

# Avaya IP Office™ Platform Release 10.0 – Release Notes / Technical Bulletin General Availability

## Contents

Contents.....	1
Introduction .....	3
What's New .....	4
Build Versions .....	5
New Phone Models .....	9
Known issues and workarounds.....	10
Application Server.....	10
Avaya Communicator for Windows.....	10
Avaya IP Office Plug-In for Microsoft® Outlook.....	11
Branch.....	12
Certificates.....	12
Contact Recorder.....	12
DevLink3 .....	13
Licensing .....	13
Manager / Web Manager.....	14
Mobility Clients.....	15
one-X® Portal .....	16
Phones .....	17
Prognosis Server .....	19
RPM Transfers.....	19
SIP .....	20
Voicemail Pro.....	21
Web Collaboration .....	21
WebRTC Gateway .....	22
Technical Notes.....	23
Basis, Norstar and Partner Edition support .....	23
Licensing .....	23

Upgrading IP Office IP500V2 core software .....	23
Upgrading IP Office Administration .....	24
Upgrade Instructions for IP Office Preferred Edition .....	24
Upgrade Instructions for IP Office one-X <sup>®</sup> Portal .....	24
Upgrade Instructions for IP Office Server Edition and Application Server .....	24
Avaya USB Creator Tool .....	29
Upgrade Instructions for IP Office Unified Communications Module (UCM) .....	29
Upgrade Instructions for Avaya Communicator for Windows .....	30
Installation Instructions for Avaya Communicator for Microsoft Lync .....	30
Operating System Support .....	31
Languages Added .....	36
Documentation errata .....	36
Contacting support .....	37
Contact Support Checklist .....	37
Contact Support Tasks .....	37
Appendix A – Licensing .....	38
Appendix B - one-X <sup>®</sup> Portal Resiliency .....	58
Overview .....	58
one-X <sup>®</sup> Portal Resiliency Setup .....	59
Hints and Tips .....	77

## Introduction

This document provides late-breaking information to supplement product software and documentation. For updated documentation, product support notices, and service pack information, go to the Avaya Support site at <http://support.avaya.com>.

Avaya is pleased to announce the General Availability of Avaya IP Office™ Platform Release 10.0. Avaya's offer is referred to as "IP Office R10.0" throughout this document. Some key highlights about how Avaya partners and customers can benefit from IP Office R10.0 include:

### Ease of doing business

As IP Office fully transitions to Product License and Delivery System (PLDS) licensing, partners will benefit from self-service licensing management and the utilization of a common licensing format across the Avaya solution stack.

### Stronger resiliency and security

Resiliency and security are strengthened by the resiliency features added to the one-X® Portal and SIP end points, in addition to emergency services API's, new voice quality monitoring functionality combined with H.323 TLS signaling security, security hardening and LDAP synchronization for Server Edition. These new capabilities are particularly important as IP Office expands its reach into the Midmarket and cloud segments while delivering higher levels of customer service and engagement.

### Increased scalability

Scalability is being increased to provide additional capacity to support solutions of up to 3,000 users and 150 nodes. A few examples include, increasing the number of hunt groups, Soft Consoles, music-on-hold sources, button modules and directory capacities.

### Enhanced Collaboration

IP Office collaboration is made richer with the H175 video endpoint and web collaboration updates. Other new capabilities include the availability of a WebRTC Software Developers Kit, enabling 3<sup>rd</sup> parties to create voice and video applications, tighter integration with the Avaya Communicator for Web, along with an impressive list of one-X® Portal and one-X® Mobile Preferred enhancements.

### Simplified Installation, Administration, and Support

IP Office R10.0 contains features aimed at making installation both faster and simpler while also lowering the effort to support. Partners can look forward to UCM improvements, reduction in configuration changes that require re-boots, and an expanded Web Manager, capable of being the administrative tool of choice for IP Office R10.0.

## What's New

The following table summarizes the features being delivered in IP Office R10.0:

Midmarket and Cloud (Server Edition and Select)	Common to All Platforms (Customer Premise and Cloud, Essential & Preferred Editions, Server Edition, and Select)	Customer Premise
<ul style="list-style-type: none"> <li>• one-X® Portal Application Resiliency*</li> <li>• LDAP Synchronization for Server Edition</li> <li>• WebLM Centralized Licensing</li> <li>• Lower Footprint</li> <li>• T38 Fax protocol support on Server Edition</li> <li>• Capacity Enhancements</li> <li>• 32 Music on Hold Sources</li> </ul> <p><b>* Exclusive to IP Office Select</b></p>	<ul style="list-style-type: none"> <li>• Resiliency for SIP Endpoints</li> <li>• Reduction in configuration changes that require a reboot</li> <li>• Proactive Voice Quality Monitoring</li> <li>• Direct Media</li> <li>• H.323 Signaling Security</li> <li>• Avaya Communicator for Web               <ul style="list-style-type: none"> <li>◦ VM to Gmail and OAuth Authentication</li> </ul> </li> <li>• H175 Video Collaboration Station</li> <li>• IP DECT R4 Edition 5</li> <li>• Web Collaboration Enhancements</li> <li>• UC Clients Enhancements</li> <li>• Open APIs/SDKs               <ul style="list-style-type: none"> <li>◦ WebRTC Connector, Location API</li> </ul> </li> <li>• Enhancement Emergency Location Services (NG911/NG112)</li> <li>• Streamline Installation and Upgrades</li> <li>• SIP Trunk Enhancements</li> <li>• Expanded Web Manager functionality</li> <li>• Avaya Communicator for Microsoft Lync adds support for Skype for Business</li> <li>• On Another Call Notification</li> </ul>	<p>Licensing Simplification</p> <ul style="list-style-type: none"> <li>◦ PLDS licensing</li> <li>◦ Centralized Server Edition / Select licensing</li> <li>◦ Upgrade/migration solution</li> </ul> <p>Contact Center ACCS – 400 Agents</p> <p>Branch Solution</p> <ul style="list-style-type: none"> <li>◦ SMGR Geo Redundancy</li> <li>◦ Expanded client support for centralized users</li> </ul>

**Note:** Features listed are available worldwide, unless otherwise specified. Not all of the features in IP Office R10.0 are supported on all Editions, platforms and phones. For further details, please consult the Offer Definition, Avaya IP Office™ Platform, Release 10.0 document located at <https://sales.avaya.com/en/ip-office-release-10.0-sales-toolkit>

## Build Versions

A new numbering scheme has been adopted to simplify how releases are identified in order to differentiate the numbering scheme that has been used in the past for SP and FP.

The marketing release number has been changed to clearly illustrate the FP number as a separate group. The old version scheme containing 4 digit groups will be changed to 5 groups having the following content:

1. Major version
2. Minor version
3. Feature Pack number
4. Maintenance Release/Service Pack number
5. Special Release number (Patches)

### IP Office 10.0 Build 550 Software Versions

Component	Version
Admin CD	10.0.0.0.0 build 550
Voicemail Pro (Linux)	10.0.0.0.0 build 469
Voicemail Pro (Windows)	10.0.0.0.0 build 469
one-X® Portal	10.0.0.0.0 build 980
Avaya IP Office Plug-In for Microsoft® Outlook	10.0.0.0.0 build 980
Avaya one-X Call Assistant	10.0.0.0.0 build 980
Server Edition DVD	10.0.0.0.0 build 550
Server Edition OVA	10.0.0.0.0 build 550
Unified Communication Module	10.0.0.0.0 build 550
Soft Console	10.0.0.0.0 build 113
Avaya Communicator for Windows	2.1.3.237
Avaya Communicator for iPad	2.0.4
Avaya Communicator for Web	1.0.16.1520
Avaya Aura System Manager for IP Office	7.0.1.1
Contact Recorder	10.0.0.15
IP Office Contact Center (IPOCC)	9.1.7.0
Avaya Contact Center Select (ACCS)	7.0
Radvision XT5000	8.3
Avaya one-X® Mobile Preferred for IP Office - Android	10.0.0.173
Avaya one-X® Mobile Preferred for IP Office - iOS	4.0.4.735
WebLM Server	7.0
Avaya USB Creator Tool	Build 74
Avaya Communicator for Microsoft Lync	6.4.0.2.6
WebRTC Gateway	10.0.0.0.0 build 140

#### IP Office Module Firmware

Module	Version
POTSV2 Module	10.0.0.0.0 build 550
DCPV2 Module	10.0.0.0.0 build 550
ATM Module	10.0.0.0.0 build 550
DS30/16 V2 Module	10.0.0.0.0 build 550
DS30A/16A BST Module	10.0.0.0.0 build 550
DS30B/16B Module	10.0.0.0.0 build 550

#### Phone Firmware Support

Phone Model	Version
4600/5600 H.323 Phone Firmware (Common Boot Code and App)	
4610SW, 4620SW, 4621SW, 5610SW, 5620SW & 5621SW	This is no longer supported with IP Office R10.0.
4625	
4620 (Not 4620SW)	
4601, 4602D, 4602SW, 5601, 5602D & 5602SW	
4601+, 4602+, 5601+ & 5602+	
4600/5600 VPN Phone Firmware (Separate Boot Code and App)	
4610SW, 4620SW, 4621SW, 5610SW, 5620SW & 5621SW Boot Code	This is no longer supported with IP Office R10.0.
4610SW, 4620SW, 4621SW, 5610SW, 5620SW & 5621SW App	
1600 H.323 Phone Firmware (Separate Boot Code and App)	
1603 & 1608 & 1616 Boot Code	1.350B
1603 & 1608 & 1616 App	1.350B
1603-L & 1608-L & 1616-L Boot Code	1.390A
1603-L & 1608-L & 1616-L App	1.390A
1616 Button Module 32 App	1.1.0
1600 Phone Language Files	502
9600 H.323 Phone Firmware (Separate Boot Code and App)	
9620 & 9630 Boot Code	3.2.2
9620 & 9630 App	3.2.2
9620L & 9620C & 9630G & 9640 & 9640G & 9650 Boot Code	3.2.5
9620L & 9620C & 9630G & 9640 & 9640G & 9650 App	3.2.5
9600 Phone Language Files	76
96x1 H.323 Phone Firmware (Separate Kernel and App)	
9608 & 9611 & 9621 & 9641 Kernel	S96x1_UKR_V25r10_V25r10 S96x1_UKR_V27r14_V27r14
9608 & 9611 Application	S9608_11HALBR6_6_2_29_V474

9621 & 9641 Application	S9621_41HALBR6_6_2_29_V474
96x1 Phone Language Files	148
Sonic Firmware	S9608_11_HALKRR6_6_2_29.bin
<b>11x0 &amp; 12x0 SIP Phone Firmware</b>	
1120 / 1140	04.04.23
12x0	04.04.23
<b>B179 Firmware</b>	
B179	2.4.1.5
<b>DECT D100 Firmware</b>	
D100_BS_MS	1.2.5
D100_BS_SL	0.9.6
<b>E129 Firmware</b>	
E129	1.25.2.26
<b>E159 Firmware</b>	
E159	8_25_5.bin
<b>E169 Firmware</b>	
E169	8_25_5.bin
<b>DCP Phone Firmware</b>	
2410 / 2420	R6
5410 / 5420	This is no longer supported with IP Office R10.0.
1403	Application R07 Boot 03
1408 / 1416	Application R46 Boot 25
9500	Application R59 Boot R17 Zarlink R0_09
<b>DCP Phone Languages</b>	
14xx	R10_v11_Pack01
<b>DCP Phone Font Files</b>	
14xx Chinese (GB) 14xx Korean (KSC) 14xx Japanese (JIS)	R02_v01

<b>IP DECT Phone Firmware/Tools</b>	
Avaya 3701	22.04.04
Avaya 3711	91.24.31.04
Avaya 3711 Global	91.24.36
Avaya 3711 USB Driver	0.8
<b>IP DECT ADMM Firmware/Tools</b>	
IP DECT - ADMM Firmware / ADMM Java Configuration	1.1.13
IP DECT - ADMM DECT Monitor	1.4
<b>DECT R4 Phone Firmware/Tools</b>	
Avaya 3720 / Avaya 3725 / Avaya 3740 / Avaya 3745 / Avaya 3749	4.3.24
Avaya 3720 / Avaya 3725 Template	0.5
Avaya 3740 / Avaya 3749 Template	0.2
Avaya 3745 Template	0.1
<b>DECT R4 Firmware/Tools</b>	
DECT R4 - IPBS1 Boot Firmware & IPBS1 Firmware	7.2.24
DECT R4 - IPBS2 Boot Firmware & IPBS2 Firmware	
DECT R4 - IPBL (DECT Gateway) Boot Firmware & IPBL (DECT Gateway) Firmware	
DECT R4 - IPBS1 Downgrade Firmware	7.1.2
DECT R4 - IPBS2 Downgrade Firmware	
DECT R4 - IPBL (DECT Gateway) Downgrade Firmware	
DECT R4 - GRBS (ISDN RFP) Firmware	R7C 3/40
DECT R4 - GRBS-DB1 (ISDN RFP) Firmware	R3F 3/80
DECT R4 - AIWS Firmware	2.73
DECT R4 - AIWS2 Firmware	4.1.1
DECT R4 - WinPDM (Windows Portable Device Manager)	3.12.0
DECT R4 - Rack Charger Firmware	2.0.7
DECT R4 - Advanced Charger Firmware	2.0.7
DECT R4 - Avaya 3720 Translation Tool	29
DECT R4 - Avaya 3725/3740/3749 Translation Tool	40
DECT R4 - Avaya 3720 Downloadable Languages	29
DECT R4 - Avaya 3725/3740/3749 Downloadable Languages	40
DECT R4 - Company Phonebook Tool	9
DECT R4 - Local Phonebook Tool	1
<b>Wi-Fi Phone Firmware/Tools</b>	
3641/3645	117.058



HAT	4.1.4
AVPP	17x.040
<b>T3 IP Phone Firmware/Tools</b>	
T3 IP Phone Firmware	T247
T3 IP Admin Tool	3.08
<b>H175 Video Collaboration Station Phone Firmware</b>	
H175	1.0.2.2.0102

### **New Phone Models**

The following phone models are now supported on IP Office:

- H175 Video Collaboration Station
- IP DECT R4 Edition 5

### **IP Office Contact Center Support**

IP Office R10.0 supports IP Office Contact Center version 9.1.7 and above

## Known issues and workarounds

### Application Server

ID	Minimum Conditions	Visible Symptoms	Workaround
<u>IPOFFICE-110663</u>	<p>1. Application server one-X<sup>®</sup> Portal Resiliency will not work if machine's default domain name is not DNS resolvable.</p> <p>2. For Application server one-X<sup>®</sup> Portal Resiliency, updating Resiliency configuration to use non-default domain name for primary and secondary one-X<sup>®</sup> Portal will not work.</p>	Application server one-X <sup>®</sup> Portal Resiliency	For Application server, Resiliency for one-X <sup>®</sup> Portal can be make workable by making default Application server machine's domain name to be DNS resolvable.
<u>IPOFFICE-110375</u>	The syslog messages are continuously re-sent on loopback interface. This is reproducible only on Application Sever.	The CPU shows high load.	Delete the default syslog entry from Manager (with IP address 127.0.0.1).

### Avaya Communicator for Windows

ID	Minimum Conditions	Visible Symptoms	Workaround
<u>IPOFFICE-105861</u>	Plantronics headset Un-mutes when there is a missed call on Avaya Communicator for Windows.	There is an active call in progress, and Caller A has the headset muted for this call. If Caller A receives another call that is not answered (missed, or abandoned by the user), the headset is unmuted.	Remove 1XC from PC.
<u>IPOFFICE-109846</u>	When the Moderator of a Meet Me conference does a mute-all operation, all the participants including the moderator are muted. Moderator should not be muted.	Moderator will also go on mute when mute all is pressed.	Moderator has to unmute manually to speak.
<u>IPOFFICE-109967</u>	If you are unable to upgrade Avaya Communicator for Windows, check the Task Manager to see if the application is running.	Avaya Communicator for Windows can't upgrade if the application is running. It asks for "Retry" and "Quit".	Quit the running application or kill the process, then start upgrade.

### Avaya IP Office Plug-In for Microsoft® Outlook

ID	Minimum Conditions	Visible Symptoms	Workaround
<u>IPOFFICE-105981</u>	When there is keyboard focus on the Avaya IP Office Plug-In for Microsoft® Outlook (any field) , and the user selects mail from the mail list and then presses the 'Delete' key on the keyboard, the mail doesn't get deleted.	A user is not able to delete highlighted mails from a list when the 'Delete' key is pressed. (Only in above Scenario)	In this scenario, there are a few workarounds as listed below:  1. Use right click menu on selected mail to Delete.  2. Use 'Delete' button option provided on the ribbon on top.  3. Make focus to reading pane content of the mail, and then press the 'Delete' key.  4. Minimize and then Maximize Outlook. Press the 'Delete' key when the mail entry is selected.

## Branch

ID	Minimum Conditions	Visible Symptoms	Workaround
<u>IPOFFICE-106576</u>	When IP Office tries to renegotiate media parameters in existing calls, there is no SIP response message.	No voice path with centralized phones on SM in case of transfer.	Disable SRTP on SM lines.

## Certificates

ID	Minimum Conditions	Visible Symptoms	Workaround
<u>IPOFFICE-110805</u>	The CA is not automatically generated when upgrading from 9.0 to 9.1 (prior to 9.1.9) and to 10.0.	Cannot generate certificates for other machines after upgrade to new versions.	Generate CA certificates by using Generate CA button from Webcontrol interface before generate certificates for other machines.

## Contact Recorder

ID	Minimum Conditions	Visible Symptoms	Workaround
<u>IPOFFICE-108259</u>	Contact Recorder accepts any administrative password on first access.		<p>New changes in Accessing Contact Recorder for the first time</p> <p>If it is the first time that the Contact Recorder has been logged into, enter username as "Administrator" and password as "Administrator". Click OK.</p> <p>Administrator user is predefined user with administrator rights. You are then redirected to Change Password page. Enter Old Password as "Administrator" and enter a password that is at least eight characters long in the New Password field. Enter the password again in the Verify New Password field.</p>

### DevLink3

ID	Minimum Conditions	Visible Symptoms	Workaround
<u>IPOFFICE-111042</u>	The following alarm should be ignored when connecting via a DevLink3 application: "Attempt to use a feature for which no license is installed" License Type:DevLink3 External Recorder"		This license is not required to connect via the DevLink3 interface and receive DevLink3 events via this interface.

### Licensing

ID	Minimum Conditions	Visible Symptoms	Workaround
<u>IPOFFICE-109077</u>	The <i>About</i> box of WebLM manager does not show the WebLM version number.	Unable to get the WebLM version	WebLM number is not required. In case of any issue, the IP Office version number is sufficient to debug an issue.
<u>IPOFFICE-110055</u>	On IP Office Server Edition/Standalone V2, when all licenses required for a particular profile are consumed and any existing user is edited, a warning of number of user exceeds available licenses is displayed.	Customer would see false license warning although existing users have consumed available licenses correctly. Users can still be saved with the warning in any case, so saving is not impacted by this issue.	Ignore this warning if the number of users matches the number of available user profile licenses.  e.g. if there are 5 power user licenses available and 5 power users have been configured, editing any of those would show a warning of license. In this case ignore it.
<u>IPOFFICE-111618</u>	A "System ID has changed" alarm can be raised even if the system is licensed using WebLM.	No impact to the customer. This alarm can be ignored if the system is in WebLM mode.	The alarm can be cleared by performing a configuration change in Manager that requires a Merge operation.
<u>IPOFFICE-111618</u>	The system is showing "WebLM Error Mode", but the licenses are showing as valid.	There is no functional impact to the customer.	This state can be cleared by either triggering a "Renew Licenses" operation from SSA or by performing a configuration change in Manager that requires a merge operation.

## Manager / Web Manager

ID	Minimum Conditions	Visible Symptoms	Workaround
<u>IPOFFICE-107704</u>	Once a system upgrade is successful, Web manager will only show “Upgrade is successful” on the IP Office system panel if the user remains logged-in during upgrade completion.		If user wants to see whether the upgrade is successful later, they can :  1. Upgrade report for that system can be checked by accessing the burger menu in front of system and clicking on “view upgrade report”.  2. Access “Solution” menu, expand the IP Office system panel, and check the version. If the version is the same as the downloaded ISO, it means the upgrade is successful.
<u>IPOFFICE-109498</u>	Systems with more than 50 nodes that are triggering an upgrade of all the systems at single click.	The upgrade progress may not be shown in the solution dashboard. This does not affect the upgrade process. The upgrade is working properly ,ONLY the progress is not shown.	The user needs to login to system to check whether the version of individual nodes has been changed.
<u>IPOFFICE-110251</u>	When creating an Offline configuration when Manager is in Simplified view, only three locales are shown as available.	Customer may get confused if want to select any locale other than US, Mexico or Canada for offline configuration.	The user needs to re-select the Configuration type as any of the available options (e.g. IP Office Standard Mode), the locales are all available now.
<u>IPOFFICE-110527</u>	While Editing all PRI channels with WM the default values are presented instead of existing values for some of the fields.	If Administrator saves without changing the existing values then the value for these fields will be set to Default.	Set the value of default fields to the expected values.
<u>IPOFFICE-110537</u>	Web Manager stuck while Saving Line Subtype from ETSI / QSIG to ETSI CHI.	Administrator will not be able to change the line Subtype for PRI using Web Manager.	Please use IP Office manager for Subtype change.
<u>IPOFFICE-110544</u>	Web Manager cannot change Line Subtype from T1 to PRI with Web Manager.	Administrator will not be able to change the line type from T1 to PRI with Web Manager.	Please use IP Office manager for changing the line type from T1 to PRI.

<u>IPOFFICE-110586</u>	Customer has configured a remote SFTP server to use as a location for IP Office backups. Then tried to backup configuration to remote server through SFTP. Backup failed from Primary Server.	Backup failed from Primary Server. The error received is 'Backup failed: Wait inventory pushed stage failed'.	Problem can be a host key stopping the backup from working.  Check if the Remote Host Identification had changed. (Try sftp from the command line - you will get the warning message of remote host identification has changed). If yes, then remove the old host key from Primary and then try backup.
<u>IPOFFICE-110862</u>	When multiple IP Address are configured to primary server (e.g. private IP Address and Public IP Address) and expansion is pointing to public IP Address as License Server Address, then Web Manager is not able to resolve this IP address as it always check for private IP address.	Because of this, In Web Manager, UI throws Null Pointer Exception and it is not able to create user.	Use Manager in this situation.
<u>IPOFFICE-110867</u>	Huntgroup membership is not reflected in Web Manager. Available Groups are not shown in Web Manager for membership enablement.	User's membership for hunt group cannot be enabled. NOTE: Hunt group membership can still be performed from User first tab. Only membership enablement is not possible,	Use Manager in this situation.

### Mobility Clients

ID	Minimum Conditions	Visible Symptoms	Workaround
<u>IPOFFICE-99979</u>	Mobile client users cannot use extension number to login.	Mobile client users cannot use extension number to login.	Username/password must be used at all times to login.

## one-X® Portal

ID	Minimum Conditions	Visible Symptoms	Workaround
<u>IPOFFICE-107348</u>	Certain users are shown as busy (telephony) in one-X® Portal after several resiliency scenarios.	Minor impact. It happens very rarely after multiple failovers.	Change status of phone (Ex:on/off hook).
<u>IPOFFICE-110225</u>	The IP Office Primary IP address shouldn't be changed when it is provisioned with one-X® Portal on the Application Server.		As a workaround: 1. Change the CSTA and DSML provider records from one-X® Portal admin to point to new IP Office IP address. Save the configuration. 2. Stop one-X® Portal service 3. Change the IP Office IP address. 4. Restart one-X® Portal
<u>IPOFFICE-110662</u>	Loss of connectivity between IPOL and external one-X® Portal server. This only appears if the link between IPOL and oneX goes down for a very short amount of time and then it is immediately restored.		Restart one-X® Portal server.
<u>IPOFFICE-111270</u>	After upgrading Voicemail Pro from 9.1 GA to 10.0 GA old voice messages cannot be played if we chose 'play on phone' option in one-X Portal	Minimal - one specific supported method of listening to Voice mail messages through the one-X® Portal is not working for older messages in the system.	If you are using one-X Web Client to play voicemail messages which were received prior to the upgrade to 10.0, please use the 'Play in Browser' option. Messages can also be retrieved using Visual Voicemail.
<u>IPOFFICE-111271</u>	In some cases, after logging into one-X® Portal for the first time after an upgrade, there is a non-functional or blank page.	Very low, as this is a rare scenario. If it occurs, the user will not be able to use one-X® Portal unless the browser cache is cleared.	Clear the browser cache and login to one-X® Portal.
<u>IPOFFICE-111671</u>	Conference scheduling email invitation is not received by the host if running Lotus Notes.	Conference scheduling host and participants running Lotus Notes may have issues viewing conference scheduling email contents.	Use any other email client to access the scheduling email (Outlook, Thunderbird, etc.)



## Phones

ID	Minimum Conditions	Visible Symptoms	Workaround
<u>IPOFFICE-104837</u>	On 16xx phones, when authentication mode is key exchange, the phone language can't be changed from core (either Manager or Web Manager)	Low, for most of the languages, only A-menu is impacted. For Mediterranean locale all the menus are impacted because the phone doesn't switch to right to left rendering	Reregister the phone or change the language from the A-menu.
<u>IPOFFICE-110229</u>	16xx Phones don't take the address via DHCP when they receive the VLAN information over LLDP from an ERS3524GTS switch	16xx Phones don't take the address via DHCP when they receive the VLAN information over LLDP from an ERS3524GTS switch	Set VLANTEST=0 in the phone settings file.
<u>IPOFFICE-110439</u>	When a direct media call is initiated from/to a 96x1 phone and the default gateway is not configured, the phone reboots.		Ensure that a gateway is defined for phones that have direct media enabled, or disable direct media.
<u>IPOFFICE-110373</u>	B179 and E129 as remote worker will send FQDN in Register message when "SIP DOMAIN" field is configured to be different from "SIP REGISTER FQDN" field in IP Office.  IP Office rejects the phones	B179 and E129 as remote worker will fail to Register when "SIP DOMAIN" is configured to be different from "SIP REGISTER FQDN" in IP Office (This is done to	SIP Server field in E129 and B179 phones can be manually edited using web interface to include IP Office public IP to Register with IP Office as remote worker.

	Register with BAD DOMAIN(403 Forbidden).	support SIP resiliency)	
<u>IPOFFICE-99778</u>	B179 phones change the SRTP master key during reINVITE request for call hold, and this can lead to a broken speech path.	Direct media is disabled when SRTP is enabled so hold, transfer, etc. will work.	None.
<u>IPOFFICE-107716</u>	E129 phone doesn't update the time according to timezone, when IP Office makes changes in timezone in manager. Same Timezone should be configured on E129 phone web GUI.	Time display will not be correct on E129 phone if only IP Office timezone is changed. Same Timezone should be configured on E129 phone web GUI.	Configuring the timezone on the E129 phone web GUI, will display the correct time on the E129 phone displays correct time.
<u>IPOFFICE-107821</u>	<p>IP Office deployment that has a SIP trunk to the Scopia environment, while the H175 endpoint is registered as a SIP endpoint to IP Office.</p> <p>When the H175 endpoint dials into a virtual meeting room hosted on the Elite 5000 MCU, it does not receive any incoming video. The remote side is able to receive the video from the H175 while the audio works both ways.</p>	H175 endpoint dials into a virtual meeting room hosted on the Elite 5000 MCU, it does not receive any incoming video, only audio works	<p>Use Elite 6000 MCU, since issue is only observed with Elite 5000 MCU. Elite 5000 MCU patch V7.7.9.0 resolves this issue. The patch will be rolled into the solution 8.3.6 GA release of Elite 5000 MCU which will also be based on the V7.7.9.x code. The 8.3.6 release is planned to for the Aug-Sep 2016 timeframe.</p> <p>Refer the below knowledge base article:  <a href="https://support.avaya.com/ext/index?page=content&amp;id=SOLN289843">https://support.avaya.com/ext/index?page=content&amp;id=SOLN289843</a></p>

<u>IPOFFICE-111894</u>	In a Partner Hosted solution with more than 255 users created as "Basic Users" with "Enable Remote Worker" selected, only 255 users can log in.	When attempting login, error message in sysmon example - CMExtnEvt: Extn457: User is not licensed for a Remote Extension: Logging Out.	Resolved in Release 10.0 SP1.  Workaround : Configure addition users as Power Users (Enable Remote Worker is selected by default)
------------------------	---	--	---

Open issues with the Avaya 96x1 phones are documented in <http://downloads.avaya.com/css/P8/documents/101023924>.

#### Prognosis Server

ID	Minimum Conditions	Visible Symptoms	Workaround
<u>IPOFFICE-98866</u>	The current release (10.4) of Prognosis (DevConnect quality monitoring application) does not match RTCP packets with the IP Office that sent them.	The Prognosis Server does not display QoS information properly.	Add the following NUSN to the IP Office configuration at Users->NoUser->SourceNumber: RTCP_COLLECTOR_IP=ip_addr where ip_addr is the IP Office's IP address as configured in the Prognosis server.

#### RPM Transfers

ID	Minimum Conditions	Visible Symptoms	Workaround
<u>IPOFFICE-110812</u>	The repository keeps all the packages that were installed starting with the fresh install and during each upgrade the rpms are added.  When one rpm is added the entire repository data is recreated to include this new one and this operation can take some time.	If the system was upgraded many times the rpm transfer can take longer.	Before starting the transfer, go to Updates tab and click on Clear Local Cache to keep only the current rpms in the repository.

## SIP

ID	Minimum Conditions	Visible Symptoms	Workaround
<u>IPOFFICE-106732</u>	Privacy ID header is added to SIP message when Local URI value in SIP URI is set to "Use Internal data" and identity header value is not "Use Internal Data".	It is a corner case scenario where different values are set for Local URI and Identity and also Anonymous check box in User --> SIP tab (for that user) is enabled.	Set Local URI value same as Identity value when Identity value.
<u>IPOFFICE-106995</u>	The new "SIP Registrar FQDN" field in Manager.	The new field was added since IP Office currently does not know its own FQDN. In some places, for the implementation of SIP terminals remote workers, we need to use this new field to support DNS for remote workers. For SIP resiliency, we need the "SIP Domain Name" where we need multiple servers in an SCN cluster with SIP resiliency to have the same SIP domain. WebRTC Configurations use the "SIP Domain name". This need not be configured manually and the value is picked from the one-X <sup>®</sup> Portal settings file.	None.
<u>IPOFFICE-107022</u>	Video Escalation fails for Non-Direct Media audio calls.	Impacts only video supported clients, and happens only for relayed audio calls.	Direct Media audio calls can be escalated to video.

## Voicemail Pro

ID	Minimum Conditions	Visible Symptoms	Workaround
<u>IPOFFICE-111738</u>	<p>If the maximum number of supported voicemail channels are allocated, the system doesn't de-allocate them and no more calls can reach voicemail. The issue is present only on IPOL and the service has to be restarted in order to de-allocate the resources.</p> <p>The maximum supported voicemail channels are:</p> <ul style="list-style-type: none"> <li>- <b>500</b> on HP DL360, Dell R620, Dell R630, Google Cloud or OVA deployments</li> <li>- <b>175</b> on HP DL120, Dell R210, Lenovo M73</li> <li>- <b>2</b> on a Demo system</li> </ul>	Voicemail is unavailable until the IP Office service is restarted	<p>Add the following line in /etc/sysconfig/ipoffice and restart ipoffice service from Webcontrol:</p> <pre>export IPOFFICE_MAX_NUM_VMAIL_CHANNELS=channels_no</pre> <p>where '<i>channels_no</i>' is greater than the number of available Voicemail Ports licenses</p>

## Web Collaboration

ID	Minimum Conditions	Visible Symptoms	Workaround
<u>IPOFFICE-103265</u>	<p>When using the Avaya Web Collaboration Agent on a Lenovo ThinkPad W520 with Windows 7, the user may find that parts of the Agent window remain visible in the background of another window on the same PC.</p> <p>With Windows 10, the user may see a vertical red line in the shared window.</p>		For both conditions, the user can minimize and then restore the affected window to clear this condition.

### WebRTC Gateway

ID	Minimum Conditions	Visible Symptoms	Workaround
<u>IPOFFICE-106189</u>	<p>An IP Office User can use WebRTC Softphone functionality from any one of the following clients at a time. ( There is no Simultaneous User support in 10.0)</p> <ul style="list-style-type: none"><li>• Avaya Communicator for Web Softphone Mode</li><li>• Web Collaboration</li><li>• Customer Engagement onAvaya</li></ul>	<p>Any new client login will unregister the previously registered client. Any active calls will be dropped.</p>	

## Technical Notes

### Basis, Norstar and Partner Edition support

Norstar SD cards and Partner SD cards will no longer be sold. The SD card loaded with the R10 system binary and image will support Basic Edition functionality.

**Note:** Basic Edition R10 will lag the general release of IP Office R10 and will be available with the September service pack. Look for updates prior to GA of R10.

### Licensing

IP Office release 10 and higher only supports the Product Licensing and Delivery System (PLDS) to manage license files. If you are upgrading from a previous release, you must migrate all of your pre-R10 licenses (ADI, PLDS, mix of ADI/PLDS, virtual) to R10 PLDS licenses. For further information, please refer to [Appendix A – Licensing](#) or the “Administering Avaya IP Office™ Platform with Web Manager” manual available from the IP Office Knowledgebase.

The Avaya R&D team have setup a forum to provide support for technical questions related to the new licensing content delivered in IP Office R10.0 and can be found here:

<https://support.avaya.com/forums/forumdisplay.php?f=86>

### Upgrading IP Office IP500V2 core software

For further information, please refer to the “Upgrading Systems” section of the IP500/IP500V2 Installation manual available from the IP Office Knowledgebase.

#### Warning:

- In all cases, always backup all application data to a separate location before upgrading.
- Check the PCS Level of the IP500V2 Control Unit. For PCS 14 and earlier, the boot loader may need to be upgraded to version 1.33 or higher. If the system is running 8.1 (65) or higher, 9.0, or 9.1, the boot loader has already been upgraded and it does not need repeating. The boot loader version can be checked on the systems details output when System Monitor connects:

```
09:16:46      54896mS PRN: ++++++
09:16:46      54896mS PRN: + loader: 1.35
09:16:46      54896mS PRN: + cpu: id 12 board 5 pld 25 type c10 options ae02
09:16:46      54896mS PRN: + cpu: sn 16WZ0440C18T
09:16:46      54896mS PRN: + fpga: id 1 issue 0 build 827
09:16:46      54896mS PRN: ++++++
09:16:46      54896mS PRN: ++++++ LIST OF MODULES ++++++
09:16:46      54896mS PRN: +-----
09:16:46      54896mS PRN: + Slot 1: Base COMBO6210 Board=0x02 PLD=0x04
09:16:46      54896mS PRN: + Mezzanine ATM4 V2 Board=0x01 PLD=0x04
```

The boot loader can be upgraded by installing either Release 8.1 (65) (or higher) or any IP Office Release 9.0, before upgrading to Release 10.0. If this has already been done, it does not need repeating.

### **Upgrading IP Office Administration**

Earlier releases of IP Office Manager are not compatible with systems running this release. Before upgrading an IP Office system to the 10.0.0.0 Build 550 release, the Administration suite must also be upgraded.

The IP Office Administration installer will detect previous installed versions and upgrade automatically. It is not necessary to restart the PC after upgrading unless instructed to do so.

Before upgrading the IP Office system software ensure a backup of the system configuration exists.

**Note:** All IP Office expansion units must also be upgraded to the version supplied with the Administration software.

**Warning:** In all cases, always backup all application data to a separate location before upgrading.

### **Upgrade Instructions for IP Office Preferred Edition**

IP Office Preferred Edition (VoiceMail Pro) 10.0.0.0 Build 550 installer will automatically detect the previous build and upgrade automatically. It is always advisable to back up the configuration, and any bespoke voice files prior to performing the upgrade. In addition, for a successful install or upgrade (from any 9.X to latest R10.0) of the Windows version of Voicemail Pro, please install all Windows updates first in order to obtain the latest WinTrust.dll on your machine. This is needed to verify the SHA256 certificate used by the Voicemail Pro installer. A backup of Voicemail Pro data should be done prior to any Major (first time 10.0) upgrade on Windows platform.

Prior to upgrading the Preferred Edition Server to 10.0.0.0 build 550, please ensure that all applications running on the PC are closed. The upgrade process will retain all the customer configuration, mailbox data and registry settings.

**Warning:** In all cases, always backup all application data to a separate location before upgrading.

### **Upgrade Instructions for IP Office one-X<sup>®</sup> Portal**

For further information, please refer to the “Implementing one<sup>®</sup>X Portal for IP Office” manual available from the IP Office Knowledgebase.

**Warning:** In all cases, always backup all application data to a separate location before upgrading.

### **Upgrade Instructions for IP Office Server Edition and Application Server**

If using a DVD install of this release of IP Office Server Edition and Application Server, you can upgrade directly from the previous GA release (9.0 or 9.1). For further information, please refer to the “IP Office Application Server 10.0 Installation and Maintenance” and the “Upgrading” section of the “Deploying IP Office Server Edition Solution” manual available from the IP Office Knowledgebase.



**Warning:** In all cases, always backup all application data to a separate location before upgrading.

If you are upgrading IP Office Server Edition and Application Server and will be using Web Manager, please read the following guidelines. **Note:** If your system is already running IP Office 9.1 software, this section is NOT applicable. It is ONLY applicable for systems running either IP Office release 8.1 or 9.0 software.

## **Web Manager Upgrade Instructions**

### **Introduction**

The following instructions describe the process for upgrading an IP Office Server Edition system that is running either release 8.1 or 9.0.

1. Transfer the ISO image.
2. Start an Upgrade of the Primary system.
3. During the Upgrade, monitor the progress on Web Manager.
4. After the upgrade, Web Manager will trigger the post-upgrade step.
5. Login to Web Manager.
6. A warning will appear that a post-upgrade step is needed.
7. Check if a link Complete for post-upgrade step appears. If not and a progress bar is shown, then the post-upgrade was successfully triggered automatically by Web Manager.
8. If that link appears, click and trigger the post-upgrade.
9. After the post-upgrade step, a reboot can be triggered automatically.
10. Follow the same steps from 2 to 9 for the other systems from the solution.

The following services will be added to IP Office Server Edition on completion of the process:

- IP Office Web Collaboration
- IP Office WebRTC
- IP Office Contact Store
- IP Office Web License Management.

## **Upgrading an OVA**

If you are upgrading an OVA and your system has been through a number of previous upgrades that introduced new kernels, the upgrade report may indicate that the yum process died before completing its job. This is because the /boot partition is almost full. Please execute the following instructions to resolve this.

**Note:** This procedure is not required if the system was upgraded to version 9.1.7 or a later version of software.

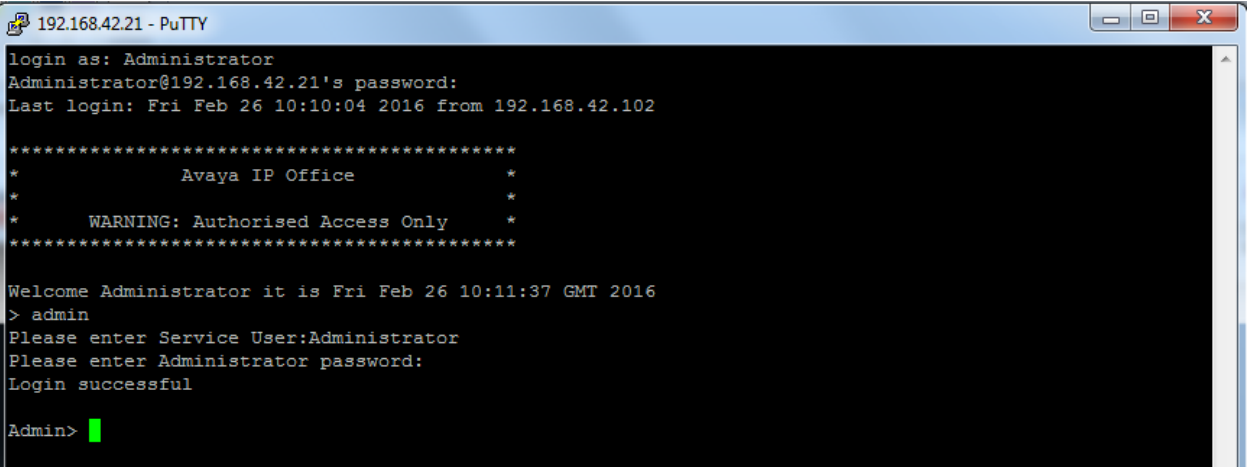
### **1. Start the Upgrade to 10.0**

If the upgrade fails, check the Upgrade Report in Web Manager. If it contains the error, **yum process died before completing its job**, please follow these instructions.

## 2. Download and execute the “UpgradeKernelFix.sh” script

From either the IP Office Admin User DVD or <https://support.avaya.com>, download the UpgradeKernelFix.sh file.

1. Using SCP/WinSCP, copy the script onto the system using the Administrator user.
2. Using PuTTY, connect to the server using the Administrator account. At the root command line,
  - a. Execute the “admin” command, and enter the IP Office Service user credentials for Administrator. Refer to the screenshot below:



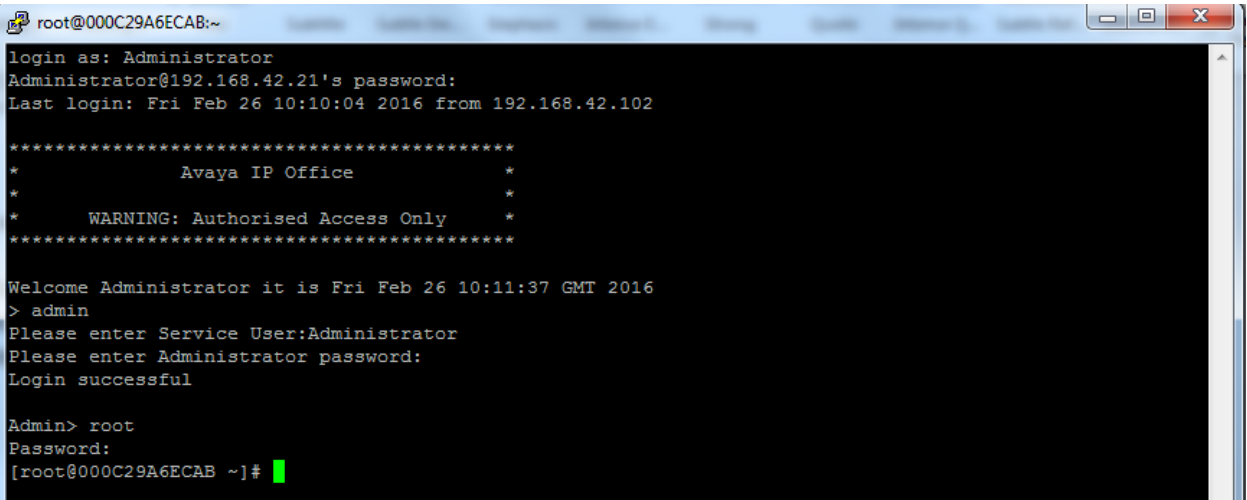
```
192.168.42.21 - PuTTY
login as: Administrator
Administrator@192.168.42.21's password:
Last login: Fri Feb 26 10:10:04 2016 from 192.168.42.102

*****
*                Avaya IP Office                *
*                *                               *
*   WARNING: Authorised Access Only   *
*                *                               *
*****

Welcome Administrator it is Fri Feb 26 10:11:37 GMT 2016
> admin
Please enter Service User:Administrator
Please enter Administrator password:
Login successful

Admin>
```

- b. Execute the “root” command and enter the root password. Refer to the screenshot below:



```
root@000C29A6ECAB:~
login as: Administrator
Administrator@192.168.42.21's password:
Last login: Fri Feb 26 10:10:04 2016 from 192.168.42.102

*****
*                Avaya IP Office                *
*                *                               *
*   WARNING: Authorised Access Only   *
*                *                               *
*****

Welcome Administrator it is Fri Feb 26 10:11:37 GMT 2016
> admin
Please enter Service User:Administrator
Please enter Administrator password:
Login successful

Admin> root
Password:
[root@000C29A6ECAB ~]#
```

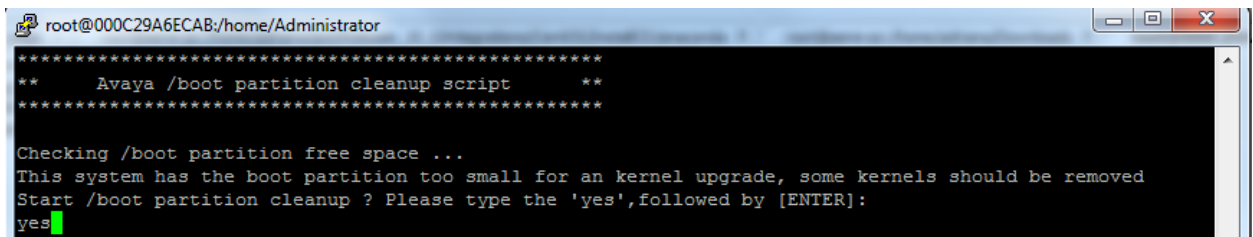
- c. Proceed to the folder where the script was copied, and give execution rights to the script using the following command:

```
chmod +x UpgradeKernelFix.sh
```

```
[root@000C29A6ECAB ~]# cd /home/Administrator  
[root@000C29A6ECAB Administrator]# chmod +x UpgradeKernelFix.sh
```

- d. Execute the **UpgradeKernelFix.sh** script using this command:  
`./UpgradeKernelFix.sh`

The `/boot` partition will be inspected to see if there is enough disk space. The script will prompt the user for a confirmation if some kernels need to be removed. Type “yes” followed by [ENTER]. Refer to the screenshot below:



```
root@000C29A6ECAB:/home/Administrator  
*****  
**      Avaya /boot partition cleanup script      **  
*****  
Checking /boot partition free space ...  
This system has the boot partition too small for an kernel upgrade, some kernels should be removed  
Start /boot partition cleanup ? Please type the 'yes', followed by [ENTER]:  
yes
```

After the script is finished and the `/boot` partition has enough space for an upgrade, a **Success** message is displayed. Refer to the following screenshot:

```
root@000C29A6ECAB:/home/Administrator
*****
**      Avaya /boot partition cleanup script      **
*****

Checking /boot partition free space ...
This system has the boot partition too small for an kernel upgrade, some kernels should be removed
Start /boot partition cleanup ? Please type the 'yes', followed by [ENTER]:
yes
Loaded plugins: fastestmirror, refresh-packagekit
--> Running transaction check
--> Package kernel.x86_64 0:2.6.32-504.23.4.el6 will be erased
--> Finished Dependency Resolution

Dependencies Resolved

=====
Package                Arch                Version                Repository                Size
=====
Removing:
kernel                  x86_64              2.6.32-504.23.4.el6    @system-sG                124 M
=====

Transaction Summary
=====
Remove                1 Package(s)

Installed size: 124 M
Downloading Packages:
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Erasing      : kernel-2.6.32-504.23.4.el6.x86_64
Unable to send message to PackageKit
  Verifying    : kernel-2.6.32-504.23.4.el6.x86_64

Removed:
kernel.x86_64 0:2.6.32-504.23.4.el6

Complete!
Success
[root@000C29A6ECAB Administrator]#
```

If an error appears please raise a ticket with the support team.

This script can be run safely, as it will not modify anything on the system if the /boot partition is large enough.

```
root@000C29A6ECAB:/home/Administrator
*****
**      Avaya /boot partition cleanup script      **
*****

Checking /boot partition free space ...
There is enough space on the /boot partition, if upgrade doesn't work please raise an issue.
[root@000C29A6ECAB Administrator]#
```

This process is now complete.

### Upgrade Instructions for using WebLM Licensing

IP Office Server Edition customers who are upgrading to 10.0 from a previous release, and who will be using WebLM licensing, will need to obtain a WebLM Host ID **before** the upgrade for generating the licenses. The WebLM Host ID is the Mac address of the WebLM server. In a virtual environment, the WebLM Host ID is a virtual Mac address that starts with the letter "V". The WebLM Host ID must be used when generating a PLDS license file for the WebLM server in order to implement a centralized licensing scheme for multiple IP Office systems. Please refer to [Appendix A – Licensing](#), for instructions on how to obtain the WebLM Host ID, and how to upgrade your system.

### Avaya USB Creator Tool

The Avaya USB Creator Tool can be used to load an ISO image onto a USB memory key from which the server can boot and either install or upgrade. This software tool is downloadable from the same page as the ISO files. For further information on this tool, please refer to the "Installing and Maintaining the Avaya IP Office™ Platform Application Server" or the "Installing and Maintaining the Unified Communications Module" located on <https://support.avaya.com>.

### Upgrade Instructions for IP Office Unified Communications Module (UCM)

When upgrading from previous releases, please refer to the following table to determine the upgrade scenario and the method to be used:

From:	To:			
	9.0.0/9.0.1/9.0.2	9.0.3/9.0.4	9.1	10.0
9.0.0	USB Unetbootin Web Control ZIP	USB Unetbootin	USB Unetbootin	USB Unetbootin
9.0.1				
9.0.2				
9.0.3		USB Unetbootin	USB Unetbootin	USB Unetbootin
9.0.4				
9.1			Avaya USB Creator Web Management	Avaya USB Creator Web Management
10.0				Avaya USB Creator Web Management

This release of UCM software also contains the Solid State Drive (SSD) firmware previously documented in IP Office Technical Tip 258.

**Note:** If upgrading to this release from 9.0.0.0.78 (9.0 GA) and earlier, the updated SSD firmware must be applied. Please follow section 3.8 of the UCM Installation and Maintenance manual. The manual can be downloaded from the Avaya Support web site:

<https://downloads.avaya.com/css/P8/documents/100173993>

If upgrading from 9.0.2.0.41 (9.0 Service Pack 2) or later to this release, it should not be necessary to re-apply the updated SSD firmware. The updated firmware should already have been applied.

**Warning:** In all cases, always backup all application data to a separate location before upgrading.

**Warning:** one-X<sup>®</sup> Portal logging MUST be disabled prior to upgrade. One-X<sup>®</sup> Portal admin will be very slow to respond if this is not done. One-X<sup>®</sup> Portal logging can be disabled using the one-X<sup>®</sup> Portal Administrator/Logging Configuration/Master Logging Level = OFF. This warning is applicable only when upgrading by using Web Manager from a release between 9.1 GA and 9.1.4. Starting with 9.1.5, the one-X<sup>®</sup> Portal service is stopped during upgrade using Web Manager,

## Upgrade Instructions for Avaya Communicator for Windows

The Avaya Communicator for Windows (ACW) installer can be downloaded from the Avaya Support site:

<https://support.avaya.com/products/P1572/avaya-communicator-for-windows/> :

Perform the following steps to install ACW:

- Install the ACW by double-clicking *Avaya-Communicator.msi*, and follow the installation wizard.
- When the installation is complete, a message will display to disable the diagnostics logs.
- Open Settings > Support, and uncheck *Enable Diagnostic Logging*.

## Installation Instructions for Avaya Communicator for Microsoft Lync

The Avaya Communicator for Microsoft Lync plug-in is distributed as a ZIP file, which contains:

- *lyncRuntime.msi*
- *AvayaCommunicatorForMicrosoft.X.IPO-X.6.X.X-SNAPSHOT.msi*

The plug-in is installed as an add-in to Lync 2010, Lync 2013 or Skype for Business clients.

Perform the following steps to install the plug-in:

1. Install the prerequisite by double-clicking *lyncRuntime.msi*, and follow the installation wizard. This step only needs to be done once per computer.
2. Install the plug-in by double-clicking *AvayaCommunicatorForMicrosoft.X.IPO-X.6.X.X-SNAPSHOT.msi*, and follow the installation wizard.

## Operating System Support

Since support for Windows XP has ended, IP Office no longer supports Windows XP or Internet Explorer version 8.

### Windows Operating System Editions and Service Packs

Operating System	Windows Service Pack	Editions
Windows 7 32/64	SP1	Professional, Enterprise, Ultimate
Windows 8.1	n/a	Pro, Enterprise
Windows 10	n/a	Pro (SMB), Enterprise
Server 2008 R2 (64 only)	SP1	Standard
Server 2012	n/a	Standard
Server 2012 R2	n/a	Standard

### Operating System Support - Server Components

Application	Win 7		Win 8.1 (2)		Win 10		Server 2008R2	Server 2012/2012R2
	32 bit	64 bit	32 bit	64 bit	32 bit	64 bit	64 bit	64 bit
Preferred Edition Server (Voicemail Pro)	✓	✓	✓	✓	✓	✓	✓	✓
Standalone								
... Plus UMS	✗	✗	✗	✗	✗	✗	✓	✓
... Plus Campaigns	✗	✗	✗	✗	✗	✗	✓	✓
... with IMS	✗	✗	✗	✗	✗	✗	✗	✗
... MAPI service for Voicemail Pro on Linux	✓	✓	✗	✗	✗	✗	✓	✓
Contact Store Server	✗	✗	✗	✗	✗	✗	✗	✗
one-X® Portal for IP Office Server, Windows	✗	✗	✗	✗	✗	✗	✓	✓
TAPI - 1st Party	✓	✓	✓	✓	✓	✓	✓	✓
TAPI - 3rd Party	✓	✓	✓	✓	✓	✓	✓	✓
TAPI – WAV (3)	✓	✗	✓	✗	✓	✗	✗	✗
IP Office Contact Centre (IPOCC)	✗	✗	✗	✗	✗	✗	✓	✓ <sup>(1)</sup>

1. IPOCC is Server 2012R2.
2. As per Microsoft, Win 8.1 is the replacement/Service Pack for 8.0 so we no longer support 8.0 - <http://windows.microsoft.com/en-GB/windows/service-packs-download#sptabs=win80ther> (link valid 16-Jun-2014)
3. TAPI WAV is not recommended for new designs and is not supported on 64-bit operating systems.

### Operating System Support - Thick Client Apps

Application	Win 7		Win 8.1		Win 10		Server 2008R2	Server 2012/2012R2
	32 bit	64 bit	32 bit	64 bit	32 bit	64 bit	64 bit	64 bit
Preferred Edition Client	✓	✓	✓	✓	✓	✓	✓	✓
Soft Console	✓	✓	✓	✓	✓	✓	✗	✗
Manager	✓	✓	✓	✓	✓	✓	✓	✓
SysMon	✓	✓	✓	✓	✓	✓	✓	✓
SSA	✓	✓	✓	✓	✓	✓	✓	✓
TAPI 1 <sup>st</sup> Party	✓	✓	✓	✓	✓	✓	✓	✓
TAPI WAV (2)	✓	✗	✓	✗	✓	✗	✗	✗
IP Office Video Softphone (1)	✓	✓	✗	✗	✗	✗	✗	✗
Avaya Communicator for Windows (ACW) (replaces Flare)	✓	✓	✓	✓	✓	✓	✗	✗
Avaya IP Office Plug-In for Microsoft® Outlook	✓	✓	✓	✓	✓	✓	✗	✗
one-X® Portal Plug-In for Salesforce.com	✗	✗	✗	✗	✗	✗	✗	✗
Avaya one-X Call Assistant	✓	✓	✓	✓	✓	✓	✗	✗
Avaya Communicator for Microsoft Lync Plug-In 2013	✓	✓	✓	✓	✓	✓	✗	✗
Web Conferencing (Adobe Flash and Java Applet for sharing)	✓	✓	✓	✓	✓	✓	✗	✗
IP Office Contact Centre	✓	✓	✓	✓	✓	✓	✗	✗

1. Legacy support only
2. TAPI WAV is not recommended for new designs and is not supported on 64-bit operating systems.

### Mac Thick Client Apps

Application	OSX 10.7 Lion	OSX 10.8 Mountain Lion	OSX 10.9 Mavericks	OSX 10.10 Yosemite	OSX 10.11 El Capitan
IP Office Video Softphone - Version 4.0	✗	✓	✓	✓	✓
Web Conferencing (Adobe Flash and Java Applet for sharing)	✗	✓	✓	✓	✓



### Browsers

Application	IE10 (2)	IE11	Edge	FFXX (1)	Chrome XX (1)	Safari 8	Safari 9
Voicemail Pro Campaigns Client	✓	✓	✓	✗	✗	✗	✗
Voicemail Pro UMS WebMail	✓	✓	✓	✗	✗	✗	✗
Contact Recorder Client	✓	✓	✗	✗	✗	✗	✗
one-X® Portal for IP Office Client	✓	✓	✓	✓	✓	✓	✓
Web Conferencing	✓	✓	✓	✓	✓	✓	✓
Web Manager	✓	✓	✓	✓	✓	✓	✓
Web Control Page	✓	✓	✓	✓	✓	✓	✓
D100 DECT Admin	✓	✓	✓	✓	✓	✓	✓
IP DECT R4 Admin	✓	✓	✓	✓	✓	✓	✓
Avaya Communicator for Web	✗	✓	✗	✗	✓	✗	✗

1. The version for FireFox and Chrome will be set - we aim to support future versions of these fast release browsers (any issues found will be accepted by life-cycle).
2. Only on Server 2012 (note Server2012R2 supports IE11)

### Exchange

Application	Exchange 2010	Exchange 2013	Exchange 2016
Voicemail Pro UMS	✓	✓	✓
one-X® Portal (IM Presence)	✓	✓	✓

### Outlook

Application	Outlook 2010	Outlook 2013	Outlook 2016
Voicemail Pro IMS	✗	✗	✗
TAPI (for dialling)	✓	✓	✓
Voicemail Pro UMS IMAP	✓	✓	✓
Avaya IP Office Plug-In for Microsoft® Outlook	✓	✓ <sup>(1)</sup>	✓ <sup>(1)</sup>

1. Currently for Outlook 2013 and higher, the contact screen popping feature is not supported.

### ***IP Office Deployed as an Aura Branch***

Key Branch Functionality (additions for 10.0 have been underlined)

- ▶ ‘SM Line’ customized and tested type of SIP trunk for SIP interoperability with Avaya Aura® Session Manager (SM) and other systems and applications connected through it
  - Support for SM redundancy via redundant SM Lines
  - Number manipulation for calls over the SM Line based on configured ‘Branch Prefix’
- ▶ Centralized management by Avaya Aura® System Manager (SMGR) of IP Office, IP Office Application Server, UCM and Voicemail Pro
  - Release 10.0 introduces support for System Manager Geo-Redundancy
- ▶ PLDS Licenses and centralized licensing by WebLM
  - Release 10.0 requires uplift of the IP Office licenses to R10
  - Release 10.0 introduces support for Secondary WebLM server as part of the support for System Manager Geo-Redundancy
- ▶ Support for centralized Voicemail including MWI by SIP interactions through SM with AAM, MM and CS1K CallPilot
  - And support for backup connection to MM and AAM via the PSTN when the SM Line is down
  - Local Auto Attendant split from local VM, can be used with centralized Voicemail
- ▶ Support for TLS and SRTP
- ▶ Support for SIP Centralized Users
  - Release 10.0 adds support for H175 Video Collaboration Station and Avaya Communicator For Windows as Centralized Users
- ▶ Support for Analog Terminal Adaptation - analog stations deployed as ATA users

### ***Key Terms used in Branch Deployments***

- ▶ **IP Office user** – a user who gets telephony features and services from the local IP Office. Previously referred to as distributed user, local user, or native user
- ▶ **Centralized user** – a user who normally (aka in **sunny-day**) registers and gets call processing service from the Avaya Aura servers in the enterprise core, and in case of WAN failure (aka in **rainy-day**) gets survivable service from the IP Office in the branch
- ▶ **IP Office phone** – a phone used by an IP Office user
- ▶ **Centralized phone** – a phone used by a centralized user (certain SIP phones only)
- ▶ **Distributed enterprise branch deployment** – a deployment where all users in a branch are IP Office users
- ▶ **Centralized enterprise branch deployment** – a deployment where all users in a branch are Centralized users
- ▶ **Mixed enterprise branch deployment** – a deployment where there are Centralized users and IP Office users in the same branch. The centralized users get their telephony services from the Avaya Aura servers in the core, and the IP Office users get their telephony services from the local IP Office.

### **Branch Deployment Restrictions**

- ▶ The branch functionality is available in IP Office Standard mode, i.e. in Essential and Preferred Editions
  - IP Office Server Edition (SE) is not positioned as a branch product
    - SE supports interoperability with Aura SM, and with CM or CS1K through the SM, using SIP through an 'SM Line' interface
    - But SE does not support the branch functionality of SMGR management, Centralized Users or voicemail over 'SM Line'
- ▶ SCN is not supported in IP Office Branch Deployments
  - Not prevented by software, hence limited co-existence
  - An SCN can connect to Avaya Aura SM through 'SM Line' on one of the SCN IP Offices
    - The whole SCN operates as a single branch
  - SCN cannot coexist with Centralized Users or with centralized voicemail over 'SM Line'
  - SMGR management of SCN is not supported
- ▶ No IP Office User Rights when managed by SMGR
- ▶ No Auto-creation of users and of IP extensions when WebLM mode and when managed by SMGR

### **Aura Load Line up**

Name	Avaya Aura "Standard" solution	Avaya Aura MidSize Enterprise Solution
AVP	latest needed for each platform	latest needed for each platform
System Manager	7.0.1.1	7.0.1.1
Session Manager	7.0.1.1	7.0.1.1
Communication Manager	7.0.1.1	7.0.1.1

## Languages Added

IP Office release 10.0.0.0 adds Mediterranean locale among the supported languages for 14xx, 16xx and 96x1 H323 phones, Embedded Voicemail and Voicemail Pro audio prompts. Hungarian is added for one-X® Mobile Preferred for Android and iOS.

## Documentation errata

The latest versions of detailed release information can be found in the below locations:

- DVD media available with Avaya IP Office R10.0 software pack
- IP Office Knowledgebase - Contains all administrator and user documentation for IP Office - <http://marketingtools.avaya.com/knowledgebase>
- The Avaya support site – Contains all administrator and user documentation for IP Office - <http://support.avaya.com>

The Release 10.0 Documentation will be available by GA:

- Go to [support.avaya.com](http://support.avaya.com)
- Select [Find Documentation and Technical Information by Product Name](#) under Downloads & Documents
- Enter 'IP Office' as your product
- Choose '10.0' as your release
- Click the 'Documents' radio button
- Click 'Enter' to see all documentation

The latest version of the 'IP Office Start Here First' document, which describes the organization of all IP Office documents and indicates the type of information in each document, can be found at <https://downloads.avaya.com/css/P8/documents/101028675>

The following release documents can be found at <https://sales.avaya.com/en/ip-office-release-10.0-sales-toolkit>

These will require a valid Single Sign On (SSO) user name and password to view online.

- IP Office Release 10 Product Offer Definition Document, which defines the IP Office product in more detail.
- IP Office 10.0 Product Update document, which is a communication that summarizes “what’s new” within the IP Office Release 10.0 product
- IP Office Release 10.0 deployed as a Branch Product Offer, which defines the branch solutions, commercial tools, licensing and migration/upgrade scenarios in more detail

## Contacting support

### Contact Support Checklist

If you are having trouble with *IP Office*, you should:

1. Retry the action. Carefully follow the instructions in written or online documentation.
2. Check the documentation that came with your hardware for maintenance or hardware-related problems.
3. Note the sequence of events that led to the problem and the exact messages displayed. Have the Avaya documentation available.

If you continue to have a problem, contact Avaya Technical Support:

1. Log in to the Avaya Technical Support Web site <https://support.avaya.com>.
2. Contact Avaya Technical Support at one of the telephone numbers in the Support Directory listings on the Avaya support Web site.

Avaya Global Services Escalation Management provides the means to escalate urgent service issues. For more information, see the Escalation Contacts listings on the Avaya Web site.

### Contact Support Tasks

You may be asked to email one or more files to Technical Support for analysis of your application and its environment.

The Technical Bulletin appendices are a new addition to the IP Office release notes and are intended to supplement our formal documentation. The appendices will provide additional guidance for some of the more complex features and components found during Beta trials of the new release.

## Appendix A – Licensing

### IP Office Release 10 Licensing Changes

IP Office Release 10 and higher only supports the Product Licensing and Delivery System (PLDS) to manage license files. PLDS is an online, web-based tool for managing license entitlements and electronic delivery of software and related license files. If you are upgrading from a previous release of IP Office software, you must migrate all of your pre-release 10 licenses (ADI, PLDS, mix of ADI/PLDS, virtual) to release 10 PLDS licenses.

### License Migration Requirements

To help with the migration of your older licenses to PLDS, a new License Migration tool has been added to the R10 Manager application. The License Migration tool extracts all of the licensing information from an IP Office system and saves it to a file. This file can then be used to prepare a software upgrade quote in the Avaya One Source Configurator in order to obtain the required new PLDS R10 licenses. License migration is supported on all IP Office modes, release 6.0 and higher.

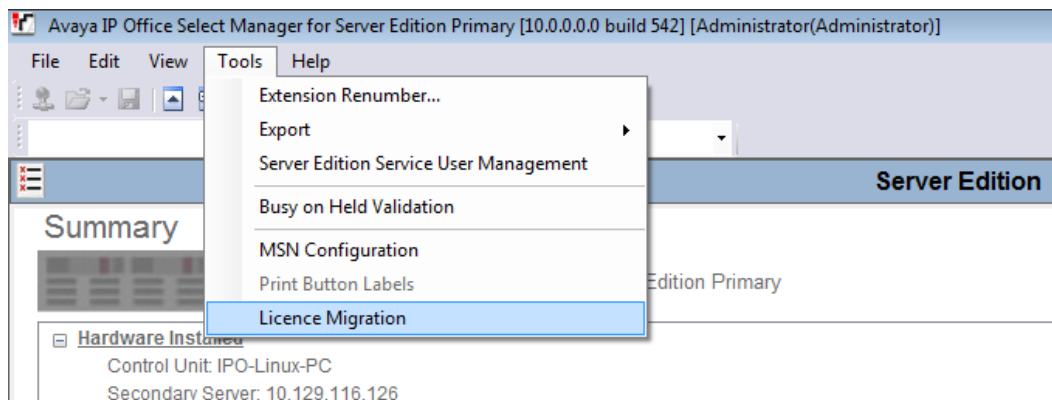
For Server Edition deployments, the License Migration tool collects licensing information from every node in the solution. For Essential/Preferred Edition systems connected via SCN, you must run the migration tool on each system in the network to extract their licensing information.

**Note:** *You must use the release 10 Manager application to extract the licensing information. You can install the R10 Manager application before upgrading your IP Office systems to release 10.*

Before you begin the License Migration process, ensure all licenses are loaded on the system before performing the license migration. For Server Edition deployments, ensure all nodes are online in order to capture the current view of systems in the solution. The IP Office configuration must be opened online. The License Migration tool is not available in offline mode.

### Using the License Migration Tool

Start the Manager application, and open the configuration from your IP Office system. With the configuration loaded, select Tools > License / License Migration.



The 'Save As' window opens, allowing you to select a location to save the License Migration file. Enter a file name and click Save. The file is saved with a .zip extension (*abc.zip*, where *abc* is the file name that you chose). If you look in the zip file, you will find an XML file (*abc.xml*, where *abc* is the file name that you chose when saving the .zip file). This actually contains details about your system, the extensions, and the users, as well as containing all of the licensing information (No user identifiable data will be retained or used by the IP Office system). This is the file that will be used to prepare a software upgrade quote in the Avaya One Source Configurator, in order to obtain the required new PLDS R10 licenses.

This XML file, *abc.xml*, has a digital signature for verification. Do not edit this file. The file is signed to prevent tampering with the contents.

The generated file can be read but must not be edited. If you attempt to alter the values in this file it will fail validation when it is uploaded and you will not be able to get your new licenses. If you need to add additional licenses, this can be done at the same time that you are preparing your upgrade quote.

- License migration is supported on all IP Office modes, release 6.0 and higher.
- The License Migration tool can only be used with an online configuration. This is because certain licenses, like virtual licenses, do not get saved in offline configuration files.
- The Tools > License Migration option is disabled for offline configurations.
- For Server Edition deployments, the License Migration tool collects licensing information from every node in the solution.
- For Essential/Preferred Edition systems connected via SCN, you must run the migration tool on each system in the network to extract the licensing information.

## Nodal Licensing

For IP Office Essential/Preferred Edition systems, Nodal licensing is the only licensing option that is available, except in Branch deployments, which also supports WebLM licensing. (Refer to the documentation of IP Office in Branch Deployments.) With nodal licensing, the licenses are managed using individual license files installed on each node in the network. This means that you need to obtain and load individual PLDS license files onto each of your systems. PLDS nodal license files are system specific and use the systems PLDS Host ID, which you can find in the configuration on the License | License tab. You would normally specify the PLDS Host ID of each system when obtaining licenses, very similar to the way that ADI licensing uses the Feature Key number or

System ID. The License Migration tool takes care of this part for you, and the XML file you extract from each system will already contain this information.

For Server Edition deployments, you can use a combination of Distributed and Nodal licensing (hybrid model), which is the current method used for systems running 8.1 or 9.x software. This would require you to obtain a PLDS license file for the Primary Server, and if there is a requirement for systems to use licenses that cannot be distributed centrally from the Primary Server, then you also need to obtain a PLDS license file for any Secondary Server or Expansion systems. An example of this would be a CTI or PRI channel license which must be installed on the specific system that needs to use it.

If using Nodal licenses for Server Edition deployments, the following six license types can be distributed by the Primary Server to the Secondary Server or Expansion systems. Any other license types would require a separate PLDS Nodal license for each system:

- Server Edition license (one required for each node in the network)
- Office Worker
- Power User
- Avaya IP Endpoint
- 3<sup>rd</sup> Party IP Endpoints
- SIP Trunk Channels

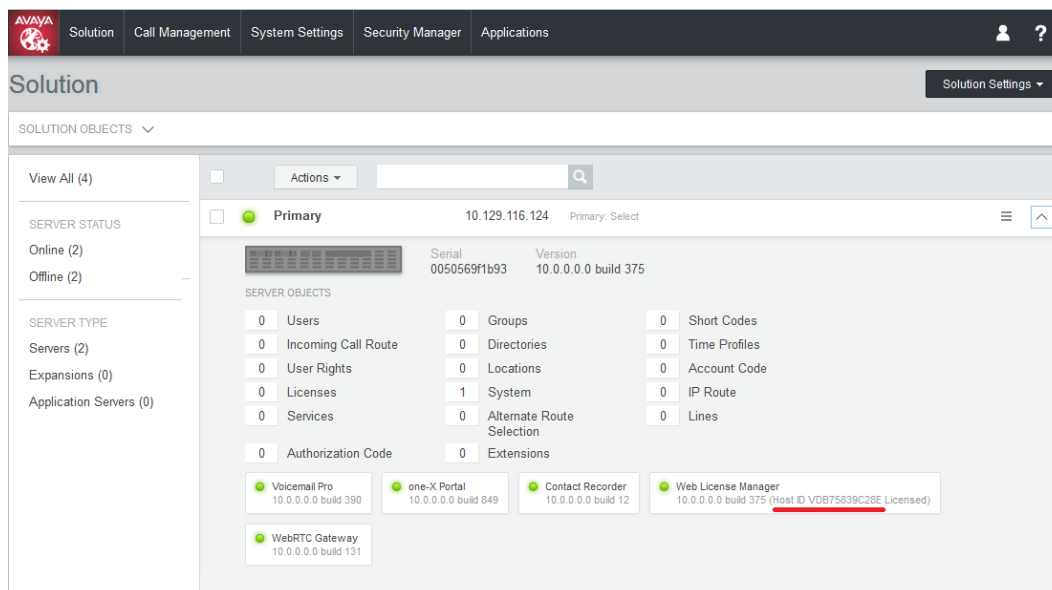
### **WebLM Centralized Licensing – Obtaining the Host ID**

IP Office Release 10 enhances the licensing mechanism further for Server Edition systems and now provides true centralized licensing for all systems in the network using the built in WebLM server on the Primary server. Please refer to the IP Office 10.0 Solution Description document for additional information of the WebLM Centralized Licensing solution.

WebLM was first introduced in the 9.1 release, but it was not supported in that release. Now with release 10, all licenses can be placed into one PLDS license file that is loaded into the WebLM server. This provides all systems in the network with the licenses that they need. It allows customers to easily move users, profile licenses, and other resources around the network to the systems that need them.

Instead of using a PLDS Host ID to generate licenses, the WebLM server uses the WebLM Host ID. The WebLM Host ID can be found in Web Manager, on the Solution View page of systems that are running IP Office 9.1. As WebLM was only introduced in 9.1, any systems being upgraded from 8.1 or 9.0 would not have WebLM installed; therefore, this information about the WebLM Host ID is not available. An alternative method for finding what the WebLM Host ID will be once the system is upgraded to release 10 is discussed later in this document.





Some pre-10.0 virtual Server Edition systems may display an obsolete WebLM Host ID. For deployments using real servers (non-virtualized), the WebLM Host ID is simply the same as the IP Office LAN1 MAC address, or Serial Number as it is shown in the screenshot above. This is the information that you would use if moving to Centralized WebLM licensing.

For virtual server deployments, the WebLM Host ID is different to the MAC address of the system and uses a virtual WebLM Host ID. This is generated using certain system parameters, in a very similar way that the System ID is generated. On these systems, the WebLM Host ID should be in the format V.....; however, on a couple of test systems, the WebLM Host ID that was displayed was the same as the MAC address of the system. All of the systems that showed this problem had been through a number of previous upgrades from versions of 9.0 and early versions on 9.1. If when you check your system, you find that the WebLM Host ID is incorrect, there are two ways to get the correct information.

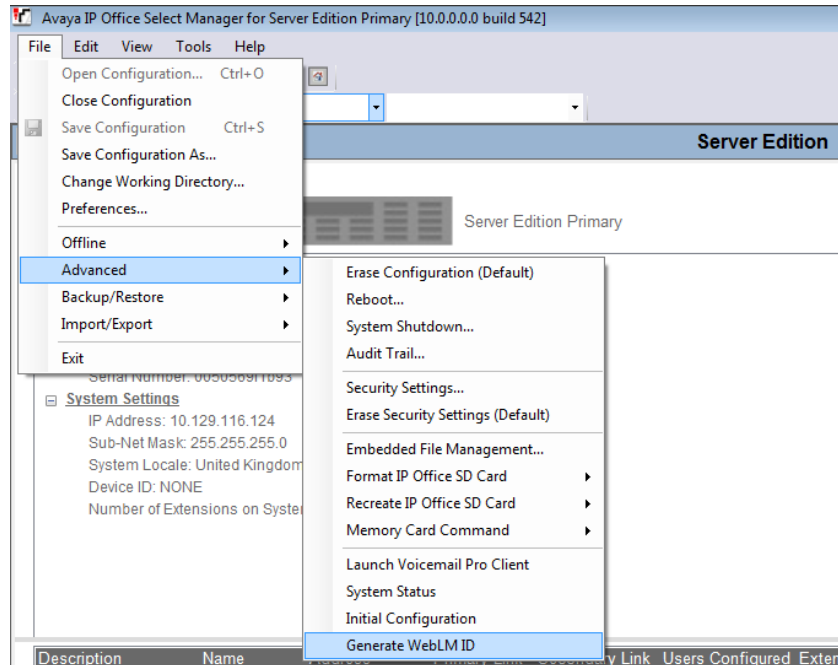
The first of these methods is to apply a WebLM patch to your system. This patch will be available from the <https://support.avaya.com> website. There are two ways to install this patch on your Primary Server. You can login directly to web control (on port 7071) or login via Web Manager (on port 7070). Go to Platform View (which will take you to the same Web Control options you get by logging in directly on port 7071).

In Web Control, go to the Settings tab. In the Software Repositories section, use the Browse button associated with Applications and locate the WebLM patch on your PC. Then click on the Add button to upload the patch to your system. Once the file has finished uploading, go to the Updates tab and look under services for 'Web License Manager'. The status should show as 'out of date'. Click on the update button to update the system. Once this has finished, go back to the Solution view page and check the WebLM Host ID. It should now show the correct ID starting V....

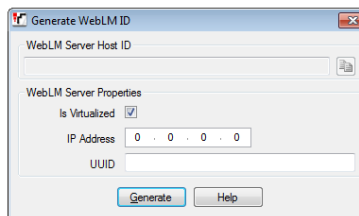
This method will work for 9.1 systems but as WebLM was only introduced in 9.1, any systems being upgraded from 8.1 or 9.0 would not have WebLM installed; therefore, this information about the WebLM Host ID is not available. If you are upgrading from these releases, another tool has been added to the release 10 Manager application to help find out what the WebLM Host ID of the system will be once it is upgraded to release 10.

This tool can also be used for 9.1 systems that have the issue described above with the incorrect WebLM ID showing, as an alternative to applying the WebLM patch.

Open the Manager application and select File > Advanced > Generate WebLM ID.

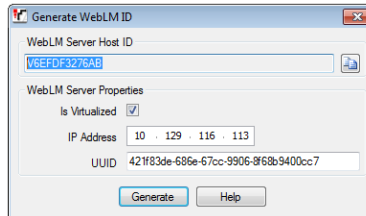


In the dialog box that appears, select the 'Is Virtualized' checkbox and enter the IP Address of the system and the UUID of the virtual machine.



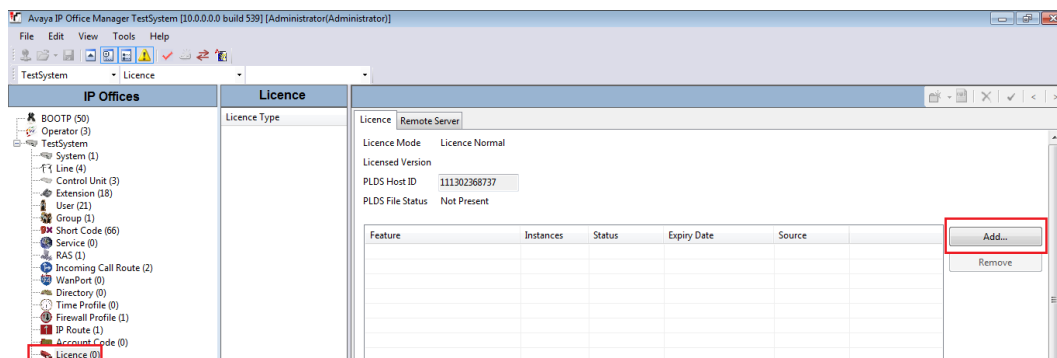
The UUID of the virtual machine can be found using the VMware vSphere client. Look at the Inventory > Virtual Machines tab and find the virtual IP Office system. One of the columns displayed will show the system UUID.

The details of this system can be copied to Notepad and then you can copy the UUID field into the Generate WebLM tool. Once all of the information has been added to the tool, click 'Generate' and the WebLM Host ID will be displayed. This can then be used to generate your Centralized PLDS license file.

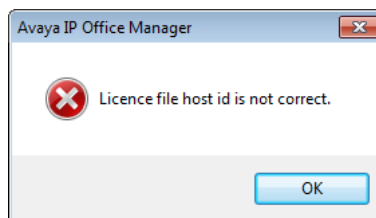


## Nodal License Configuration – IP500V2 Essential/Preferred Edition

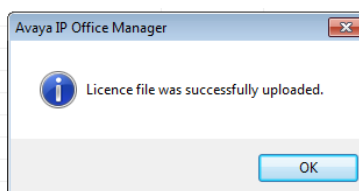
When you have obtained your release 10 PLDS licenses, save them to your PC and open your IP Office configuration using the Manager application. Go to License / License | License / License and click on the Add button.



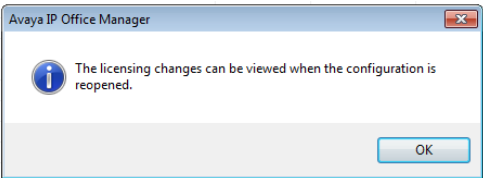
Browse to the location of your PLDS license file and click on Open. The IP Office system will then attempt to load and validate the license file. If there is a problem with the file, for example the PLDS Host ID is incorrect, you will receive an error message.



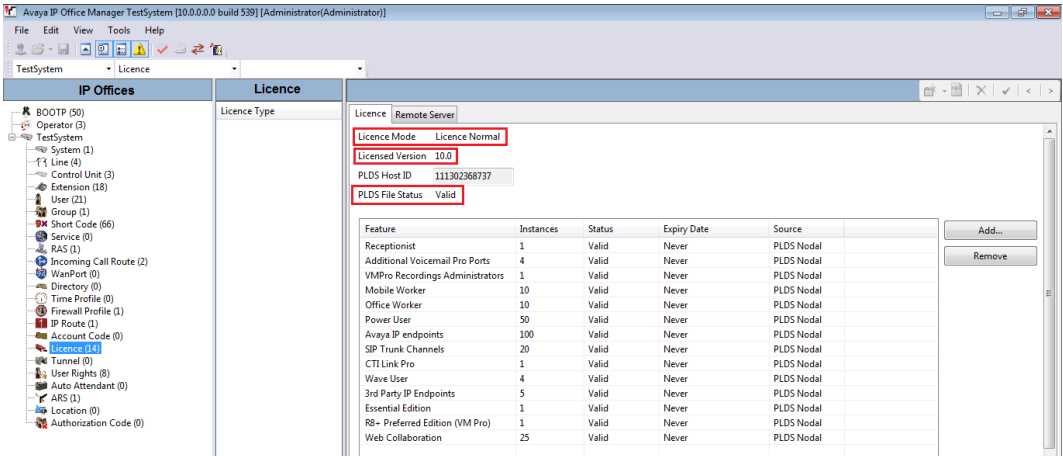
If the file is validated, you will get a popup dialog confirming that the license file was successfully uploaded.



Click on OK and an additional popup dialog appears. You must now close and re-open the configuration to view the new licenses.



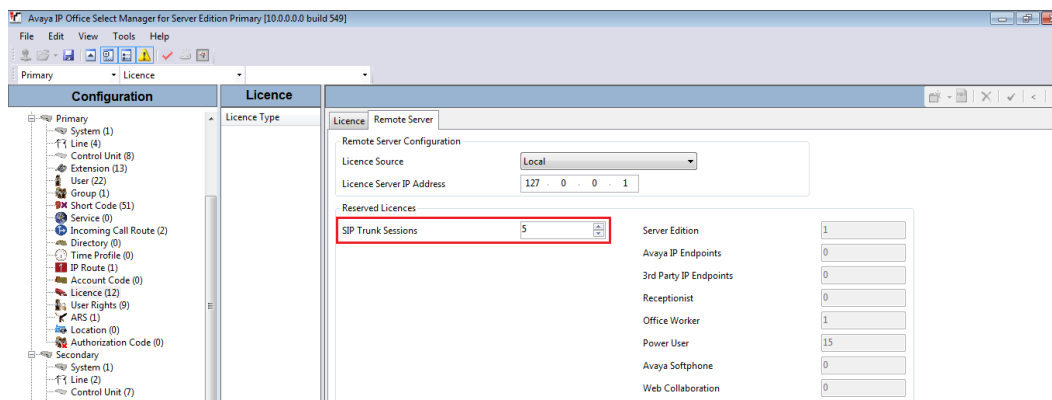
After opening the config, you can view the new PLDS licenses in the configuration.



### Nodal License Configuration – Server Edition

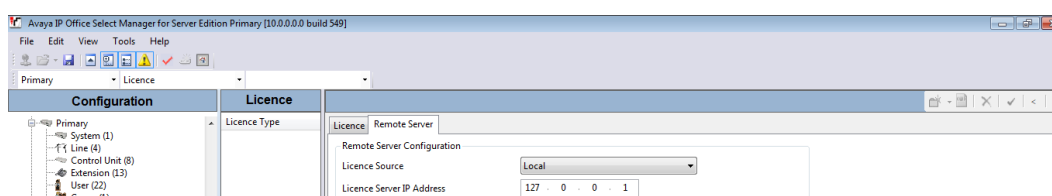
The process for adding Nodal PLDS licenses to Server Edition systems is the same process as described above. Start with the Primary Server and add the PLDS license file. If you have any Secondary Server or Expansion systems that need local licenses, follow the same process to add the licenses to those systems.

Any distributed licenses on the Primary Server will automatically be allocated to the Secondary Server and Expansion systems when they request them, except for SIP trunk channels. The number of SIP trunk licenses each system needs, including the Primary Server, needs to be set in the configuration. In previous versions of IP Office this setting, called Max SIP Sessions, was found in the System | Telephony settings tab. In release 10, this setting has been moved to License / License | Remote Server in the Reserved Licenses section and has been renamed to SIP Trunk Sessions.

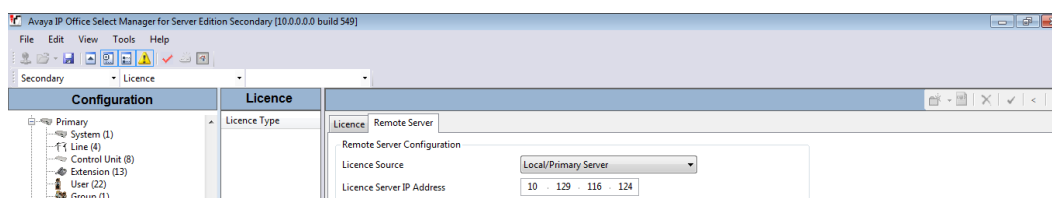


You will also notice some additional values displayed in the boxes to the right hand side of this Reserved Licences screen in Grey. These are other licenses that the system needs. These values are driven by the actual configuration of the particular node that you are looking at in Manager and cannot be set manually.

In the Remote Server tab, there is also an additional drop down configuration item added to allow you to specify the License Source for the system. For Nodal licensing, this would be set to Local on the Primary Server



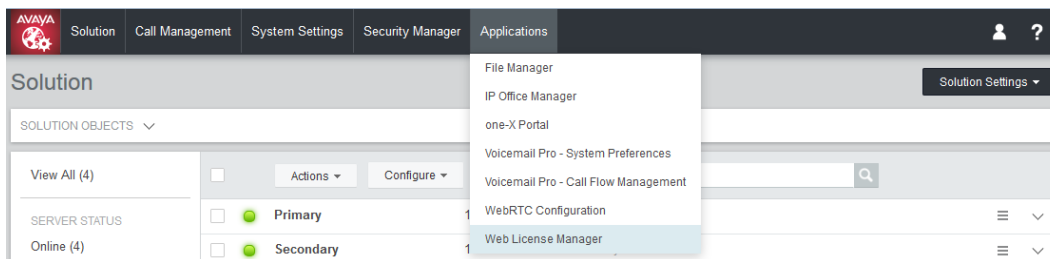
And set to Local\Primary Server on all other nodes in the solution.



## Installing a Centralized WebLM License

If you decide that you want to use Centralized WebLM licensing, first obtain a single PLDS license file, making sure that the licenses are generated against the WebLM Host ID and not the system PLDS Host ID.

Once you have obtained your license file, save it to your PC and login to your Server Edition system using Web Manager. In Web Manager, select Applications > Web License Manager.



Login to the WebLM server. If this is the first time you have logged in to WebLM the default credentials to use are:

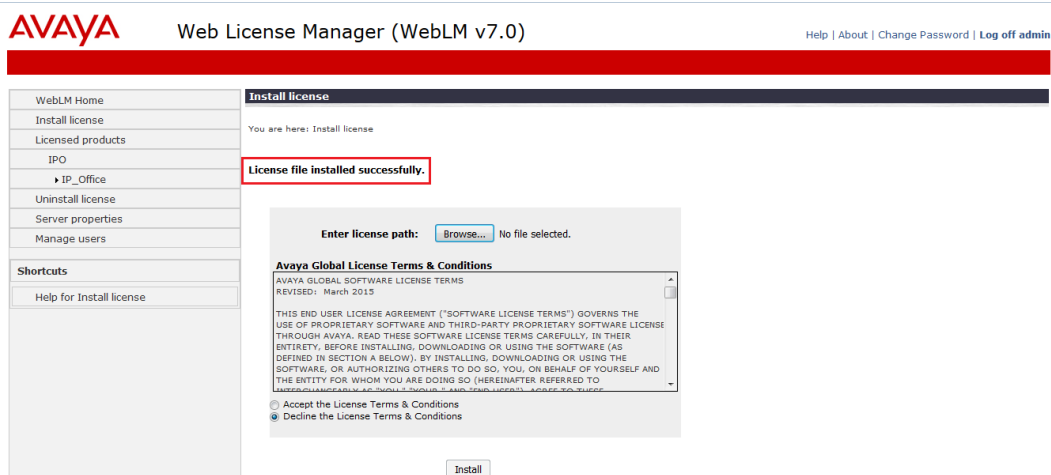
- User Name: admin
- Password: weblmadmin

© 2015 Avaya Inc. All Rights Reserved.

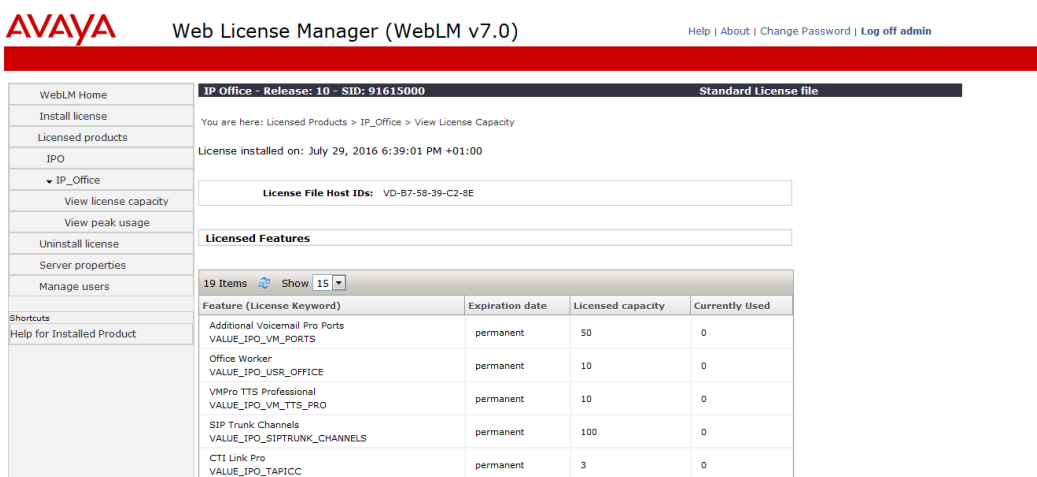
You will be forced to change the password when you login. You will then be logged out and will have to login again with your new credentials.

In the navigation pane on the left, click Server Properties. The Server Properties page displays the Host ID. The host ID is the MAC address of the Server Edition Primary server for non-virtualized deployments or will start with V... for virtualized server deployments.

In the navigation pane, click on Install license, then click on the Browse button, and navigate to your license. Make sure you select the 'Accept the License Terms & Conditions' radio button. Then click on Install. You should receive a confirmation message that the license was installed successfully.



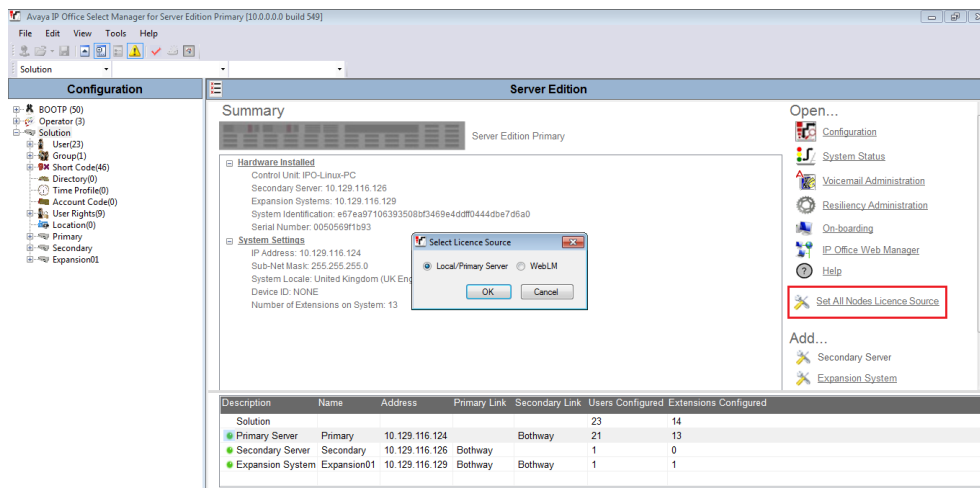
In the navigation pane on the left, under Licensed products, click on IP\_Office. Here you will see the licenses that are installed on your system along with details about how many of them are currently in use.



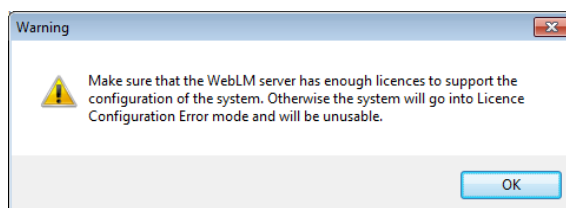
## Converting from Nodal to Centralized Licensing

For IP Office Server Edition systems that are upgraded to release 10, the default licensing mechanism will remain as Nodal licensing, the same as it would have been before upgrade. For new installations, the default setting is now WebLM.

Once you have loaded your license file into the WebLM server, open your IP Office Server Edition configuration using the Manager application. The easiest way to change the systems from Nodal to WebLM licensing is to go to the Solution View and click on 'Set All Nodes License / License Source'. This will give a popup dialog allowing you to select Local/Primary Server or WebLM.



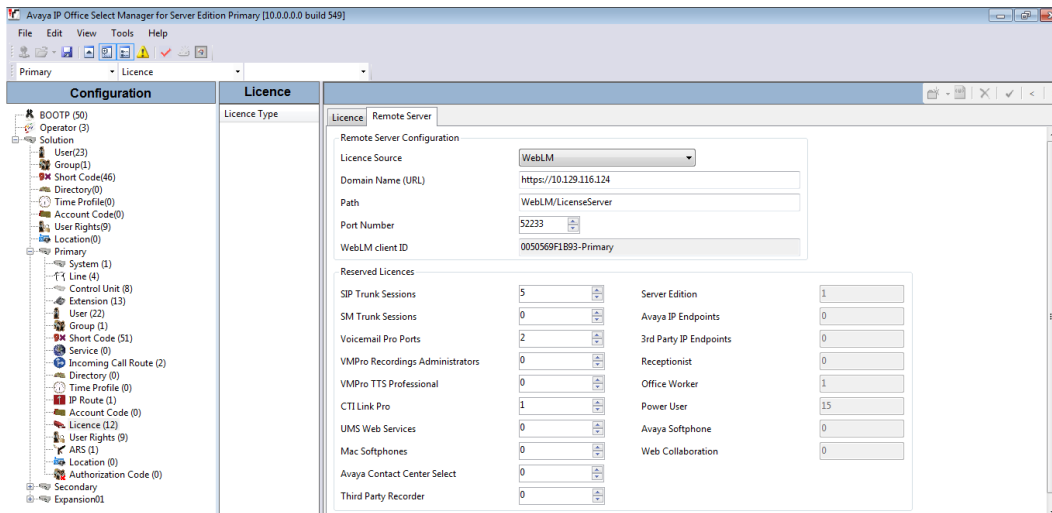
Clicking on the WebLM option will give you an additional popup dialog box with a warning about having the correct number of licenses in WebLM. More details about this will be discussed further on in this document. Click on OK, and OK again to confirm the change.



**Note:** All nodes in the solution must have the same license source. You cannot have a mixture of Local and Centralized licensing.

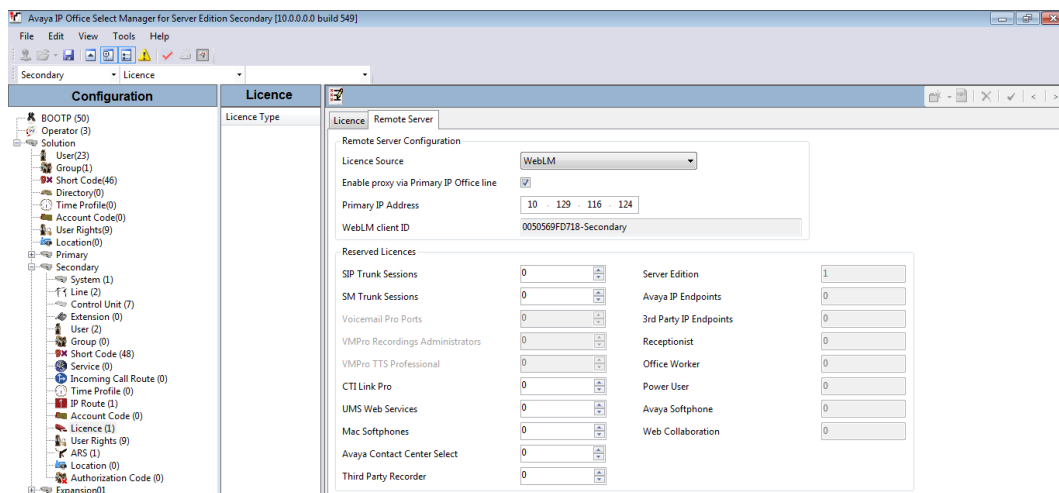
If you now go to License / License | Remote Server, you will see additional details added under the License / License Source setting. This is the URL, path, and port number of the WebLM server. You will also notice that the list of reserved licenses has also expanded. If your system needs any of the licenses from the column on the left hand side, you must set the appropriate values so that the system can request these from the WebLM server. The licenses in the right hand column cannot be set. They will automatically be requested from the WebLM server.





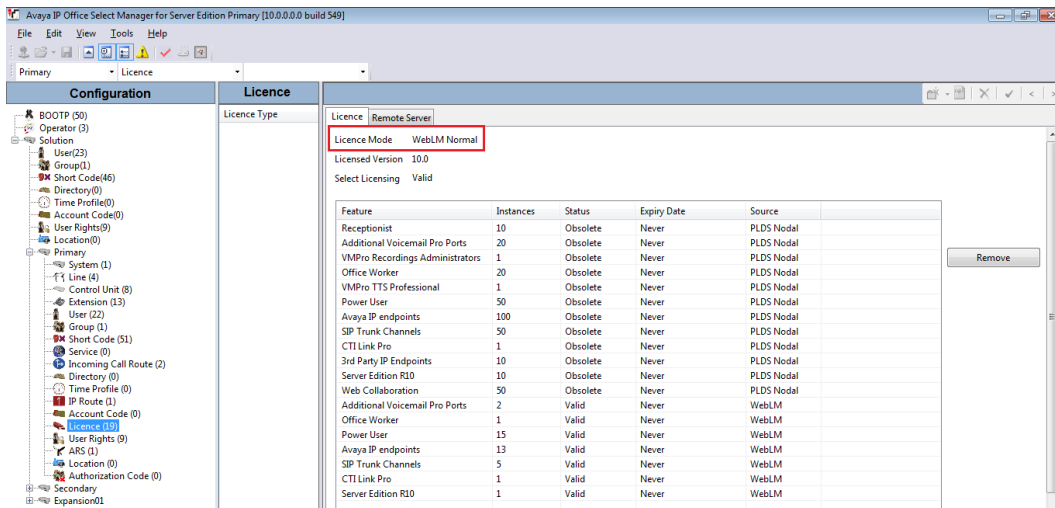
The settings on any Secondary Server and Expansion system are slightly different. There is a checkbox 'Enable Proxy via Primary IP Office line' which tells the system to use the Primary Server as a proxy to obtain the licenses from the WebLM server. It is also possible to uncheck this box and have each system go directly to the WebLM server. However, the default setting is to use the Primary as the proxy.

**Note:** The Proxy setting is not available if the transport type of the IP Office line to the Primary Server is NOT configured as a WebSocket client. In the event that the IP Office lines have been set to Proprietary, the license requests will have to go directly to the WebLM server.



Once all of the settings have been checked, and any necessary license reservations have been set, save the configurations. A reboot of all systems will be required to change the licensing mode.

After the systems have restarted, open the IP Office Server Edition configuration to check that the system has been able to obtain the licenses it requires from the WebLM Server. Provided that the system has been able to successfully acquire the licenses, you should see the License / License Mode showing 'WebLM Normal'.



Note that the previously installed Nodal licenses are now listed as obsolete. You can either leave these licenses in the config or you can delete the obsolete licenses.

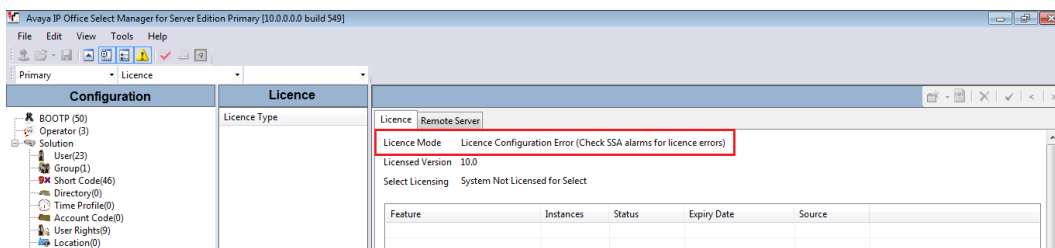
The WebLM server can show you the total amount of licenses that have been consumed by your systems and you can also see which systems have which licenses. Log in to your WebLM server. From the navigation pane on the left hand side, select Licensed Products > IP\_Office. You can view the licensed capacity as well as the number of licenses currently used. If you scroll down to the bottom of this page, you will also be able to see which systems are using these licenses.

Acquired Licenses		
12 Items  Show <span>All</span>		
Feature	Acquired by	Count
VALUE_IPO_VM_PORTS	0050569F1B93-Primary	2
VALUE_IPO_USR_OFFICE	0050569F1B93-Primary	1
VALUE_IPO_USR_POWER	0050569F1B93-Primary	15
VALUE_IPO_AVAYA_IP_ENDPOINTS	0050569F1B93-Primary	13
VALUE_IPO_SIPTRUNK_CHANNELS	0050569F1B93-Primary	5
VALUE_IPO_TAPICC	0050569F1B93-Primary	1
VALUE_IPO_EDITION_SERVER	0050569F1B93-Primary	1
VALUE_IPO_USR_POWER	0050569FD32C-Expansion01	1
VALUE_IPO_AVAYA_IP_ENDPOINTS	0050569FD32C-Expansion01	1
VALUE_IPO_SIPTRUNK_CHANNELS	0050569FD32C-Expansion01	5
VALUE_IPO_EDITION_SERVER	0050569FD32C-Expansion01	1
VALUE_IPO_EDITION_SERVER	0050569FD718-Secondary	1

## Centralized WebLM Migration Issues

WebLM licensing works differently from Nodal licensing. Depending on how you have your system configured when you migrate to Centralized WebLM licensing, you may need to do some minor re-configuration. Nodal licenses allow you to configure features without actually needing to have the licenses available for these features to work. For example, you could have 50 Power Users configured but only 45 licenses. With Nodal licenses this is allowed, but you wouldn't have all of the users working with all of their features.

WebLM is different in that the number of features that are licensed on your system must have a corresponding license available in the WebLM Server license file. When your system connects for the first time to WebLM, it attempts to acquire all of the licenses in a single block. If there is an issue getting all of the licenses, then the system will not be able to get any licenses at all, even those that you do have enough capacity for. For example, if you have 50 Power Users configured and your license file only had 49 Power Users, then this is enough to stop you from acquiring any licenses. In this scenario, you will see an error when you look at the license configuration in the Manager application. The license mode is showing an error message 'License / License Configuration Error (Check SSA alarms for license errors)'. At this stage the IP Office system is unlicensed.



SSA will provide a better indication of what is causing the issue. Looking at the screenshot below, you can see that the licensing issue is being caused by insufficient licenses being available. The error message at the bottom of the list tells us we have insufficient licenses for our current configuration.

Service Alarms		
Last Date Of Error	Occurrences	Error Description
01/08/2016 16:35:00	4	WebLM Server Error: System not licensed for Select
01/08/2016 16:33:15	1	Attempt to use a feature for which no license is installed. License Type: Avaya Softphone
01/08/2016 16:38:52	4	Attempt to use a feature for which no license is installed. License Type: CTT Link Pro
01/08/2016 16:33:42	1	Failed to load Hold Music source file Source Name: Primary
01/08/2016 16:33:45	1	There are insufficient licenses for this configuration. License Type: Avaya Softphone
01/08/2016 16:33:45	1	SIP Channel License Exceeded: There are insufficient SIP Channel licenses License Type: Maximum SIP Trunk Sessions
01/08/2016 16:33:45	1	There are insufficient licenses for this configuration. License Type: CTT Link Pro
01/08/2016 16:33:45	1	License Configuration Error: There are insufficient licenses for the current configuration

The alarm list also contains some more specific alarms about where the over configuration is. We have issues with CTI, SIP trunk channels, and Avaya Softphone licenses not being available. The license at the top of the list about the system not being licensed for Select is showing because of the other configuration issues there are, and it will clear once the other issues are fixed.

There are two ways to overcome these issues:

- 1) Reconfigure the features configured on your system so that you are not trying to use features that you have no licenses for.
- 2) If you really need these features configured, then you need to purchase the additional licenses and get a new PLDS license file.

After making some changes to the configuration, the alarms about the CTI and SIP trunk channels are now no longer active (showing in Black), but there is still an issue with an Avaya Softphone license that we do not have. This is a common issue that has been seen in trials and is normally caused by a Basic User having the 'Enable Communicator' option ticked.

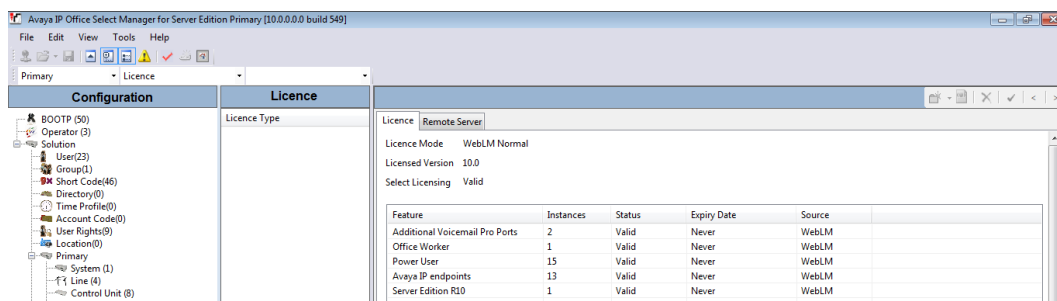
Last Date Of Error	Occurrences	Error Description
01/08/2016 16:47:55	6	WebLM Server Error: System not licensed for Select
01/08/2016 16:33:15	1	Attempt to use a feature for which no license is installed. License Type: Avaya Softphone
01/08/2016 16:47:52	22	Attempt to use a feature for which no license is installed. License Type: CTI Link Pro
01/08/2016 16:33:42	1	Failed to load Hold Music source file Source Name: Primary
01/08/2016 16:33:45	1	There are insufficient licenses for this configuration. License Type: Avaya Softphone
01/08/2016 16:33:45	1	SIP Channel License Exceeded: There are insufficient SIP Channel licenses License Type: Maximum SIP Trunk Sessions
01/08/2016 16:33:45	1	There are insufficient licenses for this configuration. License Type: CTI Link Pro
01/08/2016 16:33:45	1	License Configuration Error: There are insufficient licenses for the current configuration

You can also use the information in Manager > License / License > Remote Server to help you understand what licenses your systems are going to need if you move to Centralized WebLM licensing. Take a look at all of your systems and in the Reserved Licenses section, count up what licenses you are going to need. Make sure that you have sufficient capacity to cover this in your license file before you move over to WebLM Centralized licensing so that you do not get these issues.

Once all of the issues have been resolved, all of the SSA licensing alarms will no longer be active.

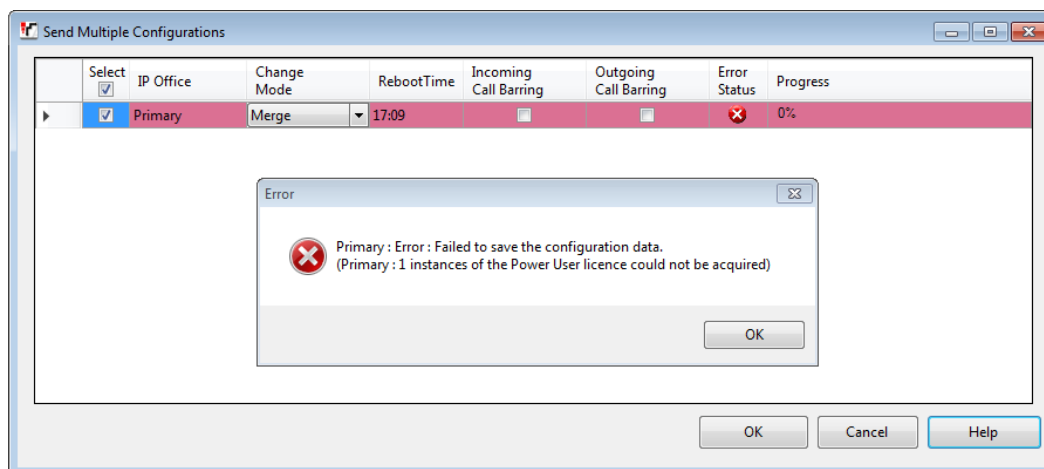
Service Alarms		
Last Date Of Error	Occurrences	Error Description
01/08/2016 16:51:45	7	WebLM Server Error: System not licensed for Select
01/08/2016 16:33:15	1	Attempt to use a feature for which no license is installed. License Type: Avaya Softphone
01/08/2016 17:00:23	47	Attempt to use a feature for which no license is installed. License Type: CTT Link Pro
01/08/2016 16:33:42	1	Failed to load Hold Music source file Source Name: Primary
01/08/2016 16:33:45	1	There are insufficient licenses for this configuration. License Type: Avaya Softphone
01/08/2016 16:33:45	1	SIP Channel License Exceeded: There are insufficient SIP Channel licenses License Type: Maximum SIP Trunk Sessions
01/08/2016 16:33:45	1	There are insufficient licenses for this configuration. License Type: CTT Link Pro
01/08/2016 16:33:45	1	License Configuration Error: There are insufficient licenses for the current configuration

And in Manager, the License / License Mode will show WebLM Normal, and the system will have successfully acquired all of the licenses it needs.



## IP Office Configuration Changes when using Centralized WebLM Licensing

When you have enabled WebLM Centralized Licensing and you want to make configuration changes to your system that will require additional licenses to be consumed, make sure that you check that you have enough license capacity before you start. When running with WebLM, the number of available licenses is checked when a configuration is saved. If the changes to the configuration would cause a licensing error condition, then the Manager application will not allow you to save the configuration and will warn you why you are unable to save the configuration.

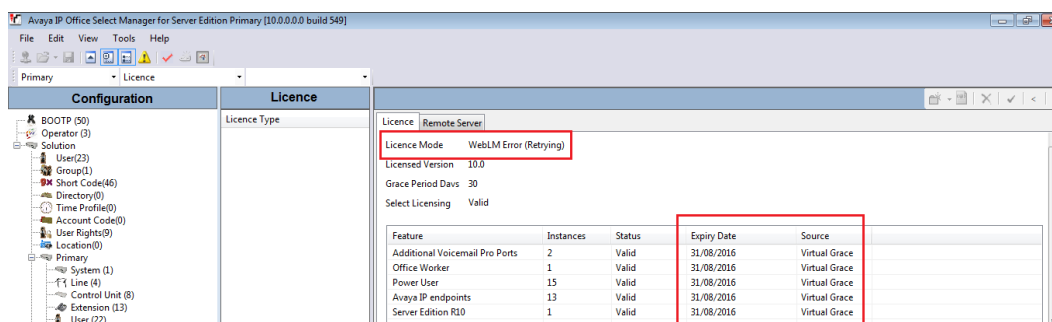


## WebLM License Renewal Period

The IP Office system requests license renewals from the WebLM server every 9 minutes. In the event of a WebLM failure or when making changes to the WebLM configuration, for example if loading an updated WebLM license file, updates might not be seen by the IP Office system immediately. If loading a new license file, it can take around 9 minutes for the new license details to sync up again. If loading a new license file and you need the updates to be applied quicker, triggering “Renew Licenses” from the SSA License page or a reboot of the IP Office systems will force them to re-acquire their license information from the WebLM server.

## WebLM Grace Period

In the event of a WebLM failure, or if a Secondary Server or Expansion system is unable to get license updates, perhaps due to a network outage, then the system will go into a grace period. The grace period will last for a maximum of 30 days, and virtual licenses for all configured features will be available. The number of days left until the grace period expires can be found in Manager and SSA. If the issue that causes the grace period is not resolved in time, the system will enter ‘WebLM Restricted’ mode. All virtual licenses for the previously configured features during the 30-day grace period are deleted, and those features are no longer available. Essentially, the system is now unlicensed.



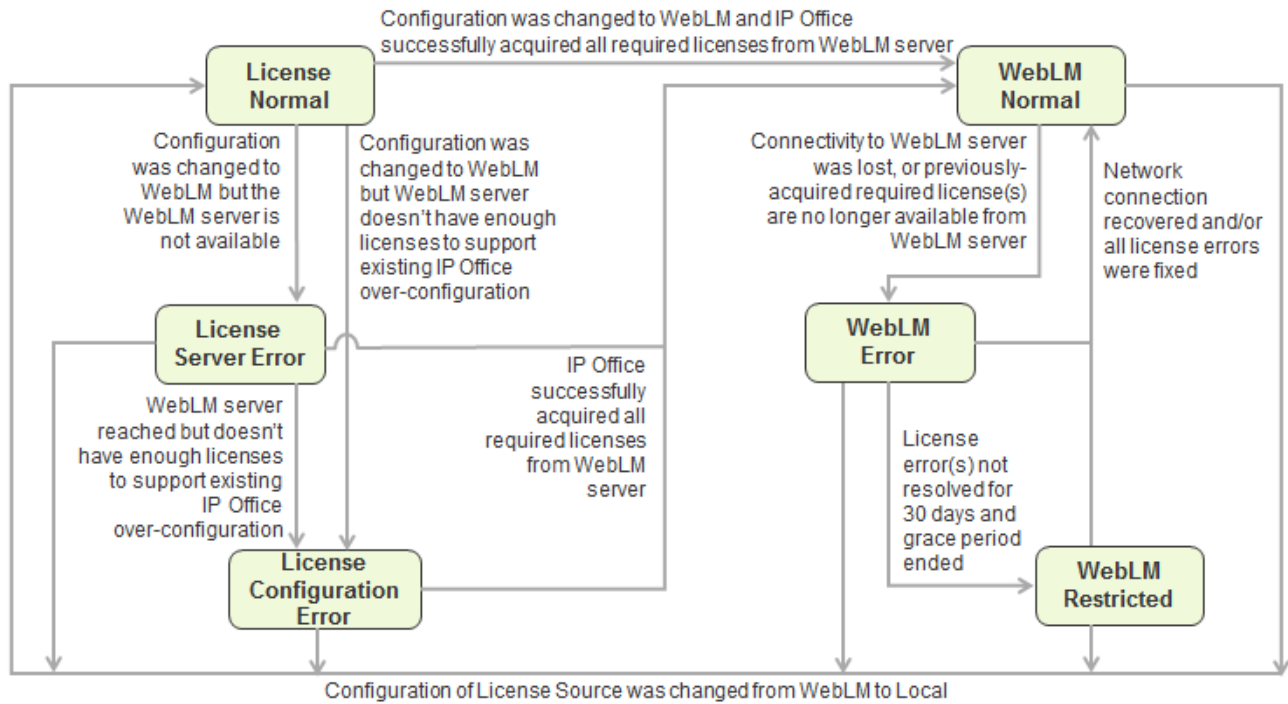
License Type	Available Instances	Number of Licenses in Use	Congestion Count	Last Date of Congestion	Status	Instances	License Expiration Date	Source
Additional Voicemail Pro (ports)	2	0			Virtual	2	31/08/2016	Virtual Grace
Avaya IP Endpoints	13 (13 reserved)	0 (1 reserved)			Virtual	13	31/08/2016	Virtual Grace
Power User	15	15			Virtual	15	31/08/2016	Virtual Grace
Office Worker	1	1			Virtual	1	31/08/2016	Virtual Grace
Server Edition R.10	1	1			Virtual	1	31/08/2016	Virtual Grace

## Summary – License Enforcement Behavior in 10.0

IP Office 10.0 has three different types of license enforcement behavior:

- Traditional Nodal licensing – licenses in local PLDS Nodal license file; Enforcement similar to previous releases that used local ADI licenses:
  - Unlicensed things don't work
  - No grace period
  - Over-configuration of licensed features is allowed
- Centralized WebLM licensing:
  - IP Office won't start WebLM licensing if it's over-configured. It must initially successfully connect to the WebLM server and acquire all the licenses required to support its existing configuration.
  - After WebLM licensing behaviour initiated successfully:
    - Grace period in 'WebLM Error' mode: Configured things keep working for up to 30 days even if licenses are lost. System uses virtual licenses.
    - 'WebLM Restricted' mode if grace period ends without resolution. Virtual licenses are deleted. Unlicensed things don't work.
    - IP Office rejects attempts to over-configure licensed features
- Server Edition legacy Primary SCN based (not WebLM) centralized licensing on Secondary and Expansion systems:
  - Over-configuration of licensed features is not prevented
  - Unlicensed things don't work
  - Grace period for central licenses if connection to Primary is lost
  - Supports hybrid of local Nodal licenses on the Expansion/Secondary and central licenses from the Primary

## WebLM License Modes State Transitions





### Summary - IP Office License Modes

<b>License Normal</b>	WebLM licensing not configured. Traditional Nodal licensing. No grace period. Over-configuration is allowed.
<b>License Server Error</b>	Configuration was changed to WebLM but the WebLM server is not available. No grace period. Until the problem is resolved, IP Office is unlicensed and unusable as in traditional Nodal licensing if no licenses are installed.
<b>License Configuration Error</b>	Configuration was changed to WebLM and the WebLM server is available but it doesn't have enough licenses to support the existing IP Office configuration. No grace period. Until the problem is resolved, IP Office is unlicensed and unusable as in traditional Nodal licensing if no licenses are installed. Licenses must be added to the WebLM license file, or the IP Office configuration must be modified to remove over-configuration.
<b>WebLM Normal</b>	IP Office is configured for WebLM licensing, the WebLM server is available and IP Office successfully acquired all the licenses required to support all of its configured features. New licenses are acquired for new configured features, and over configuration of licensed features is prevented if licenses cannot be acquired. IP Office periodically renews its acquired licenses. Failure to renew will lead to WebLM Error mode with grace period.
<b>WebLM Error</b>	IP Office is configured for WebLM licensing, and was previously in WebLM Normal mode. But IP Office now cannot renew or re-acquire all the licenses required to support all of its configured features. Over configuration of licensed features is prevented if licenses cannot be acquired. IP Office keeps operating for 30-day grace period based on its existing configuration (lost licenses are replaced with virtual grace licenses).
<b>WebLM Restricted</b>	IP Office was in WebLM Error mode but the 30-day grace period has expired and the problems causing the error have not been resolved. Unlicensed features will stop working. (virtual grace licenses are deleted). Any configuration of IP Office is not allowed, except configuration changes that reduce the licensing errors.

## Appendix B - one-X® Portal Resiliency

### Overview

### Scenario

This walk through assumes you already have a Server Edition Primary server working and licensed as “Select”. The following sections will provide you with the basic steps to install the Secondary Server Edition server to host the backup one-X® Portal for resiliency, configure the one-X® Portal settings and the IP Office settings, and provides further information on licensing and certificates. Please refer to the related reference manuals for the full details of these processes.

### Components

- IP Office Server Edition Primary (one-X® Portal - Active)
- IP Office Server Edition Secondary (one-X® Portal - Passive)
- R10.0 Software
- “Select” mode License

### Reference Manuals

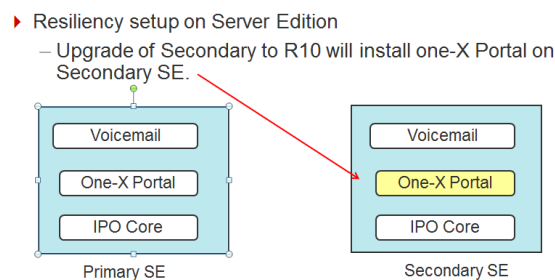
Manual	System Component	Relevant sections and notes
Deploying IP Office Platform Server Edition Solution	Primary and Secondary Server Edition servers	Chapter 4: Provisioning a Server Edition Secondary Server Chapter 12: Configuring Avaya one-X® Portal for IP Office
Administering Avaya IP Office Platform with Manager	IP Office configuration	Chapter 17: Configuring Small Community Networking
Administering Avaya one-X® Portal for IP Office	one-X® Portal service	Configuration Section
Administering Avaya IP Office Platform with Web Manager	one-X® Portal resiliency	Chapter 11: Avaya one-X® Portal resiliency Chapter 11: Configuring Resiliency>Configuring one-X® Portal Resiliency
IP Office Resiliency	one-X® Portal service	Section 6: Configuring one-X® Portal for IP Office Resilience
IP Office Platform 10.0 – IP Office Platform Security Guidelines	Certification	Appendix G – Using the IP Office Certificate Authority
IP Office R10 Offer Document	IP office Solution	Section 5.1.1: one-X® Portal Application Resiliency (overview)

## one-X® Portal Resiliency Setup

### Summary Steps

1. A Secondary Server Edition is required to be added to the Primary Server Select solution. The resilient one-X® Portal is installed automatically.
2. one-X® Portal Administration: All configuration is done on the Primary one-X® Portal Administration. The configuration will be automatically copied and configured onto the Secondary one-X® Portal
3. IP Office Configuration: Configure one-X® Portal Backup on the primary to secondary IP Office line
4. Certificate Deployment: Ensure the correct ID certificate generated on the Primary server is installed on the Secondary server.

#### One-X Portal Resiliency

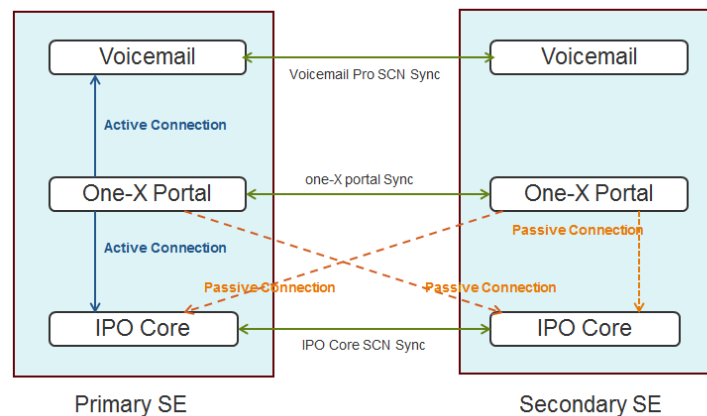


#### Note: Resiliency Terminology

- **Failover** – When service on Primary Server Edition has not started or has stopped, then the service on the Secondary Server Edition becomes active and starts serving clients.
- **Failback** – After failover of the service to secondary Server Edition, when service on the Primary Server Edition comes back, then it becomes active and starts serving clients.
- **Service in Active Mode** – When service is available and allowed to serve clients, it's referred to as it's in Active Mode.
- **Service in Passive Mode** – When service is available and not allowed to serve clients, it's referred to as it's in Passive Mode.

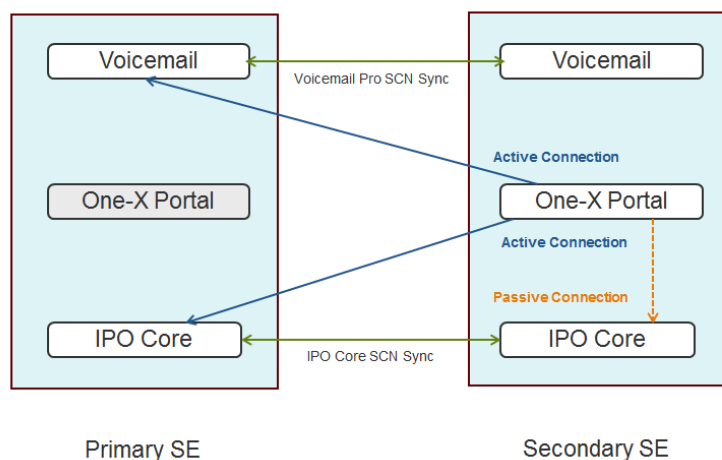
*Note: one-X<sup>®</sup> Portal default connections*

Primary and Secondary one-X<sup>®</sup> Portal services are connected over a synchronized link. They maintain active and passive links to both IP Office services on the Primary and Secondary servers. The passive links become active should any component (one-X<sup>®</sup> Portal or IP Office) become unreachable.



*Note: one-X<sup>®</sup> Portal Primary Fail scenario*

- Users already logged into one-X<sup>®</sup> Portal web client of primary Server Edition will be automatically logged into one-X<sup>®</sup> Portal on the secondary Server Edition.
- one-X<sup>®</sup> Portal UC clients detect that connectivity with Primary one-X<sup>®</sup> Portal is lost and secondary one-X Portal connectivity is available and will auto login to secondary SE one-X<sup>®</sup> Portal
- In case only one-X<sup>®</sup> Portal is Active, then new one-X<sup>®</sup> Portal users should know URL of Secondary SE one-X<sup>®</sup> Portal.

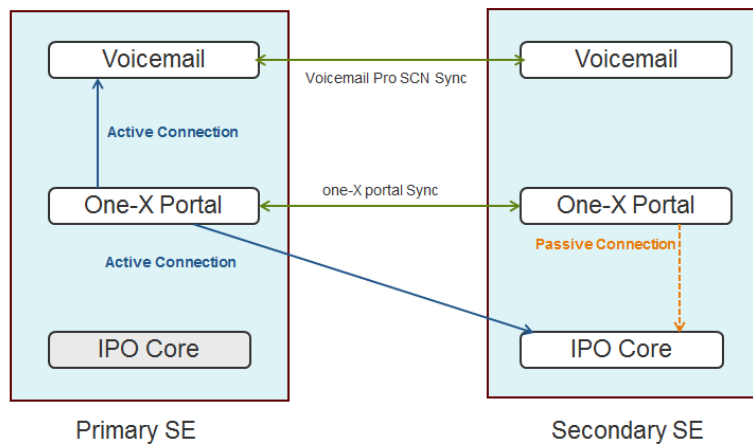


*Note: one-X<sup>®</sup> Portal Secondary Failback scenario*

- Users already logged into the secondary one-X<sup>®</sup> Portal will be automatically logged into Primary SE one-X<sup>®</sup> Portal
- After Failback Recovery, one-X<sup>®</sup> Portal of Secondary SE will not allow user login and will redirect login request to Primary SE one-X<sup>®</sup> Portal

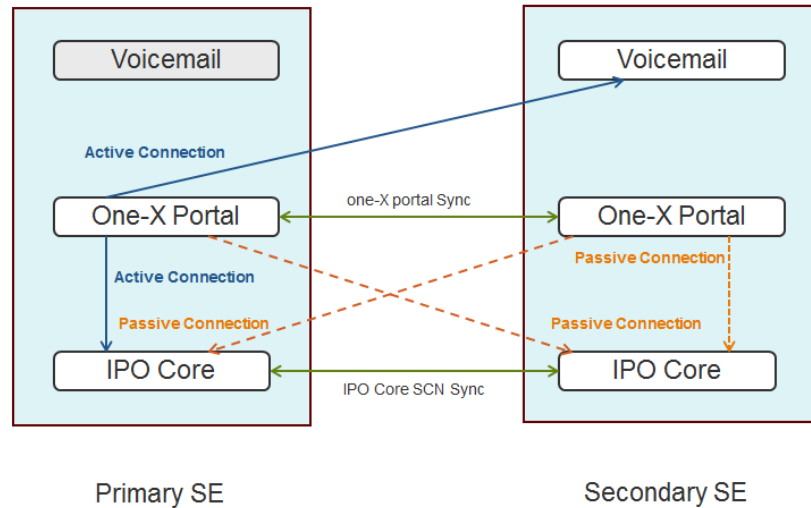
*Note: IP Office Primary Fail scenario*

If the Primary IP Office becomes unreachable, the Primary one-X<sup>®</sup> Portal passive connection to the Secondary IP Office will become active.



*Note: Voicemail Pro Primary Fail scenario*

If the Primary Voicemail Pro becomes unreachable, the Primary one-X® Portal passive connection to the Secondary Voicemail Pro becomes active.



### Step 1: Secondary Server Initialization

1. Assuming you have installed a Primary R10.0 Select Server Edition system already, the next step would be to install the Secondary Server Edition
2. Once the Secondary Server is installed:  
If this is a new installation, you need to go through the Server Edition Ignition process in the same way as the Primary Server, except you will select Secondary in the Ignite process. If you already have a Secondary Server Select, and you have upgraded it to R10.0 or above, skip this section.  
If installing a new Server Edition Secondary server, once the installation has completed, connect to the Secondary Server <https://IP Address or Host Name:7070>, then enter the initial root default password = Administrator  
Click "Agree" > Next  
Select "Secondary (Server Edition)"

## IP Office - Ignition

Accept License ✓

Server Type →

New Hardware

Configure Network

Time & Companding

Change Password

Review Settings

☐ Primary (Server Edition)  
Enables Core, one-X Portal and Voicemail Pro.

☒ Secondary (Server Edition)  
Enables Core, one-X Portal and Voicemail Pro.

☐ Expansion (Server Edition)  
Enables Core only.

☐ Application Server  
Enables one-X Portal and Voicemail Pro.  
Voicemail Pro on the Application Server is not supported in Server Edition.

Configure the required network interface configuration > Next.

## IP Office Server Edition - Ignition

Accept License ✓

Server Type ✓

New Hardware ✓

Configure Network →

Time & Companding

Change Password

Review Settings

Network interface: eth0

Assign IP Address:

Automatic (DHCP) ☐

IP Address: 10.129.116.117

Netmask: 255.255.255.0

Assign System Gateway:

Gateway: 10.129.116.254

Assign System DNS Servers:

Automatic (DHCP) ☐

Primary DNS: 135.124.138.152

Secondary DNS:

Hostname: 0050569F531C

Cancel

Previous

Next

Select the correct Timezone and Companding settings>Next

IP Office Server Edition - Ignition

Accept License ✓

Server Type ✓

New Hardware ✓

Configure Network ✓

Time & Companding →

Change Password

Review Settings

Timezone: Europe/London

Companding: ☒ μ-law ☐ A-law

Cancel Previous Next

Enter new root, Administrator and System passwords>Next (Make a record of the new passwords).



## IP Office Server Edition - Ignition

Accept License ✓

Server Type ✓

New Hardware ✓

Configure Network ✓

Time & Companding ✓

Change Password →

Review Settings

Default account passwords are required to be changed.

**"root" and "security" password**

New Password:

New Password (verify):

[View password policy](#)

**"Administrator" password**

New Password:

New Password (verify):

[View password policy](#)

**"System" password**

New Password:

New Password (verify):

[View password policy](#)

Cancel

Previous

Next

Check and confirm the settings, and click Apply.

Brad Tro...

GMI IPO ...

IP Office™ Pl...

[Gotham ...

IP Office 10.0 ...

IP Office R10...

Ignition x

https://10.129.116.117:7071/setup/

Search

Most Visited

Getting Started

Suggested Sites

Web Slice Gallery

## IP Office Server Edition - Ignition

Accept License ✓

Server Type ✓

New Hardware ✓

Configure Network ✓

Time & Companding ✓

Change Password ✓

Review Settings →

Server Type: Secondary

IP: 10.129.116.117

Netmask: 255.255.255.0

Gateway: 10.129.116.254

Primary DNS: 135.124.138.152

Secondary DNS:

Hostname: 0050569F531C

Timezone: Europe/London

Companding: A-law

Additional Hardware: No new hardware available.

Print

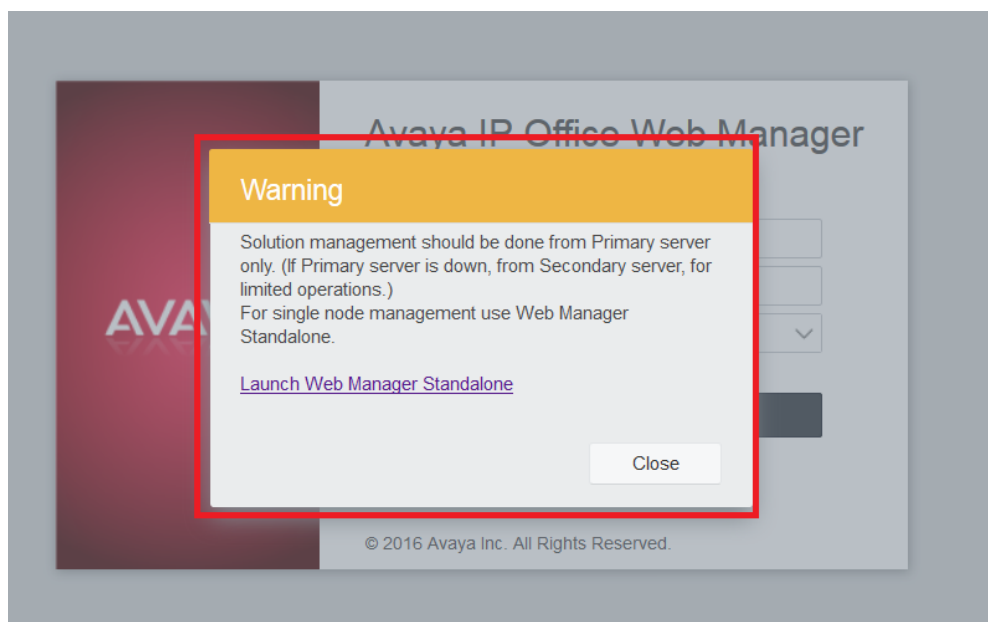
ATTENTION: Prior to ordering licenses for IP Office please confirm the following settings have been finalized: LAN1 and LAN2 IP addresses, Timezone and Hostname. Changing these settings will invalidate any existing licenses. Please see documentation for more detail.

Cancel

Previous

Apply

System will now apply settings and restart the server. This can take between 10 – 20 minutes.

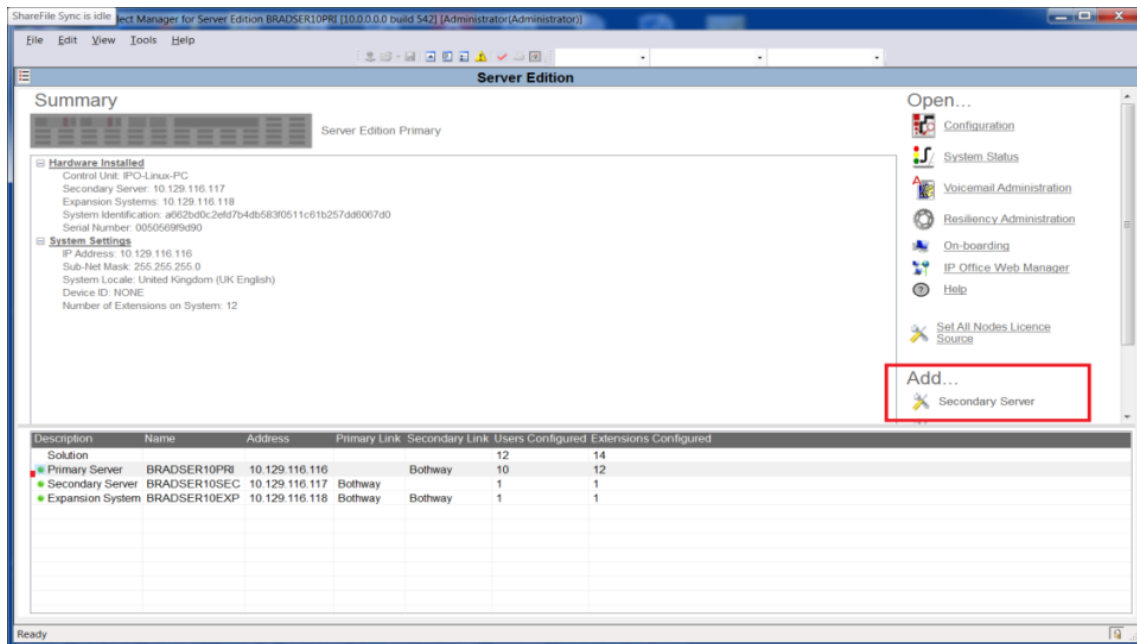


Once the Server is up, refresh your browser and you will get a message displayed. Click “Launch Web Manager Standalone” and log into the Web Manager with the new Administrator account and password set during ignition.

Accept the Google Integration Agreement about Embedded File Server > OK.

You should now see the Dashboard. No further actions are required for now.

“Add” the Secondary server to the Primary. This will automatically create the IP Office lines to the Secondary Server, there should be no need to create the IP office lines manually. This will enable automatic configuration and synchronization between the Primary and Secondary



The Secondary Server will now restart – allow 20 minutes for the server to be fully active.

## Step 2: one-X Portal® Administration

- a. Enabling one-X® Portal Resilience in one-X® Portal Administration
  1. Both primary and secondary portal servers must be set to use Centralized CTi link mode – this is new for R10.
  2. Centralized CTi mode is the default for new R10.0 installations. It must be manually enabled for existing systems that are upgraded from lower versions to R10.0 or higher.
  3. To check and enable Centralized CTi link mode, login to the Primary one-X® Portal's Administration menu. You can do this directly or via Web Manager>Applications.
  4. Select Configuration > Central CTi Link. Systems upgraded from release 9.1 display their original Auto provisioning setting. Click to convert to Central CTi link.

**AVAYA**  
**one-X™ Portal for IP Office**

<b>Health</b>	▶ Providers
<b>Configuration</b>	▶ Users
<a href="#">Providers</a>	▶ CSV
<a href="#">Users</a>	▶ Branding
<a href="#">CSV</a>	▶ IM/Presence Server
<a href="#">Branding</a>	▶ IM/Presence Exchange Service
<a href="#">IM/Presence</a>	▶ SMTP Configuration
<a href="#">Exchange service</a>	▶ Conference Dial-in Information
<a href="#">SMTP Configuration</a>	▶ Resiliency
<a href="#">Conference Dial-in</a>	▶ Host Domain Name
<a href="#">Resiliency</a>	▶ Conference Clean Up
<a href="#">Host Domain Name</a>	▼ Central CTI Link Configuration
<a href="#">Conference Clean Up</a>	Central CTI Link <input checked="" type="checkbox"/>
<b>Security</b>	<input type="button" value="Save"/>
<b>Diagnostics</b>	<b>Description</b>
<b>Directory Integration</b>	<ul style="list-style-type: none"> <li>Centralized Mode is a feature available for IP Office Server Edition pl</li> <li>If Resiliency is configured for one-X Portal the Centralized Mode is er</li> <li>If Application Server is provisioned with IP500 V2 unit, the Centralizer</li> <li>Restart of one-X Portal service is required if Centralized Mode is enal</li> </ul>
<b>Gadgets Configuration</b>	
<b>IM Archive</b>	
<b>Web Conferences</b>	
<b>Help &amp; Support</b>	

5. Check that the CTI link is enabled.
6. Click Save.
7. Navigate to Configuration > Host Domain Name and enter either the Host Domain name or IP Address of the Primary and Secondary Server Edition Servers. Click Save.  
Note: It is preferable to use the Host Domain Names.
8. Navigate to Configuration > Resiliency and configure failover, Failback (auto or Manual), and the Failover Detection Time in minutes.

AVAYA

oneX™ Portal for IP Office

Health

Configuration

Providers

Users

CSV

Branding

IM/Presence

Exchange service

SMTP Configuration

Conference Dial-in

Resiliency

Host Domain Name

Conference Clean Up

Central CTI Link

Security

Diagnostics

Directory Integration

Gadgets Configuration

IM Archive

Web Conferences

Help & Support

Providers

Users

CSV

Branding

IM/Presence Server

IM/Presence Exchange Service

SMTP Configuration

Conference Dial-in Information

Resiliency

Host Domain Name

Primary Host Domain Name	brad-se-r10-pri.avayatrial.com
Secondary Host Domain Name	10.129.116.117
Web Collaboration Domain Name	brad-se-r10-pri.avayatrial.com

**Note:**

- Web Collaboration Domain Name will be used to generate Conference Web Collaboration URL.
- Changes to Domain Name configuration require one-X Portal server restart.

Save

Clear

Refresh

AVAYA

oneX™ Portal for IP Office

Health

Configuration

Providers

Users

CSV

Branding

IM/Presence

Exchange service

SMTP Configuration

Conference Dial-in

Resiliency

Host Domain Name

Conference Clean Up

Central CTI Link

Security

Diagnostics

Directory Integration

Gadgets Configuration

IM Archive

Providers

Users

CSV

Branding

IM/Presence Server

IM/Presence Exchange Service

SMTP Configuration

Conference Dial-in Information

Resiliency

Failover and Failback Controls

Failover	Enabled	<div>Failover Now</div>
Failover Detection Time	3	mins
Failback	Automatic	

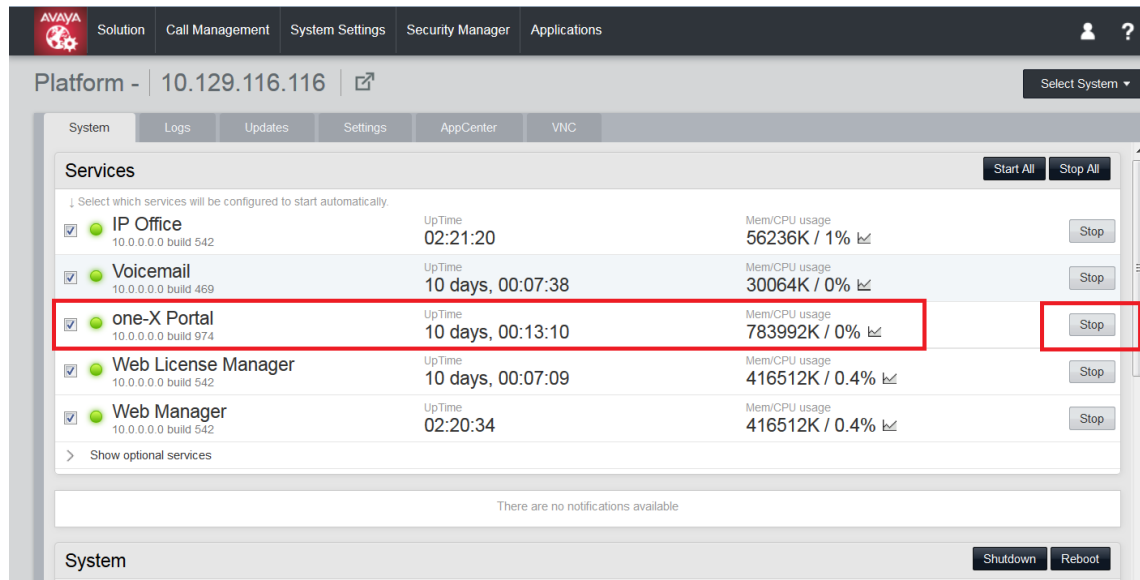
Save

Clear

Refresh

Defaults

- If changes have been made, restart the portal service by clicking the restart icon or going to services in WebManager > Platform View>Services



### Step 3: IP Office Configuration

- Using Web Manager > Secondary Server > Licensing or Manager > Secondary Server > License, configure/check licensing is set as Select and licenses are allocated as required -- either as Nodal licensing (as with 9.1) or utilizing the WebLM server on the Primary (see Technical Bulletin section and manuals for reference). You can select whether to connect directly via IP Address of the Primary, or alternatively utilize the IP Office line acting as a proxy to the primary server/WebLM Server.

#### Notes:

- Utilizing the IP Office line for licensing requires that the IP Office lines are configured as “WebSockets”. Setting them as “Proprietary” does not support connect to WebLM over the IP Office line. If Proprietary IP Office line is selected, you must configure the direct IP Address to the Primary Server and not use the “proxy” option.
- Once the configuration is saved, it can take up to 9 minutes for the Secondary (and expansions) system to obtain licenses from WebLM.
- See the License information below displayed in both WebManager and Manager applications.

Web Manager License Tab

AVAYA

Solution

Call Management

System Settings

Security Manager

Applications

License | BRADSER10SEC

Manage Licenses

Manage Solution-Wide Licenses

Remote Server

Configure License Server

License Source

WebLM

Enable Proxy via Primary IP Office line

YES

Primary IP Address

10 . 129 . 116 . 116

WebLM Client ID

0050569F531C-BRADSER10SEC

RESERVED LICENSES

VMPro Recordings Administrators	VMPro TTS Professional	CTI Link Pro
0	1	0
Voicemail Pro Ports	SIP Trunk Sessions	Avaya Contact Center Select
50	10	0
SM Trunk Sessions	UMS Web Services	Mac Softphones
0	4	0
Third Party Recorder	Server Edition	Avaya IP Endpoints
0	1	1
3rd Party IP Endpoints	Receptionist	Basic User
1	0	0
Office Worker	Power User	Avaya Softphone
0	1	0
Web Collaboration		
0		

Manager Licenses page

File Edit View Tools Help

BRADSER10SEC License

Configuration

License

License Type

License Remote Server

Remote Server Configuration

License Source

WebLM

Enable proxy via Primary IP Office line

☒

Primary IP Address

10 . 129 . 116 . 116

WebLM client ID

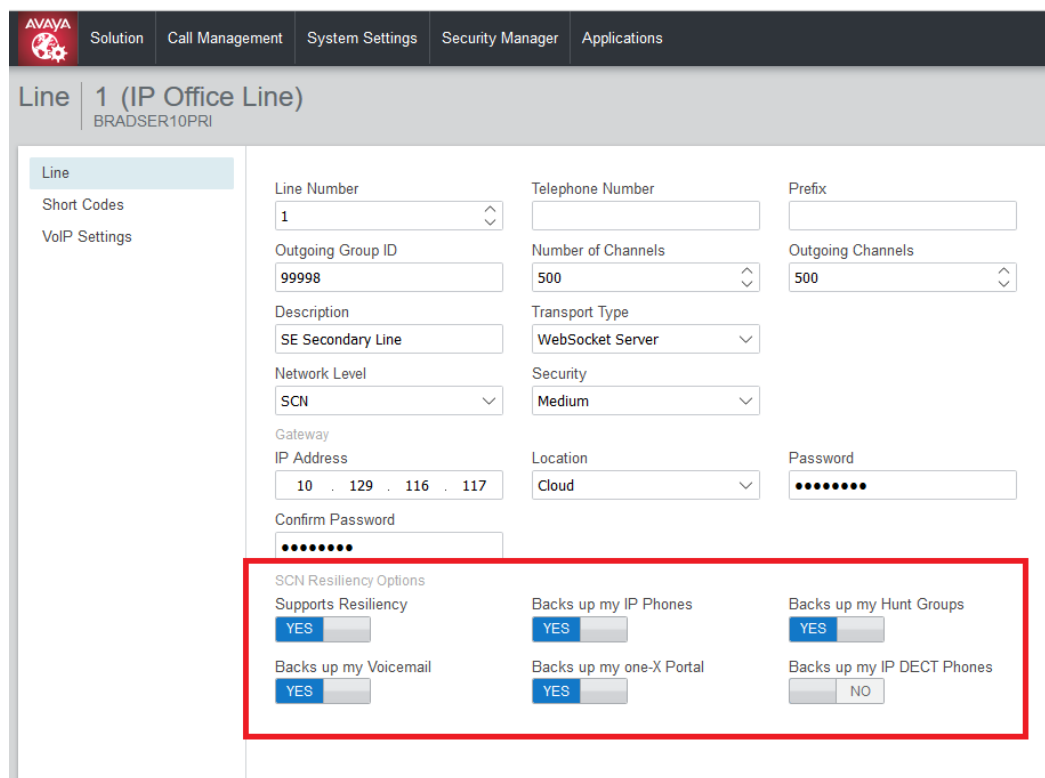
0050569F531C-BRADSER10SEC

Reserved Licenses

SIP Trunk Sessions	10	Server Edition	1
SM Trunk Sessions	0	Avaya IP Endpoints	1
Voicemail Pro Ports	50	3rd Party IP Endpoints	1
VMPro Recordings Administrators	0	Receptionist	0
VMPro TTS Professional	1	Basic User	0
CTI Link Pro	0	Office Worker	0
UMS Web Services	4	Power User	1
Mac Softphones	0	Avaya Softphone	0
Avaya Contact Center Select	0	Web Collaboration	0
Third Party Recorder	0		

- Using Web Manager or IP Office Manager, open the Primary IP Office configuration  
Select the IP Office line to the Secondary, and select Resiliency and “Backs up up my one-X® Portal”. Then save the configuration. This will activate resiliency settings and synchronization between the Primary and Secondary one-X® Portal services.

## Web Manager Line Tab



AVAYA Solution Call Management System Settings Security Manager Applications

Line 1 (IP Office Line)  
BRADSER10PRI

Line  
Short Codes  
VoIP Settings

Line Number: 1  
Telephone Number:   
Prefix:   
Outgoing Group ID: 99998  
Number of Channels: 500  
Outgoing Channels: 500  
Description: SE Secondary Line  
Transport Type: WebSocket Server  
Network Level: SCN  
Security: Medium  
Gateway  
IP Address: 10 . 129 . 116 . 117  
Location: Cloud  
Password:   
Confirm Password:   
SCN Resiliency Options  
Supports Resiliency: YES  
Backs up my IP Phones: YES  
Backs up my Hunt Groups: YES  
Backs up my Voicemail: YES  
Backs up my one-X Portal: YES  
Backs up my IP DECT Phones: NO



## Manager Line form

**IP Office Line - Line 1\***

Line | Short Codes | VoIP Settings

Line Number: 1

Transport Type: WebSocket Server

Networking Level: SCN

Security: Medium

Telephone Number:

Prefix:

Outgoing Group ID: 99998

Number of Channels: 500

Outgoing Channels: 500

Gateway

Address: 10 . 129 . 116 . 117

Location: Cloud

Password:

Confirm Password:

SCN Resiliency Options

- ☒ Supports Resiliency
  - ☒ Backs up my IP phones
  - ☒ Backs up my hunt groups
  - ☒ Backs up my voicemail
  - ☐ Backs up my IP DECT phones
  - ☒ Backs up my one-X Portal

Description: SE Secondary Line

3. Connect to both the Primary and Secondary Server WebManager > Platform View > Services and restart the IP Office and one-X<sup>®</sup> Portal services for both servers.

Primary – Platform View

AVAYA Solution Call Management System Settings Security Manager Applications

Platform - 10.129.116.116

System Logs Updates Settings AppCenter VNC

Services Start All Stop All

Select which services will be configured to start automatically.

<input checked="" type="checkbox"/>	<b>IP Office</b> 10.0.0.0.0 build 542	UpTime 6 days, 00:32:51	Mem/CPU usage 62124K / 6.4%	Stop
<input checked="" type="checkbox"/>	<b>Voicemail</b> 10.0.0.0.0 build 469	UpTime 6 days, 01:19:45	Mem/CPU usage 33980K / 0%	Stop
<input checked="" type="checkbox"/>	<b>one-X Portal</b> 10.0.0.0.0 build 974	UpTime 6 days, 01:23:31	Mem/CPU usage 810140K / 0%	Stop
<input checked="" type="checkbox"/>	<b>Web License Manager</b> 10.0.0.0.0 build 542	UpTime 6 days, 01:19:25	Mem/CPU usage 375500K / 0.4%	Stop
<input checked="" type="checkbox"/>	<b>Web Manager</b> 10.0.0.0.0 build 542	UpTime 6 days, 01:23:09	Mem/CPU usage 375500K / 0.4%	Stop

> Show optional services

There are no notifications available

System Shutdown Reboot

Secondary – Platform View

AVAYA Solution Call Management System Settings Security Manager Applications

Platform - 10.129.116.116

System Logs Updates Settings AppCenter VNC

Services Start All Stop All

Select which services will be configured to start automatically.

<input checked="" type="checkbox"/>	<b>IP Office</b> 10.0.0.0.0 build 542	stopped	Mem/CPU usage 0K / 0%	Start
<input checked="" type="checkbox"/>	<b>Voicemail</b> 10.0.0.0.0 build 469	UpTime 6 days, 01:22:12	Mem/CPU usage 33984K / 0%	Stop
<input checked="" type="checkbox"/>	<b>one-X Portal</b> 10.0.0.0.0 build 974	stopped	Mem/CPU usage 0K / 0%	Start
<input checked="" type="checkbox"/>	<b>Web License Manager</b> 10.0.0.0.0 build 542	UpTime 6 days, 01:21:51	Mem/CPU usage 373352K / 0.4%	Stop
<input checked="" type="checkbox"/>	<b>Web Manager</b> 10.0.0.0.0 build 542	UpTime 6 days, 01:25:35	Mem/CPU usage 373352K / 0.4%	Stop

> Show optional services

There are no notifications available

System Shutdown Reboot

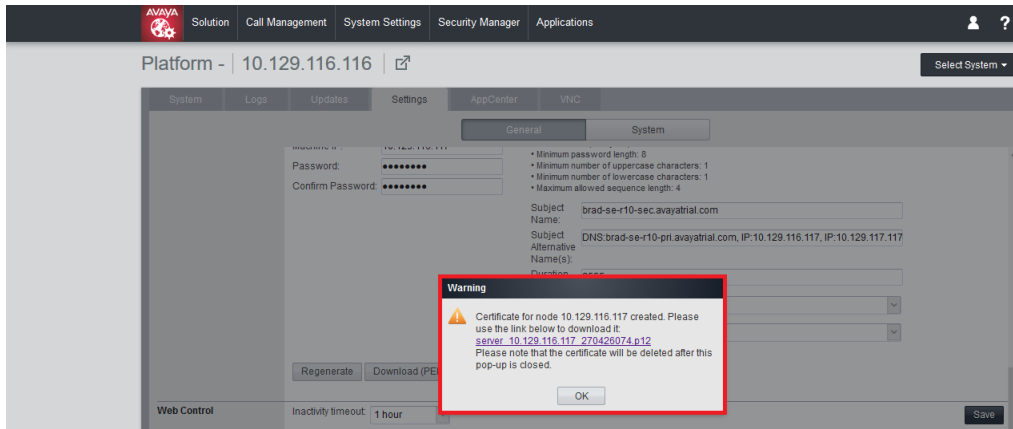
#### Step 4: Certificate Deployment

This is a walk-through to create and install an identity certificate generated from the primary server's root certificate onto the secondary server. Certificate types and scenarios can vary from this example depending on the solution requirements. It is advised that you read the R10.0 IP Office Platform Security Guidelines Manual for a full description of this process with special reference to section 9.7.1 – Generating Identity Certificates for other Devices.

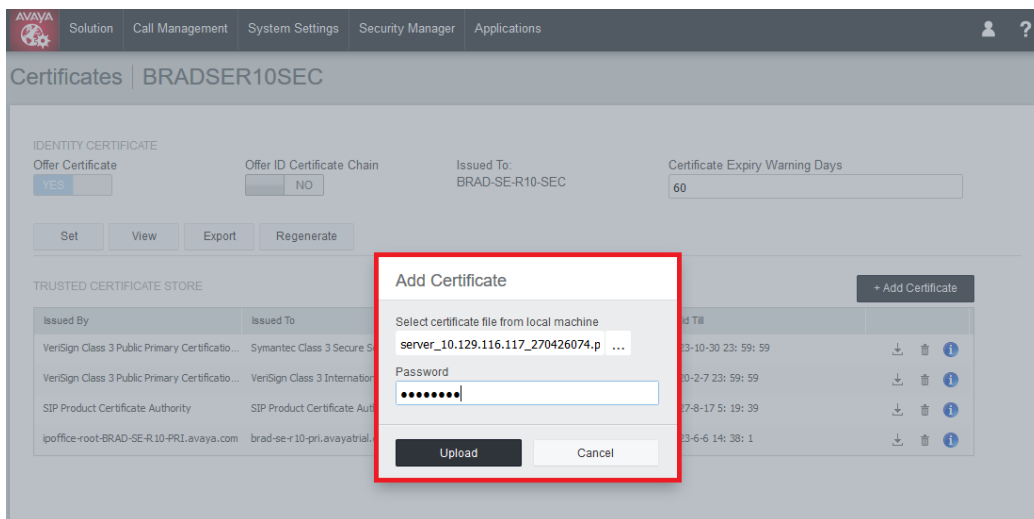
- a) Log into the primary server Web Management > Platform View > Settings
- b) Check: "Create certificate for a different machine"

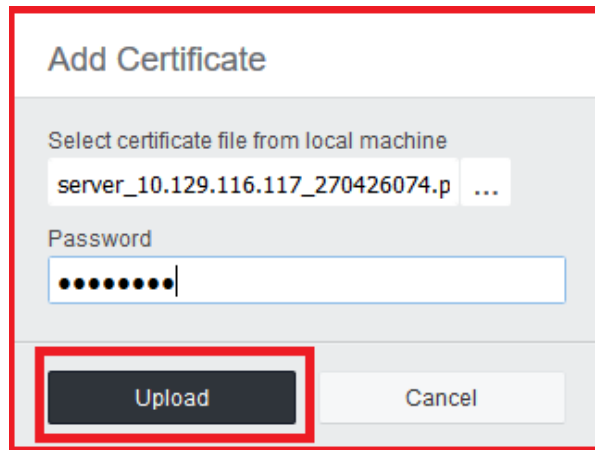
The screenshot shows the Avaya Web Management interface. The top navigation bar includes 'Solution', 'Call Management', 'System Settings', 'Security Manager', and 'Applications'. The main header shows 'Platform - 10.129.116.116'. The left sidebar has tabs for 'System', 'Logs', 'Updates', 'Settings', 'AppCenter', and 'VNC'. The 'Settings' tab is active, and the 'Certificates' section is selected. The 'CA Certificate' section has radio buttons for 'Create new', 'Renew existing' (selected), 'Import', and 'Export'. Below these are buttons for 'Regenerate', 'Download (PEM-encoded)', and 'Download (DER-encoded)'. The 'Identity Certificates' section has a checked box for 'Renew automatically' and a warning message. A red box highlights the 'Create certificate for a different machine' checkbox. Below this, the 'Machine IP' is set to '10.129.116.117', and there are fields for 'Password' and 'Confirm Password'. To the right, there are fields for 'Subject Name' (brad-se-r10-sec.avayaatrial.com), 'Subject Alternative Name(s)' (yatrial.com, IP:10.129.116.116, IP:10.129.117.116, SIP-URI:brad-se-r10-pri), 'Duration (days)' (2555), 'Public Key Algorithm' (RSA-2048), and 'Secure Hash Algorithm' (SHA-256). A red box highlights the 'Regenerate' button at the bottom left.

- c) Enter the IP Address of the secondary server, a certificate password and make any other changes required. Check the R10.0 IP Office Platform Security Guidelines manual for further information.
- d) Click on "Regenerate".



- e) You will see a popup message allowing you to download the new PKCS#12 certificate for the secondary server using the link. Save the file to your local machine.
- f) In WebManagement, select Platform View > Certificates for the secondary server.
- g) Set "Offer Certificate" to "Yes", then Click "Set".
- h) A popup appears – browse and select the PKCS#12 Identity certificate, enter the password previously configured in Platform View.
- i) Click "Upload".





**Configuration of one-X<sup>®</sup> Portal resiliency solution is complete.**

## **Hints and Tips**

### ***How do clients work?***

one-X<sup>®</sup> Portal resiliency enables the following clients to fallback to the secondary one-X<sup>®</sup> Portal when the primary portal is unreachable. In all cases, you only need to configure the primary server. The fallback (secondary) server FQDN/IP Address is sent to the client on login:

- one-X<sup>®</sup> Portal client
- Avaya Communicator for Windows
- Avaya one-X<sup>®</sup> Mobile Preferred for IP Office – iOS
- Avaya one-X<sup>®</sup> Mobile Preferred for IP Office - Android
- Avaya IP Office Plug-In for Microsoft<sup>®</sup> Outlook
- Avaya one-X Call Assistant
- IP Office Soft Console

### ***How does the one-X<sup>®</sup> Portal Client Fallback to secondary one-X<sup>®</sup> Portal?***

When the primary portal service goes down, one-X<sup>®</sup> Portal client will detect the server is unreachable and will connect to the secondary one-X<sup>®</sup> Portal. This is not an immediate fallback. The resilience settings in one-X<sup>®</sup> Portal administration provide a wait in case of simple network outages etc.

Browser tabs: IP Office..., IP Office..., Function..., Shared D..., Index of /mnt..., IP Office R10..., Gotham..., [I]POFFIC..., [Brad Bu..., one..., Avaya IP...

Address bar: <https://brad-se-r10-pri.avayatrial.com:9443/onexportal.html>

Page Title: **AVAYA** onex Portal for IP Office

Navigation: Office | **Brad SE Server** | BTrower(1001) | Available | Help | Logout | Version: 10.0.0.0.0 build 980

Menu: Main | Configure | Add tab

**Calls**

Enter a name or number

1 2 3 4

Drop Hold Record Mute Conference

**Directory**

Personal System External Search All

All Outlook + Add group

Enter a name or number

**Messages (New: 6, Total: 6)**

Phone Enter a name or number

State	From	Time	
	MGibson (1002)	Jul 19, 2016 3:04 PM	11 s
	MGibson (1002)	Jul 19, 2016 3:04 PM	17 s
	MGibson (1002)	Jul 19, 2016 3:00 PM	6 s

Save Delete Page 1 of 1

**Conference Scheduling**

Meetings View Calendar View Schedule a Conference

Search meetings Search Clear New Historic All Host Invite Recurring

Subject	Bridge Details	Date	Start Time	End Time
You have no scheduled conferences.				

**Conversation History**

All Calls Incoming Outgoing Missed IM

Type	Name	Time	Length	Calls
	BTrower (1001)	Jul 25, 2016 2:34 PM	19 s	9
	MGibson (1002)	Jul 25, 2016 2:34 PM	46 s	43
	MGibson (1002)	Jul 25, 2016 2:10 PM	53 s	5

Clear Log

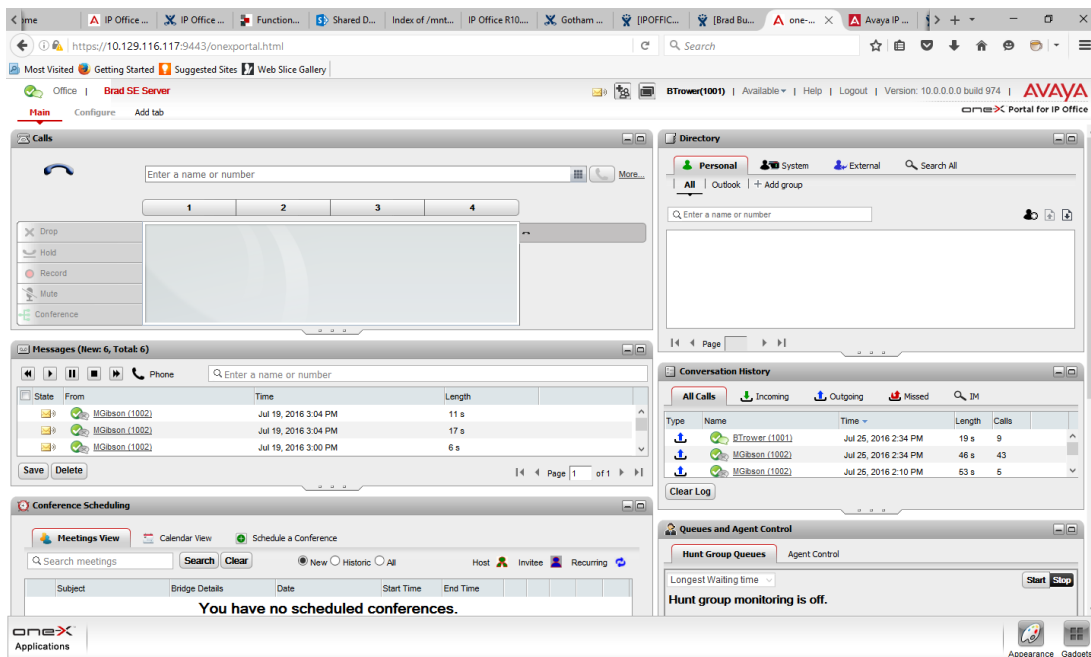
**Queues and Agent Control**

Hunt Group Queues Agent Control

Longest Waiting time Start Stop

Hunt group monitoring is off.

onex Applications Appearance Gadgets



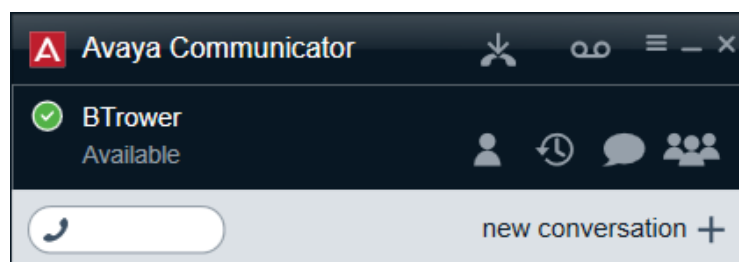
## How does the Avaya Communicator for Windows Fallback to the secondary one-X® Portal?

Avaya Communicator for Windows displays the status of its portal presence connection by showing the green tick icon next to the User name.

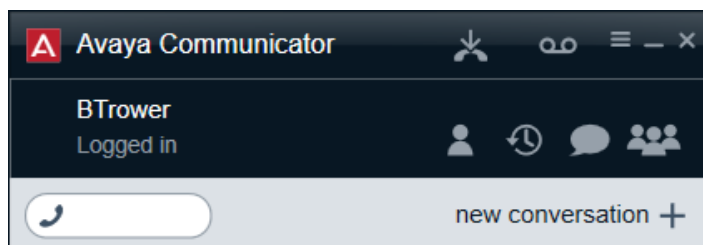
When the primary portal is unreachable, the Communicator stays logged in to the primary IP Office, and will then connect to the secondary portal automatically and display the green presence icon again.

Once the primary portal is again reachable, the Communicator can automatically reconnect

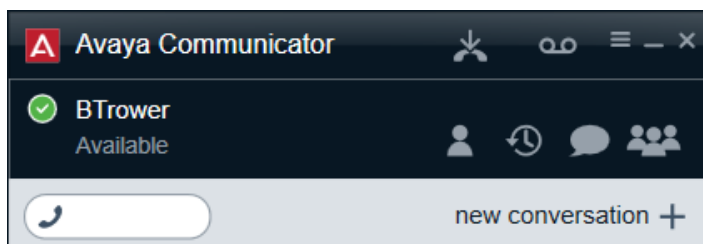
*Primary one-X® Portal connected*



*Primary one-X® Portal is down/unreachable, presence icon disappears*



*Communicator is connected to the secondary portal, presence icon is restored.*





### What should the one-X® Portal Status look like?

To view one-X® Portal resiliency status, the one-X® Portal Administration > Health > Resiliency table displays the state of the connections from one-X® Portal to the various services.

In the example below, the primary portal service has stopped for some reason. You can see that the primary one-X® Portal connection is “Stopped” and the secondary one-X® Portal is “Started”.

AVAYA

one-X™ Portal for IP Office

Health

[Dashboard](#)

[Component Status](#)

[IM/Presence Server Status](#)

[Resiliency](#)

[Key Recent Events](#)

[Active Sessions](#)

[Environment](#)

Configuration

Security

Diagnostics

Directory Integration

Gadgets Configuration

IM Archive

Web Conferences

Help & Support

► Dashboard

► Component Status

► IM/Presence Server Status

▼ Resiliency

Resiliency Component	FQDN / IP Address	Status
Primary one-X Portal	brad-se-r10-pri.avayatrial.com	Stopped
Secondary one-X Portal	10.129.116.117	Started
Primary IP Office Connection	10.129.116.116	Connected Active
Secondary IP Office Connection	10.129.116.117	Connected Passive
Primary DB State	-	Stopped
Secondary DB State	-	Started Active

Refresh

► Key Recent Events

► Active Sessions

► Environment

# **one-X™ Portal for IP Office**

---

**Health**

- [Dashboard](#)
- [Component Status](#)
- [IM/Presence Server Status](#)
- [Resiliency](#)
- [Key Recent Events](#)
- [Active Sessions](#)
- [Environment](#)

**Configuration**

**Security**

**Diagnostics**

**Directory Integration**

**Gadgets Configuration**

**IM Archive**

**Web Conferences**

**Help & Support**

- ▶ Dashboard
- ▶ Component Status
- ▶ IM/Presence Server Status
- ▼ Resiliency
 

Resiliency Component	FQDN / IP Address	Status
Primary one-X Portal	brad-se-r10-pri.avayatrial.com	Started
Secondary one-X Portal	10.129.116.117	Started
Primary IP Office Connection	10.129.116.116	Failed Passive
Secondary IP Office Connection	10.129.116.117	Connected Active
Primary DB State	-	Started Active
Secondary DB State	-	Started Passive

- ▶ Key Recent Events
- ▶ Active Sessions
- ▶ Environment

- one-X® Portal Administration for IP Office Manual
- IP Office Resilience Manual