IP Office Technical Bulletin

Bulletin no: **175**

Date: December 22, 2014

Title: General Availability (GA) of IP Office Release 9.1

Table of Contents

IP Office Technical Bulletin

Bulletin No: **175**

Date: **December 22, 2014**

Region: **GLOBAL**

General Availability (GA) of IP Office R9.1

1.1 Overview

Avaya is pleased to announce the general availability of IP Office Release 9.1 software.

With the IP Office 9.1 release Avaya continues its focus on strengthening the position of IP Office (IPO) as a market leader within the SME, Mid-Market, and Branch market segments as well as to augment the key differentiating competitive attributes that the IP Office product line offers.

IP Office R9.1 contains new and innovative features that enhance the user experience and user productivity, and simplify deployment, configuration, and management of the IP Office product.

The major themes that the IP Office R9.1 release focuses on are:

- Premium product offering
  - IP Office “Select” (SE platform)
- IP Office Server Edition Enhancements
  - System Expansions
  - IP Office Resiliency
- IP Office when deployed as a Branch Enhancements
  - Aura® Avaya Aura System Manager for IP Office and Central Management
  - Aura® Centralized Applications, Services and Solutions
  - Branch VM Pro and Centralized Management
- IP Office Unified Communications and Video
  - Mobile VoIP Client Enhancements
  - Lync Plugin Evolution
  - Exchange 2013 Integration
  - Avaya Communicator (Flare) enhancements
- IP Office Key Features
  - New System Capacity Expansion
  - SIP service provider SIP trunk features
  - SSL/VPN remote access and continued IPOSS support improvements.
  - Communications accessibility solutions

    - Call Center enhancements
- IP Office Web Manager Evolution
    - Expanded integration of management capabilities
    - Continued simplification
    - Server Edition and Standard Editions
- Call Center Enhancements
- IP Office Security Enhancements
    - TLS and SRTP support for all SIP traffic
    - Encryption of all H.323 traffic via Line, Trunk, and SCN

This Technical Bulletin announces the release and provides technical details not covered by other documents in the IP Office documentation library. Other documents that detail new features are the IP Office 9.1 Product Update and the 'IP Office Release 9.1 deployed as a Branch Product Offer' documents.

2 IP Office Platform, Offerings, and Version Details

2.1 Platform Support and Platform Features

IP Office R9.1 supports the following platforms:

- IP500 V2
- Server Edition - IP Office for Linux
- Virtualized IP Office - IP Office for Linux

As of the IP Office 9.1 release, the IP500 (non V2) platform is no longer supported.

Just as with previous IP Office releases, there is a selection of IP Office options that are only supported on the IP500 V2 platform (i.e., not on Server Edition or Virtualized IP Office).

	IP500 V2	Server Edition
Basic Edition – PARTNER® Mode	✓	X
Basic Edition – Norstar™ Mode	✓	X
Combination cards	✓	X
SD cards	✓	X
Essential Edition additional ports license	✓	X
Norstar™/BCM Digital phones on IP Office	✓	X
TCM8	✓	X
DS16A/DS30A and DS16B/DS30B	✓	X
Unified Communications Module (UCM)	✓	X
SSL/VPN	✓	✓
On-Boarding Automation	✓	✓
SSL/VPN NAPT	✓	✓
IP Office Web Manager	✓	✓

The following features can be used only when IP Office 500V2 is deployed in Branch mode and are not supported on Server Edition:

- Centralized management through Avaya Aura® System Manager
- Centralized licensing through Avaya WebLM
- Centralized users
- Centralized Avaya Aura® applications and services (for example: centralized voice mail)

  Note: With the release of IP Office R9.1 Avaya no longer provide support for R8.1 software.

2.2 IP Office Select

On the Server Edition platform, IP Office R9.1 provides a new “Select” offering which complements the delivery of the R9.1 “Standard” offering.

The IP Office R9.1 Standard offering continues to address the needs of the market segment currently served by IP Office R9.0.

The IP Office Select offering enables access to an additional set of content/features delivered in IP Office R9.1. This additional content is designated as a Select only content/feature set. Availability of Select content/features on an installation is controlled via licensing.

The Select feature/content is available only on the IP Office Server Edition platform. It is not available on the 500V2 platform.

A comparison of content and features for IP Office R9.1 Select vs. Standard follows (again, for R9.1, Select options are available on the SE platform only):

	IP Office R9.1 Select	**IP Office R9.1 (Standard)**
Scalability		
SE capacity - max 2,500 users (up from 2,000)	**Yes**	N/A
SE capacity on single server - max 2,500 users (up from 1,500)	**Yes**	N/A
SE nodes - max 150 (up from 32)	**Yes**	N/A
SE 1,000 UC (up from 750)	**Yes**	N/A
SE VM Pro scalability to 250 ports (up from 150)	**Yes**	N/A
SE VM Dual Active to 500 ports	**Yes**	N/A
SE Hunt Groups - max 500 (up from 300)	**Yes**	N/A
SE Conference ports – max 512 (up from 256)	**Yes**	N/A
SE SIP channels per node – max 1024 (up from 512)	**Yes**	N/A
SE SCN channels per trunk – max 500 (up from 250)	**Yes**	N/A
SE Soft Consoles – max 50 (up from 32)	**Yes**	N/A
BHCC – max 20,000 (up from 18,000)	**Yes**	N/A
Resiliency		
Improved SE resiliency	**Yes**	N/A
SE resiliency to expansion (500V2)	**Yes**	N/A
SE VMWare HA	**Yes**	N/A
Remote Worker phone resiliency	**Yes**	**Yes**
DECT 4 resiliency	**Yes**	**Yes**
Security		
TLS/SRTP	**Yes**	**Yes**
H.323 encryption	**Yes**	**Yes**
Strengthened security / hacking prevention	**Yes**	**Yes**
New Capabilities	**Yes**	**Yes**
Integration with LDAP and Active Directory	**Yes**	N/A
Web Collaboration	**Yes**	**Yes**
ACCS Integration	**Yes**	**Yes**
Conference Scheduling and port reservation	**Yes**	**Yes**
Voice Quality Monitoring (Ph 1)	**Yes**	**Yes**

2.3 IP Office R9.1 Software Versions

The following component versions comprise the parts of the complete IP Office R9.1 Release.

Component	Version
Admin CD	9.1.0.0 build 437
VMPro	9.1.0.0 build 166
One-X Portal	9.1.0.0 build 306
Server Edition DVD	9.1.0.0 build 437
Server Edition OVA	9.1.0.0 build 437
Unified Communication Module	9.1.0.0 build 437
SoftConsole	9.1.0.0 build 146
Avaya Communicator for Windows	2.0.3.29
Avaya Communicator for iPad	2.0.4.2 build 25
Avaya Aura System Manager for IP Office	6.3.11 GA + Latest Patch from Avaya Support Site
Contact Recorder	9.1.0.0 build 3
IPOffice Contact Center (IPOCC)	9.1.0.1900
Avaya Contact Center Select (ACCS)	ACCS-6.4-FP2
Radvision XT5000	8.3
Avaya one-X Mobile Preferred for IP Office (Android version)	9.0.9821
Avaya one-X® Mobile Preferred for IP Office (iOS version)	3.0.2

Module	Version
POTSV2 Module	9.1.0.0 build 437
DCPV2 Module	9.1.0.0 build 437
ATM Module	9.1.0.0 build 437
DS30/16 V2 Module	9.1.0.0 build 437
DS30A/16A BST Module	9.1.0.0 build 437
DS30B/16B Module	9.1.0.0 build 437

2.4 Release Documentation

The latest versions of detailed release information can be found in the following documents available with the Avaya IP Office R9.1 software pack available on DVD media or downloadable from support.avaya.com

- Product Description (Release 9.1)
- 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
- IP Office Documentation Library roadmap document - Describes the organization of all IP Office documents and indicates the type of information in each document

The Release 9.1 Documentation will be available by GA:

- Go to support.avaya.com
- Select Find Documentation and Technical Information by Product Name under Downloads & Documents
- Enter ‘IP Office’ as your product
- Choose ‘9.1’ as your release

- Click the ‘Documents’ radio button
- Click ‘Enter’ to see all documentation

The latest version of the IP Office Product Description Document, which defines the IP Office product in more detail, is found on the Avaya Partner Portal (www.avaya.com/salesportal) and will require a valid Single Sign On (SSO) user name and password to view it online.

For the latest version of the IP Office 9.1 Product Update document, which is a communication that summarizes “what’s new” within the IP Office Release 9.1 product, can be found on the Avaya Partner Portal at the following: https://sales.avaya.com/cs/Sites?lookuphost=/&lookuppage=/en/pss/ip-office-release-9.1-sales-toolkit

For the latest version of the IP Office Release 9.1 deployed as a Branch Product Offer, which defines the branch solutions, commercial tools, licensing and migration/upgrade scenarios in more detail, can also to be found on the Avaya Partner Portal at the following: https://avaya.my.salesforce.com/apex/sp_ViewDetailPage?c=a3da0000000LOquAAG&Id=a3ja0000000LZI4AAO Refer to “Branch Training Materials & Collateral” section.

Refer to the appropriate Avaya website(s) for the latest version of product documentation.

3 IP Office R9.1 Main Enhancements

Refer to the Release Documentation section above for details to download the IP Office Release 9.1 Product Update document and the IP Office Release 9.1 deployed as a Branch Product Office which provide details about the following new main enhancements:

- Cloud/Hosted IPO and IPOCC Security Enhancements
- Mid Market
  - Scalability to 2500 users
  - Scalability to 150 sites
  - 100% UC for all 2500 users
  - Resiliency improvements
  - VM Ware HA
- Branch – Enhanced Centralized Management and new Aura Solutions
  - Enhancements for Aura System Manager
  - Additional Aura Centralized Applications, Services, and Solutions
- Contact Center – Mid-Market improvements
  - Expand addressable market
  - IPOCC 250 agents, single server
- UC/Video
  - Web Collaboration
  - IP Office Video Softphone Receptionist Console NAT
  - Avaya Communicator
  - Lync Plug-In
  - Mobility Enhancements
  - Meet-Me Conference Scheduling with port reservation
- Web Management – Continued Evolution to a single management tool
  - Expanded set of management capabilities
  - Improved performance and user experience
  - End-User management
  - Accessibility (508) for Day 2 admin
- New Key Features – contributing to enabling full UC
  - UCM V2
  - DECT R4 resiliency
  - SIP trunk enhancements
  - SSL/VPN remote access and IPOSS improvements
  - Voice quality monitoring
  - 52 GRIP enhancement requests completed
- Security
  - TLS and SRTP support for IP endpoints
  - Encryption of all H.323 traffic via Line, Trunk, and SCN
  - Security Enhancements to combat attacks & hacking/cracking attempts

4 Phone Support

Refer to the Release Documentation section to download the IP Office Release 9.1 Product Update document which provides phone support details. For details on supported phones as related to Centralized users within an IP Office deployed as a branch solution, please download the IP Office Release 9.1 deployed as a Branch Product Offer document.

4.1 New Phone Models

There following phone models are new supported phones on IP Office.

- SIP phone models
  - Avaya B179 Conference Phone
  - Avaya E129 Deskphone

4.2 Phone Firmware Support

The detail below lists the phone firmware versions that are supported by IP Office Release 9.1.

Phone Model	Version
4600/5600 H.323 Phone Firmware (Common Boot Code and App)	
4610SW, 4620SW, 4621SW, 5610SW, 5620SW & 5621SW	2.9.1 (2.9 SP1)
4625	2.9.1 (2.9 SP1)
4620 (Not 4620SW)	2.3
4601, 4602D, 4602SW, 5601, 5602D & 5602SW	2.3
4601+, 4602+, 5601+ & 5602+	2.9.1 (2.9 SP1)
4600/5600 H.323 Phone Firmware (Common Boot Code and App)	
4610SW, 4620SW, 4621SW, 5610SW, 5620SW & 5621SW Boot Code	2.3.252
4610SW, 4620SW, 4621SW, 5610SW, 5620SW & 5621SW App	2.3.252
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	1.360A
1603-L & 1608-L & 1616-L App	1.360A
1616 Button Module 32 App	1.1.0
1600 Phone Language Files	69
9600 H.323 Phone Firmware (Separate Boot Code and App)	
9620 & 9630 & 9640 & 9650 Boot Code	3.2.2
9620 & 9630 & 9640 & 9650 Application	3.2.2
9620D01A & 9630D01A Boot Code	3.2.2
9620D01A & 9630D01A Application	3.2.2
9600 Phone Language Files	76
96x1 H.323 Phone Firmware (Separate Kernel and App)	
9608 & 9611 & 9621 & 9641 Kernel	S96x1_UKR_V22r11_V22r11
9608 & 9611 Application	S9608_11HALBR6_4_0_14_V452
9621 & 9641 Application	S9621_41HALBR6_4_0_14_V452
96x1 Phone Language Files	87
11x0 & 12x0 SIP Phone Firmware	
1120	04.04.18.00
1140	04.04.18.00
12x0	04.04.18.00
B179 Firmware	
B179	2.4.0.8
DECT D100 Firmware	
D100_BS_MS	1.2.1
D100_BS_SL	0.9.6
E129 Firmware	
E129	1.25.1.1
DCP Phone Firmware	

2410	R6
2420	R6
5410	R6
5420	R6
1403 Application	Application R07
1403 Boot	Boot 03
1408 Application	Application R40
1408 Boot	Boot 25
1416 Application	Application R40
1416 Boot	Boot 25
9500 Application	Application R55
9500 Boot	Boot R15
9500 Zarlink	Zarlink R0_09
DCP Phone Languages	
14xx	R10_v11_Pack01
DCP Phone Font Files	
14xx Chinese (GB)	R02_v01
14xx Korean (KSC)	R02_v01
14xx Japanese (JIS)	R02_v01
IP DECT Phone Firmware/Tools	
Avaya 3701	22.04.04
Avaya 3711	91.24.31.04
Avaya 3711 Global	91.24.36
Avaya 3711 USB Driver	0.8
IP DECT ADMM Firmware/Tools	
IP DECT - ADMM Firmware	1.1.13
IP DECT - ADMM Java Configuration	1.1.13
IP DECT - ADMM DECT Monitor	1.4
DECT R4 Phone Firmware/Tools	
Avaya 3720	4.3.3
Avaya 3725	4.3.3
Avaya 3740	4.3.3
Avaya 3749	4.3.3
Avaya 3720 Template	0.4
Avaya 3725 Template	0.4
Avaya 3740 Template	0.1
Avaya 3749 Template	0.1
DECT R4 Firmware/Tools	
DECT R4 - IPBS1 Boot Firmware	7.2.7
DECT R4 - IPBS1 Firmware	7.2.7
DECT R4 - IPBS1 Downgrade Firmware	7.1.2
DECT R4 - IPBS2 Boot Firmware	7.2.7
DECT R4 - IPBS2 Firmware	7.2.7
DECT R4 – IPBS2 Downgrade Firmware	7.1.2
DECT R4 - IPBL (DECT Gateway) Boot Firmware	7.2.7
DECT R4 - IPBL (DECT Gateway) Firmware	7.2.7
DECT R4 - IPBL (DECT Gateway) Downgrade Firmware	7.1.2
DECT R4 - GRBS (ISDN RFP) Firmware	R7C 3/40
DECT R4 - GRBS-DB1 (ISDN RFP) Firmware	R3B 3/80
DECT R4 - AIWS Firmware	2.73
DECT R4 - AIWS2 Firmware	3.70-A
DECT R4 - WinPDM (Windows Portable Device Manager)	3.11.0
DECT R4 - Rack Charger Firmware	1.5.1
DECT R4 - Advanced Charger Firmware	1.5.1
DECT R4 - Avaya 3720 Translation Tool	26
DECT R4 - Avaya 3725/3740/3749 Translation Tool	31
DECT R4 - Avaya 3720 Downloadable Languages	26
DECT R4 - Avaya 3725/3740/3749 Downloadable Languages	31
DECT R4 - Company Phonebook Tool	9
DECT R4 - Local Phonebook Tool	1
Wi-Fi Phone Firmware/Tools	
3641/3645	117.058
HAT	4.1.4
AVPP	17x.040

T3 IP Phone Firmware/Tools	
T3 IP Phone Firmware	T247
T3 IP Admin Tool	3.08

For details on supported phones as related to Centralized users within an IP Office deployed as a branch solution, please download the IP Office Release 9.1 deployed as a Branch Product Offer document.

5 Upgrading

5.1 Upgrading IP Office IP500v2 core software

When upgrading to Release 9.1 from a previous release an upgrade license is required. It is recommended that the IP Office Release 9.1 Software Upgrade license is installed before upgrading the system. Although the license key may not be recognized immediately by the system running an earlier major release of software, it will be recognized when the system is upgraded to Release 9.1.

Note: An IP Office 8.0 system with Essential Edition functioning but not enabled with the required Essential Edition license key will have all telephony functionality disabled after the 9.1 upgrade. It is important to verify the license information prior to upgrading. If Essential Edition is not visible in the license summary, an Essential Edition license must be purchased and installed prior to attempting the 9.1 upgrade.

This table shows the necessary steps that must be taken to upgrade the IP Office system unit to Release 9.1:

Platform	Current Release	Upgrade Step 1	Upgrade Step 2
IP500v2	8.1.0.0 and earlier	Load 8.1.1.0 or 9.0	Load 9.1
All modules	8.1.0.0 and earlier	Load 8.1.1.0 or 9.0	Load 9.1
IP500v2	8.1.1.0 and later	-	Load 9.1
All modules	8.1.1.0 and later	-	Load 9.1

Note: IP500v2 Control Units identified as PCS 14 and below must first install Release 8.1(65) (or higher 8.1) or any Release 9.0 before upgrading to Release 9.1. This will expand the loader to accommodate the 9.1 software image. If the control unit has not been used previously, care should be taken to ensure that no calls are made before the upgrade to Release 9.1; otherwise the system will require a 9.1 upgrade license despite being "new".

For further information please see the “Upgrading Systems” section of the IP500/IP500v2 Installation manual available from the IP Office Knowledgebase.

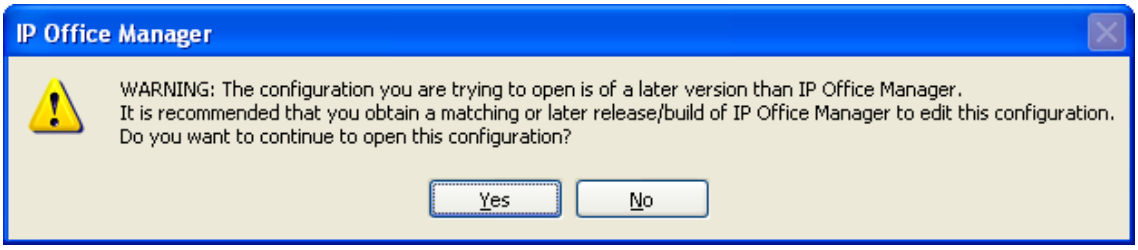
Note: IP Office Release 9.1 will no longer support the following legacy IP 400 modules:

- Phone 8/16/30
- DS 16/30
- DIGITAL S0x8 and DIGITAL S0x16
- Extension/VCM Carrier

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

5.2 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 9.1.0.0 release, the Administration suite must also be upgraded. The following message will be displayed if attempting to access a system running the 9.1.0.0 release with an earlier version of Manager:



The IP Office Administration installer will detect previous installed versions and upgrade automatically. If a version earlier than 9.0 is installed, this must first be uninstalled before installing 9.1.0.0. 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.

5.3 Upgrade Instructions for IP Office Preferred Edition

IP Office Preferred Edition (VoiceMail Pro) must be at a minimum of 8.0 GA to upgrade directly to 9.1. Previous versions must be upgraded to 8.0 first, before upgrading to 9.1.
The Preferred Edition 9.1.0.0 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.

Prior to upgrading the Preferred Edition Server to 9.1.0.0 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.

5.4 Upgrade instructions for IP Office one-X Portal

The IP Office one-X Portal server must be running a minimum software level of 8.0 to upgrade to 9.1. Any previous versions must be upgraded to 8.0 first before upgrading to this release. Further information can be found in the “Implementing one-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.

5.5 Upgrade Instructions for IP Office Server Edition and Applications Server

If using a DVD install of this release of IP Office Server Edition and Applications Server, you can upgrade directly from the previous GA release (8.1 or 9.0). For further information please refer to “IP Office Application Server 9.1 Installation and Maintenance” and the “Upgrading” section of the “Deploying IP Office Server Edition Solution” manual.

If you are upgrading via the Web Manager, these steps should be followed:

1. Transfer the ISO image.
2. Start Upgrade of 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 b to i for the other systems from the Solution.

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

5.6 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				
	8.0	8.1	9.0.0/9.0.1/9.0.2	9.0.3/9.0.4	9.1
8.0	Web Control ZIP	Web Control ZIP	USB Unetbootin	USB Unetbootin	USB Unetbootin
8.1		Web Control ZIP	USB Unetbootin	USB Unetbootin	USB Unetbootin
9.0.0 9.0.1 9.0.2			USB Unetbootin Web Control ZIP	USB Unetbootin	USB Unetbootin
9.0.3 9.0.4				USB Unetbootin	USB Unetbootin
9.1					USB Unetbootin Web Control ZIP Web Management

This release of UCM Service Pack 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 Portal logging MUST be disabled prior to upgrade. One-X Portal admin will be very slow to respond if this is not done. One-X Portal logging can be

disabled using the one-X Portal Administrator/Logging Configuration/Master Logging Level = OFF

If VMPro is not manageable by Web Manager post upgrade, check the VMPro Web Service using the Web Control Panel and start it manually.

5.7 Force Password Change

Release 9.1 introduced many security enhancements. When deploying new 500v2 systems users are now required to change default passwords for most critical administrative IP Office accounts. Also if security settings are erased to return to defaults settings, users logging into 500v2 or Server Edition systems will be required to change the default passwords for these critical accounts. When new Server Edition systems are deployed, the passwords specified during ignition phase are also applied to IP Office accounts. This mechanism updates default IP Office passwords eliminating the need to change them upon first login.

Upgrading from previous release to 9.1 does not affect passwords that were set before upgrade. However it is recommended that - as a good security practice - users change IP Office passwords if they were left as default in the original deployment. The passwords that should be updated are Service User Administrator, Security Administrator and unsecure interface System password. These passwords can be changed in the Security Settings accessible with IP Office Manager.

Additional functionality was also added to simplify synchronization of passwords in a solution with multiple nodes (e.g. Primary + Secondary + Expansion(s)). In Server Edition deployment with multiple nodes user can synchronize passwords from the Primary node to others using Web Manager | Security Manager | Service Users option. Manual synchronization can be initiated by pressing “Synchronize Security User and System Password” button. There is also an option for automated synchronization that can be further configured in Web Manager Preferences. If other nodes have different passwords set than on the Primary, user will be prompted to provide credentials for those nodes when synchronizing. Default accounts IP Office R9.1 Solution:

Component	Account User Name	Usage	Default Password	Notes
Linux Server	root	Root access local Linux server	Administrator	Local Linux account
Linux Server	Administrator	SSH access local Linux server Web control non-referred	Administrator	Local Linux account
IP Office	security	IPO security access • Security Manager • Web Mgmt	securitypwd	IPO security database
IP Office	Administrator	IPO configuration/security • Manager • Web Mgmt (includes web control) • System Status (SSA) VmPro configuration • VmPro Client	Administrator	IPO security database

IP Office	EnhTcpaService	One-X/IP Office service interface	EnhTcpaPwd1	IPO security database. No forced change
VmPro	Administrator	VmPro administrator access	Administrator	Local VmPro server. Default is referred authentication
One-X	Administrator	One-X admin portal	Administrator	Local One-X server. Default is referred authentication
One-X	Superuser	Backup restore One-X configuration	MyFirstLogin1_0	Local One-X server
Contact Recorder	Created when first accessed	Contact recorder admin	Created when first accessed	Local server account. Optional component
WebLM	admin	WebLM server configuration	weblmadmin	Local server account. Optional component
Manager upgrade		System password	password	
SysMonitor DevLink (includes TAPI)		System password	“” (blank)	If blank the System password is used
VmPro/IP Office service interface		VmPro password	“” (blank)	

6 Operating System Support

Microsoft Windows XP is no longer supported with IP Office applications.

6.1 Windows Operating System Editions and Service Packs

Operating System	Service Pack	Editions
Windows 7 32/64	SP1	Professional, Enterprise, Ultimate
Windows 8.1	n/a	Pro, Enterprise
Server 2008 32/64	SP2	Standard, Small Business Server
Server 2008 R2 (64 only)	SP1	Standard
Server 2012	n/a	Standard
Server 2012 R2	n/a	Standard

6.2 Operating System Support - Server Components

Application	Win 7		Win 8.1 (3)		Server 2008 /2008R2 (2)		Server 2012/2012R2
	32 bit	64 bit	32 bit	64 bit	32 bit	64 bit	64 bit
Preferred Edition Server (VMPro) Standalone	✓	✓	✓	✓	✓	✓	✓
... Plus UMS	✗	✗	✗	✗	✓	✓	✓
... Plus Campaigns	✗	✗	✗	✗	✓	✓	✓
... with IMS	✗	✗	✗	✗	✓	✗	✗
... MAPI service for VMPro on Linux	✓	✓	✗	✗	✓	✓	✓
Contact Store Server	✗	✗	✗	✗	✓	✗	✗
one-X Portal for IP Office Server	✗	✗	✗	✗	✓	✓	✓
TAPI - 3rd Party & TAPI WAV	✓	✓	✓	✓	✓	✓	✓
IP Office Contact Centre (IPOCC)	✗	✗	✗	✗	✗	✓(1)	✓(1)

(1) - Phoenix is Server 2008R2 and 2012R2
(2) - 2008R2 is 64 bit only
(3) - 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=win8other (link valid 16-Jun-2014)

6.2.1 Operating System Support - Thick Client Apps

Application	Win 7		Win 8.1		Server 2008/2008R2		Server 2012/2012R2
	32 bit	64 bit	32 bit	64 bit	**32 bit**	**64 bit**	**64 bit**
Preferred Edition Client	✓	✓	✓	✓	✓	✓	✓
SoftConsole	✓	✓	✓	✓	✗	✗	✗
Manager	✓	✓	✓	✓	✓	✓	✓
SysMon	✓	✓	✓	✓	✓	✓	✓
SSA	✓	✓	✓	✓	✓	✓	✓
TAPI 1st Party	✓	✓	✓	✓	✓	✓	✓
TAPI WAV	✓	✓	✓	✓	✓	✓	✓
IP Office Video Softphone (2)	✓	✓	✗	✗	✗	✗	✗
Flare	✓	✓	✓	✓	✗	✗	✗
one-X Portal Plug-In for Outlook	✓	✓	✓	✓	✗	✗	✗
one-X Portal Plug-In for Salesforce.com	✓(1)	✓(1)	✓(1)	✓(1)	✗	✗	✗
Call Assistant	✓	✓	✓	✓	✗	✗	✗
Plug-In for MS Lync 2010	✓	✓	✓	✓	✗	✗	✗
Plug-In for MS Lync 2013	✓	✓	✓	✓	✗	✗	✗
Web Conferencing (Adobe Flash and Java Applet for sharing)	✓	✓	✓	✓	✗	✗	✗
IP Office Contact Centre (Phoenix)	✓	✓	✓	✓	✗	✗	✗

(1) With matching IE - use IE8-32bit on Win7-32bit, IE8-64bit on Win7-64bit
(2) Legacy support only

6.2.2 Mac Thick Client Apps

Application	OSX 10.5 Leopard	OSX 10.6 Snow Leopard	OSX 10.7 Lion	OSX 10.8 Mountain Lion	OSX 10.9 Maverics	OSX 10.10 Yosemite
IP Office Video Softphone - Version 4.0	✗	✗	✗	✓	✓	✓
Web Conferencing (Adobe Flash and Java Applet for sharing)	✗	✗	✓	✓	✓	✓

6.2.3 **Browsers**

Application	IE8	IE10	IE11	FFXX	Chrome XX	Safari 7
VMPro Campaigns Client	✓	✓	✓	✗	✗	✗
VMPro UMS WebMail	✓	✓	✓	✗	✗	✗
Contact Store Client	✓	✓	✗	✗	✗	✗
one-X Portal for IP Office Client	✓	✓	✓	✓	✓	✓
Web Conferencing	✗	✓	✓	✓	✓	✓
Web Manager Web Control Page	✗	✓	✓	✓	✓	✓
Salesforce.com Plug-In	✓(1)	✓(1)	✗	✓	✓	✗
D100 DECT Admin	✓	✓	✓	✓	✓	✓
IP DECT R4 Admin	✓	✓	✓	✓	✓	✓

(1) Not on Server O/S

6.2.4 **JRE**

Application	Version 6 Update 16	Version 7 Update 51	Version 7 Update 5
SSA	✓	✓	
one-X Portal Server			✓ one-X Windows uses embedded jre and doesn't install or interfere with the installed JRE on the system.

7 Security Enhancements

7.1 TLS/sRTP/HTTPS Support in IP Office R9.1

In IP Office R9.1 the following SIP phones/clients are supported with TLS/sRTP:

- 11xx/12xx SIP phone
- Avaya Communicator (iPad and Windows)
- B179 conference SIP phone
- E129 RAPID SIP phone
- oneX Mobile Preferred (iOS and Android)
- Radvision XT 4000/5000 series

SIP phones/clients not listed above are not supported for use with TLS/sRTP/HTTPS with IP Office R9.1.

In IP Office R9.1 the following H323 phones/clients are supported with TLS/sRTP:

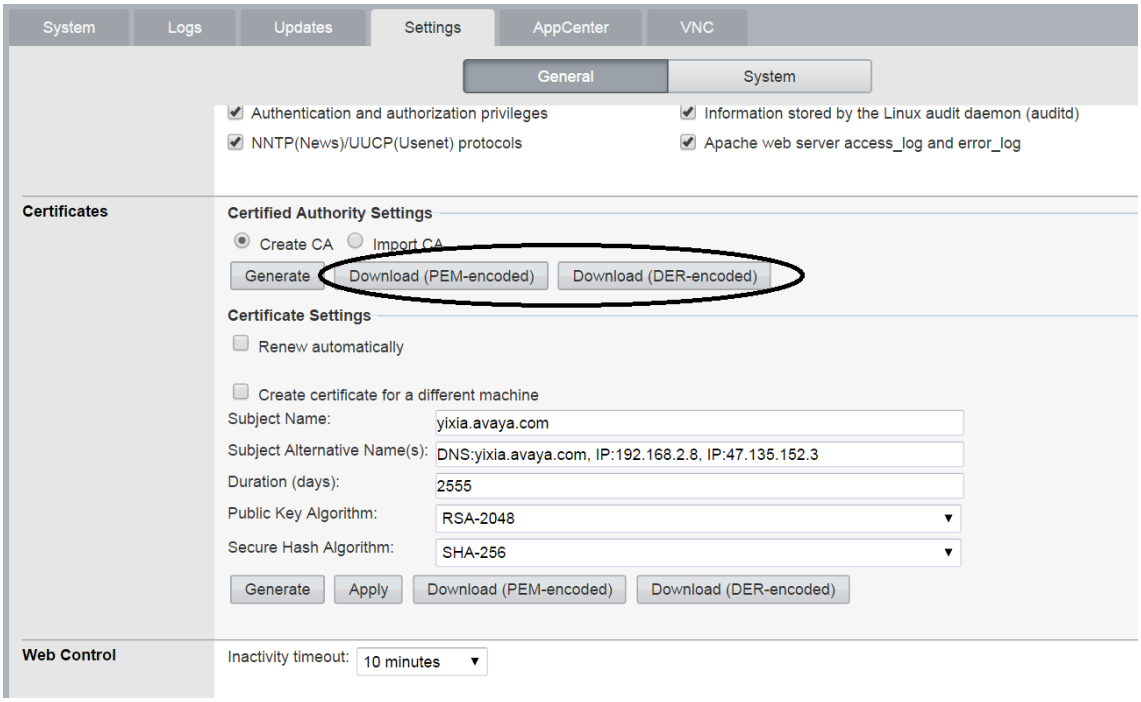
- 96x1 running H323 software release 6.4.0 or above

In IP Office R9.1 SRTP is supported on IP Office lines that link IP Office systems.

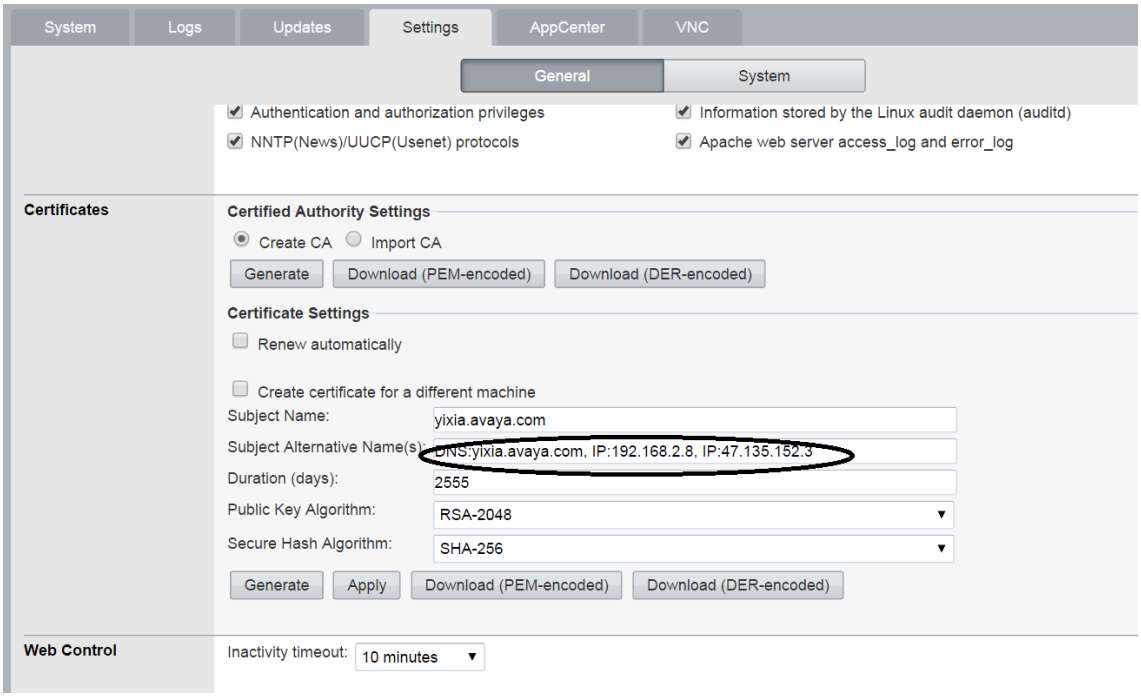
7.1.1 **IP Office Configuration**

The following notes assume that a root CA has not already been created as part of system ignition. If this system is a new deployment in IPO 9.1, then the system ignition should have already created a root CA and there is no need to create a new one. The existing one can be downloaded and used instead of creating a new one. If this system has been upgraded from an older IP Office release, it is quite possible that a root CA has not yet been created and these instructions include notes on how to create one now.

- TLS
    - Turn on TLS for SIP extensions and SIP trunks
        - SIP Client: Manager->System->LANx->VoIP->SIP Registrar Enable->Layer 4 Protocol
            - UDP/TCP/TLS
            - UDP Port/TCP Port/TLS Port
            - Remote UDP Port/TCP Port/TLS Port
        - SIP Trunk: System->Lines->LineX
            - Create SIP trunk (points to Radvision Elite MCU iView server)
            - Transport->Layer 4 Protocol: TLS
            - Transport->Send Port
            - Transport->Listen Port
    - IPOL WebControl Manager Certificate Management (https://ipol:7071)
        - Generate root CA:
            - WebControl Manager->settings->Certificate->Create CA
                - Generate: generate a new root CA
                - Download: The root CA generated by IPOL can be downloaded in either PEM or DER format. This root certificate needs to be uploaded to various SIP phone/clients for certificate verification.

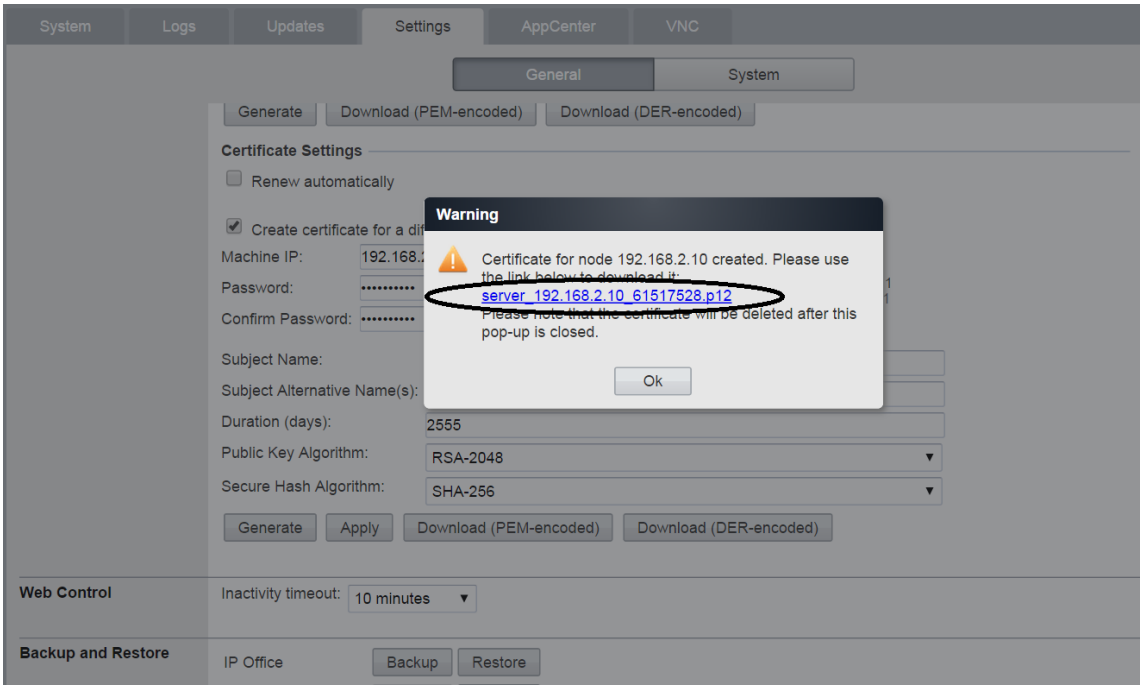


- Import third party root CA:
  - WebControl Manager->settings->Certificate->Import CA
    - Browse rootCA or intermediate CA file. The file needs to be p12 format and contains the certificate and
    - private key.
    - Enter the export password for CA p12 file, and then upload.
    - This root certificate will then be used to generate identity certificate.
- Generate identity certificate
  - IPOL's server identity certificate can be generated using the current root certificate.
  - Avaya security council's guideline for Avaya products identity certificates is
    - Common name: IP Office's fully qualified domain name (FQDN)
    - SubjectAltName extension:
      - DNS: FQDN
      - IP.1: IP address of IP Office LAN1
      - IP.2: IP address of IP Office LAN2 or public IP address if remote clients are involved.
      - URI: SIP domain specified in Manager->LANx->VoIP->SIP Register Enable->Domain Name.
    - SHA256/2048-bit key length

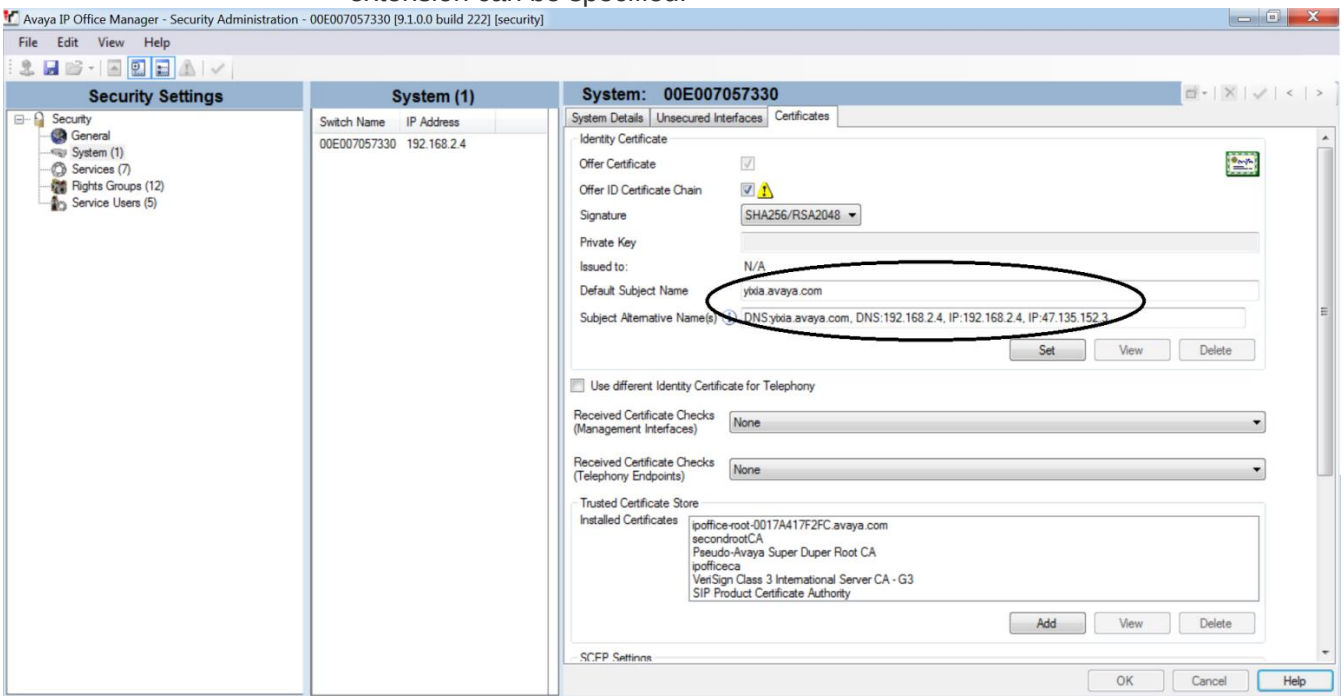


- "Generate", then "Apply". When applying the newly generated identity certificate, all apps on IPOL server will be stopped then restarted.

- Create Certificate for IPO500v2 expansion
  - Identity certificate for another server (for example an IPO500V2 expansion) can be generated using "Create certificate for another machine".
  - Machine IP: IP address of the other machine
  - Password: export password for the identity certificate. This password is required later when uploading the certificate to the designated server.
  - Generate: After "Generate", the system will prompt the user to download the certificate file in p12 format. This certificate file can be uploaded to IP Office using security manager.



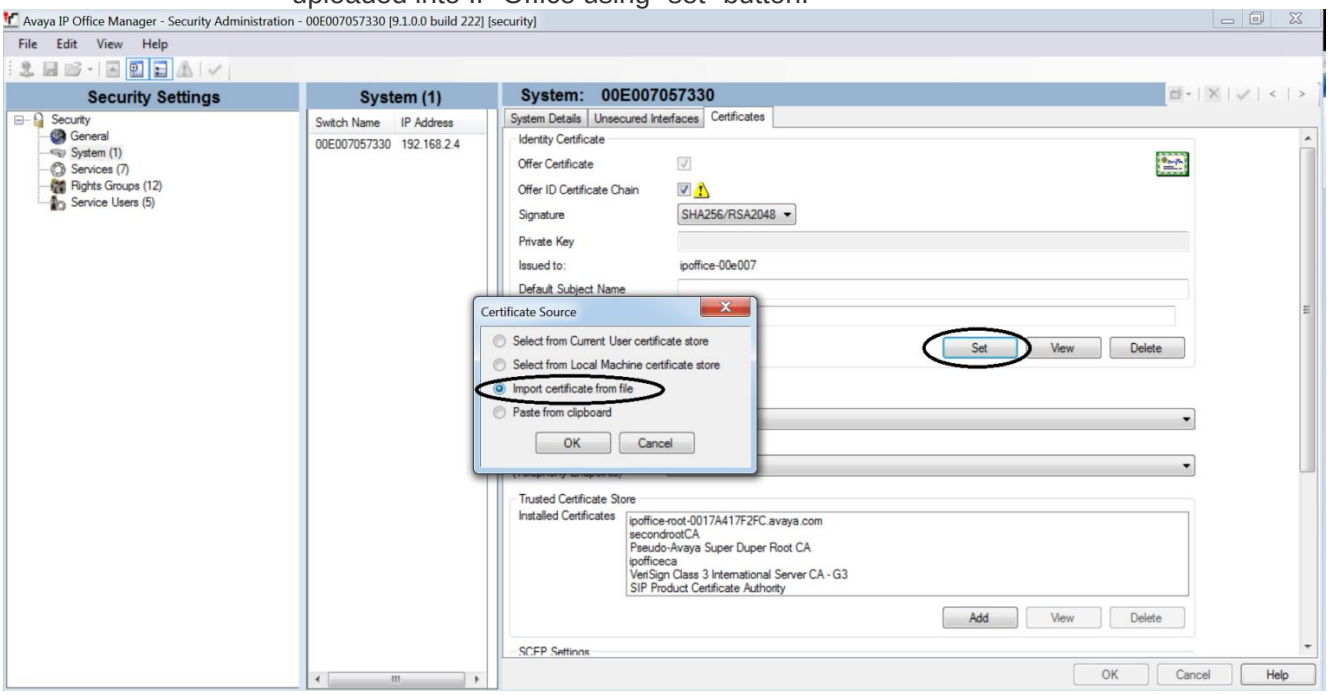
- IP Office Manager Security Settings->System->Certificates
  - Generate self-signed identity certificate:
  - Upload customer IP Office's identity certificate using "Set" button.
  - By default, IP Office security manager will generate a self-signed identity certificate. It's common name and subjectAltName extension can be specified:



  - Please be aware, not all TLS-capable SIP phone/client accepts self-signed server identity certificate.
    - Accept self-signed certificate: Avaya Communicator for Windows/iPad, oneX Mobile Preferred iOS/Android, E129, B179
    - Reject self-signed server identity certificate: 11xx/12xx, Radvision XT-series

- Upload a signed server identity certificate:

        - An identity certificate signed by a certificate authority can be uploaded into IP Office using "set" button.



        - Make sure "Offer ID Certificate Chain" is checked if the identity certificate is signed by an intermediate certificate and the intermediate certificate is not distributed to SIP phones/clients.
    - Use different Identity Certificate for Telephony
        - If this flag is checked, upload a telephony-specific identity certificate using "Set" button.
        - Check "Offer ID Certificate Chain" if the identity certificate is signed by an intermediate certificate.
        - If this flag is not checked, IP Office's main identity certificate is used for telephony endpoint.
    - Received Certificate Checks (Management): Optional.
    - Received Certificate Checks (Telephony Endpoint): None. In IP Office R9.1, client identity certificate is not supported.
    - Trusted Certificate Store: Upload all intermediate CA certificates and root CA certificate to IP Office trusted certificate store.
- SIPS URI
    - Some SIP clients support SIPS URI and some don't:
        - Use SIPS URI when TLS is chosen and not configurable: Avaya Communicator for iPad, Avaya Communicator for Windows, OneX Mobile Preferred iOS, Radvision 4000/5000 series.
        - SIPS URI can be configured using configuration file: E129, B179. In this release, both phones are not configured with SIPS URI.
        - SIPS URI is not supported: 11xx/12xx. OneX Mobile Preferred Android
    - When both "System->LANx->VoIP->Layer4Protocol->TLS" and "System->VoIP Security->Strict SIPS" are selected, all remote SIP phones/clients are required to connect to IP Office using TLS. Local network is deemed secure and local SIP phones/clients are not subject to this requirement.
- sRTP
    - System level
        - System->VoIP Security->Media Security: "Disable", "Enforce", "Best Effort", "Prefer Direct Media", default "Disabled"
        - System->VoIP Security->Media Security Options:

        - Encryption and Authentication: ENCRYPTED_RTP, AUTHENTICATED_RTP, UNENCYPTED_RTCP, AUTHENTICATED_RTP
        - Replay Protection sRTP window size: 64
        - Crypto Suite: AES_CM_128_HMAC_SHA1_80 (default), AES_CM_128_HMAC_SHA1_32
    - Extension level
        - Extension->VoIP-> Media Security: "Same as System", "Disable", "Enforce", "Best Effort", default "Same as System"
        - Some SIP phones like E129 is not supported for extension level media security. For these phones, extension media security should always set as "Same as System".
        - SIP soft-clients that register with IP Office in simultaneous mode are not supported for extension level media security. Their media security settings are always set as "Same as System".
    - Video sRTP transcoding is not supported in IP Office R9.1.

7.1.2 **1120e, 1140e, 1220, 1230 SIP Phones**

- TLS
    - Verify IP Office identity certificate through certificate chain up to the root certificate.
        - Customer root certificate needs to be uploaded to the phone.
    - Perform hostname validation on IP Office identity certificate.
        - Requires IP Office identity certificate containing subjectAltName extension with the following field:
            - IP.1: IP address of IP Office LAN1 if local 11xx/12xx sets are supported
            - IP.2: IP address of IP Office LAN2 if local 11xx/12xx sets are supported through LAN2
            - IP.3: Public IP address if remote 11xx/12xx sets are supported
        - In IP Office release 9.1, 11xx/12xx SIP phone will not validate server FQDN (DNS field of subjectAltName extension).
    - Root certificate distribution
        - Root certificate can be uploaded to the phone as part of auto-configuration procedure. For details, please refer to HTTPS session below.
    - Fall back to TCP/UDP:
        - When TLS connection fails, phone would fall back to TCP/UDP if either TCP or UDP are selected in "IP Office manager->system->LANx->VoIP->SIP Registrar Enable". Please be aware that TLS is the only transport protocol allowed for remote SIP clients when strict SIPS is selected in IP Office.
    - Phone configuration:
        - Auto-configuration is supported for this phone. For details, please refer to HTTPS section.
        - 11xxsettings.txt
            - SERVER_TLS_PORT_1
            - SERVER_TLS_PORT_2
        - Root Certificate: 11xxSIP.cfg
            - USER_KEYS
    - SIPS URI
        - 11xx/12xx SIP phone does not support SIPS URI.

- sRTP
  - sRTP parameters supported:
    - Crypto suite (configurable): AES_CM_128_HMAC_SHA1_80, AES_CM_128_HMAC_SHA1_32
    - Encryption/Authentication flags (configurable): ENCRYPTED_RTP, AUTHENTICATED_RTP, UNENCRYPTED_RTCP, AUTHENTICATED_RTCP
    - Options (configurable): BestEffort
  - Phone configuration
    - Auto-configuration is supported for this phone. Media security is always configured as best-effort capability negotiation on the phone.
    - 11xxsettings.txt
      - SRTP Enabled – YES
      - SRTP_MODE – BE-Cap Neg
      - USE_UNENCRYPTED_SRTCP – YES
      - SRTP_CIPHER_1 AES_CM_128_HMAC_SHA1_80
      - SRTP_CIPHER_2 AES_CM_128_HMAC_SHA_32
  - IP Office system media security maps to 11xx/12xx sRTP mode:

IP Office System Media Security	11xx/12xx sRTP Options
Disabled	BE-Cap Neg
Best Effort	BE-Cap Neg
Enforce	BE-Cap Neg

- Extension level media security configuration is supported for this phone.
- Key Negotiation
  - 11xx/12xx SIP phone changes its sRTP master key during reINVITE. Therefore direct media is not supported for 11xx/12xx sRTP mode.

7.1.3 **11xx/12xx HTTPS**

- Use of the secure https connection
  - The secure https connection for operations like configuration files download, firmware upgrade, directory download is enforced when possible.
  - The use of the secure https connection will be determined based on the IPO's configuration under System->LAN->VoIP->Layer 4 Protocol. If the TLS transport protocol is selected, then the secure connection for config/firmware download will be enforced regardless if the phone is connected locally or it is in the remote location. If the TLS protocol is not selected then the unsecure http connection will be used. This is based on the assumption that if the secure communication is required for the SIP communications then the secure connection should also be used for the configuration/firmware download.
  - On the 11xx/12xx phones if the IPOs root certificate is not installed on the phone the https will not be properly established and the file downloads will fail.
  - If the secure communication is required, the Security Policy file and the IPO's Root certificate have to be installed on the phone before the phone can properly register with the IP Office.
- Server ROOT Certificate installation
  - If the 11xx/12xx phone is installed in the local network, the phone automatically downloads the Security Policy file and the IPO's root certificate using unsecure http connection. This is exactly the

same mechanism that is already used for the phones deployed in the Branch mode. In the Branch mode the IPO's root certificate is pushed to the IPO from the SM but in the non-branch deployments an Administrator has to make sure that the IPOs root certificate(s) are installed in the IPOs Secure Certificate store. This is done using IPO Manager Security->System->Certificates->Trusted Certificate Store.

- In case when the phone is installed in the remote network environment (cloud/remote worker) the IPO's Security Policy file and the IPO's root certificate have to be pre-installed on the phone before phone can be connected in the remote network. There are 2 options how to do this:

  Option 1:
  If possible, connect the phone to the local IPO network and make sure that the phone's provisioning server points to the IPO and the provisioning protocol is http. In the initial installation the phone will download the Security Policy file and the IPO's root certificate(s) from the IPO's http server.

  IMPORTANT: Please stand by the phone during the initial installation. After the security policy file is downloaded, the phone will prompt for the policy file to be accepted. Accept the Policy file as prompted. If you miss to accept the Policy file do not accept the Root certificate(s). Just reboot the phone and repeat the initial installation.

  Option 2:
  Setup the third party http server and place the 1140eSIP.cfg/1120eSIP.cfg/1230SIP.cfg/1220SIP.cfg, Security Policy file (11xxsecpolicy.txt) and IPO's Root certificate(s) on that server. Sample contents for these 5 files are appended at the end of this section.

  11xxsecpolicy.txt
  1140eSIP.cfg
  1120eSIP.cfg
  1230SIP.cfg
  1220SIP.cfg

  The file name for the Main root certificate should be WebRootCA.pem and the telephony root certificate filename should be TelRootCA.pem. You can just rename the root certificates files. If the same root CA is used for the Main and the Telephony IPO's identity certificate then just place the WebRootCA.pem file on the HTTP server.

  Make sure that the phone's provisioning server points to the third party http server and the provisioning protocol is http.

  IMPORTANT: Please stand by the phone during the initial installation. After the security policy file is downloaded, the phone will prompt for the policy file to be accepted. Accept the Policy file as prompted. If you miss to accept the Policy file do not accept the Root certificate(s). Just reboot the phone and repeat the initial installation.

        - **Note**: If the root certificate has to be changed on the phone then the previously installed root certificate has to be removed from the phone and the procedure for the phone installation has to be repeated. The certificate can be removed using phone's UI under Menu->3.Diagnostics->5.Certificates Administration->1.Trusted Certificates. Find the installed certificates and press View and then Delete. The other option for removing root certificates is to reset the phone to the factory defaults.
    - Phone Installation procedure
        - Local phone installation.
            - Make sure that phone's provisioning server point to the IPO.
                - If the IPO's DHCP server is used this will be done automatically.
                - If the third party DHCP server is used the DHCP server should be configured with option 66 to point to the IPO's IP address
                - If the static configuration is used then the Provisioning should be set to the IPO'IP and the protocol should be http.
            - Phone will automatically download all the configuration files from the IPO and phone should successfully register with the IPO.
        - Remote phone installation.
            - Pre-install Security Policy file and the IPO's root certificate using Option 1 or Option 2 above.
            - Connect phone in the remote location using one of the scenarios for the phone installation in the remote location. Use the third party DHCP server or the static IP configuration for the phone. Make sure that the Provisioning server parameter on the phone points to the Public IPO address and if desired protocol can be set to https. This setting is done using phone's UI in case of static phone configuration or using option 66 in your DHCP server.
- Sample File Contents illustrating the relevant sections. The actual files on your system may contain other sections not illustrated here
    - 11xxsecpolicy.txt

```
CERT_ADMIN_UI_ENABLE        YES
SECURITY_LOG_UI_ENABLE      NO
KEY_SIZE                         KEY_SIZE_1024
KEY_ALGORITHM               KEY_ALG_RSA
TLS_CIPHER                  RSA_WITH_AES_256_CBC_SHA
SIGN_SIP_CONFIG_FILES            NO
SEC_POLICY_ACCEPT                VAL_MANUAL_A
CUST_CERT_ACCEPT                 VAL_NO_CHECK
SUBJ_ALT_NAME_CHECK_ENABLE  YES
```

    - 1140eSIP.cfg

```
[SEC_POLICY]
DOWNLOAD_MODE   AUTO
VERSION         000002
PROTOCOL        HTTP
FILENAME        11xxsecpolicy.txt
```

```
[USER_KEYS]
DOWNLOAD_MODE   AUTO
VERSION         000002
PROTOCOL        HTTP
FILENAME        WebRootCA.pem

[USER_KEYS]
DOWNLOAD_MODE   AUTO
VERSION         000003
PROTOCOL        HTTP
FILENAME        TelRootCA.pem
```

- 1120eSIP.cfg

```
[SEC_POLICY]
DOWNLOAD_MODE   AUTO
VERSION         000002
PROTOCOL        HTTP
FILENAME        11xxsecpolicy.txt

[USER_KEYS]
DOWNLOAD_MODE   AUTO
VERSION         000002
PROTOCOL        HTTP
FILENAME        WebRootCA.pem

[USER_KEYS]
DOWNLOAD_MODE   AUTO
VERSION         000003
PROTOCOL        HTTP
FILENAME        TelRootCA.pem
```

- 1230SIP.cfg

```
[SEC_POLICY]
DOWNLOAD_MODE   AUTO
VERSION         000002
PROTOCOL        HTTP
FILENAME        11xxsecpolicy.txt

[USER_KEYS]
DOWNLOAD_MODE   AUTO
VERSION         000002
PROTOCOL        HTTP
FILENAME        WebRootCA.pem

[USER_KEYS]
DOWNLOAD_MODE   AUTO
VERSION         000003
PROTOCOL        HTTP
FILENAME        TelRootCA.pem
```

- 1220SIP.cfg

```
[SEC_POLICY]
DOWNLOAD_MODE   AUTO
VERSION         000002
PROTOCOL        HTTP
```

```
FILENAME        11xxsecpolicy.txt

[USER_KEYS]
DOWNLOAD_MODE   AUTO
VERSION         000002
PROTOCOL        HTTP
FILENAME        WebRootCA.pem

[USER_KEYS]
DOWNLOAD_MODE   AUTO
VERSION         000003
PROTOCOL        HTTP
FILENAME        TelRootCA.pem
```

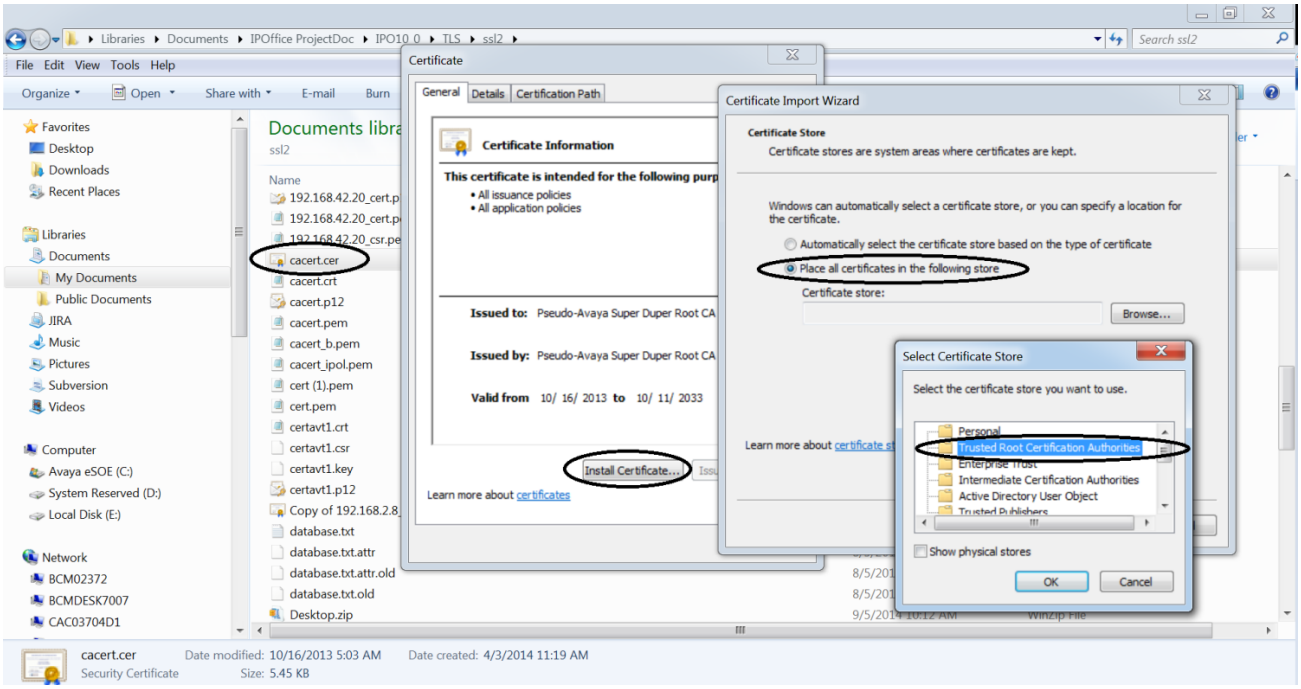
7.1.4 **Avaya Communicator iPad**

- TLS
  - Verify IP Office identity certificate through certificate chain up to the root certificate.
    - Customer root certificate needs to be uploaded to the phone.
  - Does not perform hostname validation for SIP server in Avaya Communicator release 2.0.
  - Root certificate distribution
    - Root certificate can be uploaded to the phone in the following ways:
      - Through secure email (for illustration, see oneX mobile iOS session below)
      - Using "iPhone Configuration Utility"
  - Fall back to TCP/UDP: when TLS connection fails, phone would not register.
  - Phone configuration
    - Auto-configuration is not supported.
    - Configuration using SIP client application interface:
      - To turn on TLS, go to "app->configuration_icon->Accounts and Services->Phone Services->TLS"
      - To specify TLS port, go to "app->configuration_icon->Accounts and Services->Phone Services->Phone Server Port". This port can be left empty if default TLS port 5061 is used.
  - SIPS URI
    - When TLS is selected, Avaya Communicator for iPad uses SIPS URI. This is not configurable.
  - Presence Server
- sRTP
  - sRTP parameters supported:
    - Crypto suite (non-configurable): AES_CM_128_HMAC_SHA1_80, AES_CM_128_HMAC_SHA1_32
    - Encryption/Authentication flags (non-configurable): ENCRYPTED_RTP, AUTHENTICATED_RTP, UNENCRYPTED_RTCP, AUTHENTICATED_RTCP
    - Options (non-configurable): Disabled, BestEffort
    - Avaya Communicator for iPad supports (sRTP audio + RTP video) combination.

- Phone configuration
    - Auto-configuration is not supported for this phone. Most sRTP parameters are not configurable.
    - When SIP signaling is secured by TLS, best effort sRTP is always offered by Avaya Communicator for iPad client. When SIP signaling is not secured (TCP instead of TLS), no sRTP is supported.
    - Extension level media security configuration is supported in stand-alone mode. It is not supported in simultaneous mode.
- Key negotiation
    - Avaya Communicator for iPad does not change its sRTP master key during reINVITE.

7.1.5 **Avaya Communicator For Windows**

- TLS
    - Verify IP Office identity certificate through certificate chain up to the root certificate.
        - Customer root certificate needs to be installed in Windows' trusted certificate store.
    - The Avaya Communicator for Windows does not validate a security certificate chain unless all intermediate certificates are available in the Windows intermediate certificate store. This means that administrators who wish to use their own certificates for signalling and media between the IP Office and Communicator for Windows must provide all of the intermediate certificates to the end users. The end user must install the intermediate certificates in the Windows Certificate Store for Intermediate Certification Authorities.
        - This only impacts systems where TLS/SRTP is used for signalling and media for SIP endpoints.
        - This does not impact systems where the default IP Office certificates are used.
        - The only workaround is to install the intermediate certificates in the Windows Certificate Store for Intermediate Certification Authorities.
    - Does not perform hostname validation for SIP server in Avaya Communicator release 2.0.
    - Root certificate distribution
        - Root certificate can be distributed in the following ways:
        - Through secure email
        - Copy the certificate directly to PC
        - Change the certificate's extension to .cer
        - Double click the file to install the root certificate in Windows's trusted certificate store.



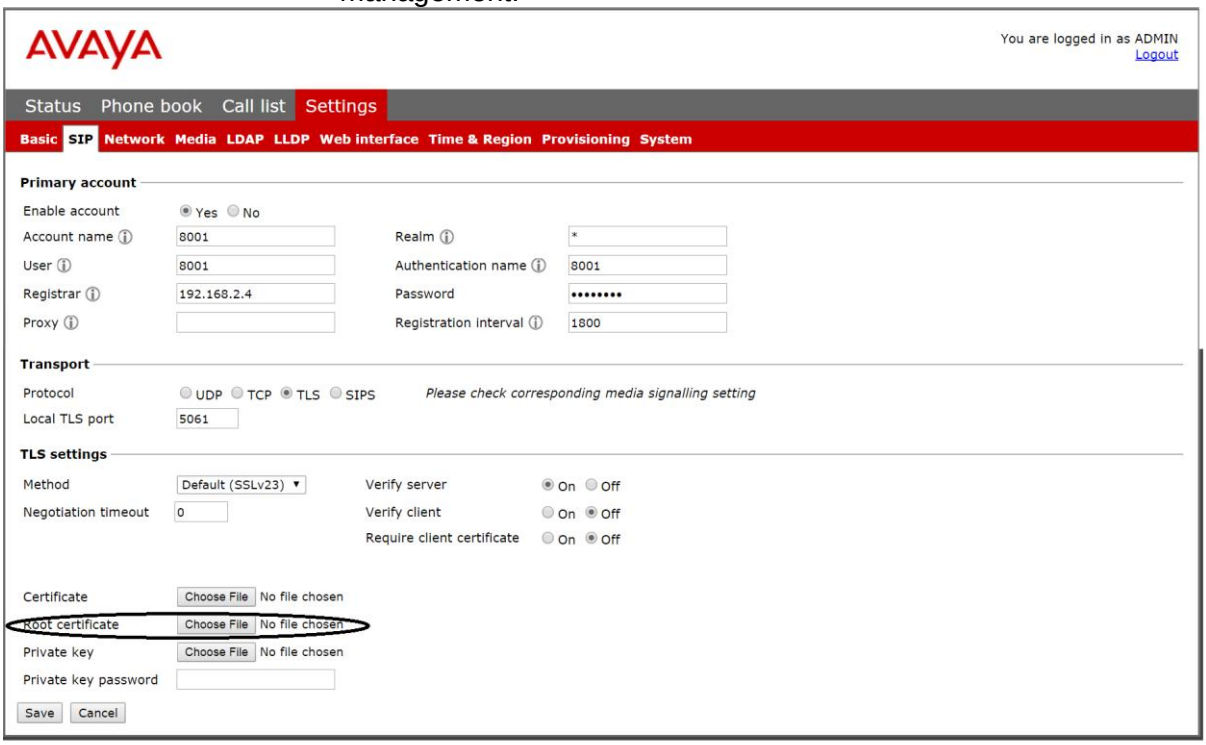
- Fall back to TCP/UDP: when TLS connection is failed, phone would not register.
- Phone configuration
  - Auto-configuration is not supported.
  - Configuration using SIP client application interface:
    - To turn on TLS, go to "app->settings->other settings->Server->Transport Type" and select "TLS".
    - To specify TLS port, go to "app->settings->other settings->Server->Server Port". This port can be left empty if default TLS port 5061 is used.
- SIPS URI
  - When TLS is selected, Avaya Communicator for Windows uses SIPS URI. This is not configurable.
- Presence Server

- sRTP
  - sRTP parameters supported:
    - Crypto suite (non-configurable): AES_CM_128_HMAC_SHA1_80, AES_CM_128_HMAC_SHA1_32
    - Encryption/Authentication flags (non-configurable): ENCRYPTED_RTP, AUTHENTICATED_RTP, UNENCRYPTED_RTCP, AUTHENTICATED_RTCP
    - Options (non-configurable): Disabled, BestEffort
    - Avaya Communicator for iPad supports (sRTP audio + RTP video) combination.
  - Phone configuration
    - Auto-configuration is not supported for this phone. Most sRTP parameters are not configurable.
    - When SIP signaling is secured by TLS, best effort sRTP is always offered by Avaya Communicator for Windows client.
    - Extension level media security configuration is supported in stand-alone mode. It is not supported in simultaneous mode.
  - Key negotiation

- Avaya Communicator for Windows does not change its sRTP master key during reINVITE.

7.1.6 B179 SIP Phone

- **TLS**
  - Verify IP Office identity certificate through certificate chain up to the root certificate.
    - Root certificate needs to be uploaded to the phone
  - Does not perform hostname validation for SIP server in IP Office R9.1 time frame
  - Root certificate distribution
    - Root certificate can be uploaded to the phone using web management interface. For details, please refer to HTTPS session below
  - Fall back to TCP/UDP: when TLS connection is failed, phone would fall back to TCP if TCP is selected in "IP Office manager->system->LANx->VoIP->SIP Registrar Enable"
  - Phone configuration:
    - Auto-configuration is supported for this phone. For details, please refer to HTTPS section.
    - avayab179.xml
      - <tls_transport> TLS flag </tls_transport> : set to 1
      - <tls_port> TLS port</tls_port> : set to TLS port
      - <tls_verify_server>verify server certificate</tls_verify_server>: set to 1
    - Root Certificate: upload root certificate using phone web management.



- **SIPS URI**
  - SIPS URI is configurable in B179 SIP phone.
    - avayab179.xml

        - <sips_transport> SIPS flag </sips_transport> : set to 0
    - SIPS URI is not used for B179 for IP Office R9.1 release.
    - SHA1-1024 bit Certificate: B179 does not support SHA1-1024 bit certificate for IP Office R9.1 time frame.

- **sRTP**
    - sRTP parameters supported:
        - Crypto suite (non-configurable): AES_CM_128_HMAC_SHA1_80
        - Encryption/Authentication flags (configurable): ENCRYPTED_RTP, AUTHENTICATED_RTP, UNENCRYPTED_RTCP, AUTHENTICATED_RTCP
        - Options (configurable): Disabled, BestEffort, Enforced
    - Phone configuration
        - Auto-configuration is supported for this phone. Media security is always configured as best-effort capability negotiation on the phone.
        - avayab179.xml
            - <use_srtp>1</use_srtp>
            - <use_srtcp>false</use_srtcp>
            - <srtp_secure_signaling>0</srtp_secure_signaling>
    - IP Office system media security maps to B179 sRTP mode:

IP Office System Media Security	B179 sRTP Options
Disabled	SRTP Optional
Best Effort	SRTP Optional
Enforce	SRTP Optional

- Extension level media security configuration is supported for this phone.

- Key negotiation
    - B179 does not change its sRTP master key during reINVITE.

- **HTTPS**
    - Use of the secure https connection
        - The secure https connection for operations like configuration files download, firmware upgrade, directory download is enforced when possible.
        - The use of the secure https connection will be determined based on the IPO's configuration under System->LAN->VoIP->Layer 4 Protocol. If the TLS transport protocol is selected, then the secure connection for config/firmware download will be enforced regardless if the phone is connected locally or it is in the remote location. If the TLS protocol is not selected then the unsecure http connection will be used. This is based on the assumption that if the secure communication is required for the SIP communications then the secure connection should also be used for the configuration/firmware download.
    - Server ROOT Certificate installation
        - The IPO's root certificate has to be installed on the phone before phone can be deployed. This has to be done using phone's WEB interface. In the WEB browser go into Settings-> Provisioning->Device Management->Root Certificate->Browse and from your

file system select the same Root Certificate that is used for the IPO's Identity certificate and press the "Save" button. The certificate should be installed.

- If the Root CA certificate is not installed on the B179 then the TLS connection is established but without Server certificate validation.
- If the Root certificate is installed on the phone then to allow validation of the server certificate to pass the time setting on the phone has to be configured to the value that is in the range of the validity period for the IPOs certificate. This is done using phone's WEB browser under Settings->Time and Region->Time. If you have NTP server accessible then you can set the NTP server address. If you don't have accessible NTP server then Set the NTP server to off and set the Time and Date to the correct values. Note: After phone successfully registers with the IPO, the time on the phone will be controlled by the IPO.

- Phone Installation Procedure
  - After the B179 makes the first contact with the IPO the configuration and upgrade server address and protocol are controlled by the IP Office.
  - There are some differences in installation procedure depending on the network setup where the phone is installed:
  - **The DHCP server is on the IPO (local phone installation)**
    In this scenario the DHCP reply will include option 242 set to point to the private IP address of the IPO "http://<IPO IP>".

    The phone will request its configuration file from the IPO. The IPO will disable use of the DHCP option to obtain configuration server and will set the file server address to the private IP address of the IPO and the protocol will be set depending on the IPO's configuration under the System->LAN->VoIP->Layer 4 Protocol. It will be set to "https://<IPO_IP>" if the TLS protocol is set and to "http://<IPO_IP>" if it is not set.

  - **The third party DHCP server is used (local phone installation)**
    In this scenario the DHCP server will be configured with the option 242 pointing to the private IP address of the IPO "http://<IPO IP>" or "https://<IPO_IP>". If the DHCP server cannot be configured with the Option 242 then the phone would have to be pre-configured using phone's Web UI under Settings->Provisioning->File server address with "http://<IPO IP>" or "https://<IPO_IP.

    In both cases, the B179 will request its configuration file from the IPO. The IPO will disable use of the DHCP option to obtain the configuration server and will set the file server address to the private IP address of the IPO and the selected protocol will be set depending on the IPO's configuration under System->LAN->VoIP->Layer 4 Protocol. It will be set to "https://<IPO_IP>" if the TLS protocol is set and to "http://<IPO_IP>" if it is not set.

  - **The third party DHCP server is used (remote phone installation)**
    In this scenario the DHCP server will be configured with the option 242 pointing to the public IP address of the IPO "http://<IPO Public IP>" or "https://<IPO Public_IP>". If the DHCP server cannot be configured with the Option 242 then the phone has to be pre-

configured using phone's Web UI under Settings->Provisioning->File server address with "http://<IPO Public IP>" or "https://<IPO_Public IP>.

In both cases the B179 will request its configuration file from the IPO. The IPO will disable use of the DHCP option to obtain the configuration server and will set the file server address to the public IP address of the IPO and the selected protocol will be set depending on the IPO's configuration under System->LAN->VoIP->Layer 4 Protocol. It will be set to "https://<IPO_Public_IP>" if the TLS protocol is set and to "http://<IPO_Public_IP>" if it is not set.

- **Static IP configuration (local phone installation)**
  In this scenario the B179 will be configured with the static IP and the configuration server should be pre-configured with the private IP address of the IPO "http://<IPO IP>" or "https://<IPO_IP>".

  In this case the B179 will request its configuration file from the IPO. The IPO will set the file server address to the private IP address of the IPO and the selected protocol will be set depending on the IPO's configuration under System->LAN->VoIP->Layer 4 Protocol. It will be set to "https://<IPO_IP>" if the TLS protocol is set and to "http://<IPO_IP>" if it is not set.

- **Static IP configuration (remote phone installation)**
  In this scenario the B179 will be configured with the static IP and the configuration server should be pre-configured with the public IP address of the IPO "http://<IPO PUBLIC IP>" or "https://<IPO PUBLIC_IP>".

  In this case the B179 will request its configuration file from the IPO. The IPO will set the file server address to the public IP address of the IPO and the selected protocol will be set depending on the IPO's configuration under System->LAN->VoIP->Layer 4 Protocol. It will be set to "https://<IPO_Public_IP>" if the TLS protocol is set and to "http://<IPO_Public_IP>" if it is not set.

- **Note**: In all the cases the file server address set on the phone will not be affected by the subsequent DHCP requests. In order for the B179 to use the option 242 from the DHCP reply again, the phone has to be reset to the factory defaults or manually re-configured using the WEB UI under Settings->Provisioning->Device Management. This mainly affects cases when the phone is moved to a different IP Office.

7.1.7 **E129 SIP Phone**

- **TLS**
  - Does not verify server identity certificate through certificate chain in IP Office R9.1 time frame.
  - Perform Hostname validation on IP Office identity certificate.
    - Requires IP Office identity certificate containing subjectAltName extension with the following field:
      - DNS.1: IP Office's FQDN if remote E129 SIP phone is supported

                - DNS.2: IP Office's LAN IP address if local E129 SIP phone is supported.
                - SIP URI: IP Office's LAN IP address
            - Root certificate distribution
                - Not applicable
            - Fall back to TCP/UDP: when TLS connection is failed, phone would fall back to TCP if TCP is selected in “IP Office manager->system->LANx->VoIP->SIP Registrar Enable".
            - Phone configuration:
                - Auto-configuration is supported for this phone. For details, please refer to HTTPS section.
                - cfg.xml
                    - <p47>addr:port</p47> : set the port to TLS port
                    - <p130>SIP transport</p130> : set to 2 (TCP/TLS)
                    - <p2311>check domain certificate<p2311> : set to 1
            - SIPS URI
                - SIPS URI is configurable in E129 SIP phone:
                    - cfg.xml
                        - <P2329>SIPS URI</P2329> : set to 0 (SIP URI)
            - SIPS URI is not configured in E129 for IP Office R9.1 release.

    - **sRTP**
        - sRTP parameters supported:
            - Crypto suite (non-configurable): AES_CM_128_HMAC_SHA1_80, AES_CM_128_HMAC_SHA1_32
            - Encryption/Authentication flags (non-configurable): ENCRYPTED_RTP, AUTHENTICATED_RTP, UNENCRYPTED_RTCP, AUTHENTICATED_RTCP
            - Options (configurable): Disabled, Enforced (E129 does not support RFC5939 capability negotiation at this release and therefore can only support enforced sRTP).
        - Phone configuration
            - Auto-configuration is supported for this phone. Media security auto-configuration is done at system level. Extension level media security configuration is not supported for E129 in IP Office R9.1. Extension level media security configuration will be disabled in IP Office manager if the device is detected as E129.
                - cfg.xml
                    - <P183>2</P183> // sRTP mode: 0 - disabled, 2 - enabled and enforced
        - IP Office system media security maps to E129 sRTP mode:

IP Office System Media Security	E129 sRTP Options
Disabled	SRTP Disabled
Best Effort	SRTP Enabled and Enforced
Enforce	SRTP Enabled and Enforced

    - **Key negotiation**
        - E129 does not change its sRTP master key during reINVITE.
- HTTPS

- **Use of the secure https connection**
  - The secure https connection for operations like configuration files download, firmware upgrade, directory download is enforced when possible.
  - The use of the secure https connection will be determined based on the IPO's configuration under System->LAN->VoIP->Layer 4 Protocol. If the TLS transport protocol is selected, then the secure connection for config/firmware download will be enforced regardless if the phone is connected locally or it is in the remote location. If the TLS protocol is not selected then the unsecure http connection will be used. This is based on the assumption that if the secure communication is required for the SIP communications then the secure connection should also be used for the configuration/firmware download.
  - The http access for the configuration file downloads will be blocked if it is determined that the access should be secure.

- **Server ROOT Certificate installation**
  - The IPO's root certificate does not need to be installed as E129 does not perform server certificate authentication. The TLS connection is established without an authentication.

- **Phone Installation Procedure**
  - After the E129 makes the first contact with the IPO the configuration and upgrade server address and protocol are controlled by the IP Office.
  - There are some differences in installation procedure depending on the network setup where the phone is installed:

    - **The DHCP server is on the IPO (local phone installation)**
      In this scenario the DHCP reply will include option 66 set to point to the private IP address of the IPO "http://<IPO IP>".

      The phone will request its configuration file from the IPO. The IPO will disable use of the DHCP option 66 to override the configuration server (P145) and will set the firmware and configuration server path parameters (P192 and P237) to the private address of the IPO. The upgrade protocol parameter (P212) and the phonebook download protocol (P330) will be set to the "http" or "https" depending on the IPO's configuration under System->LAN->VoIP->Layer 4 Protocol. It will be set to "https" if the TLS protocol is set and to "http" if it is not set.

    - **The third party DHCP server is used (local phone installation)**
      In this scenario the DHCP server will be configured with the option 66 pointing to the private IP address of the IPO "http://<IPO_IP>" or "https://<IPO_IP>". If the DHCP server cannot be configured with the Option 66 then the phone would have to be pre-configured using phone's menu with the private IP address of the IPO "http://<IPO IP>" or "https://<IPO_IP".

      In both cases, the E129 will request its configuration file from the IPO. The IPO will disable use of the DHCP option 66 to override the configuration server (P145) and will set the firmware and configuration server path parameters (P192 and P237) to the

private address of the IPO. The upgrade protocol parameter (P212) and the phonebook download protocol (P330) will be set to the "http" or "https" depending on the IPO's configuration under System->LAN->VoIP->Layer 4 Protocol. It will be set to "https" if the TLS protocol is set and to "http" if it is not set.

- **The third party DHCP server is used (remote phone installation)**
  In this scenario the DHCP server will be configured with the option 66 pointing to the public IP address of the IPO "http://<IPO Public IP>" or "https://<IPO Public_IP>". If the DHCP server cannot be configured with the Option 66 then the phone has to be pre-configured using phone's menu with the public IP address of the IPO "http://<IPO_Public_IP>" or "https://<IPO_Public_IP".

  In both cases, the E129 will request its configuration file from the IPO. The IPO will disable use of the DHCP option 66 to override the configuration server (P145) and will set the firmware and configuration server path parameters (P192 and P237) to the public address of the IPO. The upgrade protocol parameter (P212) and the phonebook download protocol (P330) will be set to the "http" or "https" depending on the IPO's configuration under System->LAN->VoIP->Layer 4 Protocol. It will be set to "https" if the TLS protocol is set and to "http" if it is not set.

- **Static IP configuration (local phone installation)**
  In this scenario the E129 will be configured with the static IP and the configuration server should be pre-configured with the private IP address of the IPO "http://<IPO IP>" or "https://<IPO_IP>".

  In this case the E129 will request its configuration file from the IPO. The IPO will set the firmware and configuration server path parameters (P192 and P237) to the private address of the IPO. The upgrade protocol parameter (P212) and the phonebook download protocol (P330) will be set to the "http" or "https" depending on the IPO's configuration under System->LAN->VoIP->Layer 4 Protocol. It will be set to "https" if the TLS protocol is set and to "http" if it is not set.

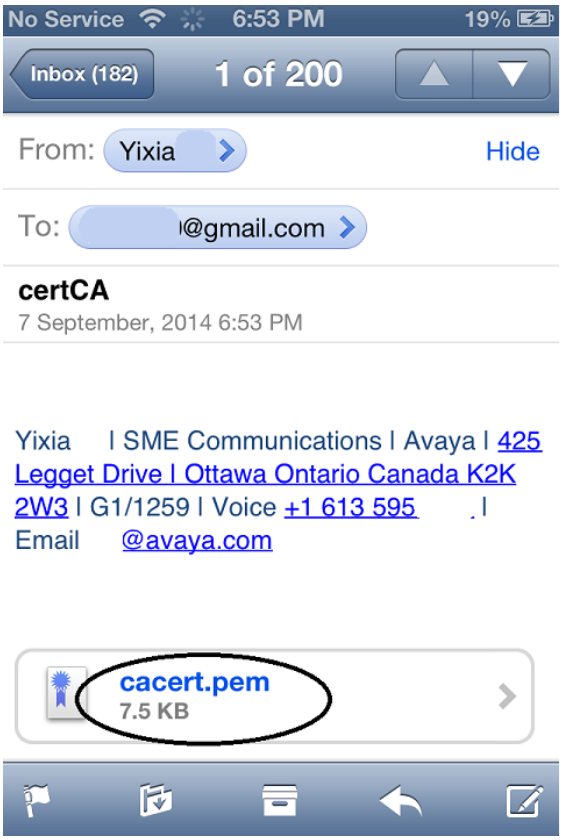
- **Static IP configuration (remote phone installation)**
  In this scenario the E129 will be configured with the static IP and the configuration server should be pre-configured with the public IP address of the IPO "http://<IPO_PUBLIC_IP>" or "https://<IPO_PUBLIC_IP>".

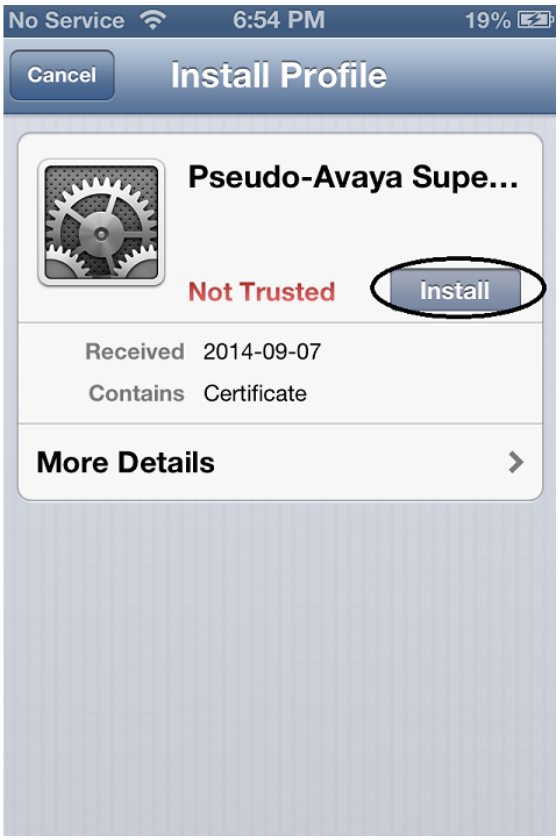
  In this case the E129 will request its configuration file from the IPO. The IPO will set the firmware and configuration server path parameters (P192 and P237) to the public address of the IPO. The upgrade protocol parameter (P212) and the phonebook download protocol (P330) will be set to the "http" or "https" depending on the IPO's configuration under System->LAN->VoIP->Layer 4 Protocol. It will be set to "https" if the TLS protocol is set and to "http" if it is not set.

- **Note**: In all the cases the file server address set on the phone will not be affected by the subsequent DHCP requests. In order for the E129 to use the option 66 from the DHCP reply again, the phone has to be reset to the factory defaults or manually re-configured using phone's menu. This mainly affects cases when the phone is moved to a different IP Office.

7.1.8 OneX Mobile Preferred iOS

- **TLS**
  - Verify IP Office identity certificate through certificate chain up to the root certificate.
    - Customer root certificate needs to be uploaded to the phone.
  - Does not perform hostname validation for SIP server in IP Office R9.1 time frame.
  - Root certificate distribution
    - Root certificate can be uploaded to the phone in the following ways:
      - Through secure email





      - Using "iPhone Configuration Utility"
  - Fall back to TCP/UDP: when TLS connection fails, phone would not register.
  - Phone configuration
    - Auto-configuration is not supported.
      Configuration using SIP client application interface:
      - Secure VoIP->Enable TLS: ON
      - Secure VoIP->Certificate Validation: ON
  - SIPS URI

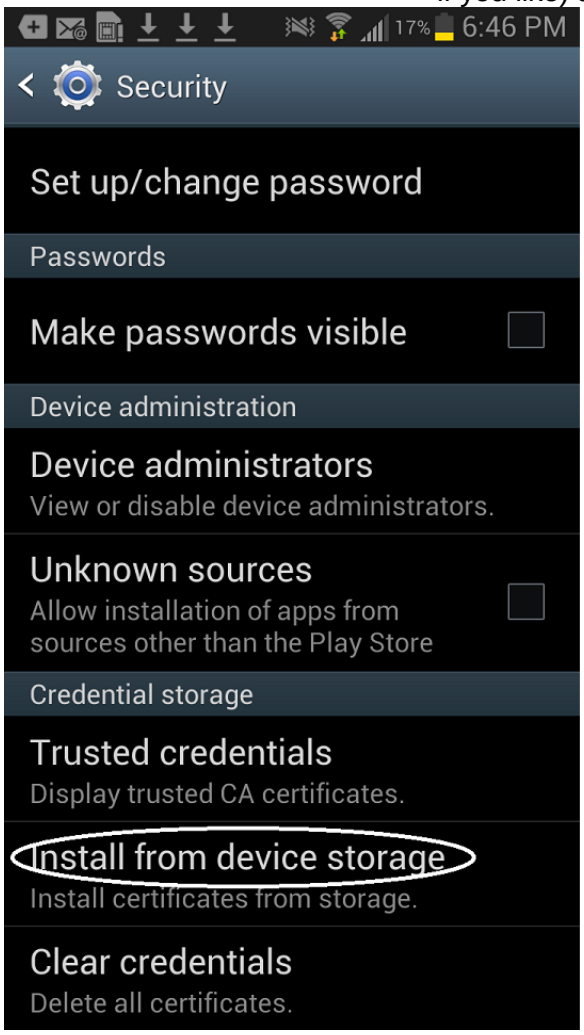
        - When TLS is selected, OneX Mobile Preferred iOS uses SIPS URI. This is not configurable.
    - Presence Server

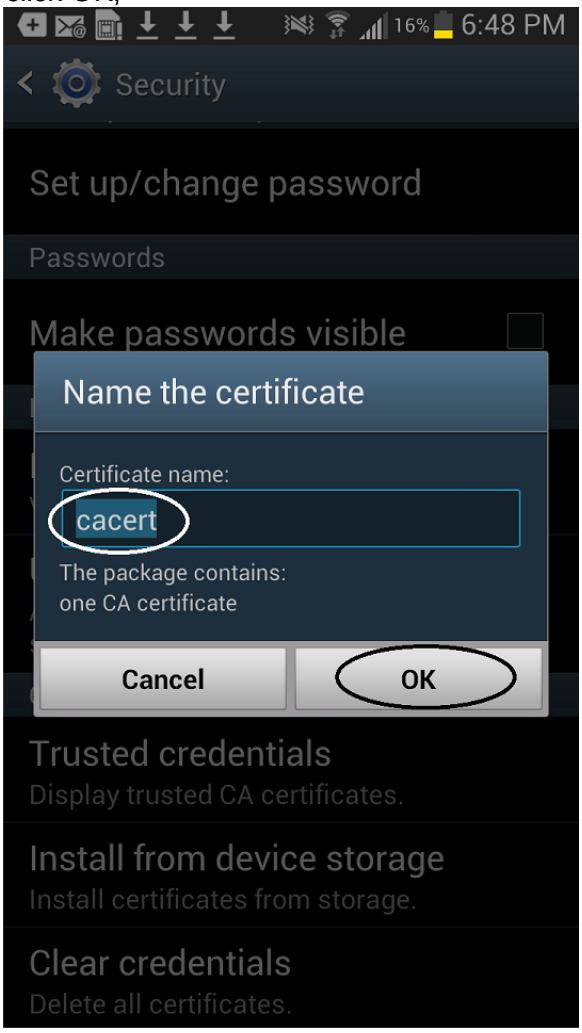
- **sRTP**
    - sRTP parameters supported:
        - Crypto suite (non-configurable): AES_CM_128_HMAC_SHA1_80, AES_CM_128_HMAC_SHA1_32
        - Encryption/Authentication flags (non-configurable): ENCRYPTED_RTP, AUTHENTICATED_RTP, UNENCRYPTED_RTCP, AUTHENTICATED_RTCP
        - Options (configurable): Never, If Available, Mandatory
    - Phone configuration
        - Auto-configuration is not supported for this phone. Most sRTP parameters are not configurable.
        - When SIP signaling is secured by TLS, best effort sRTP is always offered by oneX Mobile Preferred iOS client.
        - Extension level media security configuration is supported in stand-alone mode. It is not supported in simultaneous mode.
        - Configuration using SIP client application interface: Secure VoIP->sRTP mode->"If Available"
    - Key negotiation
        - OneX Mobile Preferred iOS client does not change its sRTP master key during reINVITE.

7.1.9 **OneX Mobile Preferred Android**

- **TLS**
    - Verify IP Office identity certificate through certificate chain up to the root certificate.
        - Customer root certificate needs to be uploaded to the phone.
    - Perform Hostname validation
        - Requires IP Office identity certificate containing subjectAltName extension with the following field:
            - DNS.1: IP Office's FQDN
            - IP.1: IP address of IP Office LAN1
            - IP.2: IP address of IP Office LAN2
            - IP.3: Public IP address of IP Office if remote oneX Mobile Preferred Android client connects to IP Office using IP Office's public address.
    - Root certificate distribution
        - Root certificate can be uploaded to the phone in the following ways:
            - Install from Android SD storage
                - Copy DER formatted root certificate (file extension needs to be .crt) onto Android phone's SD root directory.
                - Goto "Phone->Settings->Security->Certificate storage->Install from device storage".

- Accept certificate default name (or rename it if you like) and click OK;





- Verify certificate appears in "Phone->Settings->Security->Certificate storage->Trusted credentials->User" list.

- Fall back to TCP/UDP: when TLS connection is failed, phone would not register
- Phone configuration
  - Auto-configuration is not supported.
  - Configuration using SIP client application interface:
    - Advanced->Server certificate: check
    - Advanced->Advanced VoIP->Secure connection: check
    - Security Settings: Validate Server Certificate: check. Please be aware that when the server identity certificate has been successfully validated, this check box becomes disabled and the user cannot un-check it later.
- SIPS URI: OneX Mobile Preferred Android does not support SIPS URI for IP Office R9.1 time frame.
- SHA1-1024bit Certificate: OneX Mobile Preferred Android does not support SHA1-1024 bit certificate for IP Office R9.1 time frame.
- Presence Server

- **sRTP**
  - sRTP parameters supported:
    - Crypto suite (non-configurable): AES_CM_128_HMAC_SHA1_80, AES_CM_128_HMAC_SHA1_32
    - Encryption/Authentication flags (non-configurable): ENCRYPTED_RTP, AUTHENTICATED_RTP, UNENCRYPTED_RTCP, AUTHENTICATED_RTCP
    - Options (non-configurable): Disabled, BestEffort
  - Phone configuration
    - Auto-configuration is not supported for this phone. Most sRTP parameters are not configurable.
    - When "Security Connection" is selected, best effort sRTP is always offered by oneX Mobile Preferred Android client.
    - Extension level media security configuration is supported in stand-alone mode. It is not supported in simultaneous mode.
    - Configuration using SIP client application interface: Advanced->Advanced VoIP->Secure Connection: check
  - Key negotiation
    - OneX Mobile Preferred Android client does not change its sRTP master key during reINVITE.

7.1.10 **Radvision XT 4000/5000 Series**

- **TLS**
  - Verify IP Office identity certificate through certificate chain up to the root certificate.
    - Customer root certificate needs to be uploaded to the phone.
  - Perform Hostname validation on IP Office identity certificate.
    - Requires IP Office identity certificate containing subjectAltName extension with the following field:
      - DNS.1: IP Office's FQDN
      - IP.1: IP address of IP Office LAN1
      - IP.2: IP address of IP Office LAN2
  - Root certificate distribution
    - Root certificate can be uploaded to the system using web management. For details, please see phone configuration below.
  - Fall back to TCP/UDP: when TLS connection fails, system would fail to register.
    - Phone configuration:
      - Auto-configuration is not supported for this conferencing system
      - Configuration From Web Management Interface
        - Administrator Settings->Protocols->SIP
          - Transport Outbound Call: TLS
          - Use TLS: Yes
          - TLS listening port: 5061
          - Verify certificate: yes
    - Root Certificate Provisioning From Web Management Interface
    - Administrator Settings->Utilities->Certificates->TLS

- Create certificate signing request
- Download certificate signing request from Radvision system
- Upload CA to Radvision system: make sure the root CA is in PEM format.
- Upload signed certificate to Radvision system: no need for this step since client certificate is not supported in IP Office R9.1

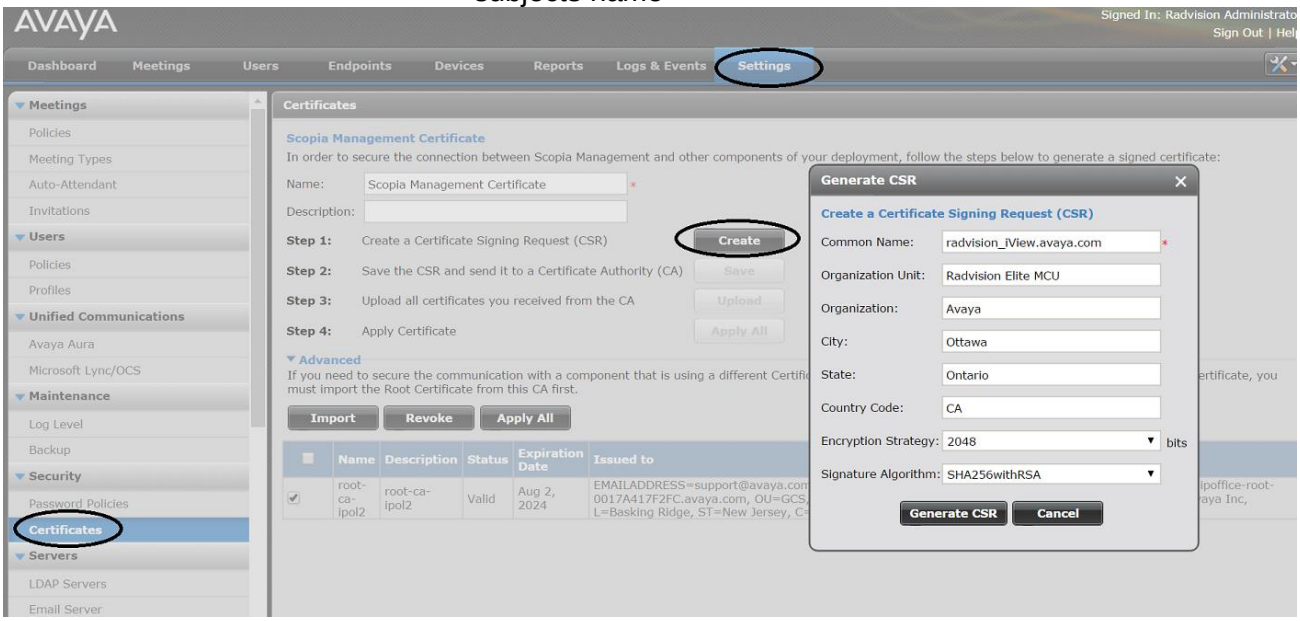
- SIPS URI
  - When TLS is selected, Radvision XT 4000/5000 uses SIPS URI. This is not configurable.

- **sRTP**
  - sRTP parameters supported:
    - Crypto suite (non-configurable): AES_CM_128_HMAC_SHA1_80
    - Encryption/Authentication flags (non-configurable): ENCRYPTED_RTP, AUTHENTICATED_RTP, UNENCRYPTED_RTCP, AUTHENTICATED_RTCP
    - Options (configurable): Disabled, BestEffort, Enforce
    - Radvision XT 4000/5000 supports (sRTP audio + RTP video) combination.
  - Phone configuration
    - Auto-configuration is not supported for this phone.
    - Configuration From Web Management
      - Administrator Settings->Calls->Encryption:
      - Enable Encryption: NO (Disabled), YES (Best Effort, Enforced)
      - Unprotected Calls:
      - Disconnect (Enforce),
      - Inform, Show Status, Ask Confirmation (Best Effort)
    - Please make sure the media security configuration above is matching the extension level media security configuration at IP Office.
    - Extension level media security configuration is supported.
  - Key negotiation
    - Radvision 4000/5000 does not change its sRTP master key during reINVITE.

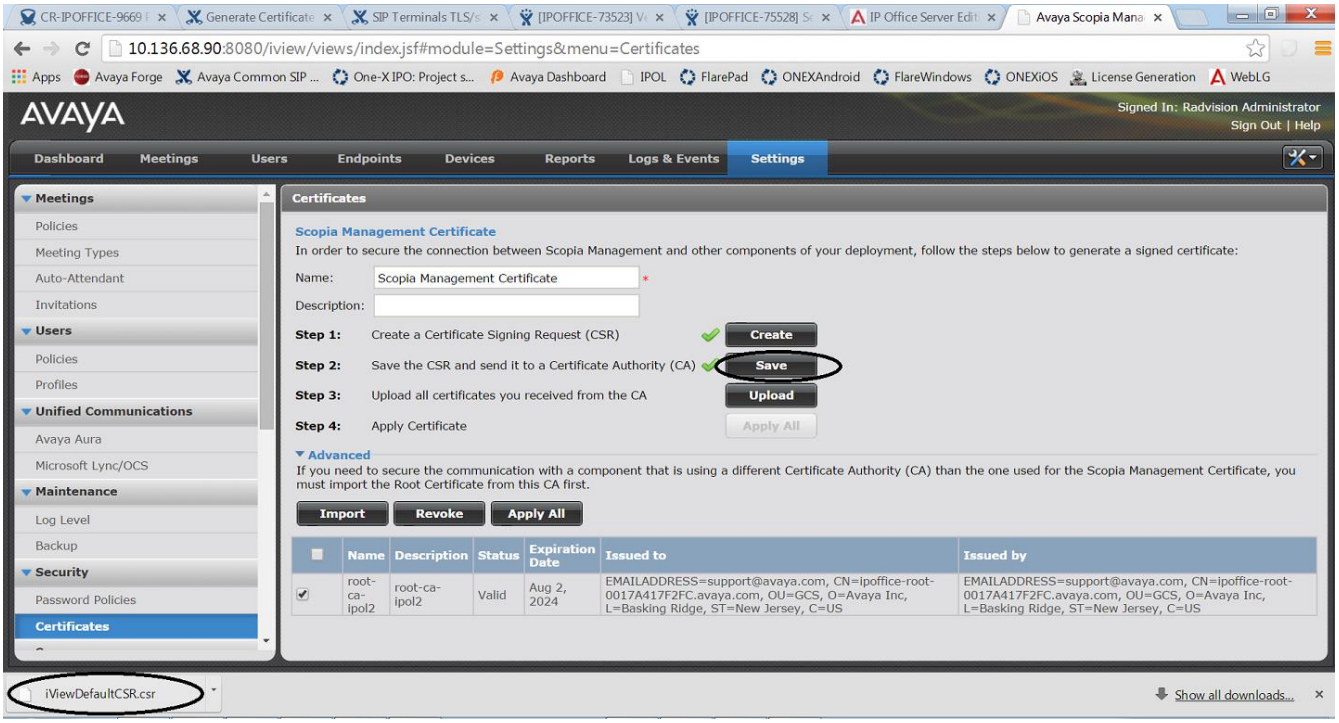
7.1.11 **Radvision Elite MCU iView Server (SIP trunk)**

- **TLS**
  - Verify IP Office identity certificate through certificate chain up to the root certificate.
    - Customer root certificate needs to be uploaded to iView server trusted certificate store under "settings->security->certificate->Advanced".
  - Does not perform hostname validation for SIP servers in IP Office R9.1 time frame.
  - Radvision Elite MCU iView Server Configuration
    - Turn on TLS
      - Devices->SIP Servers->Add
        - Transport Type: TLS

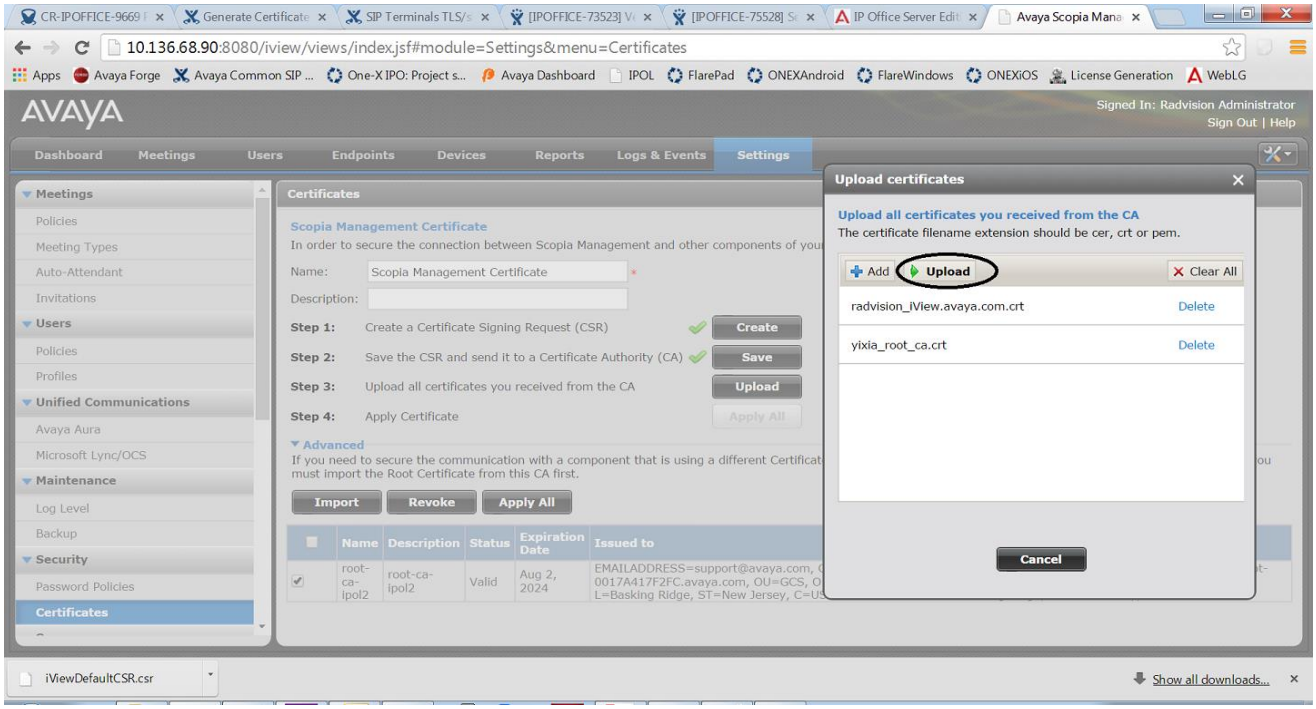
- Port: 5061
- Certificate Provisioning
  - Settings->Security->Certificates->New
  - Create certificate signing request: specify certificate subjects name



  - Download certificate signing request from iView server



- Sign the identity certificate by either
  - Sending certificate request file to certificate authority or
  - Sign the identity certificate using a certificate management tool like XCA (XCA wiki page: Managing Certificates Using XCA)
- Upload signed identity certificate and root certificate to iView server



- Apply certificate
- Settings->Security->Certificates->Advanced
  - Upload root CA used to sign IP Office identity certificate if it is different from the root certificate uploaded above.

7.1.12 **96x1 H.323 sets**

96x1 phones running H.323 software release 6.4.0 or above can be deployed to use secure interactions with IP Office.

If media encryption is enabled in the IP Office configuration then the 96x1 H.323 phones will use SRTP and secure signalling with IP Office. The phones do not use TLS for their H.323 signalling with IP Office but the H.323 signalling between the phones and the IP Office is secured by a different mechanism (referred to as Annex H).

In addition, the 96x1 H.323 phones can optionally be configured to use HTTPS over TLS, rather than HTTP over TCP, to get their settings and other files from the IP Office. This does not include the firmware files which are not downloaded by the phone over HTTPS but over HTTP.

In order for the 96x1 H.323 phones to use HTTPS over TLS with IP Office, the phones have to be provisioned with the certificate of the root CA that issued the IP Office identity certificate. This can be done by staging the phones with a different file server before installation, or by preparing the IP Office SD card to facilitate this. The file server, or the IP Office SD card, has to contain the following:

- A manually-edited 46xxsettings.txt file that includes the following setting: TRUSTCERTS <filename of root CA certificate>
- The certificate of the root CA that issued the IP Office identity certificate.

8 IP Office Release 9.1 Interoperability

With the IP Office R9.1 release a number of interoperability scenarios with other Avaya products have been tested and will be supported going forward. Refer to the Release Documentation section to download the IP Office Compatibility Matrix that covers all interoperability details. For more specific details on branch related interoperability download the IP Office Release 9.1 deployed as a Branch Product Offer document.

8.1 ASBCE and SIP Phones (1120e, 1140, 1220, 1230, E129)

SIP phone provisioning for 11xx/12xx and E129 phones does not work as expected when configured as remote workers with Avaya Session Border Controller for Enterprise (ASBCE) deployments. Specifically, the provisioning file 11xxsettings.txt for the 11xx/12xx phones (or the cfg.xml file for the E129 phone) comes from the IP Office to the phone (through corporate router) and contains information specific to the IP Office's LAN.

The SIP Server IP in the file is not the SBC public IP address, and TLS, TCP, and UDP ports are not the ASBCE ports. Also, the SRTP settings are not correct since SRTP for remote workers can differ from the IP Office SRTP settings.

The solution is to create NoUser Source Number IDs to give the IP Office the correct data to send in a configuration file for these phones.

Create the following NoUser Source Number IDs:

RW_SBC_REG	=	sbc-public-sip-ip-address
RW_SBC_PROV	=	sbc-private-HTTP-HTTPS-reverse-proxy-ip-address
RW_SBC_TLS	=	tls-port (SBC TLS port)
RW_SBC_TCP	=	tcp-port (SBC TCP port)
RW_SBC_UDP	=	udp-port (SBC UDP port)

- These IDs are applicable only to IP Office SIP ASBCE remote worker 11xx, 12xx, or E129 phones.
- If RW_SBC_REG_IP and RW_SBC_PROV_IP are not entered, other RW* source number IDs are ignored.
- One of three ASBCE ports (RW_SBC_TLS/RW_SBC_TCP/RW_SBC_UDP) port must be entered. The recommendation is to enter all relevant SBC ports.
- For 11xx/12xx phones all ports will be sent to the phone and the phone will choose the protocol to register to ASBCE in the following priority: tls, tcp, udp.
- For E129 phones IP Office will choose SBC TLS port if configured.
    - If ASBCE TLS is not configured, IP Office will choose the ASBCE TCP port if configured.
    - If an ASBCE TCP port is not configured IP Office will choose the ASBCE UDP port.
- IP Office will check whether the SIP phone provisioning HTTP/HTTPS requests are coming from the RW_SBC_PROV_IP address.
    - In this case IP Office will send RW_SBC_REG_IP to the phone as a SIP Server for E129 (or S1/S2 for 11xx/12xx).
    - For E129 phones outbound-proxy filed is used to provide RW_SBC_REG_IP.
    - In addition, Config path, Provisioning path, and Phonebook path are removed from the cfg.xml file for IP Office ASBCE remote workers

because they must be manually configured by the administrator once before moving E129 phones to the remote location on ASBCE public side.

- It is strongly recommended to use a homogeneous protocols configuration:
  - If TLS is used between remote workers and ASBCE then TLS should be used between ASBCE and IP Office
  - If TCP is used between remote workers and ASBCE then TCP should be used between ASBCE and IP Office
  - If UDP is used between remote workers and ASBCE then UDP should be used between ASBCE and IP Office
  - If SRTP is used between remote workers and ASBCE then SRTP should be used between ASBCE and IP Office
  - If RTP is used between remote workers and ASBCE then RTP should be used between ASBCE and IP Office

8.2 IPO Office Deployed as an Aura Branch

8.2.1 Key Branch Functionality (additions for IP Office R9.1 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)
  - Release 9.1 introduces Centralized Management of IP Office Application Server, UCM and VMPro,
- PLDS Licenses and centralized licensing by WebLM
  - Release 9.1 introduces separate SM trunk channel license , Branch System license and WebLM 9.1 Model license
- 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
  - Changes to location where System-wide SRTP is configured
  - Additional IP Office endpoints supported with TLS/SRTP in Release 9.1
- Support for SIP Centralized Users
  - Release 9.1 adds support for E129 as a centralized User phone
- Support for Analog Trunk Adaptation
  - Release 9.1 enhances Centralized feature set available to ATA users as well as adds fax capability for ATA
- Release 9,1 introduces support for India Toll-bypass restrictions in concert with Avaya Aura CM

8.2.2 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

8.2.3 **Branch Deployment Restrictions**

- Branch functionality is available in IP Office Standard mode on the 500V2 platform
    - 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
        - SE does not support the *Branch* functionality of SMGR management, WebLM licensing, Centralized Users or voicemail over 'SM Line'
    - The branch functionality is not available in IP Office Basic Edition
- 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 and WebLM licensing of SCN are 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

8.2.4 **Aura Load Line up**

Name	**Avaya Aura "Standard" solution**	**Avaya Aura MidSize Enterprise Solution**
vsp	latest needed for each platform	latest needed for each platform
System Manager	6.2 FP4 SP2 (6.3.10.7.2683)	6.2 FP4 SP2 (6.3.10.7.2683)

Session Manager	GA 6.2 FP4 SP1 (6.3.9.0.639011)	GA 6.2 FP4 SP1 (6.3.9.0.639011)
Communication Manager	6.2 FP4 SP2 (03.0.124.0-21920))	6.2 FP4 SP2 (03.0.124.0-21920))
CM Messaging	6.3 SP3 (03.0.124.0-0304)	6.3 SP3 (03.0.124.0-0304)
Utility Server	GA 6.3 SP5 (6.3.5.0.20)	GA 6.3 SP5 (6.3.5.0.20)

8.2.5 Issues in Centralized licensing

JIRA	Description	Impact	Mitigation
IPOFFICE-77721	SCALE: High rate of Alarms makes SMGR unusable	If the SMGR is handling high number of IPOs (appr 500 IPOs and 12000 users)	Make sure only Critical alarms are configured to be reported on IPO.

8.2.6 Issues in Speech Path

JIRA	Description	Impact	Mitigation
IPOFFICE-75006	SRTP: One way speech path when ATA user does a supervised transfer across branches	Affect call redirections from ATA phones	Do not configure ATA on Branches where we are testing SRTP

9 Known Issues

The following is a list of issues and workarounds, if available, that exists in this release of IP Office R9.1 software and where applicable will be addressed in a future release of software.

Key	Release Note
IPOFFICE-80617	Issue: In branch deployment with SRTP and ATA users, call might fail if transferred by ATA user. The issue only occurs if a Nortel Ethernet Routing Switch 4526T-PWR having following specifications is used: HW: 11 FW:5.1.0.8 SW:v5.4.0.008 BN:08 (c) Nortel Networks is used Platforms affected: IP500v2 The only workaround is to eliminate or upgrade the ethernet switch.
IPOFFICE-75006	Issue: In branch deployment with SRTP and ATA users, call might fail if transferred by ATA user. The issue only occurs if a Nortel Ethernet Routing Switch 4526T-PWR having following specifications is used: HW: 11 FW:5.1.0.8 SW:v5.4.0.008 BN:08 (c) Nortel Networks is used Platforms affected: IP500v2 The only workaround is to eliminate or upgrade the ethernet switch.
IPOFFICE-80318	Issue: In the IPO Branch configuration, when using local SIP Trunks and centralized Avaya Aura Messaging with local call flows within the Branch handled by Embedded Voice Mail (EVM) digits for transfers to AAM from the local EVM call flow are not transmitted to the AAM. Workaround: do not use a combination of local EVM based call flows with centralized AAM with local SIP Trunks. This scenario does work if the local trunks are digital trunks (PRI)
IPOFFICE-80564	When a SIP Terminal has a current call and TAPI messaging is used to put the current call on hold and a new call is initiated and is not in the connected state, the new call will not be dropped if the held call is unheld.. The only endpoints where this will work correctly is the counterpath softphone and 1100/1200 SIP phones.
IPOFFICE-80803	The voice from other end is being heard distorted when answering a call waiting from IP DECT. Workaround it to unset Direct Media on DECT line.
IPOFFICE-80666	Sometimes Call Waiting doesn't work for DECT R4 and parties have one way speech path. Workaround is to enable Direct Media on IP Dect Line
IPOFFICE-80350	IP DECT Line parameters are not propagated over SCN when Manager uses save with merge (without reboot) Workaround is to reboot the secondary IPO in order to get the config.

Key	Release Note
IPOFFICE-81237	Description: ACCS TFQ feature is enabled. An outage occurs on IP Office Primary, ACCS switches over from the IP Office Primary to the IP Office Secondary. The IP Office Primary then comes back online, ACCS remains registered with the IP Office Secondary. At this point any local users (local to IP Office) that make calls to ACCS will not hear media treatments that are streamed by ACCS prior to ACCS connecting the incoming early media call. At this point any local users (local to IP Office) that make calls to ACCS will not hear media treatments that are streamed by ACCS prior to ACCS connecting the incoming early media call. Impact: Local callers will not hear treatments such as Play Prompt IVR, RAN, Music, Ring back that are streamed from the Contact Center via scripting prior to connect of the call. Note: Play and Collect IVR will be heard as this requires a connect of the incoming call Workaround: Revert the ACCS back to the IP Office Primary (it is back in service)
IPOFFICE-80138	This bug occurs when the central server providing the voicemail reboots. It occurs when there is a triangle in the network, so an expansion system can be reached directly or via (eg) the secondary. If the link to the secondary comes up well before the link to the expansion, the primary may ask the secondary to forward details about the expansion users. This would be standard resilience functionality, but represents a problem if this is the first contact between the primary and the expansion users. There is no reliable work-around. There is also no simple indicator of the problem existing, without testing a mailbox. If you configure a set of distributed huntgroups on the primary containing all the users on each expansion, you should be able to recover the situation by dialling the appropriate huntgroup. The users do not all have to ring. It could be a sequential group, and you only have to let it ring for 5 seconds.
IPOFFICE-80282	A DECT user from Primary won't be able to be hot-desked on Secondary
IPOFFICE-78961	*Issue description* : When using Generic Actions in a VMPro call flow to set huntgroup configuration changes or using TUI to change huntgroup mailbox settings (i.e. VM mailbox password), the following huntgroup configuration settings will be changed to incorrect values: - _service mode_ - _broadcast_ - _source number list_ - _ex-directory_ *Workaround* : Enable outcalling setting for the huntgroup for which the configuration settings are being changed. NOTE: The problem appears only when using VMPro as VM solution, not reproducible on EVM.
IPOFFICE-80605	Some Kingston USB3.0 FLASH devices don’t work in UCMv2 top USB Port Workaround: Use a different USB FLASH device or use the bottom USB Port to install UCMv2 software

Key	Release Note
IPOFFICE-75895	Upgrade of IP 500v2 standard mode via Web Manager fails from 9.0.3 to 9.1.0. Please use the IP Office Manager for upgrade from R9.0 to R9.1 for IP500V2 standard mode.
IPOFFICE-73661	16xx phones cannot establish a TLS connection to IPOffice to retrieve the settings files. To avoid seeing the alarms in SSA, a No User Source Number can be added: SUPPRESS_TLS_ALARM_PORT=411. This suppresses all TLS alarms on port 411.
IPOFFICE-76838	Issue Description: Web Management Embedded File Manager does not handle files larger than 2MB Platform: ip500v2 Workaround: File management in Web Manager is a new feature in ipoffice 9.1 and it has limitation of uploading max. 2MB of file. So use the existing feature of ipoffice Manager Embedded File Management to manage files.
IPOFFICE-81276	When SE Select system with PLDS licenses is restarted, System Status application will show four cleared SE license related alarms in Alarms | Service. Workaround is to ignore these alarms since they are cleared (in black text and not red), subsequently the alarms can be removed in System Status application with “Clear All” button.
IPOFFICE-81165	Issue: When using the 9.1 Manager to manage a 9.0 config, the group Night Service radio button is not visible. The workaround is to use the 9.0 version of the manger to manage the config or to upgrade the 9.0 system to 9.1
IPOFFICE-81325	As per the IPO Manager help (for groups), if a user is added to an XMPP group then that user can only see presence from other users in that same XMPP group. If an administrator wants to each user to see the presence of any other user then he/she can create an XMPP group that contains all users. Note that if the number of users is large then this will result in increased mobility client network traffic and server load.
IPOFFICE-80840	In non-cloud deployment of IP Office Server Edition, the expansion nodes should be reachable from one-X server machine on port 50814 and 50802. The nodes will have to be provisioned with one-X if auto provisioned is not enabled.
IPOFFICE-80551	In the context of One-X Portal auto provisioning, when we add a secondary to the solution post upgrade, the CSTA provider entry is not shown in one-X admin console. After a restart of the one-x portal service this provider is now present. So it seems provider was properly configured at first place but entry was not shown in one-X ‘component status’ at admin console. No impact to the user
IPOFFICE-77735	After upgrading one-X Portal for IP Office to 9.1 release, when one-X Portal Admin application is accessed for the first time, the Local one-X Administrator Password will have to be changed if the previous password is default (i.e. Administrator) or blank.
IPOFFICE-81248	The XMPP domain name (DNS name/IP address) configured in the one-X portal should not be configured in the OS host configurations pointing back to localhost/127.0.0.1/loop back address.

Key	Release Note
IPOFFICE-76452	An Avaya Communicator for iPad user attempting to use the same credentials on two different iPads will have difficulty switching back and forth between the iPads if the IP Office is protected by an Avaya Session Border Controller for Enterprise (ASBCE). The problem arises if the user does not log off from the Avaya Communicator on one iPad before logging in on Communicator on a different iPad. Ordinarily the first user would be automatically logged out on the first iPad. The problem occurs when the user does not log out from Communicator on the second iPad but moves back to the first iPad and logs in to Communicator there. In this case no logout notification is sent to the second iPad, and the Communicator on the second iPad thinks that it is still registered. This problem only occurs if the IP Office is protected by an Avaya Session Border Controller for Enterprise (ASBCE). To work around this limitation it is recommended that users who wish to use the same credentials on multiple Avaya Communicator clients log off from Communicator on one device before logging in on another device.
IPOFFICE-75173	After encountering exception when switching between categories, user can still do the shortcut key mapping by closing and relaunching 'User Preferences' dialog.
IPOFFICE-79050	Issue: System Status Application (SSA) cannot connect over modem in secure mode. Workaround: Use SSA over modem in “insecure” mode. In the login SSA window simply uncheck the “Secure connection” checkbox and connect to IP Office over modem.
IPOFFICE-78269	If IP Office Web Manager for R9.0 is accessed from browsers and from the same browser Web manager for IP Office upgraded to R 9.1 is accessed the screens will have abrupt text. After upgrade please clear the cache of the browser.
IPOFFICE-81226	The IP Office Web Manager remains stuck in the Loading state when trying to create an extension template. The Administrator should create a new extension or edit the existing extension and then save it as template.
IPOFFICE-80926	Using IP Office Web Manager the Phone Password for H.323 extension is not getting saved correctly. If Administrator has to set the Phone Password for H323 extension then the IP Office manager thick client should be used.
IPOFFICE-81102	At the end of the upgrade process for Secondary server or IP Office Linux expansion the system will be rebooted and can take up to 20 minutes to completely restart while the software is being installed.
IPOFFICE-81236	The “system” password is not synchronized on initial manual synchronization operation in Web Management | Security Manager. The workaround is to repeat the manual synchronization or enable auto synchronization after the initial manual synchronization is done.
IPOFFICE-81162	The IP Office Web manager self Administration force user to change the password if it is not matching the password complexity. Once end user changes the password, the application does not logged out the user. But the user should logged out from the application and re-login again to make further changes.
IPOFFICE-81220	Issue: When using Web Manager Self Admin to add buttons to your phone, the view of the added buttons in Web Manager Self Admin is incorrect. These buttons do appear correctly on the phone and within Manager/Web Manager. If a new button is subsequently added via the Web Manager Self Admin, the previous buttons are deleted. Workaround, use Manager/Web Manager to admin buttons on the phone rather that the Web Manager Self Admin tool

Key	Release Note
IPOFFICE-81223	Issue: When using Avaya Communicator for Windows, if the user's name contains a space character, the Web Collaboration button is grayed out and cannot be used. If the user's name does not contain any space characters, for example "Extn202", the web collaboration button is active. Web collaboration for the same user works fine if it's initiated from the browser using the web collaboration url, or if it's started from One-X Portal using the designated button.

10 Demo Kits

Refer to the Release Documentation section to download the IP Office Release 9.1 Product Update document which provides demo kit details.

11 Logistics and Ordering

Refer to the Release Documentation section to download the IP Office Release 9.1 Product Update document which provides logistics and ordering details including:

- IP Office R9.1 DVD Sets
- IP Office System SD cards
    - Also refer to the Release Documentation section for details to download the IP Office Release 9.1 deployed as a Branch Product Offer document.
- IP Office Release License
- Software Pricing
- IP Office Software Applications and License Key Process

12 Avaya Global Services

Refer to the Release Documentation section to download the IP Office Release 9.1 Product Update document which provides Avaya Global Services details including:

- IP Office Software Availability
- Avaya Maintenance, Lifecycle and Warranty Information
- Additional Avaya IP Office Support Services Information

For details on service options available for IP Office based branch solutions, refer to the Release Documentation section for details on how to download the IP Office Release 9.1 deployed as a Branch Product Offer.

13 IP Office Credentials and Avaya University Training

Refer to the Release Documentation section to download the IP Office Release 9.1 Product Update document which provides IP Office Credentials and Avaya University Training details.

For details on credentials and available training required in support of IP Office based branch solutions please refer to the Release Documentation section for details to download the IP Office Release 9.1 deployed as a Branch Product Offer.

Issued by:
Avaya SMEC Technology

Contact details:-
EMEA/APAC

*Email: **gsstier4@avaya.com***

NA/CALA

*Email: **iponacalat4@avaya.com***

*Internet: **http://www.avaya.com***