#) on page 10

Server Edition Network

The main hub of an IP Office Server Edition network is the mandatory primary server. That is a Linux-based IP Office server supporting both IP telephony and a range of supporting application services for the telephony users.

The network is then expanded using the optional secondary server and expansion servers. These provide additional features and direct support for IP telephony services in different physical locations.

In addition, in some scenarios an IP Office Application server can be used to support the primary and/or secondary server. For details of the server roles, see [Server Types and Roles](#) on page 14. For details of capacity support, see [Avaya IP Office™ Platform Guidelines: Capacity](#).

 **Important:**

- All additional servers in the network must be configured to the same licensing mode as the primary server, that is **Server Edition**, **Server Edition - Select** or **Server Edition - Subscription**.

Related links

[Purpose](#) on page 10

Small Community Network Support

When used to support a network of IP500 V2 systems, the IP Office Application server is subject to the following

one-X Portal for IP Office

A Small Community Network only supports a single Avaya one-X Portal server. The application can support up to 500 simultaneous Avaya one-X Portal users.

Voicemail Pro

In an Small Community Network, one Voicemail Pro server stores all mailboxes and their related messages, greeting and announcements. Additional Voicemail Pro servers installed in the network perform other specific roles. For full details, refer to the Voicemail Pro manual (see [Administering IP Office Voicemail Pro](#)).

Setting	Description
Centralized Voicemail Server	<p>In the network, one Voicemail Pro server acts as the centralized voicemail server for all IP Office systems. This server stores all mailboxes and their related messages, greeting and announcements. This is mandatory regardless of the presence of any additional options below.</p> <p>The IP Office associated with the centralized server holds the licenses for voicemail server support. The other servers in the network do not require any voicemail licenses in order to use this server as their voicemail server.</p>
Fallback IP Office	<p>Without needing to install another Voicemail Pro server, you can configure the IP Office hosting the centralized voicemail server such that, if for any reason it is stopped or disabled, the centralized voicemail server accepts control from another IP Office in the network.</p>
Distributed Voicemail Servers	<p>You can install additional Voicemail Pro servers and associated these with other IP Office systems to provide call services for those systems. For example to record messages, play announcements. However, any messages they record are automatically transferred to and stored on the centralized server. The IP Office associated with the distributed server requires the appropriate licenses for voicemail server support.</p>

Table continues...

Setting	Description
Backup Voicemail Server	<p>You can specify an additional voicemail server as the backup server for the centralized server. If for any reason the voicemail application on the centralized server is stopped or disabled, the centralized IP Office will switch to using the backup voicemail server for its voicemail functions.</p> <ul style="list-style-type: none"> • During normal operation the centralized and backup voicemail servers automatically exchange information about mailboxes and voicemail service configuration. • The backup voicemail server uses the licenses provided by the centralized IP Office. A distributed server cannot also be used as a backup server and vice versa.

Related links

[Purpose](#) on page 10

Additional Documentation

For a list of IP Office manuals and user guides, refer to [Avaya IP Office™ Platform Manuals and User Guides](#).

The following additional documentation are useful references for planning the server installation:

- [Avaya IP Office™ Platform Guidelines: Capacity](#)
- [IP Office Resilience Overview](#)
- [Deploying Avaya IP Office Servers as Virtual Machines](#)
- [Administering Avaya IP Office™ Platform with Manager](#)
- [Administering Avaya IP Office™ Platform with Web Manager](#)
- [Administering Avaya IP Office™ Platform Media Manager](#)
- [Administering IP Office Voicemail Pro](#)
- [IP Office SIP Telephone Installation Notes](#)
- [Avaya IP Office™ Platform H.323 Telephone Installation](#)

Related links

[Purpose](#) on page 10

Chapter 2: Subscriptions

Subscriptions are monthly paid entitlements. They can be divided into two main groups;

- per-user per-month user subscriptions
- per-month application subscriptions for selected applications.

In practice, subscriptions are purchased for a specific duration. For example; 6-months, 1-year, 3-years.

During operation:

- If connection to the subscription server is lost, the IP Office system continues running with the existing subscription entitlements it has already received for 30-days.
- If when connected, any subscription expires, the feature or features associated with the expired subscriptions cease operation immediately.
 - The person responsible for ordering subscriptions must ensure that they are aware of subscription expiry dates. They must renew subscriptions in a timely manner, including time for renewal orders to be processed.

Related links

[Ordering Subscriptions](#) on page 18

[Trial Mode](#) on page 19

[User Subscriptions](#) on page 19

[Application Subscriptions](#) on page 20

[Customer Operations Manager \(COM\)](#) on page 21

[Subscription Connection Operation](#) on page 22

[Subscription Network Requirements](#) on page 23

[Subscription Mode Ports](#) on page 24

[Migrating Existing IP Office Systems to Subscription Mode](#) on page 25

Ordering Subscriptions

Subscription for an IP Office subscription mode system are ordered from the Avaya Channel Marketplace. The subscriptions are ordered against the PLDS ID of the IP Office system.

After ordering the subscriptions, details of the customer number and address of the subscription server are supplied in an email. Those details are required during the initial system configuration.

- The person responsible for ordering subscriptions must ensure that they are aware of subscription expiry dates. They must renew subscriptions in a timely manner, including time for renewal orders to be processed.

Related links

[Subscriptions](#) on page 18

Trial Mode

When ordering an IP Office subscription system through the Avaya Channel Marketplace, trial mode can be selected. Trial mode enables the IP Office to operate for up to 30-days using free subscriptions.

- The trial mode IP Office system indicates that it is in 30-day subscription error mode in applications such as the System Status Application and through system alarms.
- Before the 30-day trial period ends, the subscriber can return to Avaya Channel Marketplace and request a conversion to paid-subscriptions mode.

Important:

- To avoid any interruptions to customer telephony services, you must request the change to paid-subscriptions before the end of the 30-day trial period. That request must include allowance for sufficient working time to implement the request.

Related links

[Subscriptions](#) on page 18

User Subscriptions

Each user on the system requires a subscription. All subscribed users are then able to use an the system's telephone extension (analog, digital or IP) and voicemail features. The following user subscriptions can be ordered: **Telephony User**, **Telephony Plus User** and **Unified Communications User**. The subscriptions are applied to individual users through their **User Profile** setting.

Feature	Subscription Mode		
	Telephony User	Telephony Plus User	Unified Communications User
one-X Portal Services	–	–	✓

Table continues...

Feature	Subscription Mode		
	Telephony User	Telephony Plus User	Unified Communications User
Telecommuter options	–	–	✓
UMS Web Services	–	–	✓
TTS for Email Reading	–	–	✓
Remote Worker	✓	✓	✓
Avaya Workplace Client	–	✓ ^[1]	✓
WebRTC	–	–	✓
Mobility Features	–	–	✓

- By default, users on a new or defaulted system are configured a **Telephony User** users.
- Users without a subscription are shown as **Non-licensed User** and cannot use any system features.
- If there are insufficient subscriptions for the number of users configured to a particular profile, some of those users will not receive any services. On suitable Avaya phones, they display as logged out and an attempt to log in displays a no license available warning.
 1. Only supports Avaya Workplace Client basic mode (telephony and local contacts only).

Related links

[Subscriptions](#) on page 18

Application Subscriptions

The following application subscriptions can be ordered for a IP Office subscription system:

Subscription	Description
Receptionist Console	This subscription is used to enable the IP Office SoftConsole application to answer and redirect calls. The number of subscriptions allows the matching number of users to be configured as IP Office SoftConsole users. Those users still require a user subscriptions for their telephone connection (IP Office SoftConsole is not a softphone).
Avaya Call Reporter	This subscription enables support for the Avaya Call Reporter application, hosted on a separate server.
Avaya Contact Center Select	This subscription enables support the Avaya Contact Center Select (ACCS) service hosted on a separate server.

Table continues...

Subscription	Description
Media Manager	This subscription enables support for Media Manager. This can either be locally hosted on an IP Office Application Server or provided centrally by the same cloud-based servers providing the system's subscriptions. In either case: <ul style="list-style-type: none"> • A local Voicemail Pro service running on an IP Office Application Server is used to do the actual recording. • The recordings are then collected by the Media Manager service for archiving.
Third-Party CTI	This subscription enables support for CTI connections by third-party applications. This includes DevLink, DevLink3, Third-party TAPI and TAPI WAV.

Related links

[Subscriptions](#) on page 18

Customer Operations Manager (COM)

IP Office subscription services are a set of cloud-based services provided by Avaya to support IP Office subscription systems. A separate set of these services is provided for each geographic region to support Avaya business partners and their customer systems in that region.

The key service is Customer Operations Manager (COM). COM provides:

- Subscriptions to the IP Office systems.
- Displays the status of the IP Office systems and information about current alarms, type of system, software level.
- Each business partner has an account that allows them to access COM but only see their own customer's systems. They can create additional COM user accounts and control which of their customer systems those accounts can see.
- Avaya have access to COM for their support staff in order to manage the COM services and to assist business partners when required.
- COM can provide the files used to customize various features such as phone background and screen saver images. This can be configured to provide common files to all the business partner's systems or individual files to individual end-customer systems.
- COM can act as the file server for firmware files used by Vantage phones and Avaya Workplace Client.
- For full documentation of COM, refer to the [Using Customer Operations Manager for IP Office Subscription Systems](#) manual.

Additional Support Features

A number of additional support services can be enabled through settings in the IP Office system configuration.

Feature	Description
Remote Backup/Restore	Subscription systems can automatically upload daily backups to the cloud. In addition, COM operators can perform both manual backups and restores operation
Remote Upgrade	Avaya provide COM with updated IP Office software images. COM operators can use these to perform immediate or scheduled system upgrades.
Log File Collection	Subscriptions systems can automatically upload all available log files to the cloud each day.
Centralized Management	Administrator connections for IP Office Web Manager, SysMonitor and System Status Application can be routed through COM to the customer's IP Office systems. The connects use the TLS tunnel used for the subscriptions.
Remote Access	Connections for HTTPS and SSH/SFTP connection can also be routed through COM to the customer IP Office systems. The connects use the TLS tunnel used for subscription.
Co-located Servers	When remote access is enabled, access to other servers and services on the same network as the customer IP Office system can be enabled. That includes access to non-IP Office servers and services subject to their own authentication.

Related links

[Subscriptions](#) on page 18

Subscription Connection Operation

The connection between the IP Office and COM operates are follows:

Outgoing Connection

For the connection from the IP Office to COM:

- The destination is a single static IP address resolved by DNS of the subscription server address entered during the system's initial configuration.
- The IP Office alternates between TCP ports 443 and 8443 until successful.
- The link uses the HTTP 'WebSocket' protocol and TLS 1.2 with mutual authentication.
- The link carries a regular heartbeat, subscription information and basic details of the IP Office system (type of servers and software version).
- All other traffic on the link is controlled by the IP Office system settings; there are no access controls elsewhere.
- If the link is interrupted, the IP Office system goes into a 30-day error mode with daily alarms.
 - If connection to the subscription server is lost, the IP Office system continues running with the existing subscription entitlements it has received for 30-days.
 - During the error mode period, all operations and features are unaffected. The system outputs daily alarms in the system logs.
 - Successful reconnection clears the alarms and error mode.
 - If the 30-day error mode period expires, all subscription features and telephony are deactivated.

- If when connected, any subscriptions expire, the feature or features associated with the expired subscriptions cease operation immediately.
- • The person responsible for ordering subscriptions must ensure that they are aware of subscription expiry dates. They must renew subscriptions in a timely manner, including time for renewal orders to be processed.

Incoming Connection

All incoming traffic from COM is routed to the IP Office through the existing subscription connection established above. It should not require any additional configuration on the customer network if the system has successfully obtained its subscriptions.

Related links

[Subscriptions](#) on page 18

Subscription Network Requirements

In order to obtain its subscriptions and to be remotely monitored and managed through COM, the IP Office system requires the following:

Feature	Description										
Subscription details	<p>Details of the customer ID and subscription server address are provided by email. Those details are entered during the system's initial configuration.</p> <ul style="list-style-type: none"> • For an IP500 V2 SCN, each IP500 V2 requires a License Server Link. • For a Server Edition deployment, only the Primary server has a License Server Link. 										
Internet access	<p>The system needs to be able to access the external internet. This is normally achieved during initial configuration of the system by entering the default gateway address of the outgoing router on the customer network.</p> <ul style="list-style-type: none"> • That value is used to configure a default IP route in the system configuration with the following settings: <table border="1" data-bbox="418 1318 1469 1600"> <thead> <tr> <th>IP Route Setting</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>IP Address</td> <td>0.0.0.0</td> </tr> <tr> <td>IP Mask</td> <td>0.0.0.0</td> </tr> <tr> <td>Gateway IP Address</td> <td>The address of the external network router on the customer network</td> </tr> <tr> <td>Destination</td> <td>The IP Office LAN interface (LAN1 or LAN2) which is connected to the customer network.</td> </tr> </tbody> </table> <ul style="list-style-type: none"> • Maximum round trip delay 200ms. • Minimum connection bandwidth 128kb/s. • If the customer firewall or router controls the ports used for outgoing internet access, ensure that outgoing HTTPS traffic on TCP ports 8443 and 443 are allowed. 	IP Route Setting	Value	IP Address	0.0.0.0	IP Mask	0.0.0.0	Gateway IP Address	The address of the external network router on the customer network	Destination	The IP Office LAN interface (LAN1 or LAN2) which is connected to the customer network.
IP Route Setting	Value										
IP Address	0.0.0.0										
IP Mask	0.0.0.0										
Gateway IP Address	The address of the external network router on the customer network										
Destination	The IP Office LAN interface (LAN1 or LAN2) which is connected to the customer network.										

Table continues...

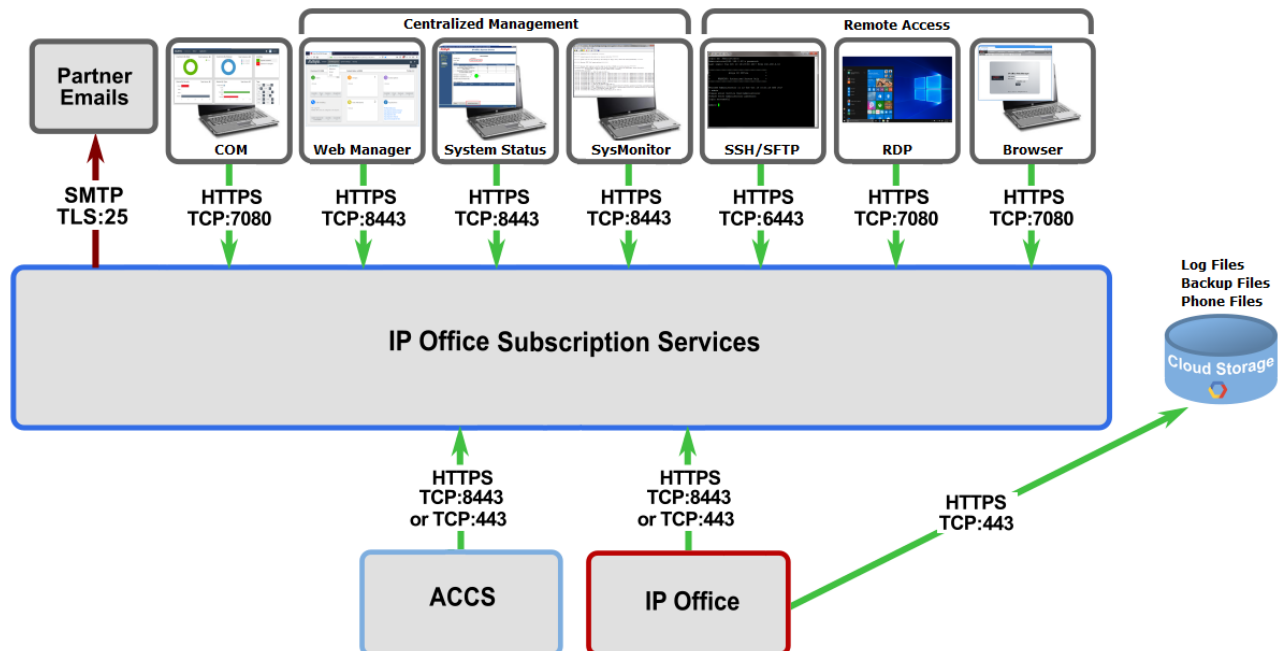
Feature	Description
DNS Service	<p>The address of the customer's DNS server or service. If the customer does not have a specific DNS service, then use 8.8.8.8.</p> <p>If the customer has their own DNS server:</p> <ul style="list-style-type: none"> • Ensure that it is configured to allow external access to addresses in the <code>avaya-sub.com</code> domain. That domain is used to the COM servers that support subscription systems in various geographic regions. For example: <code>admin.uk1.avaya-sub.com</code>. • Ensure that it is also configured to allow external access to <code>storage.googleapis.com</code>. This address is used for subscription features that require access to file storage.
Time source	<p>Subscriptions requires an accurate time source. The recommendation is to use the Google time service at <code>time.google.com</code>. The system's time zone should also be set correctly.</p>
COMAdmin Security User	<p>The connection from the system to COM uses the security settings of the COMAdmin service user account in the IP Office system's security settings. This account is created by default on new and default systems.</p>

Related links

[Subscriptions](#) on page 18

Subscription Mode Ports

The following schematic shows the ports used for connections to and from the subscription service running on COM.



Related links[Subscriptions](#) on page 18

Migrating Existing IP Office Systems to Subscription Mode

The process for migrating an existing IP Office Essential Edition or Preferred Edition system to IP Office system is can be performed by rerunning the initial configuration menu. The assumed mapping of existing user profiles to their subscription equivalents is as follows:

Essential/Preferred Edition Mode	Subscription Mode
Non-Licensed User	Non-Licensed User
Basic User	Telephony User
Mobile User	
Office Worker	UC User
Power User	

Related links[Subscriptions](#) on page 18

Part 2: Server Software Installation

Chapter 3: Server Software Installation

The following stages outline installing the software for a Linux-based IP Office server.

- This is a general process for all types of IP Office server, that is - primary, secondary, expansion and application server. The server's specific role is selected during the final ignition stage.
- If using a pre-built IP Office server, proceed directly to software ignition (see [Igniting the server](#) on page 35) using the default IP address settings (see [Default parameters](#) on page 13),

Network Installation

If the server is intended to be part of a network of IP Office servers, then install the servers in the following order:

1. Primary server
2. Secondary server (if required)
3. Expansion servers

Related links

[Adding and Configuring Additional Hard Disks](#) on page 27

[Downloading the Software](#) on page 28

[Creating a bootable USB key](#) on page 29

[Creating a bootable DVD](#) on page 31

[Installing the software manually \(DVD/USB\)](#) on page 32

[Installing the software manually \(USB\)](#) on page 34

[Igniting the server](#) on page 35

Adding and Configuring Additional Hard Disks

The server running Media Manager must include an additional hard disk or disks. That additional hard disk is used to store the call recordings collected by Media Manager and must be separate from the disk used by the other IP Office services including Voicemail Pro.

- This applies on the primary server for IP Office Server Edition/Select systems or when using an IP Office Application server to support an IP500 V2.
- If the additional disk is added after initial server configuration, see the [Administering Avaya IP Office™ Platform Media Manager](#) manual for details of initializing the disk.

For R11.1 FP2 and higher, a separate hard disk is not required for Media Manager in the following scenarios:

- For local Media Manager, the application can be configured to use the customer's own cloud storage as its primary store for call recordings. See the [Administering Avaya IP Office™ Platform Media Manager](#) manual.
- Subscription mode systems can use a centralized Media Manager service. That uses cloud storage provided by the Avaya COM service providing the system subscriptions.

If using an additional hard disk for local Media Manager:

- It is strongly recommended that a pair of additional hard-disks are used, configured in the server BIOS to act as a RAID1 pair.
- These additional drives should be added and configured before installation of the IP Office software. Details of the additional drive are set as part of the IP Office server ignition.
- The exact process of adding and/or configuring the additional drive for Media Manager use depends on the server being used. Refer to the documentation for the particular server platform.

Related links

[Server Software Installation](#) on page 27

Downloading the Software

Avaya makes IP Office software for each IP Office release available from the Avaya support website (<https://support.avaya.com>) :

Software	Description
ISO Image	You can use this type of file to install the full set of IP Office server services including the underlying operating system.
Avaya USB Creator Tool	This tool is used to load an ISO image onto a USB memory key from which the server can boot and either install or upgrade. • Note: You must use the R11.1 version of this tool for R11.1 and higher systems.
Text-to-Speech Languages ISO Images	No TTS languages are installed by default. This set of 3 ISO files contain the files from which the TTS services for different languages can be installed if required.
IP Office Administration Suite	This ZIP file contains the installation package for a number of applications required for the installation and maintenance of IP Office systems; IP Office Manager, SysMonitor and System Status Application. Avaya expects anyone installing an IP Office server to be familiar with the use of these applications.

To download Avaya software

1. Browse to <https://support.avaya.com> and log in.
2. Select **Support by Product** and click **Downloads**.

3. Enter `IP Office` in the **Enter Product Name** box and select the matching option from the displayed list.
4. Use the **Choose Release** drop-down to select the required IP Office release.
5. The page lists the different sets of downloadable software for that release. Download the software packages listed above.
6. The page displayed in a new tab or windows details the software available and provides links for downloading the files.
7. Also download the documents listed under the **RELATED DOCUMENTS** heading if shown.

Related links

[Server Software Installation](#) on page 27

Creating a bootable USB key

You can install and upgrade IP Office Server Edition using a USB key.

Related links

[Server Software Installation](#) on page 27

[Downloading the Avaya USB Creator Tool](#) on page 29

[Creating a USB Drive using the Avaya USB Creator](#) on page 29

[Creating a USB Drive using Rufus](#) on page 30

Downloading the Avaya USB Creator Tool

Creating a USB drive for software installation or upgrade requires the following software from the Avaya support site. See [Downloading the Software](#) on page 28.

Software	Description
IP Office Server Edition ISO image	This ISO file is used for types of all Linux-based IP Office server.
Avaya USB Creator Tool	For Release 11.1 and higher, you <i>must</i> use the Release 11.1 version of this tool. Using a previous version will cause installation and upgrade issues.

Related links

[Creating a bootable USB key](#) on page 29


Creating a USB Drive using the Avaya USB Creator

Before you begin

- You need a USB drive with at least 8GB storage space.
 - If using a USB of 64GB or larger, see [Creating a USB Drive using Rufus](#) on page 30.
- Install the Avaya USB Creator Tool.

Procedure

1. Insert the USB drive into a USB port on the PC.
2. Start the Avaya USB Creator. Select **All Programs > All Programs > Avaya USB Creator > Avaya USB Creator** .
3. Click **Browse** and select the ISO file.
4. In the **Select Target USB Drive** field, select the USB memory key. Ensure that you select the correct USB device as this process overwrites all existing content on the device.
5. In the **Select Installation Mode** field, select what type of process the key performs when the server is booted from that key:

Option	Description
Server Edition – Attended Mode	Creates a USB key that present a series of menus from which an installation or upgrade can be performed.
Server Edition – Auto Install	Creates a USB key which does an automatic installation of the software with a default set of IP address details. This method should be used with caution as it automatically erases any existing content on the server’s first hard disk.
Server Edition – Auto Upgrade	<p>Creates a USB key that does an automatic upgrade of the existing software on a server.</p> <p> Warning:</p> <ul style="list-style-type: none"> • This method of upgrading is not supported for upgrades to IP Office R12.0 from pre-R12.0 systems. See Upgrading Linux-based IP Office Systems to R12.0.

6. Under **Select Locals to Install / Upgrade**, select the check boxes for the voicemail prompts languages to install or upgrade. Selecting only the languages required significantly reduces the time required to create the USB key and the installation or upgrade time.
7. Click **Start** and then confirm.

Related links

[Creating a bootable USB key](#) on page 29

Creating a USB Drive using Rufus

This process should only be used with USB memory keys of 64GB or larger. For smaller keys, see [Creating a USB Drive using the Avaya USB Creator](#) on page 29.

Warning:

- This process will erase all existing files and folders on the USB key without any chance of recovery.

Procedure

1. Insert the USB memory key into a Windows PC.

2. Start Rufus.
3. Use the **Device** field to select the USB memory key.
4. Next to the Boot selection field, click **SELECT** and select the ISO file. Ensure that you select the correct ISO file. For PC servers, the file name is prefixed with `c110` followed by the software version.
5. Select the following other options:
 - a. **Volume label** - Change this to **AVAYA** with no quotation marks.
 - b. **File System** - Leave this as **Large FAT32**.
6. Click **Start**.
7. The progress of the unpacking of the ISO file onto the USB memory key is displayed. Allow this process to continue without any interruption. It takes approximately 4 to 10 minutes depending on the size of the USB memory key.
8. When Rufus has completed the process and shows `READY`, click **CLOSE**.
9. Open the USB memory key in file manager.
10. Open the USB folder.
 - For an installation key: Copy and paste the `avaya_autoinstall.conf` and `syslinux.cfg` files to the root folder of the USB memory key.
 - For an upgrade key: Copy and paste the `avaya_autoupgrade.conf` and `syslinux.cfg` files to the root folder of the USB memory key.
 - **! WARNING** - Do not copy any other files. Copying any other files will cause the USB to run a new install, erasing all existing files on the server.
11. The USB upgrade key is now ready for use.

Related links

[Creating a bootable USB key](#) on page 29

Creating a bootable DVD

To install from a DVD, you need to burn the Server Edition ISO file onto a bootable DVD. Avaya do not provide any software for this process.

The exact process for that depends on which software you use for the burning process. However, the following general recommendations apply:

- For R11.1 FP2 and higher, the size of the ISO file requires the use of dual-layer DVD discs and a dual-layer recorder. The target server PC also needs to support dual-layer discs.
- Do not use reusable DVDs.
- Burning the DVD at a slower speed such as 4x takes longer but increases the reliability of the transfer.

Burning a DVD using Windows

If you do not have any specific DVD burning software, you can burn a DVD directly from Windows. Right-click on the downloaded `.iso` file and select **Burn disc image**.

If the option to burn a disc is not shown, the most likely cause is that another application such as WinZip has associated itself with the `.iso` file extension. If that is the case, use the following process:

1. Right-click on the `.iso` file and select **Open with**.
2. Select **Choose another app**.
3. Select **Windows Explorer**.
4. Select **Always use this app to open .iso files**.
5. Click **OK**.
6. A window showing the contents of the file is opened. Close that window.
7. Right-click on the file and select **Burn disc image**.

Related links

[Server Software Installation](#) on page 27

Installing the software manually (DVD/USB)

This process covers installing the server software from a bootable DVD or a USB key configured to **Server Edition – Attended Mode**.

Warning:

- This process will erase all existing software and data on the server.

Before you begin

- Create the bootable installation media:
 - For a USB key, see [Creating a bootable USB key](#) on page 29.
 - For a DVD, see [Creating a bootable DVD](#) on page 31.

Procedure

1. Attach a monitor and keyboard to the server.
2. Insert the bootable DVD or USB key into the server.
3. Start or restart the server.
4. If the system does not boot from the install media, verify the boot order in the server's BIOS settings.
5. Reboot the server. A series of text messages are displayed and then a *"Welcome to Avaya R12"* menu.

6. Select the language you want used for the installation menus and click **Continue**.
7. Read the **EULA** (end-user license agreement). If you accept it, click **Continue**.
8. Read the **Release notes** and click **Continue**.
9. The **Installation Summary** menu is displayed.
10. Click **Keyboard**:
 - a. Check that the correct keyboard type is shown at the top of the list. If necessary, use the +/- icons to add/remove keyboard layouts and the ^/v icons to shuffle the order of listed keyboard layouts.
 - b. Click **Done**.
11. Click **Installation Destination**:
 - a. Check that the servers primary hard disk is selected.
 - b. Click **Done**.
12. Click **Root Password**:
 - a. Enter and confirm a temporary password for the root account. This does not need to be a strong password as it changed again during a later stage of the installation. However, note the password as you will need it for the server ignition process.
 - b. When completed, press **Done**.
13. Click **Network & Host Name**:
 - a. In the **Host name** field, enter the host name for the server. Click **Apply**.
 - b. Select the **Ethernet (eth0)** port.
 - c. Ensure that the port is enabled.
 - d. Click **Configure**.
 - e. Select **IPv4 Settings**.
 - f. Set the IP address details (**Address**, **Netmask**, and **Gateway**) to match the values the server must use on the customer network.
 - g. If separate, enter the networks **DNS server**.
 - h. Click **Save**.
 - i. Repeat the process for the **Ethernet (eth1)** port is present.
 - j. Click **Done**.
14. Click **Begin Installation**.
15. The next stage takes approximately 30 minutes as the software is installed.
16. When the `Complete!` message is shown, remove the CD or USB used for the installation.
17. Click **Reboot System**.
18. The reboot is completed when the server displays address details and an **Command:** prompt.

Next steps

- You can now ignite the server. See [igniting the server](#) on page 35.

Related links

[Server Software Installation](#) on page 27

Installing the software manually (USB)

A USB key can be used to automatically install the software using a set of default settings, see [Default parameters](#) on page 13. The process of installation can still be observed on a monitor attached to the server.

Warning:

- This process will erase all existing software and data on the server.

Before you begin

- Create a USB key set to **Server Edition – Auto Install**. See [Creating a USB Drive using the Avaya USB Creator](#) on page 29.
- Directly connect a laptop to the server's first network port. The laptop will need to be configured with an IP address such as 192.168.42.203/255.255.255.0. This allows configuration and ignition of the server before it is connected to the customer network.

Procedure

1. Attach a monitor and keyboard to the server.
2. Connect the laptop and check that the server is not currently connected to the network.
3. Insert the USB key into the server.
4. Start or restart the server.
5. If the system does not boot from the install media, verify the boot order in the server's BIOS settings.
6. Observer the installation as it progresses.
7. Remove the bootable media used and select **Continue**.
8. Following the reboot, a series of text messages are shown as the various services are checked and started.
9. Eventually a screen with the message IP Office Server Edition is displayed, along with the server's IP address.
10. The server can now be ignited for the particular server role for which it is needed. See [igniting the server](#) on page 35.

Next steps

- The server now needs to be ignited. See [igniting the server](#) on page 35.

Related links

[Server Software Installation](#) on page 27

Igniting the server

About this task

Each server needs to go through a server ignition process. During this process, the server's particular role is configured and key settings are set.

- To perform ignition, you need the current IP address of the server. That is shown on the monitor connected to the server.
 - For servers supplied pre-installed by Avaya or installed using automatic USB installation, the address is `192.168.42.1/255.255.255.0`.
- Ignition is performed by browser from another PC.
- You can only run the ignition process once. To rerun the process requires a complete software reinstall.
- If the Ignition process is not completed, for example if you click **Cancel**, the system displays the Ignition menu when you next login.

Procedure

1. On a PC on the same network as the server, open a web browser.
2. Enter the address `https://<Server_IP_Address>:7070`.
3. Because the browser does not have a copy of the server's root certificate, it displays a warning regarding an unsafe connection.
 - You can ignore this at this stage. Proceed with connecting your browser.
 - Following ignition, you can download the server certificate and add it to the certificate repository used by the browser.
4. Note the **WebLM ID** and **PLDS ID** values displayed on the logging menu. These are required for licensing or subscription of the server.
5. Login to the server. The password depends on how the software was installed:
 - a. In the **User Name** field, enter `root`.
 - b. In the **Password** field, enter one of the following:
 - If you installed the software manually, use the password you specified during that process.
 - If the software was installed automatically, use the password `Administrator`.
 - c. Click **Login**.
6. The server displays the **Accept License** menu. Click **I Agree** and click **Next**.

7. The server displays the **Server Type** menu. Select the particular IP Office role the server will perform:

Server Type	Description
Primary	If setting up an IP Office network, this is the first type of server that must be added to the network.
Secondary	This type of server supports the same services as the primary and can temporarily take over its role in some situations (known as “resilience”).
Expansion	This type of server can be used to support additional IP telephony services in a primary server’s network.
Application Server	<p>This type of server can be used in a number of ways:</p> <ul style="list-style-type: none"> • Within a primary server network, it can be used to host the Avaya one-X Portal application service (removing it from the primary). This can be used when the primary is hosted on a lower specification server. • For an IP500 V2 system, it can be used to host the Voicemail Pro and/or Avaya one-X Portal applications for the IP500 V2 server. • An application server can also be ignited with no user services and then used as a backup server for other servers.

8. Select the required server role and click **Next**. The following menus vary depending on the selected role.
9. The server displays the **New Hardware** menu. This contains details if any additional hard drive installed in the server. This is required for a primary or application server supporting the Media Manager application. If the server has an additional drive, check the following steps. Otherwise click **Next**:
- a. For a new server, select **Format Hard Drive**. Only select this if you are sure that all data on the hard drive should be erased. For example, do not select it if reigniting the server as part the process to recover a failed server.
 - b. Select **Mount Hardware**.
 - c. Leave all the other settings at their defaults unless you have a specific reason to be otherwise. Note the **Mount Point** path settings. You need this as part of the Media Manager application configuration.
 - d. Click **Next**.
10. The server displays the **Configure Network** menu:
- a. Ensure that the **Hostname** is unique within the network domain. It can be a string of characters 63 characters in length. The characters can be upper-case or lower-case letters A through Z, digits 0 through 9, the minus sign (-), and the period (.).
 - b. Check that the settings match those required for the customer network.
 - c. Click **Next**.
11. The server displays the **Time & Companding** menu:

! **Important:**

- An accurate time source and settings are vital to many functions, including subscriptions and any services that use certificates.
- a. Select **Use NTP Client** and set the **Timezone**.
 - b. On server's that support telephony operation, select the **Companding** mode.
 - **μ-law** is typically used for North America and Japan.
 - **A-law** is used for Europe and other parts of the world.
 - c. Click **Next**.
12. The server displays the **Change Password** menu. Set the passwords as required. If igniting a server for addition to a network of servers, set passwords that match those used on the network's primary server.

Option	Description
'root' and 'security' password	This sets the initial password of both the Linux <code>root</code> user account and the IP Office security administrator. <ul style="list-style-type: none"> • After ignition, the passwords for these accounts can be changed separately.
'Administrator' password	This sets the initial password of both the Linux and IP Office <code>Administrator</code> user accounts. <ul style="list-style-type: none"> • After ignition, the passwords for these accounts can be changed separately.
'System' password	This sets the system password of the IP Office system.

Set the passwords as required and click **Next**.

13. On an IP Office Application server, the server displays a **Configure Services** menu:
- a. Select the services that the application server should provide. The voicemail service is only supported when using the application server to support an IP500 V2 system.
 - b. Click **Next**.
14. On a primary or application server, the server displays the **Security** menu:
- a. Select whether to upload a certificate for the server or to let the server generate a self-signed certificate.
 - b. Select whether you want the server to support the Avaya EASG server. Enabling EASG is a requirement for systems included in an Avaya IPOSS support contract.
 - c. Click **Next**.
15. The server displays the **Review Settings** menu:
- a. Check that the settings are correct. Use the **Back** control if necessary to change or correct any of the settings.,
 - b. Use the certificate links to download copies of the server's certificate file.
 - c. When satisfied with the settings, click **Apply**.

Next steps

You can now proceed to the initial configuration of the server. The process depends on the selected server role:

- **Primary Server:** See [Primary Server Installation and Initial Configuration](#) on page 40.
- **Secondary Server:** See [Secondary Server Installation and Initial Configuration](#) on page 69.
- **Expansion Server:** See [Expansion Server \(Linux\) Installation and Initial Configuration](#) on page 77.
- **Application Server:** See [Application Server Installation](#) on page 93.

Related links

[Server Software Installation](#) on page 27

Part 3: Primary Server Installation

Chapter 4: Primary Server Installation and Initial Configuration

Once the server software has been installed (see [Server Software Installation](#) on page 27) and the server ignited as a primary server, it can be configured using the processes in this section.

This section only covers the minimal configuration to have the server licensed and operation. Full configuration to match the customer requirements is covered in the documentation for the IP Office Manager and Web Manager applications.

You can perform the initial configuration using either IP Office Manager or Web Manager.

Related links

[Primary server initial configuration using Web Manager](#) on page 40

[Primary server initial configuration using IP Office Manager](#) on page 42

Primary server initial configuration using Web Manager

This process uses IP Office Web Manager to perform the initial configuration of the primary server.

Before you begin

- Ignite the server as a primary server. See [Igniting the server](#) on page 35.

Procedure

1. On a PC on the same network as the server, start a web browser. Enter `https://<Server_IP_Address>:7070`.
2. Enter `Administrator` and the password set for that user during the server ignition process.
3. In the **Agreement** menu, select **Accept** and click **OK**.
4. If the server displays a background synchronization warning, click **Yes**.
5. The server displays the dashboard. If not, select **Solution** > **Server Menu** > **Dashboard**.
6. Click on the **System** widget.
7. In the **System Mode**, select one of the following:

System Mode	Description
Server Edition	Select this option for a primary server that will use a PLDS file for licensing.
Server Edition - Select	Select this option for a primary server that will use a PLDS file for licensing that includes Select licenses. Note that if in a network, all servers in the network requires a Select license.
Server Edition - Subscription	Select this option for a primary server that will use subscriptions for licensing.

8. Set a unique **System Name** for the system. This will appear in other administration menus and helps identify the particular server.
9. If applicable, enter the **Services Device ID** issued for support of the server.
10. Set the **Locale** to match the customer location. Set this accurately as it affects a number of default telephony settings that the system will then use.
11. Set and confirm the **Default Extension Password**. This is used to set the extension password required to register IP extension unless a separate specific password is configured in the extension's own settings.
12. For a **Server Edition - Subscription** system, a section for entry of the **Subscription System Details** is displayed. Enter the details supplied in the email provided after the primary server's PLDS ID was registered for subscription:

Setting	Description
System ID	This field is not changeable. However, check that it matches the details shown in the system's subscription email.
Customer ID	Enter the customer ID provided in the system's subscription email.
License Server Address	Enter the address provided in the system's subscription email.

13. Using the **Public LAN Interface** control:
 - a. Select **LAN1** and check that the **IP Address** and **IP Mask** match the network settings that the server should use for its eth0 port.
 - b. Select which **DHCP Mode** the server should support on the LAN.

Option	Description
Server	The server will act as a DHCP server for the network on that interface. For its own address it will use the IP Address details entered in this menu.
Client	The server will obtain its IP address settings automatically from a DHCP server elsewhere on the network.
Dial In	This DHCP mode is not supported on Linux-based IP Office servers.
Disabled	The server will use the fixed IP address details entered in this menu.

- c. Select **LAN2** and check that the **IP Address** and **IP Mask** settings match the network settings that the server should use for its eth1 port.

- d. Set the **Gateway** address for the customer network.
14. Having set and checked the IP address and DHCP details, select which port, **LAN1** or **LAN2**, will be used for outgoing connections from the customer network for general internet access. This choice adds a default IP route from that LAN to the specified **Gateway** address.
15. Enter the IP address of the **Server Edition Primary**.
16. For **Server Edition Secondary**, enter the IP address of the planned secondary server. If there is no plan to add a secondary server, enter a dummy address.
17. If the customer network has a specific **DNS Server**, enter its address.
18. Enter an **Web Socket Password** password. This password is used for the links to other IP Office servers in the network.
19. Check the settings are all as required and match the customer network requirements.
20. Click **Apply**.
21. Work through the other widgets on the dashboard and configure the system as required, see [The Setup Wizard/Initial Configuration](#) on page 45.
22. Click **Save to IP Office** shown at the top of the browser window.
23. The **Save IP Office Configuration** menu is preset to save the new settings and restart the server. Select the server and click **OK**.

Next steps

Having completed the primary server's initial configuration:

- For non-subscription mode systems, proceed to adding the PLDS license file. See [Adding the PLDS License File](#) on page 65.
- For subscription mode systems, check the subscriptions have been received and enable the **COMAdmin** service user account. See [Subscription and COM Support Setup](#) on page 61.

Related links

[Primary Server Installation and Initial Configuration](#) on page 40

Primary server initial configuration using IP Office Manager

This process uses IP Office Manager to perform the initial configuration of a primary server.

Before you begin

- Ignite the server as a primary server. See [Igniting the server](#) on page 35.

Procedure

1. Start Manager. See [Starting IP Office Manager](#) on page 150.
 - a. Click **File > Open Configuration**.
 - b. From the **Select IP Office** menu, select the primary server and click **OK**.
 - c. Enter `Administrator` and the password configured for that user account during the primary server's ignition. Click **OK**.
2. Manager is reloaded and the initial configuration utility (ICU) menu for a new server is displayed.
3. In the **System Mode**, select one of the following:

System Mode	Description
Server Edition	Select this option for a primary server that will use a PLDS file for licensing.
Server Edition - Select	Select this option for a primary server that will use a PLDS file for licensing that includes Select licenses. Note that if in a network, all servers in the network requires a Select license.
Server Edition - Subscription	Select this option for a primary server that will use subscriptions for licensing.

4. Set a unique **System Name** for the system. This will appear in other administration menus and helps identify the particular server.
5. Set the **Locale** to match the customer location. Set this accurately as it affects a number of default telephony settings that the system will then use.
6. Set and confirm the **Default Extension Password**. This is used to set the extension password required to register IP extension unless a separate specific password is configured in the extension's own settings.
7. For a **Server Edition - Subscription** system, a section for entry of the **Subscription System Details** is displayed. Enter the details supplied in the email provided after the primary server's PLDS ID was registered for subscription:

Setting	Description
System ID	This field is not changeable. However, check that it matches the details shown in the system's subscription email.
Customer ID	Enter the customer ID provided in the system's subscription email.
License Server Address	Enter the address provided in the system's subscription email.

8. Using the **Public LAN Interface** control:
 - a. Select **LAN1** and check that the **IP Address** and **IP Mask** match the network settings that the server should use for its eth0 port.
 - b. Select which **DHCP Mode** the server should support on the LAN.

Option	Description
Server	The server will act as a DHCP server for the network on that interface. For its own address it will use the IP Address details entered in this menu.
Client	The server will obtain its IP address settings automatically from a DHCP server elsewhere on the network.
Dial In	This DHCP mode is not supported on Linux-based IP Office servers.
Disabled	The server will use the fixed IP address details entered in this menu.

- c. Select **LAN2** and check that the **IP Address** and **IP Mask** settings match the network settings that the server should use for its eth1 port.
 - d. Set the **Gateway** address for the customer network.
9. For **Server Edition Secondary**, enter the IP address of the planned secondary server. If there is no plan to add a secondary server, enter a dummy address.
 10. If the customer network has a specific **DNS Server**, enter its address.
 11. Enter an **Web Socket Password** password. This password is used for the links to other IP Office servers in the network.
 12. Check the settings are all as required and match the customer network requirements.
 13. Click **Save**. The server's configuration is opened in manager. At this stage it has not been saved to the system.
 14. Click **File > Save Configuration**
 15. Check that the **Change Mode** is set to **Reboot** and click **OK**.
 16. Click **Next**. The IP Office service on the server is restarted using the new configuration.

Next steps

Having completed the primary server's initial configuration:


- For non-subscription mode systems, proceed to adding the PLDS license file. See [Adding the PLDS License File](#) on page 65.
- For subscription mode systems, check the subscriptions have been received and enable the **COMAdmin** service user account. See [Subscription and COM Support Setup](#) on page 61.

Related links

[Primary Server Installation and Initial Configuration](#) on page 40

Chapter 5: The Setup Wizard/Initial Configuration

IP Office Web Manager displays the setup wizard when it connects to a new IP Office server for the first time (except IP Office Application Server). The setup wizard consists of a number of panels, each of which you can use to configure a different area of the IP Office server configuration.

- Click on a panel to access its settings.
 - On a new IP Office system, you can only access the panels in sequence, starting with the **System** panel.
 - After you have configured the settings in a panel, the panel displays a summary of those settings and you can access the next panel.
 - After you have configured the settings within a panel, you can return to it at any time.
- Some of the panels alter settings that require an IP Office system reboot. Therefore, on a new server the setup wizard runs in offline mode. When completed, clicking **Save to IP Office** applies the settings and restarts the IP Office.
- The **System** panel is also called the **Initial Configuration Utility (ICU)**.
 - On systems that have already completed initial configuration, you can return to this menu using  > **Initial Configuration** (IP500 V2: **Actions** > **Initial Configuration** for IP500 V2).
- On standalone IP500 V2 systems, IP Office Web Manager displays the panels as the system's **Solution** display and as the dashboard (**Solution** > **Server Menu** > **Dashboard**).

Related links

[Setup Wizard: Panels Summary](#) on page 46

[Setup Wizard: System Panel \(Initial Configuration Utility\)](#) on page 47

[Setup Wizard: VoIP](#) on page 51

[Setup Wizard: Voicemail](#) on page 55

[Setup Wizard: Subscription](#) on page 57

[Setup Wizard: Licensing](#) on page 58

[Setup Wizard: User](#) on page 58

[Setup Wizard: Groups](#) on page 58

[Setup Wizard: Lines](#) on page 58

[Setup Wizard: Incoming Call Routes](#) on page 59

[Setup Wizard: Outgoing Call Routes](#) on page 60

Setup Wizard: Panels Summary

The following tables provide a brief summary of the role of each panel. It also indicates their availability which may depend on other settings or the type of IP Office server.

Panel	Description
System	Configure general system settings such as IP Office mode, locale and IP addresses.
VoIP	Configure the system's settings for H.323 and SIP telephony.
Voicemail	Configure the system's use of voicemail to handle unanswered and missed calls.
Licensing	Configure the system PLDS license settings and upload a license file. This panel is not shown on IP Office subscription systems.
Subscription	Display details of the system subscription settings and subscriptions. This panel is only shown on IP Office subscription systems.
Users	Configure the system users.
Groups	Configure groups of users. Each group has its own extension number which allows it to be used as the destination for calls.
Lines	Configure external telephone lines.
Incoming Call Routes	Configure the destination for incoming external calls based on the lines being used and the incoming telephone number.
Outgoing Call Routes	Configure the settings applied to outgoing external calls by default and for particular users if required.


Panel	Server Edition		IP500 V2
	Primary Secondary	Expansion	
System	✓	✓	✓
VoIP	✓	×	✓
Voicemail	✓	×	✓
Licensing	✓	×	✓
Subscription	✓	×	✓
Users	✓	×	✓
Groups	✓	×	✓
Trunks	✓	×	✓
Incoming Call Routing	✓	×	✓
Outgoing Call Routing	✓	×	✓

Related links

[The Setup Wizard/Initial Configuration](#) on page 45

Setup Wizard: System Panel (Initial Configuration Utility)

This is the only mandatory panel in the setup wizard. This menu is also called the **Initial Configuration** utility.

On IP Office systems that have already completed initial configuration, you can return to this menu using  > **Initial Configuration** (IP500 V2: **Actions** > **Initial Configuration**).

Common Settings

Option	Description
System Mode	<p>Sets the operating mode of the server. The options available depend on the type of server platform. For further details, refer to the appropriate IP Office deployment manual.</p> <ul style="list-style-type: none"> For Linux-based servers: <ul style="list-style-type: none"> - Server Edition - Server Edition - Select - Server Edition - Subscription For an IP500 V2 server: <ul style="list-style-type: none"> - IP Office Standard Edition - IP Office Subscription - IP Office ACO ATA Gateway - Server Edition Expansion - Server Edition Expansion - Subscription For an existing IP Office being reconfigured, the choice of system modes is restricted. For example, you cannot change a subscription mode system to non-subscription mode. In order display the full set of options, you must default the IP Office system configuration .
System Name	<p>A name to identify this system. This is typically used to identify the configuration by the location or customer's company name. Some features require the system to have a name.</p> <ul style="list-style-type: none"> This field is case sensitive and within any network of systems must be unique. Do not use <, >, , \0, :, *, ?, . or /.
Retain Configuration Data	<p>This option is shown for existing servers where the initial configuration menu is being rerun.</p> <ul style="list-style-type: none"> If cleared, the existing configuration of the IP Office system is defaulted. If enabled, the existing configuration is retained. However, some elements of that configuration may be invalid or ignored. It is your responsibility to ensure that the final configuration is valid.

Table continues...

Option	Description
Locale	This setting sets default telephony and language settings based on the selection. It also sets various external line settings and so must be set correctly to ensure correct operation of the system. See Avaya IP Office Locale Settings . For individual users, the system settings can be overridden through their own locale setting (User > User > Locale).
Default Extension Password	Default = Existing default extension password The field provides you with option to view and edit the existing default extension password. The default extension password is set up during IP Office installation either by the administrator or is randomly generated by the system. The system generated random password is of 10 digits. Use the Eye icon to see the existing default password. The password must be between 9 to 13 digits.
Hosted Deployment	This option is only used on non-subscription Server Edition system. If enabled, it indicates that the system is a hosted deployment.
Services Device ID	This setting is shown for Server Edition servers only. The ID is displayed on the Solution view, System Inventory and on the System > System tab in the configuration. <ul style="list-style-type: none"> The value can be changed using the Device ID field on the System > System Events configuration tab.

Subscription System Details

These details are only shown for subscription mode systems. They are used by the system to obtain its subscriptions. They details required are supplied when the system is registered for subscription.

Name	Description
System ID	This is a fixed value against which the system's subscriptions are issued and validated. <ul style="list-style-type: none"> For an IP500 V2 system, this ID is based on the System SD card installed in the system.
Customer ID	The customer ID specified when the system was registered for subscriptions.
License Server Address	The address of the server which provides the system with its subscriptions.

LAN Configuration Settings

Name	Description
Public LAN Interface	Select which of the server's LAN interfaces is connected to the customer network routed to the external internet. Additional IP Route details are added to the system configuration based on this choice.
Gateway	The address of the default gateway on the customer network to which non-LAN traffic should be routed. After initial configuration, a default IP route is created, using this address and the selected Public LAN Interface setting.

Table continues...

Name	Description
DNS Server	The address used on the customer network for resolution of DNS queries. This is either the customer's DNS server or the DNS address provided by their internet service provider.
LAN1 CONFIGURATION/LAN2 CONFIGURATION	
Separate sets of LAN configuration details are shown for LAN1 and LAN2.	
IP Address	The base IP address for the LAN. The defaults are 192.168.42.1 for LAN1 and 192.168.43.1 for LAN2. If the server is acting as the DHCP server for the LAN, this is the starting address for the DHCP address range.
IP Subnet Mask	Default = 255.255.255.0. This is the IP subnet mask used with the IP address.
DHCP Mode	Select whether the server performs DHCP for the LAN. <ul style="list-style-type: none"> • Server - When this option is selected, the system will act as a DHCP Server on this LAN, allocating address to other devices on the network and to PPP Dial in users. <ul style="list-style-type: none"> - Devices on requesting an address are allocated addresses from the bottom of the available address range upwards. - Dial In users are allocated addresses from the top of the available range downwards. - If the control unit is acting as a DHCP server on LAN1 and LAN2, Dial in users are allocated their address from the LAN1 pool of addresses first. • Disabled - When this option is selected, the system will not use DHCP to get or issue IP addresses. • Dial In - When this option is selected, the system will allocate DHCP addresses to PPP Dial In users only. On systems using DHCP pools, only addresses from a pool on the same subnet as the system's own LAN address will be used. • Client - When this option is selected, the system request its IP Address and IP Mask from another DHCP server on the LAN.
Enable NAT	Default = Off. Shown for IP500 V2 systems only. This setting controls whether NAT should be used for IP traffic from LAN1 to LAN2.

Solution Settings

These settings are shown for Linux-based systems. The options vary depending on the server's role in the network (primary, secondary or expansion).

Name	Description
Server Edition Primary Server	For secondary and expansion servers, specify the address of the primary server.
Server Edition Secondary Server	For primary and expansion servers, specify the address of the secondary server.

Table continues...

Name	Description
WebSocket Password	For each of the addresses set above, a bi-directional WebSocket connection is created. A matching password must be set at each end of the line.
DNS Server	This is the IP address of a DNS Server. If this field is left blank, the system uses its own address as the DNS server for DHCP client and forwards DNS requests to the service provider when Request DNS is selected in the service being used (Service > IP).

Time Settings

These settings are shown for non-subscription IP500 V2 servers only. They are only shown in the IP Office Web Manager initial configuration menu.

Name	Description
Time Setting Configuration Source	<p>An accurate time source and settings are vital to many functions, including any services that use certificates. Avaya recommend that you use SNTP and a reliable source such as <code>time.google.com</code>.</p> <ul style="list-style-type: none"> • None Set the system date and time manually using a phone with System Phone Rights (User > User). • SNTP Use a list of SNTP servers to obtain the UTC time. The IP Office tries the addresses in the list one at a time in order until there is a response. The system makes a request to the specified addresses following a reboot and every hour afterwards. • Voicemail Pro/Manager (Obsolete) The Windows-based Voicemail Pro service and the IP Office Manager program can act as RFC868 Time servers for the IP Office system. Use of other RFC868 server sources is not supported. They provide both the UTC time value and the local time as set on the PC. The system makes a request to the specified address following a reboot and every 8 hours afterwards.
The following setting is available when the Time Setting Configuration Source is set to SNTP .	
Time Server Address	<p>Default = Blank</p> <p>A list of SNTP servers the used to obtain the UTC time.</p> <ul style="list-style-type: none"> • The records in the list are used one at a time until there is a response. <p>The system makes a request to the specified addresses following a reboot and every hour afterwards.</p>

Centralized Management

The following settings are used for IP Office systems being deployed as branch systems in a network managed using System Manager. Refer to the [Deploying Avaya IP Office™ Platform as an Enterprise Branch with Avaya Aura® Session Manager](#) manual.

Name	Description
Under Centralized Management	When selected, the additional fields below are shown.
SMGR Address	Enter the IP address of the System Manager server managing the branch network.
Redundant SMGR Address	Enter the IP address of the secondary System Manager server managing the network.
SMGR Community	The shared community name for servers within the branch network.
SNMP Device ID	The unique SNMP ID for the IP Office server within the network.
Trap Community	The public name for sending SNMP trap alarms.
SCEP Domain Certificate Name	The domain name for SCEP (Simple Certificate Enrollment Protocol) operation in the branch network.
Certificate Enrollment (SCEP) Password	The password for requesting certificates from the network's SCEP server.

Related links

[The Setup Wizard/Initial Configuration](#) on page 45

Setup Wizard: VoIP

You can use this panel to configure the H323 Gatekeeper and SIP Registrar support provided on each of the system's LAN interfaces.

LANS

Field	Description
Select LAN	Use this control to switch between configuring LAN1 or LAN2.

H.323 Gatekeeper

These settings relate to the H.323 extension support provided by the system on the currently selected LAN.

Field	Description
H.323 Gatekeeper Enable	Default = Off If enabled, the system will support H.323 trunk and extension connections on the LAN.

Table continues...

Field	Description
H.323 Signaling over TLS	<p>Default = Disabled. For hosted deployments, default = Preferred.</p> <p>When enabled, TLS is used to secure the registration and call signaling communication between IP Office and endpoints that support TLS. The H.323 phones that support TLS are 9608, 9611, 9621, and 9641 running firmware version 6.6 or higher.</p> <p>When enabled, certificate information is configured in the <code>46xxSettings.txt</code> file on IP Office and automatically downloaded to the phone. When IP Office receives a request from the phone for an identity certificate, IP Office searches its trusted certificate store and finds the root CA that issued its identity certificate. IP Office then provides the root CA as an auto-generated certificate file named <code>Root-CA-xxxxxxxxx.pem</code>.</p> <p>For information on IP Office certificates, see Security > Certificates.</p> <p>The options are:</p> <ul style="list-style-type: none"> • Disabled: TLS is not used. • Preferred: Use TLS when connecting to a phone that supports TLS. • Enforced: TLS must be used. If the phone does not support TLS, the connection is rejected. <p>When set to Enforced, the Remote Call Signaling Port setting is disabled.</p> <p>If TLS security is enabled (Enforced or Preferred), it is recommended that you enable a matching level of media security on System Settings > System > VoIP Security.</p>
H.323 Remote Extn Enable	<p>Default = Off</p> <p>The system can be configured to support remote H.323 extensions in the case where NAT is used in the connection path. This could be the case where the IP Office is located behind a corporate NAT/Firewall router and/or the H.323 phone is located behind residential NAT enable router.</p> <p>Currently, only 9600 Series phones are supported as H.323 remote extensions.</p>
Remote Call Signaling Port	<p>Default = 1720</p> <p>The call signaling port used for remote H.323 extensions.</p>
Auto-create Extension	<p>Default = Off</p> <p>If enabled, the system will automatically create a extension entry in its configuration in respond to successful registration by an H.323 IP phone.</p> <ul style="list-style-type: none"> • This setting is automatically disabled 24-hours after being enabled.
Password	<p>Default = Blank</p> <p>If set, sets the password for extension registration using auto-creation. If left blank, the system Default Extension Password setting is used.</p>

Table continues...

Field	Description
Auto-create User	Default = Off If enabled, the automatic creation of an H.323 extension entry in the system configuration also causes the automatic creation of a matching user entry for the extension.

SIP Trunks


Field	Description
SIP Trunks Enable	Default = On. This settings enables support of SIP trunks. It also requires entry of SIP Trunk Channels licenses. Enabling SIP Trunks Enable allows configuration of the RTP Port number Range (NAT) settings.

SIP Registrar

These setting relate to the support of SIP extensions on the selected LAN.

Field	Description
SIP Registrar Enable	Default = Off Used to set the system parameters for the system acting as a SIP Registrar to which SIP endpoint devices can register. Separate SIP registrars can be configured on LAN1 and LAN2. Registration of a SIP endpoint requires an available IP Endpoints license. SIP endpoints are also still subject to the extension capacity limits of the system.
Auto-create Extn/User	Default = Off. The field to set up auto creation of extensions for SIP phones registering themselves with the SIP registrar. If selected, the system prompts you to enter and confirm the password is used for subsequent auto creation of extensions. <ul style="list-style-type: none"> • This setting is not supported on systems configured to use WebLM server licensing. • For security, any auto-create settings set to On are automatically set to Off after 24 hours.

Table continues...

Field	Description
SIP Remote Extn Enable	<p>Default = Off.</p> <p>The system can be configured to support remote SIP extensions in the case where NAT is used in the connection path. This could be the case where the IP Office is located behind a corporate NAT/Firewall router and/or the SIP phone is located behind residential NAT enable router.</p> <ul style="list-style-type: none"> • This option cannot be enabled on both LAN1 and LAN2. • The use of this option and the interaction and configuration of external third party elements is beyond the scope this help file. <p>In the case where the public IP address of the corporate router is unknown, the LAN's Network Topology settings should be used to configure a STUN Server. Enabling SIP Remote Extn Enable allows configuration of:</p> <ul style="list-style-type: none"> • the Remote UDP Port, Remote TCP Port, Remote TLS Port settings • the Port Number Range (NAT) settings
SIP Domain Name	<p>Default = Blank</p> <p>This value is used by SIP endpoints for registration with the IP Office system. SIP endpoints register with IP Office using their SIP address that consists of their phone number and IP Office SIP domain. Since IP Office does not allow calls from unauthorized entities, the SIP domain does not need to be resolvable. However, the SIP domain should be associated with FQDN (Fully Qualified Domain Name) for security purposes. The entry should match the domain suffix part of the SIP Registrar FQDN below, for example, <code>example.com</code>. If the field is left blank, registration uses the LAN 1, LAN2, or public IP address.</p> <p> Note:</p> <p>For Avaya SIP telephones supported for resilience, the SIP Domain Name must be common to all systems providing resilience.</p>
SIP Registrar FQDN	<p>Default = Blank</p> <p>The fully-qualified domain name to which the SIP endpoint send their registration requests. For example, <code>sbc.example.com</code>.</p> <ul style="list-style-type: none"> • This FQDN is also used for Avaya Cloud Services and Avaya Push Notification Services <p>The customer DNS must resolve this FQDN to an IP address that routes to the IP Office. That is:</p> <ul style="list-style-type: none"> • For local extensions, the IP address of the IP Office LAN. • For remote extensions, the external IPv4 address of the Avaya SBC or customer firewall that routes to the IP Office.

Related links

[The Setup Wizard/Initial Configuration](#) on page 45

Setup Wizard: Voicemail

Voicemail

Name	Description
Voicemail Type	<p>Sets the type of voicemail service used by the system. The options supported depend on the type of IP Office system.</p> <ul style="list-style-type: none"> • Server Edition Systems <p>These systems are supported by Voicemail Pro running on the primary server. All other servers in the Server Edition network should be set to Centralized Voicemail.</p> • Standalone IP500 V2 Systems <p>These can support a range of options:</p> <ul style="list-style-type: none"> - Voicemail Pro - Use the Voicemail Pro service provided by an IP Office Application server. - Centralized Voicemail - In an SCN network of IP500 V2 systems, only the Voicemail Pro server associated with one IP500 V2 system holds the messages and recording (the centralized voicemail server). All other systems should be set to Centralized Voicemail or Distributed Voicemail. - Embedded Voicemail - Use the voicemail service provided internally by the system itself. This uses the system's System SD card to store messages and prompts. - Group Voicemail - Used with some 3rd-party voicemail services. - Distributed Voicemail - In an SCN network of IP500 V2 systems, only the Voicemail Pro server associated with one IP500 V2 system holds the messages and recording (the centralized voicemail server). However, the other IP500 V2 systems can be associated with their own Voicemail Pro server which handles that systems calls. - Analog Trunk MWI - Use voicemail provided by the analog trunk provider.
Voicemail IP Address	<p>Default = Primary Server IP Address</p> <p>The IP address of the server hosting the voicemail service for the IP Office system.</p>

Hold Music

This section is used to define the source for the system's default music on hold source. Once the system is installed, additional music on hold sources can be configured for specific groups and incoming call routes

- You must ensure that any MOH source you use complies with copyright, performing rights and other local and national legal requirements.

Name	Description
System Source	<p>Select the source the system should use its default music on hold. The options available depend on the type of system.</p> <ul style="list-style-type: none"> • WAV File - Use a WAV file called <code>HoldMusic.wav</code>. The file can be uploaded using the controls below. Note that on Linux systems, the file name is case sensitive. • External - IP500 V2 systems only. Use the audio source connected to the back of the control unit. • Tone - Use of a repeated double tone generated by the system. This tone is also automatically used if, for any of the .WAV file options the has not yet been successfully uploaded. • WAV (Restart): Identical to WAV File above except that for each new listener, the file plays from the beginning. Not supported on IP500 V2 systems.
Select a File Upload	<p>If use of a wav file is selected, use these fields to select and upload the file to the system. The file should be in the following format:</p> <ul style="list-style-type: none"> • PCM • 8kHz 16-bit • Mono • Maximum length: <ul style="list-style-type: none"> - IP500 V2 = 90 seconds. - Linux-based Server = 600 seconds.

Auto Attendants

These settings are shown for an IP500 V2 systems with the **Voicemail Type** set to **Embedded Voicemail**. It allows configuration of auto-attendant services. These can then be used as the destination for external calls in incoming call routes.

Name	Description
Name	<p>Range = Up to 12 characters</p> <p>This field sets the name for the auto-attendant service. This can be used to route calls to the auto-attendant.</p>
Maximum Inactivity	<p>Default = 8 seconds; Range = 1 to 20 seconds.</p> <p>This field sets how long, after playing the prompts, the auto-attendant waits for a valid key press. If exceeded, the call is transferred to the Fallback Extension if set, otherwise the call is disconnected.</p>
AA Number	<p>This number is assigned by the system and cannot be changed. It is used in conjunction with short codes to access the auto attendant service or to record auto attendant greetings.</p>

Table continues...

Name	Description
Direct Dial-By-Number	<p>Default = Off.</p> <p>This setting affects the operation of any key presses in the auto attendant menu set to use the Dial By Number action.</p> <p>If selected, the key press for the action is included in any following digits dialed by the caller for system extension matching. For example, if 2 is set in the actions to Dial by Number, a caller can dial 201 for extension 201.</p> <p>If not selected, the key press for the action is not included in any following digits dialed by the caller for system extension matching. For example, if 2 is set in the actions to Dial by Number, a caller must dial 2 and then 201 for extension 201.</p>
Dial by Name Match Order	<p>Default = First Name/Last Name.</p> <p>Determines the name order used for the Embedded Voicemail Dial by Name function.</p>
Enable Local Recording	<p>Default = On.</p> <p>When off, use of short codes to record auto-attendant prompts is blocked. The short codes can still be used to playback the greetings.</p>

Related links

[The Setup Wizard/Initial Configuration](#) on page 45

Setup Wizard: Subscription

This panel is only shown for subscription mode systems. It display details of the system's subscription settings and the subscriptions obtained.

The panel is only shown on systems that have completed their initial configuration. The settings cannot be edited. For systems going through initial configuration, the subscription settings are set through the **System** panel.

Name	Description
System ID	<p>This is a fixed value against which the system's subscriptions are issued and validated.</p> <ul style="list-style-type: none"> For an IP500 V2 system, this ID is based on the System SD card installed in the system.
Customer ID	The customer ID specified when the system was registered for subscriptions.
License Server Address	The address of the server which provides the system with its subscriptions.

Available Subscriptions

These fields indicate the subscriptions provided to the system. For user subscriptions, the number of subscriptions are shown. For feature subscriptions, true indicates that the system has obtained that subscription.

Related links

[The Setup Wizard/Initial Configuration](#) on page 45

Setup Wizard: Licensing

This panel is shown for non-subscription systems. It allows configuration of where the system should obtain its licenses.

Related links

[The Setup Wizard/Initial Configuration](#) on page 45

Setup Wizard: User

This panel lists the users configured on the system. It allows you to add, delete or edit entries.

For IP500 V2 control units, user and extension records are automatically created for each physical extension port detected at system start.

Related links

[The Setup Wizard/Initial Configuration](#) on page 45

Setup Wizard: Groups

This panel lists the groups configured on the system. It allows you to add, delete or edit entries.

Each group has its own extension number and settings for how calls directed to that number should be presented to the users added to the group.

Related links

[The Setup Wizard/Initial Configuration](#) on page 45

Setup Wizard: Lines

This panel lists the lines configured on the system. It allows you to add, delete or edit entries.

For IP500 V2 control units, line records are automatically created for each physical line detected at system start.

Related links

[The Setup Wizard/Initial Configuration](#) on page 45

Setup Wizard: Incoming Call Routes

You can use this panel to configure where incoming external calls should be routed.

Working Hours Time Profile

These settings are used to define a default time profile for the customer's normal hours of business. This profile is then used to alter the routing of incoming calls inside and outside those times.

Once the system has been configured, additional time profiles can be added if required.

Setting	Description
Start Time	The time when normal working hours begin.
End Time	The time when normal working hours end.
Days	The days of the week when the working hours apply.

Incoming Call Routes

You can create and edit incoming call routes for the lines setup in the previous setup wizard panel. A route is required for each of the incoming line group IDs used for the lines in the system configuration.

Setting	Description
Incoming Line Group ID	Each of the lines in the system is configured with an Incoming Line Group ID. The same ID can be used for on several line. The incoming call route with the same ID is then used to route calls on those lines.
Trunk Identifier	This is a unique name added by the system for the set of trunks
Incoming Number	<p>If required, in addition to matching the Incoming Line Group ID you can also match the incoming number received to route the calls for that number to different destinations.</p> <p>This option is not supported on all trunks. For example it is not supported with analog trunks.</p>
Working Hours Destination	<p>The destination for calls that match the incoming call route during the times defined by the working hours time profile.</p> <p>The destination number can be selected from the drop-down list. This lists:</p> <ul style="list-style-type: none"> • All existing users, groups and auto-attendants. • Voicemail for caller access to voicemail to collect messages. <p>For destinations not listed in the drop-down list, the destination number can be entered manually.</p>
Out of Office Hours Destination	The destination for calls that match the incoming call route outside the times defined by the working hours time profile.

Related links

[The Setup Wizard/Initial Configuration](#) on page 45

Setup Wizard: Outgoing Call Routes

This panel is only shown for systems where the **Locale** is set to **United States (US English)** or **Canada (Canadian French)**.

Telephony Settings

Setting	Description
Directory Overrides Barring	Default = On. When enabled, the Outgoing Call Bar setting on any user is not applied to the dialing of numbers that are in the system directory. This does not affect other methods of call barring.
Bar outgoing calls for Out of Office hours	Default = Off. When enabled, outgoing external calls are barred during times outside the default working hours time profile settings.

Line Selection for Outgoing Calls

Setting	Description
Select Line for Outgoing Calls	This field selects the default outgoing line group ID that should be used for all outgoing calls. That outgoing group ID can be assigned to multiple lines. Outgoing calls will then use any available line that has the same outgoing group ID
Outgoing Group ID	These fields show a summary of the existing outgoing group IDs configured and the lines using those settings. To edit the outgoing line groups use the Lines panel.
Line Information	

Assign Users to Outgoing Route

By default the dialing of external numbers is processed through alternate route selection (ARS) entries in the configuration. These contain setting that control what numbers are allowed, add or remove prefixes, etc.

The default ARS entry is called **Main**. However, the number of additional outgoing call routes exist (**Unrestricted**, **International**, **National** and **Long Distance**). The menu below allows you to select which of these ARS entries should be used by each user.

Setting	Description
Name	The user name.
Outgoing Route	The ARS entry that should be applied to the users outgoing calls. Click on the current setting to select a different ARS entry.

Related links

[The Setup Wizard/Initial Configuration](#) on page 45

Chapter 6: Subscription and COM Support Setup

For systems running in IP Office Subscription mode, the network's primary server is configured with details of a Customer Operations Manager (COM) service. Through that service, the primary server receives subscription entitlements for the users and IP Office services supported by the network.

COM users can see the status of the primary and other servers plus any alarms. COM can also support a range of other support features such as backup, restore, upgrade, remote access. For full details, refer to "[Using Customer Operations Manager for IP Office Subscription Systems](#)".

Related links

[Checking the System Subscriptions](#) on page 61

[Enabling COM Support on Server Edition Systems](#) on page 62

[Enabling Additional COM Support Settings](#) on page 63

[Setting All Servers to Subscription Mode](#) on page 64

Checking the System Subscriptions

Having installed a primary server in subscription mode, the subscriptions received should be checked.

Procedure

1. Connect to the primary server using IP Office Web Manager. See [Starting Web Manager](#) on page 149.
2. Select **System Settings > Subscription**.
3. If the system has successfully connected with the subscription server, the **Available Subscriptions** section will show the number of subscriptions the system has.
4. If the system has not received any subscriptions, check the following configuration settings:
 - a. Check that the **Subscription** settings match those shown in the subscription email received for the customer's system.
 - b. Select **System Settings > System > DNS**. Check that the values matches that used for the customer's network or a know default such as 8 . 8 . 8 . 8.

- c. Select **System Settings > IP Routes**. For the primary server there should be a default route, that is one with the **IP Address** and **IP Subnet Mask** set to 0.0.0.0. For the route, the **Destination** and **Gateway** address should match the customer's network connection for outgoing internet connections.
- d. The system should be set to obtain time from an internet time server. That can be checked through the web control settings (**Settings > System > Date and Time > Enable Network Time Protocol Client**).

Related links

[Subscription and COM Support Setup](#) on page 61

Enabling COM Support on Server Edition Systems

To connect to a customer's IP Office systems, by default Customer Operations Manager (COM) uses the settings of a security user account called **COMAdmin** configured on those systems.

On customer premises systems, the **COMAdmin** security user is disabled by default and doesn't have a password set.

About this task

The process below sets the password for the **COMAdmin** security user and enables the user account.

- The process affects all servers in the network.
- If adding multiple servers, this process can be run when all the servers have been added.
- If at a later date, the customer adds another server to their network, you should repeat this process.

Procedure

1. Connect to the primary server using IP Office Web Manager. See [Starting Web Manager](#) on page 149.
2. Click **Solution**.
3. Click on the **Actions** drop-down and select **Remote Operations Management**.
4. Enter and confirm the password that the systems in the customer solution should use for their COM connection.

Important:

- Note the password with care. It needs to be added to the customer's details in Customer Operations Manager in order to config the connection from COM.
5. Click **Enable & Synch**.
 6. This enables the **COMAdmin** security user account on the primary system and sets its password. The change is then synchronizes to all other systems in the solution. This process can take several minutes depending on the number of systems in the solution.

- When the successful synchronization message appears, click **Cancel**.

Related links

[Subscription and COM Support Setup](#) on page 61

Enabling Additional COM Support Settings

Systems using IP Office Subscription mode can be supported by COM users. In addition to monitor the system status and alarms, the COM users can access a number of additional support options.

About this task

The settings described below are normally automatically configured as required by the system provider or reseller when the system first subscribes. However, it is useful to understand where the settings are set and to check their values.

- These settings are configured on a primary server only. However, they apply to all IP Office servers connected to the primary using a websocket line except for any standalone IP Office Application server.

Procedure

- Connect to the primary server using IP Office Web Manager. See [Starting Web Manager](#) on page 149.
- Select **System Settings > System > Remote Operations**.
- Check the settings are configured as required by the customer:

Setting	Description
Centralized Management	Enables remote connections through COM to the primary IP Office server for IP Office admin tools. Those tools are System Status Application, SysMonitor and IP Office Web Manager.
Centralized Diagnostics Log	When enabled, system log files are regularly automatically uploaded to COM. COM users can also manually request the latest files.
Remote Upgrade/ Backup	When enabled, COM automatically requests a daily backup. COM users can also perform manual backup, restore and upgrade operations.
Remote Access	Support HTTPS, SFTP, SSH and RDP connections to IP Office servers and other servers running on the same network.
Co-located Servers	Extend Remote Access support to other server on the same network as the COM managed IP Office. This can include connection to standalone IP Office Application servers. Connect to other servers and services also requires a tunnel to be added to the IP Office system configuration for the specific connection.

- If you make any changes, click **Update**.

Related links

[Subscription and COM Support Setup](#) on page 61

Setting All Servers to Subscription Mode

All the IP Office servers in a network should operate in the same mode. The administration application will show an alarm if that is not the case.

Procedure

1. Connect to the primary server using IP Office Web Manager. See [Starting Web Manager](#) on page 149.
2. Select **Configure > Set All Nodes to Subscription Mode**.

Related links

[Subscription and COM Support Setup](#) on page 61

Chapter 7: Server PLDS Licensing

For non-subscription system or network, the primary server needs a PLDS license file added. That license file is unique to the PLDS ID of the primary server and the major level of software (for example 11.x) that it is running.

Once the license file has been added, the licenses in that file need to be assigned:

- Some licenses are assigned automatically to reflect the configuration of a particular server. For example, the user profile licenses are assigned to match the users on each system.
- Other licenses are assigned manually. For example you can configure how many SIP channel licenses each system in the network can take from the total number available in the license file.

Related links

[Adding the PLDS License File](#) on page 65

[Assigning PLDS licenses](#) on page 66

Adding the PLDS License File

The primary server (unless in subscription mode) is licensed by the uploading of a PLDS license file to the server. The license file contains license information for both the primary server and for all other IP Office servers in the network.

This process is not application to subscription systems. They obtain their license entitlements using the subscription details entered during their primary server's initial configuration.

Note:

- The PLDS license file is an XML file. It can be opened and view in a text editor. However, making any changes will invalidate the file and cause license errors.

Before you begin

- Obtain the PLDS XML license file for the primary server.

Procedure

1. Connect to the primary server using IP Office Web Manager. See [Starting Web Manager](#) on page 149.
2. Select **Applications > Web License Manager**. The **Web License Manager** opens in a separate browser window.

3. Enter `admin` as the **User Name** and `weblmadmin` as the **Password**.
4. Change the default password by entering the old password again and then entering the new password. Click **Submit**.
5. Login again by entering `admin` and the new password.
6. Click **Install license**.
7. Click **Choose File**. Browse to and select the PLDS XML file.
8. Click **Accept the License Terms & Conditions**.
9. Click **Install**.
10. Click **Licensed product > IPO > IP_Office**. The menu should show a list of the licenses now available to the servers in the primary server's network.
11. Close the **Web License Manager** window.

Next steps

- You can now assign the licenses that the server needs. See [Assigning PLDS licenses](#) on page 66.

Related links

[Server PLDS Licensing](#) on page 65

Assigning PLDS licenses

For systems using PLDS licenses, once the primary server is licensed (see [Adding the PLDS License File](#) on page 65) those licenses can be assigned to systems. Some licenses are assigned automatically based on items in the configuration of the server, for example extension licenses. Other licenses are assigned manually using the process below.

Procedure

1. Login to manager or web manager.
2. Select **System Settings > License**.
3. The **License** tab lists the licenses currently being used by the system.
4. Click on **Remote Server**.
5. Use the **Reserved Licenses** section to specify the number of licenses that the server should request from those specified in the license file loaded on the primary server.
 - Grayed out choices indicate licenses requested automatically based on the server's configuration.
6. Save the new settings.

Next steps

- Once the primary server is configured and correctly licensed, proceed with the secondary server installation. See [Secondary Server Installation and Initial Configuration](#) on page 69.

Related links

[Server PLDS Licensing](#) on page 65

Part 4: Secondary Server Installation

Chapter 8: Secondary Server Installation and Initial Configuration

The Server Edition Secondary server is an optional server which can support additional users, IP trunks, and conference channels.

The secondary server provides resilience to the users, phones and hunt groups configured on the primary server and any expansion servers. It also provides resilience for the voicemail and one-X Portal services normally provided by the primary server.

Once the server software has been installed (see [Server Software Installation](#) on page 27) and the server ignited as a secondary server, it can be configured using the processes in this section.

Important:

- All servers in the network must be configured and licensed for the same operation mode. For example, all as **Server Edition**, **Server Edition – Select** or all as **Sever Edition – Subscription**.
- The primary and secondary servers must be matching servers in terms of supported capacity. See the [Avaya IP Office™ Platform Guidelines: Capacity](#) document. That should include capacity on both servers to support reciprocal resilience of the other server's extensions.

Related links

[Adding a Secondary server using Web Manager](#) on page 69

[Adding a Secondary server using Manager](#) on page 71

[Enabling COM Support on Server Edition Systems](#) on page 74

[Assigning PLDS licenses](#) on page 74

Adding a Secondary server using Web Manager

This process adds the secondary server to the primary server's network. For a new server it also takes the server through its initial configuration.

If required you can separate the two processes. Do that by first logging in to the new server's IP address and completing its initial configuration. Then log in to the primary server's address and add the new server.

Before you begin

- Complete primary server setup and licensing before installing any secondary or expansion server. See [Primary Server Installation and Initial Configuration](#) on page 40.
- Ignite the server as a secondary server. See [Igniting the server](#) on page 35.

Procedure

1. Connect to the primary server using IP Office Web Manager. See [Starting Web Manager](#) on page 149.
2. Click **Solution**.
3. Select **Configure > Add System to Solution**.
4. Select **Secondary server**.
5. Enter the IP address set during its ignition. Otherwise click on **Discovery Preferences** and configure the range of addresses that should be searched.
6. Click **Discover**.
7. From the list of discovered systems, select the required server and click **Next**.
8. If prompted, select the primary server IP address to link and click **OK**.
9. For a newly ignited server, the initial configuration menu server is displayed.
10. In the **System Mode**, select one of the following:

System Mode	Description
Server Edition	Select this option for a primary server that will use a PLDS file for licensing.
Server Edition - Select	Select this option for a primary server that will use a PLDS file for licensing that includes Select licenses. Note that if in a network, all servers in the network requires a Select license.
Server Edition - Subscription	Select this option for a primary server that will use subscriptions for licensing.

11. Set a unique **System Name** for the system. This will appear in other administration menus and helps identify the particular server.
12. If applicable, enter the **Services Device ID** issued for support of the server.
13. Set the **Locale** to match the customer location. Set this accurately as it affects a number of default telephony settings that the system will then use.
14. Set and confirm the **Default Extension Password**. This is used to set the extension password required to register IP extension unless a separate specific password is configured in the extension's own settings.
15. Using the **Public LAN Interface** control:
 - a. Select **LAN1** and check that the **IP Address** and **IP Mask** match the network settings that the server should use for its eth0 port.
 - b. Select which **DHCP Mode** the server should support on the LAN.

Option	Description
Server	The server will act as a DHCP server for the network on that interface. For its own address it will use the IP Address details entered in this menu.
Client	The server will obtain its IP address settings automatically from a DHCP server elsewhere on the network.
Dial In	This DHCP mode is not supported on Linux-based IP Office servers.
Disabled	The server will use the fixed IP address details entered in this menu.

- c. Select **LAN2** and check that the **IP Address** and **IP Mask** settings match the network settings that the server should use for its eth1 port.
 - d. Set the **Gateway** address for the customer network.
16. Having set and checked the IP address and DHCP details, select which port, **LAN1** or **LAN2**, will be used for outgoing connections from the customer network for general internet access. This choice adds a default IP route from that LAN to the specified **Gateway** address.
 17. Check that **Server Edition Primary** is set to the IP address of the primary server.
 18. If the customer network has a specific **DNS Server**, enter its address.
 19. Enter an **Web Socket Password** password. This password is used for the links to other IP Office servers in the network.
 20. Check the settings are all as required and match the customer network requirements.
 21. Click **Next**. The IP Office services on the servers are restarted using the new configuration.

Next steps

- For subscription mode systems:
 - If this is the final system being added, enable COM support on the systems. See [Enabling COM Support on Server Edition Systems](#) on page 74.
 - Otherwise, proceed to adding the expansions servers. See [Expansion Server \(Linux\) Installation and Initial Configuration](#) on page 77 and [Expansion Server \(IP500 V2\) Initial Configuration](#) on page 84.
- For non-subscription systems, assign the licenses required by the server from those available on the networks primary server. See [Assigning PLDS licenses](#) on page 74.

Related links

[Secondary Server Installation and Initial Configuration](#) on page 69

Adding a Secondary server using Manager

This process adds the secondary server to the primary server's network. For a new server it also takes the server through its initial configuration.

Before you begin

- Complete primary server setup and licensing before installing any secondary or expansion server. See [Primary Server Installation and Initial Configuration](#) on page 40.
- Ignite the server as a secondary server. See [Igniting the server](#) on page 35.

Procedure

1. Start Manager. See [Starting IP Office Manager](#) on page 150.
 - a. Click **File > Open Configuration**.
 - b. From the **Select IP Office** menu, select the primary server and click **OK**.
 - c. Enter `Administrator` and the password configured for that user account during the primary server's ignition. Click **OK**.
2. Click **Solution**. On the **Summary** menu, on the right under **Add**, click **Secondary Server**.
3. In the **Add Secondary Server** window, either:
 - Enter the IP address of the server and click **OK**.
 - Click on the search icon. Select the server from those listed and click **OK**.
4. The initial configuration menu for the secondary server is displayed. This is similar to that shown for the primary server.
5. In the **System Mode**, select one of the following:

System Mode	Description
Server Edition	Select this option for a primary server that will use a PLDS file for licensing.
Server Edition - Select	Select this option for a primary server that will use a PLDS file for licensing that includes Select licenses. Note that if in a network, all servers in the network requires a Select license.
Server Edition - Subscription	Select this option for a primary server that will use subscriptions for licensing.

6. Set a unique **System Name** for the system. This will appear in other administration menus and helps identify the particular server.
7. If applicable, enter the **Services Device ID** issued for support of the server.
8. Set the **Locale** to match the customer location. Set this accurately as it affects a number of default telephony settings that the system will then use.
9. Set and confirm the **Default Extension Password**. This is used to set the extension password required to register IP extension unless a separate specific password is configured in the extension's own settings.
10. Using the **Public LAN Interface** control:
 - a. Select **LAN1** and check that the **IP Address** and **IP Mask** match the network settings that the server should use for its eth0 port.
 - b. Select which **DHCP Mode** the server should support on the LAN.

Option	Description
Server	The server will act as a DHCP server for the network on that interface. For its own address it will use the IP Address details entered in this menu.
Client	The server will obtain its IP address settings automatically from a DHCP server elsewhere on the network.
Dial In	This DHCP mode is not supported on Linux-based IP Office servers.
Disabled	The server will use the fixed IP address details entered in this menu.

- c. Select **LAN2** and check that the **IP Address** and **IP Mask** settings match the network settings that the server should use for its eth1 port.
 - d. Set the **Gateway** address for the customer network.
11. Having set and checked the IP address and DHCP details, select which port, **LAN1** or **LAN2**, will be used for outgoing connections from the customer network for general internet access. This choice adds a default IP route from that LAN to the specified **Gateway** address.
 12. Check that **Server Edition Primary** is set to the IP address of the primary server.
 13. If the customer network has a specific **DNS Server**, enter its address.
 14. Enter an **Web Socket Password** password. This password is used for the links to other IP Office servers in the network.
 15. Check the settings are all as required and match the customer network requirements.
 16. Click **Save**. The server's configuration is opened in manager. At this stage it has not been saved to the system.
 17. Click **File > Save Configuration**
 18. Check that the **Change Mode** is set to **Reboot** and click **OK**.
 19. Click **Next**. The IP Office services on the servers are restarted using the new configuration.
 20. For non-subscription systems, assign the licenses required by the server in the same way as done for the primary server. See [Assigning PLDS licenses](#) on page 66.

Next steps

- For subscription mode systems:
 - If this is the final system being added, enable COM support on the systems. See [Enabling COM Support on Server Edition Systems](#) on page 74.
 - Otherwise, proceed to adding the expansions servers. See [Expansion Server \(Linux\) Installation and Initial Configuration](#) on page 77 and [Expansion Server \(IP500 V2\) Initial Configuration](#) on page 84.
- For non-subscription systems, assign the licenses required by the server from those available on the networks primary server. See [Assigning PLDS licenses](#) on page 74.

Related links

[Secondary Server Installation and Initial Configuration](#) on page 69

Enabling COM Support on Server Edition Systems

About this task

The process below sets the password for the **COMAdmin** security user and enables the user account.

- The process affects all servers in the network.
- If adding multiple servers, this process can be run when all the servers have been added.
- If at a later date, the customer adds another server to their network, you should repeat this process.

Procedure

1. Connect to the primary server using IP Office Web Manager. See [Starting Web Manager](#) on page 149.
2. Click **Solution**.
3. Click on the **Actions** drop-down and select **Remote Operations Management**.
4. Enter and confirm the password that the systems in the customer solution should use for their COM connection.

 **Important:**

- Note the password with care. It needs to be added to the customer's details in Customer Operations Manager in order to config the connection from COM.
5. Click **Enable & Synch**.
 6. This enables the **COMAdmin** security user account on the primary system and sets its password. The change is then synchronizes to all other systems in the solution. This process can take several minutes depending on the number of systems in the solution.
 7. When the successful synchronization message appears, click **Cancel**.

Related links

[Secondary Server Installation and Initial Configuration](#) on page 69

Assigning PLDS licenses

For systems using PLDS licenses, once the primary server is licensed (see [Adding the PLDS License File](#) on page 65) those licenses can be assigned to systems. Some licenses are assigned automatically based on items in the configuration of the server, for example extension licenses. Other licenses are assigned manually using the process below.

Procedure

1. Login to manager or web manager.

2. Select **System Settings > License**.
3. The **License** tab lists the licenses currently being used by the system.
4. Click on **Remote Server**.
5. Use the **Reserved Licenses** section to specify the number of licenses that the server should request from those specified in the license file loaded on the primary server.
 - Grayed out choices indicate licenses requested automatically based on the server's configuration.
6. Save the new settings.

Next steps

- Once the secondary server is licensed, proceed with installation of any Linux-based expansion servers. See [Expansion Server \(Linux\) Installation and Initial Configuration](#) on page 77.

Related links

[Secondary Server Installation and Initial Configuration](#) on page 69

Part 5: Expansion Server Installation

Chapter 9: Expansion Server (Linux) Installation and Initial Configuration

Having installed the primary server, and if required the optional secondary server, you can now install and add expansion servers. An expansion server can be used to support additional extensions and lines in a separate location.

- This section covers installing a Linux-based expansion server. For an IP500 V2 based expansion server, see [Expansion Server \(IP500 V2\) Initial Configuration](#) on page 84.

Related links

[Adding an Expansion Server Using Web Manager](#) on page 77

[Adding an Expansion Server Using Manager](#) on page 79

[Enabling COM Support on Server Edition Systems](#) on page 82

[Assigning PLDS licenses](#) on page 82

Adding an Expansion Server Using Web Manager

Use this procedure to add a Linux-based Server Edition Expansion System.

If required you can separate the two processes. Do that by first logging in to the new server's IP address and completing its initial configuration. Then log in to the primary server's address and add the new server.

Before you begin

- Install and license the network's primary and secondary servers before installing any expansion servers. See

[Primary Server Installation and Initial Configuration](#) on page 40 and [Secondary Server Installation and Initial Configuration](#) on page 69.

- Ignite the server as an expansion server. See [Igniting the server](#) on page 35.

Procedure

1. Connect to the primary server using IP Office Web Manager. See [Starting Web Manager](#) on page 149.

2. Click **Solution**.
3. Select **Configure > Add System to Solution**.
4. Select **Expansion server**.
5. Enter the IP address set during its ignition. Otherwise click on **Discovery Preferences** and configure the range of addresses that should be searched.
6. Click **Discover**.
7. From the list of discovered systems, select the required server and click **Next**.
8. If prompted, select the primary server and secondary server IP addresses and click **OK**.
9. For a newly ignited server, the initial configuration menu server is displayed.
10. In the **System Mode**, select one of the following:

System Mode	Description
Server Edition	Select this option for a primary server that will use a PLDS file for licensing.
Server Edition - Select	Select this option for a primary server that will use a PLDS file for licensing that includes Select licenses. Note that if in a network, all servers in the network requires a Select license.
Server Edition - Subscription	Select this option for a primary server that will use subscriptions for licensing.

11. Set a unique **System Name** for the system. This will appear in other administration menus and helps identify the particular server.
12. If applicable, enter the **Services Device ID** issued for support of the server.
13. Set the **Locale** to match the customer location. Set this accurately as it affects a number of default telephony settings that the system will then use.
14. Set and confirm the **Default Extension Password**. This is used to set the extension password required to register IP extension unless a separate specific password is configured in the extension's own settings.
15. Using the **Public LAN Interface** control:
 - a. Select **LAN1** and check that the **IP Address** and **IP Mask** match the network settings that the server should use for its eth0 port.
 - b. Select which **DHCP Mode** the server should support on the LAN.

Option	Description
Server	The server will act as a DHCP server for the network on that interface. For its own address it will use the IP Address details entered in this menu.
Client	The server will obtain its IP address settings automatically from a DHCP server elsewhere on the network.

Table continues...

Option	Description
Dial In	This DHCP mode is not supported on Linux-based IP Office servers.
Disabled	The server will use the fixed IP address details entered in this menu.

- c. Select **LAN2** and check that the **IP Address** and **IP Mask** settings match the network settings that the server should use for its eth1 port.
 - d. Set the **Gateway** address for the customer network.
16. Enter the IP address of the **Server Edition Primary**.
 17. For **Server Edition Secondary**, enter the IP address of the planned secondary server. If there is no plan to add a secondary server, enter a dummy address.
 18. For a **Server Edition - Select** and **Server Edition - Subscription** network, you can selection whether the primary or secondary should provide the voicemail services for the expansion server.
 19. If the customer network has a specific **DNS Server**, enter its address.
 20. Enter an **Web Socket Password** password. This password is used for the links to other IP Office servers in the network.
 21. Check the settings are all as required and match the customer network requirements.
 22. Click **Save**. The server's configuration is opened in manager. At this stage it has not been saved to the system.
 23. Click **File > Save Configuration**
 24. Check that the **Change Mode** is set to **Reboot** and click **OK**.
 25. Click **Next**. The IP Office services on the servers are restarted using the new configuration.

Next steps

- For subscription mode systems, if this is the final system being added, enable COM support on the systems. See [Enabling COM Support on Server Edition Systems](#) on page 82:
- For non-subscription systems, assign the licenses required by the server from those available on the networks primary server. See [Assigning PLDS licenses](#) on page 74.

Related links

[Expansion Server \(Linux\) Installation and Initial Configuration](#) on page 77

Adding an Expansion Server Using Manager

Use this procedure to add a Linux-based Server Edition Expansion System.

Before you begin

- Install and license the network's primary and secondary servers before installing any expansion servers. See

[Primary Server Installation and Initial Configuration](#) on page 40 and [Secondary Server Installation and Initial Configuration](#) on page 69.

- Ignite the server as an expansion server. See [igniting the server](#) on page 35.

Procedure

1. Start Manager. See [Starting IP Office Manager](#) on page 150.
 - a. Click **File > Open Configuration**.
 - b. From the **Select IP Office** menu, select the primary server and click **OK**.
 - c. Enter `Administrator` and the password configured for that user account during the primary server's ignition. Click **OK**.
2. Click **Solution**. On the **Summary** menu, on the right under **Add**, click **Expansion Server**.
3. In the Add Expansion System window, either:
 - Enter the IP address of the server and click **OK**.
 - Click on the search icon. Select the server from those listed and click **OK**.
4. The initial configuration menu for the expansion server is displayed.
5. In the **System Mode**, select one of the following:

System Mode	Description
Server Edition	Select this option for a primary server that will use a PLDS file for licensing.
Server Edition - Select	Select this option for a primary server that will use a PLDS file for licensing that includes Select licenses. Note that if in a network, all servers in the network requires a Select license.
Server Edition - Subscription	Select this option for a primary server that will use subscriptions for licensing.

6. Set a unique **System Name** for the system. This will appear in other administration menus and helps identify the particular server.
7. If applicable, enter the **Services Device ID** issued for support of the server.
8. Set the **Locale** to match the customer location. Set this accurately as it affects a number of default telephony settings that the system will then use.
9. Set and confirm the **Default Extension Password**. This is used to set the extension password required to register IP extension unless a separate specific password is configured in the extension's own settings.
10. Using the **Public LAN Interface** control:
 - a. Select **LAN1** and check that the **IP Address** and **IP Mask** match the network settings that the server should use for its eth0 port.
 - b. Select which **DHCP Mode** the server should support on the LAN.

Option	Description
Server	The server will act as a DHCP server for the network on that interface. For its own address it will use the IP Address details entered in this menu.
Client	The server will obtain its IP address settings automatically from a DHCP server elsewhere on the network.
Dial In	This DHCP mode is not supported on Linux-based IP Office servers.
Disabled	The server will use the fixed IP address details entered in this menu.

- c. Select **LAN2** and check that the **IP Address** and **IP Mask** settings match the network settings that the server should use for its eth1 port.
 - d. Set the **Gateway** address for the customer network.
11. Enter the IP address of the **Server Edition Primary**.
 12. For **Server Edition Secondary**, enter the IP address of the planned secondary server. If there is no plan to add a secondary server, enter a dummy address.
 13. For a **Server Edition - Select** and **Server Edition - Subscription** network, you can selection whether the primary or secondary should provide the voicemail services for the expansion server.
 14. If the customer network has a specific **DNS Server**, enter its address.
 15. Enter an **Web Socket Password** password. This password is used for the links to other IP Office servers in the network.
 16. Check the settings are all as required and match the customer network requirements.
 17. Click **Save**. The server's configuration is opened in manager. At this stage it has not been saved to the system.
 18. Click **File > Save Configuration**
 19. Check that the **Change Mode** is set to **Reboot** and click **OK**.
 20. Click **Next**. The IP Office services on the servers are restarted using the new configuration.

Next steps

- For subscription mode systems, if this is the final system being added, enable COM support on the systems. See [Enabling COM Support on Server Edition Systems](#) on page 82:
- For non-subscription systems, assign the licenses required by the server from those available on the networks primary server. See [Assigning PLDS licenses](#) on page 74.

Related links

[Expansion Server \(Linux\) Installation and Initial Configuration](#) on page 77

Enabling COM Support on Server Edition Systems

About this task

The process below sets the password for the **COMAdmin** security user and enables the user account.

- The process affects all servers in the network.
- If adding multiple servers, this process can be run when all the servers have been added.
- If at a later date, the customer adds another server to their network, you should repeat this process.

Procedure

1. Connect to the primary server using IP Office Web Manager. See [Starting Web Manager](#) on page 149.
2. Click **Solution**.
3. Click on the **Actions** drop-down and select **Remote Operations Management**.
4. Enter and confirm the password that the systems in the customer solution should use for their COM connection.

 **Important:**

- Note the password with care. It needs to be added to the customer's details in Customer Operations Manager in order to config the connection from COM.
5. Click **Enable & Synch**.
 6. This enables the **COMAdmin** security user account on the primary system and sets its password. The change is then synchronizes to all other systems in the solution. This process can take several minutes depending on the number of systems in the solution.
 7. When the successful synchronization message appears, click **Cancel**.

Related links

[Expansion Server \(Linux\) Installation and Initial Configuration](#) on page 77

Assigning PLDS licenses

For systems using PLDS licenses, once the primary server is licensed (see [Adding the PLDS License File](#) on page 65) those licenses can be assigned to systems. Some licenses are assigned automatically based on items in the configuration of the server, for example extension licenses. Other licenses are assigned manually using the process below.

Procedure

1. Login to manager or web manager.

2. Select **System Settings > License**.
3. The **License** tab lists the licenses currently being used by the system.
4. Click on **Remote Server**.
5. Use the **Reserved Licenses** section to specify the number of licenses that the server should request from those specified in the license file loaded on the primary server.
 - Grayed out choices indicate licenses requested automatically based on the server's configuration.
6. Save the new settings.

Next steps

- Repeat the process of installation for any other Linux-based expansion servers.
- Then proceed with installation of any IP500 V2 expansion servers. See [Expansion Server \(IP500 V2\) Initial Configuration](#) on page 84.

Related links

[Expansion Server \(Linux\) Installation and Initial Configuration](#) on page 77

[Expansion Server \(IP500 V2\) Initial Configuration](#) on page 84

Chapter 10: Expansion Server (IP500 V2) Initial Configuration

Having installed the primary server, and if required the optional secondary server, you can now install and add expansion servers. An expansion server can be used to support additional extensions and lines in a separate location.

This section covers the initial configuration of an IP500 V2 expansion server. For an Linux-based expansion server, see [Expansion Server \(Linux\) Installation and Initial Configuration](#) on page 77.

These details should be used in conjunction with the documentation for installation of the IP500 V2 hardware:

- For a subscription system: ["Deploying an IP500 V2 IP Office Subscription System"](#)
- For other systems: ["Deploying an IP500 V2 IP Office Essential Edition System"](#)

Related links

[Initial IP500 V2 Configuration using Web Manager](#) on page 84

[Initial IP500 V2 Configuration using Manager](#) on page 86

[Adding an IP500 V2 Expansion using Web Manager](#) on page 88

[Adding an IP500 V2 Expansion using Manager](#) on page 89

[Enabling COM Support on Server Edition Systems](#) on page 90

[Assigning PLDS licenses](#) on page 82

Initial IP500 V2 Configuration using Web Manager

Before you begin

Assembly and setup of the IP500 V2 hardware following the instructions in the appropriate document:

- For a subscription system: ["Deploying an IP500 V2 IP Office Subscription System"](#)
- For other systems: ["Deploying an IP500 V2 IP Office Essential Edition System"](#)

Procedure

1. Using IP Office Web Manager, connect directly to the new IP500 V2 system.
2. Login using the default user name `Administrator` and password `Administrator`.

3. You are prompted to change the default passwords.

Password	Description
Administrator Password	This password is used for access to the system's telephony and security configuration.
Security Administrator Password	This password is used for access to the system's security configuration only.
System Password	This password is used for system upgrades and can also be used for connections using SysMonitor.

4. The server's initial configuration menu is now shown. Ensure that you select the correct **System Mode**. Either:
- For a subscription system: **Server Edition Expansion - Subscription**.
 - For other systems: **Server Edition Expansion**.
5. Set a unique **System Name** for the system. This will appear in other administration menus and helps identify the particular server.
6. If applicable, enter the **Services Device ID** issued for support of the server.
7. Set the **Locale** to match the customer location. Set this accurately as it affects a number of default telephony settings that the system will then use.
8. Set and confirm the **Default Extension Password**. This is used to set the extension password required to register IP extension unless a separate specific password is configured in the extension's own settings.
9. Using the **Public LAN Interface** control:
- a. Select **LAN1** and check that the **IP Address** and **IP Mask** match the network settings that the server should use for its eth0 port.
 - b. Select which **DHCP Mode** the server should support on the LAN.

Option	Description
Server	The server will act as a DHCP server for the network on that interface. For its own address it will use the IP Address details entered in this menu.
Client	The server will obtain its IP address settings automatically from a DHCP server elsewhere on the network.
Dial In	This DHCP mode is not supported on Linux-based IP Office servers.
Disabled	The server will use the fixed IP address details entered in this menu.

- c. Select **LAN2** and check that the **IP Address** and **IP Mask** settings match the network settings that the server should use for its eth1 port.
 - d. Set the **Gateway** address for the customer network.
10. Enter the IP address of the **Server Edition Primary**.
11. For **Server Edition Secondary**, enter the IP address of the planned secondary server. If there is no plan to add a secondary server, enter a dummy address.

12. For a **Server Edition - Select** and **Server Edition - Subscription** network, you can selection whether the primary or secondary should provide the voicemail services for the expansion server.
13. If the customer network has a specific **DNS Server**, enter its address.
14. Enter an **Web Socket Password** password. This password is used for the links to other IP Office servers in the network.
15. Check the settings are all as required and match the customer network requirements.
16. Click **Apply**.
17. The configuration menu provides a range of other options. For an expansion system these can be skipped and the system configured once it is part of the full network. Click **Save to IP Office**.
18. Select **Immediate** and click **OK**.

Next steps

- Once the server has restarted (approximately 6 minutes), the new expansion server can be added to the network. See [Adding an IP500 V2 Expansion using Web Manager](#) on page 88.

Related links

[Expansion Server \(IP500 V2\) Initial Configuration](#) on page 84

Initial IP500 V2 Configuration using Manager

Before you begin

Assembly and setup of the IP500 V2 hardware following the instructions in the appropriate document:

- For a subscription system: ["Deploying an IP500 V2 IP Office Subscription System"](#)
- For other systems: ["Deploying an IP500 V2 IP Office Essential Edition System"](#)

Procedure

1. Using Manager, connect directly to the new IP500 V2 system.
2. Login using the default user name `Administrator` and password `Administrator`.
3. You are prompted to change the default passwords.

Password	Description
Administrator Password	This password is used for access to the system's telephony and security configuration.
Security Administrator Password	This password is used for access to the system's security configuration only.

Table continues...

Password	Description
System Password	This password is used for system upgrades and can also be used for connections using SysMonitor.

4. The server's initial configuration menu is now shown. Ensure that you select the correct **System Mode**. Either:
 - For a subscription system: **Server Edition Expansion - Subscription**.
 - For other systems: **Server Edition Expansion**.
5. Set a unique **System Name** for the system. This will appear in other administration menus and helps identify the particular server.
6. If applicable, enter the **Services Device ID** issued for support of the server.
7. Set the **Locale** to match the customer location. Set this accurately as it affects a number of default telephony settings that the system will then use.
8. Set and confirm the **Default Extension Password**. This is used to set the extension password required to register IP extension unless a separate specific password is configured in the extension's own settings.
9. Using the **Public LAN Interface** control:
 - a. Select **LAN1** and check that the **IP Address** and **IP Mask** match the network settings that the server should use for its eth0 port.
 - b. Select which **DHCP Mode** the server should support on the LAN.

Option	Description
Server	The server will act as a DHCP server for the network on that interface. For its own address it will use the IP Address details entered in this menu.
Client	The server will obtain its IP address settings automatically from a DHCP server elsewhere on the network.
Dial In	This DHCP mode is not supported on Linux-based IP Office servers.
Disabled	The server will use the fixed IP address details entered in this menu.

- c. Select **LAN2** and check that the **IP Address** and **IP Mask** settings match the network settings that the server should use for its eth1 port.
 - d. Set the **Gateway** address for the customer network.
10. Enter the IP address of the **Server Edition Primary**.
11. For **Server Edition Secondary**, enter the IP address of the planned secondary server. If there is no plan to add a secondary server, enter a dummy address.
12. For a **Server Edition - Select** and **Server Edition - Subscription** network, you can selection whether the primary or secondary should provide the voicemail services for the expansion server.
13. If the customer network has a specific **DNS Server**, enter its address.

14. Enter an **Web Socket Password** password. This password is used for the links to other IP Office servers in the network.
15. Check the settings are all as required and match the customer network requirements.
16. Click **Save**. The server's configuration is opened in manager. At this stage it has not been saved to the system.
17. Click **File > Save Configuration**
18. Check that the **Change Mode** is set to **Reboot** and click **OK**.

Next steps

- Once the server has restarted (approximately 6 minutes), the new expansion server can be added to the network. See [Adding an IP500 V2 Expansion using Manager](#) on page 89.

Related links

[Expansion Server \(IP500 V2\) Initial Configuration](#) on page 84

Adding an IP500 V2 Expansion using Web Manager

This process adds an IP500 V2 control unit to the network as an expansion server.

Before you begin

- Complete the IP500 V2 system's initial configuration. See [Initial IP500 V2 Configuration using Manager](#) on page 86.

Procedure

1. Connect to the primary server using IP Office Web Manager. See [Starting Web Manager](#) on page 149.
2. Click **Solution**.
3. Select **Configure > Add System to Solution**.
4. Select **Expansion server**.
5. Enter the IP address set during its ignition. Otherwise click on **Discovery Preferences** and configure the range of addresses that should be searched.
6. Click **Discover**.
7. From the list of discovered systems, select the required server and click **Next**.
8. If prompted, select the primary server IP address to link and click **OK**.
9. For a newly ignited server, the initial configuration menu server is displayed.
10. Click **Save**. The server's configuration is opened in manager. At this stage it has not been saved to the system.
11. Click **File > Save Configuration**

12. Check that the **Change Mode** is set to **Reboot** and click **OK**.
13. Click **Next**. The IP Office services on the servers are restarted using the new configuration.

Next steps

- For subscription mode systems, if this is the final system being added, enable COM support on the systems. See [Enabling COM Support on Server Edition Systems](#) on page 90:
- For non-subscription systems, assign the licenses required by the server from those available on the networks primary server. See [Assigning PLDS licenses](#) on page 74.

Related links

[Expansion Server \(IP500 V2\) Initial Configuration](#) on page 84

Adding an IP500 V2 Expansion using Manager

This process adds an IP500 V2 control unit to the network as an expansion server.

Before you begin

- Complete the IP500 V2 system's initial configuration. See [Initial IP500 V2 Configuration using Manager](#) on page 86.

Procedure

1. Start Manager. See [Starting IP Office Manager](#) on page 150.
 - a. Click **File > Open Configuration**.
 - b. From the **Select IP Office** menu, select the primary server and click **OK**.
 - c. Enter `Administrator` and the password configured for that user account during the primary server's ignition. Click **OK**.
2. Click **Solution**. On the **Summary** menu, on the right under **Add**, click **Expansion Server**.
3. In the Add Expansion System window, either:
 - Enter the IP address of the server and click **OK**.
 - Click on the search icon. Select the server from those listed and click **OK**.
4. If the initial configuration menu appears for the server, complete it. See [Initial IP500 V2 Configuration using Manager](#) on page 86.
5. Click **File > Save Configuration**
6. Check that the **Change Mode** is set to **Reboot** and click **OK**.
7. Click **Next**. The IP Office services on the servers are restarted using the new configuration.
8. For non-subscription systems, assign the licenses required by the server in the same way as done for the primary server. See [Assigning PLDS licenses](#) on page 66.

Next steps

- For subscription mode systems, if this is the final system being added, enable COM support on the systems. See [Enabling COM Support on Server Edition Systems](#) on page 90:
- For non-subscription systems, assign the licenses required by the server from those available on the networks primary server. See [Assigning PLDS licenses](#) on page 74.

Related links

[Expansion Server \(IP500 V2\) Initial Configuration](#) on page 84

Enabling COM Support on Server Edition Systems

About this task

The process below sets the password for the **COMAdmin** security user and enables the user account.

- The process affects all servers in the network.
- If adding multiple servers, this process can be run when all the servers have been added.
- If at a later date, the customer adds another server to their network, you should repeat this process.

Procedure

1. Connect to the primary server using IP Office Web Manager. See [Starting Web Manager](#) on page 149.
2. Click **Solution**.
3. Click on the **Actions** drop-down and select **Remote Operations Management**.
4. Enter and confirm the password that the systems in the customer solution should use for their COM connection.

Important:

- Note the password with care. It needs to be added to the customer's details in Customer Operations Manager in order to config the connection from COM.
5. Click **Enable & Synch**.
 6. This enables the **COMAdmin** security user account on the primary system and sets its password. The change is then synchronizes to all other systems in the solution. This process can take several minutes depending on the number of systems in the solution.
 7. When the successful synchronization message appears, click **Cancel**.

Related links

[Expansion Server \(IP500 V2\) Initial Configuration](#) on page 84

Assigning PLDS licenses

For systems using PLDS licenses, once the primary server is licensed (see [Adding the PLDS License File](#) on page 65) those licenses can be assigned to systems. Some licenses are assigned automatically based on items in the configuration of the server, for example extension licenses. Other licenses are assigned manually using the process below.

Procedure

1. Login to manager or web manager.
2. Select **System Settings > License**.
3. The **License** tab lists the licenses currently being used by the system.
4. Click on **Remote Server**.
5. Use the **Reserved Licenses** section to specify the number of licenses that the server should request from those specified in the license file loaded on the primary server.
 - Grayed out choices indicate licenses requested automatically based on the server's configuration.
6. Save the new settings.

Next steps

- Repeat the process of installation for any other Linux-based expansion servers.
- Then proceed with installation of any IP500 V2 expansion servers. See [Expansion Server \(IP500 V2\) Initial Configuration](#) on page 84.

Related links

[Expansion Server \(Linux\) Installation and Initial Configuration](#) on page 77
[Expansion Server \(IP500 V2\) Initial Configuration](#) on page 84

Part 6: Application Server Installation

Chapter 11: Application Server Installation

The installation process for an application server is similar to that for other Linux-based IP Office servers:

1. Use the standard server software installation. See [Server Software Installation](#) on page 27.
2. Ignite the server as an application server. See [Igniting the server](#) on page 35.
3. Continue with the processes in this section of the documentation:
 - a. For use with subscription mode IP Office systems, set the service user password. See [Service User Configuration for COM Support](#) on page 93. This needs to be done before initial configuration of the application server.
 - b. Perform the application server's initial configuration. See [Application Server Initial Configuration](#) on page 94.

Related links

[Service User Configuration for COM Support](#) on page 93

[Application Server Initial Configuration](#) on page 94

Service User Configuration for COM Support

Subscription mode IP Office systems can be remotely managed through Customer Operations Management (COM). That is, they can be remotely configured, upgraded, backed up, restored and various other services.



For IP Office R11.1 FP2 and higher, the same functionality can also include any application server associated with the subscription mode IP Office systems. To support that, a websocket connection is configured between the application server and IP Office systems it is supporting.

About this task

If using the application server with a subscription mode IP Office system, use the following process to set the password for the websocket connected required between the two servers to allow COM support of the application server. This password is required for the initial configuration of the application server.

Procedure

1. Connect to the IP Office system using IP Office Web Manager. See [Starting Web Manager](#) on page 149.

2. Select **Security > Security Settings**
3. Click **Service Users**.
4. Locate the **Adjunct Server** service user and click .
5. Click the  icon next to **Password** and enter the password for the websocket connection between the two servers.
6. Change the service user's **Account Status** to **Enabled**.
7. Click **Save**.

Next steps

- Perform the initial configuration of the application server. See [Application Server Initial Configuration](#) on page 94.

Related links

[Application Server Installation](#) on page 93

Application Server Initial Configuration

Before you begin

1. Complete the installation and licensing/subscription of the IP Office system which the application server will be supporting.
2. If the IP Office server is being managed through COM, ensure that the adjunct server service user password has been set. See [Service User Configuration for COM Support](#) on page 93.
3. Ignite the server as an application server. See [Igniting the server](#) on page 35.

Procedure

1. Connect to the application server using IP Office Web Manager. See [Starting Web Manager](#) on page 149.
2. Set a unique **System Name** for the system. This will appear in other administration menus and helps identify the particular server.
3. If applicable, enter the **Services Device ID** issued for support of the server.
4. If the customer network has a specific **DNS Server**, enter its address.
5. Set the **Locale** to match the customer location. Set this accurately as it affects a number of default telephony settings that the system will then use.
6. In **IP Office FQDN/IP Address**, enter the address of the IP Office system which the application server will be supporting.
7. For the **Adjunct Server Password**, enter the password set for the Adjunct Server service user configured on the IP Office system which the application server will be supporting. See [Service User Configuration for COM Support](#) on page 93.

8. Using the **Public LAN Interface** control:
- Select **LAN1** and check that the **IP Address** and **IP Mask** match the network settings that the server should use for its eth0 port.
 - Select which **DHCP Mode** the server should support on the LAN.

Option	Description
Server	The server will act as a DHCP server for the network on that interface. For its own address it will use the IP Address details entered in this menu.
Client	The server will obtain its IP address settings automatically from a DHCP server elsewhere on the network.
Dial In	This DHCP mode is not supported on Linux-based IP Office servers.
Disabled	The server will use the fixed IP address details entered in this menu.

- Select **LAN2** and check that the **IP Address** and **IP Mask** settings match the network settings that the server should use for its eth1 port.
 - Set the **Gateway** address for the customer network.
9. Click **Apply**.

Next steps

The remaining stages depend on whether the application server will be supporting a Server Edition network or an IP500 V2 systems.

- **Server Edition:** See [Application Server configuration in a Server Edition network](#) on page 96.
- **IP500 V2:** See [Application Server Configuration for IP500 V2 Support](#) on page 99.

Related links

[Application Server Installation](#) on page 93

Chapter 12: Application Server configuration in a Server Edition network

An IP Office Application Server can be used to provide Avaya one-X Portal services for the primary or secondary server in a Server Edition network. When doing this, you must the existing portal service on the Server Edition server and configure the server with details of the application server.

Related links

[Disabling the local portal service](#) on page 96

[Entering the address of the remote portal service](#) on page 97

[Adding the application server to the network](#) on page 97

Disabling the local portal service

Before you begin

- **Ignite the server as an application server:** See [igniting the server](#) on page 35.

Procedure

1. Login to the web control/platform view menus on the primary or secondary server which the application server is supporting.
2. If the **one-X Portal** service is shown as running, click **Stop**.
3. Check that the **Auto Start** option next to the service is not selected.

Next steps

- **Enter the remote portal service address:** See [Entering the address of the remote portal service](#) on page 97.

Related links

[Application Server configuration in a Server Edition network](#) on page 96

Entering the address of the remote portal service

When using the portal service provided by an application server, the primary or secondary server needs to be configured with the address of the application server.

Before you begin

- Disable the local portal service: See [Disabling the local portal service](#) on page 96.

Procedure

1. Login to the web control/platform view menus on the primary or secondary server which the application server is supporting.
2. Select **Settings > General**
3. In the **one-X Portal Settings** section, untick **Use Local IP**.
4. In the **Remote IP** field, enter the address of the application server.
5. Click **Save**.

Next steps

- **Add the application server to the Server Edition solution:** See [Adding the application server to the network](#) on page 97.

Related links

[Application Server configuration in a Server Edition network](#) on page 96

Adding the application server to the network

Before you begin

- **Enter the remote portal service address:** See [Entering the address of the remote portal service](#) on page 97.

Procedure

1. Connect to the primary server using IP Office Web Manager. See [Starting Web Manager](#) on page 149.
2. Select the **Solution** view.
3. Click on **Solution Settings**.
4. Click **Application Server** and select **Add**.
5. Enter the IP address of the application server and click **Add**.

Next steps

- **Configure the remote portal service:** See [one-X Portal Configuration](#) on page 110.

Application Server configuration in a Server Edition network

Related links

[Application Server configuration in a Server Edition network](#) on page 96

Chapter 13: Application Server Configuration for IP500 V2 Support

Having ignited the server as an application server (see [Igniting the server](#) on page 35), each of the services that it is intended to support need to be configured separately.

- **Voicemail Pro:** See [Voicemail Server Configuration](#) on page 101.
- **one-X Portal for IP Office:** See [one-X Portal Configuration](#) on page 110.
- **WebRTC Gateway:** See [Configuring the WebRTC Gateway](#) on page 116.
- **Media Manager:** Refer to the [Administering Avaya IP Office™ Platform Media Manager](#) manual.

Part 7: Application Configuration

Chapter 14: Voicemail Server Configuration

By default the voicemail service is started automatically on the server is configured as a primary or secondary server. It is also started automatically on an IP Office Application server if selected as a service during the server's ignition process.

Related links

[Configuring Voicemail Pro](#) on page 101

[Adding TTS Languages](#) on page 102

[Downloading and installing the Voicemail Pro client](#) on page 103

[Enabling Voicemail Pro client connection](#) on page 103

[Logging into Voicemail Pro server](#) on page 104

Configuring Voicemail Pro

The Voicemail Pro application provides the mailbox services for all users and hunt groups created in the IP Office configuration. In a setup where there is a single IP Office and Voicemail Pro server you need not do any configuration. This section describes only the minimum steps that Avaya recommends to ensure that the Voicemail Pro server operates correctly and is secure.

For more details about IP Office and Voicemail Pro configuration, such as enabling TTS, or enabling exchange integration, see the ["Administering IP Office Voicemail Pro"](#) manual.

About this task

Add the Voicemail Pro licenses in IP Office Server Edition Manager.

Note:

A single instance of IP Office Server Edition provides only two Voicemail Pro channels. The number of Voicemail Pro channels that the system displays depends on the number of instances of IP Office Server Edition. If you have licenses for any additional channels, you must add those licenses as well.

In a resilience setup, when Server Edition Primary is not active, the system displays a voicemail failure message even though Voicemail Pro is working. The system displays a voicemail failure message for the Voicemail Pro on Server Edition Primary that is not active.

Related links

[Voicemail Server Configuration](#) on page 101

Adding TTS Languages

The Voicemail Pro application can use Text-to-speech (TTS). This can be done using either locally installed TTS or, for subscription systems, TTS provide by Google services.

- Google TTS does not require any installation, just configuration of the Speeach UI setting in the system configuration. When configured, Google TTS overrides locally installed TTS.
- The process below covers the installation of local TTS. The TTS languages are downloadable as 3 separate DVD's. To use these TTS languages, you need to upload and install the additional languages on the server or servers running the Voicemail Pro application.

Warning:

- TTS files from pre-11.1 releases are not compatible with R11.1.
- During this process, the server needs to restart the voicemail service each time it installs a new TTS language.

Checking the TTS Languages Installed

1. Access the server's web control/platform view menus.
2. Select **Updates**.
3. In the list of **Services**, each TTS language is shown with the prefix TTS.

Downloading the TTS Languages

1. The supported TTS languages can be downloaded as a set of 3 ISO files from support.avaya.com.

1. Select the IP Office release and locate the Text-to-Speech for IP Office Server Edition and Application Server link.
2. Download the ISO image containing the languages required:
 - **DVD 1:** English, Spanish, French, German, Italian.
 - **DVD 2:** Swedish, Norwegian, Finnish, Dutch, Danish, Portuguese, Greek.
 - **DVD 3:** Chinese, Polish, Russian.
3. The individual RPM installation files for each file can be extracted from the ISO files by treating them as zipped archives.

Adding a New Language

Note that this process will cause the voicemail service to be restarted, ending all calls currently being handled by the voicemail service.

1. Access the server's web control/platform view menus.
2. Select **Settings | General**.
3. In the **Software Repositories** section, click on the **Browse** button for **Application**. Browse to and select the RPM file for the required language and click **OK**.
4. Click **Add**.
5. Select **Updates**.

6. In the **Services** section, locate the newly added TTS language. Click **Install**.

Related links

[Voicemail Server Configuration](#) on page 101

Downloading and installing the Voicemail Pro client

About this task

The Voicemail Pro client can be downloaded and installed from the web-control menus of a server. The client is a Windows application.

Procedure

1. Access the server's web control menus. See [Accessing the Server's Web Control Menus](#) on page 150.
2. Click **AppCenter** tab.
3. In the **Download Applications** section, click the `.exe` file link for Voicemail Pro client.
4. Download the file following the process used by your browser.
5. Once the file has been downloaded, run the `.exe` file to install the client.

Related links

[Voicemail Server Configuration](#) on page 101

Enabling Voicemail Pro client connection

About this task

Connection to the voicemail service by the Windows Voicemail Pro client can be enabled or disabled. This process enables connection.

Procedure

1. Login to the server hosting the voicemail service.
2. Select **Applications > Voicemail Pro - System Preferences** Applications | Voicemail Pro - System Preferences.
3. Select the **General** tab.
4. Change the status of **Enable Voicemail Pro Client Interface** to allow connection using the client.

Related links

[Voicemail Server Configuration](#) on page 101

Logging into Voicemail Pro server

Before you begin

To log into a Voicemail Pro server you should configure an *Administrator* user name and password on the Voicemail Pro server. The default user name for Voicemail Pro server is *Administrator* and the password is *Administrator*.

 **Note:**

To ensure that the system is secure you must always change the default password.

About this task

To log into Voicemail Pro server using Voicemail Pro client, do the following:

Procedure

1. Click **Start**.
2. Select **Program >IP Office > Voicemail Pro Client**.

The system displays Select Voicemail Pro Client Mode window. If you started the client before, the system attempts to start in the same mode that you used earlier. If you start the client for the first time, the system displays the Select Voicemail Pro Client Mode dialog box.

3. Select **Online**.

The system displays VmPro Login dialog box.

4. Type *Administrator* in the **User Name** field.
5. Type the pass word in the **User Password** field.

The default password is *Administrator*.

6. Type the IP address of the voicemail server in the **Unit Name \ IP Address** field.
You can also click **Browse** to search for Voicemail Pro server in the local network.
7. Click **Login**.

 **Note:**

After three unsuccessful attempts to login as an *Administrator* the system locks the *Administrator* account for an hour.

Next steps

Change the default password for Voicemail Pro *Administrator* account.

1. In the Voicemail Pro client, select **File > Change Password**.
2. Type the new password in the **New Password** and **Verify New Password** fields.
3. Click **OK**.

Related links

[Voicemail Server Configuration](#) on page 101

Backing up and restoring voicemail

Backing up Voicemail Pro

You can take a backup of voicemail, user settings & greetings, call flows, modules and conditions, module recordings, campaigns, and system settings on a local drive. You can take backup once everyday, every week or every month.

 **Note:**

To perform a backup and restore always use Web Manager. For more information, see [Backing up and restoring the server](#) on page 129 . If you use Voicemail Pro to backup and restore, the system does not provide the integrations.

About this task

To take a backup of the voicemail server do the following:

Procedure

1. Launch Voicemail Pro client.
2. Log in as *Administrator*.
3. Select **Administration > Preferences > General**.
4. Click the **Housekeeping** tab.
5. Click **Backup Now**.

The system displays the various backup options. For more information on the backup settings, see the *Administering Voicemail Pro* document.

6. Click **OK** to start backup.

Related links

[Voicemail Server Configuration](#) on page 101

Restoring Voicemail Pro stored on IP Office Server Edition server

You can restore the voicemails, user settings & greetings, call flows, modules and conditions, module recordings, campaigns, and system settings that were backed up on a local drive.

 **Note:**

Use this procedure to restore voicemail backups for the Release 8.0, 8.1 and 8.1 FP1. To restore the voicemail backup of Release 9.0 always use Web Manager. For more information, see [Restoring IP Office Server Edition server](#) on page 107

Before you begin

- Ensure that you shutdown all the services on the server.
- Start Linux Platform settings.

- Login as *Administrator*.

Ensure that you shutdown all the services on the server.

About this task

To restore a backup file that is stored on IP Office Server Edition server:

Procedure

1. Select **Settings > General**.
2. Select **Restore** in the **Backup and Restore**.

Note:

You can only restore the backup files for the voicemail using Linux Platform settings. You can restore a complete backup data set. You cannot select a particular item that needs to be restored.

Result

The system displays a list of backup files, select the backup file you want to restore.

Related links

[Voicemail Server Configuration](#) on page 101

Migrating Voicemail Pro to IP Office Server Edition

Related links

[Voicemail Server Configuration](#) on page 101

[Backing up an existing Voicemail Pro server](#) on page 106

[Restoring Voicemail Pro not stored on IP Office Server Edition server](#) on page 107

[Backup and restore limitations](#) on page 108

Backing up an existing Voicemail Pro server

When you replace an existing Voicemail Pro server with IP Office Server Edition server you must take a backup of all the settings, prompts and messages from the existing server. If the existing server is a Linux based server, you must use SSH file transfer to retrieve the backup files from the server. If the existing server is a Windows based server you copy the backup files on a folder in the server and then use the SSH file transfer to migrate the back up files to IP Office Server Edition server.

About this task

To take backup of an existing Voicemail Pro server:

Procedure

1. Log in to Voicemail Pro server using Voicemail Pro client.

You can use the **File > Voicemail Shutdown > Suspend Calls** to display the number of voicemail sessions that are active. You can stop any new sessions or end the sessions before to take a backup.

2. Select **Preferences >General**.
3. Click the **Housekeeping** tab.
4. Select **Backup Now**.
5. Select all the backup options for a complete backup and click **OK**.

The time take to complete a backup varies depending on the number of mailboxes and messages that Voicemail Pro server supports.

The system creates a backup of folder. The name of the folder includes the date and time of the backup and Immediate. For example, *VMPro_Backup_26012011124108_Immediate*.

Next steps

Shutdown the voicemail server:

1. Select **File>Voicemail Shutdown > Shutdown**.
2. Select **Shut Down Immediately**.

Related links

[Migrating Voicemail Pro to IP Office Server Edition](#) on page 106

Restoring Voicemail Pro not stored on IP Office Server Edition server

Before you begin

Ensure that you shutdown all the services on the server.

About this task

To restore a backup file that is not stored on IP Office Server Editions server:

Procedure

1. Connect to IP Office Server Edition using an SSH File transfer tool.
 - a. Type the IP address of IP Office Server Edition server in the **Host Name** field.
 - b. Type the **User Name** as *Administrator*.
 - c. Set the **Protocol** as **SFTP/SSH**.
 - d. Set the **Port** as **22**.

When you connect to IP Office Server Edition using an SSH File transfer tool for the first time the system prompts you to accept the trusted key. Accept the trusted key.
 - e. Type the password for the *Administrator*. The default password for the *Administrator* is *Administrator*.
2. Copy the backup folder in the `/opt/vmpro/Backup/Scheduled/OtherBackups`.
3. Login as an Administrator into IP Office Server Edition using the Web Control Panel.
4. Select **Settings > General**.
5. Select **Restore** in the **Backup and Restore**.

*** Note:**

You can only restore the backup files for the voicemail using the Web Control Panel. You can restore a complete backup data set. You cannot select a particular item that needs to be restored.

Result

The system displays a list of backup files, select the backup file you want to restore.

Related links

[Migrating Voicemail Pro to IP Office Server Edition](#) on page 106

Backup and restore limitations

If you have created extra folders on the Voicemail Pro server, in IP Office Server Edition server these folders are not included in the restore process. Instead the extra folders need to be copied manually. For example, if you created a folder containing custom prompts for use in call flows in addition to the default language folders used for prompts, then the system does not backup or restore the custom folder. To resolve this, the extra folders must be backed up and restored manually. In the following example, a folder *Custom* is manually copied from an existing server to create a backup. It is then manually restored.

Before you begin

Using SSH file transfer tool copy the folder *Custom* from `/opt/vmpro` in the old server to your computer to create a backup of the folder.

About this task

To restore the *Custom* folder, using an SSH file transfer tool, copy the folder to the `/home/Administrator` folder on the IP Office Server Edition server:

Procedure

1. Login to the command line interface of the system using the root user password. You can log in directly on the IP Office Server Edition server or remotely using an SSH File transfer tool.
 - Log in directly to the IP Office Server Edition server:
 - a. At the `Command:` prompt, type `login`
 - b. At the `login:` prompt, type `Administrator`
 - c. At the `Password:` prompt, type the default password `Administrator`
 - Log in as `Administrator` using the SSH file transfer tool.
 - . The default password is `Administrator`
2. In a new terminal window at the command prompt, type `admin`
The system prompts for a password. The default password is `Administrator`
3. At the `Admin >` prompt, type `root`

4. Type the `root` password. The default password is `Administrator`

The system displays the root user prompt. For example, `root@<name of the server>`

```
*****
*           IP Office for Linux           *
*                                         *
*       WARNING: Authorised Access Only   *
*****

Welcome Administrator it is Wed Jun 13 05:05:03 BST 2012
> admin
Please enter password:
Admin> root
Password:
[root@localhost ~]#
```

5. Type `cd /home/Administrator`
6. Type `mv Custom /opt/vmpro`

Next steps

Using the SSH file transfer tool, verify that the *Custom* folder has been copied to `/opt/vmpro`

Related links

[Migrating Voicemail Pro to IP Office Server Edition](#) on page 106

Chapter 15: one-X Portal Configuration

For the primary and secondary servers in a Server Edition network, the portal services is normally automatically configured and started. The processes in this section of the documentation are typically only needed for the installation of an IP Office Application server.

Related links

[one-X Portal Service Initial Configuration](#) on page 110

[Configuring portal users](#) on page 112

[Administering a standalone portal server](#) on page 112

[If the Portal Server Status Remains Yellow](#) on page 113

one-X Portal Service Initial Configuration

For the primary and secondary servers in a Server Edition network, the portal services is normally automatically configured and started. The processes in this section of the documentation are typically only needed for the installation of an IP Office Application server.

Procedure

1. Open a web browser and enter `https://` followed by the IP address of the IP Office Application Server and then: `9443/onexportal-admin.html`.
2. The login menu appears. If the message “System is currently unavailable - please wait” appears, the one-X Portal for IP Office application is still starting. When the message disappears, you can login.
3. Enter the default administrator name (Administrator) and password (Administrator) and click **Login**.
4. The **License Agreement** page appears. When you have read the license, select **Have Read & Agree** and then click on **Next**.
5. The menu now allows entry of the IP address of the IP Office system to which you want the portal to connect.
 - In the following menus, the Status icon is used to show/hide status messages about the installation process.
 - You can enter the addresses of multiple IP Office systems in your network. For IP Office Release 10 and higher, you can enter just one address. The one-X Portal for IP Office is informed by that system about the others systems in the network and

about the voicemail server. However, this takes a while to occur after initial installation and assumes that the security settings of all the systems are the same. If you want to configure portal resiliency at this stage, enter the address of both the primary and secondary IP Office systems.

6. Enter the addresses in the form and select **Check IP Office(s)**. The one-X Portal for IP Office server will attempt to connect to each of the indicated systems. The amber background will change to green if this is successful.
7. Click on **Advanced Installation** and expand the **Advanced Provider Options** section.
 - a. Select **Telephony (CSTA)**. If you changed the password used for the IP Office system's **EnhTcpsaService** user, set the same password here.
 - b. Select **Directory (IP Office)**. Check that the provider address and port match those expected.
 - c. If the customer has an LDAP directory source that they want used for the external directory, select **Directory (LDAP)**. Enter the details for the LDAP connection.
 - d. Select **VoiceMail-Provider**. Enter the IP address of the voicemail server. If the application server is running the voicemail service, set this to the IP address of the application server.
 - e. Select **IM/Presence**. Enter the DNS domain name that the server should use for IM/presence service.
8. Note: This step is only possible if the addresses of both the primary and secondary IP Offices were entered at the start. If the application server is going to be used to support a Server Edition network, expand the Resiliency Configuration option. In a Server Edition network, separate portal services can be associated with the network's primary server and its secondary server. While normally only the primary portal server is active, the secondary can become active if the primary is unavailable for some reason. For further details of portal resiliency, refer to the Administering Avaya one-X Portal for IP Office manual.
 - a. If the application server is supporting the primary server in a Server Edition network and portal resilience is required, select **Primary**.
 - b. If the application server is supporting the secondary server in a Server Edition network and portal resilience is required, select **Secondary**.
 - c. Complete the table of addresses for the primary and secondary portal and IP Office services.
9. Click on **Configure for IP Office(s)**. The one-X Portal for IP Office server will connect with each IP Office and automatically extract details of the IP Office users. If **Simple Installation** was selected, the installer will go through this and the following steps automatically. If **Advanced Installation** was selected, the installer will require you to select **Next** after each step.
10. Having extracted user details, the one-X Portal for IP Office server extracts directory details from the IP Office systems.

11. The one-X Portal for IP Office server now prompts you to change the password used for administrator access.
 - a. Enter a new password and click **Change Password**. The initial configuration is complete. Note that it will still be at least another 5 minutes before the one-X Portal for IP Office is usable by end users.
 - b. You now have access to the one-X Portal for IP Office administration menus. For full details refer to the Administering one-X Portal for IP Office manual.
12. Click on **Log Out**.
13. Click on **User Login** shown top-right.
14. The login window will display System in currently unavailable. When this message is no longer displayed, attempt to login as a user.

Related links

[one-X Portal Configuration](#) on page 110

Configuring portal users

Portal only supports users with an appropriate user profile licensed by license file or subscription.

Procedure

1. Connect to the primary server using IP Office Web Manager. See [Starting Web Manager](#) on page 149.
2. Select **Call Management > Users**.
3. Select the user you want to edit.
4. Check that their **Profile** is set to one of the following: **Office Worker**, **Teleworker**, **Power User** or **Unified Communications User**.
5. Select **Enable one-X Portal Services**.
6. Click **Update**.

Related links

[one-X Portal Configuration](#) on page 110

Administering a standalone portal server

By default the Server Edition Primary uses its own portal service running on the same server. However, where required a separate IP Office Application server running portal can be installed, referred to as a 'standalone portal server'. The primary server is then configured to use the portal service on the standalone server.

Procedure

1. Access the server's web control menus. See [Accessing the Server's Web Control Menus](#) on page 150.
2. Select **Settings > General** in the tab select .
3. In the **one-X Portal Settings** section, clear **Use Local IP**.
4. Select **System > Services**.
5. Click **Stop** to stop the services of Avaya one-X® Portal for IP Office on Server Edition Primary server.
6. Clear **Auto Start** for Avaya one-X® Portal for IP Office on Server Edition Primary server.
7. Go to **Settings > General**.
8. In the **one-X Portal Settings** section, type the IP address of the separate Avaya one-X® Portal in the **Remote IP** field.
9. Click **Save**.
10. In the **Home** tab, click **one-X Portal**.

Related links

[one-X Portal Configuration](#) on page 110

If the Portal Server Status Remains Yellow

The most likely cause for the one-X Portal for IP Office service not working and remaining yellow in the platform view of the services is a password mismatch. The mismatch is between the EnhTcpaService service user in the IP Office system's security settings and two of the providers within the portal configuration (the **Default-CSTA-Provider** and the **Default-DSML-IPOProvider**).

This password mismatch causes the IP Office to automatically lock the EnhTcpaService user account.

Procedure

1. Change the portal provider passwords to the new, strong password:
 - a. Login to the portal services administrator menus. You can do this by logging in to the portal server's Web Manager menus, clicking on **Applications** and selecting **one-X Portal**.
 - b. Click **Configuration** and select **Providers**.
 - c. Set the **Provider Name** field to **Telephony (CSTA)**.
 - d. Click on the edit icon next to the listed provider.
 - e. Set the **Password** and click **Save**.
 - f. Set the **Provider Name** field to **Directory (IP-Office)** and repeat the process.

2. Stop the one-X Portal for IP Office service:
 - a. Login to the server's web manager menus.
 - b. From the **Solution** page, click on the icon next to the portal server and select **Platform View**.
 - c. Stop the **one-X Portal** service. Wait until the status icon changes to red.
3. Change the password of the **EnhTcpaService** service user:
 - a. Click on **Security Manager** and select **Service Users**.
 - b. Click on the edit icon for the **EnhTcpaService** user.
 - c. Set the **Password** to the same as was set for the portal providers above and click **Save**.
 - d. Change the **Account Status** back to **Enabled**.
 - e. Click **Update**.
4. Restart the one-X Portal for IP Office service:
 - a. Select the platform view for the portal server again.
 - b. Start the **one-X Portal** service. Wait for the status icon to change to green. This can take up to 5 minutes.

Related links

[one-X Portal Configuration](#) on page 110

Chapter 16: Avaya one-X Portal WebRTC Configuration

This section refers to the **WebRTC Gateway** service running on the same server as the **one-X Portal** service. This service is used for WebRTC clients that connect through Avaya one-X® Portal for IP Office. For remote clients, refer also to [Deploying Remote IP Office SIP Phones with an ASBCE](#)

Supported clients are:

- The Avaya one-X® Portal for IP Office Chrome browser client.
- The Avaya Spaces Chrome browser extension for Space Calling.

 **Note:**

- IP Office User Portal uses the separate WebRTC gateway provided by the IP Office service rather than Avaya one-X Portal.

System Requirements

- IP Office Release R11.0 or higher.
- For non-IP Office Subscription mode IP500 V2 system, licenses to support Avaya one-X Portal.

User Requirements

- The user browser needs to be configured with the server certificate.
- Windows or macOS Chrome.
- PC with speaker and microphone. Optional camera for video calls.
- Configured as Avaya one-X Portal user.

Related links

[Enabling the WebRTC Service](#) on page 115

[Enable SIP Support](#) on page 116

[Configuring the WebRTC Gateway](#) on page 116

[Testing and Logging WebRTC](#) on page 118

[WebRTC External Client Access](#) on page 120

Enabling the WebRTC Service

In addition to the portal service, the IP Office Web Client client uses two additional services.

Procedure

1. Login to the server's web configuration menus.
2. Click **Solutions**.
3. In the displayed list of systems, click on the icon next to the required system and select **Platform View**.
4. Click on **Show optional services**.
5. Check that the **WebRTC Gateway** service is ticked to automatically start.
6. Check that both services have started. If necessary, click the **Start** button next to each service.

Related links

[Avaya one-X Portal WebRTC Configuration](#) on page 115

Enable SIP Support

To allow the use of the WebRTC clients, the IP Office system needs to be configured as a SIP registrar to support SIP extensions. This is then used from the media connection between the IP Office service and the WebRTC Gateway service.

Related links

[Avaya one-X Portal WebRTC Configuration](#) on page 115

Configuring the WebRTC Gateway

The following settings are for the WebRTC gateway service being run by the application server.

Procedure

1. Login to the server's web configuration menus.
2. Click **Solutions**.
3. Click **Applications** and select **WebRTC Configuration**.

Important:

- To access the WebRTC Gateway configuration settings in IP Office Web Manager, you must login using an account that belongs to a security rights group that has WebRTC Gateway Administrator rights enabled. That is configured through the servers security setting using IP Office Manager.
4. On the **System Settings** menu, check the settings:

Setting	Description
Network Interface	For information only. This is the server interface used by the gateway service.
Local IP Address	For information only. This is the current IP address associated with the selected Network Interface.
Gateway Listen Port	This is the port on which the gateway listens for any incoming calls from the IP Office system. This setting is used when configuring an application server for operation with an IP500 V2.
SIP Trunk Listen Port	This is the port on which the gateway listens for SIP trunk connections from the IP Office system. Not currently used.
Logging Level	This sets the level of logging used by the gateway. The log files, prefixed WebRTCGateway, can be downloaded through the server's web control/platform view menus (Logs > Download). The default setting is Info .
Allow Origins	This field sets the domains and/or IP addresses from which the WebRTC gateway service will accept web socket (IP Office service) connections. Multiple entries can be added, each separated by ; semi-colon.

- Click **Save** to save any changes.
- On the **SIP Server Settings** menu, adjust the settings to match the SIP extension configuration of the IP Office system:

Setting	Description
Configuration Mode	For Server Edition servers, the Automatic setting can be used. That automatically configures the gateway to match other IP Office service settings. For an application server, select Manual .
Domain Name	Set this field to match the domain name configured in the SIP Registrar settings of the IP Office system.
Private IP Address	Set this to the address of the IP Office system configured as the SIP registrar for WebRTC client users.
Private TCP Port Private UDP Port Private TLS Port	Set these fields to match the protocol ports configured for the SIP registrar on the IP Office.
Public IP Address	Leave this set to 0.0.0.0 to use the application server's IP address.
Public TCP Port Public UDP Port Public TLS Port	Use these fields to set the ports that should be used for each protocol by client applications.
Transport Type	Select the protocol that the gateway and clients should use. This must match the Layer 4 Protocol settings of the IP Office SIP Registrar . <ul style="list-style-type: none"> Do not enable a protocol unless it is intended to be used. Most phones and clients only use the first enabled protocol they support, in the order TLS, TCP, UDP. They will not rollover to another enabled protocol if problems are encountered in previous protocol.

- Click **Save** to save any changes.

8. Select the **Media Gateway Settings** menu and adjust the settings if required:

Setting	Description
RTP Port Range (Private)	These fields set the minimum and maximum RTP ports for connections between the gateway services and the IP Office system.
RTP Port Range (Public)	These fields set the minimum and maximum RTP ports for connections from the WebRTC clients. If supporting external clients, these ports should be allowed for routing to the gateway server in the customer's external firewalls. Ensure that these do not overlap with the RTP port range configured for the IP Office SIP registrar.
Codecs - Audio	Use this list to adjust the order of codec preference. It is recommended that both the PCM codec choices are kept at the top of the list.
Codecs - Video	Currently VP8 is the only supported video codec.
DTMF Payload Type	Default = 101 This field set the default value for RFC2833 payload negotiation. This value is used with clients and services that do not support dynamic payload negotiation.
STUN/TURN Settings	
The following setting allow the media gateway to be used with external clients via STUN and TURN servers. If enabled, the settings need to match the STUN/TURN server. For details of doing this with an Avaya Session Border Controller for Enterprise, refer to the "IP Office SIP Phones with ASBCE" manual.	
STUN Server Address	Default = 0.0.0.0 (Disabled) The gateway service can use STUN to attempt to resolve issues caused by network address translation (NAT) being applied to traffic between it and external clients. The gateway attempts to use STUN if a STUN server address is set.
STUN Server Port	Sets the port used for connection to the STUN server. The default is 3478.
TURN Server Address	Default = 0.0.0.0 (Disabled) The gateway service can use TURN to attempt to resolve issues caused by network address translation (NAT) being applied to traffic between it and external clients. Unlike STUN, all traffic is routed via a TURN server. The gateway attempts to use TURN if a TURN server address is set.
TURN Server Port	Sets the port used for connection
TURN User Name TURN Password	Enter the name and password of the account on the TURN server if authentication is being used.

9. Click **Save** to save any changes.

Related links

[Avaya one-X Portal WebRTC Configuration](#) on page 115

Testing and Logging WebRTC

You can obtain log messages from the WebRTC Gateway service.

Related links

[Avaya one-X Portal WebRTC Configuration](#) on page 115

[Setting the Server's Logging Level](#) on page 119

[Downloading Server Log Files](#) on page 119

[Viewing WebRTC Log Messages](#) on page 119

[Running the WebRTC Test Application](#) on page 120

Setting the Server's Logging Level

You can adjust the level of details recorded by the server in its WebRTC log files.

Procedure

1. Login to the server's web manager menus. See [Starting Web Manager](#) on page 149.
2. Click **Solution**.
3. Click **Applications** and select **WebRTC Configuration**.
4. On the **System Settings** menu, set the **Logging Level** required.
 - **Info** is the normal level for an operating system.
 - Select **Debug** when necessary to resolve existing issues.
 - **Trace** provides maximum detail if **Debug** proves insufficient to resolve the issue.
5. Click **Save** to save any changes.

Related links

[Testing and Logging WebRTC](#) on page 118

Downloading Server Log Files

Use the following process to download the server's WebRTC log files.

Procedure

1. Access the server's web control menus. See [Accessing the Server's Web Control Menus](#) on page 150.
2. Click on **Logs** and select the **Download** sub tab.
3. Click on the **Create Archive** button.
4. Download the **WebRTC Gateway** log file from the list.

Related links

[Testing and Logging WebRTC](#) on page 118

Viewing WebRTC Log Messages

The WebRTC Gateway server includes a packet monitoring service. You can use this service to view WebRTC messages as they occur or to view the contents of downloaded WebRTC log files.

Procedure

1. Browse to `http://<server_address>:9443/netz`.
2. Select the function required:
 - For **Live Monitoring**, login with the user name/password details of a WebRTC client user.
 - To display packet information previously downloaded in RTCmon log files, select **Offline Analyzer**
3. Click **Start** to collect and display data on the clients WebRTC calls.

Related links

[Testing and Logging WebRTC](#) on page 118

Running the WebRTC Test Application

To check basic WebRTC client connection, the WebRTC Gateway service includes a simple test application. You can also use this to generate log traffic in the WebRTC logs to investigate issues.

Procedure

1. Browse to `http://<server_address>:9443/PhoneService`.
2. Login using the user details of a user configured for portal use.

Related links

[Testing and Logging WebRTC](#) on page 118

WebRTC External Client Access

External client access uses the following ports. These ports need to be enabled and correctly routed to the WebRTC Gateway:

- TCP/HTTPS/Web Socket access on port 9443. Not adjustable.
- TCP or TLS on the public ports range set in the WebRTC Gateway service configuration. The defaults are 56000 to 58000.
- To handle address translation between the external and internal networks, the WebRTC Gateway supports STUN and TURN.
- The devices used must also support the security certificate CA chain as the WebRTC Gateway.

Using an Avaya Session Border Controller for Enterprise

All the above requirements can be configured on an Avaya Session Border Controller for Enterprise. Refer to the [Deploying Remote IP Office SIP Phones with an ASBCE](#) manual.

The basic steps required are:

1. Enable STUN and TURN operation on the Avaya Session Border Controller for Enterprise and in the WebRTC Gateway settings.
2. Create a reverse proxy policy for HTTPS connections to the server hosting the WebRTC Gateway service.
3. Add security certificates that use the same CA source to the ABSCE and create a TLS profile that uses those certificates.

Related links

[Avaya one-X Portal WebRTC Configuration](#) on page 115

Part 8: Backup/Restore

Chapter 17: Backup and Restore

This chapter looks at how the web manager menus can be used to configure backup and restore operation between servers.

- If the IP Office server hard disk has sufficient capacity, you can use it to receive backups from other IP Office servers. However, this is not a suitable solution for its own backups. Therefore, the recommendation is to backup to another IP Office server.
- Within a primary/secondary server pair, you can configure reciprocal backups.
- The preferred option is a separate backup server. This can be done by installing an IP Office Application server with a sufficiently large hard disk (see [Disk space required for backups](#) on page 126) and no services (Voicemail Pro and Avaya one-X Portal) enabled.

Warning:

- Backup/restore is not supported between different server software release levels. Any exceptions are specifically documented in software release notes and migration documents.
- You cannot restore data to a server unless either the IP Address or the system id (LAN1 MAC address) match the server from which it was backed up.
- Backup and restore action must only be performed using servers inside a secure, trusted network.

Related links

- [Backup and restore policy](#) on page 124
- [Backup and restore protocols](#) on page 125
- [Enabling HTTP backup support](#) on page 125
- [Disk space required for backups](#) on page 126
- [Checking the backup server's backup quota](#) on page 127
- [Backup data sets](#) on page 127
- [Creating a remote server connection](#) on page 129
- [Backing up a server/servers](#) on page 129
- [Restoring from the backup server](#) on page 130
- [Restoring a failed server](#) on page 131

Backup and restore policy

It is essential to implement a comprehensive, robust and secure backup policy as part of a Business Continuity plan before any failure or other data restoration requirement. It is not possible to define a single approach that would meet all possible customer needs. Each installation should be assessed and an backup policy implemented. .

Backup Key Information

The backup process supported by web manager only includes specific data, see [Backup data sets](#) on page 127. There is key information which, though included in the backup data, should also be recorded separately in case it is necessary to rebuild a failed sever:

- The ignition settings for each server should be recorded. For example, IP address and host name settings, server role, etc. These details may be required if a full reinstallation of the server becomes necessary before any data restoration operation.

In addition, the following are not included in the web manager backup processes and so must be backed up using other manual processes.

- Copies of any PLDS license key files used by the system.
- If using web manager to load custom voicemail prompts, copies of those prompt files.
- Copies of any custom phone settings files plus phone screen saver and background images.

Backup Schedule

In addition to performing backups before major system changes such as an software upgrade, you must consider having a regular backup schedule.

- Periodic configuration backup for every IP Office.
- Periodic configuration backup for one X Portal – Server Edition Primary server and Application Server only
- Periodic configuration backup for Voicemail Pro – Server Edition Primary server only
- Periodic voice mailbox and recording data backup – Server Edition Primary server only
- The period and number of unique instances selected should reflect the frequency of change, the consequence due to data loss, and the storage capacity of the backup data server. It should also be bourne in mind that the backup server used will only retain up to 14 backups, after which any further backup will cause the automatic deletion of the oldest previous backup.
- The timing of backup operation: This should be done when little or no traffic is present on the target system(s), but the backup process itself is not service-affecting.

Additional Backup Options

This documentation only looks at the backup/restore process provided through the server's own web manager menus. The IP Office Manager and Voicemail Pro client application also provide methods for backing up the current IP Office service configuration and the voicemail configuration/mailbox contents respectively. Therefore also consider:

- Manual backup of the IP Office service configurations before major configuration changes.
- Manual backup of the Voicemail Pro before major configuration changes.

Related links

[Backup and Restore](#) on page 123

Backup and restore protocols

Backup and restore is only supported using another IP Office server as the backup server. If necessary, an IP Office Application Server can be installed without enabling the Voicemail Pro and one-X Portal for IP Office services on that server.

 **Warning:**

- Backup and restore action must only be performed using servers inside a secure, trusted network.

The server being backed up requires a remote server connection to the backup server. That connection is configured with the settings below (see [Creating a remote server connection](#) on page 129). For a set of networked servers, the connection from the primary server is used for all the servers.

Protocol	Port	Path	User Name/Password	Notes
HTTPS	5443	/avaya/backup	none	HTTPS backup is enabled by default.
HTTP	8000	/avaya/backup	none	HTTP backup is disabled by default. To enable it on the backup server, see Enabling HTTP backup support.
SFTP	22	/var/www/html/avaya/backup	Administrator account.	–

Related links

[Backup and Restore](#) on page 123

Enabling HTTP backup support

By default, HTTP support for backup/restore is disabled. You can enable it using the following process on the backup server.

 **Security alert:**

- Backup and restore action must only be performed using servers inside a secure, trusted network.

Enabling HTTP Backup Support on the Backup Server

1. Login to the web manager menus of the backup server.
2. Select the servers **Platform View** option.

3. Within the platform view menus, select **Settings > System > HTTP Server**.
4. Select the **Enable HTTP file store for backup/restore** option and click **Save**.

Related links

[Backup and Restore](#) on page 123

Disk space required for backups

The space required for a backup is highly variable. It depends on the number of servers included in the backup and the data sets selected. However, the largest and most significant backup is that required for voicemail.

The following tables show the potential space required for a worst case full backup. That is, one that assumes all the users have used their voicemail mailbox and other facilities to their maximum capacity.

The minimum disk size column indicates the disk hard disk size required to have a sufficiently large backup quota (see above) for at least one maximum full backup.

Backup for a Sever Edition Network

Users	Maximum Full backup	Minimum Backup Server Disk Size
100	35GB	160GB
750	78GB	214GB
1500	127GB	275GB
2000	158GB	320GB
2500	189GB	360GB

Backup for an IP Office Application Server

Users	Maximum Full backup	Minimum Backup Server Disk Size
20	30GB	160GB
50	32GB	160GB
100	34GB	160GB
150	37GB	165GB

Related links

[Backup and Restore](#) on page 123

Checking the backup server's backup quota

Backup is supported to a server with a hard disk of 160GB or larger. The actual portion of that space, the backup quota, available for backup usage can be checked using the process below. On servers with a smaller hard disk, no backup quota is supported.

Estimating the Backup Quota

The approximate space that will be allocated for the backup quota can be calculated as follows:

- Backup Quota = (0.8 x Hard Disk Capacity) – 92GB if the Hard Disk Capacity is greater than 160GB, otherwise zero.
 - The capacities are all approximate. The quoted disk capacity from a disk manufacturer or a virtual server platform will differ from the capacity reported by the operating system.
 - For example: For a 500GB hard disk, the backup quota is approximately 308GB.

Checking the Backup Server's Backup Quota

Once a server is installed, the actual space allocated for backups can be checked as follows:

1. Login to the backup server's web manager menus.
2. Click and select **Platform View**.
3. On the **System** tab, note the **Quota available for backup data** value. Note this is the total space usable for backups, it does not account for the space already used by any existing backups.
4. Click **Solution** to exit the platform view.

Related links

[Backup and Restore](#) on page 123

Backup data sets

Each backup can include multiple selected servers. Within that backup a number of different data sets can be selected for inclusion in the backup.

The table summarizes the data included in the different backup data sets. Some data sets are greyed out if the related service is not running on one of the servers included in the backup.

When performing a restore it is also possible to select which servers and which data sets are included in the restore operation.

Data Set	Options	Contents
IP Office Sets	IP Office Configuration	<p>When selected for Linux-based IP Office servers:</p> <ul style="list-style-type: none"> • Server Settings • Web Management Settings • IP Office Service Configuration • IP Office Security Settings • DHCP Allocations • Call logs <p>When selected for IP500 V2 Expansion systems:</p> <ul style="list-style-type: none"> • IP Office Configuration • IP Office Security Settings • DHCP Allocations • Call logs
one-X Portal Sets	one-X Portal Configuration	one-X Portal server settings
Voicemail Pro Set	Voicemail Pro Configuration	<ul style="list-style-type: none"> • Voicemail Pro server preferences • Call flows
	Messages & Recordings	<ul style="list-style-type: none"> • Voicemail mailbox contents
	Voicemail Pro Full	<ul style="list-style-type: none"> • Voicemail Pro server preferences • Call flows • Mailbox contents including greetings, announcements and name prompts. <p>Note: This does not include any custom prompts from the Web Manager customer prompts folder. Separate manual copies of those prompts must be kept.</p>
	Selective Voicemail Users	This option backs up a group of preselected mailboxes. The mailbox group is specified through Applications > Voicemail pro — System Preferences > User Group .
WebLM Sets	WebLM Configuration	Note that this data set does not include the license file being used by the server. A separate manual copy of any license file uploaded to the system should be retained.
WebRTC Sets	WebRTC Configuration	
Media Manager Sets	Media Manager Configuration	This is the configuration of the Media Manager service only. It does not include the call recordings and other data stored on the additional hard drive used for Media Manager.

Related links

[Backup and Restore](#) on page 123

Creating a remote server connection

Once the backup server has been configured, a remote server connection is required on the server to be backed up. In a network of servers, the remote connections are defined on the primary server.

Procedure

1. In the Web Manager menu bar, click **Solution**.
2. Click **Solution Settings** and select **Remote Server**.
3. Click **Add Remote Server**.
4. Enter a name that identifies the connections use.
5. Set the **Protocol** to **HTTPS**, **HTTP** or **SFTP** as required.
 - These are the only protocols supported for backup/restore operations.
 - **HTTP** is only supported if the backup server has had HTTP enabled. See [Enabling HTTP backup support](#) on page 125.
6. Set the **Port** to match the selected protocol. The default ports are not necessarily correct.
 - For **HTTPS**, set the port to 5443.
 - For **HTTP**, set the port to 8000.
 - For **SFTP**, set the port to 22.
7. Set the **Remote Path** to `/avaya/backup`.
8. For **HTTP/HTTPS**, no **User Name** or **Password** details are required. For **SFTP**, use the details of a Web Manager administrator account.
9. Click **Save**.
10. The new remote server connection is now shown in the list of remote servers. It can now be selected for backup and restore actions.

Related links

[Backup and Restore](#) on page 123

Backing up a server/servers

The system backs up the configuration of the server, application and user data in a single file set. You can use this backup file to restore the server or a failed server upgrade. The system backs up the configuration of the application to a local drive, in a predefined directory. You can take a backup of the primary server on a remote file server, which can optionally be the secondary server.

Before you begin

- Create a remote server connection for the backup server. See [Creating a remote server connection](#) on page 129.

About this task

You can take a back up of the primary server on a remote file server using Web Manager:

Procedure

1. In the Web Manager menu bar, click **Solution**.
2. In the Solution page, select the servers that you want to backup.
3. Click **Actions** and select **Backup**.
4. Select which data sets you want to include in the backup. See [Backup data sets](#) on page 127 for details of the different sets contents.
5. In the **Backup Label** field, type a label for the backup.
6. In **Select Remote Server** drop down list, select the remote server that you have set.
7. To back up at a scheduled time:
 - a. In **Select Remote Server** drop down list, select the remote server that you have set.
 - b. Under **Schedule Options**, enable **Use Schedule**.
 - c. In the **Select Schedule** list, select the schedule option that you created.
 - d. Set a **Start Date** and a **Start Time**.
 - e. To configure a recurring backup, set **Recurring Schedule** to **Yes** and then set the **Frequency** and **Day of Week**.
8. Click **OK**.
9. The progress of the backup process is shown on the **Solution** menu.

Related links

[Backup and Restore](#) on page 123

Restoring from the backup server

The following process is used to restore previously backed up data.

Warning:

- Backup/restore is not supported between different server software release levels. Any exceptions are specifically documented in software release notes and migration documents.
- You cannot restore data to a server unless either the IP Address or the system id (LAN1 MAC address) match the server from which it was backed up.

- Close any Voicemail Pro client before attempting a restore. The restore process requires the voicemail service to restart. That will not occur if the Voicemail Pro client is connected to the service and will lead to incorrect restoration of data.
- During the restore process, the services being restored are restarted. This will end any calls using those services.

Procedure

1. In the Web Manager menu bar, click **Solution**.
2. Select the servers onto which you want to restore data sets.
3. Click **Actions** and select **Restore**.
4. Select the **Remote Server** connection that points to the backup server.
5. Click **Get Restore Points**.
6. The system displays the backup data sets that it has for the selected servers.
7. Highlight the data sets that you want to restore.
8. Click **OK**.
9. The progress of the backup process is shown on the **Solution** menu.

Related links

[Backup and Restore](#) on page 123

Restoring a failed server

The backup data can be used to attempt to restore a server that has failed.

Procedure

1. Reinstall the original server software, ensuring that the same original IP address and host name settings are used.
2. Reignite the server back to its original role. If the server includes an additional hard drive containing call recordings for Media Manager, ensure that the option to reformat the additional drive is not selected during the server ignition.
3. Login to the server and complete its initial configuration.
4. If the server was part of a network, use the options within Manager to add it back into the network and ensure that the connections between the primary, secondary and expansions are all present.
5. At this stage, use the restore process (see [Restoring from the backup server](#) on page 130) to reload the original data.

Backup and Restore

Related links

[Backup and Restore](#) on page 123

Part 9: Upgrading Servers

Chapter 18: Server Upgrades

This section of the documentation covers the general processes for upgrade Linux-based IP Office servers.

Warning:

- Upgrading to R11.1 from any pre-R11.1 release is not supported using the methods covered in this document. Refer to the *R11.1 Release Notes* and [Upgrading Linux-based IP Office Systems to R12.0](#) documents.

Note:

Before performing any server upgrades:

- You must obtain and check all relevant release notes and documentation prior to any upgrade.
- Ensure that you have backed up the server before performing the upgrade. See [Backup and Restore](#) on page 123.
- Some upgrades require a new set of licenses, typically when upgrading to another major release rather than to a service pack or feature pack within the current release. Obtain and install the new license file before upgrading. A license file for a higher release will still allow the existing release to continue operating.
- If the server is part of a network of IP Office servers:
 - The primary server must be upgraded first.
 - Once the primary server has been upgraded, any other servers can be upgraded individually or simultaneously.
- Upgrading will cause service disruption and end calls in progress. If possible it should be performed outside normal business hours. Using ISO transfer and upgrade through web manager is recommended as that method allows for scheduled upgrading if required.

Related links

[Upgrade methods](#) on page 134

[Upgrade policy](#) on page 135

[Server Edition downgrade policy](#) on page 137

Upgrade methods

You can upgrade Linux-based IP Office servers using a number of methods. These are:

Upgrade Method	Description
Subscription Mode System Upgrade	For subscription mode IP Office systems, upgrades can be scheduled and performed remotely using Customer Operations Manager.
Transferring an ISO file	The new release ISO file can be transferred directly to the server. See Upgrading systems using an ISO file transfer on page 139. <ul style="list-style-type: none"> • The ISO transfer can be performed using a number of methods. • Once the ISO file has been transferred, web manager is used to perform the upgrade. This method allows for the option of setting a scheduled upgrade.
Upgrading from a bootable USB	Upgrade using a USB memory key. See Upgrading using a USB key on page 147. This can be an attended or automatic upgrade. <ul style="list-style-type: none"> • An automatic upgrade proceeds without requiring any menu inputs. • An attended upgrade requires you to respond to menu prompts as the upgrade proceeds.
Upgrading from a bootable DVD	Having created a bootable DVD from the ISO file of the new release, reboot from the DVD. The installer will detect the existing software and prompt whether to upgrade. See Upgrading the system using a bootable DVD on page 145.

Related links

[Server Upgrades](#) on page 134

Upgrade policy

Minor and *Major* upgrades are supported.

Minor Upgrades

- A *Minor* upgrade is an upgrade from one release to a Service Packs (SP) in the same series.
- A *Minor* upgrade does not require pre or post upgrade activities such as database exporting/import, configuration resets. However, you must still take a full server backup as a precaution before the upgrade.

Major Upgrades

- A *Major* upgrade is an upgrade to:
 - A Feature Pack (FP) in the same series. For example, from R11.1 to R11.1 FP3.
 - From one series to the next series. For example, from R10.0 to R11.0.
- A *Major* upgrade may require additional activities before or after the upgrade. For example a database export/import, configuration resets, and so on.

Upgrades with Patches Present

Major or Minor upgrades to systems that are patched are supported. However, depending upon the patched component, the process may differ from the standard case.

- Before any activity, you must check with the group that issued the patch and review any patch notes.
- You must revert any patches before upgrading. You must do this if the Server Edition Primary server is patched, otherwise the solution upgrade will fail.
- The normal upgrade process can then be followed, including taking a backup.
- After the upgrade, if you need to reapply the original or updated patch, apply the patch as per the patch instructions.
- Perform a backup after applying the patches.

Upgrade Licenses

- Upgrading to a new release series requires a software upgrade license. For example, upgrading from R10.0 to R11.0. You can add the upgrade license before upgrading.
- Upgrading within a release series, including to a Feature Pack in the series does not require a software upgrade license. For example, from R11.1 to R11.1 FP2.
- R10.0 onwards uses PLDS licenses only. ADI licenses are no longer supported in R10.
- Pre-R11 IP Office releases supported Avaya WebLM R7 which used a 12–digit Host ID. IP Office Release 11 supports Avaya WebLM R7.1 which uses a 14–digit Host ID.
 - On upgraded systems, the old Host ID has an 03 suffix added. Customers upgrading IP Office from previous releases, must apply for the upgrade license based on the 12–digit Host Id prior to upgrading.
- When you upgrade IP Office Server Edition from R10 to R11, the WebLM password is automatically reset to default password, that is, `weblmadmin`.

Upgrade Configuration Data

IP Office component configuration data is upgraded automatically when the new version is initially executed for both major and minor upgrades. Typically new attributes are set to a default value although this is overridden in some instances. Consult the release notes of the prospective version.

Upgrading IP500 V2 Expansion Systems to Release 9.1

Existing IP500 V2 expansion systems running a release lower than R8.1.1.0 must first upgrade to R8.1.1.0 (or higher) or and R9.0 (any) before being upgraded to R9.1. The upgrade licenses for R9.1 are also valid for the lower releases.

Viewing Application Servers in Web Manager After Upgrade to Release 10

After upgrading to release R10, Application Servers are not visible on the Web Manager **Solution** page. They must be manually added.

1. On the Web Manager **Solution** page, click **Solution Settings > Application Server > Add**.
2. In the Add Application Server window, enter the **Application Server IP Address**.

Related links

[Server Upgrades](#) on page 134

Server Edition downgrade policy

Both *Minor* and *Major* Server Edition downgrades are supported, however for a major downgrade you need to install Server Edition again:

1. Review the release notes of the current version before you downgrade.
2. Take a backup of the solution backup from Web Manager of Server Edition Primary before you downgrade. The backup should include all systems, components and configuration data sets.
3. Perform downgrade when there is no traffic on the system because it affects the service of the system.
4. *Minor* downgrade is a downgrade from one previously installed minor release to another in the same series. For example: 8.1 SP to 8.1 SP or 8.1 SP to 8.1 GA
5. *Minor* Linux server downgrade can be performed using the Web Manager package manager by qualified personnel only for the following IP Office components: IP Office, Jade Media Server, Avaya one-X[®] Portal for IP Office, Voicemail Pro Server or client, Web Control and Web Manager. You cannot downgrade any other component.
6. You can perform a *Minor* Linux server downgrade by performing a complete reinstallation and re-ignition.
7. You can perform a *Major* Linux server downgrade, for example, a downgrade from 9.0 to 8.1 or from 9.1 to 9.0 GA only by reinstallation and re-ignition. Do not attempt to downgrade a component through the Web Manager. In addition, all servers require downgrade because IP Office Server Edition Solution does not support mixed versioning.
8. You can downgrade Server Edition Expansion System through the IP Office Manager memory card Restore command.

After you downgrade, to restore the corresponding backup, use Web Manager.

 **Note:**

For Release 8.1 when you restore the system through Web Control, the system does not restore IP Office Security settings for any device other than Server Edition Primary . To restore the IP Office configurations, use the configuration synchronization feature of IP Office Manager .

9. Ensure that all components of a Server Edition deployment have the same software version.
10. Subsequent upgrade of a *Minor* or *Major* downgrade are supported

 **Note:**

Avaya reserves the right to change Server Edition downgrade policy at some time in the future.

Downgrade configuration data

When you downgrade, the system does not downgrade the configuration data of the component automatically when the new version is initially executed. You need to restore the correct configuration version or administer new configuration data.

To achieve IP Office configuration reuse where no corresponding backup data is available, use the CSV export/import feature of IP Office Manager:

- Read the latest configuration into IP Office Manager offline. IP Office Manager supports all configuration versions up to its own version.
- Export configuration using File | Import/Export | Export, CSV, All of the configuration
- Default the configuration on the target system and read into IP Office Manager.
- Import each configuration using the File | Import/Export | Import, CSV, All of the configuration.
- Check/correct errors and warnings.
- Check configuration settings are as expected.
- Send to system and check operation
- For a IP Office Server Edition Solution , the process should start with the Primary, then secondary then expansion systems. Each should be done individually using Manager in 'standard' not IP Office Server Edition Solution mode.

Related links

[Server Upgrades](#) on page 134

Chapter 19: Upgrading systems using an ISO file transfer

This method of upgrading consists of two stages:

1. Transfer the ISO file to the server.
2. Upgraded the server using the transferred file.

Related links

[Transferring the ISO File](#) on page 139

[Upgrading using a transferred ISO file](#) on page 143

Transferring the ISO File

Use one of the following methods to transfer the ISO file to the primary server or application server.

Related links

[Upgrading systems using an ISO file transfer](#) on page 139

[Transferring an ISO file from a remote file server](#) on page 139

[Transferring an ISO file using a browser](#) on page 140

[Transferring an ISO file via SSH](#) on page 141

[Transferring an ISO file from a DVD](#) on page 142

[Transferring an ISO file from a USB Key](#) on page 142

Transferring an ISO file from a remote file server

You can transfer an ISO file from a file server that supports HTTP, HTTPS, FTP, SFTP or SCP.

Before you begin

- Download the ISO file for the release from the Avaya support site (<https://support.avaya.com>).
- Also download any related documentation from the same page as the ISO file.

Procedure

1. Login to web manager on the server.

2. Create a connection for a link to the file server:
 - a. Click on **Solution Settings** and select **Remoter Server Options**.
 - b. Click **Add Remote Server**.
 - c. Enter the details for the file server on which you have stored the ISO file.
 - d. Click **Save**.
 - e. Click **Close**.
3. Click **Actions** and select **Transfer ISO**.
4. Click **Transfer from** and select **Remote Location**.
 - a. Click **Select Remote Server** and select the previously configured remote file server connection from the list.
 - b. In **File path**, enter the name of the ISO file.
 - c. Click **OK**.
5. The menu displays the progress of the file transfer.

Result

When the transfer has completed, the **Solution** menu displays **Upgrade Available**. You can now upgrade the servers, see [Upgrading using a transferred ISO file](#) on page 143.

Related links

[Transferring the ISO File](#) on page 139

Transferring an ISO file using a browser

You can transfer an ISO file through a web browser connection to the server. However, whilst this works for a sever on the same network as the browser, in other scenarios it is slow. In addition, the transfer is cancelled if the browser window is closed during the transfer.

Before you begin

- Download the ISO file for the release from the Avaya support site (<https://support.avaya.com>).
- Also download any related documentation from the same page as the ISO file.

Procedure

1. Login to web manager on the server.
2. Click **Actions** and select **Transfer ISO**.
3. Click **Transfer from** and select **Client Machine**.
 - a. From the **Select ISO** field, click **Browse**.
 - b. Locate the ISO file and click **Open**.
 - c. Click **OK**.
4. The menu displays the progress of the file transfer.

Result

When the transfer has completed, the **Solution** menu displays **Upgrade Available**. You can now upgrade the servers, see [Upgrading using a transferred ISO file](#) on page 143.

Related links

[Transferring the ISO File](#) on page 139

Transferring an ISO file via SSH

You can use SFTP/SSH to upload an ISO file directly to a folder on the server. This upload process is typically slow, taking several hours, but reliable.

Before you begin

- Download the ISO file for the release from the Avaya support site (<https://support.avaya.com>).
- Also download any related documentation from the same page as the ISO file.

Procedure

1. Using an SSH file transfer application, connect to the server. The exact method depends on the application that you are using:
 - a. For the host name, use the IP address or FQDN of the server.
 - b. For the user name and password details use the Administrator account.
 - c. The protocol is SFTP or SSH.
 - d. The port is 22.
 - e. If this is the first time the application has connected to the server, accept the trusted key.
 - f. The default folder displayed after logging in is /home/Administrator. Upload the ISO file to that folder.
2. Login to web manager on the server.
3. Click **Actions** and select **Transfer ISO**.
4. Click **Transfer** from and select **Server Path**.
5. In the **File path**, enter the path to the uploaded ISO file. For example /home/Administrator/abe-11.1.0.227_el6.iso.
6. The menu displays the progress of the file transfer.

Result

When the transfer has completed, the **Solution** menu displays **Upgrade Available**. You can now upgrade the servers, see [Upgrading using a transferred ISO file](#) on page 143.

Related links

[Transferring the ISO File](#) on page 139

Transferring an ISO file from a DVD

If the sever has a DVD drive, you can transfer an ISO file from the DVD.

Before you begin

- Download the ISO file for the release from the Avaya support site (<https://support.avaya.com>).
- Also download any related documentation from the same page as the ISO file.
- Create a DVD with the ISO file on the DVD. Note, this is the ISO file simply copied onto the DVD as a single file, not a ISO burnt onto the DVD in order to create a bootable disc.

Procedure

1. Login to web manager on the server.
2. Click **Actions** and select **Transfer ISO**.
3. Click **Transfer from** and select **DVD Primary Server**.
4. From the **Select ISO** field, click **Browse**. Locate the ISO file and click **Open**.
5. The menu displays the progress of the file transfer.

Result

When the transfer has completed, the **Solution** menu displays **Upgrade Available**. You can now upgrade the servers, see [Upgrading using a transferred ISO file](#) on page 143.

Related links

[Transferring the ISO File](#) on page 139

Transferring an ISO file from a USB Key

You can copy an ISO file from a USB memory key inserted into one of the server's USB ports.

Before you begin

- Download the ISO file for the release from the Avaya support site (<https://support.avaya.com>).
- Also download any related documentation from the same page as the ISO file.
- Copy the ISO file onto the USB memory key. Do not use the Avaya USB Creator to unpack the ISO file onto the USB.

Procedure

1. Login to web manager on the server.
2. Click **Actions** and select **Transfer ISO**.
3. Click **Transfer from** and select **USB Primary Server**.
4. From the **Select ISO** field, click **Browse**. Locate the ISO file and click **Open**.
5. The menu displays the progress of the file transfer.


Result

When the transfer has completed, the **Solution** menu displays **Upgrade Available**. You can now upgrade the servers, see [Upgrading using a transferred ISO file](#) on page 143.

Related links

[Transferring the ISO File](#) on page 139

Upgrading using a transferred ISO file

After you transfer an ISO file to the primary server, the Solution menu displays  **Update Available** next to each server in the solution.

Before you begin

- You must obtain and check all relevant release notes and documentation prior to any upgrade.
- Ensure that you have backed up the server before performing the upgrade. See [Backup and Restore](#) on page 123.
- Some upgrades require a new set of licenses, typically when upgrading to another major release rather than to a service pack or feature pack within the current release. Obtain and install the new license file before upgrading. A license file for a higher release will still allow the existing release to continue operating.
- If the server is part of a network of IP Office servers:
 - The primary server must be upgraded first.
 - Once the primary server has been upgraded, any other servers can be upgraded individually or simultaneously.
- Upgrading will cause service disruption and end calls in progress. If possible it should be performed outside normal business hours. Using ISO transfer and upgrade through web manager is recommended as that method allows for scheduled upgrading if required.
- Transfer the ISO file to the server. See [Transferring the ISO File](#) on page 139.

About this task

- If this is a network of servers:
 1. Upgrade the primary server on its own first.
 2. Once the primary server has been upgraded, the remaining servers in the network can be upgraded simultaneously if required.
- You can select to schedule the upgrades if required.

Procedure

1. Login to web manager on the server.
2. Log in to Web Manager.

3. In the server list on the Solution page, select the server.
 - If this is a multi-server network. Select the primary server on its own.
4. Click **Actions** and then select **Upgrade**.
5. If required, select **Use Schedule** and defining a scheduled time.
6. Select the **Restart IP Phones** check box if you want all the connected IP Phones to restart after the upgrade is complete.
7. You receive a prompt regarding upgrade licenses. Click **Yes**.
8. You receive a prompt for the License Agreement. Click **Accept** and then **Next**.
9. Click **Close** to close the Upgrade window.
10. You receive a prompt to confirm the upgrade. Click **OK**.
11. The upgrade process begins and progress is shown. However during the process you may be logged off and need to log in again. Allow approximately 30 minutes before logging in again.
12. Once the upgrade has completed, check the operation of the service provided by that server.
13. If this is a multi-server network, you can now upgrade the other servers in the network.

Related links

[Upgrading systems using an ISO file transfer](#) on page 139

Chapter 20: Upgrading the system using a bootable DVD

If the server has a DVD drive, it can be upgraded from a bootable DVD.

Before you begin

- You must obtain and check all relevant release notes and documentation prior to any upgrade.
- Ensure that you have backed up the server before performing the upgrade. See [Backup and Restore](#) on page 123.
- Some upgrades require a new set of licenses, typically when upgrading to another major release rather than to a service pack or feature pack within the current release. Obtain and install the new license file before upgrading. A license file for a higher release will still allow the existing release to continue operating.
- If the server is part of a network of IP Office servers:
 - The primary server must be upgraded first.
 - Once the primary server has been upgraded, any other servers can be upgraded individually or simultaneously.
- Upgrading will cause service disruption and end calls in progress. If possible it should be performed outside normal business hours. Using ISO transfer and upgrade through web manager is recommended as that method allows for scheduled upgrading if required.
- Download the ISO file for the release from the Avaya support site (<https://support.avaya.com>).
- Also download any related documentation from the same page as the ISO file.
- Create a bootable DVD from the ISO file.

Procedure

1. Insert the bootable DVD into the server's DVD drive.
2. Restart the server using web manager.
3. Start or restart the server.
4. If the system does not boot from the install media, verify the boot order in the server's BIOS settings.
5. Click **Change Language** to select the language for use during the installation or upgrade process.
6. Click **Next**.

7. Select the type of keyboard you would like to use for the system.
8. Click **Next**.
9. Select the language in which you would like to read the End User License Agreement (EULA).
10. Click **OK**.
11. Click **Yes, I have read, understood and accepted the terms of Avaya EULA**.
12. Click **Next**.
13. You receive a prompt regarding licenses. Click **Next**.
14. Click **Next** to start the upgrade. The upgrade process can take up to one hour to complete.
15. You receive a prompt that the system has been successfully upgraded. Click **Next**.
16. You receive a prompt to install additional TTS languages. Click **Next**.
17. Remove the DVD and click **Reboot**. The upgrade continues and the server is rebooted. The server can take up to 20 minutes to completely restart.
18. Log in to Web Manager.
19. You receive a prompt regarding background synchronization. Click **Yes**.

Chapter 21: Upgrading using a USB key

You can upgrade a server using a bootable USB key. This can be an automatic upgrade or one where you need to respond to menu prompts.

Before you begin

- You must obtain and check all relevant release notes and documentation prior to any upgrade.
- Ensure that you have backed up the server before performing the upgrade. See [Backup and Restore](#) on page 123.
- Some upgrades require a new set of licenses, typically when upgrading to another major release rather than to a service pack or feature pack within the current release. Obtain and install the new license file before upgrading. A license file for a higher release will still allow the existing release to continue operating.
- If the server is part of a network of IP Office servers:
 - The primary server must be upgraded first.
 - Once the primary server has been upgraded, any other servers can be upgraded individually or simultaneously.
- Upgrading will cause service disruption and end calls in progress. If possible it should be performed outside normal business hours. Using ISO transfer and upgrade through web manager is recommended as that method allows for scheduled upgrading if required.
- Download the ISO file for the release from the Avaya support site (<https://support.avaya.com>).
- Also download any related documentation from the same page as the ISO file.
- Download and install the Avaya USB Creator tool for the same release. See [Downloading the Avaya USB Creator Tool](#) on page 29.
- Create a bootable USB key with the mode set to **Server Edition – Auto Upgrade**. See [Creating a USB Drive using the Avaya USB Creator](#) on page 29. If you want to use **Server Edition – Attended Mode**, follow the same process as for upgrading from a bootable DVD. See [Upgrading the system using a bootable DVD](#) on page 145.

Procedure

1. Insert the installation USB drive in the USB port of the server.
2. Start or restart the server.
3. If the system does not boot from the install media, verify the boot order in the server's BIOS settings.
4. The upgrade proceeds automatically. When completed, remove the USB key and allow the server to restart again.

Part 10: Server Maintenance

Chapter 22: Configuration

This sections covers some general configuration processes.

Related links

- [Administration tools](#) on page 149
- [Starting Web Manager](#) on page 149
- [Accessing the Server's Web Control Menus](#) on page 150
- [Starting IP Office Manager](#) on page 150
- [Setting a login warning banner](#) on page 151

Administration tools

After you have provisioned all the required components in an IP Office Server Edition Solution, use IP Office Manager and IP Office Web Manager to configure additional settings. Refer to

- [Administering Avaya IP Office™ Platform with Manager](#)
- [Administering Avaya IP Office™ Platform with Web Manager](#)

Warning:

Only use CLI commands only if you are Avaya support personnel. You must not install any third party applications on IP Office Server Edition components.

Related links

- [Configuration](#) on page 149

Starting Web Manager

IP Office Web Manager is a set of menus that are installed as part of the server software. They can be used to configure and manager most aspects of the server's operation..

Before you begin

You must have the IP address of IP Office Server Edition server.

Procedure


1. On a PC on the same network as the server, start a web browser. Either:
 - Enter `https://<Server Address>`. From the menu that appears, select **IP Office Web Manager**.
 - Alternatively, enter `https://<Server Address>:7070`.
2. In the login form, enter the name and password for a service user account that has been configured in the system's security settings.

Related links

[Configuration](#) on page 149

Accessing the Server's Web Control Menus

The web control menus are a set of menus supported on all Linux-based IP Office servers. They provide access to a number of underlying server settings separate from the services being provided by the server. For example, the server's date and time settings.

The process below can be used to directly access the server's web control menus. The menus can also be accessed via Web Manager by selecting the  > **Platform View** option next to the server.

Before you begin

- You must have the IP address of the server.

Procedure

1. On a PC on the same network as the server, start a web browser.
2. Enter `https://<Server Address>:7071`.
3. In the login form, enter the name and password for a service user account that has been configured in the system's security settings.

Related links

[Configuration](#) on page 149

Starting IP Office Manager

You can start IP Office Manager using Web Manager. When a Server Edition Secondary server is present, you cannot launch Manager using Web Manager from the Server Edition Secondary server, unless the Server Edition Primary server is down.

You can start Manager without using Web Manager if you installed Manager on your computer. To install Manager, use the IP Office Admin DVD or **AppCenter** page of the Server Edition Primary server. For more information, see [Administering Avaya IP Office™ Platform with Manager](#).

*** Note:**

When you start Manager using Web Manager for the Server Edition Secondary server, you can manage only the systems that are online. After the Server Edition Primary server is up, you must synchronize the offline and online configurations.

Before you begin

- Start Web Manager.
- Log in as *Administrator*.
- To start Manager using Web Manager, install the latest Java Runtime Environment (JRE) Oracle version.

Procedure

In the Web Manager menu bar, click **Applications** and then **IP Office Manager**.

The system automatically loads the IP Office configuration file from the primary server. To load an alternate IP Office configuration file, select the appropriate server.

Result

The system checks if Manager is installed. The system also checks for the version of Manager that is installed.

The system prompts you to download and install the latest version of Manager in the following situations:

- If the version of Manager is not the latest.
- If Manager is not installed.

Next steps

Do one of the following:

- Click **OK**, to open the current version of Manager that the system has detected.
- Download and install the latest version of Manager. Then restart your browser.
- Select **Start > Programs > IP Office > Manager** to open Manager directly from the computer.

Related links

[Configuration](#) on page 149

Setting a login warning banner

When a user logs in to IP Office Server Edition you can set a warning banner. A warning banner displays the terms and conditions to use IP Office Server Edition.

Procedure

1. Log in to Web Manager.
2. On the Solution page, for the system where you want to set a login banner, select **Server Menu > Platform View**.
3. Select **Settings > General**.
4. In the **Set Login Banner** section, type the warning message in the text area.
5. Click **Save**.

Result

The system displays the warning banner in the login page when you log in to IP Office Server Edition next time.

Related links

[Configuration](#) on page 149

Chapter 23: General Maintenance

This section covers general server maintenance and configuration actions.

Related links

[Changing the Server Date and Time Settings](#) on page 153

[Checking the Services](#) on page 154

[Rerunning the Initial Configuration Menu](#) on page 156

Changing the Server Date and Time Settings

You can change the date and time settings used by the server through the server's web configuration pages. The System menu shows the server's current date and time.

Procedure

1. Access the server's web control menus. See [Accessing the Server's Web Control Menus](#) on page 150.
2. Select **Settings**.
3. Select **System**.
4. Select the **Date and Time** section.

Setting	Description
Date	For a server not using NTP, this field shows the server's current date and allows that to be changed. If using NTP this field is greyed out. For virtual servers this field is not used. If not using NTP, the virtual server takes its time from the virtual server host platform.
Time	For a server not using NTP, this field shows the server's current UTC time and allows that to be changed. If using NTP this field is greyed out. For virtual servers this field is not used. If not using NTP, the virtual server takes its time from the virtual server host platform.

Table continues...

Setting	Description
Timezone	In some instances the time displayed or used by a function needs to be the local time rather than UTC time. The Timezone field determines the appropriate offset applied to the UTC time above. Note that changing the timezone can cause a "Session expired" message to appear in the browser in which case you need to login again.
Enable Network Time Protocol Client	
When selected, the server obtains the current date and time from the NTP servers using the settings below.	
NTP Servers	Use this field to enter the IP address of an NTP server or servers to use. Enter each address as a separate line. The network administrator or ISP may have an NTP server for this purpose. A list of publicly accessible NTP servers is available at http://support.ntp.org/bin/view/Servers/WebHome . However, it is your responsibility to comply with the usage policy of the chosen server. Choose several unrelated NTP servers in case one of the servers becomes unreachable or its clock unreliable. The server uses the responses it receives from each NTP server to determine reliability.
Synchronize system clock before starting service	Use this option to synchronize the system clock to an NTP time server before starting other services. Do not use this option if the time server cannot be reliably reached. Waiting for synchronization to occur may block use of the system until a timeout has passed.
Use local time source	When not selected, external NTP takes priority over the internal system clock. If selected, the local system clock is used as the time source. Only use this option if system clock is synchronized with another reliable source, for example a radio controlled clock device.

5. Click **Save**.

Related links

[General Maintenance](#) on page 153

Checking the Services

Through a server's web control menus, you can view the services that the server has been configured to run.

Procedure

1. Access the server's web control menus. See [Accessing the Server's Web Control Menus](#) on page 150.
2. Check that the expected services have been started. If not, start the required services using the **Start** buttons on the right. Select **Show optional services** to show all services.

Service	Description
IP Office	This is the telephony service. It supports the configuration of features such as users, groups, lines, system security, and IP routing. <ul style="list-style-type: none"> On IP Office Application servers, this is replaced by the Management Service below.
Management Service	This is a shell version of the IP Office service that only allows basic configuration of services such as remote SSL VPN connections for server support. It does not support telephony features such as users, extensions or trunks.
one-X Portal	This is a web browser based application that users can use to control making and answering calls on their phone. It also provides a range of gadgets for the user to access features such as their directory, call log and voicemail messages. The one-X Portal for IP Office application is configured and managed remotely via web browser.
Collaboration Services	This service is used to support connection between the IP Office service and external services such as LDAP integration.
Voicemail	This is a voicemail server. It provides mailbox services to all users and hunt groups on the IP Office system.
Web License Manager	This service allows the server to act as a WebLM server. IP Office systems using PLDS licenses can then use the address of the server for license validation.
Web Manager	You can configure and manage the server via browser access to the Web Manager menus. The menus also allow the launching of other clients used to configure and monitor the services run by the server.
Optional Services	
The server can include a number of additional services. Click Show optional services to display those services.	
Media Manager	This application can be used for the long term storage and retrieval of call recordings. The recordings are made by voicemail service. Those recordings are then collected by Media Manager and stored by it. This service is used to provide local Media Manager support. It is not required for system's using centralized Media Manager.

- The one-X Portal for IP Office service remains yellow until its configuration is completed.
- Note that The Voicemail service shows green even if it is not connected to the IP Office due to a password mismatch.

Related links

[General Maintenance](#) on page 153

Rerunning the Initial Configuration Menu

If necessary, the initial configuration menu for a server can be rerun. Note however that there are differences from running the initial configuration on a newly installed server:

- The operating mode of the server cannot be changed. For example a subscription mode system cannot be changed to a non-subscription mode system.
- If the server is running the IP Office server, the **Retain Configuration** option should be used to retain that service's existing configuration.

Procedure

1. Connect to the IP Office system using IP Office Web Manager. See [Starting Web Manager](#) on page 149.
2. Click on the ☰ icon adjacent to the server details and select **Initial Configuration**.
3. The initial configuration menu for the server is displayed with the server's existing settings.
4. Change the settings as required.
5. Click **Apply**.

Related links

[General Maintenance](#) on page 153

Chapter 24: Changing Server Password

The following processes can be used to manage and change administrator passwords.

- These processes require knowledge of the existing administration passwords. If no passwords are known, see [Resetting a server's security settings](#) on page 175.

Related links

[Synchronizing the system service users and passwords](#) on page 157

[Changing the Administrator password using Web Manager](#) on page 158

[Changing the root user password](#) on page 158

[Changing the common Administrator passwords using IP Office Manager](#) on page 159

Synchronizing the system service users and passwords

When managing a network of servers, it is possible to synchronize the service user accounts and their passwords on all the servers with those of the primary server.

Before you begin

- To use this process, the administrator account password for each system should already match.

Procedure

1. Connect to the primary server using IP Office Web Manager. See [Starting Web Manager](#) on page 149.
2. Select **Solution**.
3. Select the checkbox next to each server to which the synchronization action should be applied.
4. Select **Actions > Synchronize Server User and System Password**.
5. The system will confirm when the action has been completed.

Related links

[Changing Server Password](#) on page 157

Changing the Administrator password using Web Manager

About this task

You can administer all the systems configured in IP Office Server Edition Solution using Web Manager . The components that you can administer are the Server Edition Primary, Server Edition Secondary, and Server Edition Expansion System (L).

Procedure

1. Connect to the primary server using IP Office Web Manager. See [Starting Web Manager](#) on page 149.
2. Click **Tools**. The system displays the Services window.
3. Click **Preferences** .
4. Type the new password in the **Password** field.
5. Retype the new password in the **Confirm Password** field.
6. Click **Save**.

Result

The system changes the password and displays the status of the password change.

Related links

[Changing Server Password](#) on page 157

Changing the root user password

You can change the Linux *root user* password through the server's web control menus.

Procedure

1. Access the server's web control menus. See [Accessing the Server's Web Control Menus](#) on page 150.
2. Select > **Settings** > **SystemSettings** > **System**.
3. Type the new password in the **New Password** field of the **Change Root Password** section.
4. Retype the password in the **Confirm New Password** field.
5. Click **Save**.

Related links

[Changing Server Password](#) on page 157

Changing the common Administrator passwords using IP Office Manager

In a network of IP Office servers, you can create and maintain a common administrator user name and password for all the systems. This then allows a range of centralized actions, such as synchronizing all security settings.

This process can also be done using Web Manager (see [Synchronizing the system service users and passwords](#) on page 157). Use this procedure only if you are not able to access Web Manager.

Before you begin

- You must have an existing user name and password for each of the systems in IP Office Server Edition Solution to access the security configuration.

Procedure

1. Connect to the server using IP Office Manager. See [Starting IP Office Manager](#) on page 150.
2. Select **Tools > Server Edition Service User Management**.
3. In the **Select IP Office** window, select the systems for which you want to create a common configuration account.
4. Click **OK**.
5. Type the user name and password to access the security configuration of each of the system that you have selected.
6. To use the same user name and password for the selected systems, select **Use above credentials for all remaining, selected IPOs**.
7. The system displays the list of all the systems in the network and whether they already a common service user account.
8. To change the password, click **Change Password**.
9. Click **Update Password**.
10. Enter and confirm the new password.
11. Click **OK**.
12. Click **Close**.

Related links

[Changing Server Password](#) on page 157

Chapter 25: Log Files

By default, each IP Office server (other than IP500 V2 systems) stores up to 4GB of logs files per day. It stores those logs for up to 3 days.

When required, the oldest logs are automatically deleted in order to provide space for new logs.

Whilst you may not be able to interpret the logs, you should know how to obtain logs from a system in order to provide them when raising an issue for support.

Related links

[Viewing the Debug log files](#) on page 160

[Configuring syslog files](#) on page 160

[Viewing the syslog records](#) on page 161

[Configuring the age of the log files](#) on page 162

[Downloading the log files](#) on page 162

Viewing the Debug log files

About this task

You can view the log files of the various applications that the server supports.

Procedure

1. Access the server's web control menus. See [Accessing the Server's Web Control Menus](#) on page 150.
2. Select **Logs > Debug Logs** .
3. To view the logs for a specific application, select the application from the **Application** list .

Related links

[Log Files](#) on page 160

Configuring syslog files

You can configure the server to receive and the forward the syslog records.

*** Note:**

You cannot configure Server Edition Expansion System(L) or the Application Sever to receive and forward the syslog records.

Procedure

1. Access the server's web control menus. See [Accessing the Server's Web Control Menus](#) on page 150.
2. Select **Settings > General**.
3. In the **Syslog** section do the following:
 - a. In **Log files age (days)**, set the number of the days that the server has to retain the log files.
You can set the age of the different types of log files. If you select **Apply general settings to all file types**, the same age is used for all types.
 - b. In **Max log size (MB)**, set the maximum size for each type of log files.
You can set the maximum size for the different types of log files. If you select **Apply general settings to all file types**, the same size is used for all types.
 - c. In **Receiver Settings**, select **Enable**.
 - d. Set the protocol and the port number that the system should use to receive the syslog records.
 - e. Select **Forward Destination 1**.
 - f. Set the protocol that the system should use to send the syslog records. Type the address of the server and the port number in **IP Address: Port** field.
To send the syslog records to a second server, select **Forward Destination 2**.
 - g. In **Select Log Sources**, select the type of server reporting that the system should include in the syslog records.
4. Click **Save**.

Related links

[Log Files](#) on page 160

Viewing the syslog records

The system displays the syslog files or records that are received by the server.

Before you begin

Configure the syslog events that the server should receive by performing the procedure [Configuring syslog files](#) on page 160.

Procedure

1. Access the server's web control menus. See [Accessing the Server's Web Control Menus](#) on page 150.
2. Select **Logs > Syslog Event Viewer** .
3. Use the **Host**, **Event Type**, **View** and **Tag** options to select the log records shown.

Related links

[Log Files](#) on page 160

Configuring the age of the log files

About this task

The system notifies you regarding the status of the application service or the server in the event of any failure or outage. The system displays the notifications along with time stamps and records them in a log file. You can configure the number of days that these log files need to be retained in the system.

Procedure

1. Access the server's web control menus. See [Accessing the Server's Web Control Menus](#) on page 150.
2. Select **Settings > General**.
3. In the **Watchdog** section, type the number of days in the **Log files age (days)** field.

 **Note:**

- The system does not apply the number of days that you set to the log files that have already been archived.

Related links

[Log Files](#) on page 160

Downloading the log files

The system archives the log files of the applications in *.tar.gz* format.

Procedure

1. Access the server's web control menus. See [Accessing the Server's Web Control Menus](#) on page 150.

2. Select **Logs > Download** .

- The system displays the files that you need for debugging in the **Debug Files** section and log files in the **Logs** section.

3. Any existing zipped log files are shown. Click **Create Archive** to also create zipped files from any current logs that have not already been zipped.

4. Click the files that you want to download.

- The process for the download and the location to which the system downloads the files depends on the browser that you use to access Linux Platform settings.

Related links

[Log Files](#) on page 160

Chapter 26: Shutting Down/Restarting Servers

The following processes can be used to shut-down and restart servers.

Related links

[Shutting down an IP500 V2 Expansion](#) on page 164

[Shutting Down a Linux Server Using Web Manager](#) on page 165

[Shutting down a server using Web Control](#) on page 165

[Removing a Secondary server](#) on page 166

[Removing an expansion system](#) on page 166

Shutting down an IP500 V2 Expansion

You can shut down a Server Edition Expansion System (V2) using the IP Office Server Edition Manager.

About this task

Warning:

- Do not remove the power cords or turn off the power input to the system to shut down the system.
- All user calls and services that are in progress stop. After you shut down, you cannot use the system to make or receive any calls until you restart the system.
- To restart a system after you shut down indefinitely, or to restart a system before the timed restart, turn on the power supply to the system again.

Procedure

1. Select **File > Advanced > System Shutdown**.
2. In the **Select IP Office** window, select the system that you want to shutdown.
3. In the **System Shutdown Mode** dialog box:
 - Select **Indefinite**, to shut down the system for an indefinite time. If you shut down the system for an indefinite time, you must turn off the power to the system and then turn on the power supply gain to restart the system

- Select **Timed** and set the time to restart after the system is shut down.

4. Click **OK**.

Related links

[Shutting Down/Restarting Servers](#) on page 164

Shutting Down a Linux Server Using Web Manager

To ensure that the system saves the configuration file always shut down the system using Web Manager.

Procedure

1. Log in to Web Manager
2. On the Solution page, click the Server Menu icon to the right of the server you want to shut down.
3. Select **Platform View** and then **System**.
4. Under **System**, click **Shutdown**.

Related links

[Shutting Down/Restarting Servers](#) on page 164

Shutting down a server using Web Control

About this task

To shut down a server using the server's web control (platform view) menus:

Procedure

1. Access the server's web control menus. See [Accessing the Server's Web Control Menus](#) on page 150.
2. On the **Home** tab, in the **System** section, click **Shutdown**.
3. In the warning dialog that appears, click **Yes** to confirm that you want to shut down the system.
4. The system displays the login page. Do not log in again because the system is in the process of stopping the services.
5. After the server is shut down, turn off the power to the server.

Related links

[Shutting Down/Restarting Servers](#) on page 164

Removing a Secondary server

Before you begin

- Ensure that there are no active calls.
- Ensure that phones and users are not active on Server Edition Secondary server.

Procedure

1. Login using IP Office Manager. See [Starting IP Office Manager](#) on page 150.
2. In the **Solution** view, at the bottom, right-click on the server.
3. Select **Remove**.
4. Click **Yes** to confirm.
5. Save the changes.

Related links

[Shutting Down/Restarting Servers](#) on page 164

Removing an expansion system

Before you begin

Ensure that there are no active calls in the expansion system.

Procedure

1. Login using IP Office Manager. See [Starting IP Office Manager](#) on page 150.
2. In the **Solution** view, at the bottom, right-click on the server.
3. Select **Remove**.
4. Click **Yes** to confirm.
5. Save the changes.

Related links

[Shutting Down/Restarting Servers](#) on page 164

Chapter 27: Changing Server Addresses

Use these procedures to change the major IP address of a Server Edition Server. The major IP address is the address used to manage the Server Edition Primary server, typically LAN1.

 **Warning:**

- For virtualized servers, the server's **Host Name**, **IP Address** and **Use DHCP** settings are used to generate the server's unique **Host PLDS ID** used for licensing. Changing any of those values will change the ID. If that ID has been used to generate local (nodal) PLDS licenses, those licenses become invalid. This does not affect WebLM (centralized) PLDS licenses.

Related links

[Changing the IP Address of the Primary Server](#) on page 167

[Changing the IP Address of a Secondary or Expansion Server](#) on page 168

Changing the IP Address of the Primary Server

About this task

 **Warning:**

- For virtualized servers, the server's **Host Name**, **IP Address** and **Use DHCP** settings are used to generate the server's unique **Host PLDS ID** used for licensing. Changing any of those values will change the ID. If that ID has been used to generate local (nodal) PLDS licenses, those licenses become invalid. This does not affect WebLM (centralized) PLDS licenses.

Procedure

1. Use IP Office Manager to run the Initial Configuration Utility (ICU) on each Server Edition Secondary and Server Edition Expansion System.

When running the ICU, ensure the **Retain Existing Configuration** setting is checked.

- a. Enter the new Server Edition Primary server IP address/Netmask. This may require a different Gateway IP Route.
- b. Save the configuration to the system. This results in the system going offline from the Server Edition Primary server and Manager.
- c. Once the ICU has been run on each system, close Manager.

2. Use IP Office Web Manager to log in to the Server Edition Primary server and change the IP address.
 - a. Select **System Settings > System**
 - b. On the System screen, click **View AutoPrimary** located at the right.
 - c. Change the IP address as required and click **Update**.
3. Restart the Server Edition Primary server.
4. Use Manager to log in to the Server Edition Primary server and check that all the IP Office systems are online.
5. Review and test the configuration.
6. Perform a backup.

Related links

[Changing Server Addresses](#) on page 167

Changing the IP Address of a Secondary or Expansion Server

About this task

Warning:

- For virtualized servers, the server's **Host Name**, **IP Address** and **Use DHCP** settings are used to generate the server's unique **Host PLDS ID** used for licensing. Changing any of those values will change the ID. If that ID has been used to generate local (nodal) PLDS licenses, those licenses become invalid. This does not affect WebLM (centralized) PLDS licenses.

Procedure

1. Use IP Office Manager to run the Initial Configuration Utility (ICU) on the Server Edition Secondary or Server Edition Expansion System.

When running the ICU, ensure the **Retain Existing Configuration** setting is checked.
2. Change the IP address.
3. Save the configuration to the system. This results in the system going offline from the Server Edition Primary server and Manager.
4. Log in to the Server Edition Primary server and remove the Server Edition Secondary or Server Edition Expansion System from the solution.
5. Run the ICU and add the Server Edition Secondary or Server Edition Expansion System to the solution.

If requested, use the consolidate from Primary (Replace option).

6. Launch one-X Portal administration and configure the DSML and CSTA providers with the new IP address. The one-X Portal service may require a restart.
7. Review and test the configuration.
8. Perform a backup.

Related links

[Changing Server Addresses](#) on page 167

Chapter 28: Hardware Replacement

This section covers general details for replacing hardware involved in a server configuration.

Related links

[Replacing IP500 V2 system](#) on page 170

[Replacing System SD Card](#) on page 171

[Replacing an IP 500 V2 Field Replacable Unit](#) on page 171

[Replacing a Linux server](#) on page 172

Replacing IP500 V2 system

At all times follow the relevant safety and static handling procedures. For further information see, *Warnings* section of [Deploying an IP500 V2 IP Office Essential Edition System](#).

Before you begin

Take an SD card backup using either Manager, SSA or system phone. Do not take a backup of the current configuration or the SD card if it is suspicious.

Procedure

1. Shutdown system using Manager, SSA or system phone.
2. Remove the SD card.
3. Replace system hardware and swap all expansion modules, units and cables with similar kind.
4. Insert SD card.
5. Power on of the system with local connectivity only.
6. Check status using the locally attached IP Office Manager and SSA.
7. Reconnect to the network.
8. Check the configuration using IP Office Manager and Web Manager.

A restore is not required since all necessary data is on the SD card. Licenses remain valid.

Related links

[Hardware Replacement](#) on page 170

Replacing System SD Card

At all times follow the relevant safety and static handling procedures. For further information see, *Warnings* section of [Deploying an IP500 V2 IP Office Essential Edition System](#).

Before you begin

The replacement SD card should be of same type for example, A-Law, U-Law and firmware version with no configuration data. Use the *Recreate IP Office SD Card* feature to load the correct firmware.

Procedure

1. Shutdown the SD card using IP Office Manager, SSA or system phone.

You do not need to shutdown the system.

2. Remove SD card.
3. Insert replacement SD card in System SD slot and wait for System SD LED to be constant green.

The systems save internal flash copy of configuration, security settings, DHCP and call log to the SD card.

 **Note:**

Any local licenses will fail in 2-4 hours if not failed already. All Server Edition central licenses remain valid.

4. Using IP Office Manager, administer new local licenses and delete old.
5. Validate status and configuration with IP Office Manager, Web Manager, , and SSA.
6. Take a backup using Web Manager and an SD card backup using IP Office Manager, SSA or system phone.

The SD card backup provides a local copy, and resilience to a multiple reboot scenario.

Related links

[Hardware Replacement](#) on page 170

Replacing an IP 500 V2 Field Replacable Unit

Procedure

When another field replaceable IP500 V2 component has failed or Expansion module, Expansion Unit, or cable, replace the defective component according to section “Replacing Hardware” section of [Deploying an IP500 V2 IP Office Essential Edition System](#).

Related links

[Hardware Replacement](#) on page 170

Replacing a Linux server

At all times follow the relevant safety and static handling procedures. For further information see document IP Office Installation guide of the Avaya Common Server installation guides.

Before you begin

- At all times follow the relevant safety and static handling procedures.
- The hard drives and power supplies on some particular servers are hot swappable. There is no need for chassis replacement. These items should can be replaced while the system is running. For further information see the Avaya Common Server installation guides.
- If viable and appropriate, take server backup using Web Manager. Take a backup of all components, all data sets, and to a remote server. Note any parameters required for the new server's ignition process
- If not down already, shut down the server using Web Manager, then power off.
- Ensure any resilient switch over of phones, hunt groups, voicemail services has taken place.
- Remove and replace chassis with same capacity.

About this task

Use this procedure to replace all Avaya-supplied Linux servers. The procedure may differ for non-Avaya supplied, but you can use the procedure as the basis for replacement:

Procedure

1. Power on the system with local connectivity only
2. Upgrade to the latest version of IP Office Server Edition Solution using Web Manager DVD, or USB.
3. Configure the server using the ignition process, using the same settings as the original ignition.
4. Configure the server using IP Office Manager Initial Configuration Utility (ICU) to provide management connectivity and valid IP address. Use the same settings as the original ICU.
5. Using Web Manager, on the Server Edition Primary server, run node restore with override for new ID .

The system restores all configuration and data saved in the original backup except security settings. If this is an Application Server that is not a part of Server Edition, use Web Manager to restore.

6. Reconstitute the security settings as these will be default.
 - If you are replacing a Server Edition Primary server, set all the non-default security settings using IP Office Manager.
 - If you are replacing a Server Edition Secondary server, a Server Edition Expansion System, or an Application Server, use the **Synchronize Security** feature of Web Manager.
7. Validate status and configuration with Web Manager, Manager, and SSA.

8. Perform a backup using Web Manager.
9. Using IP Office Manager, administer new local licenses and delete old.

Any local licenses will become invalid after 30 days. An offline license swap-out exists.

Related links

[Hardware Replacement](#) on page 170

Chapter 29: Troubleshooting

The following sections cover a number of known issues and their solutions.

Related links

[Warning message](#) on page 174

[“IP Office is under Server Edition Manager Administration”](#) on page 175

[Resetting a server's security settings](#) on page 175

[All systems online in Web Manager but unable save configurations from Manager](#) on page 177

[All systems online in Manager but offline in Web Manager/Web Control](#) on page 177

[Debugging steps](#) on page 177

[IP Office Server Edition certificates](#) on page 181

[Identity certificates](#) on page 181

[After failback, the H323 phones do not automatically register back to the original server](#) on page 182

[Unable to export template](#) on page 182

[Expansion users disconnected from portal when the system registers SIP phones](#) on page 183

Warning message

When you open a web browser and type `https://<IP address of Server Edition server>:<port number>`, the system displays the following warning message:

This Connection is Untrusted

1. Click **I Understand the Risks**.
2. Click **Add Exception**.
3. Click **Confirm Security Exception**.

The system displays IP Office Server Edition login page.

Related links

[Troubleshooting](#) on page 174

“IP Office is under Server Edition Manager Administration”

When you attempt to configure an IP Office Server Edition system that is managed by an IP Office Server Edition Manager using the IP Office Standard Manager, the system displays an error message:

```
Unable to login. IP Office is under Server Edition Manager
Administration
```

1. Go to **File >Advanced > Security Settings**.
2. Select the IP Office Server Edition system, in the Select IP Office window.
3. Click **OK**.
4. Type the name of the *Security Administrator* in the **Service User Name** field.
5. Type the name of the *Security Administrator* in the **Service User Password** field.
6. Select **Services** in the navigation pane.
7. In the Service: Configuration section, set the **Service Access Source** field as *Unrestricted*.
8. Click **OK**.
9. Select **File > Save Security Settings**.

The system unlocks the access for the *Administrator*.

10. Open the configuration and log in as *Administrator*.

Related links

[Troubleshooting](#) on page 174

Resetting a server's security settings

This process can be used if none of the existing passwords are known. This is a two part process:

1. Reset the Linux root password through the command line.
2. Erase the existing IP Office security settings from the command line.
3. Set new IP Office passwords when prompted at first login.

Procedure

1. Attach a monitor and keyboard to the IP Office system.
2. Reboot the system and at the start of the boot process, press any key to display the grub menu.

3. Select the CentOS Linux line and press e.

```
GRUB version 2.06

load_video
set gfxpayload=keep
insmod gzio
linux ($root)/vmlinuz-5.14.0-362.18.1.el9_3.x86_64 root=/dev/mapper/avaya-r\
oot ro audit=1 resume=/dev/mapper/avaya-swap rd.lvm.lv=avaya/root rd.lvm.lv\
=avaya/swap biosdevname=0 net.ifnames=0
initrd ($root)/initramfs-5.14.0-362.18.1.el9_3.x86_64.img
```

4. Scroll down to the line starting linux.
5. Replace the ro argument with rw init=/sysroot/bin/sh

```
GRUB version 2.06

load_video
set gfxpayload=keep
insmod gzio
linux ($root)/vmlinuz-5.14.0-362.18.1.el9_3.x86_64 root=/dev/mapper/avaya-r\
oot rw init=/sysroot/bin/sh audit=1 resume=/dev/mapper/avaya-swap rd.lvm.lv=\
avaya/root rd.lvm.lv=avaya/swap biosdevname=0 net.ifnames=0
initrd ($root)/initramfs-5.14.0-362.18.1.el9_3.x86_64.img
```

6. Press Ctrl-X to restart the boot process with the new setting.
7. Once the boot up has completed, enter the following commands:
 - a. Enter `chroot /sysroot/`.
 - b. Enter `passwd`.
 - c. Enter and confirm a new password for the Linux root user.
 - d. Enter `exit`.
 - e. Enter `reboot`.
8. Log in as root using the new password.
9. Reset the security settings by entering `/usr/bin/dbgclient erasesecurity`. This resets the IP Office *security* and *Administrator* passwords to the same defaults as used for a new install.
10. Login to IP Office Manager or IP Office Web Manager using the default *Administrator* password. When prompted, change the IP Office passwords.

Related links

[Troubleshooting](#) on page 174

All systems online in Web Manager but unable save configurations from Manager

All systems appear online in the Linux Platform settings of the primary server, but appear offline in the IP Office Server Edition Manager.

Solution:

Ensure that there is a bidirectional IP connectivity from IP Office Server Edition Manager personal computer to the devices for the TCP ports 50802–50815.

Related links

[Troubleshooting](#) on page 174

All systems online in Manager but offline in Web Manager/Web Control

All systems appear online in IP Office Server Edition Manager but appear offline on the Linux Platform settings of the primary server.

Solution:

- Ensure that the password of the *Administrator* account on each of the Server Edition Expansion Systems is same as the *Administrator* password of Server Edition Primary server in Linux Platform settings.
- Ensure that the *Administrator* account on each of the Server Edition Expansion Systems is the member of Administrator rights group.
- Ensure that there is a bidirectional connectivity from Server Edition Primary server to Server Edition Expansion System and Server Edition Secondary server for the TCP ports 8443 and 9080.

Related links

[Troubleshooting](#) on page 174

Debugging steps

This section lists the key steps that you need perform to obtain information.

Warning:

You must run the CLI commands only if you are an Avaya support personnel.

About this task

The key steps are:

Procedure

1. Check and report the status of the application.

The status of the application such as: running, stopped, stuck in starting, and stopping.

2. Check the usage of memory.

Check for details such as: the memory that is available on the system and the amount of memory that each application uses.

3. Check for the notifications.

When you restart an application the system displays the notification.

4. View and download the log files.

For more information about viewing and downloading the log files, see *Chapter 10* of this guide.

Related links

[Troubleshooting](#) on page 174

[Logging in as a root user](#) on page 178

[Checking memory usage](#) on page 179

Logging in as a root user

Occasionally it may be necessary to login as the Linux root user.

Before you begin

Download and install an SSH secure shell application.

About this task

To login as a root user using SSH Secure Shell.

- Only use this process when instructed to do so by Avaya.
- Logging in as the root user is only supported when connected directly to the server (or the console on virtual servers).

Procedure

1. Connect to the IP Office Server Edition using an SSH tool.
 - a. Type the IP address of the IP Office Server Edition server in the **Host Name** field.
 - b. Type the **User Name** as `Administrator`.
 - c. Set the **Protocol** as **SFTP/SSH**.
 - d. Set the **Port** as **22**.

When you connect to the IP Office Server Edition using an SSH File transfer tool for the first time the system prompts you to accept the trusted key. Accept the trusted key.

- e. Type the password for the *Administrator*. The default password for the *Administrator* is `Administrator`.

2. In a new terminal window at the command prompt, type `admin`

The system prompts for a password. The default password is `Administrator`

3. At the `Admin >` prompt, type `root`

4. Type the `root` password. The default password is `Administrator`

The system displays the root user prompt. For example, `root@<name of the server>`

```
*****
*           IP Office for Linux           *
*                                           *
*      WARNING: Authorised Access Only    *
*                                           *
*****

Welcome Administrator it is Wed Jun 13 05:05:03 BST 2012
> admin
Please enter password:
Admin> root
Password:
[root@localhost ~]#
```

Related links

[Debugging steps](#) on page 177

Checking memory usage

To debug a case you need to check the memory that the system uses.

* Note:

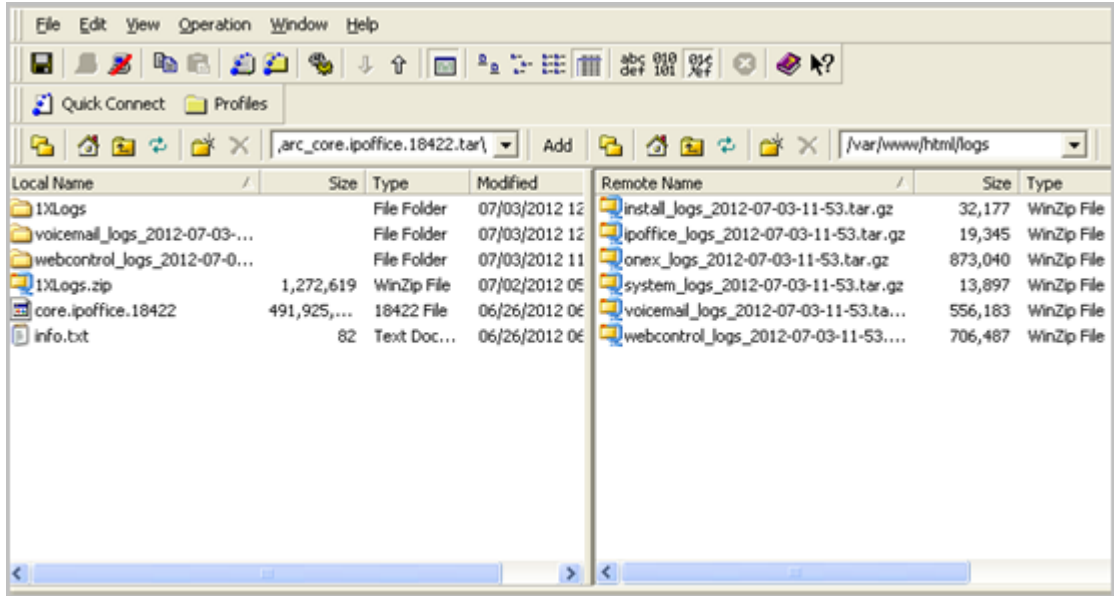
You can also check the memory usage in the **Home** page of the Web Control Panel.

Before you begin

Log in as *Administrator* using SSH Secure File Transfer client

Procedure

1. Type the path of the system logs folder in the Remote View of the File Transfer window.
The path is `/var/www/html/logs`.
The system displays the list of all the logs.



2. Move the *system_logs < time and date stamp> tar.gz* file from the Remote View to a location in the Local View of the File Transfer window.
3. In the local computer extract the *system_logs < time and date stamp> tar.gz* file.
4. Go to the `tmp` folder located in the *system_logs < time and date stamp> tar* that you extracted.
5. Open the *avayasyslog.txt* file.

Result

The system displays the details of memory usage in the table that follows the text `+ free`.

```

/dev/sda2:
+ /sbin/hdparm -I '/dev/hd*'
/dev/hd*: No such file or directory
+ df -h
Filesystem          Size  Used Avail use% Mounted on
/dev/mapper/rootvg-rootvol1
                    38G   11G   26G   30% /
tmpfs                1004M    0 1004M    0% /dev/shm
/dev/sda1            512M   38M  449M    8% /boot
+ free
      total        used        free      shared    buffers
Mem:   2055876    1995232     60644         0       6116
128240
-/+ buffers/cache:  1860876    195000
Swap:  1048568    101172    947396
+ ps -eo rss,cmd --sort=rss
  RSS CMD
   0 [kthreadd]
   0 [migration/0]
   0 [ksoftirqd/0]
   0 [migration/0]

```

Related links

[Debugging steps](#) on page 177

IP Office Server Edition certificates

IP Office Server Edition server uses the following X.509 certificates to identify secure web server and administrative interfaces.

Linux Web Control identity certificate

IP Office Server Edition server uses the Linux Web Control identity certificate for:

- Browser access to Web Control.
- Secure Shell access (SSH v2).

IP Office identity certificate

IP Office Server Edition server uses the IP Office identity certificate for:

- Access IP Office Server Edition Manager.
- Browser access to Web Management for on boarding.

Avaya one-X[®] Portal for IP Office identity certificate

IP Office Server Edition server uses the Avaya one-X[®] Portal for IP Office identity certificate for:

- Browser access to Avaya one-X[®] Portal for IP Office when you choose to use HTTPS.

Related links

[Troubleshooting](#) on page 174

Identity certificates

Certificates are used to provide assurance of identity in a secure environment. Each IP Office component that supports a web server or TLS interface comes with a default identity certificate and a mechanism to change that certificate. For information on certificates, see [Avaya IP Office™ Platform Security Guidelines](#).

Related links

[Troubleshooting](#) on page 174

After failback, the H323 phones do not automatically register back to the original server

IP Office Server Edition Solution provides resilience to some of the functions. When the Primary server is non functional the Secondary server provides resilience and vice versa. The system temporarily logs the users of the H323 phones in to the other server. However, after the original server is functional, the users of the H323 phones remain logged in to the failback server.

Solution

To manually log H323 phone users back into the original server, reset the H323 phones.

If the setting **Phone Failback** is set to **Automatic**, and the phone's primary gatekeeper has been up for more than 10 minutes, the system causes idle phones to perform a failback recovery to the original system. The setting is located at

Manager: System | Telephony | Telephony | Phone Failback

Web Manager: System Settings > System > Telephony > Phone Failback

Related links

[Troubleshooting](#) on page 174

Unable to export template

After you change the common configuration Administrator password for the servers using the IP Office Server Edition Manager, when you export a template from Server Edition Primary server, Server Edition Secondary, or Server Edition Expansion System (L). The system displays an error message: `HTTP request failed:401 Unauthorized`

Related links

[Troubleshooting](#) on page 174

Solution

About this task

After you change the common configuration Administrator password for the servers using the IP Office Server Edition Manager you must also update the same password for *Administrator* account of the Server Edition Primary and Server Edition Secondary servers using Web Manager.

Procedure

Change the password for *Administrator* account using Web Manager.

Expansion users disconnected from portal when the system registers SIP phones

When the users configured on Server Edition Expansion System log into Avaya one-X[®] Portal for IP Office of Server Edition Primary and then start registering the SIP phones on Server Edition Expansion System, the users are disconnected from Avaya one-X[®] Portal for IP Office.

Possible reasons

This issue appears when there are not enough third party IP Endpoint licences when a SIP extension registers on Server Edition Expansion System, the system logs the user off Avaya one-X[®] Portal for IP Office. The system also sends a request to Server Edition Primary to obtain the necessary licences. If the system obtains the license, then the system logs in the users, else the users remain logged out.

Work around

Enable **Reserve 3rd Party IP Endpoint licence** check box on the SIP extensions that you plan to register. This ensures that the system obtains licences from Server Edition Primary and the licenses are present in the configuration when SIP extensions register. Alternatively, ensure that there are enough third party IP endpoints licenses on Server Edition Expansion System.

Related links

[Troubleshooting](#) on page 174

Part 11: Appendix

Chapter 30: IP Office LAN support

You must ensure the IP Office Line network links between servers are either all on **LAN1** or **LAN2**. Failure to adhere to this can reduce efficiency and limit some functionality.

The recommended configuration is to use the Server Edition Linux **LAN1** for all Ethernet traffic with **LAN2** disconnected, and all nodes connected via **LAN1**.

Related links

[IP Office LAN differences](#) on page 185

[IP Office LAN features](#) on page 185

IP Office LAN differences

There are some differences between the functionality of the LAN interfaces of the Server Edition Expansion System (L) and IP500 V2 based Server Edition Expansion System (V2) platforms. Some of the differences are:

- No IPsec, PPP, NAT or NAPT support on Server Edition Linux.
- No IP routing support on Linux.
- Configuration of a Linux Firewall is limited. No traffic is routed between LAN1 and LAN2, except VoIP media (RTP).

The LAN2 interface of the Server Edition Linux platform has fewer capabilities than LAN1.

- A one-X Portal client cannot listen to voicemail messages.
- You cannot launch the Server Edition Manager and other clients from Web Control.
- External MAPI and SMTP voicemail servers cannot be accessed via LAN2.

Related links

[IP Office LAN support](#) on page 185

IP Office LAN features

The following table details the LAN supported features for Server Edition Expansion System (V2) and Server Edition Expansion System (L) platforms.

Feature	IP500 V2 LAN1		Linux LAN1	
	LAN1	LAN2	LAN1	LAN2
Interface Layer1 - Layer4				
Interface Support	✓	✓	✓	✓
Physical<>logical interface mapping	Fixed: 'LAN'	Fixed: 'WAN'	✓	✓
Speed	10/100	10/100	10/100/ 1000	10/100/ 1000
Duplex	Full/half	Full/half	Full/half	Full/half
802.1Q VLAN support Static o/g VLAN assignment via administration. IP500 V2 strips any received VLAN tag, all o/g packets have no VLAN tag	–	–	✓	✓
DSCP/ToS Linux LAN2 uses LAN1 DSCP settings – any LAN2 settings are ignored	✓	✓	✓	✓
Default gateway/route Linux via ignition or Web Control	✓	✓	✓	✓
Proxy ARP IP500 V2 acts as an L3 router	✓	✓	–	–
IP Multicast	✓	✓	–	–
Inter LAN				
Firewall A Linux ingress/egress firewall can be activated, with further controls for specific unsecure ports such as TFTP and HTTP. No differentiation between LAN1 and LAN2.	✓	✓	✓	✓
IP Routes No configurable IP routing between Linux LAN interfaces. All received Linux LAN traffic that is not destined for the node is discarded except VoIP media which is allowed to traverse with NAT.	✓	✓	–	–
NAT/NAPT	✓	✓	–	–
PPP	✓	✓	✓	–
Clients				
one-X Portal client – basic	–	–	✓	✓
one-X Portal client – VM listen	–	–	✓	–
one-X Plugins	–	–	✓	✓
SoftConsole	✓	✓	✓	✓

Table continues...

Feature	IP500 V2 LAN1		Linux LAN1	
	LAN1	LAN2	LAN1	LAN2
Voicemail Pro – MAPI Link Two way MS Exchange VM Integration via MAPI or EWS.	–	–	✓	✓
Voicemail Pro – SMTP One way IMAP/Exchange VM integration.	–	–	✓	–
Administration				
IP Office Manager Also accessible via IPOSS remote tunnel (SSLVPN).	✓	✓	✓	✓
Server Edition Manager Access should be the same LAN1/2 interface as the inter-node connections.	✓	✓	✓	✓
SSA	✓	✓	✓	✓
SysMon	✓	✓	✓	✓
Web Manager Cannot launch other clients (including Manager and Linux Platform Management) when not accessed via LAN1.	✓	✓	✓	✓
Voicemail Pro Client	n/a	n/a	✓	✓
Linux Platform Management	n/a	n/a	✓	✓
Protocols				
DHCP Client and server	✓	✓	✓	✓
BOOTP	✓	✓	✓	–
TFTP	✓	✓	✓	✓
HTTP/S	✓	✓	✓	✓
SCP	–	–	✓	✓
FTP	–	–	✓	✓
SFTP	–	–	✓	✓
PPP	✓	✓	–	–
IPsec	✓	✓	–	–
VPN (L2TP/PPTP)	✓	✓	–	–
RIPv2	✓	✓	–	–
SSLVPN	✓	✓	✓	✓

Table continues...

Feature	IP500 V2 LAN1		Linux LAN1	
	LAN1	LAN2	LAN1	LAN2
NTP Client and server SNTP operation	✓	✓	✓	✓
TIME RFC 868	✓	✓	–	–
TSPI CTI interface for TAPI and one-X Portal	✓	✓	✓	✓
SNMP Traps and MIBs, v1 only	✓	✓	✓	✓
SMDR	✓	✓	✓	✓
DNS	✓	✓	✓	–
Syslog (UDP+TCP+TLS)	✓	✓	✓	✓
Telephony				
H.323 trunks (including SCN) LAN1 and LAN2 should not be mixed for SCN. Should be all LAN1 or all LAN2. This also includes SE Manager access.	✓	✓	✓	✓
H.323 phones Phones must be configured with 'local' registrar IP address – e.g. not possible to access LAN2 registrar via LAN1.	✓	✓	✓	✓
H.323 Remote worker phone	✓	✓	✓	✓
IP DECT	✓	✓	✓	✓
SIP trunks	✓	✓	✓	✓
SIP phones	✓	✓	✓	✓
STUN	✓	✓	✓	✓
IP Office Softphone	✓	✓	✓	✓

Related links

[IP Office LAN support](#) on page 185

Part 12: Further Help

Chapter 31: Additional Help and Documentation

The following pages provide sources for additional help.

Related links

- [Additional Manuals and User Guides](#) on page 190
- [Getting Help](#) on page 190
- [Finding an Avaya Business Partner](#) on page 191
- [Additional IP Office resources](#) on page 191
- [Training](#) on page 192

Additional Manuals and User Guides

The [Avaya Documentation Center](#) website contains user guides and manuals for Avaya products including IP Office.

- For a listing of the current IP Office manuals and user guides, look at the [Avaya IP Office™ Platform Manuals and User Guides](#) document.
- The [Avaya IP Office Knowledgebase](#) and [Avaya Support](#) websites also provide access to the IP Office technical manuals and users guides.
 - Note that where possible these sites redirect users to the version of the document hosted by the [Avaya Documentation Center](#).

For other types of documents and other resources, visit the various Avaya websites (see [Additional IP Office resources](#) on page 191).

Related links

- [Additional Help and Documentation](#) on page 190

Getting Help

Avaya sells IP Office through accredited business partners. Those business partners provide direct support to their customers and can escalate issues to Avaya when necessary.

If your IP Office system currently does not have an Avaya business partner providing support and maintenance for it, you can use the Avaya Partner Locator tool to find a business partner. See [Finding an Avaya Business Partner](#) on page 191.

Related links

[Additional Help and Documentation](#) on page 190

Finding an Avaya Business Partner

If your IP Office system currently does not have an Avaya business partner providing support and maintenance for it, you can use the Avaya Partner Locator tool to find a business partner.

Procedure

1. Using a browser, go to the [Avaya Website](#) at <https://www.avaya.com>
2. Select **Partners** and then **Find a Partner**.
3. Enter your location information.
4. For IP Office business partners, using the **Filter**, select **Small/Medium Business**.

Related links

[Additional Help and Documentation](#) on page 190

Additional IP Office resources

In addition to the documentation website (see [Additional Manuals and User Guides](#) on page 190), there are a range of website that provide information about Avaya products and services including IP Office.

- [Avaya Website](#) (<https://www.avaya.com>)

This is the official Avaya website. The front page also provides access to individual Avaya websites for different regions and countries.

- [Avaya Sales & Partner Portal](#) (<https://sales.avaya.com>)

This is the official website for all Avaya business partners. The site requires registration for a user name and password. Once accessed, you can customize the portal to show specific products and information type that you want to see.

- [Avaya IP Office Knowledgebase](#) (<https://ipofficekb.avaya.com>)

This site provides access to an online, regularly updated version of IP Office user guides and technical manual.

- [Avaya Support](#) (<https://support.avaya.com>)

This site provide access to Avaya product software, documentation and other services for Avaya product installers and maintainers.

- [Avaya Support Forums](https://support.avaya.com/forums/index.php) (<https://support.avaya.com/forums/index.php>)

This site provides forums for discussing product issues.

- [International Avaya User Group](https://www.iuag.org) (<https://www.iuag.org>)

This is the organization for Avaya customers. It provides discussion groups and forums.

- [Avaya DevConnect](https://www.devconnectprogram.com/) (<https://www.devconnectprogram.com/>)

This site provides details on APIs and SDKs for Avaya products, including IP Office. The site also provides application notes for third-party non-Avaya products that interoperate with IP Office using those APIs and SDKs.

- [Avaya Learning](https://www.avaya-learning.com/) (<https://www.avaya-learning.com/>)

This site provides access to training courses and accreditation programs for Avaya products.

Related links

[Additional Help and Documentation](#) on page 190

Training

Avaya training and credentials ensure our Business Partners have the capabilities and skills to successfully sell, implement, and support Avaya solutions and exceed customer expectations. The following credentials are available:

- Avaya Certified Sales Specialist (APSS)
- Avaya Implementation Professional Specialist (AIPS)
- Avaya Certified Support Specialist (ACSS)

Credential maps are available on the [Avaya Learning](#) website.

Related links

[Additional Help and Documentation](#) on page 190

Index

A

add	
application server	97
Additional documentation	17
Additional hard disks	27
address	
remote portal	97
administrator	
common password	159
Administrator	158 , 190
Amazon Web Services	15
APIs	191
Application Notes	191
Application Server	
Initial Configuration	94
Installation	93
auto attendant	
setup wizard	55
automatic	
default parameters	13
install	34
upgrade	147
AWS	15
Azure	15

B

backup	105 , 123 , 129
Backup	21
backup and restore	
disk space	126
backup and restore policy	124
business partner locator	191

C

call routes	
incoming	59
outgoing	60
certificates	181
changing the IP address	167
Check services	154
Collaboration Service	154
COM	21
configuration field	
subscription	18
configurations	
offline	177
upload	177
Configure	
one-X Portal	110
configuring	40

courses	191
CTI	
Subscription	20
custom folder	108
Customer Operations Manager	21

D

dashboard	40 , 45
Dashboard	46
data sets	127
debug	177
Debug logs	160
deploying	11
disable	
portal	96
disk usage	127
DNS	
Subscription	23
document purpose	10
Documentation	17
downgrade	137
download	
log files	162
Download	
Log files	160

E

error	182
expansion server	77
add using Web Manager	77
expansion system	166
add using Manager	79

F

failed server	
restore	131
forums	191

G

groups	
setup wizard	58

H

H.323	
setup wizard	51
Hard disks	
Additional	27

Help	190	Media Manager	154
hold music		Additional drive	27
setup wizard	55	Subscription	20
Hyper-V	15	memory	179
I		migrate	106
ICU	45, 47	Migrate	
identity certificates	181	Subscription	25
ignite	35	Monitor	
incoming call routes		WebRTC	119
setup wizard	59	O	
Initial Configuration		offline	177
Application Server	94	one-X Portal	112, 154
Initial Configuration Menu		Configure	110
Rerunning	156	WebRTC	115
initial configuration utility	42, 45, 47	outgoing call routes	
install	32	setup wizard	60
Application Server	93	P	
Voicemail Pro	103	Panels	46
installing automatically	34	password	
IP address		common administrator	159
changing	167	reset	175
IP Office		root user	158
shutting down expansion server	164	PhoneService	120
IP Office Select	15	portal	
ISO download	139-142	remote address	97
ISO file transfer	139	stop	96
L		Portal	
LAN support	185	Configure	110
licensing		Ports	
setup wizard	58	Subscription	24
lines		primary server	27
setup wizard	58	purpose of document	10
Linux		Q	
expansion server	77	Quick Reference Guides	190
location	125	R	
lockout	175	Receptionist	
log files	162	Subscription	20
Log files	21, 160	Recordings	
Logging		Additional hard disks	27
WebRTC	119	Remote access	21
logging in	104	remote server connection	129
login	178	remove	166
Login		replace	
Web Control	149, 150	FRU	171
logs		IP500 V2	170
download	162	Linux server	172
M		SD card	171
Management service	154	Reseller	190
Manager	150		
Manuals	17, 190		

reset all passwords	175	Subscription	
resilience		DNS	23
H323	182	Internet Access	23
restore	105, 123, 130	IP Route	23
Restore	21	Migrate to	25
restoring	107	Ports	24
root		Time Source	23
reset password	175	subscription configuration fields	18
root user		Subscriptions	
password	158	Applications	20
S		CTI	20
sales	191	Media Manager	20
SDKs	191	Receptionist	20
secondary server	69, 166	SoftConsole	20
add using Manager	71	Telephony User	19
add using Web Manager	69	Telephony User Plus	19
security		Trial Mode	19
synchronize	157	Unified Communications User	19
Select	15	User Subscriptions	19
server		support	191
ignite	35	synchronize	157
Server Edition Network	15	syslog	160
Services	154	view	161
Set All Nodes	64	system	
setup wizard	45, 57	setup wizard	47
auto attendant	55	System Administrator	190
groups	58	T	
H.323	51	Technical Bulletins	191
hold music	55	Telephony User	19
incoming call routes	59	Telephony User Plus	19
LAN settings	47	Time	
licensing	58	Subscription	23
lines	58	training	191, 192
outgoing call routes	60	Trial Mode	
SIP	51	Subscription	19
system	47	trunks	
users	58	setup wizard	58
voicemail	55	U	
VoIP	51	Unified Communications User	19
shut down	165	untrusted connection	174
shutting down		upgrade	134, 145
expansion server	164	web manager	143
SIP		Upgrade	134
setup wizard	51	ISO file transfer	139
SIP phones	183	upgrade policy	135
SoftConsole		USB drive	29
Subscription	20	creating	29
Standalone portal server	112	downloading software	29
stop		Rufus	30
portal service	96	User Guides	190
subscription		users	
error mode	22	setup wizard	58
expiry	22		
grace period	22		
setup wizard	45, 57		

V

View	
Log files	160
syslog	161
Virtual server	15
VMware	15
voicemail	105
setup wizard	55
Voicemail	154
Voicemail Pro	101
VoIP	
setup wizard	51

W

warning banner	151
Web control	
Services	154
Web Control	
Login	150
Web License Manager	154
Web Manager	
Administrator	158 , 190
Login	149
restarting server	165
WebRTC	
Download Logs	119
Logging Level	119
Monitoring	119
one-X Portal	115
PhoneService	120
Test Application	120
websites	191
widgets	45
Widgets	46
wizard	45