IP Office Technical Bulletin

Bulletin no: **90**

Date: 17th December 2007

Title: General Availability (GA) of IP Office 4.1 Software

Table of Contents

1 Product Overview 4
2 IP Office Hardware 6
2.1 IP500 Universal PRI Daughter Card (not available in all territories) 6
2.2 New IP500 Expansion Modules 8
2.3 New 3641 and 3645 IP Wireless (WiFi) Phones 10
2.4 Simplified IP DECT Licensing 12
3 IP Office Software Enhancements 13
3.1 VPN Phone support in 4600 and 5600 Series IP Phones 13
3.2 Embedded Voicemail Enhancements 17
3.3 Internal Twinning of Appearance Keys 20
3.4 Tagging on Incoming Call Routes 21
3.5 Time of Day and Date Routing of calls 21
3.6 Time Profile Support on Incoming Call Routes 22
3.7 Queue Threshold Alert 22
3.8 Security Enhancements 23
3.8.1 Transport Layer Security (TLS) 23
3.8.2 Enhanced Password Policy 29
3.8.3 Additional Manager Security Changes 34
3.9 Syslog support 34
3.10 Disable Speakerphone 34
3.11 Group Listen 35
3.12 Manager Start-Up Banner 35
3.13 Manager Warning Dialogue 36
3.14 LAN2 Interface on port 8 of the IP406v2 37
3.15 Force Feed in Headset Mode 38
3.16 Local Administration Enhancements 38
3.17 Avaya SIP for Branch 38
3.18 Recording Enhancements 43
3.19 Abbreviated Ring 43
3.20 TAPI Enhancements 43
3.21 Enhanced Meet Me Conferencing 44
3.22 Extension Number / Base Extension Number Mergeable 44
3.23 Small Community Networking on IP500 45
3.24 System Status Application Enhancements 45
4 IP Office Applications 46
4.1 VoiceMail Pro 46
4.1.1 Call Transfer Announcements 46
4.1.2 Call Transfer Data Tagging 47
4.1.3 LIFO/FIFO Message Playback 47
4.1.4 Queuing Enhancements 47
4.1.5 Variable Routing Action 48
4.1.6 Castelle Fax Server Support 49
4.1.7 Connection Tool 49
4.2 Phone Manager Pro Telecommuter Mode 49
5 Windows Operating System Support 53
6 Issues Resolved in IP Office 4.1 Software 54
7 Known Issues 57
8 Technical Notes 59
8.1 Upgrade Installation Notes 59
8.2 IP Office 4.1 Admin Suite Upgrades 60

8.3 Core Software Upgrade Instructions 63
8.4 Unit Compatibility - Expansion Unit Interoperability 65
8.5 Phone Firmware Support 65
8.6 IP DECT Firmware Support 65
8.7 VoiceMail Pro Software Upgrade Summary 66
8.8 Upgrading from 2.1 / 3.0 / 3.1 VoiceMail Pro 66
8.9 Upgrading from 3.2 / 4.0 VoiceMail Pro 70
8.10 IP Office User Applications Software Upgrade Summary 71
8.11 Upgrading from 2.1 / 3.0 / 3.1 User Applications 72
8.12 Upgrading from 3.2 / 4.0 User Applications 72
8.13 Delta Server Upgrade 73
9 Assistance 73
9.1 Documentation 73
9.2 Software 73
9.3 IP Office Technical Training 74

IP Office Technical Bulletin

Bulletin No: 90

Date: 17th December 2007

Region: GLOBAL

General Availability (GA) of IP Office 4.1 Software

Avaya is delighted to announce the launch and availability of IP Office 4.1 software. IP Office is Avaya's Small and Medium Enterprise (SME) solution designed as a global solution for customers with up to 360 extensions and 240 trunks.

1 Product Overview

The Avaya IP Office 4.1 software is the latest advancement in converged voice and data technology from Avaya. IP Office combines high-end voice and data applications, allowing the smallest of businesses to deliver cutting edge customer service.

IP Office 4.1 is the entry-level software to support the following new hardware:

- **IP500 Universal PRI Daughter Card**
- **New IP500 Expansion Modules**
- **New 3641 and 3645 IP Wireless (WiFi) Phones**
- **Simplified IP DECT Licensing**

As well as increased reliability through improvements to the core system software, IP Office 4.1 also supports the following new features:

IP Office Core Software (Version 4.1.9)

- VPN Phone support in 4600 and 5600 Series IP Phones
- Embedded Voicemail Enhancements
- Internal Twinning of Appearance Keys
- Tagging on Incoming Call Routes
- Time of Day and Date Routing of calls
- Queue Threshold Alert
- Security Enhancements
- Syslog Support
- Disable Speakerphone
- Group Listen
- Manager Start-up Banner

- Manager Warning Dialogue
- LAN2 Interface on port 8 of the IP406v2
- Force Feed in Headset Mode
- Local Administration Enhancements
- Avaya SIP for Branch
- Recording Enhancements
- Abbreviated Ring
- TAPI Enhancements
- Enhanced Meet Me Conferencing
- Extension/Base Extension Mergeable
- Small Community Networking on IP500
- System Status Application Enhancements

- **IP Office VoiceMail Pro (Version 4.1.27)**
  - Call Transfer Announcements
  - Call Transfer Data Tagging
  - LIFO\FIFO Message Playback
  - Queuing Enhancements
  - Variable Routing Action
  - Castelle Fax Server Support

- **Phone Manager (Version 4.1.14)**
  - Phone Manager Pro Telecommuter Mode

****

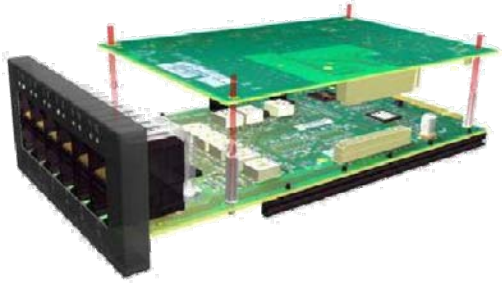
Note: *IP Office 4.1 is not supported on the IP401, IP403, IP406v1 and early IP406v2 systems that only have 16mb of memory. If your IP406v2 unit does not meet the minimum requirements then there is a procedure in place to enable you to upgrade these units free of charge. Please refer to the Technical Notes section of this document for further details.*

****

2 IP Office Hardware

2.1 IP500 Universal PRI Daughter Card (not available in all territories)

IP Office 4.1 supports a new universal PRI daughter card for the IP500 hardware platform. The daughter card is installed onto an IP500 base card (Phone, DS or VCM but not the Legacy Card Carrier). The new card provides greater flexibility in configuration owing to being a daughter card and therefore not taking up a slot in the IP500 chassis as the Legacy Card Carrier does. Up to 4 IP500 universal PRI cards can be installed into the system expanding the trunk capacity of the IP500 to a maximum 240 E1 or 196 T1 channels.



The Universal PRI card is available in single and dual circuit varieties and supports both T1 (1.544Mbps) and E1 (2.048Mbps), with DSP resources to support CAS (Robbed bit and R2) signaling. For a Dual universal PRI card both circuits must be of the same basic type: T1 or E1, E1 and E1R2. T1RBS and T1PRI may be mixed. The card also offers protected test-points via RJ45 connectors to allow the monitoring of the PRI line without disrupting the connection.

To provide lower pricing the channels on the Universal PRI card are licensed and will initially support 8 channels per circuit without the need for a license key. Any additional channels above this number will require a license key, available in 2 and 8 channel increments, to enable them. The Additional Channels license will specify the number of channels that may be supported on circuits over and above the initial 8. This licensing will not apply to IP400 PRI Trunk cards fitted to a Legacy Carrier Card.

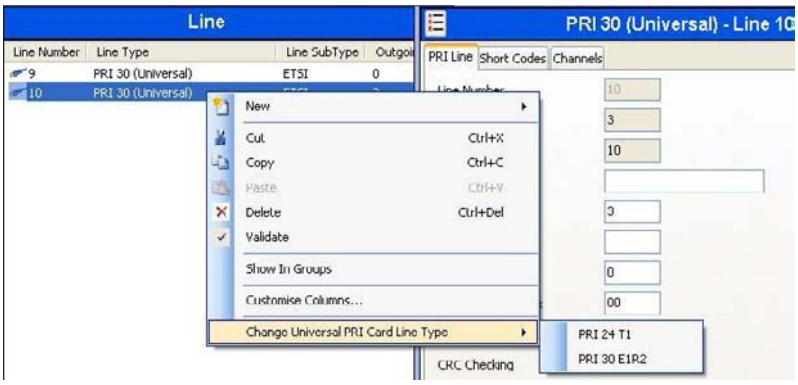
Additional channels licenses are consumed by the number of configured channels on each circuit, over and above the initial 8, starting from the first circuit (port number 9) on the first card (number 1 - left hand side). Then onto the second circuit on that card if it is a dual, then on to cards 2, 3 and 4. If a circuit has less than 8 channels configured the difference between the number configured and 8 will not be added to the additional channels count.

For a single Universal PRI card the line is connected on port 9 and the associated monitoring port is port 11. For a dual Universal PRI card the lines are connected on ports 9 and 10 with the associated monitoring ports being ports 11 and 12 (9 → 11, 10 → 12).

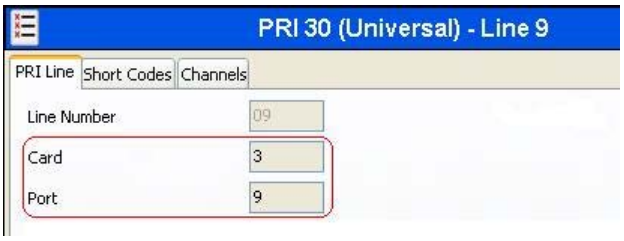
The LEDs on ports 9 and 10 act as Link state indicators and have the ability to show connected, in use, AIS, and Loopback state, the same as IP400 PRI cards on a Legacy Carrier Card.

Link State	1st Circuit (LED 9)	2nd Circuit (LED 10)
Link Detected	Green On	Green On
AIS	Red/Green Fast Flash	Green Fast Flash
In Use	Green Slow Flash	Green Slow Flash
Loopback	Red with Green Blink	Green Blink
No Link	Off	Off

The Line Type will default to T1 for IP Office systems with a U-Law Smart Card, otherwise E1 will be the default. The Line Type (T1, E1 or E1R2) for the universal PRI can be changed by a new option on the right click context menu when a Universal PRI line is selected.



The IP Office Manager has been enhanced to indicate the Module and Socket/Port number for each Line on the system. For example the first trunk on Card 2 is called Line 5. In release 4.1 this is enhanced to include the physical address as printed on the hardware; "Card 2, Port 9" similar to extensions.



This will apply for all physical Trunks, including:

- IP400 trunk cards on legacy carriers.
- IP400 trunk cards in IP400 control units.
- Analogue Trunk 16 Expansion Modules.

A validation rule has also been added to Manager to produce an error if an IP Office system has digital trunks without at least one having its Clock Quality set to “Network”. In order to have a stable synch source every system with digital trunks should have one trunk set to supply synchronization.

IP500 Universal PRI Daughter Card Availability

Owing to the extended product approval processes, the IP500 Universal PRI Daughter card may be delayed in the following countries: Argentina, Hong Kong, India, Mexico, New Zealand and South Africa.

IP Office 500 hardware and license codes will not be orderable in these countries until product approvals are complete. Please check with your local Avaya representative for information about the IP500 Universal PRI availability. This does **NOT** affect the availability of Release 4.1 software for existing platforms.

There are no plans to obtain product approvals for the IP500 Universal PRI cards in the following countries: Brazil, Korea and Taiwan.

2.2 New IP500 Expansion Modules

Avaya has introduced new versions of the following IP Office expansion modules. They are functionally identical to the existing IP400 versions but have been refreshed in the look and feel of the IP500 (dark gray color) and require the IP500 rack mounting kit. New modules:

- IP500 DS 16
- IP500 Phone 16
- IP500 Analog Trunk 16 (North American version)
- IP500 BRI So8

These new expansion modules work with IP406v2 and IP412 control units, as well as the IP500.

Updated IP Office Control Unit Comparison

Feature	Small Office Edition	IP406 V2	IP412	IP500
Digital Station (DS) Ports	0 or 8	8	0	Up to 24
Analog Phone (PHONE) Ports	2 or 4	2	0	Up to 32
Optional Embedded Voicemail Card Slot	✓	✓	✗	✓
Integral WAN Ethernet Port (LAN 2)	✓	✗	✓	✓
Integral WAN Serial Port (X21/V35)	✗	✓	✓	✗
Expansion Ports	0	6	12	8
DTE Port	9-way	9-way	9-way	9-way
Audio In (MOH) Port	✓	✓	✓	✓
External O/P Switch Port	✓	✓	✓	✓
Conference Parties (max participants)	6	64	2 x 64	64
Maximum Extension Capacity	**28**	**190**	**360**	**272**
Digital (DS) Phones only	8	188	360	264
Analog Phones only	4	182	360	272
IP Phones only	16	190	360	272
IP400 Trunk Cards Supported	**1**	**2**	**2**	**2***
Analog trunk cards	✗	✓	✓	✓
Quad BRI trunk cards	✓	✓	✓	✓
Single PRI trunk cards	✓ (T1)	✓	✓	✓
Dual PRI trunk cards	✗	✓ (Slot A only)	✓	✓
Serial WAN port card	✓	✗	✗	✗
IP500 Daughter Cards	**0**	**0**	**0**	**4**
IP500 Analog trunk card	✗	✗	✗	✓
IP500 BRI trunk card (4 or 8)	✗	✗	✗	✓
IP500 Universal PRI trunk card	✗	✗	✗	✓
VCM Cards				
IP400 VCM Cards	✗	1	2	2*
IP500 VCM Cards	✗	✗	✗	2
Maximum voice compression channels	3 or 16	30	60	128
Data Channels	**18**	**40**	**100**	**48**
Useable for Voicemail Pro/TAPI WAV	10	20	30	30
Dimensions				
Height x Width x Depth	76x255x241mm 3"x10"x9.5"	71x445x245mm 2.8"x17.5"x9.7"		73x445x365mm 2.9"x17.5"x14.4"

✓ - "supported"
✗ - "not supported"

* Requires the IP500 Legacy Card Carrier

Material codes for the IP Office 500

The following table lists the new material codes for the IP500 Universal PRI Card, Universal PRI additional channel licenses and new expansion modules.

Material Code	Description
700417439	IPO 500 TRNK PRI UNI SINGLE
700417462	IPO 500 TRNK PRI UNI DUAL
215180	IPO LIC IP500 T1 CHANNELS ADD 2
215181	IPO LIC IP500 T1 CHANNELS ADD 8
215182	IPO LIC IP500 T1 CHANNELS ADD 32
215183	IPO LIC IP500 E1 CHANNELS ADD 2
215184	IPO LIC IP500 E1 CHANNELS ADD 8
215185	IPO LIC IP500 E1 CHANNELS ADD 22
215186	IPO LIC IP500 E1R2 CHANNELS ADD 2
215187	IPO LIC IP500 E1R2 CHANNELS ADD 8
215188	IPO LIC IP500 E1R2 CHANNELS ADD 22
700449473	IPO 500 EXP MOD ANLG TRNK 16
700449499	IPO 500 EXP MOD DGTL STA 16
700449507	IPO 500 EXP MOD PHONE 16
700449515	IPO 500 EXP MOD BRI SO8

Note: *For configurations using common channel signaling, the D-channel is always enabled and does not consume a license. So the card by default supports 8 B-channels plus one D-channel.*

2.3 New 3641 and 3645 IP Wireless (WiFi) Phones

The new 3641 and 3645 IP wireless (WiFi) phones are supported on IP Office Release 4.1 in all regions where available. Please contact your local Avaya representative to establish local availability.

3641

3645

These handsets support the following:

- 128 x 96 backlit display with icons and line-status indicators
- Standard Battery – 4 hours talk time, 80 hours standby time
- Optional Extended Battery – 6 hours talk time, 120 hours standby time
- Optional Ultra-Extended Battery – 8 hours talk time, 160 hours standby time
- 802.11a, 802.11b, and 802.11g standard-compatible
- Dust, shock and liquid damage resistant
- Headset jack (2.5mm)
- Speakerphone
- Audible and vibrating alerting
- Push-to-talk (3645 only)

Avaya WiFi telephony relies on special WiFi infrastructure that in combination with the Avaya Voice Priority Processor can assure best of class Quality of Service and battery run time. For details on supported infrastructure please go to:

http://www.spectralink.com/products/netlink/interfaces/wifi.jsp

A WiFi site survey should be done before installation to ensure sufficient network coverage and to guarantee reliable functionality. If a technical ticket is raised against these products Avaya Tier3 support will ask for the site survey results if any voice-quality issues are raised. We recommend that the planning and installation team has a deep understanding of WiFi infrastructure. Avaya recommends CWNA certification or a similar level of expertise.

Please refer to: http://www.cwnp.com/cwna/ for more details.

The Avaya Wireless phones have received type approval in many regions. Currently the 3641 and 3645 and the Classic phones have type approval in North America (US and Canada) and Europe (all countries where the “CE” mark is recognized including all of the EU).

The Classic phones in addition have type approval in some CALA and APAC regions. APAC certification is in planning for the new 3641 and 3645 phones. Please contact your Avaya representative to establish local availability if in doubt.

Material codes for the 3641 and 3645 phones are as follows:

Material Code	Description
700430408	AWTS 3641 WRLS PHONE
700430416	AWTS 3645 WRLS PHONE
700436736	AWTS 3641 Single Charger Bundle- includes phone, standard battery and single charger
700436744	AWTS 3645 Single Charger Bundle- includes phone, single charger and standard battery
700436751	AWTS 3641 Dual Charger Bundle- includes phone, dual charger and two extended batteries
700436769	AWTS 3645 Dual Charger Bundle- includes phone, dual charger and two extended batteries

Material codes for AVPPs, SMB Bundles, phones, power supplies, batteries, chargers and accessories can be found in the IP Office Release 4.1 Product Update.

2.4 Simplified IP DECT Licensing

In IP Office 4.1, a new “Plug and Play Licensing” scheme for IP DECT is available. It consists of a “Starter Kit” and “Upgrade Kits”. Upgrade kits are pre-licensed IP DECT base stations, making both first time installation and upgrades easier and more flexible. Upgrade Kits will be available for both RFP 32 and RFP 34.

Installations start with a “Starter Kit” that includes:

- a license key
- two base stations
- activation information

The “Starter Kit” can be expanded with the RFP32 and RFP34 Upgrade kits that include the "built-in license", without the need to order any other upgrade licenses. Once 8 upgrade kits have been added an unlimited license comes into effect (so further unlicensed base stations can be added up to the maximum of 32 base stations on the IP Office).

The current “Classic” license will stay available and can also be used going forward. Upgrade kits can also be used with existing installations if they have been upgraded to the latest ADMM software, currently this is version 1.1.9. It is possible to mix the Classic License and the new licensing scheme.

This means there is no need ever to access the License server during installation. It’s easy to add a single base-station when required, no need to buy an upgrade license.

New material codes for the IP DECT Starter and Upgrade kits are as follows:

EMEA and APAC Starter Kit

Material Code	Description
700378995	IP DECT IPO BNDL 2 STR KIT LIC:CU

EMEA and APAC Upgrade Kits

Material Code	Description
700436561	IP DECT RFP32 UPG KIT INTL LIC:CU
700436587	IP DECT RFP34 UPG KIT INTL LIC:CU

North America Starter Kit

Material Code	Description
700436538	IP DECT IPO STARTER KIT NAR LIC:CU

North America Upgrade Kits

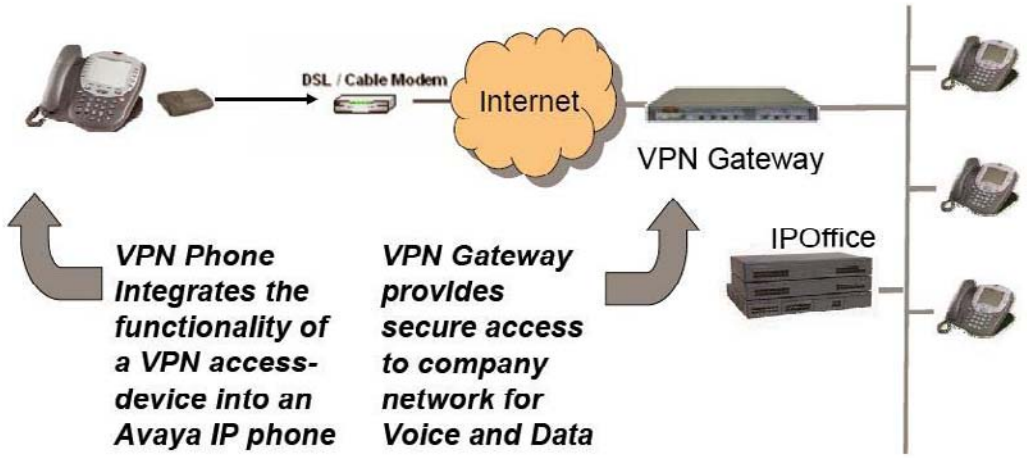
Material Code	Description
700436579	IP DECT RFP32 UPG KIT NAR LIC:CU
700436595	IP DECT RFP34 UPG KIT NAR LIC:CU

3 IP Office Software Enhancements

3.1 VPN Phone support in 4600 and 5600 Series IP Phones

IP Office Release 4.1 supports the connection of remote Avaya IP Phones over a secure IPsec Virtual Private Network (VPN) without the need for a separate VPN gateway at the remote location. The VPN phone uses a high-speed connection to the Internet and then to the VPN solution in the corporate network. The VPN Phone is compatible with the Avaya Security Gateway and with third-party security devices using IKE Extended Authentication (Xauth) with Pre-shared Key.

A special version of the IP Phone firmware, which has the VPN client built-in, is used to convert the phone into a remote VPN phone. Once downloaded to the IP phone all of the same features and functions are available to the phone, the same as if it were connected locally on the LAN to the IP Office.



The VPN phone feature is licensed on IP Office 4.1 with each VPN phone requiring a license to enable it to register with the IP Office. A new checkbox, called “VPN Phone Allowed”, has been added to the Extension\VoIP configuration form for IP Phones in the Manager application. This checkbox is greyed out until a valid VPN Phone license has been loaded and once the number of VPN phones configured matches the VPN IP Extension license value this checkbox will be greyed out again.

Note: *This feature is only supported on the 4610, 4620, 4621, 5610, 5620 and 5621 telephones (not the 4625).*

Supported Security Gateways

To create a successful VPN tunnel, the VPN phone must be capable of setting up an IPsec tunnel between itself and a Security Gateway. The following SMB-targeted VPN gateway devices are supported at launch:

- Adtran Netvanta 3305 VPN Router
- Kentrox Q2300 VPN Router
- Netgear FVS338 VPN Router
- SonicWALL TZ 170 SP Series

Application notes are available from http://support.avaya.com for the following VPN gateways:

- Global IP Office Technical Tip No. 184 - Configuring a VPN Remote IP Phone with a Netgear FVS338 VPN Router
- Global IP Office Technical Tip No. 185 - Configuring a VPN Remote IP Phone with a Kentrox Q2300 VPN Router
- Global IP Office Technical Tip No. 186 - Configuring a VPN Remote IP Phone with an Adtran Netvanta 3305 VPN Router
- Global IP Office Technical Tip No. 196 - Configuring a VPN Remote IP Phone with a Sonicwall Tz170 Standard / Enhanced VPN Router

Note: *These application notes were written for IP Office 4.0 software so they do not show the "VPN Phone Allowed" checkbox option being selected where they cover the required IP Office setup.*

In addition, a number of enterprise class gateways have been tested and can also be used:

Supported Device	Minimum Software Requirement
Cisco VPN 3000 Series Concentrators	Any
Cisco PIX 500 Series Security Appliances	Any
Juniper Networks NetScreen series VPN devices	Screen OS 5.1.0 or above
Juniper Networks Secure Services Gateway 500 Series devices	Screen OS 5.1.0 or above
Juniper Networks Integrated Security Gateway (ISG) Series devices	Screen OS 5.1.0 or above
Nortel Contivity VPN Appliances	V06_00.310 or higher
Checkpoint VPN	Any

Note: *The VPN tunnels must be terminated on 3rd party equipment. IPsec connections directly to the IP Office are not supported.*

Voice quality over an unmanaged IP network is unpredictable. While great care has been taken to make the VPN Phone highly reliable, Avaya has no influence and therefore cannot guarantee the quality of the IP network used. Avaya therefore cannot assume responsibility for voice quality problems incurred.

.

Note*: While Avaya has tested these gateways, they are not Avaya products and must therefore be sourced and supported through third parties.*

When setting up a Security Gateway you can verify the configuration by using the manufacturer provided IPsec Client to setup a VPN tunnel using the protocol selected. If the VPN tunnel is successfully established you have verified that the security gateway is correctly configured and the step of creating a VPN tunnel between the VPN phone and the security gateway should be successful.

IMPORTANT*: Many VPN Routers will not allow a direct media path to be established between two VPN Endpoints. It will be necessary to uncheck the Direct Media Path checkbox in the Extension Configuration in IP Office. Failure to do so may result in No Speech path when two VPN extensions try and establish a call.*

Converting an IP Phone

The VPN Phone software package comes in zip format and can be found in the \bin\VPN Phone directory on the IP Office 4.1 Administration CD and includes the following Application files and script files.

1. 46xxvpn.scr
2. 46vpnupgrade.scr
3. 46vpnsetting_Template.txt
4. 46vpnsetting_readme.txt
5. Application Files for all supported 4600/5600 series IP telephones

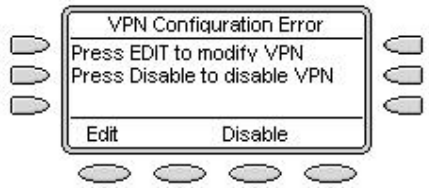
Copy the above files onto the TFTP Server that you currently use to provide the firmware to the IP Phones. Also make sure that the latest 46xxupgrade.scr file provided with and installed by the IP Office 4.1 Administration CD is copied over as this has some modifications in it to allow the conversion of an IP phone into a VPN phone.

Once the necessary files are on your TFTP server either setup and register a new IP phone onto your IP Office system or go to an existing IP Phone that you want to convert and use the following procedure to convert the phone into a VPN phone:

1) Allow the telephone to initialize and register with IP Office.
2) After the phone is registered, set the GROUP for each phone you want to upgrade to a VPN telephone to 876. To initiate the GROUP command from the telephone key pad, press: **Mute 4-7-6-8-7 #** (G-R-O-U-P #)
3) After the GROUP command is initiated, enter **8-7-6 #** (V-P-N #) for the New value. Use Page LEFT key to erase any errors.
4) Press # to save the new value. **Save new value? * = no # = yes**
5) Now restart the IP phone by entering: **Mute 7-3-7-3-8 #** (R-E-S-E-T #)
6) Press ***** when asked to **Reset Values? * = no # = yes**
7) Press # when asked to **Restart Phone? * = no # = yes**

Depending on the speed of your network and existing firmware version on the phone it may take up to 5 minutes to load the necessary firmware.

When the phone has loaded the VPN firmware it should show the following screen when it restarts. This error message is shown as the configuration details for the VPN tunnel have not yet been entered.



When you press the ‘Edit’ key you will be presented with the necessary screens to setup the VPN configuration. The first thing you need to set is the type of VPN device that you will be connecting to, there are eight possible choices:

1) Avaya Security Gateway
2) Cisco Xauth with Pre-Shared Key
3) Juniper Xauth with Pre-Shared Key
4) Checkpoint
5) Cisco Xauth with Certificates
6) Juniper Xauth with Certificates
7) Generic Pre-Shared Key
8) Nortel Contivity

When you select one of these options you are then presented with another set of screens allowing you to enter the necessary information required to setup the tunnel.

Once you have entered the minimum configuration details required a ‘Done’ option will appear allowing you to save these details. At this stage the phone will attempt to start the VPN connection. If it is unable to connect the phone will show an error message.

When the tunnel has successfully been built and the phone is connected to the VPN it will then attempt to register with the IP Office. The 56xx series IP phones will automatically identify themselves to the IP Office as a VPN phone in the registration request they pass to the IP Office, if the VPN Phone Allowed checkbox has not been selected for this user when the phone attempts to register it will fail and ‘Wrong Set Type’ will be displayed on the phone.

If using a 46xx series IP phone by default it will attempt to register as a normal IP phone meaning that the VPN is running un-licensed and will stop working after 180 days. To enable the phone to consume a license you need the phone to load a file called ‘46vpnsetting.txt’ that contains the relevant details. This file can also be used to configure all of the parameters of the VPN setup on the phone which is useful if deploying a large number of VPN phones.

You will need to use the file called 46vpnsetting_Template.txt file, provided with the VPN firmware bundle, to create the 46vpnsetting.txt file. Please read the accompanying file provided with the VPN firmware bundle, 46xxvpnsetting_readme.txt, for further information on which parameters need to be setup.

The entry in this file that is required to allow the 46xx phones to register as IP phones is ‘SMBLIC 1’. An easy way to test that the phone has picked this setting up is to make sure that the VPN Phone Allowed checkbox is not selected for this user. If the phone has correctly picked up this setting it will display ‘Wrong Set Type’ on the phone screen when it attempts to register. Once you see this message open the IP Office configuration and select the VPN Phone Allowed checkbox and restart the VPN phone to allow it to successfully register with the IP Office.

Note: *The VPN phone does not need to be able to read the 46vpnsetting.txt file every time it starts as it caches the settings.*

Once the VPN phone is running you can make any changes to the VPN settings by doing the following:

1) To view the VPN settings from the telephone key pad, press: **Mute 8-7-6-6-6-3 #** (V-P-N-M-O-D #)
2) Press ***** to modify the settings * **= Modify # = OK**
3) You can then view the settings and make any changes required. Pressing the button labelled 'Profile' allows you to change the type of VPN device that you are connecting to.

3.2 Embedded Voicemail Enhancements

Increased Number of Auto Attendants

The number of Auto Attendants available on the IP500, IP406v2 and Small Office Edition has been increased to 40. These Auto Attendants are independent of each other and to facilitate multi-tier operation are provided with the ability to link to each other to enable multiple tiers (e.g. 8 attendants with 5 levels each, or other similar permutations).

The new Auto Attendants will be allocated a number automatically by Manager, starting from 01 through to 40. The number allocated to the Auto Attendant will be two digits and will be the lowest number that is currently unused in the configuration. For example, if 4 Auto Attendants had been created in a configuration file they will have been allocated 01, 02, 03, 04 respectively, if at a later date the Auto Attendant numbered 02 is deleted the next Auto Attendant created in this configuration file will be allocated 02.

When creating a new Auto Attendant if recording short codes do not exist these will be generated to provide access to the configured greeting recordings for the Auto Attendant.

The short codes needed to access the greetings will follow the format *8NXX, where:

- *8 is fixed
- N represents the greeting being recorded
    - 1 = Morning greeting
    - 2 = Afternoon greeting
    - 3 = Evening Greeting
    - 4 = Menu Options.
- XX = the AA number

When upgrading from older versions of IP Office existing Auto Attendants will be allocated Auto Attendant numbers starting with the next unused number and short code numbers will be converted to operate with the new mode of operation and configuration.

Ability to give labels to and re-use Auto Attendant prompt files

The Auto Attendant form has a new "Recording Name" field added against the Morning/Afternoon/Evening greeting options and the Menu Options. A prompt recording file can be referenced by name and re-used in multiple Auto Attendants without the need to create a recording for each occurrence.

To make use of this facility you can either record a file manually via the handset and then re-use that recording or you could use pre-recorded prompts and then convert the wav file to the correct format for the IP Office to use. This would be beneficial to those customers that have a lot of sites and want to use the same greetings for consistency.

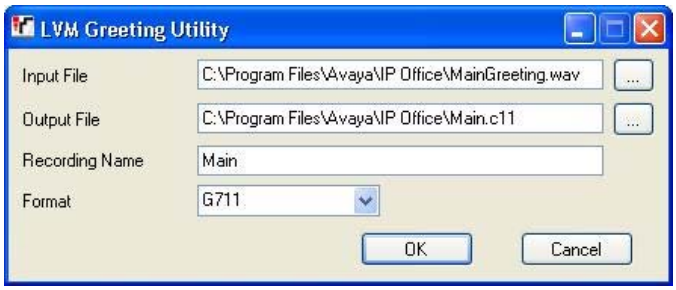
For the first option of making a manual recording you must open the configuration in Manager and setup the Auto Attendant. Type in a name to use for the recordings in the Recording Name fields where appropriate and then save the configuration. Dial into the Auto Attendant using the short codes and record each message required by following the prompts. Once this has been done you can then re-use these recordings in any Auto Attendants by selecting the Recording Name from the drop down list.

If pre-recorded prompts are provided in wav format there is a utility in the 4.1 Manager that will convert the file to the correct format for use in the Auto Attendant. The utility is launched via **File | Advanced | LVM Greeting Utility**.

Converting Pre-recorded Prompts

This process converts the source WAV file recording to the format required by the IP Office Embedded Voicemail.

1. The original recording must be in the following WAV file format. If it is in a different format convert the file using a tool such as Windows Sound Recorder.
    - **PCM/Uncompressed.**
    - **8000 KHz, 16bit, Mono.**
2. Start IP Office Manager.
3. Select **File | Advanced | LVM Greeting Utility**.



4. Click on the **...** button for **Input File** and select the WAV file.
5. Click on the **...** button for **Output File** and select the location into which you want the converted file saved.
    - Select the required file type. For Small Office Edition systems this should be ***G723 Files (*.c23)***. For other IP Office systems use ***G711 Files (*.c11)***.
    - Enter a name for the file (up to 8 characters with no spaces) and end the file name as either ***.c23*** or ***.c11*** to match the selected file type.

6. Enter a name for the recording in the **Recording Name** field. This is the name that will be entered into the IP Office configuration to use the recording. Note that the field in case sensitive.
7. Ensure that the **Format** matches that selected for the **Output File** settings chosen above.
8. Click **OK.**

Note: *If there are any errors during the conversion an error message will appear and a log file is output containing further information about the failure. The normal causes of any failure are that the input file is not in the correct format or the output file extension and format do not match.*

Editing an Auto Attendant to Use Named Recordings

1. Start IP Office Manager and receive the IP Office configuration.
2. Select the **Auto Attendant** form and select or create the required auto attendant.
3. In the **Recording Name** field enter the name of the greeting to be used. This is the **Recording Name** entered during the files conversion, not the actual file name. It is case sensitive.
4. If only converted greeting files are to be used with the auto attendant, it may be advisable to disable the **Enable Local Recording** option to stop any system user recording over the file.
5. Send the configuration back to the IP Office.

Transferring the Recording to the Embedded Voicemail Memory Card

This process uses TFTP to transfer the converted file to the Embedded Voicemail memory card. It first requires the IP Office to be configured with the IP address of the PC from which it should accept TFTP file transfers.

1. Determine the IP address of the PC from which you want to transfer the files.
2. Start IP Office Manager and receive the IP Office configuration.
3. Select the **System** configuration form.
4. Select the **System** tab.
5. In the **File Writer IP Address** field, type the IP address of the PC from which you want the sending of files to the memory card to be allowed.
6. Click to send the configuration back to the control unit.
7. Open a command window in Windows (select **Start | Run** and enter ***cmd***).
8. From the command window, you can use TFTP to upload files to the memory card.
   - The command is ***tftp -i*** *<IP Office IP address>* ***put*** *<source file>* ***a:\Ivmail\AAG****<filename>*

- For example, to transfer the file ***c:\greeting01.c11*** to an IP Office with a LAN1 IP address of 192.168.42.1, the command would be ***tftp -i 192.168.42.1 put c:\greeting01.c11 a:\Ivmail\AAG\greeting01.c11***

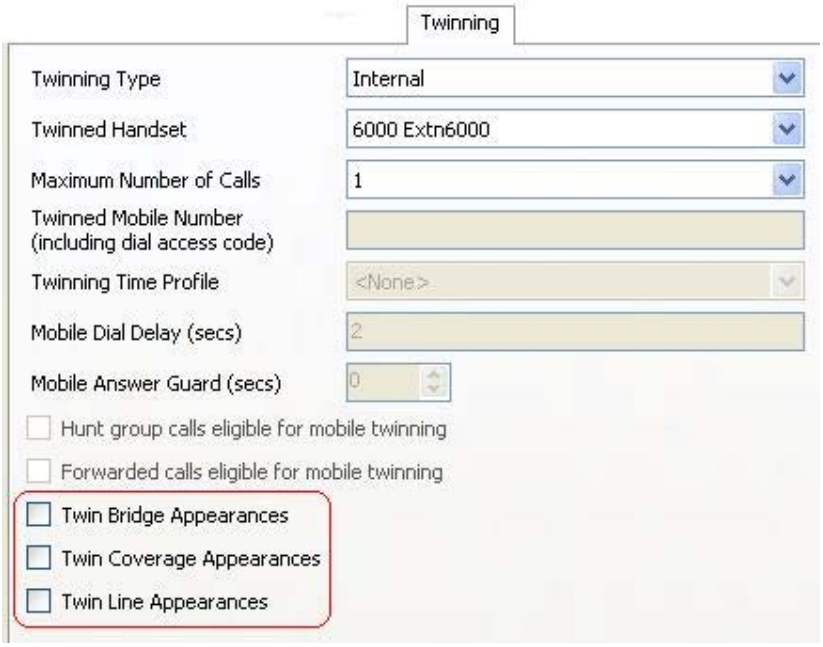
Note: a:\Ivmail\AAG *is the destination folder on the Embedded Voicemail memory card used for auto-attendant greetings.*

Preventing Over Recording of Uploaded Files

Once uploaded to the IP Office, the converted files can still be recorded over using the default short codes for recording auto attendant greetings. To prevent this de-select the Enable Local Recording option of the auto attendant.

3.3 Internal Twinning of Appearance Keys

In IP Office 4.1 it is possible for appearance calls to a twinned user to alert on both the primary and secondary phones. This applies to Internal Twinning only - not external twinning.



A set of three additional checkboxes have been added to the User/Twinning tab in Manager and will be enabled when the User's twinning is set to Internal. They are:

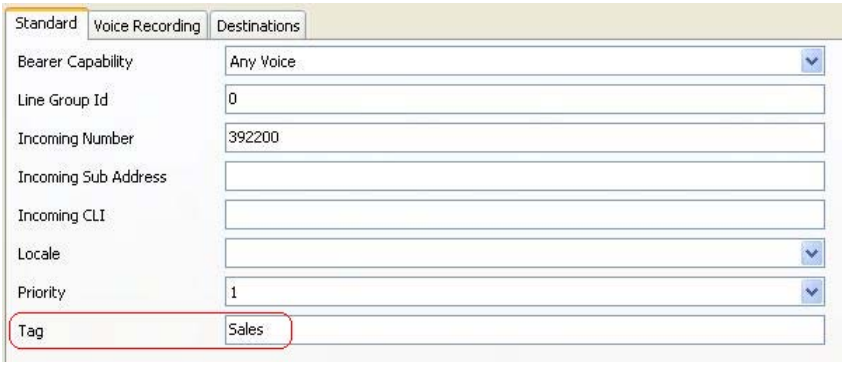
- Twin Bridge Appearances
- Twin Coverage Appearances
- Twin Line Appearances

When a call alerts on a user's phone on an appearance button other than a Call Appearance button the user's twinning setting for that type of button will be inspected and if it is enabled the call will be presented to the internal twinning destination.

If the Appearance is configured for "Immediate" or "Delayed" ring the twinning will occur immediately the call is presented to the Appearance, the delay setting will be ignored. If the Appearance is set to "No Ring" the call will not be twinned.

3.4 Tagging on Incoming Call Routes

A new field has been added to the Incoming Call Route form to allow a tag to be added to an incoming call. This is the same tagging as that done by PhoneManager and SoftConsole.

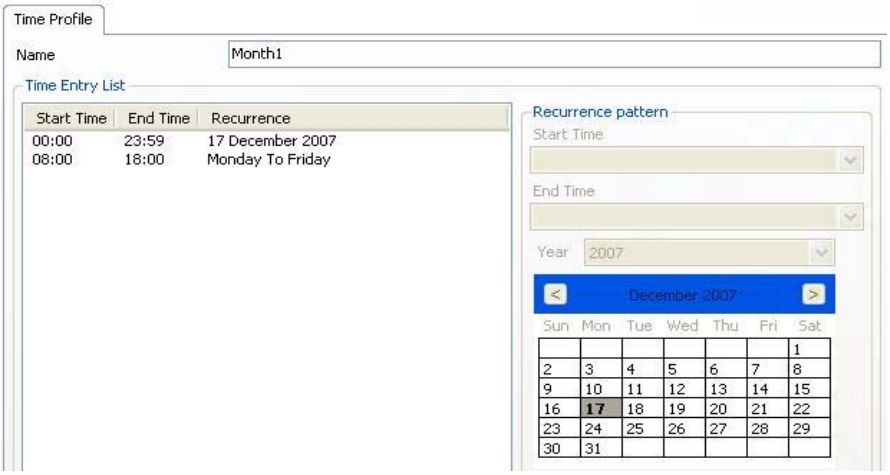


The tag is shown on the phone display when the call is alerting but is removed from the display when the call is answered. If the call is transferred the tag is displayed again while the transferred call is alerting and removed from the display when the call is answered.

The tag will also be displayed in the Phone Manager tag field and SoftConsole notes fields, it will also be displayed in their call histories. Phone Manager and SoftConsole can be used to change the tag text when transferring calls.

3.5 Time of Day and Date Routing of calls

A new calendar facility has been added to IP Office Time Profiles to define dates and times for specific operations. This provides flexibility to use date and time on any feature that makes use of Time Profiles, e.g. for public holidays. For a time profile with multiple entries, for example a week pattern and some calendar entries, the profile is valid when any entry is valid.



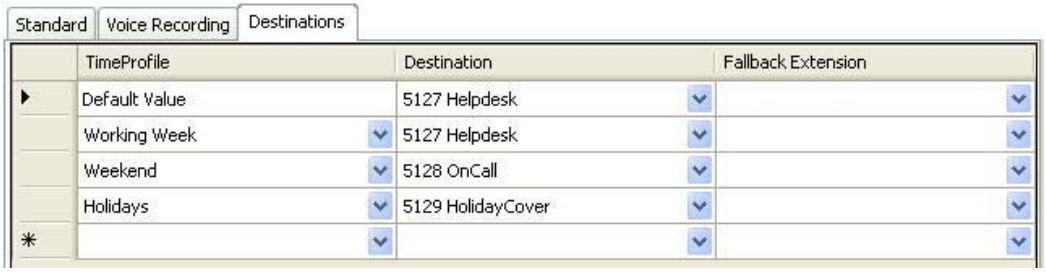
Note: *The option to set calendar based entries is limited to the current year and following year only – it is not possible to set entries more than a year in advance.*

3.6 Time Profile Support on Incoming Call Routes

In order to provide date based routing on the IP Office support for Time Profiles has been added to the Incoming Call Route. A new tab called 'Destinations' is added to Incoming Call Routes and will support multiple destinations. For each destination a Time Profile and a Fallback Extension will be configurable.

When multiple entries are added, they are resolved from the bottom up. The entry used will be the first one, working from the bottom of the list upwards, that is currently 'true', i.e. the current day and time or date and time match those specified by the Time Profile. If no match occurs the Default Value options are used.

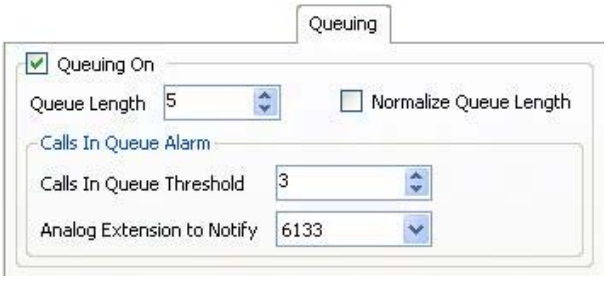
In the example below each time profile would be checked in turn starting with the one called "Holidays". As soon as an entry is matched then that is the routing that will apply to that call.



Note: *You will not be able to add multiple destinations to a call route until you have configured a time profile.*

3.7 Queue Threshold Alert

A new feature has been added to the Hunt Group Queuing tab in Manager that is used to alert at a selected analog extension port when the number of calls queued against a Hunt Group reach a specified threshold. Alerting is triggered when the number of queued calls reaches the threshold. Alerting will stop only when the number of queued calls drops back below this threshold. This value is affected by Normalize Queue Length setting.



The design intention is that the analog extension port should be connected to a loud ringer or other alerting device and is not used for making or receiving calls. The user should not be a member of any hunt groups or the queuing alarm target for any other hunt group queue. Attempting to answer the alerting device will just give ring tone. The alert does not follow user settings such as forwarding, follow me, DND, call coverage, etc or receive ICLID information.

Note: *There will be no support for CTI type interactions with the Alerted User, specifically TAPI (1st or 3rd party), Phone Manager and SoftConsole will not be supported.*

3.8 Security Enhancements

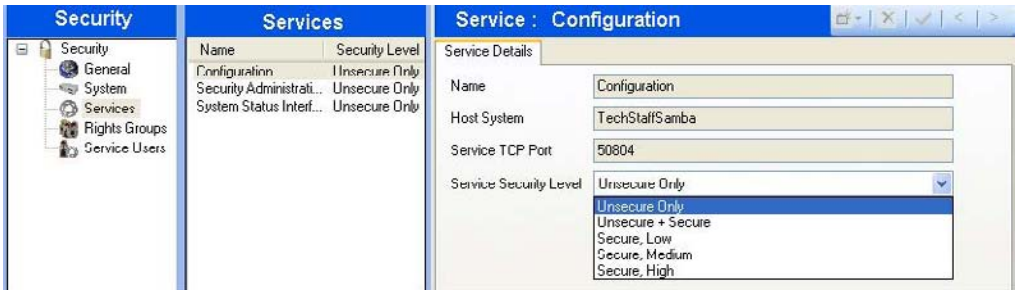
3.8.1 Transport Layer Security (TLS)

In IP Office 4.1 secured communication is supported between the IP Office system and IP Office Manager using TLS for both authentication and encryption. Each of the IP Office services (configuration and security administration) can be configured for secure and/or unsecure communication.

Service	Method	Port Used	Default	IP Office
Configuration	Unsecured	Base TCP Port	50804	3.2+
	Secured	Base TCP Port plus 1	50805	4.1+
System Status Interface	Unsecured	Base TCP Port plus 4	50808	4.0+
Security Administration	Unsecured	Base TCP Port plus 8	50812	3.2+
	Secured	Base TCP Port plus 9	50813	4.1+

Note: *The security settings can also be changed for the System Status Interface, however SSA does not yet support secure connections so this should be left to unsecure only.*

The security administrator can select whether the session between Manager and IP Office can utilize TLS v1.0. Enforcing the use will disable access to versions of Manager that do not have TLS capability. The selection of whether TLS is to be enforced resides within the security settings.

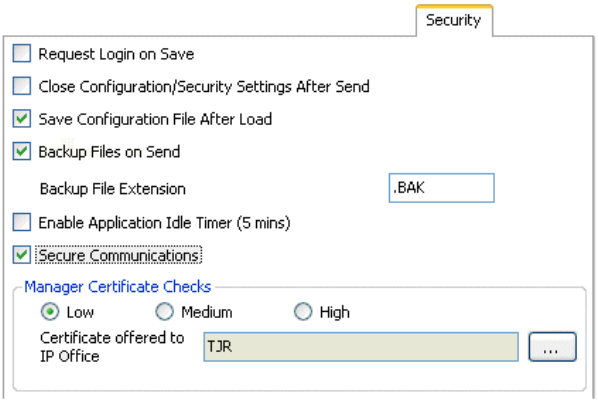


- ***Unsecure Only (Default):*** This option allows only unsecured access to the service. The service's secure TCP port is disabled.
- ***Unsecure + Secure:*** This option allows both unsecured and secure (Low) access. In addition, TLS connections are accepted without encryption, just authentication.
- ***Secure, Low:*** This option allows secure access to that service using TLS, and demands weak (for example DES_40 + MD5) encryption and authentication, or higher. The service's unsecured TCP port is disabled.
- ***Secure, Medium:*** This option allows secure access to that service using TLS, and demands moderate (for example DES_56 + SHA-1) encryption and authentication, or higher. The service's unsecured TCP port is disabled.
- ***Secure, High:*** This option allows secure access to that service using TLS and demands strong (for example 3DES + SHA-1) encryption and authentication, or higher. In addition a certificate is required of the client (usually Manager). The service's unsecured TCP port is disabled.

***WARNING:* Selecting a setting other than *Unsecure Only* will cause the IP Office system to stop responding for a period of up to 5 minutes, depending on the security level chosen, while the IP Office generates a unique security certificate. This will also affect the response of the phones so should only be done when the system is not in use.**

Once security has been setup on the IP Office the Manager will need to be setup to enable secure communication.

This is done through **File | Preferences** and then selecting the **Security** tab.



Secure Communications: *Default = Off*

When selected, any service communication from Manager to IP Office uses the TLS protocol. This will use the ports set for secure configuration and secure security access. It also requires the configuration and or security service within the IP Offices' security configuration settings to have been set to support secure access. Depending on the level of that secure access selected, it may be necessary for the Manager Certificate Checks below to be configured to match those expected by the IP Office configuration and or security service.

***Note:** When Secure Communications is set to on, a padlock icon is displayed at all times in the lower right Manager Status field.*

Manager Certificate Checks

When the Secure Communications option is used, Manager will process and check the certificate received from the IP Office. This setting can only be changed when a configuration has been opened using a user name and password with Administrator rights or security administration rights.

- **Low:** Any certificate sent by IP Office certificate is accepted without question.
- **Medium:** Any certificate sent by IP Office is accepted if it has previously been saved in the Windows certificate store. If the certificate has not been previously saved, the user has the option to review and either accept or reject the certificate.
- **High:** Any certificate sent by IP Office is accepted if it has previously been previously saved in the Windows' certificate store. Any other certificate causes a login failure.

Certificate Offered to IP Office: *Default = none*

Specifies the certificate used to identify Manager when the Secure Communications option is used and IP Office requests a certificate. Any certificate selected must have an associated private key held within the store.

IP Office Security Overview

Administration security on IP Office is achieved using a number of optional cryptographic elements:

- **Access control** to prevent unauthorized use. Supported in version 3.2+
- **Encryption** to guarantee data remains private. Supported in version 4.1+
- **Message Authentication** ensures data has not been tampered with. Supported in version 4.1+
- **Identity** assures the source of the data. Supported in version 4.1+

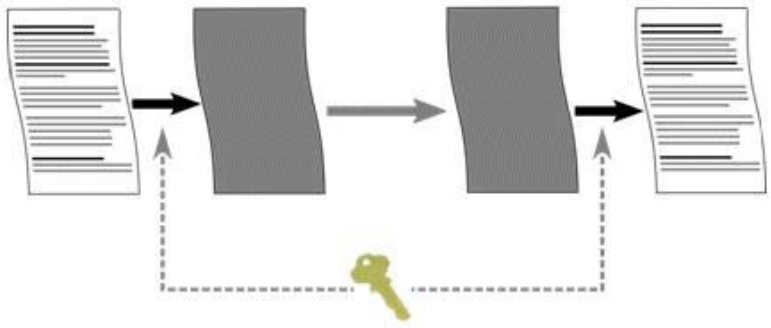
Access Control

Access to configuration, security settings and SSA on IP Office 3.2+ are controlled by the use of Service Users, passwords and Rights Groups. All actions involving communications between the Manager user and the IP Office require a Service User name and password. That Service User must be a member of a Rights Group configured to perform that action.

Encryption

Encryption ensures that all data sent by either IP Office or Manager cannot be 'read' by anyone else, even another copy of Manager or IP Office. Encryption is the application of a complex mathematical process at the originating end, and a reverse process at the receiving end. The process at each end uses the same 'key' to encrypt and decrypt the data.

IP Office supports encryption using the Transport Layer Security (TLS) v1.0 protocol. In addition, the TLS implementation has been FIPS 140-2 certified, indicating the accuracy of implementation.



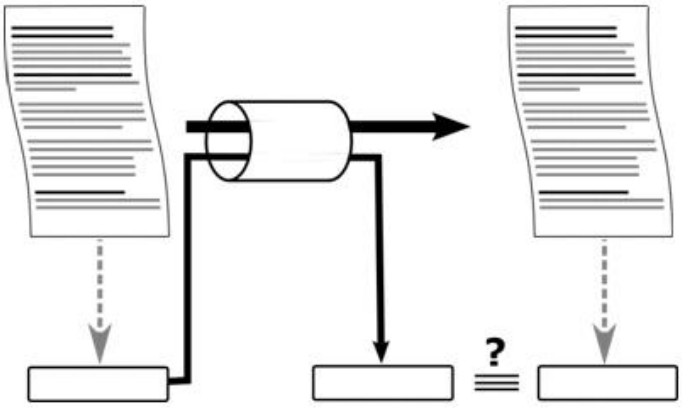
On IP Office 4.1+, any data sent may be optionally encrypted using a number of well known and cryptographically secure algorithms:

Algorithm	Effective key size (bits)	Use
DES-40	40	Not recommended
DES-56	56	'Minimal' security
3DES	112	'Strong" security
RC4-128	128	'Strong" security
AES-128	128	'Very strong" security
AES-256	256	'Very strong" security

In general the larger the key size, the more secure the encryption. However smaller key sizes usually incur less processing.

Message Authentication

Message authentication ensures that all data sent by either IP Office or Manager cannot be tampered with (or substituted) by anyone else without detection. This involves the originator of the data producing a signature (termed a hash) of the data sent, and sending that as well. The receiver gets the data and the signature and checks both match.



On IP Office 4.1+, any data sent may be optionally authenticated using a number of well known and cryptographically secure algorithms:

Algorithm	Effective key size (bits)	Use
MD5	128	'Minimal' security
SHA-1	160	'Strong' security

In general the larger the hash size, the more secure the signature. However smaller hash sizes usually incur less processing.

Identity

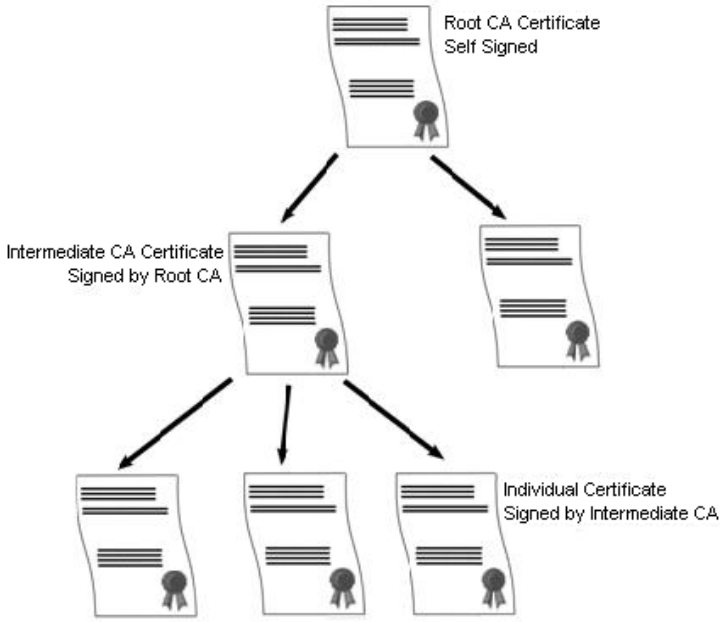
The identity of the equipment or person at each end of the link is achieved by the use of digital certificates – more specifically X.509 v3 certificates. Digital certificates are the preferred mechanism for the majority of internet-based applications including e-commerce and email, and can be thought of as a credential, just like a passport or drivers license.

A digital certificate contains at least three things:

- A public key
- Certificate information (Identity information about the user, such as name, user ID, and so on)
- One or more digital signatures

The purpose of the digital signature on a certificate is to state that the certificate information has been verified by some other person or entity. The digital signature does not verify authenticity of the certificate as a whole, it vouches only that the signed identity information goes along with, or is bound to, the public key. A certificate essentially is a public key with one or two forms of ID attached, plus a stamp of approval from some other 'trusted individual'.

Trusted individuals (also termed Certificate Authorities) themselves have publicly available certificates, which can contain signatures from their trusted authorities. These can be verified all the way up to a 'self-signed' root certificate from a root certificate authority.



Examples of root certificate authorities' certificates can be found in every web browsers certificate store.

Windows Certificate Store Usage

The certificate store that is used by the IP Office Manager to save X509 certificates to and retrieve certificates from is the default one provided by the Windows operating system. This may be accessed for maintenance purposes by a user with sufficient permission via the use of a 'snap-in'.

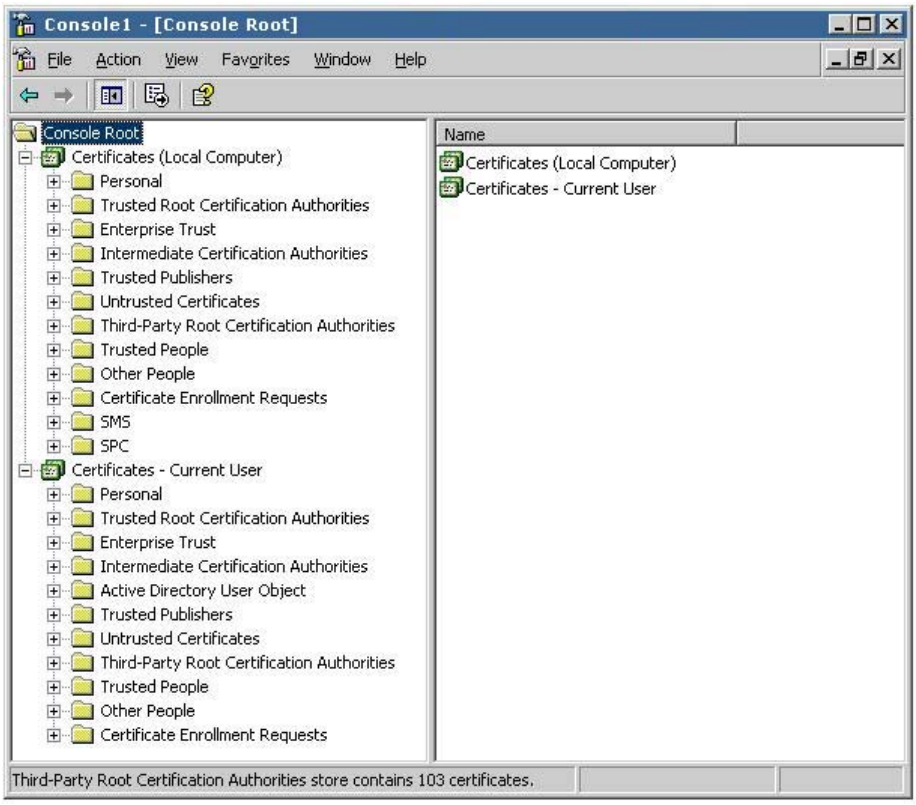
WARNING: **Avaya accept no responsibility for changes made by users to the Windows operating system. Users are responsible for ensuring that they have read all relevant documentation and are sufficiently trained for the task being performed.**

If not installed already, the Microsoft Management Console (MMC) Certificates snap-in can be installed by following the relevant instructions. Both 'user account' and 'computer' options should be installed.

- *For Windows XP Professional:* http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sag_cm_addsnap.mspx
- *For Windows Server 2003:* http://technet2.microsoft.com/windowsserver/en/library/4fa4568e-16de-4a64-b65e-12ee14b31dc21033.mspx?mfr=true
- *For Windows Vista:* http://technet2.microsoft.com/WindowsVista/f/?en/library/a8b21b9b-d102-4045-9f36-e4b3430d2f381033.mspx

Windows Certificate Store Organization

By default, certificates are stored in the following structure:



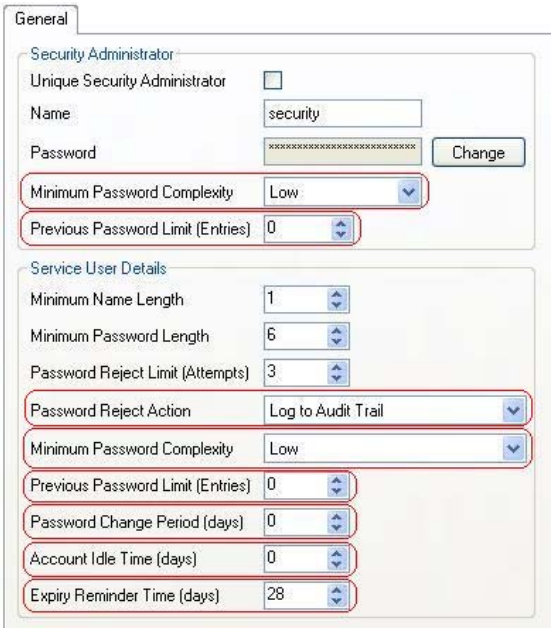
Each of the sub folders has differing usage. The Certificates - Current User area changes with the currently logged-in windows user. The Certificate (Local Computer) area does not change with the currently logged-in windows user.

For further information about Windows Certificates and examples of how to setup security on IP Office please refer to the Manager Help file.

3.8.2 Enhanced Password Policy

Service User Password Controls

Various controls have been added within the IP Office security settings for the Security Administrator and Service User passwords. These controls can be used to enforce the required level of password complexity. Service user accounts can be disabled after too many incorrect password entries, after a specified period of not being used or after a specific expiry date. Service users can also be prompted to change their password when they next login after a specified period.



Security Administrator

Minimum Password Complexity: *Default = Low.*
This setting is active for attempted password changes on both Security Manager and IP Office.

- **Low:** Any password characters may be used without constraint.
- **Medium:** The password characters used must cover two 'code point sets'. For example lower case and upper case. In addition, Medium and High do not allow more than 2 repeated characters of any type.
- **High:** The password characters used must cover three 'code point sets'. For example lower case plus upper case and numbers.

Previous Password Limit: *Default = 0. Range = 0 (Off) to 10 entries*
The number of previous passwords to check for duplicates against when changing the password. When set to 0, no checking of previous passwords takes place. This setting is active for attempted password changes on both Security Manager and IP Office.

Service User Details

Password Reject Action: *Default = Log to Audit Trail*
The action performed when a user reaches the Password Reject Limit**.**

- ***No Action***
- ***Log to Audit Trail:*** Log to Audit Trail creates an entry indicating the service user account name and time of last failure.
- ***Log and Disable Account:*** **Software level = 4.1+:** Log and Disable Account creates an audit trail entry and additionally permanently disables the service user account. This account may only be enabled using the Security Manager Service User settings.
- ***Log and Temporary Disable:*** **Software level = 4.1+:** Log and Temporary Disable creates an audit trail entry and additionally temporarily disables the service user account for 10 minutes. This account may additionally be enabled using the Security Manager Service User settings.

Minimum Password Complexity: *Default = Low.*
This setting is active for attempted password changes on both Security Manager and IP Office.

- **Low:** Any password characters may be used without constraint.
- **Medium:** The password characters used must cover two 'code point sets'. For example lower case and upper case. In addition, Medium and High do not allow more than 2 repeated characters of any type.
- **High:** The password characters used must cover three 'code point sets'. For example lower case plus upper case and numbers.

Previous Password Limit: *Default = 0. Range = 0 (Off) to 10 entries*
The number of previous passwords to check for duplicates against when changing the password. When set to 0, no checking of previous passwords takes place. This setting is active for attempted password changes on both Security Manager and IP Office.

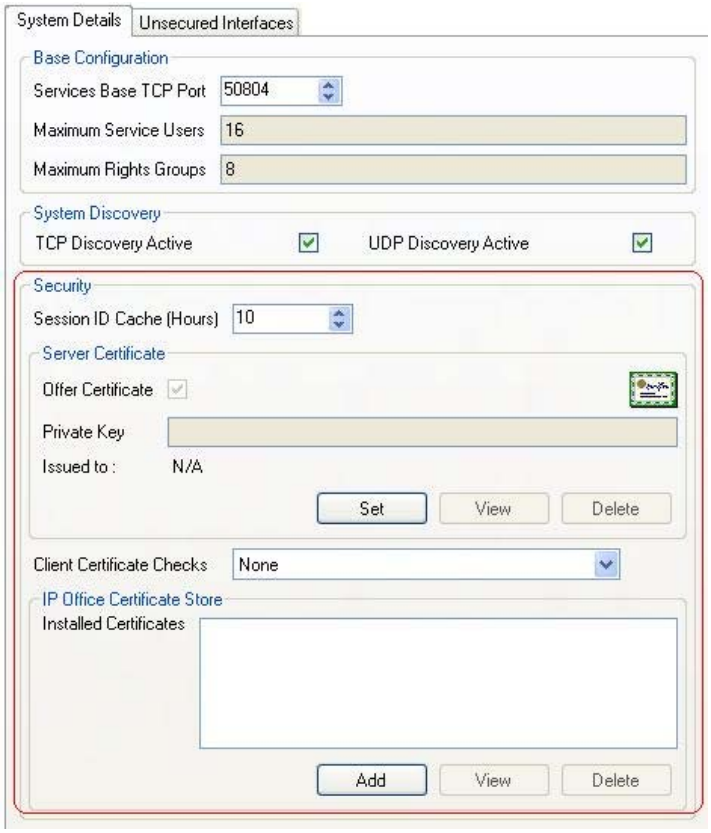
Password Change Period: *Default = 0 (Off), Range 0 to 999 days*
Sets how many days a newly changed password is valid. Selecting 0 indicates any password is valid forever. This setting is active for password changes through this form or prompted by IP Office Manager. If this timer expires, the service user account is locked. The account may only be re-enabled using the Service User Settings. To prompt the user a number of days before the account is locked set an 'Expiry Reminder Time' (see below).

Note: *Whenever this setting is changed and the* ***OK*** *button is clicked, the Security Manager recalculates all existing service user password timers.*

Account Idle Time: *Default = 0 (Off), Range 0 to 999 days*
Sets how many days a service user account may be inactive before it becomes disabled. Selecting 0 indicates an account may be idle forever. If this timer expires, the service user account is permanently disabled. The account may only be re-enabled using the Service User Settings. The idle timer is reset whenever a service user successfully logs on.

Note: *Whenever this setting is changed and the* ***OK*** *button is clicked, the Security Manager recalculates all existing service user idle timers.*

Expiry Reminder Time: *Default = 28, Range 0 (Off) to 999 days*
Sets the period before password or account expiry during which a reminder indication is given in Manager if the service user logs in. Selecting 0 prevents any reminders. Reminders are sent, for password expiry due to the 'Password Change Period' (above) or due to the 'Account Expiry' date in the Service User settings (whichever is the sooner). It is up to the IP Office application to display this reminder.



Security

These settings cover the per-system security aspects, primarily TLS settings.

Session ID Cache: *Default = 10 hours, Range 0 to 100 hours*
This sets how long a TLS session ID is retained by the IP Office. If retained, the session ID may be used to quickly restart TLS communications between the IP Office and a re-connecting IP Office application. When set to 0, no caching take place and each TLS connection must be renegotiated.

Offer Server Certificate: *Default = On*
This is a fixed value for indication purposes only. This sets whether the IP Office will offer a certificate in the TLS exchange when the IP Office is acting as a TLS server, which occurs when accessing a secured service.

Server Private Key: *Default = None*
This is a fixed value for indication purposes only. This indicates whether the IP Office has a private key associated with the Server Certificate.

Server Certificate: *Default = None*
The Server Certificate is an X.509v3 certificate that identifies the IP Office system to a connecting client device (usually a PC running an IP Office application). This certificate is offered in the TLS exchange when the IP Office is acting as a TLS server, which occurs when accessing a secured service. By default the IP Office's own self-generated certificate is used (see note below), but set can be used to replace this with another certificate.

- The Server Certificate may be generated by the IP Office itself, and can take up to 5 minutes to generate. This occurs when any of the Service Security Levels are set to a value other than Unsecure Only. During this time normal IP Office operation is suspended.

Set
Sets the current Server Certificate and associated private key. The certificate and key must be a matching pair, valid. The source may be:

- Current User Certificate Store
- Local Machine Certificate Store
- File in PKCS#12 (.pfx), DER (.cer), or password protected DER (.cer) format
- Pasted from clipboard in PEM format, including header and footer text.

View
View the current Server Certificate. The certificate (not the private key) may also be installed into the local PC certificate store for export or later use when running the manager in secured mode.

Delete
Delete the current Server Certificate. When sent to the IP Office will generate a new Server Certificate when next required. This can take up to 5 minutes to generate. During this time normal IP Office operation is suspended.

Client Certificate Checks: *Default = None*
When a Service Security Level is set to High, a certificate is requested of Manager. The received certificate is tested according to the Client Certificate Checks level:

- **None**: No extra checks are made (The certificate must be in date)
- **Low**: Certificate minimum key size 512 bits, in date.
- **Medium**: Certificate minimum key size 1024 bits, in date, match to store, no reflected.
- **High**: Certificate minimum key size 1024 bits, in date, match to store, no self signed, no reflected.

Client IP Office Certificate Store: *Default = Empty*
The certificate store contains a set of trusted certificates used to evaluate received client (IP Office Manager) certificates. Up to six X.509v3 certificates may be installed. The source may be:

- Current User Certificate Store
- Local Machine Certificate Store
- File in PKCS#12 (.pfx), DER (.cer), or password protected DER (.cer) format
- Pasted from clipboard in PEM format, including header and footer text.

Account Status: *Default = 'Enabled'*
Displays the current service user account status (correct at the time of reading from the IP Office).

- **Enabled:** This status is the normal non-error state of a service user account. This setting can be selected manually to re-enable an account that has been disabled or locked. Note that re-enabling a locked account will reset all timers relating to the account such as Account Idle Time**.**
- **Force New Password:** This status can be selected manually. The service user is then required to change the account password when they next login. Until a password change is successful, no service access is allowed. Note that the user must be a member of a Rights Group that has the Security Administration option 'Write own service user password enabled**.**'
- **Disabled:** This status prevents all service access. This setting can be selected manually. The account can be enabled manually by setting the Account Status back to Enabled.
- **Locked - Password Error:** This status indicates the account has been locked by the Password Reject Action option Log and Disable Account on the security General Settings tab. The account can be enabled manually by setting the Account Status back to Enabled.
- **Locked – Temporary:** This status indicates the account is currently locked temporarily by the Password Reject Action option Log and Temporary Disable on the security General Settings tab. The account can be enabled manually by setting the Account Status back to Enabled, Otherwise the service user must wait for the 10 minute period to expire.
- **Locked – Idle:** This status indicates the account has been locked by passing the number of days set for the Account Idle Time on the security General Settings tab without being used. The account can be enabled manually by setting the Account Status back to Enabled.

- **Locked – Expired:** This status indicates the account has been locked after passing the Account Expiry date set below. The account can be enabled manually by setting Account Status back to Enabled, and resetting the Account Expiry date to a future date or to No Account Expiry.
- **Locked – Password Expired:** This status indicates the account has been locked after having not been changed within the number of days set by the Password Change Period option on the security General Settings tab. The account can be enabled manually by setting the Account Status back to Enabled.

Account Expiry: *Default = <None> (No Expiry)*
This option can be used to set a calendar date after which the account will become locked. The actual expiry time is 23:59:59 on the selected day. To prompt the user a number of days before the expiry date, set an Expiry Reminder Time on the security General Settings tab.

3.8.3 Additional Manager Security Changes

Application Idle Timer

When a session between Manager and an IP Office unit is active an 'Application Idle Timer" can be invoked from Manager **File | Preferences | Security**. Following activation of the idle timer the service user will be presented with an option to terminate the Manager application at this time. Any data changes are lost. The timeout is 5 minutes of no mouse or keyboard activity when the Manager application is active, with or without focus.

Security Reset

Service users with sufficient rights can reset the IP Office security settings to their defaults using IP Office Manager. The command **File | Advanced | Erase Security Settings (Default)** is available in configuration mode and **File | Reset Security Settings** in security mode.

3.9 Syslog support

IP Office 4.1 and higher can send alarms to a Syslog server (RFC 3164) without needing to configure an SNMP server. The Alarms section of the System Events tab displays the currently created alarm traps. It shows the event destinations and the types of alarms that will trigger the sending of event reports. Up to 2 external Syslog servers can be connected via IP (LAN or WAN). This extends the Audit Trail functionality built into IP Office Manager.

3.10 Disable Speakerphone

A feature which is often requested by call centre users is the ability to turn off the hands free speakers on their phones. A new configuration item, called "Disable Speakerphone", has been added to the extension configuration tab and will disable the use of the speaker on both IP Office digital phones and IP phones, this is a mergeable configuration item. The default operation will be for the speaker to be enabled. When Speakerphone is disabled pressing the Speaker button will have no action and the error bleep will sound (through the speaker).

Note: *Disable Speakerphone is supported on the 2400, 5400, 4600, 5600 and 6400 series phones. It is not supported on 4400 series phones or T3 series phones (digital, IP or analog).*

3.11 Group Listen

IP Office digital phones now support the “Group Listen" feature. This is a feature that allows the audio path to be two-way on the handset (or headset) while the speaker is one-way listen only. This allows the person with the handset to speak to the far-end, while everyone else in the room can hear the responses (with side discussions, etc. that would not be picked up by the handset).

The feature is activated by use of a programmable button **Advanced -> Extension -> Group Listen On,** or by short codes ‘Group Listen On’ and ‘Group Listen Off’. Once the feature is activated it will be on for all calls until it is turned off again. If the programmable button is programmed on an IP phone the label will display ‘NOT SUPPORTED’ and the button will not work.

Note: *Group Listen is only supported on the 2402, 2410, 2420, 4406D, 4412D, 4424D, 5402, 5410, 5420, 6408, 6416 and 6424 phones. It is not supported on IP phones.*

3.12 Manager Start-Up Banner

A new feature added in release 4.1 is the ability to display an optional banner on starting Manager. This banner can display information stored within a rich text file (e.g. legal information).

When the banner is displayed the user will be required to select **Continue** to use Manager or **Cancel** to quit. If the file can not be found then no information will be presented.

The file can contain content in either plain text format or RTF format, however in either case the file name must be **etcissue.txt**.

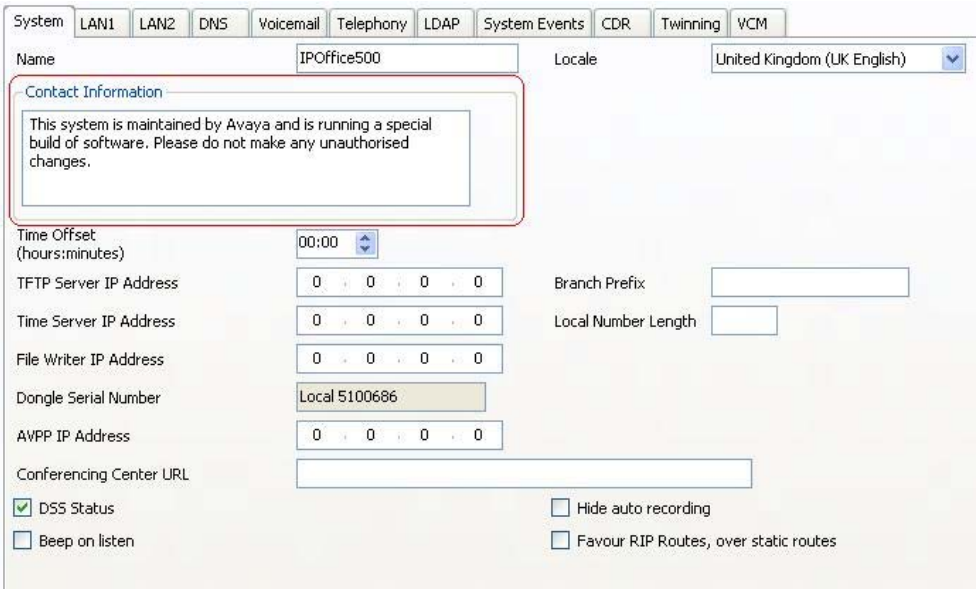
1) Create a file called **etcissue.txt** using a tool such as Windows WordPad.
2) Add the warning or information required to the file.
3) Save the file as either plain text or RTF format. RTF format allows font style and selection options and the use of graphic files within the document.

   Note: *The file must be called etcissue.txt. When saving a file as a rich text file specify the file extension with .txt and the file type as Rich Text Format.*

4) Place the text file in the Manager application program directory, by default *C:\Program Files\Avaya\IP Office\Manager*

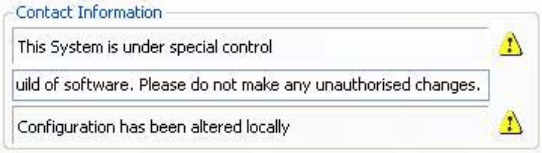
3.13 Manager Warning Dialogue

A feature specifically added for Chain Store Management, but also useful in general situations is the ability to have a small text field that might be used to record general notes about a site or contact details for a centrally managed site. When used with the appropriate flags, this feature can be used to avoid conflicts when more than one simultaneous attempt is made to configure the IP Office.



When changes are made to the configuration a 'Contact Information Check' box appears allowing the user to specify if any flags should be set.

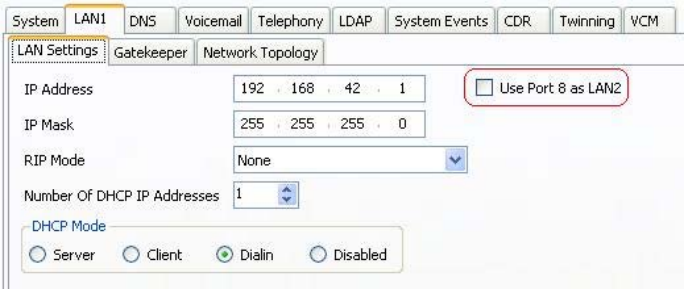
When the configuration is next opened the Contact Information box will show any flags that have been set.



If the contact information is set using Avaya Integrated Management (AIM), warnings that "This configuration is under Integrated Management Control" are given if the configuration is opened using a standalone version of IP Office Manager. If the contact information is set using a standalone version of Manager, warnings that "This configuration is under special control" are given when the configuration is opened again.

3.14 LAN2 Interface on port 8 of the IP406v2

The IP406V2 provides the facility to configure a second LAN (LAN2) interface to operate together with the primary System LAN interface (LAN1). Ethernet LAN port 8 on the front of the IP406 V2 control unit can now be specified as being the LAN2 port for the IP Office system.



When the 'Use Port 8 as LAN2' checkbox is selected this enables the **System | LAN2** tab and associated settings within the IP Office configuration. Once the LAN2 interface is created and configured it is then available as an IP route destination.

When the checkbox is selected an "Are you sure" dialog appears to allow you to confirm the changes to this configuration setting. When creating LAN2 the defaults will are the same as per the Small Office Edition/IP412/IP500.

Both the Logical and System LANs are tied to the same Physical LAN but operate on separate Layer 3 subnets. LAN port 8 will act as a separate Layer 2 domain, providing the same functionality as the Ethernet WAN ports on Small Office Edition, IP412 and IP500.

Note: *Once LAN2 has been enabled on the system erasing the configuration back to factory default will not remove the LAN2 setting. When the setting is enabled it is written to FLASH so that the Ethernet switch is programmed before the main IP Office code is loaded. When the IP Office configuration is erased the system restarts, reads the setting in FLASH and then sets up a LAN2 port in the default configuration. If you want to remove the LAN2 setting from a defaulted configuration you should un-tick the 'Use Port 8 as LAN2' checkbox, save the configuration, restart the IP Office and then default the configuration.*

3.15 Force Feed in Headset Mode

A new feature has been added to enable agents to auto answer calls in headset mode. The existing Emulation button feature Internal Auto-Answer (HFAns) has been modified to include external auto answer when the phone is logically off-hook and idle (headset mode). When a user has an "HFAns" button with "FF" in the action data and headset mode enabled (indicator on) they are said to be in Force Feed mode and the Indicator on the "HFAns FF" button will show active. The default label will be changed to "HFAns FF" when Force Feed is configured.

When Force Feed is active any call presented to the users phone, this includes Bridged Appearances, Coverage Appearances and Line Appearances, will cause a beep to be heard in the headset and will then be automatically answered in the headset.

Note: *Force Feed is only supported on phones with a Headset fixed feature key. That means 2410, 2420, 4610, 4620, 4621, 4625, 5410, 5420, 5610, 5620 and 5621.*

3.16 Local Administration Enhancements

A new option is provided to allow the Admin button to be used to access Date and Time setting options. The feature is accessed by adding a self administer button to the phone with the action data set to ‘2’. This button will also give access to a feature called “Version” which will show the current software version and CPU type.

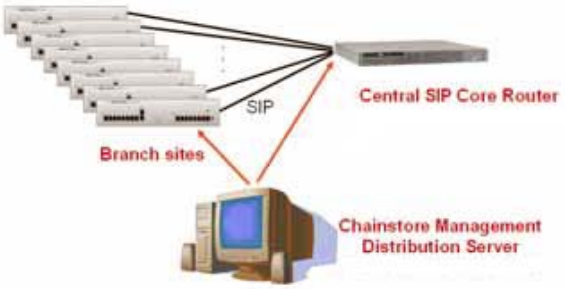
On pressing the button the user will be prompted for their Login Code if it is configured, then the user's User/Telephony/System Phone setting will be checked. If they have System Phone setting enabled they will get a menu with three options; Version, Date, and Time, otherwise they will only get Version. Version will display the system type and version number of the software. Date and Time provides access to setting the system date and time, these options are the same as currently available on 44xx and 64xx phones.

Note: *This Admin option will be supported on the 2410, 2420, 4610, 4620, 4621, 4625, 5410, 5420, 5610, 5620 and 5621 phones only.*

3.17 Avaya SIP for Branch

The primary capability delivered by the Avaya SIP for Branch solution is the ability to network multiple (up to 1000) IP Office systems as a private IP-trunked branch network. This network has a star topology, in which each of the IP Office systems is linked via a SES line to the SIP Enablement Services server (SES).

All branch extensions are reachable from any branch, using a single enterprise-wide private dialing plan. In this dialing plan, each extension number is represented by a branch prefix followed by a local extension number. The IP Office systems direct all private network calls to the SES, which acts as a SIP proxy. The SES holds a table of all branch prefixes and uses that table to route each call to the appropriate destination branch. Only the SES requires knowledge of the full private network topology, the IP Office systems rely on the lookup capabilities of the SES to provide a scaleable network solution.



The SES is configured to route calls to each IP Office system using host maps, one per prefix. Each IP Office system must also be configured in the SES as a trusted host. This uses existing SES capabilities configured via SES Master Admin and Telnet interfaces.

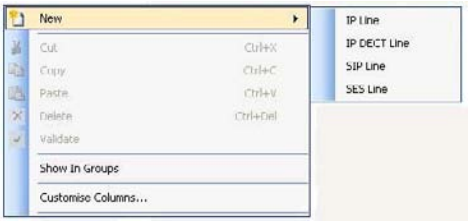
Note: *No SCN functionality is supported with the Avaya SIP for Branch solution. Systems in a SCN may be connected to an SES line, but SCN features will not be transported across it.*

The IP Office SES line is a new variant of the SIP lines that were introduced in IP Office Release 4.0. The IP Office SES line will inter-work with a SES running release 3.x or higher, although SES 4.0 is the recommended minimum version. The signaling channels between IP Office systems and the SES are encapsulated in TCP.

The changes made in IP Office 4.1 to support the Avaya SIP for Branch solution are as follows:

SES Line

This type of line is used for connection from the IP Office system to the SES server. It is a variant of the SIP line type and requires the IP Office to have SIP Trunk Channel licenses available. The line is created in the same way as a SIP line, using the right click context in Line configuration. Unlike SIP lines only one SES line can be created per system.



Branch Prefix: *Default = Blank, Range = 0 to 999999999*

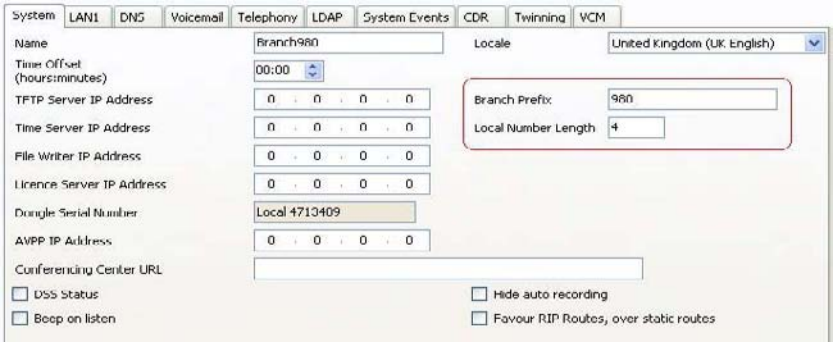
Each system within a SIP for Branch network is identified by a unique branch prefix. The Branch Prefix field on the **System | System** tab is used to set that prefix. Calls to extensions on other systems within the network require the dialling of the branch prefix followed by the extension number. The branch prefixes of each IP Office within the network must be unique and must not overlap. For example 85, 861 and 862 are okay but 86 and 861 are not okay as they overlap.

For ease of routing and maintenance the prefixes should be the same length and begin with the same digit, for example 800, 801, 802 and so on. Routing of calls to the SES line can then be based on the leading digit used for branch prefixes.

Local Number Length: *Default = Blank (Off), Range = Blank (Off) or 3 to 9*

Extension numbers on systems within a SIP for Branch network should all be the same length. The Local Number Length field on the **System | System** tab can be used to set the length of user, extension and hunt group extension numbers. Attempting to enter an extension number of a different length will cause a warning with IP Office Manager. Though intended for IP Office systems within a SIP for Branch network this field can be used in any IP Office system configuration.

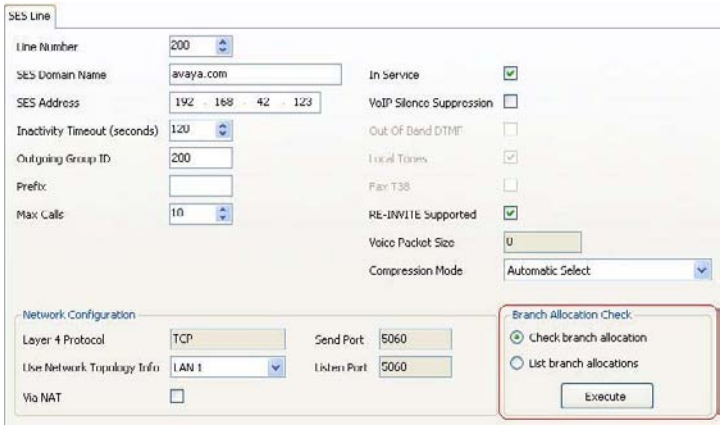
Using the same local number length for all branches is highly recommended as in addition to simplifying call routing it allows for a common number plan within the network. For example, key services such as reception or security at each branch can be given the same extension number. Those services can then be contacted at any branch simply by knowing the branch prefix and the common number for the service.



Note: *The Branch Prefix and the Local Number Length must not exceed 15 digits.*

Branch Allocation Check

As SES lines are configured within each IP Office system in the SIP for Branch network, details of the IP Office system can be written to a CSV file. Manager has a built in utility, called 'Branch Allocation Check', available from the SES line configuration form. This utility is used for checking whether or not the system IP Address or Branch Prefix clashes with any other already in use.

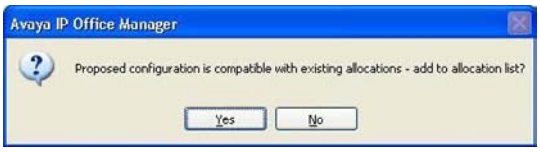


Note: *If a csv file containing the Branch Allocations does not yet exist create a blank one and place it in a directory that can be browsed by the Manager application.*

The Branch Allocation Check is used to ensure the following:

Check branch allocation

Check that the settings of the IP Office and SES line being added are both complete and do not conflict with those of other IP Office systems in the SIP for Branch network already added to the CSV file. Select this option and click **Execute** then select the CSV file containing details of the other IP Offices within the SIP for Branch network. If the settings are okay the following message will be seen:



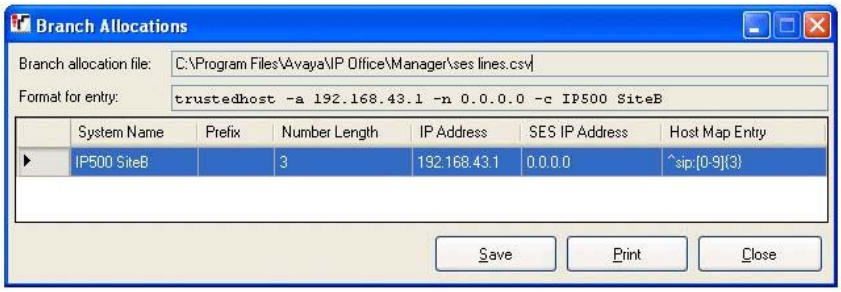
If the settings clash with another system already in the csv file one of the following messages may be shown:

Note: *In the examples above 'London' is the name of the IP Office system, taken from the System | System form.*

List branch allocations

Once the branch details have been added to the csv file listing it will provide the information that will be needed for adding each IP Office system to the SES Host Maps and also the command for adding the system as a Trusted Host*. Select this option and click **Execute** to select and display the CSV file containing details of existing IP Office systems in the SIP for Branch network.

Note: *The Trusted Host command given in the csv file is only used with SES 3.x where the command is entered via the Telnet interface. From SES 4.0 onwards this information is entered via the web browser used to manage the setup of the SES.*



Note: *This csv file used to check the branch allocations does not reside on the IP Office. To make sure that this file is referenced each time a system is added to the network it should either be available from a central location, i.e. when using Avaya Integrated Management to manage and configure the systems, or up to date copies should be help by the engineer installing the system.*

Call Routing

Calls are routed to the SES line using short codes in the same was as for other line types. The short codes can route calls directly to the SES line's Outgoing Group ID or to an ARS form configured for the SES line. If at all possible, requiring a short code for each branch within the SIP for Branch Network should be avoided.

If a common digit has been used at the start of all branch prefixes, that digit can be used as the key for a single SES routing short code. For example, first use a single range for branch prefixes, ie. 80 to 89 in a small network, 800 to 899 in a medium network or 8000 to 8999 in a large network. At each branch a single short code of the form ***8N*** could then be used to start SES routing.

If the above method cannot be used, maintaining a common branch prefix and local number length throughout the network is another option to simplify routing. For example, if all branches have a two digit branch prefixes and then 4 digit extension numbers, a short code of the form ***XXXXXX;*** could be used to only match dialed six digit numbers.

Note: *Whatever method you use to route calls to the SES you must make sure that the number is not sent until complete. Failure to do this will result in the call failing as the number initially passed to the SES will not be valid.*

Additional Notes

Voice Compression Channels

SES calls use IP Office voice compression channels in the same way as used for standard IP trunks and extensions. RTP relay is applied to SES calls where applicable.

Licensing

SIP Trunk Channels licenses is required in the IP Office configuration. These set the maximum number of simultaneous SIP and SES calls supported by the IP Office. Multiple licenses can be added to achieve a cumulative maximum number of channels supported.

IP Office Firewall

The IP Office firewall between LAN1 and LAN2 is not applied to SES calls.

Incoming Call Routing

Incoming SES calls are routed as if being internal calls. The dialled branch prefix is removed and the remaining extension number is used as if dialled on switch.

DiffServe Marking

DiffServe marking is applied to calls using the DiffServ Settings on the System | LAN | Gatekeeper tab of either LAN1 or LAN2 as set by the SES line's Use Network Topology Info setting.

Resource Limitations

A number of limits can affect the number of SES calls. When one of these limits is reached the following occurs:

- Any further outgoing SES calls are blocked unless some alternate route is available using ARS

- Any incoming SES calls are queued until the required resource becomes available.

Limiting factors are:

- The number of licensed SIP channels.
- The Max Calls setting of the SES line.
- The number of voice compression channels.

3.18 Recording Enhancements

The ability to select a target mailbox for recordings made for, or on behalf of a mailbox subscriber is currently supported. However this facility was not available for Hunt Group and Account code recording. The IP Office Manager has been enhanced to have the ability to select the mailbox that Hunt Group and Account code recordings should be targeted to.

3.19 Abbreviated Ring

The Abbreviated Ring setting specifies how a telephone rings if a call arrives when a user is already on another call. Each extension can be programmed to ring in one of the following ways:

- **Abbreviated Ring**: (Default setting). When the user is already on a call, a new call arriving on an appearance button programmed for Immediate Ring or Delayed Ring rings only once. The ring is at a lower volume (called attenuated ring) than the normal ring. This is the current default behavior for IP Office.
- **Repeated Ring**: When the user is already on a call, an incoming call continues to ring, at a lower volume (called attenuated ring) until it is answered.

A new check box option "Abbreviated Ring" is provided by Manager in the User\Telephony tab to determine whether to use the a single burst ring (checked) or a normal ring pattern (unchecked), when an incoming call presents at a phone whilst that user is already on a call. The default setting is checked which is the existing behavior, i.e. a single burst will occur. For 44xx phones if the feature is enabled for a user the ring pattern will be at the phones attenuated ring volume.

When upgrading from an earlier release of IP Office software the check box will be checked, leaving the current behavior unchanged.

Note: *This feature is only supported on Avaya digital or IP phones, it is not supported on T3 digital or T3 IP phones.*

3.20 TAPI Enhancements

In the existing TAPI interface the user outgoing call bar option can be enabled or disabled via the short codes ‘OutgoingCallBarOn’ and ‘OutgoingCallBarOff’. However this does allow selective barring of particular call types. In order to provide the ability to switch a user from one Call Baring Scheme to another via TAPI, the following enhancements have been added.

The existing lineDevStatus TAPI Message sent from IP Office each time the user configuration changes includes the values of various user configuration parameters, including the user priority. IP Office 4.1 adds the following fields:

- Working Hours User Rights Name
- Out of Hours User Rights Name
- A list of Names of all the User Rights configured for the IP Office to which TAPI is connected.

This message will also then be resent each time the list of names of configured User Rights changes.

New short codes have been added to enable the users Priority, Working Hours User Rights and Out of Hours User Rights values to be updated. These may only be used via the TAPI interface, the new short codes will not be configurable via IP Office Manager and cannot be dialed from an extension.

3.21 Enhanced Meet Me Conferencing

IP Office 4.1 makes some changes to the way that conferencing works when you have multiple calls connected to your phone. In previous versions of software any attempt to add a call to a conference would result in all calls connected to your phone being put into the conference. With IP Office 4.1 if you have a call on hold, and took a second call, but wanted to conference the caller on Appearance 2 with another caller on Appearance 3, you are able to do so, without putting the Caller on Appearance 1 into the Conference Bridge as well.

When the existing Conference Meet Me feature is programmed onto a programmable button with a conference ID programmed in the Action Data field, on an Avaya digital or IP phone supporting this feature, the button state will indicate whether the conference call is active (i.e. there are one or more parties on the call). A user will be able to transfer calls into a Conference using the transfer and Conference Meet Me buttons. This allows the user to set up conferences in which they themselves do not participate.

Note: *This feature is only supported on Avaya digital or IP phones with a fixed transfer button, it is not supported on T3 digital or T3 IP phones.*

3.22 Extension Number / Base Extension Number Mergeable

It is now possible to merge any changes made to the Extension number \ Base Extension number in Manager.

- If the extension is currently logged out the phone displays are updated.
- If the extension is currently logged out the IP Office will check to see if a user with the new extension number can be automatically logged into this phone.
- If a user is logged into the extension while its Base Extension is being updated they are not logged out.
- E911 changes to the extension list no longer require a reboot.

3.23 Small Community Networking on IP500

Since the Q3 2007 Maintenance Release of IP Office 4.0 (4.0.10) software, the Voice Networking Licenses and Advanced Networking Licenses work on IP500 Standard Edition and do not require an upgrade to Professional Edition.

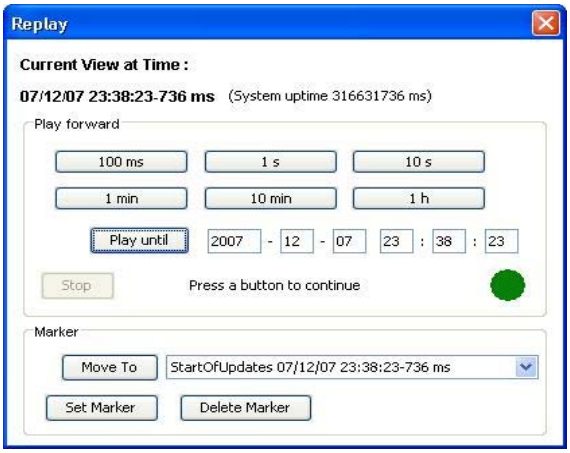
If the customer requires voice messaging, the only messaging supported in the SCN is VoiceMail Pro. Therefore, the site running VoiceMail Pro would require Professional Edition. If the customer does not require voice messaging at all, all sites in the SCN could operate running Standard Edition while still benefiting from the other SCN features:

- Desk to desk dialing
- Hold / Transfer
- Call Forward
- Conference
- Absent Text Messaging
- Busy Lamp Field
- Dynamic User Directory
- Centralized Receptionist
- Hot desking across network
- Paging
- Call Pick-Up
- Call Back When Free
- Camp – On
- Remote Hot Desking
- Distributed Hunt-Groups across network
- Anti-Tromboning

3.24 System Status Application Enhancements

Log File Replay

With the release of IP Office 4.1 the System Status Application (SSA) has the ability to replay a log file. A log file can be opened in SSA using the offline tab and selecting files of type *.slo. SSA presents the initial IP Office state at the start of the log interval. When a log file is opened a new menu item ‘Replay’ is available which produces a replay controller pop-up.



The replay controller allows the log to be advanced to any time during the logging period. The application will then show a snapshot for that time. The replay controller shows the current switch time represented by the snapshot, displayed both as system uptime in milliseconds and in SSA Time/Date format.

The log can be advanced (replayed) in steps of 100ms / 1 second / 10 seconds/ 1 minute/10 minutes and 1 hour. It can also be replayed to a specified time (if later than the current replay time). Log replay occurs as fast as the application is able, not in an accurate representation of real time. While the log is being replayed, the selected SSA view will be updated to reflect the data logged during the replay interval. If a trace has been selected, all trace events that occurred during this interval will be displayed.

When the log has been replayed to/for a specified time, a Rewind Marker can be set at that time, which will then appear in a selection box of Rewind Markers. It will then be possible to rewind to the marked time, view the snapshot for that time and then replay from that time.

Digital Trunk Clock Source Change

SSA has also been enhanced to record when a digital trunk is used as the system clock source and a change is made in the selection of this clock source.

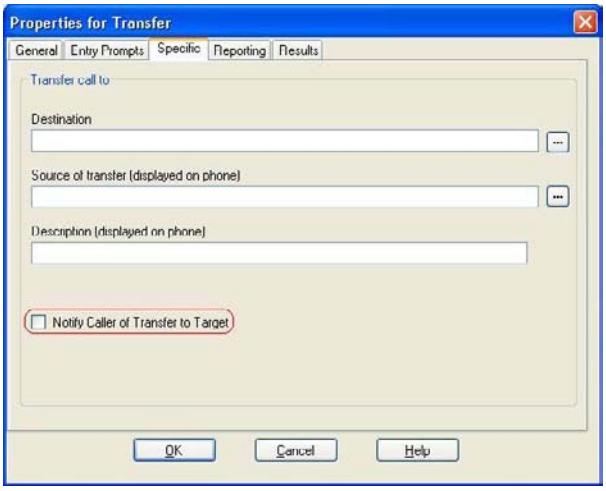
4 IP Office Applications

4.1 VoiceMail Pro

The following enhancements have been made to VoiceMail Pro

4.1.1 Call Transfer Announcements

There is a new checkbox option on the specific tab of the Assisted Transfer and Transfer call flow actions. The checkbox, called 'Notify Caller of Transfer to Target', is used to announce the transfer to the caller. The announcement played is 'Transferring To' and then the recorded name of the mailbox associated with the transfer if available or the destination number.



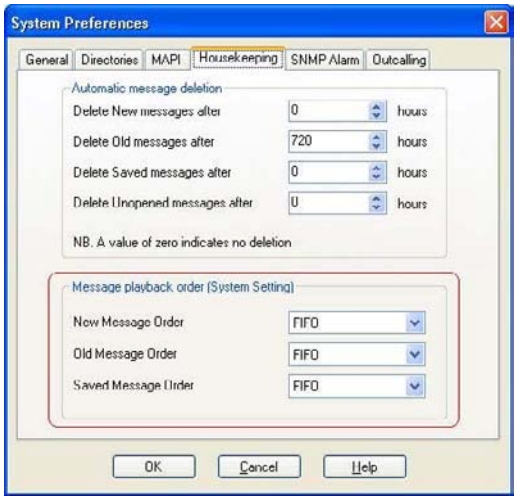
4.1.2 Call Transfer Data Tagging

Currently the Assisted Transfer call flow action has the ability for Call Data tagging info to be passed with the transferred call, this is now also support on the Transfer call flow action.

4.1.3 LIFO/FIFO Message Playback

A new option has been provided on the Housekeeping tab which allows the VoiceMail Pro administrator to select the playback order of New, Old and Saved messages.

.



The options are first in-first out (FIFO) and last in-first out (LIFO), separate settings can be applied to each message type.

Note: *These message playback settings are system wide settings.*

4.1.4 Queuing Enhancements

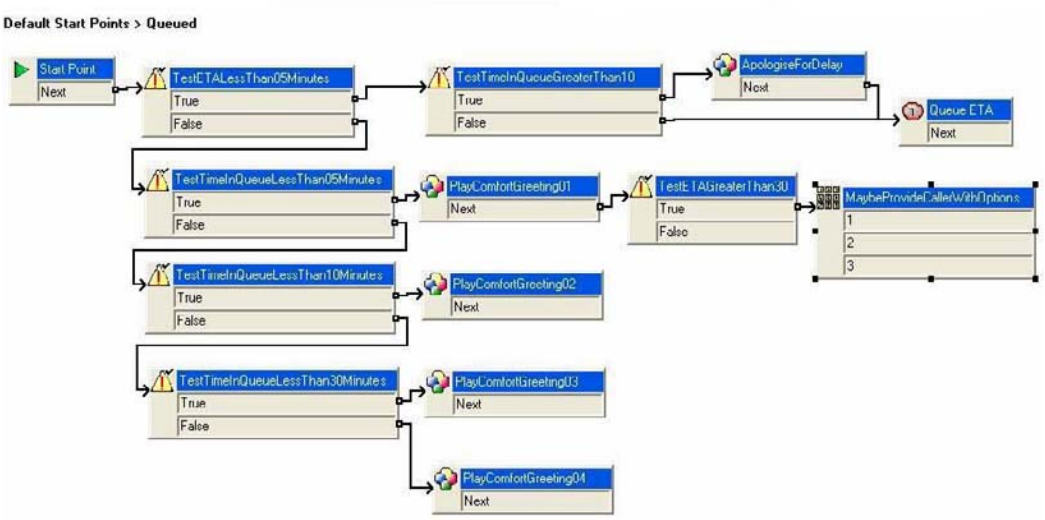
The current Queuing implementation facilitates a 'Queued' and 'Still Queued' capability with $ETA and $QPosn as the parameters supplied by the IP Office.

The current Queuing messages sent by the IP Office have been enhanced to include the length of time a caller has been queued ($TimeQueued) and the length of time the caller has been in the IP Office system ($TimeSystem).

- **$TimeQueued:** Holds the length of time, in seconds, that the call has been part of a particular hunt group queue. Only available when using Queued and Still Queued start points.
- **$TimeSystem:** Holds the length of time, in seconds, since the call was presented to the IP Office system. Only available when using Queued and Still Queued start points.

Note: $TimeQueued *and* ***$TimeSystem*** *should not be used with synchronized announcements. .*

One way that these new variables can be used is to customize a Queued call flow action based on how long the call has been in the queue. In the call flow example below the $TimeQueued variable is being used in conjunction with an $ETA check. If the ETA check determines that the call is to be answered soon, the caller will be played a prompt based upon how long they have had to wait before getting to this point. Other parts of the call flow allow the greeting\prompt played to the caller to be modified based upon how long they have been waiting. This will then allow the queuing mechanism to support the ability for multiple comfort prompts to be configured for queuing.



4.1.5 Variable Routing Action

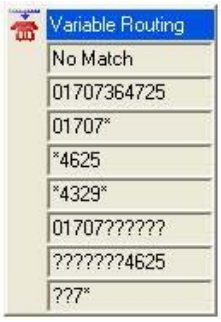
The existing CLI routing call flow action has been renamed to 'Variable Routing' and enhanced to offer routing by additional variables, including a new DDI/DID variable ($DDI).

The Variable Routing action allows the Variable against which routing checks will be made to be selected from the list of system variables. This action routes calls based on whether a selected variable associated with the call matches any of the specified numbers. The selected variable is checked for a match against all strings.

Note: *Any call flows using the $CLI routing action of the previous releases of VoiceMail Pro will be converted to the Variable routing action with $CLI selected as the system variable upon upgrade.*

The Routing Action has the ability to select routing based upon each of the following conditions:

- The User Variable number starts with
- The User Variable number ends with
- The User Variable number includes
- The User Variable is a number of length n containing



Examples of data entered in the Variable Routing Action above using the $CLI variable:

- 01707364725 – This would match against a specific CLI
- 01707* - The CLI number starts with '01707'
- *4625 - The CLI number ends with '4625'
- *4329* - The CLI number includes '4329'
- 01707?????? - The CLI number is an 11 digit number starting with '01707'
- ???????4625 - The CLI number is an 11 digit number ending in '4625'
- ??7* - The CLI number has a '7' as the third digit

Where multiple matches occur, the one with the most matching digits (excluding wildcards) is used. If several equal length matches are found, the first one in the list is used.

4.1.6 Castelle Fax Server Support

In addition to a number of other supported fax servers, VoiceMail Pro now supports Castelle FaxPress Premier (www.castelle.com) analog fax servers. For a full list of supported fax servers, please see the IP Office Knowledge Base at http://marketingtools.avaya.com/knowledgebase/.

4.1.7 Connection Tool

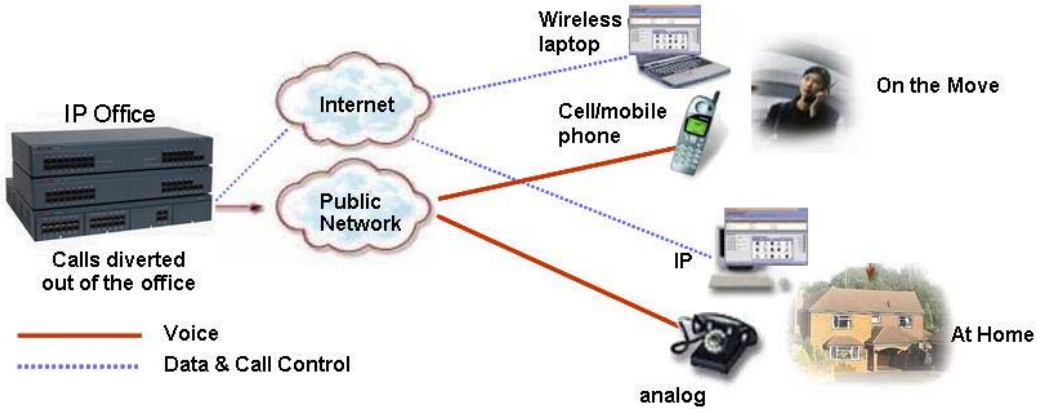
When making connections between your call flows previously you would have to select this button each time you wanted to make a connection. The button functionality has been enhanced and it now works as an on / off button.

This makes it much easier and faster to construct call flows by adding the call flow actions and then enabling this button while connecting all of the actions.

4.2 Phone Manager Pro Telecommuter Mode

Phone Manager Pro Telecommuter mode is a combination of core and application enhancements that permit an IP Office user to work from a remote, non IP Office

phone and allows the making and receiving of calls and the retrieving of voicemails from an external phone. Phone Manager is used to provide the call control, allowing the user to hold, transfer and conference calls as if the user were using a typical IP Office telephone. Outgoing calls appear to originate from the user's desk phone.



A PTSN phone (domestic, GSM etc.) must be available and provides the audio channel. An IP connection must also be available to the IP Office system. Phone Manager Pro Telecommuter mode runs at the remote location and connects to the IP Office system via the IP connection, providing call control.

Phone Manager Pro Telecommuter mode uses the standard Phone Manager Pro license. The feature is enabled on a user by user basis by the administrator who needs to setup the users Phone Manager type (**User | Phone Manager Options**) to be Telecommuter. The user also needs to be setup as a Hot Desk user, i.e. Login code set, as their extension will be logged in and out depending on what Phone Manager mode they are currently working in. If the user has not been setup as a Hot Desk user the Manager application will show a pop up message advising you of this.

When working remotely the user must first establish an IP connection to the corporate network so that when they start Phone Manager it can connect with the IP Office.

Note: *Typically Phone Manager in Telecommuter mode will connect to IP Office via an existing VPN connection.*

When a user that has been set up as a Telecommuter user starts Phone Manager and logs in a second login screen is presented to them. This allows them to select the location from which they are currently working, either Internal or Remote.

- Internal is used when the user is at their normal IP Office extension. In this state their extension and Phone Manager operate in the same way as for other internal Phone Manager users.
- Remote is used for when the user is at an external location and has a data connection for their Phone Manager to the IP Office and a phone on which they can make and receive calls. The user can specify the remote location number when logging in or use a previously saved location number. The remote phone number used must be one that can be dialled directly from the IP Office, for example not via any switch board, receptionist or auto attendant service. Normal IP Office call restrictions are applied, if any, and any external dialling prefix must be included if used on the IP Office.

The Continuous Mode checkbox on the Telecommuter login screen controls how the connection from the IP Office to the remote location is used. There are two types of Telecommuter modes available, On Request Mode or Continuous Mode.

If Continuous Mode is not selected Phone Manager Telecommuter will work in On Request mode. The IP Office will only call the remote location number when required, that is when making or receiving an IP Office call. For example when making a call using Phone Manager, the IP Office will call the remote location, when answered it will make another call using the number requested in Phone Manager. The call can be ended either through Phone Manager or by replacing the handset.

In this mode, it is possible for the remote location phone to also make and receive non-IP Office calls. IP Office calls can be distinguished by their indication in the Phone Manager call details display.

Note: *Calls will not succeed if the IP Office detects that a trunk using analog loop start or analog loop start emulation is being used.*

If required a Test Call can be made to check that the number provided can be dialled successfully. If selected, the IP Office will attempt to make a test call to the remote location number. Phone Manager will show a message asking if the call was

received, clicking on Yes completes the login, clicking on No returns you to the login details screen. If the IP Office was unable to make the call, Phone Manager will display the possible reason. For example "Call Not answered" or "Outgoing call barred". This option is grayed out if Continuous Mode is selected.

Note: *This option is grayed out if Continuous Mode is selected*

If Continuous Mode is selected, once the Phone Manager login is completed, the IP Office will call the remote location number. If the IP Office system has a music on hold source then this music will be heard when the call is answered. The connection should be left open (off-hook) and the call cleared using the Phone Managers hang up button to end that call from the IP Office. DO NOT REPLACE THE PHONE HANDSET.

.

Phone Manager is then used exclusively to make and answer calls, with the IP Office connecting the speech path to the remote location phone handset as and when required.

In this mode, if the continuous call is ended, i.e. the handset is placed on-hook, while there are parked or held calls, whether or not a new call is established when using Phone Manager to un-hold/un-park the call depends on a number of factors and may not always work.

Note: *This option should be used whenever analog loop start trunks or analog loop start emulation trunks are involved or suspected to be involved. This may include cellular phones connected to cellular gateways on analog trunks.*

Irrespective of which mode is used, Continuous or On Request, Phone Manager must be used to make and answer IP Office calls.

When using On Request mode for each inbound or outbound call IP Office establishes a new call to the user supplied contact number. For an outbound call IP Office will call the user supplied contact number first and once answered the IP Office then places the call to the destination number.

When using Continuous Mode a single call for the duration of the Telecommuter session is established between IP Office and the contact number supplied by the user. Continuous Mode means that the Telecommuter user will experience no delays when making outbound calls in Telecommuter mode. It can also be more cost effective for carriers with flat-rate tariff structures, depending on how your lines are being billed or whether payment is by the minute or per call.

Note: *Compact Contact Center (CCC) does not support the collection of statistics for an agent operating in Telecommuter mode.*

5 Windows Operating System Support

Application	XP Pro	Vista	2000 Pro	2000 Server	2003 Server
Call Status	✓	✓	✓	✓	✓
CBC	✓	✓	✓	✓	✓
CCC Server	✗	✗	✗	✓	✓
• Standalone Delta Server	✓	✓	✓	✓	✓
• Wallboard Server	✓	✗	✓	✓	✓
• Wallboard Client	✓	✗	✓	✓	✓
• PC Wallboard	✓	✗	✓	✓	✓
• Call Center View (CCC)	✓	✗	✓	✓	✓
• CCC Reporter	✓	✗	✓	✓	✓
Conferencing Center *	✗	✗	✗	✓	✓
Contact Store	✓	✗	✓	✓	✓
Feature Key Server	✓	✓	✓	✓	✓
Manager	✓	✓	✓	✓	✓
Microsoft CRM Integration	✓	✓	✓	✓	✓
Monitor	✓	✓	✓	✓	✓
Phone Manager Lite	✓	✓	✓	✓	✓
Phone Manager Pro	✓	✓	✓	✓	✓
Phone Manager PC Softphone	✓	✗	✓	✓	✓
SoftConsole	✓	✓	✓	✓	✓
System Status Application (SSA)	✓	✓	✓	✓	✓
TAPI	✓	✓	✓	✓	✓
Voicemail Lite	✓	✓	✓	✓	✓
Voicemail Pro Server	✓	✓	✓	✓	✓
• plus IMS and/or Web Campaigns	✗	✗	✗	✓	✓
• plus IVR and / or TTS	✓	✓	✓	✓	✓

Note: *Vista support is only available on Microsoft Vista Business and Ultimate editions. It is not available on Microsoft Vista Home Basic and Home Premium editions.*

* Conferencing Center full server Installation is not supported on Microsoft Vista. However, the Web Client Host application is supported.

6 Issues Resolved in IP Office 4.1 Software

IP Office 4.1 software has parity with the IP Office 4.0 Q4 2007 maintenance release as well as including the following additional fixes.

Core Software / Manager Fixes

CQ Number	Description of Issue
CQ26526	Dial from PC Wallboard on Call Back Request gives no speech path on Phone Manager PC Softphone
CQ35415	ATM4U board failing to detect incoming calls from a Xacom Celline DT system
CQ36097	IP Office directory entries are not matched when dialing out over a SIP trunk
CQ38086	Int or ext call to H/G Test does not go to overflow group but returns busy when all members of Test busy.
CQ38425	SMDR called number field contains LCR prefix
CQ38476	Manager/Line/EnablePartial Rerouting and external transfers out of VMPro disconnect
CQ38938	ICR not used over IP trunks.
CQ38946	Delay characters ignored when entered by TUI for out calling
CQ38948	Not able to enter '#' by TUI for out calling
CQ38949	Unable to wait for connect before dialing digits in out calling string
CQ38996	System Restart, possibly after merge of config.
CQ39002	Call forwarding off site fails if the inbound calls target to a HG
CQ39010	Inbound calls on SIP DID's can not be picked up using Directed Call Pickup on 4.0.5 and 4.061101.
CQ39033	Unable to transfer calls to Voicemail using user button when target ext is off hook
CQ39039	After logging out and back in, if a call is made to an external IVR requiring DTMF, the call may be disconnected
CQ39043	When doing a transfer to vm via a "user" button the call does not complete
CQ39049	Call Listen feature without beep active creates click at beginning of observation, background noise on monitored set.
CQ39052	Dial direct SC no longer plays confirmation beep to both caller and called users. Only called user beeps
CQ39054	IP500 System restart; possible Ti Vcomp compatibility issue.
CQ39065	Intermittent CLI on ATM4's See CQ39013
CQ39085	Abbreviated Dial no longer sends out DTMF while on a call
CQ39107	Restarting IP Office may cause the port used for overhead paging to hang.
CQ39110	Calls do not follow users forward settings when user is called via Voicemail auto attendant
CQ39113	Embedded VM fails to forward messages to hunt groups - behavior should be prevented.
CQ39115	Analog call disconnects after 90 secs if remote member of the group answers the call.
CQ39120	Call Record and Call Monitor/Listen will not function simultaneously
CQ39121	IP sets have one way audio after placing a call on hold or park
CQ39124	No audible ring back provided when forwarding calls off site over T1 lines.
CQ39127	ASCN overflow is not working as expected: When calls overflow, the non local HG members fail to ring
CQ39148	Call transferred from group in NS to VM AA to user back to NS group results in restart
CQ39186	Out calling failing following upgrade to 4.0.81107
CQ39255	System restart when forwarding a user to a system SC during night service
CQ39266	Correct hunt group queue messages no longer play when queuing to remote groups on 4.0.10
CQ50899	Hot Desk users - User BLF updates are not reflected on the DS visual display.
CQ51013	Outgoing H323 calls to a Cisco failing due to missing sending complete IE in setup message
CQ51233	Problem with forwarding calls to external Busy Numbers from a H/G in Rotary mode (v4.0.5)
CQ51373	IPO incorrectly decoding CLI on Siemens EWSD analogue line
CQ51453	Problem where Number restriction operation via ARS does not work (when there is a long delay when dialing digits).
CQ51845	Call to busy user (c/w Fwd on Busy to a H/G that he is only member of) never rings user once he becomes free.
CQ51921	I/C call that has CLI Withheld is fwd off switch with a Dedicated CLI (ie. Sxxx) the outbound CLI is withheld
CQ51975	Shortcode call tagging failing on 4.0.5
CQ52457	Pressing ** Voicemail Callback to caller shows "Waiting For Line" on display
CQ52775	IP Office does not act upon VM timeout
CQ53016	SCN users on remote site not updating local PM BLF with state changes

CQ53081	Call Listen Display Functions - please include standard functions as well
CQ53138	User feature "Directed Call Pickup" does not work correctly when using in a Distributed Group
CQ53185	Remote IPO running Swedish - Centralised VM Pro does not recognise alphabetic characters in Swedish
CQ53241	BLF status not updating for Hot Desk users logged into remote site with SCN
CQ53318	Outgoing SIP calls to Phonext ITSP failing
CQ53412	Forwarding No Answer 4.0 operates differently to the 3.2 operation of Forward No Answer
CQ53421	System restart when ringing HG (Longest Waiting) that has an extn with Follow Me to IP Dect Extn.
CQ53528	Short Code will not match before Huntgroup with the same leading digit
CQ53547	CQ 35328 - MCID fix only works for incoming calls. Still holds channel open for outgoing calls.
CQ53696	IP Dect on 4.07 remote site is unable to access (via SCN) centralised VM on 3.0 DT by dialing *17
CQ53754	Incoming Call Route with DDI number + "i" no longer routes to correct target in 4.0
CQ53831	IP Telephones, DTMF Keypad feedback missing tones
CQ53860	System Timechange using T3 does not affect Time Profile call routing
CQ54026	No DTMF tones received when using the PM Phone dialer.
CQ54028	Anti Trombone - SCN when an External ISDN call is received across SCN and then forwarded back to host IPO
CQ54031	The IPO needs more resilience built-in to stop reboots when users dial invalid number strings.
CQ54323	SIP: No speech path for incoming SIP call from one ITSP CFU to an external party over ISDN
CQ54331	Calls to DND User are following the Users forwarding settings
CQ54690	Merge config from Manager causes speech path on IP Phones to drop for 1 to 2 seconds
CQ54693	User passcode shown in call list when using *35 to logon.
CQ54882	Sequential or rotary group doesn't return busy in Forward Unconditional scenario
CQ54916	Missed SIP call in DS or IP Phone log is misdialed if URI is in the format 512@192.168.42.160
CQ55051	No connection when calling a Patton H323 Gateway from IP DECT handset via IPO. Works when using 3.2.57.
CQ55118	Soft Console - Drag & Drop to BLF Icon to transfer call does not work
CQ55265	System restart when Cisco tries to register and SysMon IP Phone Status is in use
CQ55525	Y Shortcode character no longer sends DTMF over ISDN after Call Proceeding Received
CQ56640	Hunt groups not presented with calls in the correct order
CQ56987	Conferencing in a remote IP Extn across an SCN results in no speech to/from remote IP Extn.
CQ57073	4.0.10 - Forwarded IP Dect Call over ISDN - no speech
CQ52955	NFR - Longest call waiting not presented to agent in multiple hunt group
CQ24312	Key and lamp documentation misleading for 5410 terminals.
CQ51491	No Speech path between an IP Dect 3711 and a IP 5620 when pickup has been invoked.
CQ56709	Intermittently no speech on IP DECT call via ARS to group on remote IP Office
CQ27692	License can be used on 2 sites temporarily
CQ53568	Italian Translations errors on SSA.
CQ53659	Italian Translation issue
CQ54241	SSA displays an incorrect number of VCM channels in use
CQ54348	System time on SSA is not updated until IPO system being monitored is rebooted
CQ54688	Incorrect number of VCM channels in use - SIP call using RTP relay.
CQ56590	SSA incorrectly alarms for non-connectivity to Feature Key Server on an IP500
CQ39118	Call recording on twinned extn results in VM greeting being delivered when call answered by twin
CQ51906	NFR - Twinning does not work when Master Extn has Line Appearance buttons for line that carries i/c call.
CQ52849	Calls not presented to twinned handset in certain call scenario
CQ53252	Cannot call twinned "slave". Call to "slave" from Digital set shows "INCOMPATIBLE".
CQ56541	Send original CLI information for mobile twin fails in 4.0.10
CQ51349	Call into Main H/G in Night Service leaves VoiceMail in the Night Service Fallback Group's Mailbox.
CQ34110	Translations required for Upgrade Wizard.
CQ34116	Translation required for "Companding Law" in System/Telephony.
CQ35093	Translation issue in Italy
CQ38105	Documentation - IPO Manager help text ambiguous
CQ38907	Setting outgoing trunk group to 50, the same as the default ARS table, can result in reboot on outgoing call
CQ38972	Unable to delete duplicate NoUser from config.

CQ39009	Documentation issue - out calling.
CQ39037	Dial Direct Hotline feature does not work
CQ51718	Clarification on Hunt-group Synchronized calls feature; working with voicemail personalised call-flows.
CQ51727	Issues with Manager User Rights - changes not reflected.
CQ51825	When font size is set to 120dpi - a number of options in manager - system - telephony - are hidden
CQ52524	Help file is misleading - DSS status only works when call is ringing - help file says whenever call connected
CQ52731	Distributed Hunt Group license requirements are incorrect in Help file
CQ52877	Disconnect Clear enabled in default but not supported in ENA.
CQ53328	Manager displays a JIT error when an unsaved field is copied to memory
CQ53382	Manager 6.0.7 - Short-code features are not translated into Italian correctly
CQ53591	Manager - User/VoiceMail tab entries missing in the dtmf fields
CQ53601	Shutdown Embedded Voicemail feature missing in Italian
CQ53770	OK button not available following a codec setting change on an IP DECT line
CQ53807	Shutdown Embedded Voicemail feature missing in German.
CQ54170	Unable to merge any changes when connected via LAN2. It always says ID upgrade required.
CQ54547	Known Units button position incorrect if window is resized.
CQ55243	Manager Help File does not give matching description of invalid characters allowed in User Name Field

VoiceMail Pro Fixes

CQ Number	Description of Issue
CQ56031	Conference Server; VCN Outdialling will not outcall to more than 5 invitees to the Conference
CQ54673	Unable to change "value" once set in the Database Execute\Specific\SQL Wizard\INSERT ...VALUES function\value field.
CQ54557	GUI not updated when unticking "Play Advice on Call Recording"
CQ54049	Numeric filenames for WAV's are played instead of the contents of the file
CQ53832	First 1 to 2 seconds of prompts are missing when recorded via VMPro Client
CQ53362	Wrong translation into Polish for "two" in messages and in queue position. Dwie should be used instead of Dwa.
CQ52281	Menu played on VMPro - User activates a Greeting incorrect in Sweden, Norway and Denmark Locale
CQ51785	Documentation incorrect? - changes to user/group names are reflected after a merge not a reboot
CQ39029	IMS client requires save to be pressed twice before message is saved.
CQ35715	Standard VM 2nd Q wav identical to the 1st Q wav - discrepancy with knowledge base
CQ35631	VMPRO Italian translation - in both 3.2 and 4.0 stream

Phone Manager Fixes

CQ Number	Description of Issue
CQ38103	Unable to add directory entry using Speed Dial > Add User
CQ38494	PMPro-Login- Profile details are missing when a user logs off via the DS phone.
CQ53895	Calls cannot be transferred using PMPro speed-dial tab.
CQ53993	I/C calls from a SIP trunk displays "user@DOMAIN" on the PM. The SRAD states the "user" part only should be displayed.
CQ54070	Phone manager - Call from Directory - Out Tab does not show Directory Name
CQ54716	Last windows position and view mode not saved when restarting Phone Manager
CQ56459	Phone Mananager shows incorrect calling number in "ALL" Call List

SoftConsole Fixes

CQ Number	Description of Issue
CQ53841	Soft Console 4.0.7 intermittent access violation when calling group from Make Call window

7 Known Issues

The following is a list of issues that exist in this release of IP Office 4.1 software. These will be addressed in a future release of software.

Core Software

- DTMFF – Digits not being detected by Fax Server. This is happening when the call is delivered to the Fax Server ports via a Hunt Group with Queuing enabled. It only appears to affect systems using trunks where CLI and Calling Name are delivered separately. If you experience this issue please turn off Queuing on the Hunt Group.

Manager

- If you type an extension or group number into the Incoming Call Route Destination field, rather than choosing it from the drop down list, and then tab to the next field the entry is not retained. You either have to press the enter key before leaving the field, or physically select your desired destination from the drop down list.
- When you enter a time server address of 0.0.0.1 to disable the time server the manager validation reports this as an error.
- It is only possible to import 500 entries into the system directory. As a workaround you can enter the NoUser Source Number 'ExtendLDAPDirectLimit'. With this entry it is then possible to import 1000 system directory entries.
- There are no scroll bars present in the User Rights | User Rights Membership form when Manager is installed on a non-English operating system.
- When you have the SHOW_LINEID_NOT_OUTSIDE NoUser Source Number it is not then possible to save a name in the Line | Name Field. Systems upgraded to 4.1 which already have the name set will not lose the name from this field.

VoiceMail Pro

- When renaming a module the module list is not re-sorted by name.
- A Calendar condition will return a result of 'True' if no dates are selected.
- Whisper Action not working consistently.
- VoiceMail Pro call flow variables containing text strings are not expanded correctly in VB scripting. *****
- Web Campaigns installed to IIS location 'DisplayName1' instead of 'Campaign'. This affects all Web Campaign installations on non-English operating systems. *****
- It is possible to induce an error when using IMS that propagates a fault to VoiceMail Pro server and makes it unresponsive when trying to access it. The VoiceMail Pro service then needs to be restarted. *****

**** Note:** If you are affected by any of these VoiceMail issues please contact Avaya via your normal support channels for further guidance.*

Phone Manager

- Phone Manager sometimes crashes on exit when closed down by clicking on the ‘X’. This can occur when the application has been idle for a few hours.
- Directory name matching does not work as expected. When typing a name into the name field the list of names displayed is not updated until a complete match is entered. If typing a name into the number field the list of entries is updated dynamically.
- the module list is not re-sorted by name.

IP DECT

- No speech path on call when using Phone Manager with IP DECT. This issue occurs if the IP DECT user attempts to transfer a call, using the F2 key in Phone Manager, and the far end does not want to answer the call so they press their drop key. When the IP DECT user goes back to the original call there is no speech.

TAPI

- It is not possible to enable TAPI tracing on the Windows Vista operating system.

8 Technical Notes

8.1 Upgrade Installation Notes

IMPORTANT INFORMATION

Please ignore this information if your IP Office system is already running version 4.0 software.

IP406v2, Small Office Edition and DSv2 Expansion Modules

IP406v2

Some early IP406v2 systems (typically pre PCS08) have not got enough memory to enable them to run IP Office 4.x software. If your IP406v2 system does not have enough memory there is a process in place to enable you to upgrade the system free of charge.

This process is covered under a Product Correction Notice (PCN), which can be found at the following location.

http://support.avaya.com/elmodocs2/qppcn/1593Bu.pdf

Small Office Edition

Before loading IP Office 4.x software onto the Small Office Edition an interim release must first be loaded to upgrade the loader used by the system. If you do NOT follow the correct process for upgrading your system only 90% of the IP Office 4.x software will be loaded onto the unit causing it to get into a reboot loop.

The intermediate version, 3.2.999, can be found in the \bin\IP401ng\V3_2_999 directory of the admin CD or in the Manager\V3_2_999 directory on a PC with the 4.x admin suite installed. Once this has been loaded the actual 4.x software may be loaded as normal.

DSv2 Expansion Modules

A new loader has been provided for the DSv2 Expansion modules. When these modules are upgraded they normally reboot twice at the end of the upgrade, this loader stops this behavior so that they will only reboot once and so speed up future upgrades.

The intermediary image can be found in the \bin\nadcpv2\V3_2_999 directory of the admin CD or in the Manager\V3_2_999 directory on a PC with the 4.x admin suite installed. Once this has been loaded the actual 4.x software may be loaded as normal.

Identifying the amount of memory in the IP406v2

Early 406v2 units only have 16Mb of memory, later units have 64Mb. Although it is possible to check the PCS version of a 406v2 system by looking at the printed label on the unit there are some pre PCS08 systems in the field that do have 64Mb of memory.

The best way to check the memory is to run the System Monitor application, this means it is possible to check this remotely. You will need to make sure that the "Resource Status Print" option on the System tab is enabled to be able to check the memory. When you connect to the system you will see a similar entry in the System Monitor output as shown below:

RES: Fri 3/2/2007 13:43:29 **FreeMem=43346748**(16) CMMsg=6 (6) Buff=100 520 500 520 1 Links=4194

If you look at the "FreeMem" value you will be able to tell what memory configuration your IP406v2 unit has. In the example above there is 43Mb free, so this is a 64Mb system. If you have a 16Mb system this value will be below 10 Mb.

If you do attempt to upgrade a system that does not meet the minimum requirements the Upgrade Wizard will show the following error.

8.2 IP Office 4.1 Admin Suite Upgrades

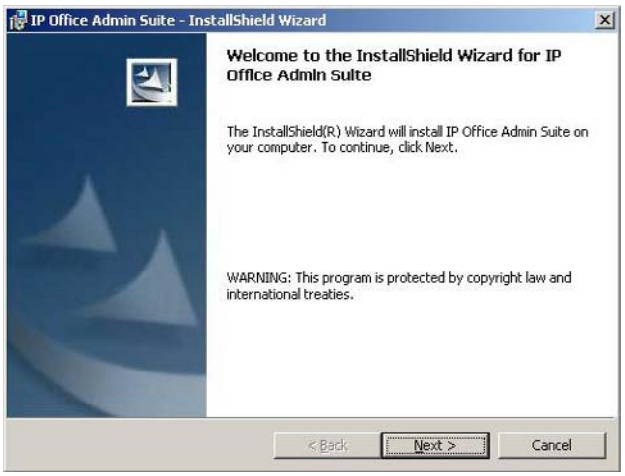
Before any upgrades commence the IP Office 4.1 Admin Suite must be installed. Admin Suite upgrades are supported from version 4.0, any version prior to this must be removed first before the latest Admin Suite can be installed.

The Admin CD will perform a Major Upgrade rather than a Minor Upgrade when upgrading from 4.0. This looks similar to a new install but if you look closely during the installation, you will see that it removes the previous installation before installing the new one. This is necessary to ensure all components are correctly upgraded.

Upgrading from IP Office Admin Suite 4.0:

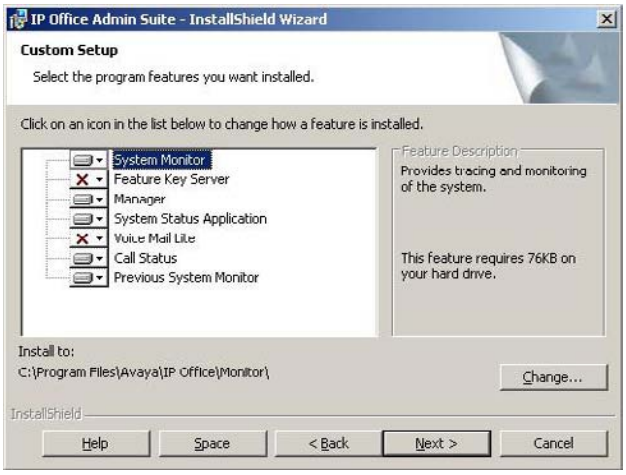
1) Insert the CD and if it does not autorun browse to the CD and click on setup.exe.
2) At the Choose Setup Language screen choose the required installation language and click on OK.

3) At the welcome screen click on Next.

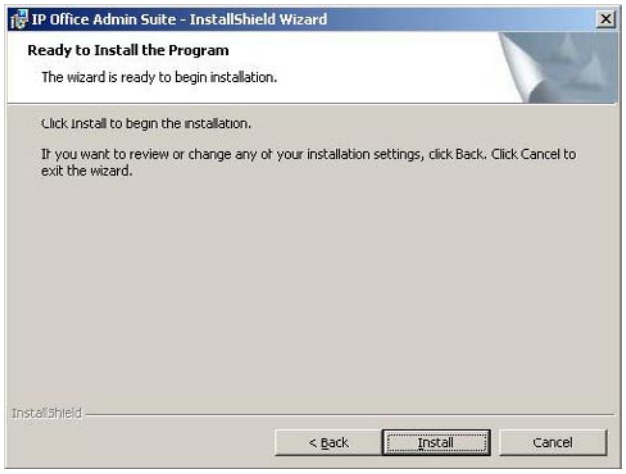


4) At the next screen either accept the default destination for the installation or change it to the required path. Click on Next.

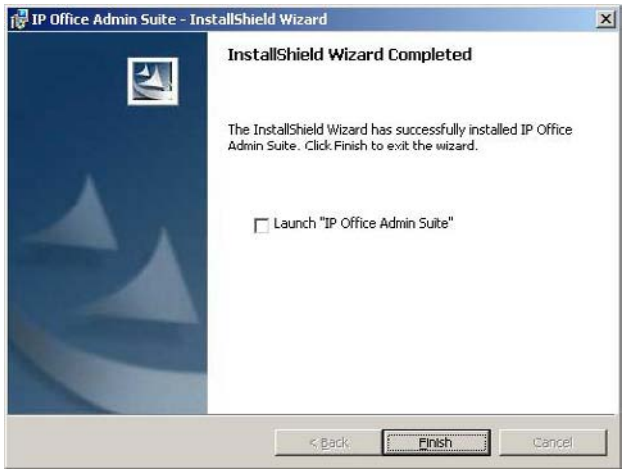
5) At the custom setup screen the components that are already installed are pre-selected. Click on Next.



6) At the next screen click on Install to start the upgrade.



7) Once the installation is complete click on Finish. You can now upgrade your IP Office units.



Installation of Java Run Time

For Vista workstations with JRE versions prior to 1.5.0_11, JRE 1.5.0_11 will be installed Automatically. For non Vista workstations with no JRE installed, or with JRE versions prior to 1.4.2_03, JRE 1.5.0_11 will be installed.

Feature Key server

If using the Feature Key Server on a Vista workstation, the 'Sentinel System Driver Installer' should be executed following the normal Admin Suite Installation. This is found in the Sentinel System driver Installer directory of the Admin CD.

8.3 Core Software Upgrade Instructions

Core Software Upgrade Summary

The table below shows the necessary steps that must be taken to upgrade to release 4.1.

Platform	Current Release	Upgrade Step 1	Upgrade Step 2
SOE	2.1	3.2(999) Loader	Load 4.1
SOE	3.0	3.2(999) Loader	Load 4.1
SOE	3.1	3.2(999) Loader	Load 4.1
SOE	3.2	3.2(999) Loader	Load 4.1
SOE	4.0	Load 4.1	
IP406v2	2.1(27)	Load 2.1(35) and higher	Load 4.1
IP406v2	2.1(35) and higher	Load 4.1	
IP406v2	3.0	Load 4.1	
IP406v2**	3.1(62) and lower	3.1.999 Loader **	Load 4.1
IP406v2	3.1(63) and higher	Load 4.1	
IP406v2	3.2	Load 4.1	
IP406v2	4.0	Load 4.1	
IP412	2.1	Load 4.1	
IP412	3.0	Load 4.1	
IP412	3.1	Load 4.1	
IP412	3.2	Load 4.1	
IP412	4.0	Load 4.1	
IP500***	4.0.0***	Load 4.1	
IP500	4.0	Load 4.1	
DSv2 module*	2.1	3.2(999) Loader*	Load 4.1
DSv2 module*	3.0	3.2(999) Loader*	Load 4.1
DSv2 module*	3.1	3.2(999) Loader*	Load 4.1
DSv2 module*	3.2	3.2(999) Loader*	Load 4.1
DSv2 module*	4.0	Load 4.1	
All other modules	2.1/3.0/3.1/3.2/4.0	Load 4.1	

**** Note**: When upgrading DSv2 modules to the 3.2(999) release an additional step may be needed. If the modules are attached to an IP406v2 system the Upgrade Wizard will report an error if there is not an IP406u.bin file in the V3_2_999 directory.*

Please copy the IP406u.bin file from the Manager directory to the V3_2_999 directory before attempting to upgrade the DSv2 expansion modules.

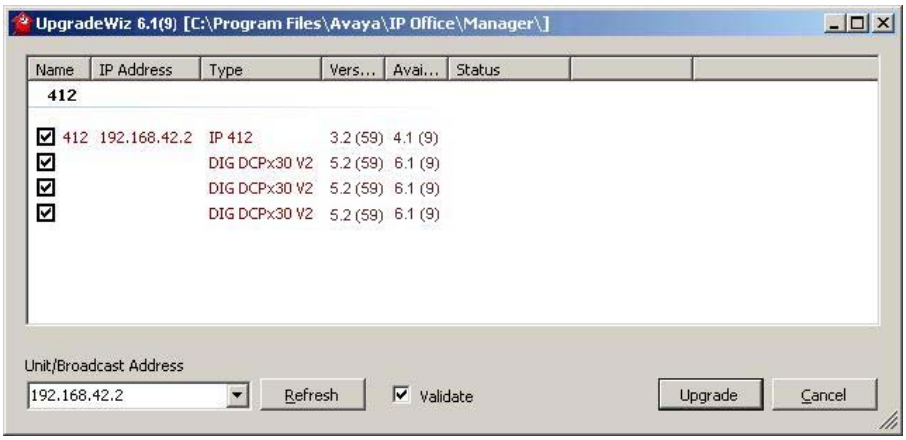
**** Note:** The 3.1.999 loader can be found in the bin\IP406v2\V3_1_999 directory of the admin CD*
or in the Manager\V3_1_999

****** Note:** The IP Office 500 system is shipped from the factory with software version 4.0.0* installed. This is not a fully functioning version of software and MUST be upgraded to the IP Office 4.1 software.

To upgrade the Control and Expansion units do the following:

If you do not need to upgrade your loader (SOE, DSv2 modules and IP406v2 running early 3.1 releases) please go to step 11. (please take note of the message that the Upgrade Wizard shows at the start of the upgrade, shown in step 9 below, before you start).

1. Install the Admin Suite as normal.
2. Open the Manager application.
3. Before starting any upgrades ensure that you have received and made a backup copy of the latest IP Office configuration. If for any reason the upgrade fails, the current configuration may be erased, so a backup copy is essential.
4. From the file menu go to Change Working Directory and change the Binary Directory to C:\Program Files\Avaya\IP Office\Manager\V3_2_999.
5. In Manager select File | Advanced | Upgrade. This will start the UpgradeWiz application.
6. After a few seconds the upgrade wizard should show the units found.
7. A window similar to the one below is displayed. The list shows the current software levels of the units and the level of the appropriate bin file that is available in the Manager/Binary working directories.



8. The current version and available versions are displayed. Tick the check box under Name if it is not already ticked then click on Upgrade.

Note: *If you are upgrading the Small Office Edition loaders then the software version reported will be 3.2(999), or 3.1(999) in the case of the IP406v2 loader. For the DSv2 Expansion Module the version reported will be 5.2(999).*

9. Enter the password of the existing configuration (not the default) and click OK, the following warning will be shown:

10. After clicking on Yes the upgrade process will begin, follow any on screen prompts. When the upgrade wizard informs you that all units have been upgraded click on OK and close down the upgrade wizard.
11. Make sure that the Manager Working Directories are set to C:\Program Files\Avaya\IP Office\Manager.
12. Now follow steps 5-9 again to upgrade your system to IP Office 4.1.

8.4 Unit Compatibility - Expansion Unit Interoperability

All expansion units must be upgraded or downgraded to match the CPU software.

8.5 Phone Firmware Support

The table below lists the phone firmware versions that are supported by IP Office 4.1 General Release software.

Phone Type	Firmware Version
2402, 5402	2.0*
2410, 2420, 5410, 5420	5.0
4606, 4612, 4624	Not supported in 4.1
4601, 4602, 4620, 5601, 5602	2.3
4601+, 4602+, 5601+ and 5602+	2.824
4610, 4620SW, 4621, 4625, 5610, 5620, 5621	2.8.24
4610, 4620SW, 4621, 5610, 5620, 5621 VPN	2.3252

Note: *The firmware of the 2402/5402 cannot be upgraded.*

8.6 IP DECT Firmware Support

The table below lists the IP DECT firmware versions that are supported by IP Office 4.1 General Release software.

ADMM Firmware	ADMM_avaya_1_1_9.tftp	1.1.9
3701 Upgrade	Up_avaya_3701_22.04.04.exe	22.04.04
3711 US Upgrade	Up_avaya_3711_91_24_31_03.exe	91.24.30.16
3711 EU Upgrade	Avaya3711_70.24.11.exe	70.24.11
ADMM Java Configuration	ADM_Configurator_1_1_9.jar	1.1.9
ADMM Dect Monitor	DECTNetMonitor1.exe	1.4

8.7 VoiceMail Pro Software Upgrade Summary

The table below shows the necessary steps that must be taken to upgrade your VoiceMail Pro system to release 4.1. Once you have identified the steps involved please proceed to section 8.8 or 8.9.

Product	Current Release	Upgrade Step
VoiceMail Pro	2.1	Uninstall 2.1 and install 4.1
VoiceMail Pro	3.0	Uninstall 3.0 and install 4.1
VoiceMail Pro	3.1	Uninstall 3.1 and install 4.1
VoiceMail Pro	3.2	Upgrade Installation Available
VoiceMail Pro	4.0	Upgrade Installation Available

8.8 Upgrading from 2.1 / 3.0 / 3.1 VoiceMail Pro

It is important that the settings of an existing VoiceMail Pro are exported before any upgrade. Although folders that contain prompts and messages are not affected by the upgrade process, the editable version of a customer call flow is lost.

1. Export the Database

Before removing VoiceMail Pro as part of an upgrade, you must create a backup copy of the call flow database. This will contain any customizations made to the default call flow.

1. Start the VoiceMail Pro Client.
2. From the **File** menu, select the option **Import or Export**.
3. Select the option **Export call flows** and click **Next**.
4. Enter a file path and file name ending in .mdb, for example **C:\temp\backup.mdb**. Click **Next**.
5. Click **Finish** to start the export then click **Close** to complete the export procedure.
6. Close the VoiceMail Pro Client.

2. Back up the Registry

Any registry settings that are associated with VoiceMail Pro need to be backed up.

1. Insert the VoiceMail Pro CD for the new VoiceMail Pro and cancel the install wizard that auto runs.
2. Right-click the CD drive and select **Open**.
3. Locate the file **backupreg.bat** and double-click it to run the application. The registry settings are backed up.

Note: *Before proceeding to the next step make sure that the registry entries have been backed up correctly. The batch file should have created 3 backup files in the Windows Temp directory. Make sure that the following 3 files exist in that location:*

- VMPro.arf
- NetAly.arf

- IMSGateway.arf (this will only be present if IMS is installed)

3. Remove VoiceMail Pro

Any previous versions of VoiceMail Pro must be removed before you start to install the new version.

1. Open the Windows Control Panel.
2. Select **Add/Remove Programs**.
3. Select **IP Office VoiceMail Pro** and click **Add/Remove**.
4. From the options offered, select **Remove** and click **Next**.
5. Follow the prompts that you see on the screen during the removal process.
6. When the process has been completed, select the option **Yes, I want to restart my computer now** and click **Finish**. If you do not get this prompt then manually restart the computer.

4. Restore the Registry

The VoiceMail Pro registry that was backed up in step 2 needs to be restored. Once the system has restarted and you have logged back on do the following:

1. Right-click the CD drive that contains the VoiceMail Pro CD and select **Open** (reinsert the CD if necessary and cancel the install wizard).
2. Locate the file **restorereg.bat** and double-click it to run the application. This restores the registry settings previously associated with VoiceMail Pro.

5. Install the New Software

The next step is to install the 4.1 VoiceMail Pro software.

1. **Browse** to locate ***Setup.exe*** on the CD and then run it. The Choose Setup Language window opens. Alternatively re-insert the CD and the installation should start automatically.
2. Select the installation language. This language is used for the installation and for the default language prompts.
3. Click **OK**. Installation preparation begins.
4. VoiceMail Pro requires Microsoft .NET 1.1 Framework. If this version is not detected, you are prompted to install it. Click **Yes** to install Microsoft .NET 1.1 Framework.
5. In the Welcome window, click **Next**. The Customer Information window opens.
6. In the Customer Information window, type a user name and the company name or use the default names that are proposed. These settings do not affect VoiceMail Pro when it is installed.
7. In the same window, choose the option that determines who should be able to use VoiceMail Pro when it has been installed. The recommended option is **Anyone who uses this computer (all users)**.
8. Click **Next**. The Choose Destination Location window opens.
9. In the Choose Destination Location window, click **Browse** and locate the folder where the VoiceMail Pro files are to be installed. Otherwise, click **Next** to use the proposed folder.

10. The Messaging Components window opens. Choose the type of installation required.

ACM Gateway - This is used to provide voicemail support for an Avaya G150 unit being used as a branch office gateway to ACM with Modular Messaging. The installation and setup of such a system, including the voicemail aspects, are covered in separate Avaya G150 documentation.

VoiceMail Pro (Full) - This option installs the VoiceMail Pro Server and the VoiceMail Pro Client. If you choose this option you can further choose a compact, typical or custom installation. The custom installation lets you select additional software features to install, for example IMS or VPNM, or remove any software features that are included in a typical installation but are not required. It is advisable to know the type of installation that you are planning so that you can ensure that the appropriate installation requirements are met before you start.

VoiceMail Pro Client Only - This option installs the VoiceMail Pro Client only.

11. In the Messaging Components window, Choose the type of installation required. For the purposes of this document we will choose **VoiceMail Pro (Full)**. For further details of the other types of installation please refer to the appropriate VoiceMail Pro Installation Manual.

12. Click **Next**. The Setup Type window opens.

13. In the Setup Type window, select the type of Installation that you require. For the purposes of this document we will chose **Compact**.

Note: *You may have been able to install Web Campaigns with previous versions of Voicemail Pro on to a PC that had an incorrectly configured IIS Admin Service as the installation would write directly to the registry for its setup without needing to interact with the IIS Admin Service. This is now not the case as the VoiceMail Pro installer must be able to interact with the service during the installation.*

Therefore where a previous installation of Voicemail Pro would have been successful Voicemail Pro 4.1 may cause an error. If you do not verify the operation of the IIS Admin Service before installing the Web Campaigns component `and have an error you will need to start your installation again, including the restoration of the registry entries.

It is worth noting that the Web Campaigns component is automatically selected as part of a Custom and Typical Installation, if you have any concerns around the IIS Admin service on the PC that you are installing on to please choose a Custom Installation and de-select the Web Campaigns component.

14. Click **Next**. The Service Account Name window opens. Details of the default administrator account are already filled in.

15. Click **Next**. The Select Program Folder window opens. By default, the program folders are created in a folder called IP Office. You can specify a different folder or select one from the list of existing folders. To specify a different folder, type the folder name in the Program Folders box. Alternatively, to use an existing folder, highlight a name in the list of existing folders.

16. Click **Next**. A summary of the components that are about to be installed is shown. Check that this list is as expected. If for any reason the details are not what you expect, click **Back** and make the necessary changes. When you are satisfied that the details are correct, click **Next** to start copying the files.

17. The Setup Status window opens to keep you informed while the installation takes place.

18. When the installation is complete you are prompted to restart the computer. Choose **Yes I want to restart my computer now**.

19. Click **Finish** to restart now.

20. When the computer restarts, log back in.

21. The IP Office VoiceMail Pro - Email Settings window opens.

22. Enter the name of the email account to use or click Browse and select an account to use.

23. Click **Next**. The IP Office VoiceMail Pro SMTP Email Settings window opens.

24. In the **Mail Server** box, type the name of the SMTP mail server or use the name that is proposed. This should be the fully qualified domain name.

25. In the **Port Number** box, type the number of the receiving port on the SMTP mail server. The default is 25.

26. To enforce server authentication, check the **Server Requires Authentication box**. This is optional. If you check it you also need to provide the Account Name and Password that need to be entered. You can also choose whether or not to set the **Use Challenge Response Authentication** option.

27. Click **Finish**. An attempt is made to validate the email settings. An error message is displayed when the attempt to connect with an SMTP server fails.

28. Click **OK** to acknowledge the message. You have now finished installing the Voicemail Pro Server and Client software.

6. Restore the Database

The copy of the call flow database that contained any customizations made to the default call flow needs to be restored.

1. Start VoiceMail Pro.

2. From the **File** menu, select **Import or Export**. The Import or Export Call Flows window opens.

3. Select **Import Call Flows**.

4. Click **Next**.

5. Click the **Browse** button and locate the file that contains the backed up call flows.

6. Select the file and click **Open**.

7. In the Import or Export Call Flows window, click **Next**.

8. Click **Finish** to start importing the database.

9. Click **Close** to complete the import process.

The new version of VoiceMail Pro has been installed. Test that the system is running by dialing *17 from any extension. You should hear the mailbox announcement.

8.9 Upgrading from 3.2 / 4.0 VoiceMail Pro

You can upgrade from IP Office VoiceMail Pro 3.2 / 4.0 to VoiceMail Pro 4.1 without having to uninstall the previous version of software.

Note: *Although it is not necessary to back your call flow database it is recommended just in case anything goes wrong with the upgrade.*

1. Insert the new **IP Office VoiceMail Pro** CD. The installation should auto-start. If it does not auto-start, click **Browse** to locate ***Setup.exe*** on the CD and then run it. The Choose Setup Language window opens.
2. Select the installation language. The language selected is used for the installation.
3. Click **OK**. A question box opens and shows 'An older version of Voicemail Pro is installed. Would you like to do a major upgrade to the new version?' A major upgrade looks very similar to a new installation and is required to make sure that all of the VoiceMail Pro components are upgraded correctly.
4. Click **Yes**. The Welcome Screen opens.
5. Click **Next**. The Welcome screen opens.
6. In the Welcome screen, click **Next**. The Customer Information window opens.
7. Click **Next**. The Setup Type window opens. Choose the type of installation required. If you have previously run a Custom Installation you will need to do this again and select the components that you want to re-install.

Note: *You may have been able to install Web Campaigns with previous versions of Voicemail Pro on to a PC that had an incorrectly configured IIS Admin Service as the installation would write directly to the registry for its setup without needing to interact with the IIS Admin Service. This is now not the case as the VoiceMail Pro installer must be able to interact with the service during the installation.*

Therefore where a previous installation of Voicemail Pro would have been successful Voicemail Pro 4.1 may cause an error. If you do not verify the operation of the IIS Admin Service before installing the Web Campaigns component `and have an error you will need to start your installation again, including the restoration of the registry entries and call flow database.

It is worth noting that the Web Campaigns component is automatically selected as part of a Custom and Typical Installation, if you have any concerns around the IIS Admin service on the PC that you are installing on to please choose a Custom Installation and de-select the Web Campaigns component.

8. Click **Next**. The Select Features window opens if you have chosen a Custom installation. Select the VoiceMail Pro components that you want to install.
10. Click **Next**. The Service Account Name window opens. Details of the administrator account should already be filled in.
11. Click **Next**. The Select Program Folder window opens. By default, the program folders are created in a folder called IP Office. You can specify a different folder or select one from the list of existing folders. To specify a

different folder, type the folder name in the Program Folders box. Alternatively, to use an existing folder, highlight a name in the list of existing folders.

12. Click **Next**. A summary of the components that are about to be installed is shown. Check that this list is as expected. If for any reason the details are not what you expect, click **Back** and make the necessary changes. When you are satisfied that the details are correct, click **Next** to start copying the files.

13. The Setup Status window opens to keep you informed while the installation takes place.

14. When the installation is complete you are prompted to restart the computer. Choose **Yes I want to restart my computer now**.

15. Click **Finish** to restart now.

16. When the computer restarts, log back in.

17. The IP Office VoiceMail Pro - Email Settings window opens.

18. Enter the name of the email account to use or click Browse and select an account to use.

19. Click **Next**. The IP Office VoiceMail Pro SMTP Email Settings window opens.

20. In the **Mail Server** box, type the name of the SMTP mail server or use the name that is proposed. This should be the fully qualified domain name.

21. In the **Port Number** box, type the number of the receiving port on the SMTP mail server. The default is 25.

22. To enforce server authentication, check the **Server Requires Authentication box**. This is optional. If you check it you also need to provide the Account Name and Password that need to be entered. You can also choose whether or not to set the **Use Challenge Response Authentication** option.

23. Click **Finish**. An attempt is made to validate the email settings. An error message is displayed when the attempt to connect with an SMTP server fails.

24. Click **OK** to acknowledge the message. You have now finished installing the Voicemail Pro Server and Client software.

8.10 IP Office User Applications Software Upgrade Summary

The table below shows the necessary steps that must be taken to upgrade your User Applications to release 4.1. Once you have identified the steps involved please proceed to section 8.11 or 8.12.

Product	Current Release	Upgrade Step
User Applications	2.1	Uninstall 2.1 and install 4.1
User Applications	3.0	Uninstall 3.0 and install 4.1
User Applications	3.1	Uninstall 3.1 and install 4.1
User Applications	3.2	Upgrade Installation Available
User Applications	4.0	Upgrade Installation Available

8.11 Upgrading from 2.1 / 3.0 / 3.1 User Applications

1. Uninstall User Applications

1. Open the Windows Control Panel.
2. Select Add/Remove Programs.
3. Select IP Office User Suite and click **Change/Remove**.
4. From the options offered select Remove and click **Next**.
5. Follow any prompts given during the removal process.

2. Install the New Software

1. Insert the User CD. The installation wizard should auto-start.

2. Select the installation language and click **Next**.

3. At the Welcome screen click **Next**.

4. In the Customer Information window, type a user name and the company name or use the default names that are proposed.

5. In the same window, choose the option that determines who should be able to use the User Applications when they have been installed. The recommended option is **Anyone who uses this computer (all users)**.

6. Click **Next**. The Choose Destination Location window opens.

7. In the Choose Destination Location window, click **Browse** and locate the folder where the User Application files are to be installed. Otherwise, click **Next** to use the proposed folder.

8. From the Setup Type screen choose the type of setup you would like, **Compact**, **Custom** or **Typical**. For the purposes of this document we will choose **Typical**. For further details of the other types of installation please refer to the appropriate Applications Installation Manual.

9. Click **Next** to continue.

10. If there are multiple IP Office units detected on your network select your unit from the list and then click on **OK**.

11. At the next screen select the User name from the list that this installation is associated with and enter a password for that user if it has one setup in the IP Office configuration.

12. Click **Next**. A summary of the components that are about to be installed is shown. Check that this list is as expected. If for any reason the details are not what you expect, click **Back** and make the necessary changes. When you are satisfied that the details are correct, click **Next** to start copying the files.

13. The Setup Status window opens to keep you informed while the installation takes place.

14. When the installation is complete you are prompted to restart the computer. Choose **Yes I want to restart my computer now** and click **Finish**.

8.12 Upgrading from 3.2 / 4.0 User Applications

You can upgrade from IP Office 3.2 / 4.0 User Applications to IP Office 4.1 User Applications without having to uninstall the previous version of software.

1. Insert the User CD. The installation wizard should auto-start.
2. At the Welcome screen click **Next**.
3. At the Upgrade Features screen make sure that the applications to be upgraded are selected and click **Next**. The upgrade will now proceed.
4. At the Update Complete screen click **Finish**.

8.13 Delta Server Upgrade

When using IP Office 4.1 software you must use a new version of Delta Server for CCC and SMDR to work correctly. The Delta Server, version 5.2.16, is found on the Administration disk in the /CBC/DeltaServer(5_2_16) directory. Although previous versions of Delta Server will work with IP Office 4.1 the statistics generated may not be correct.

1. Stop the Delta Server service.
2. Insert the IP Office 4.1 Administration CD and cancel the install wizard that auto runs.
3. Browse to /CBC/DeltaServer(5_2_16) and locate the Setup.exe file. Double click on the file to start the installation.
4. Choose the setup language and click **OK**.
5. At the Welcome screen click **Next**.
6. In the Choose Destination Location window click **Next** to use the proposed folder, or browse to change the location if the CCC software has been installed into a different directory.
7. When the installation is complete you are prompted to restart the computer. Choose **Yes I want to restart my computer now** and click **Finish**.

9 Assistance

9.1 Documentation

IP Office 4.1 Documentation can be found on http://support.avaya.com

1. Go to http://support.avaya.com
2. Select FIND DOCUMENTATION and DOWNLOADS by PRODUCT NAME.
3. Select IP Office.
4. Select the Software release required.
5. Select the Documentation Categories required.

9.2 Software

Avaya will supply CD and DVD media to Avaya Authorized Distributors that have a current contract with Avaya. Avaya will not supply CDs or DVDs directly to Business Partners. Business Partners are required to order CD/DVD media from their respective Avaya Authorized Distributors.

The following CD/DVDs are available with the release of IP Office 4.0:

Material Code	Description
700449457	IPO CD 4.1 USER/ADMIN SET
700449465	IPO DVD 4.1 USER/ADMIN SET
700448954	IPO CD 4.1 VOICEMAIL PRO CD

Note: It may be acceptable to duplicate this media (CD/DVD) but your contract with Avaya needs to be reviewed in the first instance. If permitted, copies may then be made which must contain an Avaya Proprietary Notice on the CD/DVD.

The IP Office Release 4.1 software CD images (not DVD) will be available on the Avaya Support website from December 17, 2007.

IP Office Release 4.1 will be downloadable and usable free of charge. However, please note that Avaya reserves the right to charge for future software releases at its discretion.

1. Go to http://support.avaya.com
2. Select FIND DOCUMENTATION and DOWNLOADS by PRODUCT NAME.
3. Select IP Office.
4. Select the Software release required.
5. Select Downloads from the Document Categories.

9.3 IP Office Technical Training

Training is one component that must be fulfilled prior to being an Authorized Avaya Channel Partner. The Avaya University IP Office Technical curriculum is updated to reflect IP Office Release 4.1 through the addition of a new IP Office Product Delta course that covers the major enhancements and customer benefits associated with R4.1.

New online course:

- AVA0091WEN: IP Office R4.1 Product Delta

To see a full listing of IP Office classes please visit http://www.avaya-learning.com.

For information on the courses and assessments associated with product authorization, select Product Authorization under Curriculum Maps.

Issued by:
Avaya SSD New Product Introduction

Contact details:-

EMEA/APAC
Tel: +44 1707 392200
Fax: +44 (0) 1707 376933
Email: gsstier4@avaya.com

NA/CALA
Tel: +1 732 852 1955
Fax: +1 732 852 1943
Email: ipoust4eng@avaya.com

Internet: http://www.avaya.com
© 2007 Avaya Inc. All rights reserved.