IP Office 4.1

Manager: 01. Using Manager

39DHB0002UKAA Issue 20i (29th November 2007)

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases.

Documentation Disclaimer

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya.

Link Disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this Documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all of the time and we have no control over the availability of the linked pages.

License

USE OR INSTALLATION OF THE PRODUCT INDICATES THE END USER'S ACCEPTANCE OF THE TERMS SET FORTH HEREIN AND THE GENERAL LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE AT http://support.avaya.com/LicenseInfo/ ("GENERAL LICENSE TERMS"). IF YOU DO NOT WISH TO BE BOUND BY THESE TERMS, YOU MUST RETURN THE PRODUCT(S) TO THE POINT OF PURCHASE WITHIN TEN (10) DAYS OF DELIVERY FOR A REFUND OR CREDIT.

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. "Hardware" means the standard hardware Products, originally sold by Avaya and ultimately utilized by End User.

License Type(s): Designated System(s) License (DS).

End User may install and use each copy of the Software on only one Designated Processor, unless a different number of Designated Processors is indicated in the Documentation or other materials available to End User. Avaya may require the Designated Processor(s) to be identified by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Third-Party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them is available on Avaya's web site at: http://support.avaya.com/ThirdPartyLicense/

Avaya Fraud Intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. Suspected security vulnerabilities with Avaya Products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

For additional support telephone numbers, see the Avaya Support web site (http://www.avaya.com/support).

Trademarks

Avaya and the Avaya logo are registered trademarks of Avaya Inc. in the United States of America and other jurisdictions. Unless otherwise provided in this document, marks identified by "®," "™" and "SM" are registered marks, trademarks and service marks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners.

Documentation information

For the most current versions of documentation, go to the Avaya Support web site (http://www.avaya.com/support) or the IP Office Knowledge Base (http://marketingtools.avaya.com/knowledgebase/).

Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your contact center. The support telephone number is *800-628-2888.* Business Partners would call *877-295-0099.*. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support.

Contents

Manager 5
Overview of Manager 5
What's New in 4.1 9
General Manager Changes 9
Security Enhancements 9
Avaya SIP for Branch Support 10
General IP Office Features 10
Hunt Group Operation 11
Telephony 11
Button Programming 11
Short Codes 12
IP Office 500 12
Embedded Voicemail 12
Voicemail Pro 13
Key and Lamp Operation 14
Licenses 14
Windows Operating System Support 14
System Status Application 14
What's New in 4.0 Q2 2007 15
What's New in 4.0 17
Manager Changes 17
Hardware Support Changes 18
System Status Monitoring 19
SIP Trunks 19
Hot Desking (Logging In/Out) 19
Voicemail 20
Hunt Groups 21
Alternate Route Selection (ARS) 22
ISDN Features 22
Advanced Small Community Networking (Advanced SCN) 22
Key and Lamp Operation 23
Licences 23
Other Features 24
Installing Manager 25
Starting Manager 28
Changing the Manager Language 29
Connecting Manager to IP Office 30
Backward Compatibility 37
IP Office Standard Edition and IP500 Licences 38

Avaya Integrated Management (AIM) 39
Avaya Integrated Management, IP Office and Chain Store Mangement 39
AIM Applications 40
Password Administration 42
Configuring an IP Office for AIM 43
PIM Templates 44
PIM IP Office Templates 44
Hardware Template 46
User Template 47
Auto Attendant Template 48
General Template 49

Configuration Mode 51
Configuration Mode 51
The Configuration Mode Interface 52
Security Settings 54
Title Bar 56
The Menu Bar 57
Toolbars 58
Using the Navigation Pane 60
Using the Group Pane 62
Using the Details Pane 65
Using the Error Pane 67
Altering the Configuration Interface 68
The Status Bar 70
Editing Configuration Settings 71
How the Configuration is Used 71
Mergeable Settings 72
Configuration File Sizes 73
Setting the Discovery Addresses 74
Loading a Configuration 76
Known System Discovery 80
Creating a New Configuration 82
Importing and Exporting Settings 84
Copying and Pasting 87
Saving a Configuration onto PC 87
Sending a Configuration 88
Erasing the IP Office Configuration 90

Security Mode 91
Overview of Security Settings 91
Security Settings 92
Default Security Users 94
The Security Mode Interface 95
Security Administration 97
1. Introduction 97
2. Access Control 97
3. Encryption 98
4. Message Authentication 98
5. Identity 99
6. Windows Certificate Store Usage 99
7. Windows Certificate Store Organisation 100
8. Windows Certificate Store Import 101
9. Certificate Store Export 101
10. Implementing IP Office Administration Security 102
Editing Security Settings 104
Loading and Saving Security Settings 104
General Settings 107
Security | System Details 110
Security | Unsecured Interfaces 113
Security Services Settings 114
Rights Group | Group Details 115
Rights Group | Configuration 116
Rights Group | Security Administration 117
Rights Group | System Status 118
Security Service User Settings 119

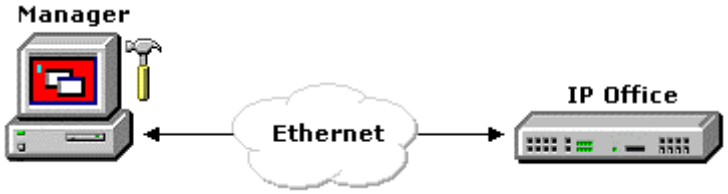
Menu Bar Commands 121
Menu Bar Commands 121
Configuration Mode 121
File Menu 122
View 138
Tools Menu 139
Security Mode 142
File | Open Security Settings 142
File | Close Security Settings 142
File | Save Security Settings 142
File | Reset Security Settings 142
File | Preferences 142
File | Configuration 142
File | Exit 142

Manager

Overview of Manager

IP Office Manager is an application for viewing and editing an IP Office system's configuration. It is a tool meant primarily for system installers and maintainers.

Manager runs on a Windows PC and connects to the IP Office via Ethernet LAN or WAN connections.



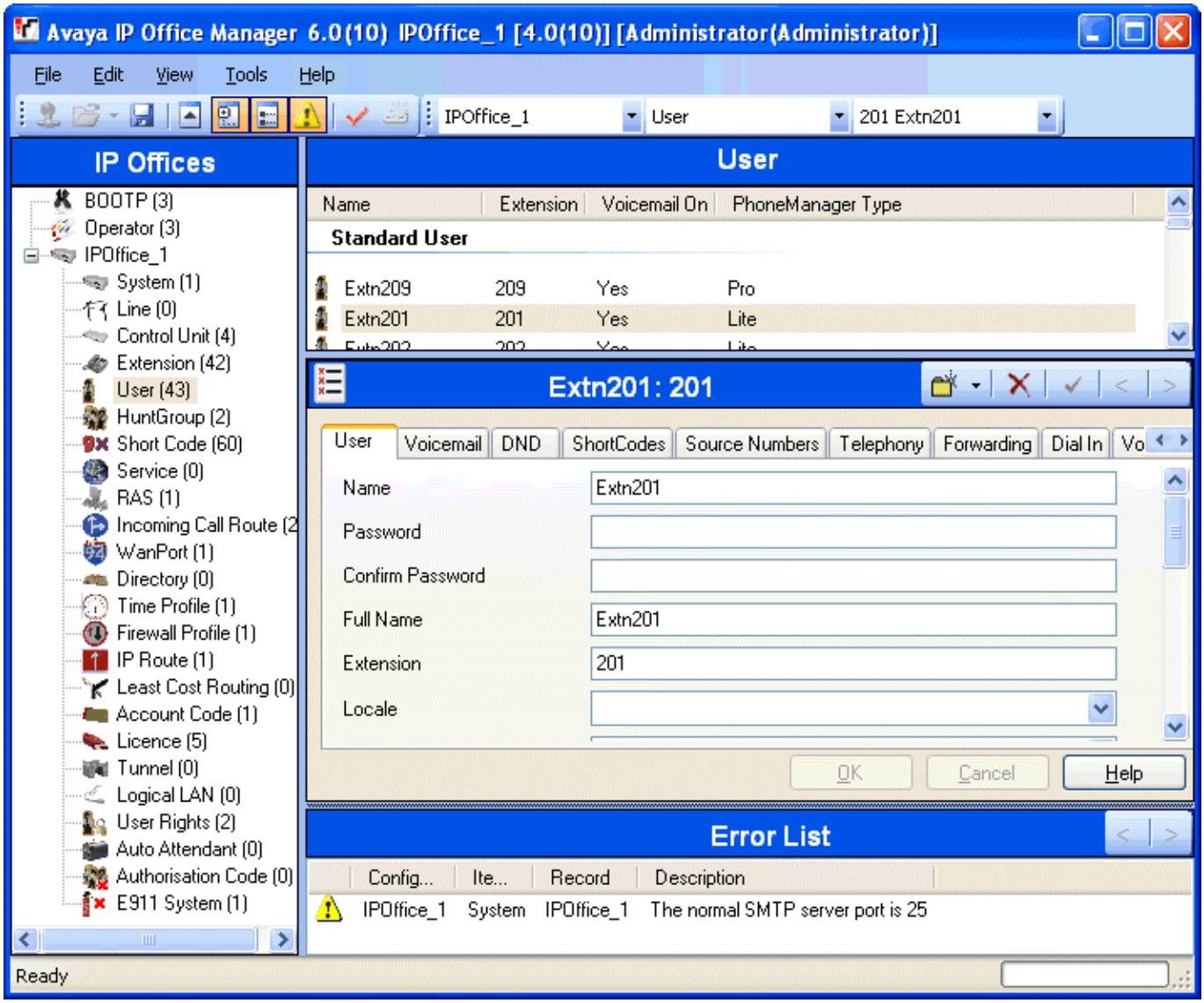
- ⚠ **WARNING - Password Change Required**
  New IP Office systems use default security settings. These settings must be changed to make the system secure. At minimum you must change the default passwords of the Security Administrator and the default Service Users. Failure to do so will render the IP Office system unsecure. See the **Security Mode** section for details.
- ⚠ **IMPORTANT**
  Manager is an off-line editor. It receives a copy of the IP Office system's current configuration settings. Changes are made to that copy and it is then sent back to the IP Office for those changes to become active. This means that changes to the active configuration in the system that occur between Manager receiving and sending back the copy may be overwritten. For example this may affect changes made by users through their phone or voicemail mailbox after the copy of the configuration is received by Manager.

Manager 6.1 is part of the IP Office 4.1 Admin suite of programs but can be used to configure IP Office systems from IP Office 2.1 upwards.

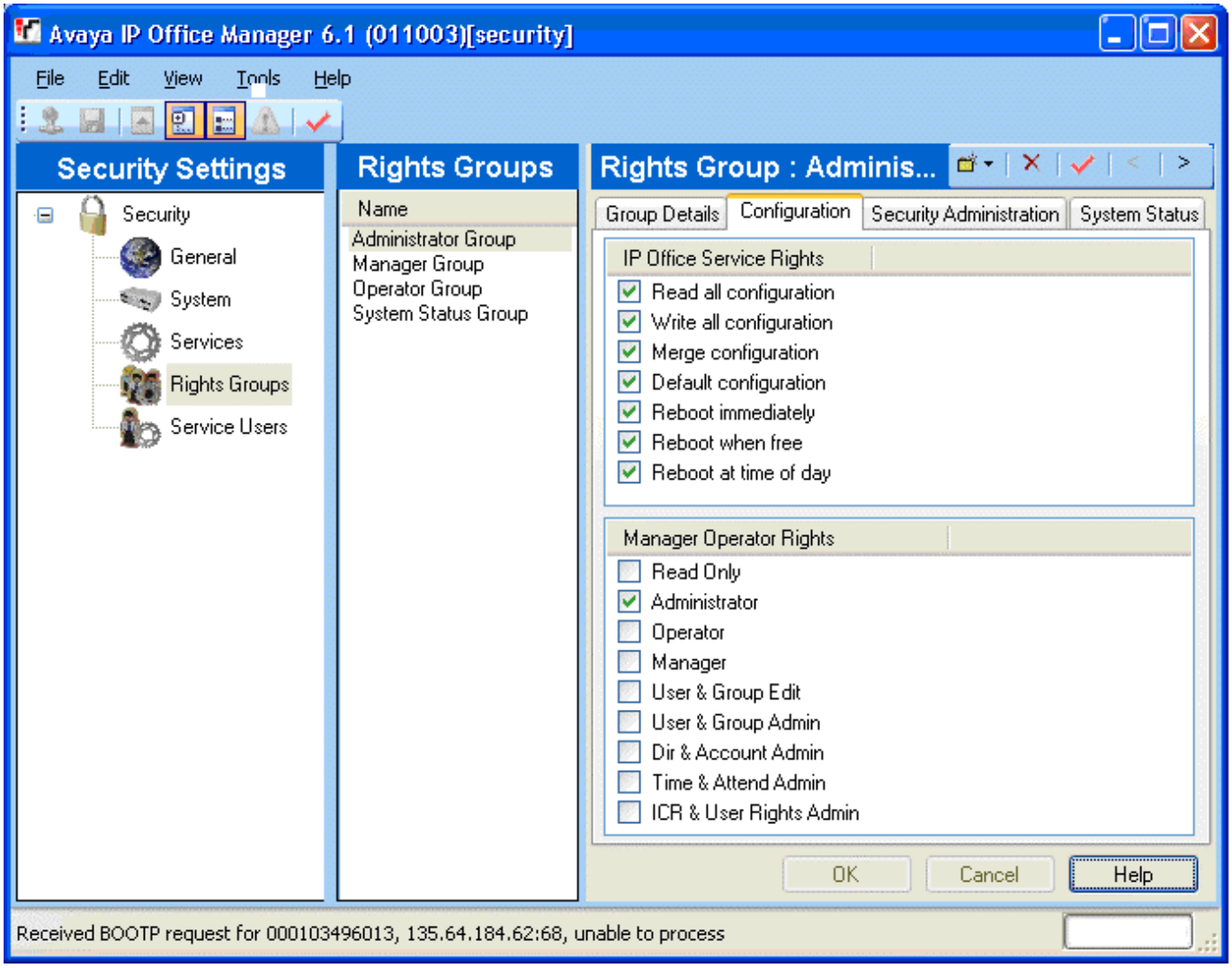
IP Office Functions

Manager performs a number of roles for IP Office systems.

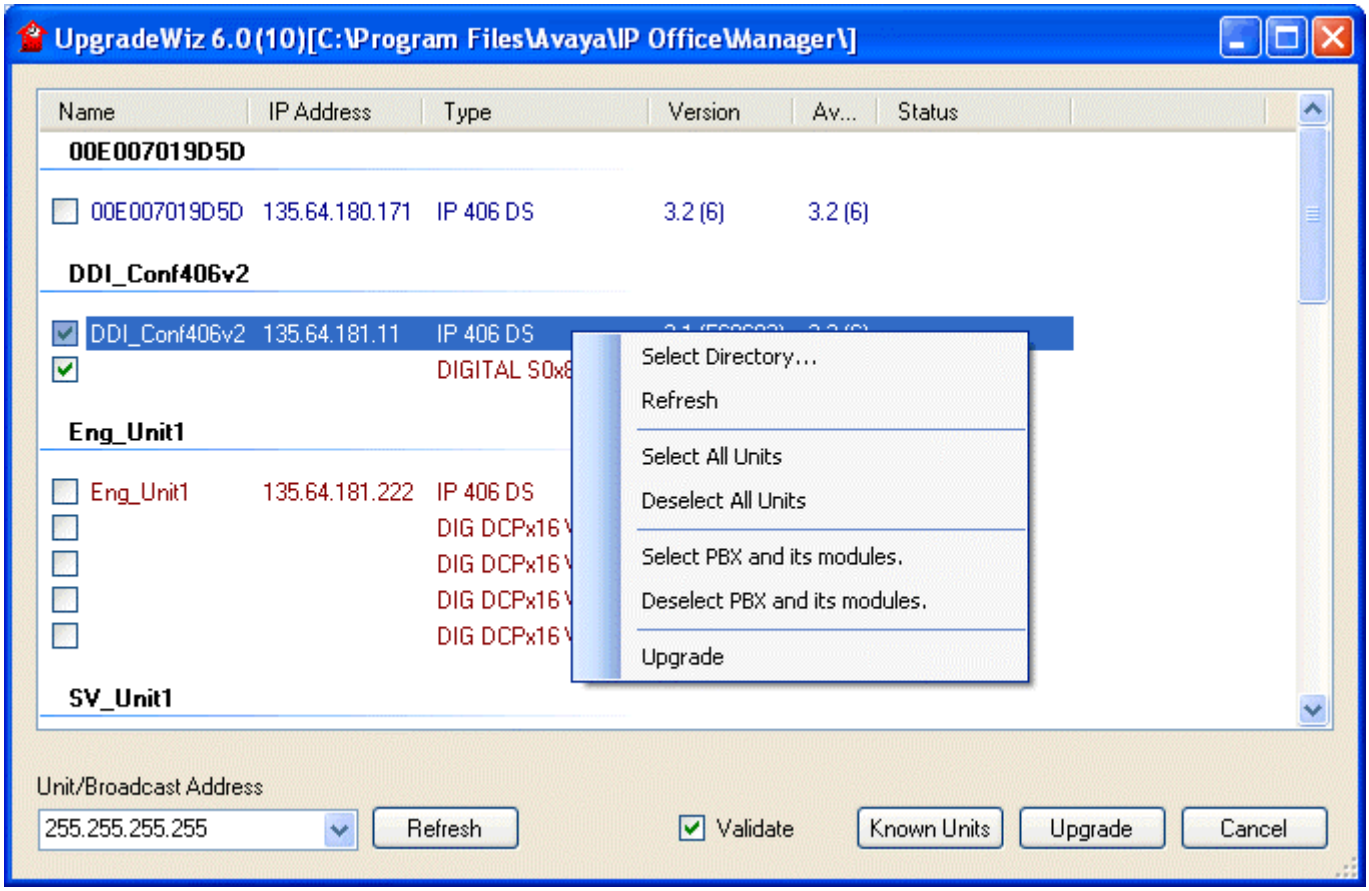
- **Configuration Settings Editor**
  In configuration mode Manager is used to edit configuration settings for IP Office systems. Those settings control the call and data function that the IP Office system provides to users and callers. Refer to the **Configuration Mode** section.



- **Security Settings Editor**
  In security mode Manager is used to edit the security settings of IP Office 3.2+ systems. Those settings are used to control user access to the configuration settings of the IP Office. Refer to the **Security Mode** section.



- **Upgrade Wizard**
  The Upgrade Wizard is a component of Manager used to upgrade the firmware run by the control unit and expansion modules within an IP Office system. See **File | Advanced | Upgrade**.



- **BOOTP Server**
  Manager acts as a BOOTP server, providing software files in response to BOOTP requests from IP Office systems. This task is required for maintenance. This function can be switched off if not required.

- **Time Server**
  Manager acts as an Internet Time server (RFC868), providing the time in response to requests for IP Office systems. This function can be switched off if not required.

- **TFTP Server**
  Manager acts as a TFTP server. This protocol is used by several types of Avaya phone to load software files during installation and upgrades. This function can be switched off if not required.

What's New in 4.1

This section summarizes the main changes in IP Office 4.1.

General Manager Changes

- **Optional Legal/Informational Message Display**
  When starting IP Office Manager, a message dialogue can be displayed which features **Continue** and **Cancel** (closing Manager) options. This can be used to display legal warning text or information text before Manager is used.
- **AIM Configured System Warning**
  If an IP Office 4.1+ configuration from an IP Office that has been configured through AIM, is opened in a standalone version of IP Office Manager, a warning message is displayed. This is to prevent misconfiguration of systems that should only be configured through the version of Manager embedded in the AIM suite of software.
- **Application Idle Timeout**
  A timeout can be enabled. After 5 minutes of no mouse or keyboard activity, Manager will request reentry of the service user password used to load the current configuration or security settings.
- **Card and Port Indication**
  For line types provided by the installation of physical trunk cards or modules, within the line settings the card slot or module location is now indicated and the port number on that device.
- **System Events**
  The System Alarms tab has been renamed Systems Events.

Security Enhancements

- **Service User Password Controls**
  Various controls have been added within the IP Office security settings for service user passwords. These control 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 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)** in available in configuration mode and **File | Reset Security Settings** in security mode.
- **Transport Layer Security (TLS) Secure Connection Support**
  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 access, security access and system status access) can be configured for secure and/or unsecure connect. Secure connect can include the exchange of security certificates between the IP Office system and the IP Office Manager PC.

Avaya SIP for Branch Support

The Avaya SIP for Branch is a service delivered by interlinking Avaya switches through an Avaya SES (SIP Enablement Service) server. IP Office 4.1+ supports connect to the SES server through the following new features:

- **SES Lines**
  This type of line is used for connection from the IP Office system to the SES server. It is a variant of the SIP trunk type and requires the IP Office to have **SIP Trunk Channel** licenses available.
- **Branch Prefix**
  Each system within a SIP for Branch network requires 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 dialing of the branch prefix followed by the extension number.
- **Local Number Length**
  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.

General IP Office Features

- **Time Profile Calendar Dates**
  IP Office Time Profiles have been enhanced. In addition to the existing weekly time patterns, specific times on particular calendar dates can now also be added. Dates in the current and next year can be specified, including multiple dates.
- Incoming Call Route Multiple Time Profile Support
  Incoming call routes have now been amended to allow the use of multiple time profiles, with separate destinations and fallback destinations for use when a particular time profile is in effect.
- **IP406 V2 LAN2 Support**
  RJ45 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. This enables the **System | LAN2** tab and associated settings within the IP Office configuration. This mode is controlled by a **Use Port 8 as LAN2** option on the **System | LAN1 | LAN Settings** tab.
- **System Events Syslog Support**
  In addition to using SNMP and SMTP email, the IP Office can now send system events to up to two Syslog server destinations. The Syslog output can include IP Office Audit Trail events (not supported for SNMP and SMTP email).
- **Phone Manager Pro Telecommuter Mode**
  This additional mode has been added to the available **Phone Manager Type** options. This mode is supported by Phone Manager Pro 4.1+. Users of this mode can start Phone Manager as either a remote or local application. In remote mode the user uses a data connection for Phone Manager and specifies a telephone number available to them to make/receive calls. The IP Office then makes calls to that number when the user makes or answer calls using their Phone Manager application. In local mode the application function as a normal Phone Manager Pro with the user's associated extension. For full details refer to the Phone Manager User Guide and Phone Manager Installation Manual.

Hunt Group Operation

- **Queuing Alert Extension**
  For each hunt group, when a number of queued calls threshold is reached, an analog extension can be alerted with ringing. This is intended for an extension connected to a loud ringer device or similar (that is calls are not answered at that extension). This feature is controlled through the **Hunt Group | Queuing** tab settings **Calls in Queue Threshold** and **Pots Extension to Notify**.

- **Automatic Recording Mailbox for Account Codes**
  By default automatic recordings for account codes are routed to the mailbox of the user making the call. Previously this could not be changed except through customized call flows on the Voicemail Pro. An alternate mailbox destination can now be specified through the **Account | Voice Recording** tab.

Telephony

- **Group Listen**
  Using group listen allows callers to be heard through the phone's handsfree speaker but to only hear the phone's handset microphone. This feature can be enabled/disabled using either short codes and or a programmable button. Note: Group listen is not supported on IP phones.

- **Disable Speakerphone**
  The handsfree speaker enabled by the **SPEAKER** key on Avaya DS and IP phones can be disabled through the IP Office extension configuration settings. This allows handsfree operation to be disabled where such operation is not desirable.

Button Programming

- **IP Office Date, Time and Version**
  The **Emulation | Self Administer** button function can be used to set the IP Office system date and time. It can also be used to view the IP Office control unit type and software version. The user must be configured as a **System Phone** (**User | Telephony**) and a value of ***2*** entered as the button's action data.

- **Headset Force Feed**
  On Avaya phones with fixed **HEADSET** buttons, a programmable button can be assigned to put the phone into headset force feed mode. In this mode, when headset mode is selected but the phone is idle, an incoming external call will cause a single tone and then be automatically connected.

- **Group Listen**
  The group listen feature (see **Telephony** above) can be assigned to a programmable button. That button can be used to switch group listen on/off and indicates when group listen is on.

- **Enhanced Conference Meet Me**
  For IP Office 4.1+ this button has been enhanced. Buttons associated with a particular conference ID will indicate when the conference is active. Callers connected on other appearance buttons can be transferred into the conference by pressing **TRANSFER** and then the Conference Meet Me button. This allows the user to place callers into the conference specified by the button without being part of the conference call themselves. This option is only support on Avaya phones with a fixed **TRANSFER** button (excluding T3 and T3 IP phones).

Short Codes

- **Group Listen On/Off**
  The group listen feature (see **Telephony** above) can be switched on/off through the use of the **Group Listen On** and **Group Listen Off** short code features.

- **Default Embedded Voicemail Auto Attendant Short Codes**
  Previously 4 system short codes were automatically added for each auto attendant added to the configuration. With the increase in the number of supported auto attendants to 40, the method of short code usage has changed to allow just 4 system short codes for all auto attendants by using the auto attendant number rather than name.

IP Office 500

- **IP Office 500 PRI Trunk Card (PRI-U)**
  This card can be added as a trunk daughter card to any IP500 base card except the Legacy Card Carrier base card. The card is available in single and dual port PRI variants. The IP500 PRI-U card supports E1, T1 and E1-R2 PRI modes. To select the mode required, right-click on the line in the group or navigation pane and select **Change Universal PRI Card Line Type**. The IP Office systems supports 8 B-channels for each IP500 PRI-U port fitted, using in-service channels from port 9 of slot 1 upwards. Additional B-channels up to the capacity of ports installed and PRI mode selected require **IP500 Universal PRI (Additional Channels)** licenses added to the configuration. D-channels are not affected by licensing.

    - With the introduction of the IP500 PRI-U trunk daughter card, the design of stand off pillars supplied with IP500 trunk daughter cards has been changed. New cards will be supplied with 2 pre-fitted metal stand off pillar and 3 loose plastic pillars. Screws and washers are provided for the metal pillars for the final installation onto the IP500 base card. This changes is required for IP500 PRI-U cards but has been applied to all trunk daughter card types. This does not affect existing trunk daughter cards supplied with 5 plastic stand off pillars.

- **H.323 Trunk Support in Standard Edition Mode**
  H.323 trunks (IP trunks and QSIG trunks) on IP Office 500 systems require the addition of IP500 Voice Networking licenses. At launch those trunk and license were only supported on IP Office 500 system running in Professional Edition mode. IP Office 4.1 allows licensed H.323 trunks to be used in Standard Edition mode also.

- **Small Community Networking in Standard Edition Mode**
  The above change allows Small Community Networking to be used with IP Office 500 systems running in Standard Edition mode. That includes Centralized Voicemail and, subject to the appropriate additional licenses, advanced Small Community Network features.

Embedded Voicemail

- **40 Auto Attendants**
  Previously on 4 auto attendants were supported with the IP Office configuration. IP Office 4.1 allows up to 40 Auto Attendants to be created and to be chained together to support a flexible multi-tiered operation. Each auto-attendant is numbered and that number can be used in short codes for accessing the auto-attendant.

- **Named Greeting Files - LVMGreeting**
  The field **Recording Name** was added in the IP Office 4.0 Q2 20007 maintenance release for use with IP Office systems being managed by the AIM suite. However the field was not useable with systems being managed by stand-alone IP Office Manager. For IP Office 4.1+ the utility required to create named greeting files (***LVMGreeting.exe***) is now provided with IP Office Manager. Those files can then be place on the embedded voicemail memory card and selected in the Recording Name field. The same recording can be shared between multiple auto-attendants. The tools is accessed from Manager via the menu command **Advanced | LVM Greeting Utility**. For full details refer to the IP Office Embedded Voicemail Installation manual.

Voicemail Pro

In conjunction with IP Office 4.1, Voicemail Pro 4.1 supports the following new features:

- **Automatic Recording Mailbox for Hunt Groups**
  By default automatic recordings for hunt groups are routed to the hunt group mailbox. Previously this could not be changed except through customized call flows on the Voicemail Pro. An alternate mailbox destination can now be specified through the **Hunt Group | Voice Recording** tab.
- **Automatic Recording Mailbox for Account Codes**
  By default automatic recordings for account codes are routed to the mailbox of the user making the call. Previously this could not be changed except through customized call flows on the Voicemail Pro. An alternate mailbox destination can now be specified through the **Account | Voice Recording** tab.
- **Call Data Tagging on Transfer Actions**
  The Transfer action now supports fields for setting the transfer source and description to display on phones receiving the transfer. The ability to associate call data for MS-CRM via **Assisted Transfer** actions is now also supported on **Transfer** actions.
- **Call Transfer Announcements**
  The **Transfer** and **Assisted Transfer** actions can be configure to announce the transfer to the caller. The announcement uses the recorded name of the mailbox associated with the transfer if available or the number if otherwise.
- **LIFO/FIFO Mailbox Operation**
  The default message playback order of First In-First Out (***FIFO***) can now be changed to Last In-First Out (***LIFO***). This is separately adjustable for new, old and saved messages. These are set through the **System Preferences | Housekeeping** tab (**Administration | Preferences | General**).
- **Time in Queue and Time on System Variables**
  Two new variables can be used in Queued and Still Queued call flows. They are **$TimeQueued** for the time in the queue and **$TimeSystem** for the time the call has been on the IP Office system.
- **Castelle Fax Server Support**
  The Voicemail Pro can be configured to recognize faxes of this type left in user's email mailboxes and include announcement of there presence in the user's mailbox prompts.
- **Hunt Group/Account Code Call Recording Destination**
  Previously the destinations for automatic call recording triggered by hunt groups or account codes could not be changed except through a custom Voicemail Pro call flow. The IP Office 4.1 configuration now allows the required destination for the call recording to be specified.
- **$DDI System variable for DDI Numbers**
  This variable is available on DDI calls passed from the IP Office to the Voicemail Pro.
- **Variable Routing (replaces the CLI Routing Action)**
  The existing CLI Routing action has been replaced by the **Variable Routing** action. This action allows the call routing to be based on matching specified values to system variables such as ***$CLI*** and ***$DDI***. The numbers to which matching is performed can include wildcards such as ***?*** for a single digits and ******* for any digits.

Key and Lamp Operation

- **Abbreviated Ring Control**
  For users with multiple call appearance buttons, it can be selected whether additional calls once a call is connected, are presented with a short single abbreviated ring or with normal ringing.
- Twinned Bridge/Coverage/Line Appearances
  For users with a twinned secondary phone, only calls on call appearances at their primary phone also alert at the secondary phone. For IP Office 4.1 it is possible to configure that calls alerting on bridged, coverage and line appearance buttons on the primary should also alert on the secondary.

Licenses

- **IP500 Voice Networking**
  This type of license is now supported on IP Office 500 systems running in Standard Edition mode. This allows those systems to use IP and QSIG trunks and to be included in a Small Community Network.
- **IP500 PRI Universal (Additional Channels)**
  The IP Office systems supports 8 B-channels for each IP500 PRI-U port fitted. Additional B-channels up to the capacity of ports installed and PRI mode selected require **IP500 Universal PRI (Additional Channels)** licenses added to the configuration. D-channels are not affected by licensing.
- **VPN IP Extensions Licenses**
  IP Office 4.1+ supports 4610, 4621, 5610 and 5621 phones running the VPNremote firmware. These work in conjunction with the **Extension | VoIP | VPN Phone Allow** setting. The phones are licensed against **VPN IP Extensions** licenses added to the IP Office configuration.

Windows Operating System Support

- **Windows Vista**
  With IP Office 4.1, Vista support is expanded to all IP Office 4.1 applications also supported on Windows XP Pro. Note that the Vista support refers to Vista Business Ultimate and Vista Enterprise editions; the Vista Home Basic and Vista Home Premium editions are not supported.

System Status Application

The following changes have been made to the System Status Application (SSA) including in the IP Office 4.1 suite.

- **Device Version Numbers**
  IP500 trunk, extension and VCM cards have electronic version numbers. SSA is now able to display those version numbers.
- **Digital Trunk Clock Source Change Alarm**
  SSA can report when the clock source being used by the IP Office system changes from one digital trunk to another.

What's New in 4.0 Q2 2007

This section summarizes the changes made for the May 2007 maintenance release of the IP Office 4.0 suite of applications. This is not an exhaustive list. For full details refer to the appropriate IP Office Technical Bulletin.

- **Line Name and Channel Name Display**
  By default, for calls where no incoming caller ID (ICLID) information is available, the IP Office inserts the word ***External*** wherever ICLID information is normally displayed. The **NoUser** source number value **SHOW_LINEID_NOT_OUTSIDE** can be used to make available for most external trunks a **Nam**e field. Any the text entered into this field is then used in place of the ***External*** indication on calls with no ICLID. This feature is not used with SIP, IP DECT, and S0 lines. On T1 lines, a **Name** field is also made available for individual channels and if set overrides the line name field. If set, the name is also used as the default label for line appearance buttons set to the line or channels on that line.
- **Call Pickup Line Short Code**
  This short code feature allows the answering of calls ringing, parked or held on a line by use of the line's Line Appearance ID. This is intended for use with phones where Line Appearance buttons cannot be programmed. Not supported on T3 phones.
- **Call Pickup User Short Code**
  This short code feature allows the answering of calls ringing, parked or held against a user by use of the user's Extension Number setting. If the targeted user has multiple calls, preference is given to ringing, parked and held calls in that order. Not supported on T3 phones.
- **Embedded Voicemail**
  The following new features appears for Embedded Voicemail:
  - **Auto Attendant Greeting 'Record Name'**
    This field appears next to the short code used for recording auto-attendant prompts. The field is only useable for IP Offices being managed through the **Avaya Integrated Management (AIM)** application.
  - **Enable Local Recording Control**
    The use of short code to record auto attendant greetings can be disabled if required. The short codes are still active and can be used to hear the current prompts, however the option to record a new prompt will not operate.
  - **Embedded Voicemail Shutdown Short Code**
    The Embedded Voicemail memory card is not a hot-swappable device, and so the IP Office system must be switched off in order to remove/replace the memory card. Use of this short code feature allows safe removal of the memory card whilst the IP Office system is running.
- **Known IP Office System Discovery**
  IP Office Manager can be configured to record details of IP Office systems it discovers and to then allow later rediscovery of those known systems. This feature is only available when Manager has been configured with a .csv file location to which to record known IP Office system details. When this has been done, a **Known Units** button is available within the IP Office Manager discovery screen.
- **Support for Avaya Integrated Management (AIM)**
  Avaya Integrated Management (AIM) is a suite of applications that can be used to monitor and maintain a large number of Avaya systems as multiple locations. Support for IP Office systems has been added to this application suite.
- **Custom Locale**
  For some systems, the locales fully supported by IP Office may not match the local requirements. In these cases, the option ***Customize*** can be selected in the **Locale** field of the **System | System** tab. Additional options are then made visible to select the tone usage, CLI type and busy tone detection settings.
- **System Time Setting Through Phones**
  For systems without access to an appropriate time server or where an immediate time and date change is required, a manual method for setting the system date and time has been added.
- **Internal Twinning for North America**
  The Internal Twinning function was added in the IP Office 3.1 release but not supported for systems with a North American locale. This feature is now supported in North American locales.
- **IP DECT**
  The Avaya IP DECT solution is now supported in North American locales. For IP Office Manager this means that an IP DECT line and IP DECT extensions can now be created on systems with a North American locale.

- **3641 and 3645 Wireless IP Phones**
  These phones are now supported. They can be used with 802.11a, 802.11b and 802.11g wireless networks.
- **T3 Direct Media Support**
  T3 IP phones have previously not supported Direct Media mode connection. For T3 IP phones with T246 or higher firmware that restriction no longer applies and the specific restrictions on the number of T3 IP phones can be removed.

What's New in 4.0

This section summarizes the main changes in the IP Office 4.0 General Availability release.

- **Manager Changes**
- **Hardware Support Changes.**
- **System Status Monitoring.**
- **SIP Trunks.**
- **Hot Desking (Logging In/Out).**
- **Voicemail.**
- **Hunt Groups.**
- **Alternate Route Selection (ARS).**
- **ISDN Features.**
- **Advanced Small Community Networking.**
- **Key and Lamp Operation.**
- **Licenses.**
- **Other Features.**

Manager Changes

- **Validation Control**
  Control of when Manager applies automatic validation to configuration files is now available through the **File | Preferences** menu.
- **Busy on Held Validation**
  The **Tools** menu now contains a **Busy on Held Validation** option that checks all users. Previously this check was only performed when a user's settings were edited.
- **Line Renumber**
  The **Tools** menu now contains a **Line Renumber** option for renumbering all Line Appearance ID's upwards from a selected base number.
- **BOOTP Entries**
  The maximum number of BOOTP entries has been increased from 20 to 50.

Hardware Support Changes

- **IP Office 500 System Unit (IP500)**
  This control unit has no integral extension or trunk ports. On its front the unit has 4 card slots into which IP500 base cards can be inserted. These card provide various combinations of digital station port, analog extension ports, voice compression channels and trunk ports. On its rear the unit has slots for embedded voicemail, a feature key dongle slot, audio port, door relay switch port and ethernet LAN/WAN ports plus 8 external expansion module ports.
    - 4406, 4412 and 4424 are only supported on external expansion modules. They are not supported directly on the IP500 system unit.
- **IP Office Standard Edition**
  By default the IP500 control unit runs a subset of full IP Office functionality called IP Office Standard Edition. In this mode the IP Office is restricted as follows. These restriction can be removed by adding an ***IP500 Upgrade Standard to Professional*** license to the configuration.
    - The IP500 is restricted to a maximum of 32 users using ports on base cards in the control unit.
    - In Standard Edition mode the IP500 does not support any external expansion modules.
    - The applications Embedded Voicemail, Phone Manager Lite/Pro, SoftConsole, TAPI, Delta Server and CBC, Manager, SSA and Monitor are supported.
        - Advanced applications such as Voicemail Lite/Pro, CCC, Conference Center, MS-CRM, etc are not supported.
    - IP trunks (H323, QSIG, SCN) not supported. IP DECT and SIP trunks are supported. Enabling IP trunks requires an ***IP500 Upgrade Standard to Professional*** license and ***IP500 Voice Networking*** licenses.
    - Meet-me conferencing is not supported.
- **Hardware Support**
  The following hardware is not supported with IP Office 4.0.
    - The WAN3 external expansion module is not supported (the WAN3 10/100 is still supported).
    - All Network Alchemy external expansion modules are no longer supported.
    - The IP403 and IP406 V1 control units are not supported.
- **Terminal Support**
  The following terminals are not supported by IP Office 4.0. They may function but have not been tested with 4.0 and any faults reported with 4.0 will not be fixed.
    - The 20DT Analog DECT phone used with IP Office Analog DECT and Compact DECT is not supported. It may be used with Avaya IP DECT but only as a generic GAP compatible DECT device.
    - The 4606, 4612 and 4624 phones are no longer supported.
    - The Transtalk 9040 is no longer supported.

System Status Monitoring

- **System Status Application (SSA)**
  This application provides information about the equipment and resources in IP Office 4.0 and higher systems. This information includes indication of alarms and details of current calls in progress. Use of SSA requires a service user name and password configured for System Status in the IP Office's security settings.
- **Call Status Application**
  This application is not supported by IP Office 4.0. It has been replaced by the IP Office System Status Application above. Call Status is still included in the IP Office Admin suite for use with pre-4.0 IP Office systems.
- **Monitor**
  The SysMonitor application has been enhanced but is no longer fully backwards compatible with pre-IP Office 4.0 systems. Therefore two versions of Monitor are included in the IP Office Admin suite; version 6.0 for use with IP Office 4.0 systems and version 5.2 for use with pre-IP Office 4.0 systems.

SIP Trunks

- IP Office 4.0+ supports SIP calls through the implementation of SIP trunks. Through normal short code routing of outgoing group ID's any user can make outgoing calls using SIP services, ie. users do not require SIP phones to make and receive SIP calls. Incoming call routing can be used to route incoming calls on SIP trunks. SIP trunks are a licensed feature.

Hot Desking (Logging In/Out)

- **Agent Status on No Answer**
  The IP Office can change the status of call center agents who do not answer a hunt group call presented to them. This can include logging the agent off the system. The change of status can be set per user and the use of this option can be set per hunt group.
- **Remote Hot Desking**
  Users can now hot desk between systems in a Small Community Network. This requires a ***Advanced Small Community Networking*** license in the system where a user logs on remotely.
- **Logging Out**
  User who do not have a login code set cannot log out.
- **NoUser User**
  By default the NoUser user's first programmable button is set to the Login function.

Voicemail

- **Voicemail Channel Reservation**
  IP Office 4.0 allows the licensed voicemail channels between Voicemail Pro and the IP Office to be reserved for particular functions or to be left unreserved for any function.
- **Visual Voice**
  Users with Avaya multi-line display phones can use a display menu driven interface for accessing and controlling the playback of messages in voicemail mailboxes. This is supported with Voicemail Pro, in Intuity emulation and IP Office modes, and Embedded Voicemail.
- **Voice Recording**
  A number of improvements have been made to call recording operation in conjunction with Voicemail Pro. In the descriptions below 'party' can mean user, hunt group or incoming call route involved in a call.
    - Calls including IP end points, including those using Direct Media, can now be recorded.
    - Voicemail Pro automatic call recording can be triggered by Incoming Call Routes.
    - Where recording is triggered by several parties within the same call, separate recordings are produced for each party.
        - For example if both automatic hunt group recording and automatic user recording are applicable to the same call, separate recordings are produced for both the hunt group and the user.
        - If a call is to be recorded multiple times to the same mailbox only a single recording is made; resolved in the order of: incoming call route, account Code, hunt group and user settings.
    - Recording only continues while the party triggering the recording is part of the call, for example:
        - Recording triggered by a user stops when that call is transferred to another user.
        - Recording triggered by a hunt group continues if the call is transferred to another member of the same group. Recording stops if the call is transferred to a user outside the hunt group.
        - Recording triggered by an incoming call route continues for the duration of the call on the IP Office system.
    - Parking and holding a call pauses recording. Recording is restarted in the same file when the calls is unparked or taken of hold.
- **User Announcements**
  With Voicemail Pro 4.0 and higher, announcements are supported for calls waiting to be answered by an individual user. User start points in Voicemail Pro now include Queued and Still Queued options.
- **Embedded Voicemail**
    - Embedded voicemail is supported on the IP500 control unit using the same options as the IP406 V2 control unit.
    - Hunt group announcements are supported using embedded voicemail.
    - The auto-attendant menu includes a Fax option for rerouting fax calls.
    - Support for Visual Voice.
    - Support for Fast Forward (#), Rewind (*), Skip message (9) and Call Sender (**) when listening to messages.
    - Support for 3 voicemail reception destinations using *0, *2 and *3.

Hunt Groups

- **Agent Status on No Answer**
  The IP Office can change the status of call center agents when a hunt group call is presented but not answered. The agent can be put into busy wrap-up, busy not available or logged off. The change of status can be set per user and the use of this option can be set per hunt group. This feature is not applied if the call is answered elsewhere before the No Answer Time expires.
- **Fallback**
  Night service fallback using a time profile is no longer applied to a hunt group already set to out of service. Short codes and buttons can be used to set a hunt group out of service, overriding the night service time profile.
- **Voicemail Answer Time**
  A separate value has been added to hunt group settings to control when hunt group calls go to voicemail if unanswered. The default value is 45 seconds.
- **Queuing**
  - Previously the definition of queued calls did not include calls ringing against hunt group members. The definition now includes ringing calls and calls waiting to be present for ringing.
  - Control and usage of announcements has been separated from queuing (see below).
  - The queue limit can be set to include queued and ringing calls or just queued calls.
- **Announcements**
  - Hunt group announcements have been separated from hunt group queuing and can be used even when queuing is off.
  - Hunt group announcements are now supported by Embedded Voicemail in addition to Voicemail Pro and Voicemail Lite.
  - The times for the first announcement, second announcement and between repeated announcements are configurable.
- **Advertised Hunt Groups**
  A hunt group can be set to be 'advertised'. This requires an ***Advanced Small Community Networking*** license. Hunt groups that are advertised can be dialed by users on other systems within the Small Community Network (SCN) without the need for short codes.
- **SCN Distributed Hunt Groups**
  Hunt groups in a Small Community Network can include members located on other systems within the network. This feature requires entry of a ***Advanced Small Community Networking*** license on each system. Distributed hunt groups are automatically advertised to other systems within the SCN.
- **Idle Status**
  For longest waiting hunt groups, the type of calls that change a hunt group member's idle status can be selected.
- **Call Presentation**
  When additional calls are waiting to be presented, additional hunt group members are alerted using the hunt group type. However when any member answers a call it will be the first waiting call that is answered.
- **Set Hunt Group Night Service and Set Hunt Group Out of Service Short Codes**
  Previously the **Set Hunt Group Night Service** and **Set Hunt Group Out of Service** short code features toggled. That behaviour is not supported in 4.0 and higher.
- **Voicemail Mailbox Operation**
  For IP Office 3.2 and earlier, when voicemail was invoked, the mailbox of whichever hunt group was currently handling the call was used, for example the mailbox of the overflow or night service hunt group might be used if the call had gone from the original hunt group to an overflow or night server hunt group. For IP Office 4.0 and higher, the mailbox of the originally targetted hunt group is used even if the call has overflowed or gone to a night server hunt group.

Alternate Route Selection (ARS)

- **Least Cost Routes (LCR)**
  LCR has been replaced by ARS. On systems being upgraded to IP Office 4.0, any LCR entries will be automatically converted as far as possible to ARS forms. However due to the difference in method of operation the ARS forms will need to be checked.
- **Secondary Dial Tone**
  Where secondary dial tone is required it is provided through a check box option in ARS. This simplifies the configuration of secondary dial tone.
- **Outgoing Call Routing**
  LCR forms were never explicitly applied to particular calls. Instead any number to be dialed externally, was compared to the LCR short codes for a possible match. In IP Office 4.0, dialing short codes are explicitly routed either to a outgoing line group or to an ARS form.

ISDN Features

The following ISDN features are now supported by IP Office 4.0+. Note that availability of these feature is dependant on their also being supported and available from the ISDN service provider for which there may be charges.

- **Malicious Call Identification - MCID**
  Short codes and button programming features have been added so that users can be configured to trigger this activity at the ISDN exchange when required.
- **Advice of Charge - AOC**
  Advice of charge during a call (AOC-D) and at the end of a call (AOC-E) is supported for outgoing ISDN calls other than QSIG. The call cost is displayable on T3 phones and included in the IP Office Delta Server output. The IP Office allows configuration of call cost currency and a call cost mark-up for each user.
- **Call Completion to Busy Subscriber - CCBS**
  CCBS can be used where provided by the ISDN service provider. It allows a callback to be set on external ISDN calls that return busy. It can also be used by incoming ISDN calls to a busy user.
- **Partial Rerouting - PR**
  When forwarding a call on an ISDN channel to an external number using another ISDN channel, partial rerouting informs the ISDN exchange to perform the forward, thus freeing the channels to the IP Office. Not supported on QSIG.

Advanced Small Community Networking (Advanced SCN)

The following new features are supported for IP Office 4.0+ Small Community Networks. Note that these feature require entry of an Advanced Networking License into systems in the network.

- **Network Hot Desking**
  Hot desking is supported between IP Office systems within the Small Community Network.
- **Distributed Hunt Groups**
  Hunt groups can now include members who are located on different IP Office systems within the Small Community Network.
- **Break Out**
  This feature is provided primarily to support network hot desking but can be used for other purposes. It allows the dialing on one system in the network to be done as if dialed locally on an other system.

Key and Lamp Operation

The following key and lamp operation features were added in IP Office 4.0:

- **Delayed Ring Preference**
  This user telephony setting works in conjunction with the user's **Ringing Line Preference** setting. It sets whether ringing line preference should use or ignore the ring delay applied to the user's appearance buttons.
- **Answer Pre-Select**
  Normally when a user has multiple alerting calls, only the details of the call on current selected button are shown. Pressing any of the alerting buttons will answer the call on that button, going off-hook will answer the current selected button. Enabling the user telephony setting **Answer Pre-Select** allows the user to press any alerting button to make it the current selected button and displaying its call details without answering that call. To answer a call when the user has **Answer Pre-Select** enabled, the user must press the alerting button to display the call details and then either press the button again or go off-hook.
- **Reserve Last CA**
  Phones with appearance buttons require a free call appearance button to perform actions such as call transfers. However it is possible in some scenarios for all available call appearances to be occupied or alerting. The user telephony setting **Reserve Last C**A can be used to restrict the user's last call appearance button for outgoing calls only.

Licences

The following new licenses are used by IP Office 4.0:

- **IP500 Upgrade Standard to Professional**
  This license is required for an IP500 system to run in IP Office Professional Edition mode rather than IP Office Standard Edition mode. It is a pre-requisite for the IP500 Voice Networking licenses and any licensed features not supported in Standard Edition mode.
- **IP500 Voice Networking (Base 4 channels)**
  For IP500 systems running in Professional Edition mode, this licences enables support for H323 IP trunks between IP Office systems and QSIG or Small Community Networking over those trunks.
    - **IP500 Voice Networking (Additional channels)**
      Allows an additional 4 H323 voice networking trunks.
- **IP500 VCM Channels**
  Used with the IP500 VCM 32 and IP500 VCM 64 base cards. Each card supports 4 channels by default, with additional channels enabled by the addition of licenses.
- **SIP Trunk Channels**
  This license is used to configure the maximum number of simultaneous SIP trunk calls supported. Multiple licenses can be added for the cumulative number of SIP trunks required.
- **Advanced Small Community Networking**
  This license is used to enable support for hosting hot deskers from remote systems, creation of distributed hunt groups and the viewing of advertised hunt groups.

Other Features

- **Private Call**
  Users can set a status of private call using short codes or a programmed button. Private calls cannot be recorded, intruded on, bridged into or monitored.
- **RTP Relay**
  RTP relay allows much more efficient use of the voice compression channels available in an IP Office system:
  - Calls between IP endpoints using the same audio codecs that are routed via the IP Office (for example when not using direct media path) no longer use voice compression channels.
  - Call setup and progress tones no longer require a voice compression channel. The exceptions are short code confirmation tones, ARS camp on tone, account code entry tone and G723 calls (except Call Waiting).
  - Page calls to IP devices use G729a only and therefore only 1 channel regardless of the number of IP devices.
  - For T3 IP devices to benefit from RTP relay they must be configured to 20ms packet size.
- **Password Lockou**t
  Any phone features that require a validated entry (for example password or account code entry) will automatically fail if they have been preceded by 4 failed attempted in the previous 90 seconds.
- **Firewall IP Office Service Controls**
  The IP Office firewall standard settings now include controls to drop or allow connects to IP Office 3.2 configuration settings, security settings and system status.
- **User Announcements**
  User announcements can be configured for use with Voicemail Pro. These announcements are used for external calls waiting to be answered.
- **Feature Key Dongle Serial Number**
  The IP Office configuration settings now displays the serial number of the last Feature Key dongle with which the system validated its licenses and whether the dongle is local (ie. serial or Smart Card) or remote (ie. USB or parallel).
- **Line ID Numbers**
  For defaulted systems, all lines supported line ID numbers are numbers from 701 upwards by default. The Line Renumber tool is now available again within Manager to renumber all lines starting from a user selected starting number.
- **Ending Conferences**
  - For pre-4.0 IP Office systems, if a conference has two parties, and one party leaves, the conference call is ended. This may affect conferences that are just beginning but currently only contain the first two parties to join.
  - For IP Office 4.0, a conference remains active until the last extension or trunk with reliable disconnect leaves. Connects to voicemail or a trunk without reliable disconnect (for example an analog loop-start trunk) will not hold a conference open.
- **Disconnect Tone:**
  For digital and IP phones, when the IP Office detects that the far end of a call has disconnected it can either make the near end go idle or play disconnect tone. By default this behaviour depends on the system locale. The **Disconnect Tone** field on the **System | Telephony** tab can be used to override the locale default and force either disconnect tone use or go idle.

Installing Manager

Manager is a component of the IP Office Admin suite of applications. This suite is supplied on the IP Office Administrator Applications CD and the IP Office DVD. In addition to Manager the suite includes:

- **System Monitor**
  This is a tool for system installers and maintainers. Interpreting the information output by System Monitor requires detailed data and telecoms knowledge.
- **Feature Key Server**
  Only install this application in the PC will be hosting the IP Office systems USB or parallel port license key dongle.
- **Voice Mail Lite**
  A license free voicemail application that provides mailboxes for all users and hunt groups. This should not be installed if another voicemail system such as IP Office Embedded Voicemail or Voicemail Pro is installed.
- **System Status Application**
  This is a Java application that can be used to monitor the status of the IP Office system such as extension, trunks and other resources. It displays current alarms and most recent historical alarms.
- **Call Status**
  This application is for pre-4.0 IP Office systems. For IP Office 4.0 and higher use the System Status Application.

PC Requirements	Minimum	Recommended
Processor	600MHz Pentium or AMD Opteron, AMD Athlon64, AMD Athlon XP.	800MHz Pentium or AMD Opteron, AMD Athlon64, AMD Athlon XP.
RAM	128MB	256MB
Hard Disk Space	1GB - 800MB for .NET2, 200MB for Manager.	1.4GB - 800MB for .NET2, 600MB for the full IP Office Admin suite.
Display	800 x 600 - 256 Colors Default 96dpi font display only.	1024 x 768 - 16-bit High Color Default 96dpi font display only.
Operating System	Windows XP Professional with SP2. Windows Vista (excluding Home Editions) (IP Office Manager 6.1+) Windows 2000 Professional with SP4. Windows 2000 Server with SP4. Windows 2003 Server. Windows 2003 SBS. Note: 64-bit versions of the operating systems above are not supported.	

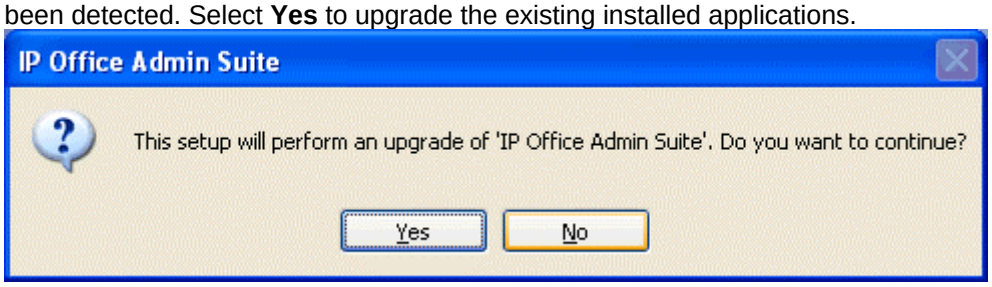
- **.NET**
  IP Office Manager requires .NET2. This is installed as part of the IP Office Admin suite if not already present on the PC. If .NET1 is present it should not be removed as .NET1 is required by other IP Office applications such as Voicemail Pro and Conferencing Center.
- **Java**
  The IP Office System Status application requires Java. This is installed as part of the IP Office Admin suite if not already present on the PC.
- **Language Support**
  The Manager application can run in English, French, German, Brazilian Portuguese, Dutch, Italian and Latin Spanish. By default this determined by the best match to the PC's regional setting. The online help is only provided in English, French and German.

Installing Manager
If applications in the IP Office Admin Suite other than Manager are required, we strongly recommend that you refer to the IP Office Installation Manual.

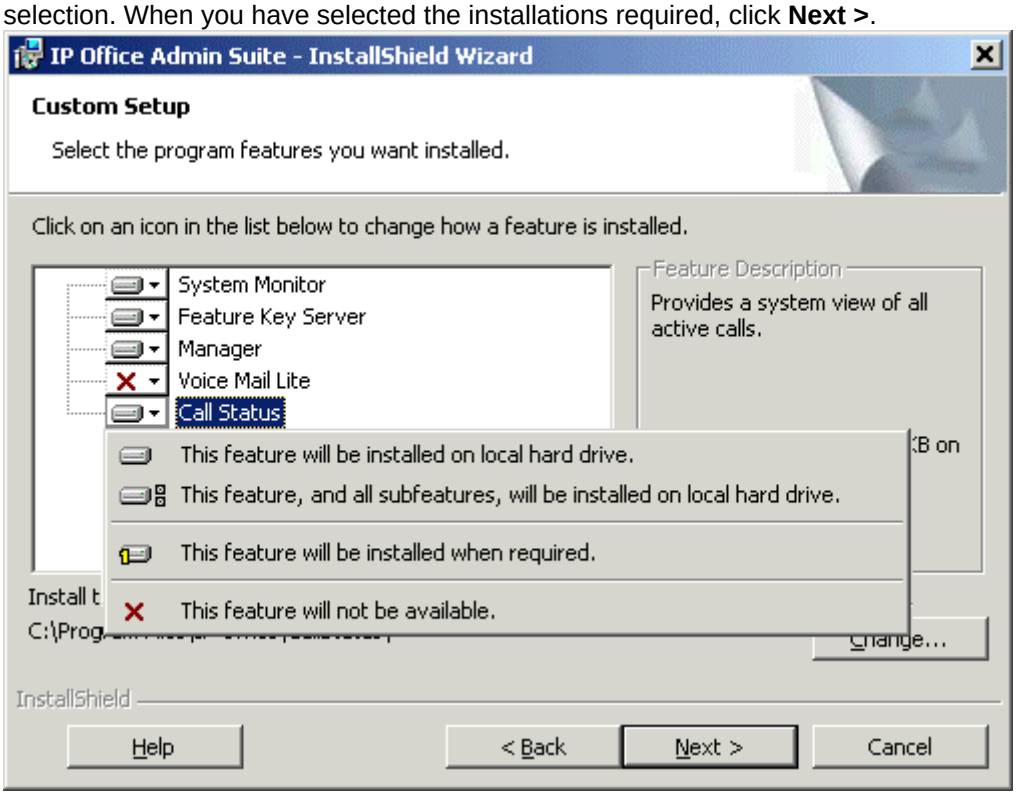
Note

- This installation process will install Windows .NET2 if not already present. The installation of .NET2 may require some systems to restart and the installation process to then be restarted.

1. If a pre-4.0 version of the IP Office Admin suite is installed it must be removed. This is done using the **Add or Remove Programs** option in the Windows **Control Panel** and selecting **IP Office Admin Suite** and then **Remove**.
2. Insert the CD. The installation process should auto start. If it does not auto start, open the CD contents and double-click **setup.exe**.
3. Select the language you want to use for the installation process. This does not affect the language used by Manager which will attempt to match the Windows regional setting. Click **Next >**.
    - If the following appears it indicates that a previous installation of the IP Office Admin suite has been detected. Select **Yes** to upgrade the existing installed applications.



4. If required select the destination to which the applications should be installed. We recommend that you accept the default destination. Click **Next >**.
5. The next screen is used to select which applications in the suite should be installed. Clicking on each will display a description of the application. Click on the ▾ next to each application to change the installation selection. When you have selected the installations required, click **Next >**.



6. The applications selected are now ready to be installed. Click **Install**.
7. Following installation, you will be prompted whether you want to run the IP Office Admin Suite. Selecting **Yes** runs IP Office Manager.
8. On some versions of Windows, you may be required to restart the PC. Allow this to happen if required.

Changing the Installed Applications
The **Add or Remove Programs** option can be used to change the selection of IP Office Admin suite applications that are installed. Locate ***IP Office Admin Suite*** in the list of programs and select **Change**.

Adding a Manager Start Dialogue
A warning or information dialogue can be added that will be displayed every time Manager is started. The user must then select **Continue** to use Manager or **Cancel** to quit.

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

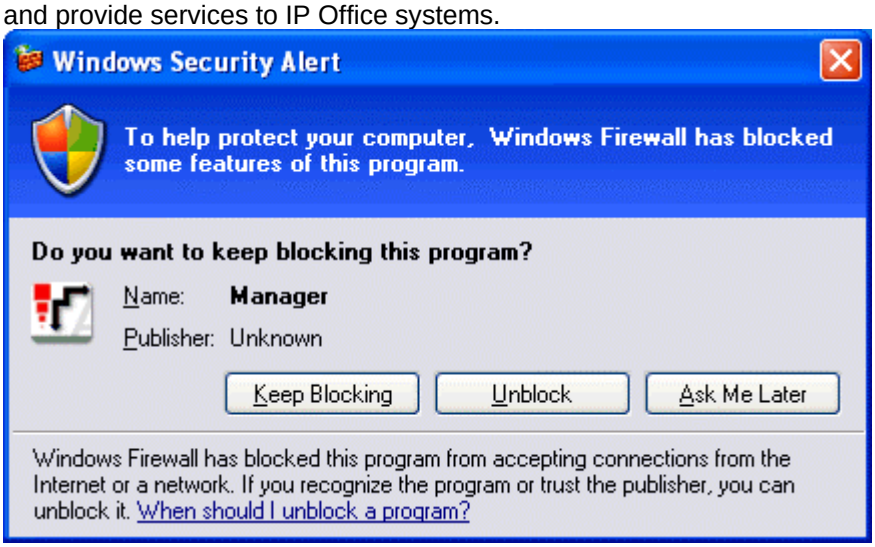
1. Create a file called **etcissue.txt** using a tool such as Windows Notepad or WordPad.
2. Add the warning or information required to the file.
3. Save the file as either plain text or RTF format. RFT format allows font style and selection options and the use of graphic files within the document.
4. Place the text file in the Manager application program directory, by default ***C:\Program Files\Avaya\IP Office\Manager***.

Starting Manager

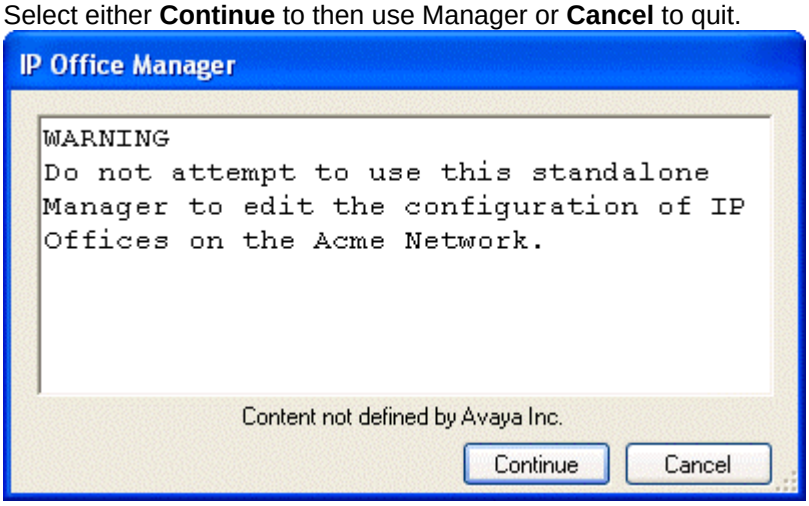
No operator name or password is required to start this version of Manager. A name and password is only required when performing an action that requires communication with an IP Office system; for example getting the configuration, send the configuration back, rebooting the system, etc.

Starting Manager

1. Select **Start** and then **Programs** or **All Programs** depending on the version of Windows.
2. Select the **IP Office** program group.
3. Select **Manager**.
4. On Windows XP systems, a Windows Security Alert may appear. Select **Unblock** to allow Manager to run and provide services to IP Office systems.



5. If an IP Office Manager dialogue appears, read the information or legal warning contained in the dialogue. Select either **Continue** to then use Manager or **Cancel** to quit.



6. The next section of this documentation describes the Manager interface and how to load and edit an IP Office's configuration settings.

Changing the Manager Language

The Manager application can run in US English, UK English, French, German, Brazilian Portuguese, Dutch, Italian and Mexican Spanish. By default it tries to use the best match to the PC's regional location settings, otherwise it will use UK English.

The process below can be used to run Manager in one of its supported languages. However it does not change the language used for help file content.

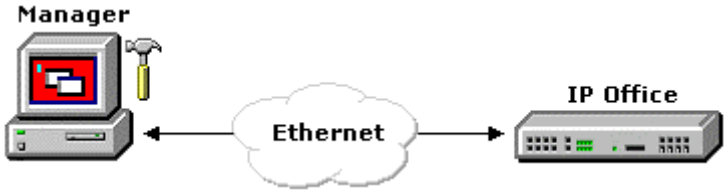
1. Create a Windows shortcut to the IP Office Manager application .exe file. By default this file is located in ***C:\Program Files\Avaya\IP Office\Manager\Manager.exe***.
2. Right-click on the shortcut and select **Properties**.
3. The **Target** field can be used to specify the locale setting that Manager should use. For example, for Italian the **Target** should have ***-locale:it-IT*** added to the end.
    - For example: ***"C:\Program Files\Avaya\IP Office\Manager\Manager.exe" -locale:it-IT***
4. The available locales for IP Office Manager are:

IP Office Manager Language	Shortcut Locale Setting
Brazilian Portuguese	-locale:pt-Br
Dutch	-locale:nl-NL
French	-locale:fr-FR
German	-locale:de-DE
Italian	-locale:it-IT
Mexican Spanish	-locale:es-MX
US English	-locale:en-US

5. Click **OK**.
6. The IP Office Manager application should now run in the selected language when launched using the updated shortcut.

Connecting Manager to IP Office

During IP Office installation and setup, connection should always be made using a Manager PC directly connected to the IP Office.



Following IP Office installation and setup, the Manager PC can be run from a variety of locations.

IP Addresses

- The IP Office address for connections from Manager is its LAN1 IP Address. That address is set through the **System | LAN1** tab within the IP Office configuration settings.
- If the IP address of the Manager PC is changed, Manager should be closed and restarted.

Discovery

The **Select IP Office** discovery process used by Manager to locate IP Office systems can use both UDP and TCP.

- Pre-3.2 IP Office systems respond to UDP discovery. The IP Office system listens for this type of discovery on port 69 (TFTP). TFTP is then used to send and receive configuration settings with the Manager PC.
- IP Office 3.2+ systems respond to both UDP and TCP discovery. The IP Office system listens for UDP discovery on port 69 (TFTP) and TCP discovery on port 50802. Unlike pre-3.2 IP Office systems, configuration settings are accessed using TCP.
- UDP can use broadcast addresses, however broadcasts are not forwarded by routers. TCP is routable but cannot use broadcast addresses. Manager however can specify a list of TCP addresses to check.

Configuration Access

Having discovered the available IP Office systems and selected one, configuration access can be attempted.

- For pre-3.2 IP Office systems, if the correct IP Office system password is entered, the configuration is transferred using TFTP.
- Access to configuration settings of an IP Office 3.2+ system, requires a valid Service User name and password. Manager does not send the name and password entered by the user to the IP Office. It sends a 'hash' of those values which are then compared against the names and passwords stored on the IP Office.
- The configuration access occurs using TCP and on port 50804 of the IP Office control unit. This port can be adjusted if required through the IP Office's security settings.

Security Settings

- Pre-3.2 IP Office systems do not have security settings that are separate from the configuration settings which include the system password.
- Access to the security settings of an IP Office 3.2 system is similar to accessing configuration settings. However, service user name and password used must have security access and the default port used is 50812.

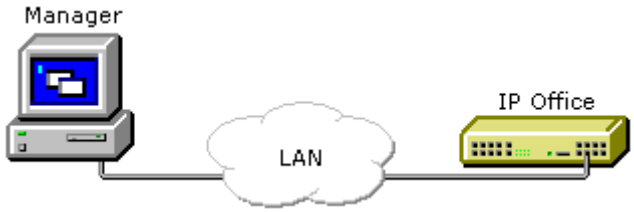
Ports

As mentioned, a number of different ports are used for access to IP Office systems. The following table lists some of the ports on which the IP Office control unit listens for different types of access.

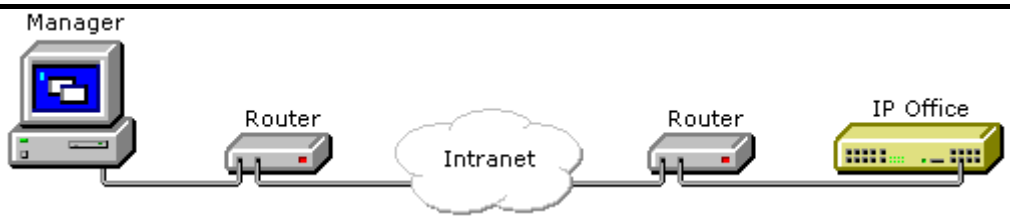
Port		Protocol	Function
	UDP	ICMP (Ping)	Used to confirm routing to addresses not on the same subnet as the Manager PC.
25	TCP	SMTP	Email system alarms from the IP Office to an SMTP server.
37	UDP	Time	Time requests from the IP Office to a Time Server (RFC868).
53	UDP	DNS	Domain Name Service responses.
67	UDP	DHCP/BOOTP	DHCP Server operation.
68	UDP	DHCP/BOOTP	DHCP Client operation.
69	UDP	TFTP	Used for UDP discovery of IP Office systems and for configuration access to pre-3.2 IP Office systems.
161	UDP	SNMP	From SNMP applications.
162	UDP	SNMP	SNMP Traps from IP Office.
500	UDP	IKE	Key exchange for IPSec protocol.
520	UDP	RIP	To the IP Office from RIP devices.
1701	UDP	L2TP	Layer 2 Tunnelling protocol.
1718	TCP	H.323	H.323 Discovery.
1719	TCP	H.323	H.323 Status.
1720	TCP	H.323	H.323 Signalling.
5060	UDP/TCP	SIP	Session Initiation Protocol.
8080	TCP	HTTP	Browser access to the IP Office Delta Server application.
8089	UDP	Enconf	IP Office to Conference Center Server.
8888	TCP	HTTP	Browser access to the IP Office ContactStore (VRL) application.
49152 t0 53247	UDP	RTP/RTCP	Dynamically allocated ports used during VoIP calls for RTP and RTCP traffic.
50791	UDP	Voicemail	Voicemail license polling
50793	UDP	Solomail	TAPI Wave Driver
50794	UDP/TCP	Sysmonitor	System monitor application access.
50795	UDP	IPO Voice Networking	Small Community Network signaling (AVRIP) and BLF updates.
50796	UDP	PCPartner	From an IP Office user applications such as Phone Manager or SoftConsole.
50797	UDP	IPO TAPI	From an IP Office TAPI user PC.
50798	UDP		IP Office Manager and Upgrade Wizard.
50799	UDP	IPO BLF	Broadcast to the IP Office LAN and the first 10 IP addresses registered from other subnets.
50800	UDP	IPO License Dongle	To the License Server IP Address set in the IP Office configuration.
50801	UDP	EConf	Conference Center Server to IP Office.

Port		Protocol	Function
50802	TCP	Discovery	Used by the IP Office to listen for discovery attempts from the Manager **Select IP Office** menu.
50804	TCP	Configuration	Manager configuration settings access to an IP Office 3.2+ system.
50805	TCP	" (Secure)	Manager configuration settings access to an IP Office 4.1+ system using TLS.
50808	TCP	System Status	Connections by the IP Office System Status Application.
50812	TCP	Security Settings	Manager security settings access to an IP Office 3.2+ system.
50813	TCP	" (Secure)	Manager security settings access to an IP Office 4.1+ system using TLS.

Scenario
In this scenario, Manager's default behavior is used to connect to an IP Office 3.2 system on the same LAN.

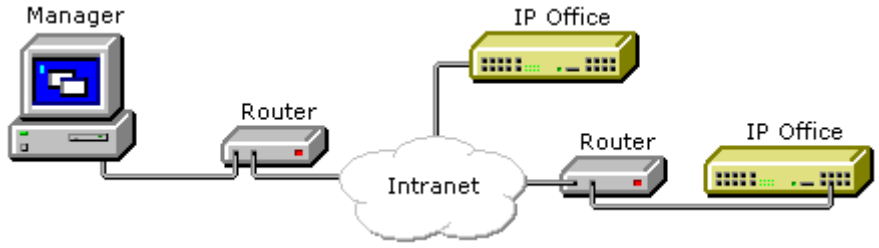
Diagram	
Sequence	1. The user starts Manager and clicks . **Select IP Office** menu appears. 2. Manager does a UDP Broadcast to 255.255.255.255, port 69 (TFTP). Since this is a broadcast, it will not be forwarded beyond the LAN by any router including the IP Office system. 3. The IP Office responds with its system details including its name, IP address and software level. 4. The **Select IP Office** menu lists the responding IP Offices. 5. The user selects the IP Office system and clicks **OK**. 6. Since the system is listed having a 3.2 software level, Manager requests the user to enter a Service User name and password. 7. Manager sends a 'hashed' version of the name and password to port 50804 at the IP Office's IP address. If valid for that IP Office system, the IP Office sends its configuration settings in the return TCP stream.
Requirements	• The IP Office must be on the same subnet as the Manager PC in order to see the UDP broadcast.
Controls	• The IP Office can be disabled from responding to UDP broadcasts if required. This is done through the IP Office's security settings. Access must then be done using TCP only.

Scenario
In this scenario, the user attempts to connect to an IP Office on another LAN using the Manager with its default settings.

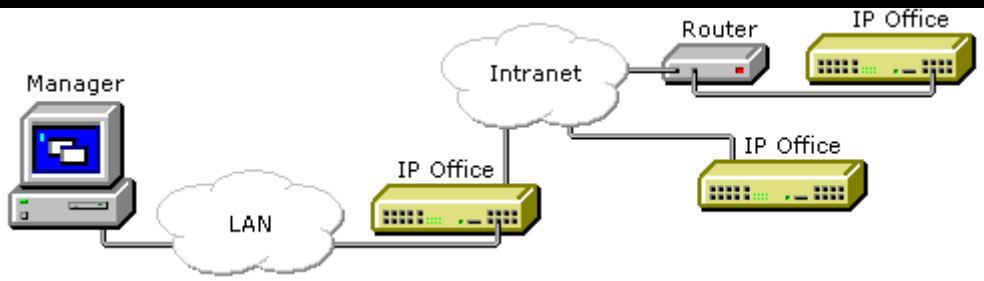
Diagram	
Sequence	1. The user starts Manager and clicks . The **Select IP Office** menu appears. 2. Manager does a UDP broadcast to 255.255.255.255. 3. The router does not forward the UDP broadcast. This is typical router behavior and would apply to any other intermediate routers. 4. The user changes the **Unit/Broadcast Address** to be the IP Office's LAN1 IP address and selects **Refresh**. 5. Manager sends an ICMP ping (UDP) to that address. 6. The router forwards the request. 7. The IP Office responds. Manager sends a TCP discovery request port 50802. 8. The IP Office responds with its system details including its name and software level. 9. The **Select IP Office** menu lists the responding IP Office. 10. The user selects the IP Office system and clicks **OK**. 11. Since the system is listed as having a 3.2 software level, Manager requests the user to enter a Service User name and password. 12. Manager sends a 'hashed' version of the name and password to port 50804 at the IP Office's IP address. If valid for that IP Office system, the IP Office sends its configuration settings in the return TCP stream.
Requirements	• The intermediate routers must be configured to route traffic for the IP Office's LAN1 IP address to that system. • The intermediate routers and any firewalls must be configured to allow pings. • The intermediate routers and any firewalls must be configured to allow a session to be started at the IP Office by incoming TCP traffic on ports 50802 (Discovery) and 50804/50805 (Configuration settings access).
Controls	• The default port on which the IP Office system listens for TCP discovery requests from Manager (50802) cannot be changed. • The port on which the IP Office system listens for configuration access requests (50804/50805) can be changed. This is done through the IP Office's security settings. • The port to which Manager sends configuration access requests can be changed to match the IP Office system. Select **File | Preferences** and on the **Preferences** tab change the **Services Base TCP** port. • The TCP address of the remote IP Office can be added to the default list of addresses scanned by the **Select IP Office** menu. Select **File | Preferences** and on the **Discovery** tab, enter the IP address in the **IP Search Criteria** area. See the following scenario.

Scenario: Managing Multiple Remote IP Offices
In this scenario, the user is maintaining a number of IP Office 3.2 systems located on others LAN's. Through Manager it is possible to preset the addresses of these systems rather than having to change the Unit/Broadcast Address each time the Select IP Office menu appears.

Addresses are entered through the **IP Search Criteria** on the **Preferences | Discovery** tab. On this tab, IP Office system addresses can be entered, separating each entry with a semi-colon.

Diagram	
Sequence	1. The user starts Manager and clicks . The **Select IP Office** menu appears. 2. Manager does a UDP broadcast to 255.255.255.255. The router does not forward the UDP broadcast. This is typical router behavior and would apply to any other intermediate routers. 3. Manager also sends TCP discovery requests to the addresses listed in the **IP Search Criteria** on the **Preferences | Discovery** tab. The requests are sent to port 50802. 4. The IP Office systems respond with their system details including their names and software levels. 5. The **Select IP Office** menu lists the responding IP Office. 6. The user selects the IP Office system required and clicks **OK**. 7. Since the system is listed as having a 3.2 software level, Manager requests the user to enter a Service User name and password. 8. Manager sends a 'hashed' version of the name and password to port 50804/50805 at the IP Office's IP address. If valid for that IP Office system, the IP Office sends its configuration settings in the return TCP stream.

Scenario
This scenario combines the previous scenarios. A UDP broadcast is used to access the users own IP Office on their LAN whilst preset TCP addresses are used to access the IP Office systems that IP Office systems that they maintain on other LAN's.

Accessing an IP Office 3.2 Configuration	
Diagram	
Sequence	1. The user starts Manager and clicks . The **Select IP Office** menu appears. 2. Manager does a UDP broadcast to 255.255.255.255. The router does not forward the UDP broadcast. This is typical router behavior and would apply to any other intermediate routers. 3. Manager also sends TCP discovery requests to the addresses listed in the **IP Search Criteria** on the **Preferences | Discovery** tab. 4. The IP Office systems respond with their system details including their names and software levels. 5. The **Select IP Office** menu lists the responding IP Office. 6. The user selects the IP Office system required and clicks **OK**. 7. Since the system is listed as having a 3.2 software level, Manager requests the user to enter a Service User name and password. 8. Manager sends a 'hashed' version of the name and password to port 50804/50805 at the IP Office's IP address. If valid for that IP Office system, the IP Office sends its configuration settings in the return TCP stream.

Backward Compatibility

IP Office Manager 6.1 is part of the IP Office 4.1 software release. However it can be used to edit configurations from IP Office systems with core software IP Office level 2.1 upwards.

When an IP Office 2.1 or higher configuration is loaded, Manager adjusts the settings and fields that it shows to match the core software level of the IP Office control unit. If you attempt to load a pre-2.1 IP Office configuration, Manager will display an error message and does not load the configuration.

To receive a pre-3.2 IP Office configuration requires entry of an operator name and the IP Office system password. To receive a 3.2 or higher IP Office configuration requires entry of a service user name and password stored by that IP Office system.

- Backwards compatibility is only supported for General Availability releases of IP Office software. It is not supported for pre-3.2 private builds.

IP Office Standard Edition and IP500 Licences

The IP500 system unit start operation in a mode called IP Office Standard Edition mode. In this mode, the number and range of features supported is limited. The limitations can be overridden by the addition of an IP500 Upgrade Standard to Professional license to the IP Office 500 configuration. Features not detailed in the table below are not affected directly by Standard Edition or Professional Edition mode selection.

Feature	Standard Edition	Professional Edition
Extensions	32	272
External Expansion Modules	✗	✓
Applications		
Phone Manager (All modes)*	✓	✓
SoftConsole *	✓	✓
IP Office TAPI	✓	✓
Delta Server	✓	✓
Compact Business Center (CBC)	✓	✓
Compact Contact Center (CCC)*	✗	✓
Embedded Voicemail	✓	✓
Voicemail Lite	✗	✓
Voicemail Pro *	✗	✓
ContactStore *	✗	✓
Conference Center *	✗	✓
MS-CRM	✗	✓
Meet-me Conferences	✗	✓
IP DECT Trunks	✓	✓
SIP Trunks *	✓	✓
SES Trunks *	✓	✓

*Also require appropriate application licenses.

The following licences are specific to IP Office 500 systems.

- **IP500 Upgrade Standard to Professional**
  This license is required for an IP500 system to run in IP Office Professional Edition mode rather than IP Office Standard Edition mode. It is a pre-requisite for any licensed features not supported in Standard Edition mode.
- **IP500 Voice Networking (Base 4 channels)**
  For IP500 systems this licences enables support for H323 IP trunks between IP Office systems and QSIG or Small Community Networking over those trunks.
- **IP500 Voice Networking (Additional channels)**
  Allows an additional 4 H323 voice networking trunks.
    - For IP Office 4.0, the IP500 Voice Networking licenses were only supported in IP Office Professional Edition mode. For IP Office 4.1 they are supported in IP Office Standard and Professional Edition modes.
- **IP500 PRI Trunk Channels**
  Each IP500 PRI-U trunk daughter card provides 8 channels by default. Additional channels are enabled by the addition of the type of license.

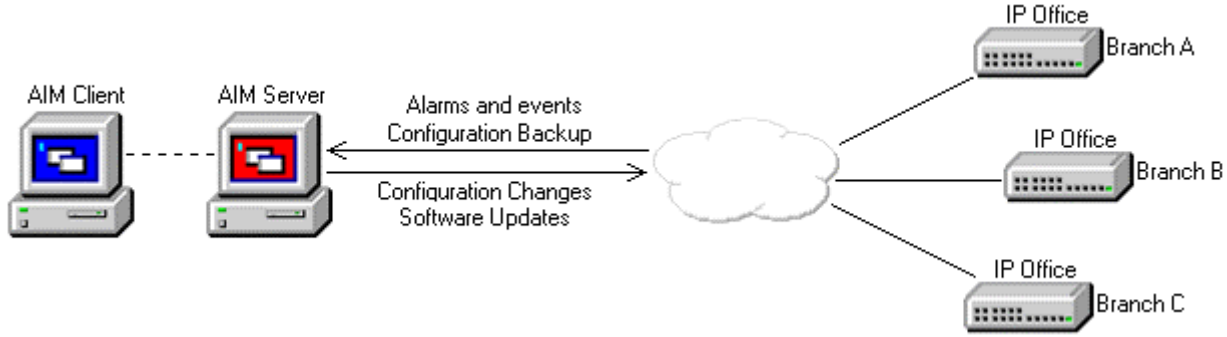
Avaya Integrated Management (AIM)

Avaya Integrated Management, IP Office and Chain Store Mangement

Avaya Integrated Management (AIM) is a suite of applications used to monitor and manage multiple phone systems. Running either from a server or through a client -server setup, AIM can be used to remotely monitor and access those phone systems.

Refer to the AIM product documentation for full details.

AIM and IP Office Manager support is aimed at customers requiring a "chain store management" solution, i.e. customers managing multiple branch office IP Office systems. Typically the dial plan and other settings of these phone systems are the same from branch to branch. Through the use of configuration templates, AIM is able to deploy the required settings following system installation and to deploy template changes to multiple systems simultaneously.



Key features provided by AIM for IP Office systems are:

- System monitoring and configuration backup.
- Rapid installation by remote software upgrading of new systems.
- Consistent programming through IP Office templates.
- Simultaneous distribution of template changes and updated auto-attendant prompts.

Use of AIM with IP Office is only supported by IP Office 4.0 and higher. Systems with IP Office 2.1 to IP Office 3.2 can be discovered by AIM NMC if they have SNMP enabled or are manually added to AIM Network Management Console (NMC). Those systems can then be upgraded to IP Office 4.1 using AIM Software Update Manager (SUM).

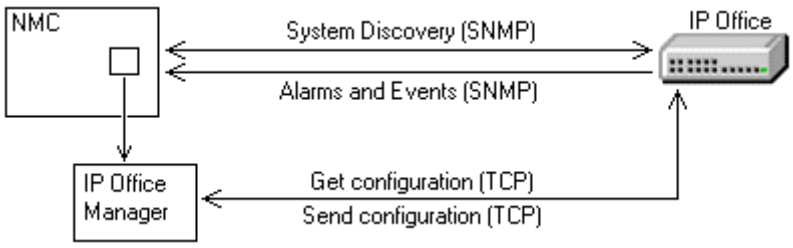
- The IP Office 500 control unit is currently not supported for use with AIM.
- **WARNING**
  IP Office systems being managed through AIM should only be accessed using the version of IP Office Manager included as part of the AIM suite installation. Similarly only the .bin files included in that installation should be used with those IP Office systems. Attempting to configure these systems using a standalone copy of Manager may cause configuration errors.

AIM Applications

IP Office 4.1 is supported by AIM. In addition to its own applications, AIM can also use IP Office Manager as a tool to configure IP Office systems. The IP Office Manager is installed as a component of AIM, either on the AIM server or the AIM client.

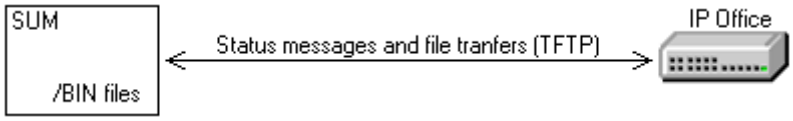
AIM consists of the following applications which interact with IP Office:

- **AIM Network Management Console (NMC)**
  NMC is used to monitor the phone systems being managed through AIM. It shows the equipment inventory of those systems, their status and system alarms. Refer to the AIM product documentation for full details.



  - NMC uses SNMP to discover IP Office systems.
  - IP Office SNMP is used to provide system information, alarms and events to NMC.
  - For any IP Office system it knows, NMC can open that systems configuration directly into IP Office Manager using the ***Tool -> Device Manager*** menu command.

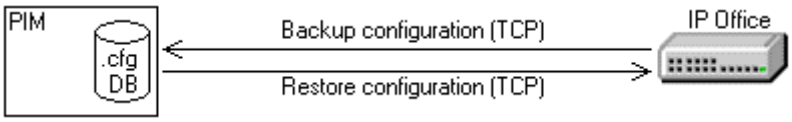
- **AIM Software Update Manager (SUM)**
  SUM is used to provide software updates to systems being managed through AIM. Refer to the AIM product documentation for full details.



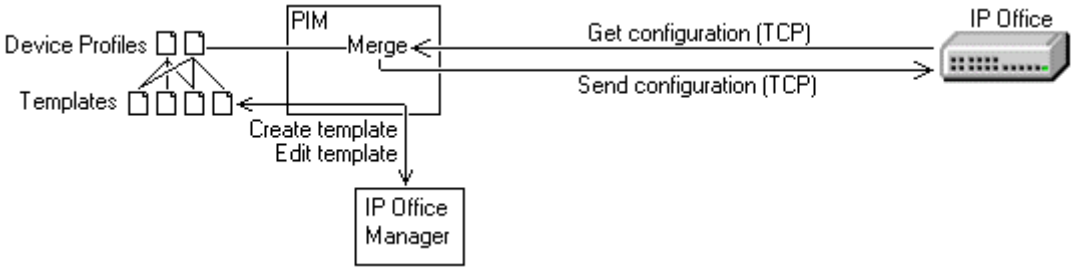
  - For IP Office systems SUM replaces Manager for control unit and external expansion unit software upgrades.

- **AIM Secure Access Administration (SAA)**
  SAA is used to maintain a database of names and passwords for accessing the systems being managed through other AIM applications. Refer to the AIM product documentation for full details.
  - SAA provides name and password details to other AIM applications as and when they are required for access to a system.
  - When passwords are changed in SAA, it accesses the security settings of IP Office systems make the matching changes.

- **AIM Provisioning and Installation Manager (PIM)**
  PIM is used for a range of functions. Refer to the AIM product documentation for full details.



  - PIM can perform scheduled backups of the configuration of IP Office systems.
  - PIM can view backup configurations as read-only files and restore an IP Office configuration from a previous backup.



  - PIM can be used to create and edit partial IP Office configurations called 'templates', using IP Office Manager to display and edit a chosen template. The different template types are:
    - IP Office Hardware Template
    - IP Office User Template
    - IP Office Auto-Attendant Template
    - IP Office General Template
  - PIM can be used create associate different templates with different IP Office systems and to then create job schedules for the deployment of those templates to the IP Office systems.
  - PIM can also be used to record and deploy auto-attendant greetings specified in auto-attendant templates.

Password Administration

The AIM Secure Admin Access (SAA) application is used to control access to the systems being managed through AIM including IP Office systems.

Configuring Access to IP Office Systems

1. Within SAA a number of IPO Users can be created. Multiple IP Offices can then assigned to each IPO User.
2. Each IPO User has a name, password and TFTP password configured within SAA.
3. SAA also has a general **AIMAdmin** password used by all IPO Users.
4. Within each IP Office's security settings, the name and password of the Unique Security Administrator must match the name and password of the IPO User with which the IP Office is associated in SAA.
5. When an IP Office system is associated with the SAA IPO User, SAA can access the IP Office system's security settings.
    1. It creates an IP Office Service User called **AIMAdmin** and belonging to the Administrator Rights Group.
    2. It sets the IP Office system password to match the IPO User TFTP Password.
        - If SAA fails to access the IP Office system's security settings using the IPO User name and password, it will attempt to access the settings using the IP Office Unique System Administrator defaults. If this succeeds it will reset the Unique System Administrator settings to match the IPO User name and password.
6. That Service User can then be used by the other AIM applications for configuration access to the IP Office.
7. SAA can also control the IP Office's System Password used for software updates.

Updating Passwords

If a password within SAA is changed, SAA will update the relevant IP Office systems to update the matching passwords.

1. If the IPO User password or TFTP password is changed, SAA will update the IP Office security settings of the IP Office system associated with that IPO User.
2. If the SAA AIMAdmin password is changed, SAA will update the IP Office security settings of all IP Office systems.

SAA Setting	IP Office Setting
IPO User name	Unique Security Administrator name
IPO User password	Unique Security Administrator password
IPO User TFTP password	System Password
SAA AIMAdmin password	AIMAdmin service user password

Configuring an IP Office for AIM

The processes below outline the basic steps for adding an IP Office system into AIM.

IP Office Systems with Pre-3.2 IP Office Software

This process covers existing IP Office systems with pre-3.2 IP Office software. It also covers new IP Office control units, except the IP500, as these may be supplied with an initial software level of IP Office 2.1.

1. Initial on-site configuration should ensure the following:
    1. IP connectivity between the IP Office and the AIM server.
    2. The System Password should be set to match that used by the IPO User.
    3. Enable SNMP.
2. Following the above, it should be possible for NMC to discover the IP Office system.
    1. If SNMP was not enabled during initial configuration, the IP Office system can be added manually to NMC.
3. SUM should be used to upgrade the IP Office system to IP Office 4.1 software. Depending on the control unit type this may be a multi-stage upgrade process.
4. Having upgraded the IP Office system to IP Office 4.1, it will have default security settings. SAA can now be used to apply the IPO User required security settings to the IP Office system.
5. PIM can now be used to apply templates to the IP Office system. The hardware template should include enabling SNMP with the appropriate community string and alarms.
6. Additional site-specific configuration, for example the addition of software licenses, can be done through NMC.

IP Office Systems with IP Office 3.2 or Higher Software

This process covers existing IP Office systems with 3.2 or higher software. It also covers new IP500 control units which are supplied with a base software level of IP Office 4.0.

1. Initial on-site configuration should ensure the following:
    1. IP connectivity between the IP Office and the AIM server.
    2. The System password should be set to match that used by the IPO User.
    3. The Unique Security Administrator name and password should be set to match the IPO User or left at default.
    4. Enable SNMP.
2. Following the above, it should be possible for NMC to discover the IP Office system.
    1. If SNMP was not enabled during initial configuration, the IP Office system can be added manually to NMC.
3. SUM should be used to upgrade the IP Office system to IP Office 4.1 software to ensure that the same software build is being used for all the systems being managed through AIM.
4. SAA can now be used to apply the IPO User required security settings to the IP Office system.
5. PIM can now be used to apply templates to the IP Office system. The hardware template should include enabling SNMP with the appropriate community string and alarms.
6. Additional site-specific configuration, for example the addition of software licenses, can be done through NMC.

PIM Templates

PIM IP Office Templates

The IP Office configuration record types within each template type are listed below. When a template of that type is created or edited, only the forms for those record types are visible.

- **Hardware Template**
  Contains **Control Unit**, **System**, **Line**, **Extension** and **Short Code** records. For some systems depending on IP Office control unit type and or location it may also contain Wireless and or E911 records.
- **User Template**
  Contains **User**, **User Rights**, **Hunt Group**, **Incoming Call Route**, **Firewall** and **Time Profile** records.
- **Auto Attendant Template**
  Contains **Auto Attendant**, **Short Code**, **Incoming Call Routes** and **Time Profile** records.
- **General Template**
  Contains **ARS**, **Account Code**, **Directory**, **Time Profile** and **Firewall** records.

Settings and record types not included in any template are referred to as 'site specific settings'. Those settings can only be edited using AIM NMC (***Tools -> Device Manager***) to launch IP Office Manager with the whole system configuration opened.

How are templates created?
PIM will first ask what type of template is being created. It then opens IP Office Manager showing only the record types that are needed for that sort of template. In the case of a Hardware template, when IP Office Manager is started the **Create Offline Configuration Wizard** appears and is used to define the IP Office system type and equipment.

How does IP Office Manager differ when creating or editing a template?
Compared to editing a full IP Office configuration the following differences are visible:

- The Manager application title bar displays the name given to the template.
- Tool and menu bar options not applicable to the template type are greyed out.
- Some fields may be shown as greyed out and empty. Those fields are not part of the template and when the template is merged with an IP Office configuration the existing site specific setting is retained.
- When using Manager to edit a full IP Office configuration, some fields act a drop-down lists from which a selection can be made. In a template, those same fields may not act as drop-downs as the relevant other configuration to list as possible selections are not available. Values must be manually typed into the template fields.
- In a full configuration some user fields can be configured if the user is not using user rights. Within a template those fields can only be set in user rights.
- For auto attendant greetings and menus, the name of wav files stored within PIM can be selected. Those files are converted and transferred to the IP Office system when the auto-attendant template is applied to that system.

How are templates associated with IP Office systems?
Once templates have been created, within PIM a Device Profile for each IP Office system can also be created. That Device Profile defines which templates, up to one of each type, the IP Office system uses.

How are templates merged with the existing configuration?
PIM is used to create Jobs. Each job specifies a date, time, which IP Office systems to update and which template or templates from each IP Office system's Device Profile to merge.

- Merging templates requires the IP Office system to reboot and so should be scheduled outside the normal business hours of the IP Office sites wherever possible.

What happens to existing records in the configuration when a template is merged?
In general all existing records of the type supported by a template are deleted unless the record appears in the template being merged. The exceptions are existing **Short Code**, **Incoming Call Route**, **Firewall** and **Time Profile** records which may not be deleted every time as these can come from more than one type of template.

What happens if there are configuration errors?
Once all the template records have been merged and all redundant records deleted, post merge validation is applied.

Hardware Template

The purpose of a hardware template is to contain those settings that are common to customer branches using the same type of IP Office control unit and associated hardware such as trunks and extensions.

When a new hardware template is created, IP Office Manager is launched and the **Create Offline Configuration Wizard** started. This then allows the physical hardware such as the IP Office control unit type, trunk interface cards and external expansion modules to be defined.

This type of template is useful for multiple branch offices that follow the same format, that is have the same hardware and dial plan.

- **WARNING**
  Care must be taken to ensure that a hardware template is only ever deployed to a matching physical IP Office. Sending a hardware template to a system with differing physical hardware such as trunks and extensions will cause unpredictable results.

Template Records

This type of template includes forms for the following types of IP Office configuration records.

- **Control Unit**
  All fields shown are greyed out and shown for information only.
- **System**
- **Line**
  Physical lines can only be added during the initial **Create Offline Configuration Wizard** stage of template creation. Only IP, IP DECT and SIP lines can be added after the template has been created.
- **Extension**
  Physical lines can only be added during the initial **Create Offline Configuration Wizard** stage of template creation. Only IP and IP DECT extensions can be added after the template has been created.
- **Short Code**
  All short code changes should be done in hardware template. Note that auto attendant related short code records are included in the Auto Attendant template deployed to a branch.
- **Wireless**
  This form is only available if an IP Office Small Office Edition control unit is selected during the initial **Create Offline Configuration Wizard** stage of template creation.
- **E911**
  This form is only available if the locale ***United States*** is selected during the **Create Offline Configuration Wizard** stage of template creation.

User Template

The purpose of this type of template is to contain the records relevant to customer branch users.

Note that during normal operation, IP Office users can change some settings using IP Office short codes, programmable buttons on phones or IP Office Phone Manager applications unless locked through a user rights template. Those changes will be overwritten whenever a user template is reapplied.

Template Records

This type of template includes forms for the following types of IP Office configuration records.

-  **User**
  The user template deployed to an IP Office should contain user records that match the extension dial plan in the hardware template also deployed to that IP Office. Those fields that can also be defined in a User Rights record are greyed out and can only be set by associating each user with a user rights record in the same template. If required, time profiles can be added to allow different user rights to be associated with the user at different times.
-  **User Rights**
  For AIM it is required that customer create user rights records to define user settings and then assign them to users. User rights allow various user settings to be defined once and then applied to multiple users by associating those user with the user rights. Changes to the user rights are then applied to all associated users.
-  **Hunt Group**
  Hunt group records are used to create groups of users. Those groups can then be called from extensions within the system or specified as the destination for incoming calls in Incoming Call Route records.
-  **Incoming Call Route**
  Incoming calls route records can be used to route incoming calls to selected users or hunt groups. Note that Incoming call route records can also be added through Auto Attendant templates to route calls to an Embedded Voicemail auto attendant.
-  **Firewall**
  In the user template, firewall records can be added for users who receive RAS data calls. Note that other general purpose Firewall records should be the General template to be deployed.
-  **Time Profile**
  In a user template, time profiles are used with users to control when features such as RAS, automatic voice recording, mobile twinning and user rights are enabled or disabled. They are also used with hunt groups to control night service fallback and automatic voice recording. Note that other time profile records can be added in the Auto Attendant and General templates deployed to a branch.

Auto Attendant Template

This type of template is only used with IP Office systems that are running Embedded Voicemail. Embedded Voicemail is supported on systems using the IP Office Small Office Edition, IP406 V2 and IP500 control units.

Embedded Voicemail requires an Embedded Voicemail memory card to be fitted to the control unit. Embedded Voicemail can be enabled through the IP Office **System |Voicemail** form settings contained in the Hardware Template.

Template Records

This type of template includes forms for the following types of IP Office configuration records.

-  **Auto Attendant**
  Each auto attendant record defines the DTMF key press actions supported by the auto attendant, the greetings the attendant uses and the time profiles that should control when each greeting is used.
  - The Recording Name fields, one each for the Morning, Afternoon, Evening and Menu Options prompts allow a WAV file name to be specified. The file names can be up to 31 characters long but should not include spaces or the .
-  **Short Code**
  Each auto attendant record created automatically adds short codes for the on-site recording of greetings. All non-auto attendant short code records should be managed via the Hardware template deployed to a branch.
-  **Incoming Call Routes**
  Once auto attendant records have been added to a template, they can be used as the destination for incoming call routes. Incoming call route records for users and hunt groups should be added by the User template deployed to a branch.
-  **Time Profile**
  Time profiles are used by auto attendant records to control when each of the auto attendant greetings are used. Other time profile records should be added in the General and User templates deployed to a branch.

How are the WAV files transferred to the IP Office?

Whenever the Auto Attendant template is deployed to an IP Office, PIM also transfers the required files named in the Auto Attendant template. The files are converted to the required format before transfer and then sent to the Embedded Voicemail Memory card within the system.

General Template

The purpose of this type of template is to include records that may be common to multiple branches but are not part of the other templates deployed to those branches.

Template Records

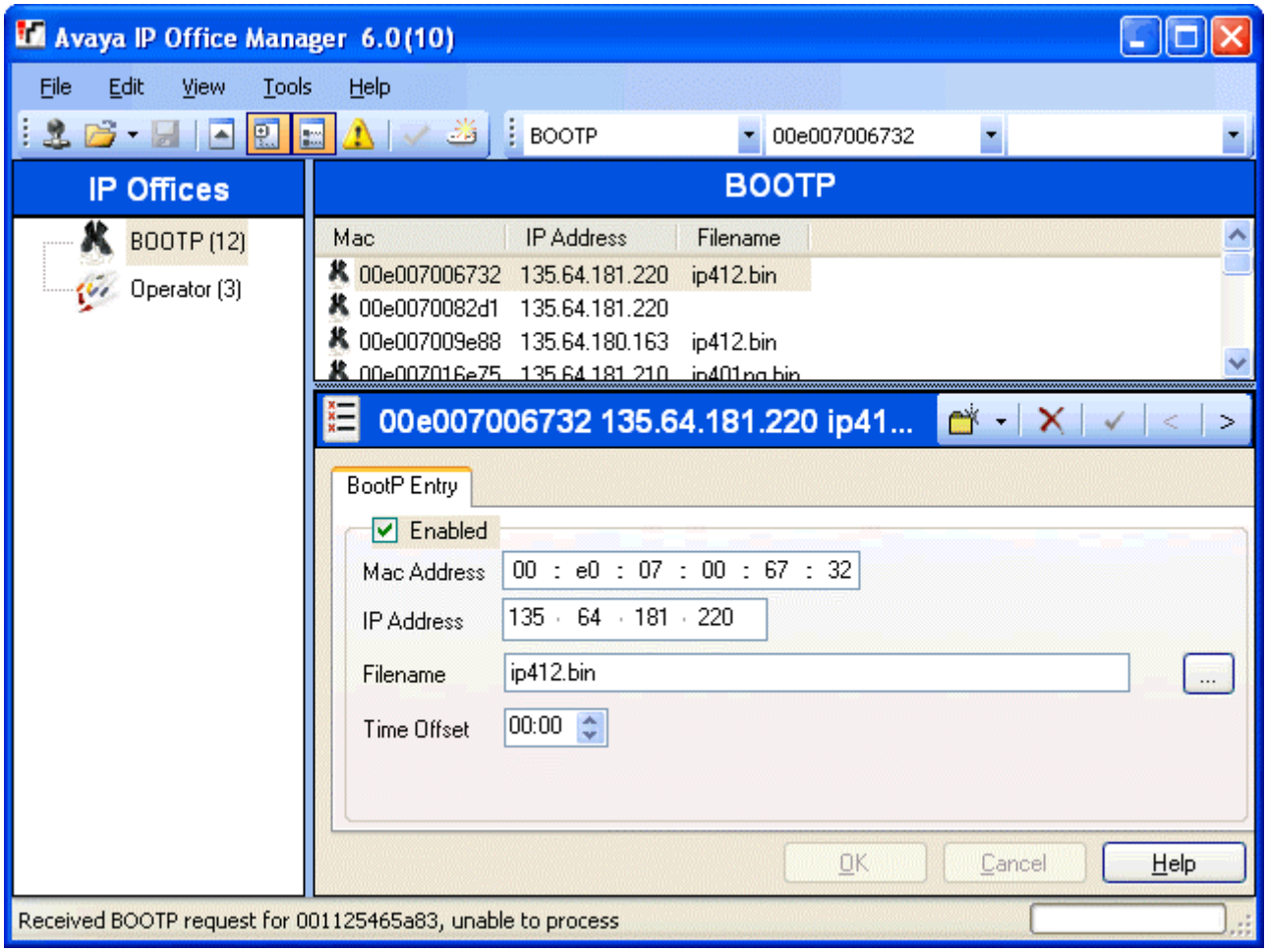
This type of template includes forms for the following types of IP Office configuration records.

-  **ARS**
  ARS is one of the methods used to select which line should be used for outgoing calls from an IP Office system.
-  **Account Code**
  Account codes can be used to control calls made by specific users or to specific numbers.
-  **Directory**
  Directory records are used to make outgoing calls and to match the ICLID of incoming calls to names for display on suitable phones.
-  **Time Profile**
  These time profile records are for general purposes such use by ARS records to switch the routing of calls from one ARS record to another. Time profile records required for auto attendants should be defined in the Auto Attendant template deployed to a branch. Similarly time profile records required for users should be defined in the User template deployed to a branch.
-  **Firewall**
  Note that firewall records can also be added by the Auto Attendant and User templates deployed to a branch.

Configuration Mode

Configuration Mode

By default Manager starts in configuration mode with no IP Office configuration settings loaded.



This section of the documentation is divided into two parts as follows.

The Configuration Mode Interface
This part details the screen elements of Manager's configuration mode interface.

- **The Menu Bar**
- **Toolbars**
- **Using the Navigation Pane**
- **Using the Group Pane**
- **Using the Details Pane**
- **Using the Error Pane**
- **Altering the Interface**

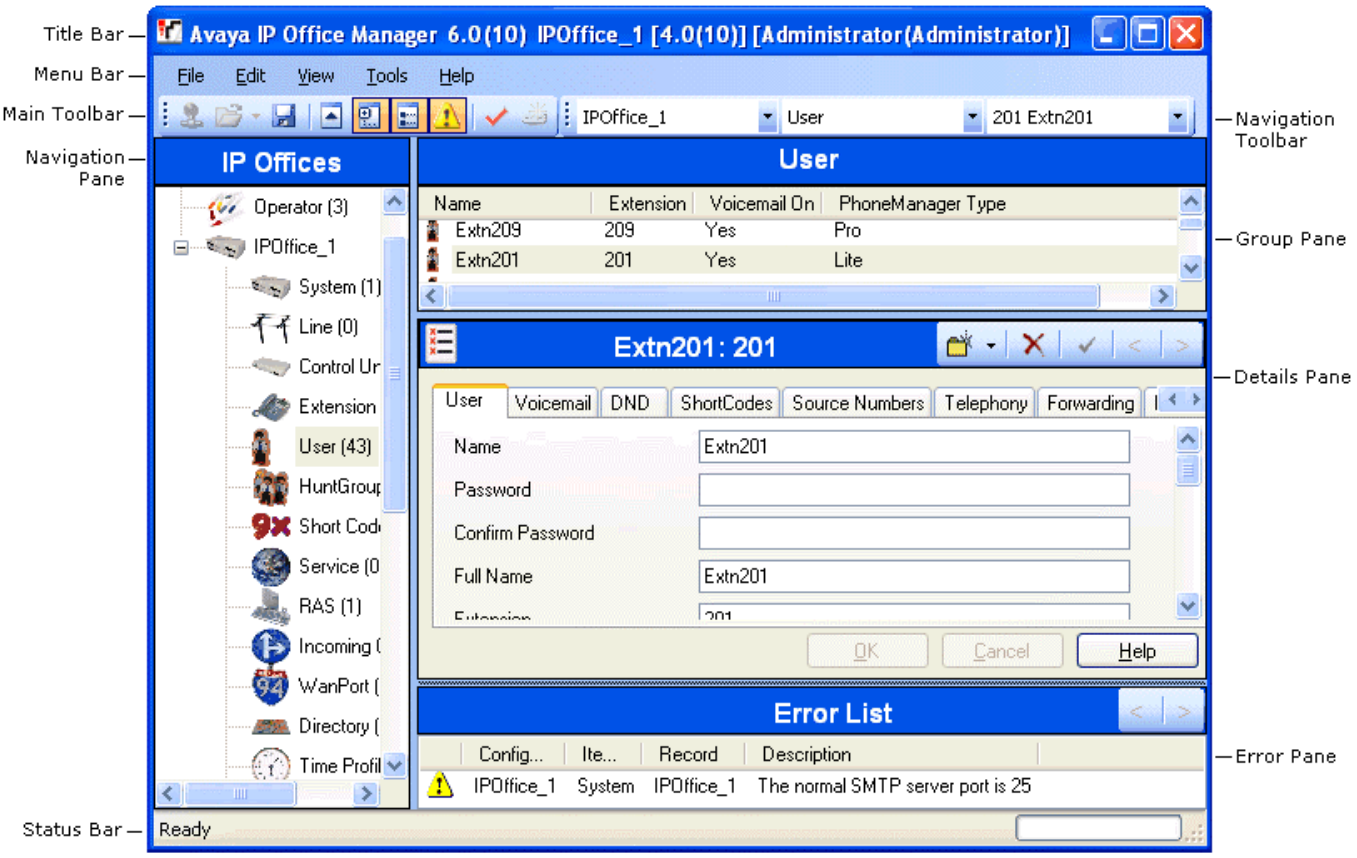
Editing Configuration Settings
This part details how Manager's configuration mode can be used for the following tasks.

- **How the Configuration is Used**
- **Loading a Configuration**
- **Creating a New Configuration**
- **Importing and Exporting Settings**
- **Sending a Configuration**
- **Saving a Configuration Offline**
- **Erasing the IP Office Configuration**

Switching Manager to Configuration Mode
Though Manager starts in configuration mode; it can also run in security mode by selecting **File | Advanced | Security Settings**. To return to configuration mode from security mode, select **File | Configuration**.

The Configuration Mode Interface

When Manager is in configuration mode, the screen elements shown are available. Some of these elements can be customized, moved and hidden.

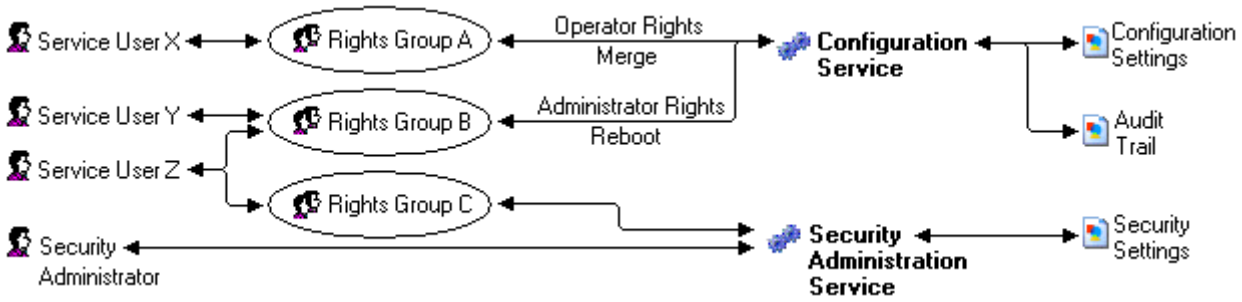


Manager Configuration Mode Screen Elements

- **Title Bar**
  In addition to the application name, when configuration settings are loaded from an IP Office system, the title bar displays the user name used to load the settings and the operator view applied.
- **Menu Bar**
  The options available with the drop down menus provided here change according to whether Manager has a set of configuration or security settings loaded or not.
- **Main Toolbar**
  This toolbar provides icon shortcuts to the most frequently required configuration setting actions.
- **Navigation Toolbar**
  This toolbar provides a set of drop downs which can be used to navigate to particular entries in the configuration settings. The selected options in the navigation pane, the group pane and the details pane are synchronized with the navigation toolbar and vice versa. This toolbar is particularly useful if you want to work with the group pane and or navigation pane hidden in order to maximize the display space for the details pane.
- **Navigation Pane**
  This pane shows icons for the different types of entry that the configuration can contain. Each type is followed by the number of entries of that type already in the configuration. Selecting an icon displays the matching entries in the group pane and navigation toolbar.
- **Group Pane**
  This pane lists all the entries that match the type selected in the navigation pane or navigation toolbar. The list can be sorted by clicking on column heading. Selecting an entry in this pane displays its details in the details pane.
- **Details Pane**
  This pane shows the configuration settings for a particular entry within the configuration. The entry is selected using the navigation toolbar or using the navigation pane and group pane.
- **Error Pane**
  This pane shows errors and warnings about the configuration settings. Selecting an item here loads the corresponding entry into the details pane.
- **Status Bar**
  This bar display messages about communications between Manager and IP Office systems. It also displays the security level of the communications by the use of a padlock icon.

Security Settings

Access to IP Office 3.2+ system settings is controlled by Service Users 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.



In the example illustrated above:

- Service User X can read and write the configuration. However they can only edit Operator settings and can only make changes that can be merged.
- Service User Y can read and write the configuration, edit all settings and make changes that require reboots.
- Service User Z can read and write the configuration, edit all settings and make changes that require reboots. They can also access the security settings.
- The Security Administrator can only access the security settings.

Security Administrators

By default the security administrator is the only user who can access the IP Office's security settings using Manager's security mode.

Service Users

Each Service User has a name, a password and is a member of one or more Rights Groups.

Rights Groups

The Rights Groups to which a Service User belongs determine what actions they can perform. Actions available to Rights Groups include configuration actions, security actions and system status actions:

Configuration	Security	System Status
• **Read the configuration.** • **Write the configuration.** • **Merge the configuration.** • **Default the configuration.** • **Reboot immediately.** • **Reboot when free.** • **Reboot at time of day.**	• **Read all security settings.** • **Write all security settings.** • **Reset all security settings.** *(IP Office 4.1+)* • **Write own password.** *(IP Office 4.1+)*	• **System Status Access.** • **Read All Configuration.**

Where a Service User has been configured as a member of more than one Rights Group, they combine the functions available to the separate Rights Groups.

Operator Rights

Each Rights Group has a **Manager Operator Rights** setting. This setting controls what types of configuration entries Manager will allow members of the Rights Group to view and what actions they can perform with those types of entries.

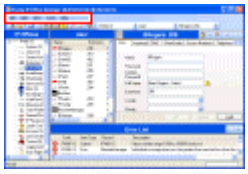
Operator	View/Edit/ New/Delete	Configuration Entry Types
Administrator	All	View, edit create and delete all configuration entries.
Manager	View	View all except **WAN Port**.
	Edit	**Extension**, **User**, **Hunt Group**, **Short Code**, **Service**, **RAS**, **Incoming Call Route**, **Directory**, **Time Profile**, **Firewall Profile**, **IP Route**, **Least Cost Route**, **Account Code**, **ARS, E911 System**.
	New	
	Delete	As edit except **Short Code**.
Operator	View	View all except **WAN Port**.
	Edit	**Extension, User**, **Hunt Group**, **Short Code**, **Service, RAS**, **Incoming Call Route**, **Time Profile**, **Firewall Profile**, **IP Route**, **Least Cost Route**, **Account Code**, **Licence, ARS**, **E911 System**.
	New	None.
	Delete	Delete **Incoming Call Route** and **Directory**.
User & Group Edit	View	**User** and **Hunt Group** entries only.
	Edit	
	New	None
	Delete	
User & Group Admin	All	**User** and **Hunt Group** entries only.
Dir & Account Admin	All	**Directory** and **Account Code** entries only.
Time & Attendant Admin	All	**Time Profile** and **Auto Attendant** entries only.
ICR & User Rights Admin	All	**Incoming Call Route** and **User Rights** entries only.
Read Only	View	View all configuration entries.
	Edit	None.
	New	
	Delete	

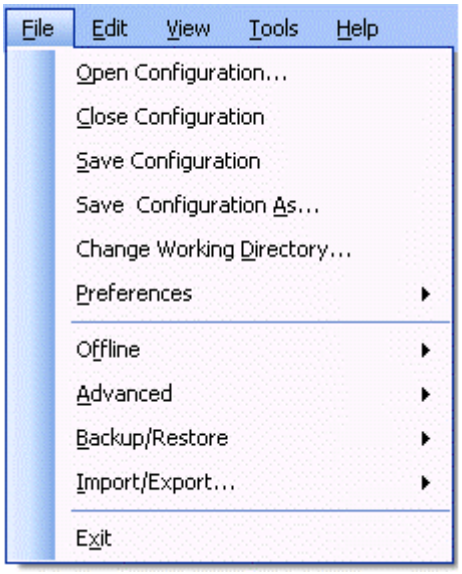
Title Bar

The IP Office Manager title bar shows several bits of information.

- The Manager application version.
- The system name of the IP Office system from which the currently loaded configuration was received.
- The software level of the IP Office system's control unit.
- For IP Office 3.2 systems, the service user name used to receive the configuration and that user's associated operator rights view level. For pre-3.2 IP Office systems this is replaced with just the operator name.

The Menu Bar





Details of all the options that may be available within the Menu Bar drop downs are contained in the section **Menu Bar Commands**.

The commands are context sensitive. Commands are grayed out when not useable.

For some commands, an ▸ symbol indicates that there are sub-commands from which a selection can be made.

File Menu	View Menu	Tools Menu
Open Configuration...	**Toolbars**	**Extension Renumber**
Close Configuration	**Navigation Pane**	**Line Renumber**
Save Configuration	**Group Pane**	**MSN Configuration**
Save Configuration As	**Details Pane**	
Change Working Directory...	**Error Pane**	
Preferences	**TFTP Log**	
Offline | Create New Config		
Offline | Open File...		
Offline | Send Config...		
Offline | Receive Config...		
Advanced | Erase Configuration (Default)		
Advanced | Reboot		
Advanced | Upgrade..		
Advanced | Audit Trail...		
Advanced | Security Settings...		
Advanced | Erase Security Settings (Default)		
Advanced | System Status		
Advanced | LVM Greeting Utility		
Backup/Restore | Backup Binaries and Configurations		
Backup/Restore | Restore Binaries and Configurations		
Import/Export | Import		
Import/Export | Export		
Exit		

Toolbars

The following toolbars are described here:

- **Main Toolbar**.
- **Navigation Toolbar**.
- **Details Toolbar**.

The Main Toolbar

- **Open Configuration from IP Office**
  Advertises to the address currently shown in the Manager's title bar for any available IP Office systems. A list of responding systems is then displayed. When a system is selected from this list, a valid user name and password must be entered. Equivalent to **File | Open Configuration**.
- **Open Configuration File**
  Opens an IP Office configuration file stored on a PC. The button can be clicked to display a browse window. Alternatively the adjacent ▾ arrow can be used to drop-down a list of the last 4 previously opened configuration files. Equivalent to **File | Offline | Open File**.
- **Save Configuration File**
  The action of this icon depends on whether the currently loaded configuration settings were received from an IP Office system or opened from a file stored on PC. If the former applies, the menu sending the configuration back to the system is displayed. In the latter case, the file changes are saved to the original file. Equivalent to **File | Save Configuration**.
- **Collapse All Groups**
  Causes all ⊟ symbols in the navigation pane to be collapsed to ⊞ symbols.
- **Show/Hide the Navigation Pane**
- **Show/Hide the Group Pane**
- **Show/Hide the Error Pane**
- **Validate Configuration**
  Runs a validation on all the currently loaded configuration settings. The results appear in the error pane.
- **Create New Configuration**
  Runs a series of dialogs that create a new configuration from scratch.

This toolbar is also available when Manager is in security mode. However the **Create New Configuration** and **MSN Configuration** buttons are not shown, and the **Show/Hide the Error Pane** and **Validate Configuration** buttons do not function.

The Navigation Toolbar

This toolbar provides drop down lists which can be used to navigate to particular entries in the configuration settings. The selected options in the navigation pane, group pane and the details pane are synchronized with the navigation toolbar and vice versa. This toolbar is particularly useful if you want to work with the group pane and or navigation pane hidden in order to maximize the display space for the details pane.

This toolbar is not available when Manager is in security mode.

Details Toolbar

This toolbar is shown in the top-right of the details pane.

- **Create New Record**
  The ▾ arrow is used to select the entry type to be created. For example; when adding an extension clicking ▾ may allow selection of a VoIP Extension or IP DECT Extension.
- **Delete Entry**
- **Validate Entry**
- **< > Show Previous/Next Entry**

Moving to the Previous or Next Entry

1. Click **<** or **>** at the top-right to move to the previous or next entry.

Altering the Toolbars

Showing or Hiding Toolbars

The different toolbars can be hidden if not required.

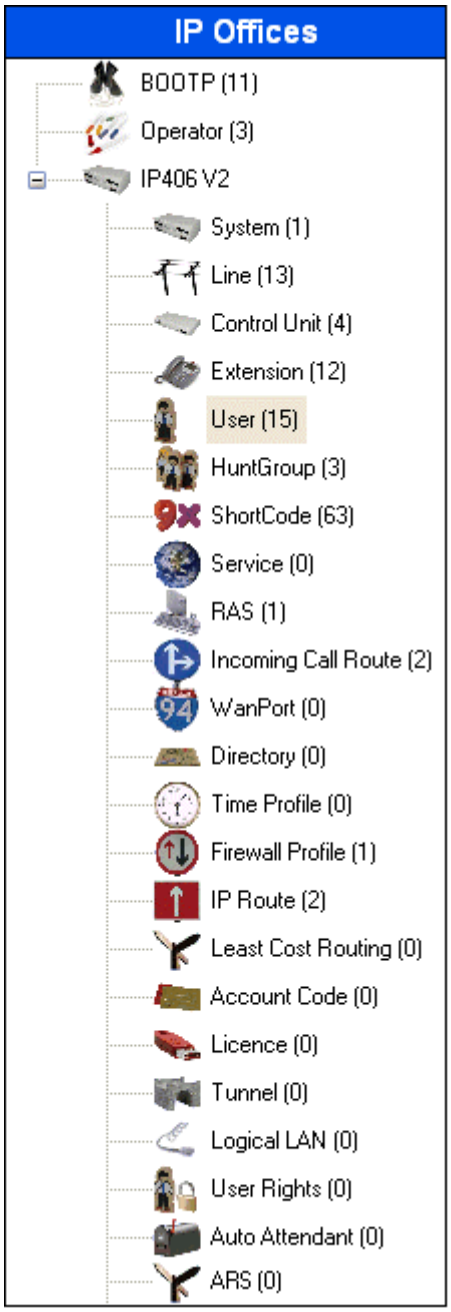
1. Select **View** and then **Toolbars**. Those toolbars currently shown are indicated by a tick mark.
2. To show or hide a toolbar, click on its name.

Moving Toolbars

The position of the Manager toolbars can be moved. Note that when moving a toolbar, the other toolbars and panes may adjust their size or position to ensure that all the toolbar icons remain visible.

1. Place the cursor over the end of the toolbar.
2. When the cursor changes to a four-way arrow, click and hold the cursor.
3. Move the toolbar to the required position and release the cursor.

Using the Navigation Pane



This pane shows icons for the different types of entry that the configuration can contain. Each type is followed by the number of entries of that type already in the configuration.

Selecting an icon displays the matching entries in the group pane and navigation toolbar.

Where ⊞ or ⊟ icons appear in the pane, they allow the structure to be expanded or collapsed. When the group pane is hidden, ⊞ and ⊟ icons are shown for each entry type and allow the entry type to be expanded to display all the existing entries of that type.

The  icon in the main toolbar can also be used to collapse all the expanded entry types shown in the navigation pane.

The icons shown in this pane will vary according to the type of IP Office system loaded. For example **Wireless** is only shown for Small Office Edition systems. They may also vary for different locales, for example **E911** is only shown in the US.

The **BOOTP** and **Operator** icons are special. They represent settings stored on the Manager PC rather than configuration settings received from an IP Office system.

When Manager is used in security mode, this pane is also used by Manager in security mode to display entries for security settings.

Navigation Pane Actions

Moving the Border Between the Panes

The border between the visible panes can be adjusted. Note that this is a proportional rather than exact position. If the whole window size is altered, the border position may also move.

1. Place the cursor over the border between two panes.
2. When the cursor changes to a double headed arrow with a bar through it, click and hold the cursor.
3. Drag the border to the required position and release the cursor.

Showing or Hiding Panes

The navigation pane can be shown or hidden. To do this use either of the following methods.

1. From the main toolbar, use the  icon.

or

1. Select **View**. Those panes currently shown are indicated by a tick mark.
2. To show or hide the navigation pane, click on its name.

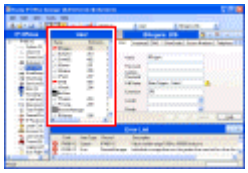
Changing the Size of Configuration Icons

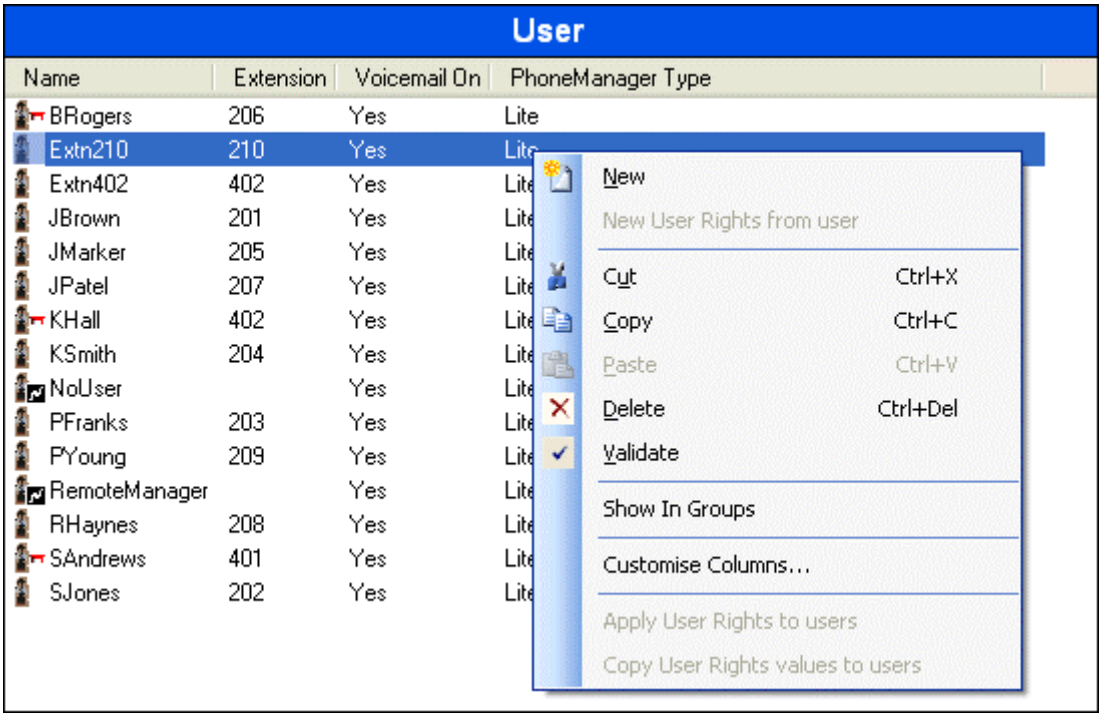
The size of the icons used on the navigation pane and details pane can be adjusted.

1. Select **File** and then **Preferences**.
2. Select the **Visual Preferences** tab.
3. Select the required icon size from **Small**, **Medium** or **Large**.
4. Click **OK**.

Using the Group Pane

This pane lists all the entries that match the type selected in the navigation pane or navigation toolbar. The list can be sorted by clicking on a column heading. Selecting an entry in this pane displays its details in the details pane.





The icons used in the pane may vary according to the state of the entry. For example, some of the users shown in this example have been configured for hot desking. This pane is also used by Manager in security mode to display entries for security settings.

Group Pane Actions

Sorting the List

The entries shown in the group pane can be sorted using any of the columns displayed.

1. To sort the list using the details in a particular column, click on the column header.
2. Clicking on the same column header again reverses the sort order.

Customizing the Columns Displayed

For each entry type, which details are shown in the group pane can be customized. Also the order of the column can be adjusted. For details of the options available for each type of entry see Appendix D: Miscellaneous.

1. Right-click on the pane and select **Customize Columns**.
2. To add a column, selects its name in the left-hand **Available Columns** list and click **>>** to move it to the right-hand **Selected Columns** list.
3. To remove a column, select its name in the right-hand **Selected Columns** list and click **<<** to move it to the left-hand **Available Columns** list.
4. To change the order of the **Selected Columns**, click on a column name and use the **^** and **V** controls.
5. Click **OK**.

Changing the Column Widths

1. In the column headers, place the cursor over the border between two columns.
2. When the cursor changes to a double headed arrow with a bar through it, click and hold the cursor.
3. Drag the border to the required position and release the cursor.

Adding a New Entry

The group pane can be used to add a new entry of the type currently displayed.

1. Right-click on the pane and select **New**.
    - A ▸ arrow symbol next to **New** indicates that you can select a particular type of new entry to create. Click the arrow and select an option from the list.
2. Use the details pane to configure the new entry.
3. Click **OK** in the details pane.

Deleting an Entry

1. Select the entry to be deleted by clicking on it.
2. Right-click on the pane and select **Delete**.

Validating an Entry

1. Select the entry to be validated by clicking on it.
2. Right-click on the pane and select **Validate**.

Show in Groups

This command groups the items shown in the group pane. The grouping method will vary depending on the entry type being listed. For example, short codes are grouped based on short code feature type such as all forwarding short codes together.

1. Right-click on the pane and select **Show In Groups**.

Moving the Border Between the Panes

The border between the visible panes can be adjusted. Note that this is a proportional rather than exact position. If the whole window size is altered, the border position may also move.

1. Place the cursor over the border between two panes.
2. When the cursor changes to a double headed arrow with a bar through it, click and hold the cursor.
3. Drag the border to the required position and release the cursor.

Showing or Hiding Panes
The group pane can be shown or hidden. To do this use either of the following methods.

1. From the main toolbar, use the  icon.

or

1. Select **View**. Those panes currently shown are indicated by a tick mark.
2. To show or hide the group pane, click on its name.

Changing the Size of Configuration Icons
The size of the icons used on the navigation pane and details pane can be adjusted.

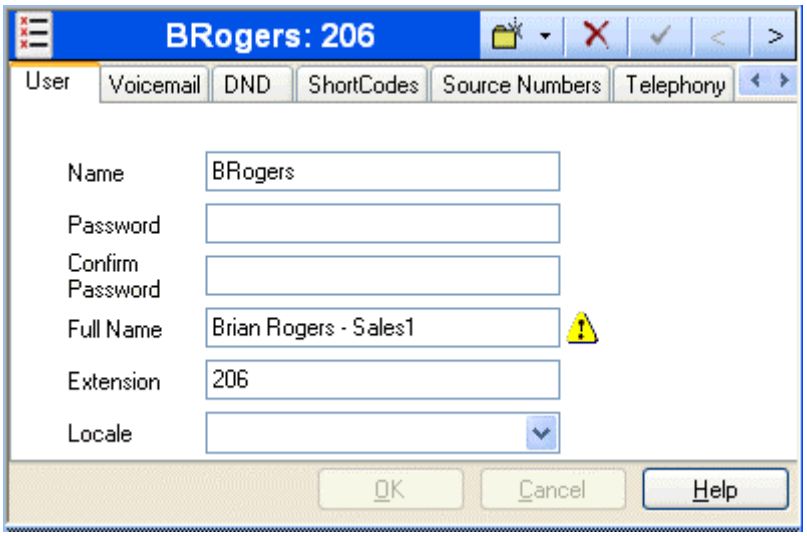
1. Select **File** and then **Preferences**.
2. Select the **Visual Preferences** tab.
3. Select the required icon size from **Small**, **Medium** or **Large**.
4. Click **OK**.

Using the Details Pane

Whenever a selection is made through the group pane or the navigation toolbar, the settings for the matching entry are shown in the details pane. This pane is also used by Manager in security mode to display entries for security settings.

The details are grouped into tabs. The tabs available may vary depending on what particular type of entry is being viewed. For example, for extension entries the **Analog** tab is only shown for analog extensions.

Individual settings may also be grayed out. This indicates that they are either for information only or that they cannot be used until another setting is enabled.



The top-left icon indicates the following:

Locked
Indicates that you can view the settings but cannot change them.

Editable
Indicates that you can change the settings if required.

Changed
Indicates that the settings have been changed since the tab was opened. Click **OK** to save the changes or **Cancel** to undo.

Various icons may appear adjacent to settings:

Locked Setting
The setting cannot be changed through this tab. This icon appears on user settings where the user is associated with User Rights that controls the setting.

Information
Indicates a value which does not have to be set but may be useful if set.

Warning
A warning indicates a configuration setting value that is not typical and may indicate misconfiguration.

Error
An error indicates a configuration setting value that is not supported by the IP Office. Such settings may cause the IP Office to not operate as expected.

Details Pane Actions

Editing an Entry

1. The method of entering an entry varies as different fields may use different methods. For example text entry boxes or drop down lists.
2. When changes are made, they are validated once another field is selected.
3. Clicking on **OK** at the base of the details pane to accept the changes or click on **Cancel** to undo the changes.

Adding a New Entry

1. Click  at the top-right of the details pane.
2. Select the type of entry required. For example, with services you can select from **Normal**, **WAN** or **Intranet**.

Deleting an Entry

1. Click  at the top-right of the details pane.

Validating an Entry

1. Click  at the top-right of the details pane.

Moving to the Previous or Next Entry

1. Click **<** or **>** at the top-right to move to the previous or next entry.

Selecting a Tab

1. To view the detail stored on a particular tab, click on the name of that tab.
2. If the tab required is not shown, use the  controls if shown on the right to scroll through the available tabs. The tabs available may vary depending on what particular type of entry is being viewed.

Changing the Position of the Details Pane

When the group pane is visible, the details pane is shown either below it or to its right. This position can be adjusted.

1. Select **View** and then **Details Pane**.
2. The current position setting is indicated by a tick mark.
3. To select a position, click on it.

Changing How the Tabs Display

For entries with more than two tabs, you can select whether Manager should use  controls or arrange the tabs as multiple rows when necessary.

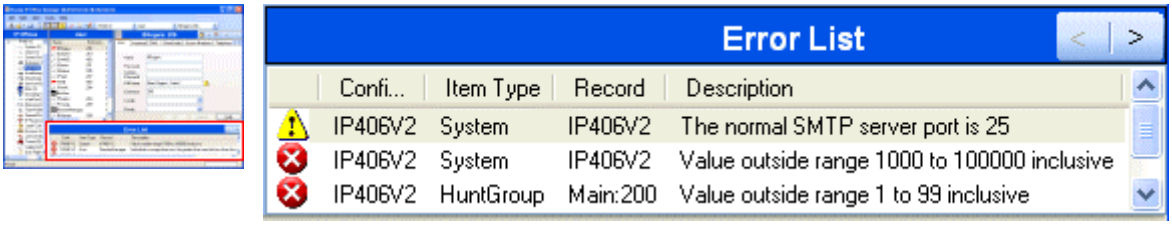
1. Select **Files | Preferences | Visual Preferences**.
2. Select **Multi-Line Tabs**.
3. Click **OK**.

Using the Error Pane

Validation is a process where Manager checks configuration entries for errors or for values for which it regards as requiring a warning. The results of this checking are shown by icons next to the field that caused the error or warning, All errors and warnings are also listed in the Error Pane.

By default validation is performed automatically whenever a configuration file is opened and when any field is edited. However, if required, the use of automatic validation can be controlled through the settings on the **File | Preference | Validation** tab.

The validation process can be run manually using the icon for the whole configuration or the icon for a particular entry.



The icons used for errors and warnings are:

Error
An error indicates a configuration setting value that is not supported by the IP Office. Such settings are likely to cause the IP Office to not operate as expected.

Warning
A warning indicates a configuration setting value that is not typical and may indicate misconfiguration.

Information
Typically indicates a setting which may be useful to set.

Error Pane Actions

Revalidating Configuration Settings

By default, the configuration is validated when loaded and individual entries are revalidated when changed.

1. To validate the whole configuration, click in the main toolbar.
2. For a particular entry, click in the details pane.

Jumping to an Error or Warning

1. Clicking on an error or warning in the error pane will load the matching entry tab into the details pane.
2. The **<** and **>** can be used to move to the next error or warning in the error pane.

Showing or Hiding Panes

The error pane is automatically displayed if a configuration containing errors or warnings is loaded into Manager. However it can be manually shown or hidden using either of the following methods.

1. From the main toolbar, use the icon.

or

1. Select **View**. Those panes currently shown are indicated by a tick mark.
2. To show or hide the error pane, click on its name.

Altering the Configuration Interface

The Manager configuration settings interface can be customized in a number of ways. These changes are remembered the next time Manager is started.

Resizing the Manager Window

When the Manager window is not maximized or minimized, it size can be adjusted.

1. Place the cursor over the edge of the current window.
2. When the cursor changes to a double-headed arrow, click and hold the cursor.
3. Drag the edge to the required position and then release the cursor.

Moving the Border Between the Panes

The border between the visible panes can be adjusted. Note that this is a proportional rather than exact position. If the whole window size is altered, the border position may also move.

1. Place the cursor over the border between two panes.
2. When the cursor changes to a double headed arrow with a bar through it, click and hold the cursor.
3. Drag the border to the required position and release the cursor.

Showing or Hiding Toolbars

The different toolbars can be hidden if not required.

1. Select **View** and then **Toolbars**. Those toolbars currently shown are indicated by a tick mark.
2. To show or hide a toolbar, click on its name.

Moving Toolbars

The position of the Manager toolbars can be moved. Note that when moving a toolbar, the other toolbars and panes may adjust their size or position to ensure that all the toolbar icons remain visible.

1. Place the cursor over the end of the toolbar.
2. When the cursor changes to a four-way arrow, click and hold the cursor.
3. Move the toolbar to the required position and release the cursor.

[break]

Showing or Hiding Panes

The details pane cannot be hidden. The navigation pane, group pane and error pane can be shown or hidden. To do this use either of the following methods.

1. From the main toolbar, use the following icons:
   -  **Hide/Show Navigation Pane**.
   -  **Hide/Show Group Pane**.
   -  **Hide/Show Error Pane**.

or

1. Select **View**. Those panes currently shown are indicated by a tick mark.
2. To show or hide a pane, click on its name.

Changing the Position of the Details Pane
When the group pane is visible, the details pane is shown either below it or to its right. This position can be adjusted.

1. Select **View** and then **Details Pane**.
2. The current position setting is indicated by a tick mark.
3. To select a position, click on it.

Changing the Size of Configuration Icons
The size of the icons used on the navigation pane and details pane can be adjusted.

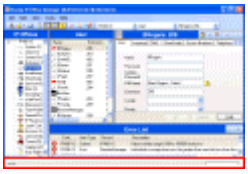
1. Select **File** and then **Preferences**.
2. Select the **Visual Preferences** tab.
3. Select the required icon size from **Small**, **Medium** or **Large**.
4. Click **OK**.

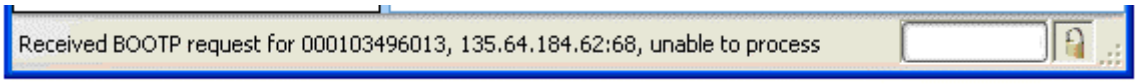
Changing How the Tabs Display
For entries with more than two tabs, you can select whether Manager should use  controls or arrange the tabs as multiple rows when necessary.

1. Select **Files | Preferences | Visual Preferences**.
2. Select **Multi-Line Tabs**.
3. Click **OK**.

The Status Bar

The status bar at the base of the Manager screen is used to display icons and messages about communications between Manager and IP Office systems. If the IP Office Manager is also acting as a BOOTP and TFTP server it will also show BOOTP and TFTP messages.





A padlock icon is displayed whenever the Manager communications settings are set to secure. This indicates all attempted configuration and security settings exchanged will be attempted over a secure TLS link:

Status bar messages display information about communications the Manager application receives. Some typical status bar messages are listed below.

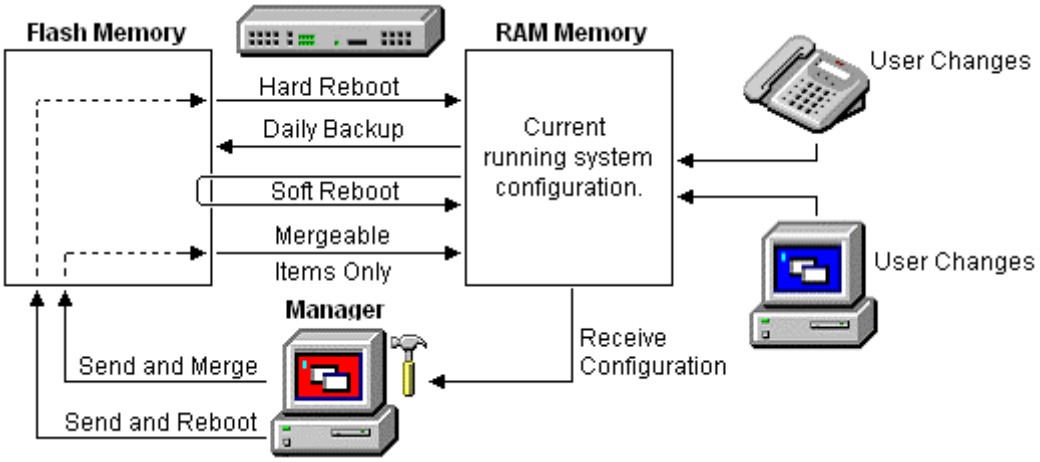
- **Ready**
  This message is normally seen when Manager has just started and no configuration has been received.
- **Received BOOTP request for 001125465ab2, unable to process**
  Manager is acting as a BOOTP server. It has received a BOOTP request that does not match an IP Office system listed in its BOOTP entries. The cause may be a device or application, other than an IP Office, that also uses BOOTP.
- **TFTP: Received TFTP Error "NotFound" from 135.64.180.171**
  An attempt to receive settings from or send settings to the IP Office failed. The most probable cause is a name or password error.
- **TFTP: Received 17408 bytes for Marks_Test**
  Manager has received configuration settings from the named system using TFTP.
- **Sent 100% of C:\Program Files\Avaya\IP Office\Manager\b10d01b2_3.bin**
  Manager has sent the indicated file in response to a BOOTP request.

Editing Configuration Settings

How the Configuration is Used

Before editing the IP Office configuration settings, it is important to understand how those settings are stored and used by the IP Office system.

- The IP Office control unit holds copies of its configuration in both Flash and RAM memory.
- The copy in Flash memory is retained even if power to the control unit is removed.
- During power up, the configuration in Flash memory is copied to the RAM memory.
- The copy in RAM memory is then used to control the IP Office system's operation.
- Users actions such as changing their forward destinations or mailbox passcode using their phone or Phone Manager are written to the configuration in RAM memory.
- Between 00:00 and 00:30, a daily backup occurs which copies the configuration in RAM back into Flash memory.



When using Manager to edit the configuration settings, the following need to be remembered:

- Manager receives the current configuration settings from RAM memory. Therefore the settings include any changes made by users up to that time.
- When sending the configuration settings back to the IP Office, Manager allows two choices, reboot or merge.
    - Reboot sends the configuration to the IP Office's Flash memory along with an instruction to reboot. Following the reboot, the new configuration in Flash memory is copied to the RAM memory and used.
    - Merge sends the configuration to the IP Office's Flash memory without rebooting. The IP Office then copies those changes that are mergeable into the RAM memory. A key point here is that not all configuration settings are mergeable, see the Reboot/Merge Configuration List that follows.

As a result of the above, it is important to bear the follow scenarios in mind:

- Changes made by users after a configuration is received by Manager may be lost when the configuration is sent back from Manager.
- If a merge is attempted with non-mergeable items, those items will be written to Flash memory but will not be copied to RAM memory. If a daily backup occurs, they will then be overwritten by the RAM. If a power loss reboot occurs, they will be written to RAM memory.

Mergeable Settings

The table below shows the configuration entries for which changes can be merged and those that require a system reboot. The **Send Configuration** menu shown when sending a configuration to the IP Office automatically indicates when the configuration is mergeable.

Mergeable		3.2+	Pre-3.2
	System	-	-
	- System	✓*1	✗
	- LAN1/LAN2	✗	✗
	- DNS	✗	✗
	- Voicemail	✓*2	✗
	- Telephony	✓*3	✗
	- H.323 Gatekeeper	✗	✗
	- LDAP	✗	✗
	- System Events	✗	✗
	- CDR	✓	✗
	- Twinning	✓	-
	Line	✗	✗
	Control Unit	✗	✗
	Extension	✗	✗
	User	✓	✓
	Hunt Group	✓	✓
	Short Code	✓	✓
	Service	✓	✓
	RAS	✓	✓
	Incoming Call Route	✓	✓

Mergeable		3.2+	Pre-3.2
	WAN Port	✗	✗
	Directory	✓	✓
	Time Profile	✓	✗
	Firewall Profile	✓	✓
	IP Route	✓	✓
	Least Cost Route	✓	✓
	Account Code	✓	✓
	License	✓	✓
	Tunnel	✗	✗
	Logical LAN	✗	✗
	Wireless	✗	✗
	User Rights	✓	✓
	Auto Attendant	✓	✗
	Authorization Code	✓	✗
	ARS	✓	-
	E911 System	✗	✗

- ***1 - 3.2+ | System | System**
  Changes to **Locale**, **License Server IP Address** and **Favor RIP Routes over Static** require a reboot.
- ***2 - 3.2+ | System | Voicemail**
  Changes to **Voicemail Type** require a reboot.
- ***3 - 3.2+ | System | Telephony**
  Changes to **Companding LAW** and **Busy Tone Detection** require a reboot.

Configuration File Sizes

There are maximum size limits to the configuration file that can be loaded into an IP Office control unit. They are:

Control Unit	Maximum Configuration File Size
Small Office Edition	192KB
IP403	192KB
IP406 V1	192KB
IP406 V2	256KB
IP412	1.0MB
IP500	1.0MB

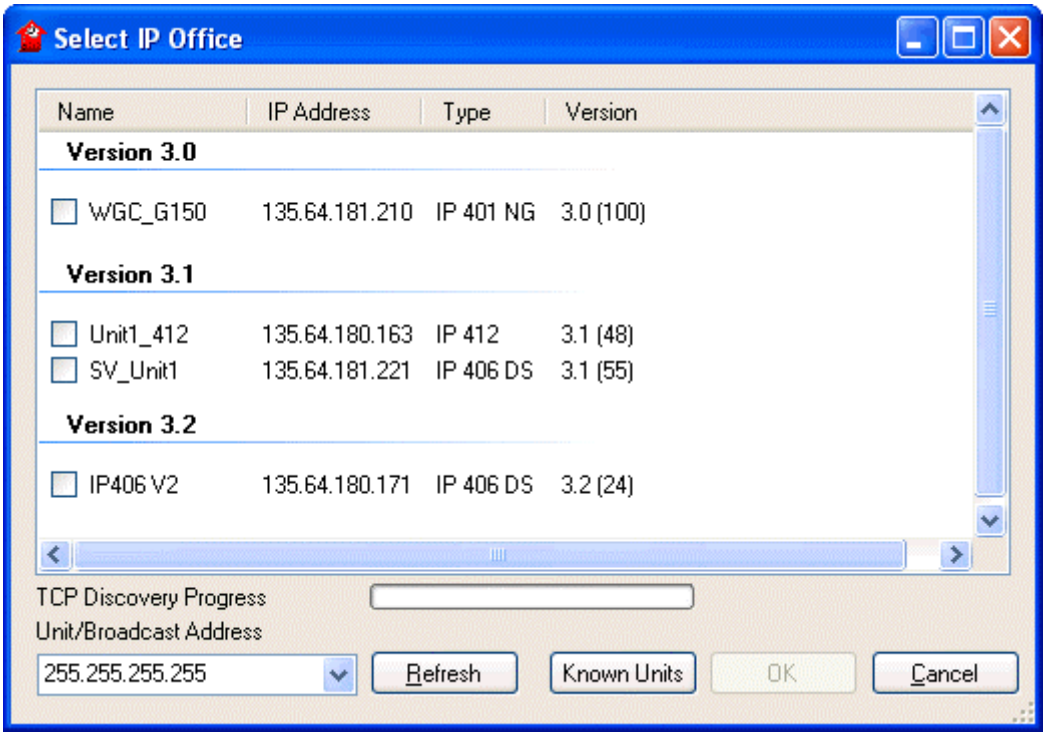
Attempting to load a configuration that exceeds the limits above will cause the system to lock and require resetting via the DTE port.

Figures for all individual entries in the configuration cannot be given as they vary between software releases. The list below gives typical values, in bytes, for common entries:

Physical Extension: 70.	**WAN Service:** 400.	**IP Route (Static):** 30.
IP Extension: 70.	**RAS Service:** 110.	**License Key:** 40.
User: 170.	**Incoming Call Route:** 30.	**Account Code:** 40.
User Short Code: 40.	**WAN Port (PPP):** 70.	**Logical LAN:** 60.
DSS Button: 20.	**WAN Port (FR):** 120.	**Tunnel (L2TP):** 200.
Hunt Group: 100.	**Directory Entry:** 70.	**Tunnel (IPSec):** 110.
Hunt Group member: 10.	**Time Profile:** 40.	
System Short Code: 10.	**Time Profile Entry:** 20.	
Normal Service: 220.	**Firewall Profile:** 40.	
Intranet Service: 240.	**Custom Firewall Entry:** 80.	

Setting the Discovery Addresses

By default, when or **File | Open configuration** is selected, Manager's **Select IP Office** menu appears. It performs a UDP broadcast to the address 255.255.255.255. This broadcast will only locate IP Office systems that are on the same network subnet as the PC running IP Office Manager.



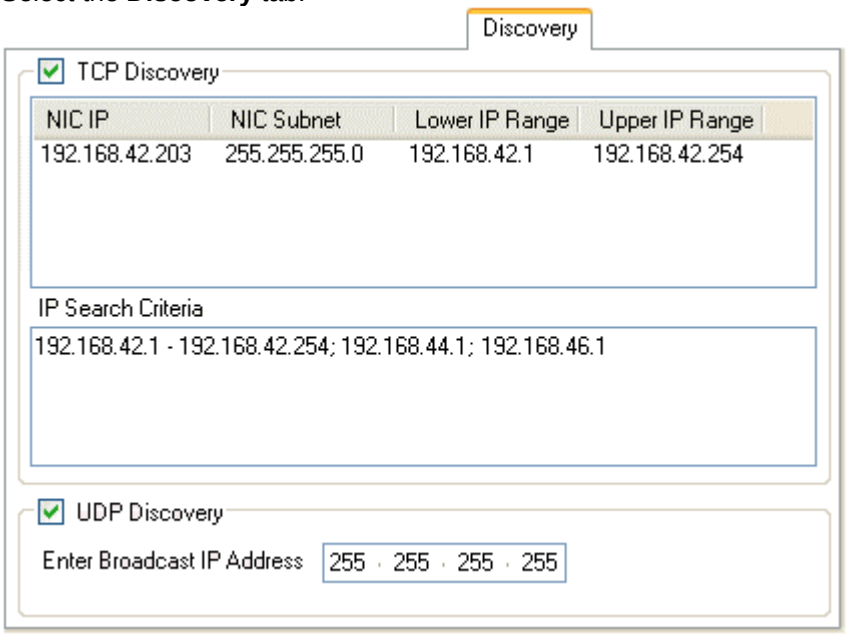
The process above is called discovery. A UDP broadcast will not be routed to other networks and subnets. Therefore to find IP Office systems not located on the same subnet as the Manager PC, the following other options are supported.

- **Specific Addressing**
  The **Unit/Broadcast Address** shown on the Select IP Office menu can be changed to the specific IP address of the required system. A single address is routable and so can be used to discover an IP Office system on another subnet.
- **TCP Discovery Address Ranges**
  IP Office 3.2+ systems support discovery by TCP as well as UDP. To support this, a set of TCP addresses and address ranges can be specified for use by the **Select IP Office** discovery process.
- **Known IP Office System Discovery**
  The IP Office 4.0 Q2 2007 maintenance release adds supports for a system whereby IP Office Manager can write the details of systems it discovers to a file. The list of systems in that file can then be used for access to those systems. See Known IP Office Discovery.

Changing the Initial Discovery Settings

The **Discovery** tab of the Manager **Preferences** menu can be used to set the UDP and TCP addresses used by the discovery process run by the Select IP Office menu.

1. Select **File | Preferences** menu.
2. Select the **Discovery** tab.



3. Under **UDP Discovery** you can enter the default UDP broadcast address to be used by the discovery process.
4. In the **IP Search Criteria** box you can enter IP addresses and IP address ranges for TCP discovery. Addresses are should be separated by semi-colons, ranges by - dashes.

Loading a Configuration

Manager can be used to load configuration settings directly from a running IP Office system or from a configuration file previously saved on the PC.

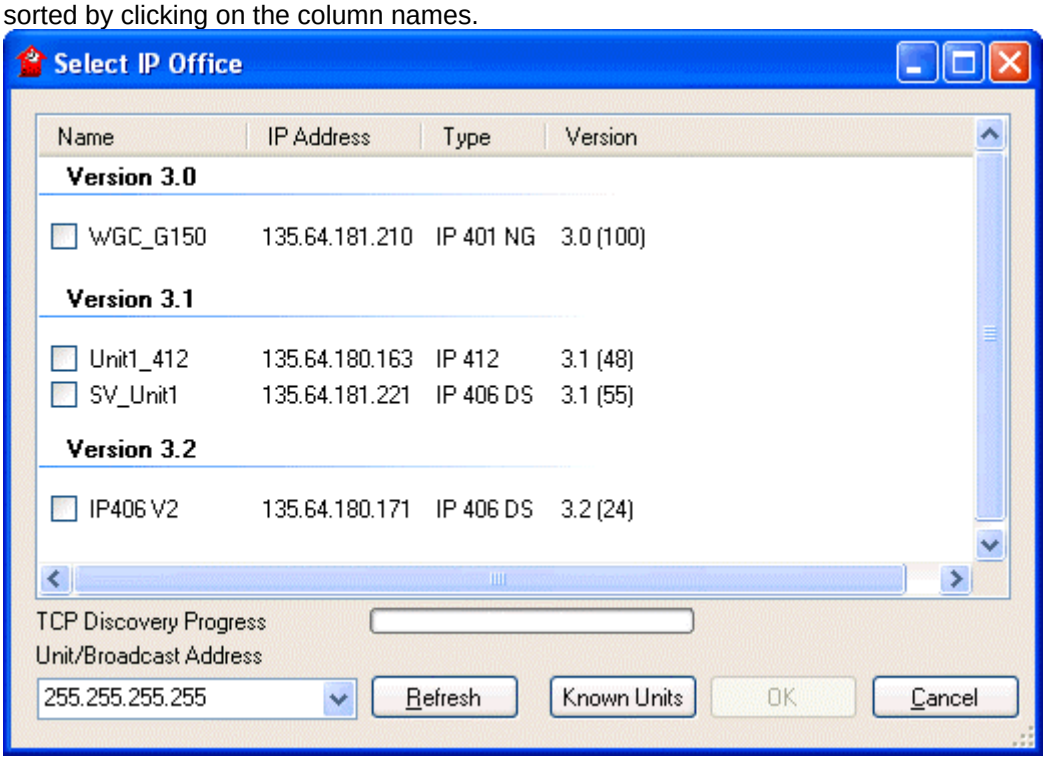
An important change for IP Office 4.1 is to optionally secure the link between the IP Office system and Manager for configuration and security settings exchanges. By default Manager and the IP Office will always attempt to use the original, unsecured link. The control of which mechanism is used by Manager is determined through Manager preferences (**File | Preferences | Security | Secure Communications**).

When secure communications mode is selected a padlock icon is present on the Manager status bar.

Loading the Current Configuration from an IP Office

The initial address ranges in which Manager searches for IP Office systems are set through the Manager preferences (**File | Preferences | Discovery**). The security mechanism used for configuration transfer between Manager and an IP Office are set through the Secure Communications attribute of Manager preferences (**File | Preferences | Security**).

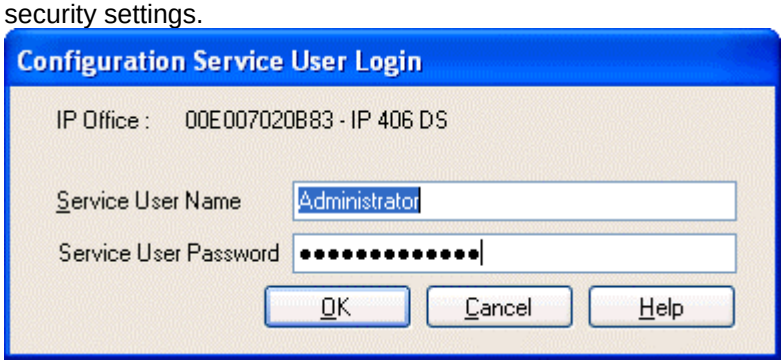
1. Click in the main toolbar or select **File | Open Configuration** from the menu bar.
2. The **Select IP Office** window appears, listing those IP Office systems that responded. The list can be sorted by clicking on the column names.



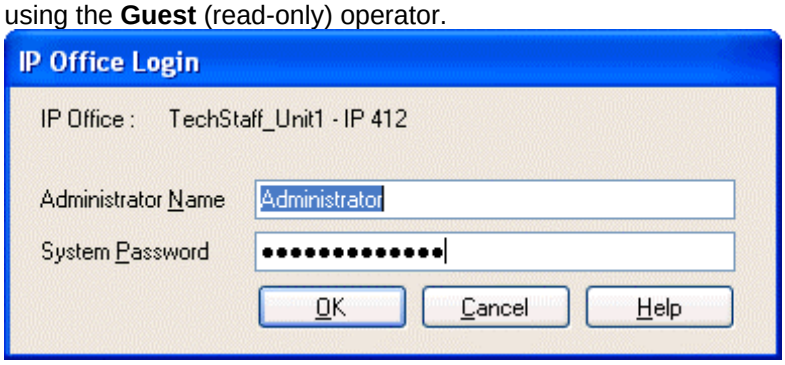
   - If the system required was not found, the address used for the search can be changed. Enter or select the required address in the **Unit/Broadcast Address** field and then click **Refresh** to perform a new search.
   - **Known Units** is not available unless configured, see **Known IP Office Discovery**.
3. When the system required is located, check the box next to the system and click **OK**.

4. The name and password request is displayed. Enter the required details and click **OK**.

   - **IP Office 3.2 and higher Systems:**
     The name and password used must match a Service User configured within the IP Office system's security settings.



   - **Pre-3.2 IP Office Systems:**
     The name must match a Manager operator and the password must match the IP Office system's system password. If the name does not match a Manager operator, the config will still be loaded by using the **Guest** (read-only) operator.



5. If the configuration is not loaded it may be for various reasons:

   - ***Access Denied***
     This is displayed as the cause if the service user name/password were incorrect, or the service user has insufficient rights to read the configuration. The **Retry** option can be used to login again but multiple rejections in a 10 minute period may trigger events, such as locking the user account, set by the **Password Reject Limit** and **Password Reject Action** options in the IP Offices security settings.

   - ***Failed to communicate with IP Office***
     This is displayed as the cause if the network link fails, or the secure communication mode is incorrect (for example Manager is set to unsecured, but the IP Office is set to secure only).

   - ***Account Locked***
     The account of the Service User name and password being used is locked. This can be caused by a number of actions, for example too many incorrect password attempts, passing a fixed expiry date, etc. The account lock may be temporary (10 minutes) or permanent until manually unlocked. An account can be enabled again through the IP Office's security settings.

6. Following a successful login, addition messages may also appear before the configuration is loaded, such as:

    - ***Your service user account will expire in X days***
      This message indicates that an **Account Expiry** date has been set on the IP Office service user account and that date is approaching. Someone with access to the IP Office's security settings will be required unlock the account and set a new expiry date.
    - ***Your password will expire in X days. Do you wish to change it now?***
      This message indicates that password ageing has been configured in the IP Office's security settings. If your password expires, someone with access to the IP Office's security settings will be required to unlock the account.
    - ***Change password***
      Through the IP Office's security settings, a service user account can be required to change their password when logging in. The menu provides fields for entering the old password and new password.
    - ***Contact Information Check - This configuration is under Integrated Management control***
      This message will appear if you use a standalone copy of IP Office Manager to load the configuration from an IP Office system that is being managed through the Avaya Integrated Management (AIM) suite. Normally such as system should only be accessed using the tools included in AIM. The options available are:
        - **Cancel**
          Select this option to close the configuration without making any changes.
        - **Set configuration alteration flag**
          Select this option if the configuration is being opened because some urgent maintenance action. When the configuration is next opened, the fact that it has been altered will be indicated on the **System | System** tab.
        - **Delete Contact Information**
          Select this option if the IP Office system is being permanently taken outside of management using AIM.
    - ***Contact Information Check - This configuration is under special control***
      This message will appear if a Manager user with administrator rights has entered their contact information into the configuration. For example to indicate that they do not want the configuration altered while a possible problem is being diagnosed. The options available are:
        - **Cancel**
          Select this option to close the configuration without making any changes.
        - **Set configuration alteration flag**
          Select this option if the configuration is being opened because some urgent maintenance action. When the configuration is next opened, the fact that it has been altered will be indicated on the **System | System** tab.
        - **Delete Contact Information**
          Select this option to take the IP Office system out of special control.
        - **Leave contact information and flags unchanged (Administrators only)**
          This option is only available to service users logging in with administrator rights.

Loading a Configuration Stored on PC

A configuration file previously saved on the PC can be reopened in Manager. This method of access does not require entry of a Service User name and password. All parts of the configuration are visible. In order to send a configuration opened this way to an IP Office 3.2 system, you must use a service user name with the **Administrator** operator rights view and rights to write with a reboot.

Use either of the following processes to load a saved configuration file:

1. If the files is one that has previously been opened offline, click the ▾ symbol next to  in the main toolbar. From the list of files displayed select the file required.

or

1. Click  the main toolbar or select **File | Offline | Open File** from the menu bar.
2. An **Open configuration file** window appears. Use this to browse to the required configuration file.
3. Select the file and click **Open**.

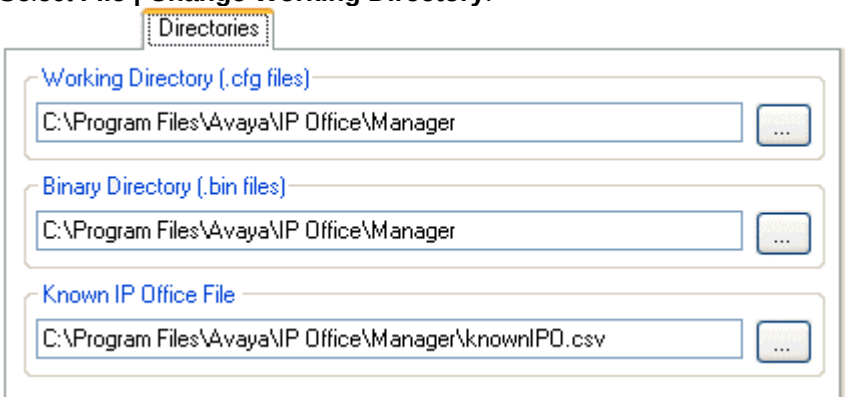
Known System Discovery

When or **File | Open Configuration** is used, Manager displays the Select IP Office screen. This displays the IP Office systems discovered by either UDP broadcast and or TCP requests (see Setting the Discovery Addresses). The IP Office 4.0 Q2 2007 maintenance release adds a additional method which is to record details of discovered units and then display a list of those previously discovered ('known') IP Office systems.

Configuring Manager for Known System Discovery

Use of known systems discovery is not enabled by default. The IP Office Manager must be configured for the feature with a file location to which it can store and retrieve know system details.

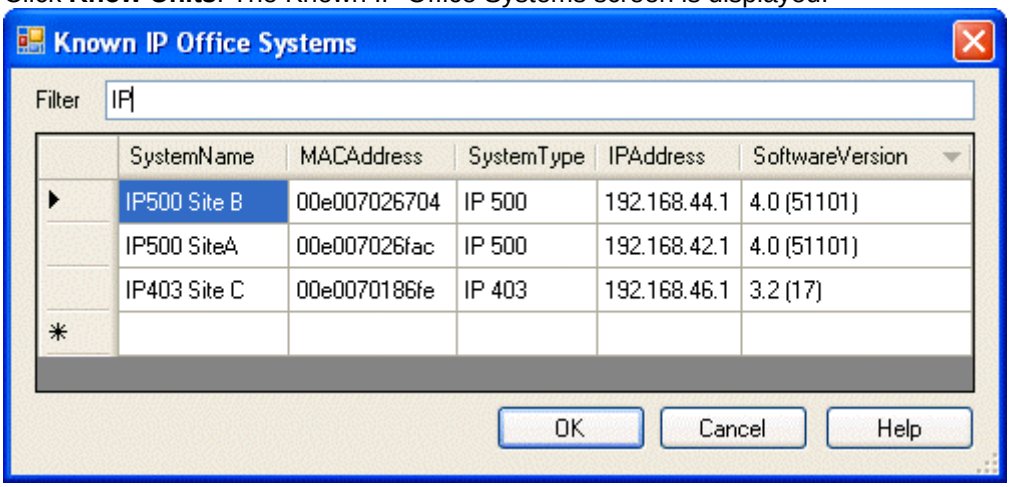
1. Select **File | Change Working Directory**.



2. In the **Known IP Office File** field, enter the directory path and file name for a CSV file into which Manager can write details of the IP Office systems it discovers. If the file specified does not exist it will be created the next time IP Office system discovery is performed from Manager.
3. Click **OK**.
4. When or **File | Open Configuration** is used, a Known Units button is now available on the Select IP Office screen.

Using Know System Discovery

1. Select or **File | Open Configuration**.
2. The Select IP Office screen is displayed.
3. Click **Know Units**. The Known IP Office Systems screen is displayed.



4. The screen displays the list of IP Office systems previously discovered and stored in the CSV file.
    - To select an IP Office control unit, highlight the row containing unit data and click **OK**. The selected unit will appear in the discovery list of the Select IP Office window. See Loading a Configuration.
    - To filter displayed units, type the first few characters of the unit name in the **Filter** field. Any unit whose name does match the filter from left to right will be temporarily hidden.
    - Each discovery appends data to the known unit list. It is possible that details of some entries in the list may be out of date. Right clicking on the leftmost (grey) column of any row will bring up a floating menu offering the options of **Refresh** and **Delete**.
    - A new entry may be manually added without having to access the system first through normal discovery. Enter the IP address of the new system in the IP Address column of the blank row shown with a * and select **Refresh** from the floating menu. This will update the Known Units file with data relating to the unit with the specified address.
    - Selecting the **Cancel** button will terminate the selection operation. It will not revert any manually created entries.

Note:

- The key used by the Known Systems CSV file is the IP address. The file cannot contain entries for separate systems that use the same IP address for access.
- The file can be made read only. In that case any attempts using Manager to update the file will be ignored.

Creating a New Configuration

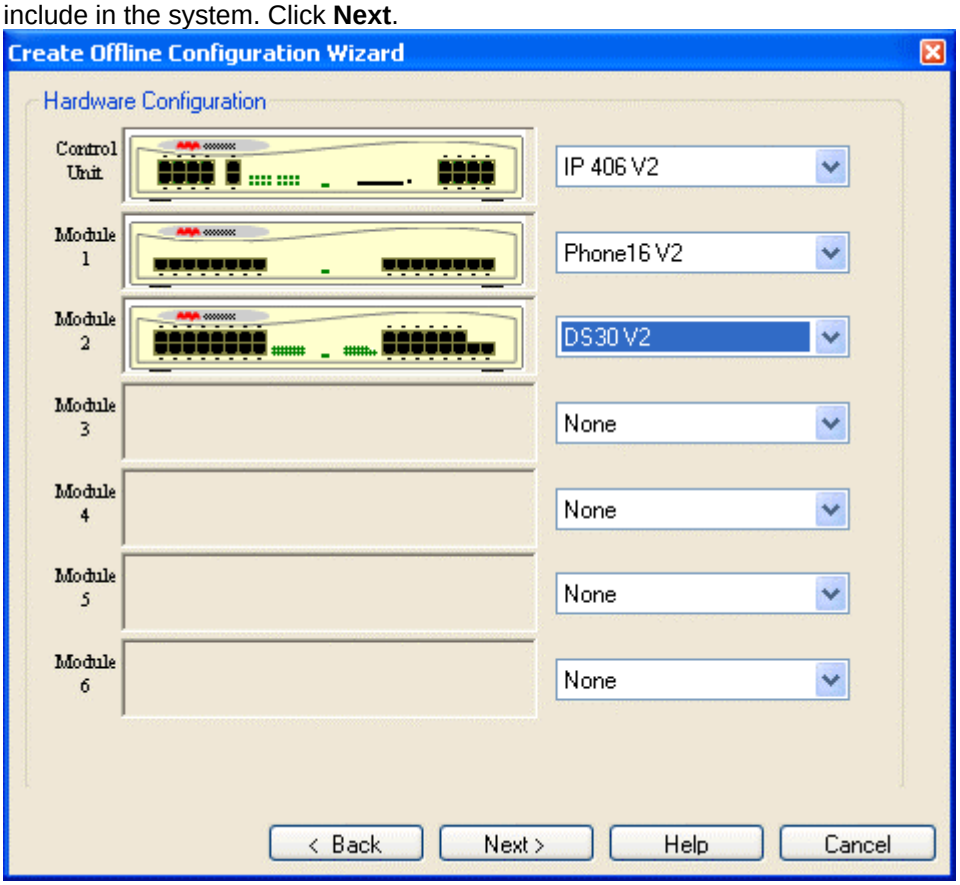
Manager can be used to create a new configuration without connecting to an IP Office system. During the process, you can specify the locale of the system, what type of trunk cards it uses and what type of control unit and expansion modules to include.

This allows the creation of a configuration prior to installation of the real system and so can be used to speed up installation.

- The configuration created must match the physical equipment in the IP Office system onto which the configuration will be loaded. Doing otherwise may cause the IP Office system to reset and experience other problems.
- The **Create Configuration** tool includes all control units, external expansion modules and trunk cards supported by IP Office. It is you responsibility to confirm what IP Office equipment is supported in your locale.

Creating a New Configuration

1. Click  in the main toolbar or select **File | Offline | Create New Config** from the menu bar.
2. Select the **Locale** for the system. This defines a range of features such as default telephony settings. Click **Next**.
3. Fixed Length Numbering is supported for IP Office 4.1+. The value can be ***None*** or ***3*** to ***9***. Click **Next**.
    - If a value is selected, all default extension, user and hunt group extension numbers created by Manager will be that length. in addition Manager will display a warning if an extension number of a different length is entered when editing the configuration.
4. Select the type of IP Office control unit. Then select the expansion modules, excluding WAN3, to also include in the system. Click **Next**.



5. The next step will depend on the type of IP Office control unit selected.
    - For Small Office Edition and IP400 series control units select the trunks cards to be included and the IP address of a WAN3 module if required.
    - For IP500 control units, first select the extension/VCM base cards required. Depending on the card selection different trunk daughter cards can then be added.

6. Click **Finish**.
7. The configuration is created and loaded into Manager.
8. Once this configuration has been edited as required it can be saved on the PC. In order to send it to the matching IP Office system, **File | Offline | Send Configuration** has to be used.

Importing and Exporting Settings

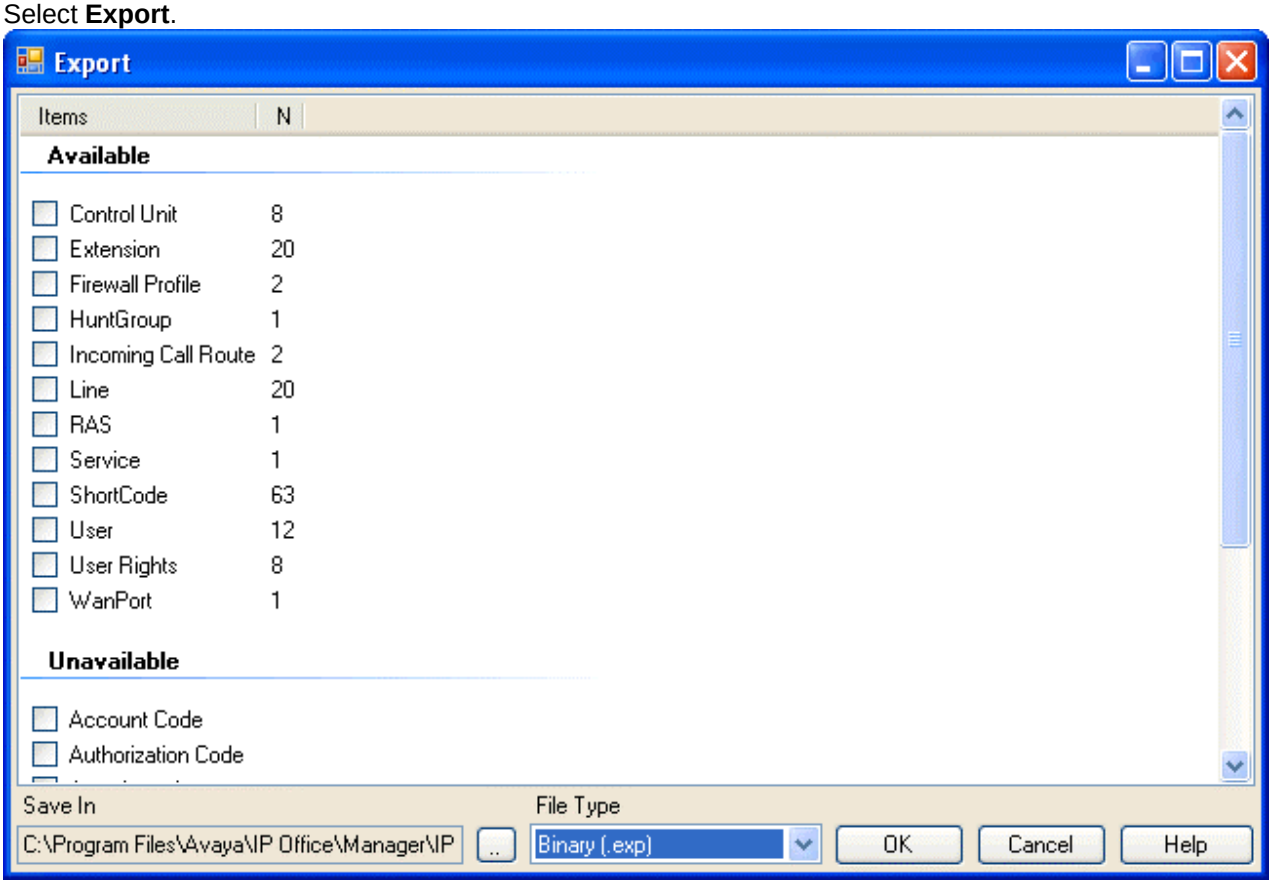
Manager can import configuration settings created elsewhere. This can be useful when setting up a new system or sharing common settings such as a directory between systems.

Settings are imported and exported in two formats:

- **Binary Files (.exp)**
  These are non-editable files. During import and export it is possible to select what types of entries should be included in the file. During import the whole file is imported.
- **Comma Separated Variable Text Files (.csv)**
  These are plain text files. In addition to being exported from an IP Office system these files can be created and edited using programs such as WordPad or Excel.
    - Manager imports and exports CSV files using UTF8 character encoding which uses a double byte to support characters with diacritic marks such as ä. Other applications such as Excel, depending on the user PC settings, may use different single-byte encoding which will cause such characters to be removed. Care should be taken to ensure that any tool used to create or edit a CSV supports all the characters expected and is compatible with UTF8.

Exporting Settings

1. Select **File | Import/Export...** from the menu bar.
2. Select **Export**.

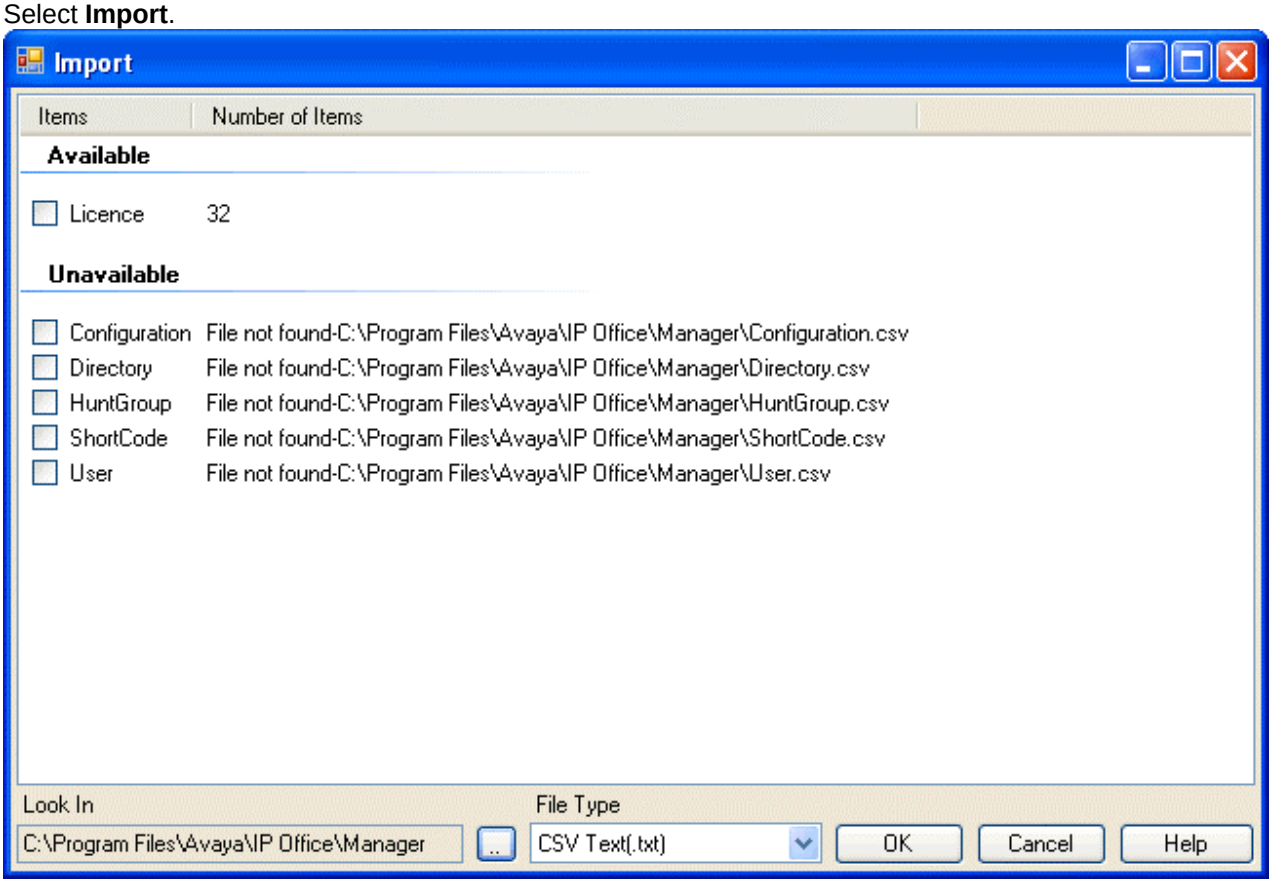


3. Select the type of file. The list of exportable entry types will change to match the file type.
4. Select the types of items that should be exported.
5. Use the **Save In** path to select the location for the exported files. The default location used is sub-directory of the Manager application directory based on system name of the currently loaded IP Office system.
6. Click **OK**.

Importing Settings

Importing settings will overwrite any existing entries that match an entry being imported.

1. Select **File | Import/Export...** from the menu bar.
2. Select **Import**.



3. Select the type of file. The list of items will change to match the type of file selected and whether a matching file or files is found in the current file path.
4. Use **Look In** to adjust the file path. The default location used is sub-directory of the Manager application directory based on system name of the currently loaded IP Office system.
5. Select the types of items that should be imported.
6. Click **OK**.

CSV File Formats

The format is CSV using commas as field separator, no text delimiters and no header row. The simplest way to check the required format for a CSV file prior to import, is to export and study the settings from an existing system.

File Name	Fields in Order
Directory	Name, Number.
HuntGroup	Name, Extension, Group, Hunt, Rotary, Longest Waiting, Queuing On, Voicemail On, Broadcast, Voicemail Email.
License	License, License Key
ShortCode	Code, Telephone Number, Feature.
User	Name, Extension, User Restriction/Rights, Voicemail Email.
Configuration	*Proprietary format*

Notes

- **Hunt Group:** Apart from Name, Extension and Voicemail Email, the fields use a 1 or 0 value for on or off.
- **License:**
  - The License field is for information only and is ignored during import.
  - Following import the License name may appear as invalid with Manager. To resolve this save and then reload the configuration file.
- The format of the system CSV is too complex to be described. It is a full export of all the IP Office system's configuration settings. This file format should only be used for export and import between systems and not for any offline editing.

Copying and Pasting

IP Office Manager supports the normal Windows methods of cutting, copying, pasting and deleting entries and settings. These can be accessed through the **Edit** menu in the menu bar or using the standard Windows keyboard shortcuts for those actions. They can also be accessed by selecting an entry or text field and then right-clicking.

Copy and paste can be used with the navigation and group panes to create a new entry with the same settings as the original. The copy will be renamed as ***Copy of ...*** to avoid conflicting with the original.

When using copy and paste between individual settings fields, whether on the same entry or a different entry, care should be taken to ensure that the fields use the same type of data. Similarly copying an entry in the navigation or group pane and then pasting it into the details pane will prompt Manager to paste the copied entries data into the first field of the current entry in the details pane. As a general rule, cut and paste actions should be used with the same pane and within similar entry types.

For users and user rights, a number of controls have been provided to copy settings between a user and a user right or vice versa. See User Rights Overview in the Configuration Settings section.

Saving a Configuration onto PC

The IP Office system configuration settings shown within Manager can be saved as a .cfg file on the Manager PC. These files can be used as backups or sent to other persons to aid problem diagnostics. Note however that an offline configuration file does not include the Audit Trail records for the IP Office system.

Automatically Saving Sent Configurations

By default, Manager creates a file copy of the configuration before it is sent to the IP Office. This copy is stored in Manager's Working Directory using the IP Office's system name and .cfg. This behavior is controlled by the **Save configuration file before send** setting (**File | Preferences | Edit | Preferences**).

Saving a Configuration Received from an IP Office

1. Select **File | Save Configuration as** from the menu bar.

Saving a Configuration opened on the PC

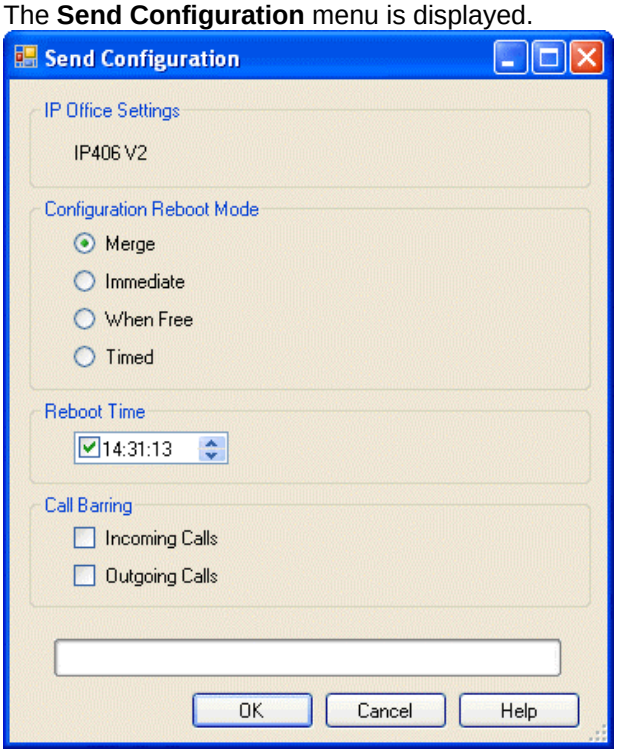
1. Click  in the main toolbar or select **File | Save Configuration** from the menu bar.

Sending a Configuration

The current configuration settings open within Manager can be sent to the IP Office system.

Sending a Configuration to an IP Office

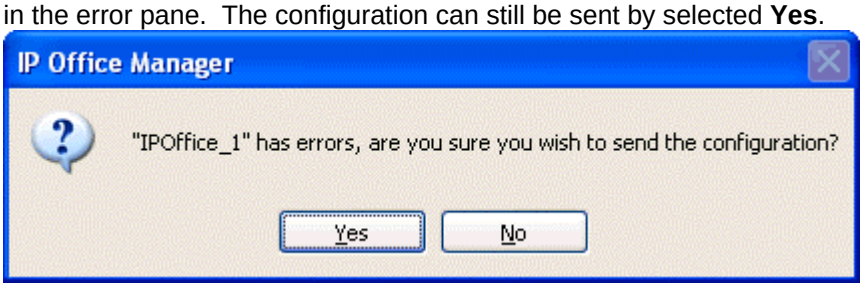
1. The first steps of this process depend on whether you are sending a configuration received from the IP Office system or sending one opened offline/created new.
   - **Received Configuration**
     Click in the main toolbar or select **File | Save Configuration** from the menu bar.
   - **Opened Offline/Newly Created Configuration**
     Select **File | Offline | Send Config** from the menu bar.
2. The **Send Configuration** menu is displayed.



- **Password** - Pre-3.2 Systems Only
  This field appears for pre-3.2 IP Office system. The system password should be entered. If sending the configuration to an IP Office 3.2 system, a Service User name and password are requested when **OK** is clicked.
- **Configuration Reboot Mode**
  If Manager thinks the changes made to the configuration settings are mergeable, it will select ***Merge*** by default, otherwise it will select ***Immediate***.
  - **Merge**
    Send the configuration settings without rebooting the IP Office. This mode should only be used with settings that are mergeable. Refer to Mergeable Settings.
  - **Immediate**
    Send the configuration and then reboot the IP Office.
  - **When Free**
    Send the configuration and reboot the IP Office when there are no calls in progress. This mode can be combined with the **Call Barring** options.
  - **Timed**
    The same as When Free but waits for a specific time after which it then wait for there to be no calls in progress. The time is specified by the **Reboot Time**. This mode can be combined with the **Call Barring** options.

- **Reboot Time**
  This setting is used when the reboot mode **Timed** is selected. It sets the time for the IP Office reboot. If the time is after midnight, the IP Office's normal daily backup is canceled.
- **Call Barring**
  These settings can be used when the reboot mode **When Free** is selected. They bar the sending or receiving of any new calls.

3. Click **OK**. For IP Office 3.2 systems a Service User name and password will be requested.
   - If the service user name or password used do not have a match on the IP Office, *"Access Denied"* is displayed.
   - If the service user name used does not have rights to send a configuration or to request a reboot or merge, *"Insufficient service user rights"* is displayed.
   - If the service user name used does not have operator rights to make the changes that have been made to the configuration, *"Insufficient operator rights. Operator cannot modify xxxx records"* is displayed.
4. The following warning will appear if the configuration being sent contain any errors indicated by a icon in the error pane. The configuration can still be sent by selected **Yes**.



Erasing the IP Office Configuration

The configuration settings on an IP Office can be erased. During this process the IP Office is rebooted and starts with a set of default settings.

This process does not erase the security settings of the IP Office system. Those can only be reset by a separate process detailed in the IP Office Installation Manual.

Erasing the Configuration

This action returns the IP Office system to its default settings as listed below.

1. Select **File | Advanced | Erase Configuration (Default)**.
2. Enter a valid user name and password.
3. The IP Office system will be rebooted.

Default Data Settings

When a defaulted IP Office control unit is switched on, it requests IP address information from a DHCP Server on the network.

- If a DHCP server responds, the control unit defaults to being a DHCP client and uses the IP address information supplied by the DHCP server.
- If no DHCP Server responds, the control unit defaults to being the DHCP server for the LAN using the following settings:
    - For its LAN1 it allocates the IP address 192.168.42.1 and IP Mask 255.255.255.0.
    - It supports 200 DHCP clients using the addresses range 192.168.42.2 and 192.168.42.201, the IP Mask 255.255.255.0 and default gateway address 192.168.42.1 (the Control Unit's LAN1 address).
    - On Small Office Edition, IP412 and IP500 control units, LAN2 is allocated the address 192.168.43.1 with IP Mask 255.255.255.0. On Small Office Edition and IP500 control units, the RJ45 Ethernet WAN port is treated as LAN2.

Default Telephony Settings

- Extension and user entries are created for all physical analog and DS phone ports on the control unit and any connect expansion modules. Users are assigned extension numbers from 201 upwards.
- User names are defaulted to "Extn201", "Extn202", etc.
- A hunt group called **Main** is created, containing the first 10 user extensions.
- A default incoming call route is created for voice calls with the hunt group Main as its destination.
- A default incoming call route is created for data calls with the RAS service as its destination.

Exceptions

- The status of the **Use Port 8 as LAN2** setting is retained even if the IP Office system is defaulted.

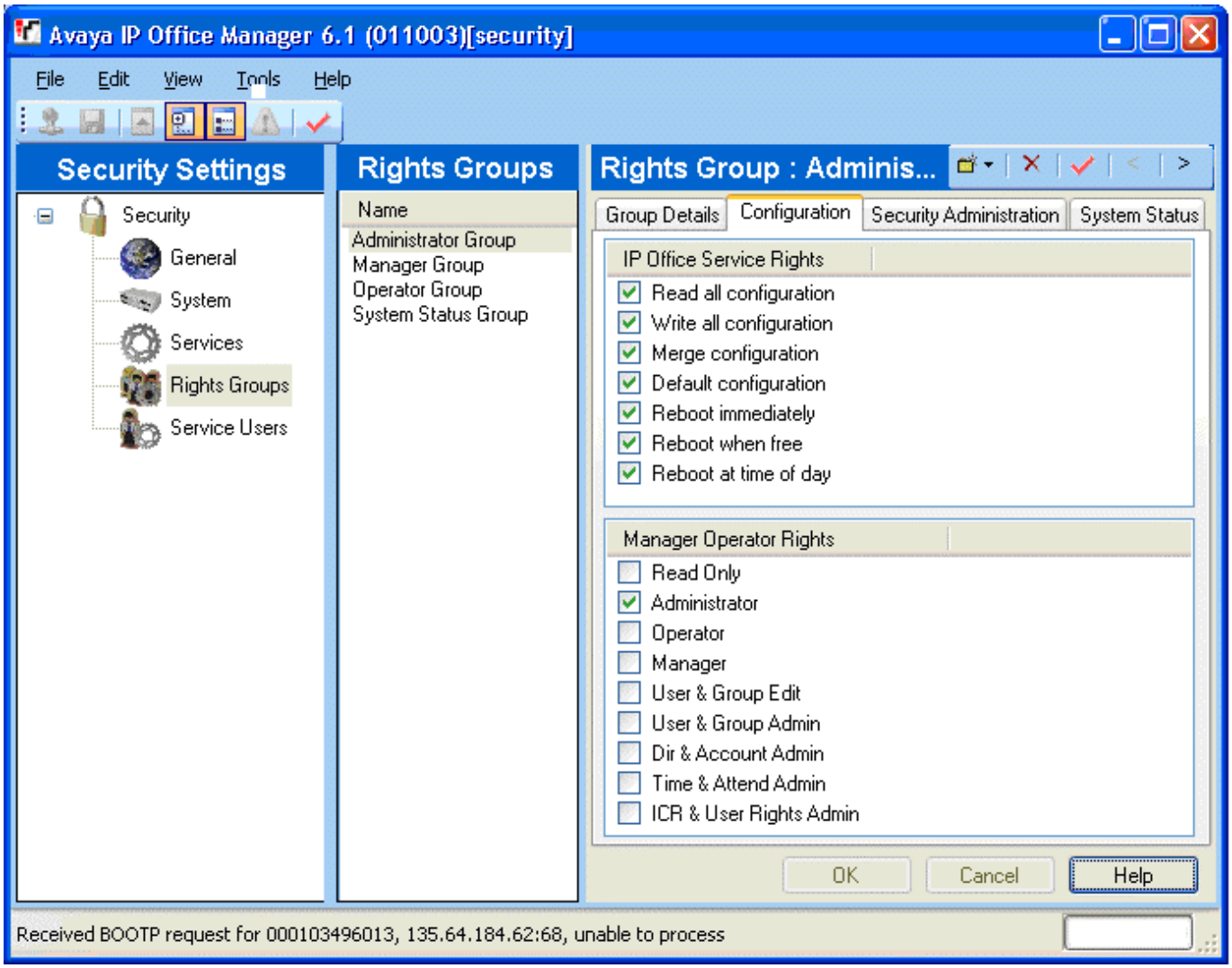
Security Mode

Overview of Security Settings

Security settings are used to control who can access the configuration settings of an IP Office system and what they are able to do with that access. They also control which applications are able to access the configuration settings.

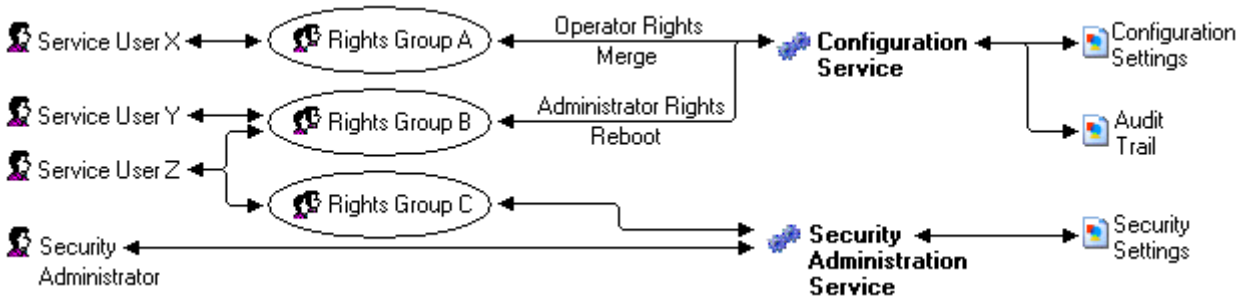
The security settings are stored on the IP Office system and are separate from the system's configuration settings.

To change a system's security settings, Manager must first be switched to security mode by selecting **File | Advanced | Security Settings** from the menu bar.



Security Settings

Access to IP Office 3.2+ system settings is controlled by Service Users 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.



In the example illustrated above:

- Service User X can read and write the configuration. However they can only edit Operator settings and can only make changes that can be merged.
- Service User Y can read and write the configuration, edit all settings and make changes that require reboots.
- Service User Z can read and write the configuration, edit all settings and make changes that require reboots. They can also access the security settings.
- The Security Administrator can only access the security settings.

Security Administrators

By default the security administrator is the only user who can access the IP Office's security settings using Manager's security mode.

Service Users

Each Service User has a name, a password and is a member of one or more Rights Groups.

Rights Groups

The Rights Groups to which a Service User belongs determine what actions they can perform. Actions available to Rights Groups include configuration actions, security actions and system status actions:

Configuration	Security	System Status
• **Read the configuration.** • **Write the configuration.** • **Merge the configuration.** • **Default the configuration.** • **Reboot immediately.** • **Reboot when free.** • **Reboot at time of day.**	• **Read all security settings.** • **Write all security settings.** • **Reset all security settings.** *(IP Office 4.1+)* • **Write own password.** *(IP Office 4.1+)*	• **System Status Access.** • **Read All Configuration.**

Where a Service User has been configured as a member of more than one Rights Group, they combine the functions available to the separate Rights Groups.

Operator Rights

Each Rights Group has a **Manager Operator Rights** setting. This setting controls what types of configuration entries Manager will allow members of the Rights Group to view and what actions they can perform with those types of entries.

Operator	View/Edit/ New/Delete	Configuration Entry Types
Administrator	All	View, edit create and delete all configuration entries.
Manager	View	View all except **WAN Port**.
	Edit	**Extension**, **User**, **Hunt Group**, **Short Code**, **Service**, **RAS**, **Incoming Call Route**, **Directory**, **Time Profile**, **Firewall Profile**, **IP Route**, **Least Cost Route**, **Account Code**, **ARS, E911 System**.
	New	
	Delete	As edit except **Short Code**.
Operator	View	View all except **WAN Port**.
	Edit	**Extension, User**, **Hunt Group**, **Short Code**, **Service, RAS**, **Incoming Call Route**, **Time Profile**, **Firewall Profile**, **IP Route**, **Least Cost Route**, **Account Code**, **Licence, ARS**, **E911 System**.
	New	None.
	Delete	Delete **Incoming Call Route** and **Directory**.
User & Group Edit	View	**User** and **Hunt Group** entries only.
	Edit	
	New	None
	Delete	
User & Group Admin	All	**User** and **Hunt Group** entries only.
Dir & Account Admin	All	**Directory** and **Account Code** entries only.
Time & Attendant Admin	All	**Time Profile** and **Auto Attendant** entries only.
ICR & User Rights Admin	All	**Incoming Call Route** and **User Rights** entries only.
Read Only	View	View all configuration entries.
	Edit	None.
	New	
	Delete	

Default Security Users

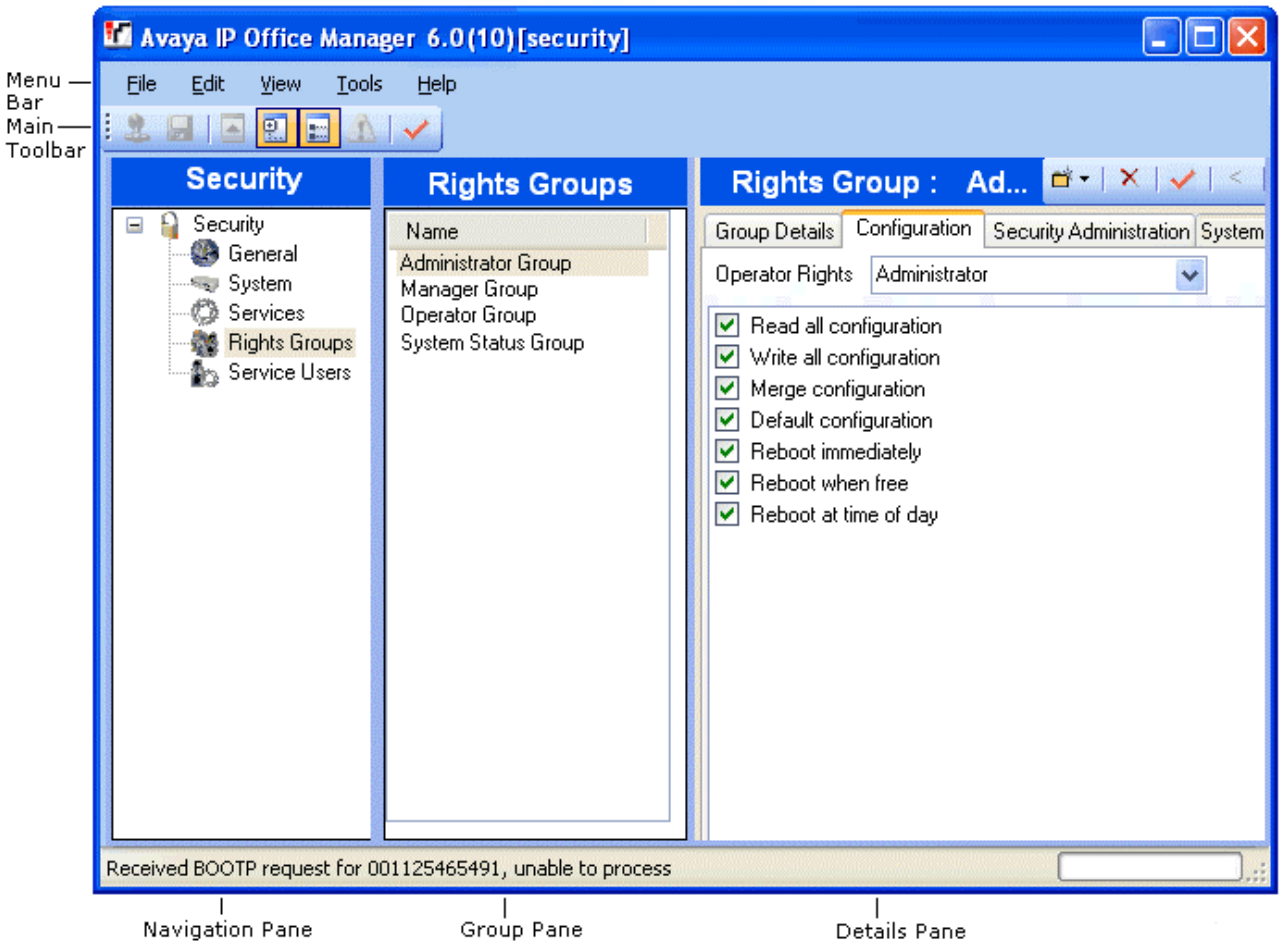
This section lists the default Rights Groups and Service Users for IP Office 4.0+ systems.

- ⚠ **WARNING: Change Passwords**
  New IP Office systems and systems upgraded from pre-IP Office 3.2 use default security settings. These settings must be changed to make the system secure. At minimum you must change the default passwords of the Security Administrator and the default Service Users. Failure to do so will render the IP Office system unsecure.

Unique Security Control Unit			
Enabled	✓		
Name	security		
Password	securitypwd		
Default Service Users			
Name	Administrator	Manager	Operator
Password	Administrator	Manager	Operator
Rights Group Membership			
- Administrator Group	✓	✗	✗
- Manager Group	✗	✓	✗
- Operator Group	✗	✗	✓
- System Status Group	✓	✓	✓
Default Rights Groups			
Name	Administrator Group	Manager Group	Operator Group
Operator View	Administrator	Manager	Operator
Read Configuration	✓	✓	✓
Write Configuration	✓	✓	✓
Default Configuration	✓	✓	✓
Merge	✓	✓	✓
Reboot Immediately	✓	✓	✓
Reboot When Free	✓	✓	✓
Reboot at Time	✓	✓	✓
Read All Security Settings	✗	✗	✗
Write All Security Settings	✗	✗	✗
Reset All Security Settings *(IP Office 4.1+)*	✗	✗	✗
Write own service user password *(IP Office 4.1+)*	✗	✗	✗

The Security Mode Interface

Manager can be switched to security mode. This mode it is used to load and edit the security settings of an IP Office 3.2 system. How the controls operate is the same as for Manager in configuration mode.



Switching Manager to Security Mode

1. Select **File | Advanced | Security Settings**.

Switching Manager Back to Configuration Mode

1. Select **File | Configuration**.

Manager Security Mode Screen Elements

- **Menu Bar**
  Provides commands for loading and saving security settings. See the **Menu Bar Commands** section.
- **Main Toolbar**
  The toolbar icons perform the following actions:
  - **Get the Security Settings.**
  - **Save the Security Settings.**
  - ***Not Used in security mode.***
  - **Show/Hide the Navigation Pane.**
  - **Show/Hide the Group Pane.**
  - ***Not used in security mode.***
  - ***Not used in security mode.***
- **Security Settings Pane**
  This pane is used to select the type of security entries that should be displayed in the group pane or details pane.
  - **General**
    Defines general security controls for the IP Office system. When selected, the settings are displayed in the details pane.
  - **System**
    Defines security settings for the IP Office such as application access. When selected, the settings are displayed in the details pane.
  - **Services**
    Secure services supported by the IP Office. Currently these are access to security settings and access to configuration settings.
  - **Rights Groups**
    Create groups with different access rights. When selected, the existing Rights Groups are displayed in the group pane.
  - **Service Users**
    Sets the name and password for an administrator. Also allows selection of the Rights Groups to which the user belongs. When selected, the existing Service Users are displayed in the group pane.
- **Group Pane**
  This pane is used to display the existing Right Groups or Service Users when those options are selected in the security settings pane.
- **Details Pane**
  This pane shows the settings selected in the security settings pane or the group pane.
- **Status Bar**
  This bar display messages about communications between Manager and IP Office systems. It also displays the security level of the communications by the use of a padlock icon.

Security Administration

This appendix covers the background to administrating IP Office 4.1+ in a secure environment, including policy considerations and implementation choices. This section also covers a basic introduction to security principles and the security mechanisms on IP Office.

NOTE: If IP Office administration security is of no concern, the default settings allow modification of all IP Office features without restriction. It is recommended as a minimum that default passwords are changed.

1. Introduction

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+.

2. 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.

In the example illustrated above:

- Service User X can read and write the configuration. However they can only edit Operator settings and can only make changes that can be merged.
- Service User Y can read and write the configuration, edit all settings and make changes that require reboots.
- Service User Z can read and write the configuration, edit all settings and make changes that require reboots. They can also access the security settings.
- The Security Administrator can only access the security settings.

Security Administrator
By default the security administrator is the only user who can access the IP Office's security settings using Manager's security mode.

Service Users
Each Service User has a name, a password and is a member of one or more Rights Groups.

Rights Groups
The Rights Groups to which a Service User belongs determine what actions they can perform. Actions available to Rights Groups include configuration actions, security actions and system status actions.

Where a Service User has been configured as a member of more than one Rights Group, they combine the functions available to the separate Rights Groups.

3. 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:

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.

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.

4. Message Authentication

Message authentication ensures that all data sent by either IP Office or Manager cannot be tempered 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 check 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 hash 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.

IP Office supports message authentication 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.

5. Identity

The identity of the equipment or person at each end of the link is achieved by the used 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 to 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.

6. 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 ensure 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

7. Windows Certificate Store Organisation

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.

IP Office Manager only accesses some of the certificate sub folder:

Certificates (Local Computer) Folder	IP Office Manager Use
Personal | Certificates	• Folder searched by Manager 1st for matching certificate to send to IP Office when requested. Certificate matched by the subject name contained in File | Preferences | Security | Certificate offered to IP Office. • Folder accessed whenever 'Local Machine certificate store' used for Security Settings. • Folder searched by Manager for matching certificate when certificate received from IP Office, and File | Preferences | Security | Manager Certificate Checks = Medium or High.
Trusted Root Certification Authorities | Certificates	• Folder searched by Manager for matching parent certificates when non-self signed certificate received from IP Office, and File | Preferences | Security | Manager Certificate Checks = Medium or High.

Certificates – Current User Folder	IP Office Manager Use
Personal | Certificates	• Folder searched by Manager 2nd for matching certificate (subject name) to send to IP Office when requested. Certificate matched by the subject name contained in File | Preferences | Security | Certificate offered to IP Office. • Folder accessed whenever 'Current User certificate store' used for Security Settings. • Folder searched by Manager for matching certificate when certificate received from IP Office, and File | Preferences | Security | Manager Certificate Checks = Medium or High.
Trusted Root Certification Authorities | Certificates	• Folder searched by Manager for matching parent certificates when non-self signed certificate received from IP Office, and File | Preferences | Security | Manager Certificate Checks = Medium or High.
Other People | Certificates	• Folder searched by Manager for matching parent certificates when non-self signed certificate received from IP Office, and File | Preferences | Security | Manager Certificate Checks = Medium or High.

8. Windows Certificate Store Import

In order to use certificates – either for IP Office security settings or Manager operation – they must be present in the windows certificate store. Certificates may be placed in the store by the Certificate Import Wizard or the Certificate MMC snap-in

The Certificate Import Wizard can be used whenever a certificate is viewed. In order for Manager to subsequently access this certificate the Place all certificate in the following store option must be selected:

- If the certificate is to subsequently identify the IP Office, the Other People folder should be used.
- If the certificate is to subsequently identify the Manager, the Personal folder should be used, and the associated private key saved as well.

If the saved certificate is to be used by other windows users, the MMC certificate snap-in must be used to move it to the Certificates (Local Computer) folder.

9. Certificate Store Export

Any certificate required outside of the Manager PC required to be first saved in the Certificate store, then exported using the MMC snap-in.

If the certificate is to be used for identity checking (i.e. to check the far entity of a link) the certificate alone is sufficient, and should be saved in PEM or DER format.

If the certificate is to be used for identification (i.e. to identify the near end of a link) the certificate and private key is required, and should be saved in PKCS#12 format, along with a password to access the resultant .pfx file.

10. Implementing IP Office Administration Security

This section suggests IP Office security settings that could implement possible security requirements. This section does not cover the general aspects of security policy analysis or definition, or how IP Office administration security interacts with other security mechanism.

10.1. Negligible Security

If all Manager and IP Office security settings are left at default, no security mechanisms are active, other than the use of default service user names and passwords. In addition, all legacy interfaces are active, and all configuration and security data is sent unencrypted.

It is recommended that at the very least, the default service user passwords are changed.

10.2. Minimum Security

A minimum security scenario could be where configuration data is open, but the security settings are constrained: Any individual with the correct service user name and password can access the configuration from any PC installation of Manager, no logging of access: Passwords can be simple, and will never age.

- Change all default passwords of all service users and Security Administrator
- Set IP Office Security Administration service security level to Secure, Low.
- Set IP Office Service User Password Reject Action to None.
- Set IP Office Client Certificate Checks level to None (default).
- Set IP Office Minimum Password Complexity to Low (default).
- Set IP Office Previous Password Limit to zero (default).
- Set IP Office Password Change Period to zero (default).
- Set IP Office Account Idle Time to zero (default).
- Set certificate check level to low in Manager Security Preferences (default).

In addition, any PC installation of Manager can manage any IP Office.

10.3. Medium Security

A medium security scenario could be where both configuration and security settings are constrained and a level of logging is required: Any individual with the correct service user name and password can access the configuration from any PC installation of Manager: Passwords cannot be simple, and will age.

- Change all default passwords of all service users and Security Administrator
- Set IP Office Security Administration service security level to Secure, Medium.
- Set IP Office Configuration service security level to Secure, Medium.
- Set IP Office Service User Password Reject Action to Log to Audit Trail (default).
- Set IP Office Client Certificate Checks level to None (default).
- Set IP Office Minimum Password Complexity to Medium.
- Set IP Office Previous Password Limit to non zero.
- Set IP Office Password Change Period to non zero.
- Set IP Office Account Idle Time to zero (default).
- Disable all IP Office Unsecured Interfaces.
- Set certificate check level to low in Manager Security Preferences (default).

10.4. Maximum Security

A maximum security scenario could be where both configuration and security settings are constrained and a full level of logging is required: Certified individuals with the correct service user name and password can access the configuration from specific PC installations of Manager: Passwords cannot be simple, and will age: Manager can managed specific IP Office systems.

- Change all default passwords of all service users and Security Administrator
- Set IP Office Security Administration service security level to Secure, High.
- Set IP Office Configuration service security level to Secure, High.
- Set IP Office Service User Password Reject Action to Log and Disable Account.
- Set IP Office Client Certificate Checks level to High.
- Set IP Office Minimum Password Complexity to High.
- Set IP Office Minimum Password Length to >8.
- Set IP Office Previous Password Limit to non zero (>5).
- Set IP Office Password Change Period to non zero.
- Set IP Office Account Idle Time to non zero.
- Set IP Office Session ID Cache to zero.
- Install valid, 1024 bits+, non self signed certificates (+private key) in all IP Office server certificates, derived from a trusted certificate authority.
- Install the corresponding trusted CA certificate in each of the Manager's windows certificate stores.
- Install valid, 1024 bits+, non self signed certificate (+ private key) in all Manager Certificate Stores.
- Install the corresponding certificates in all IP Office Certificate Stores of all permissible Manager entities, and the trusted CA certificate.
- Disable all IP Office Unsecured Interfaces.
- Set Manager Certificate Checks level to high in Manager Security Preferences.
- Set Certificate offered to IP Office in Manager Security Preferences.

The above essentially locks the IP Office systems and corresponding Managers together. Only recognised (by strong certificate) entities may communicate successfully on the service interfaces. All services use strong encryption and message authentication.

The use of intermediate CA certificates can be used to overcome the limit of 6 maximum certificates in each IP Office Certificate Store.

Editing Security Settings

Loading and Saving Security Settings

Security settings can only be loaded directly from an IP Office system. These settings cannot be saved as a file on the local PC, nor do they appear as a temporary file at any time.

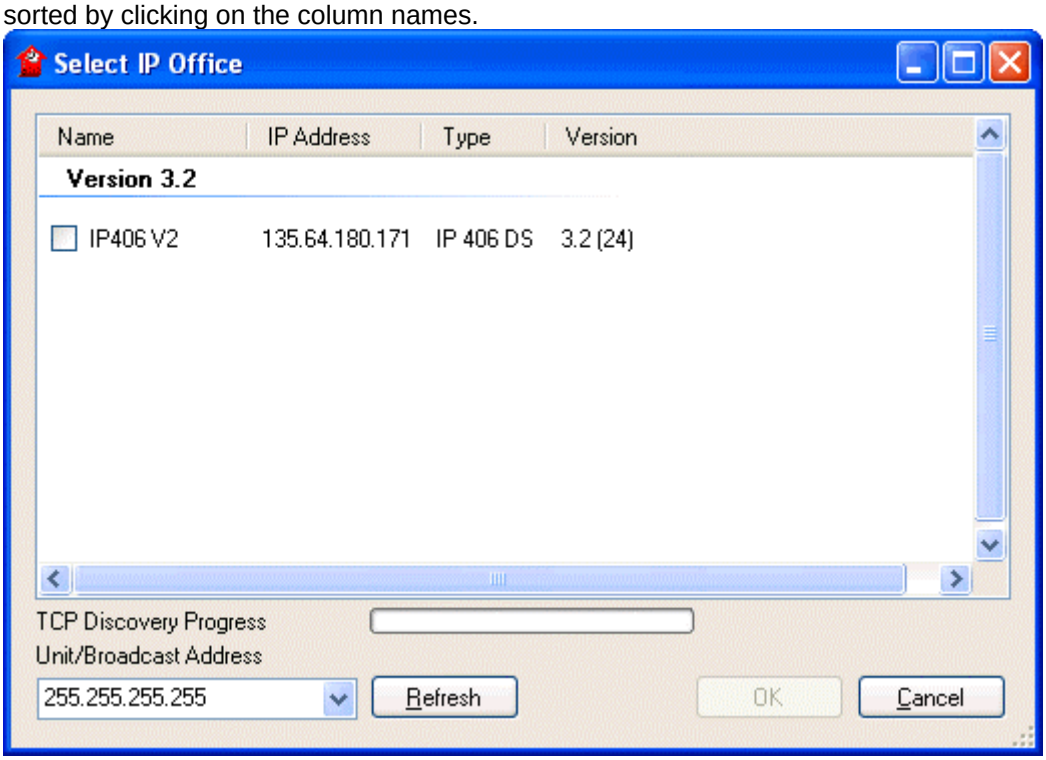
An important change for IP Office 4.1 is to optionally secure the link between the IP Office system and Manager for configuration and security settings exchanges. By default Manager (and IP Office) will always attempt to use the original, unsecured link. The control of which mechanism is used by Manager is determined Manager preferences.

When secure communications mode is selected a padlock icon is present on the Manager status bar.

Loading an IP Office's Security Settings

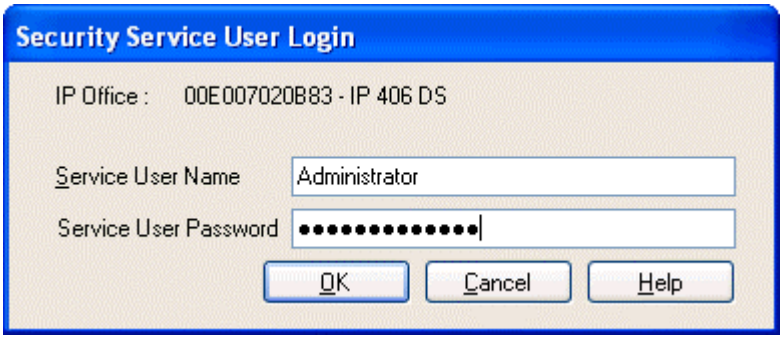
The address ranges in which Manager searches for IP Office systems are set through the Manager preferences (**File | Preferences | Edit | Discovery**). The security mechanism used for security settings transfer between Manager and an IP Office are set through the Secure Communications attribute of Manager preferences (**File | Preferences | Edit | Security**).

1. If not already done, switch Manager to security mode by selecting **File | Advanced | Security Settings**.
    - Note: If the IP Office system's configuration settings have already been loaded using a Service User name and Password that also has security access, then the security settings are automatically loaded when Manager is switched to security mode.
2. If already in security mode, click in the main toolbar or select **File | Open Security Settings** from the menu bar.
3. The **Select IP Office** window appears, listing those IP Office systems that responded. The list can be sorted by clicking on the column names.



4. If the system required was not found, the address used for the search can be changed. Enter or select the required address in the **Unit/Broadcast Address** field and then click **Refresh** to perform a new search.
5. When the system required is located, check the box next to the system and click **OK**.

6. The user name and password request for the system is then displayed. Enter the required details and click **OK**. By default this is a different user name and password from those that can be used for configuration access.



7. If the security settings are received successfully, they appear within Manager.
    - If the service user name/password is incorrect, or the service user has insufficient rights to read the security settings, *"Access Denied"* is displayed.
    - If the network link fails, or the secure communication mode is incorrect (for example Manager is set to unsecured, but the IP Office is set to secure only), *"Failed to communicate with IP Office"* is displayed.

Editing Security Settings

Editing security settings differ from editing configuration settings in a number of ways:

1. Editing of security settings may only be done online to an IP Office. No offline saving or editing is allowed for security purposes.
2. No errors in the security settings are allowed to persist. This prevents the IP Office becoming inaccessible through operator error.
3. Sets of changes to security objects may be made without the need for the **OK** button to be selected every time. This allows a coordinated set of changes to be accepted or cancelled by the operator.

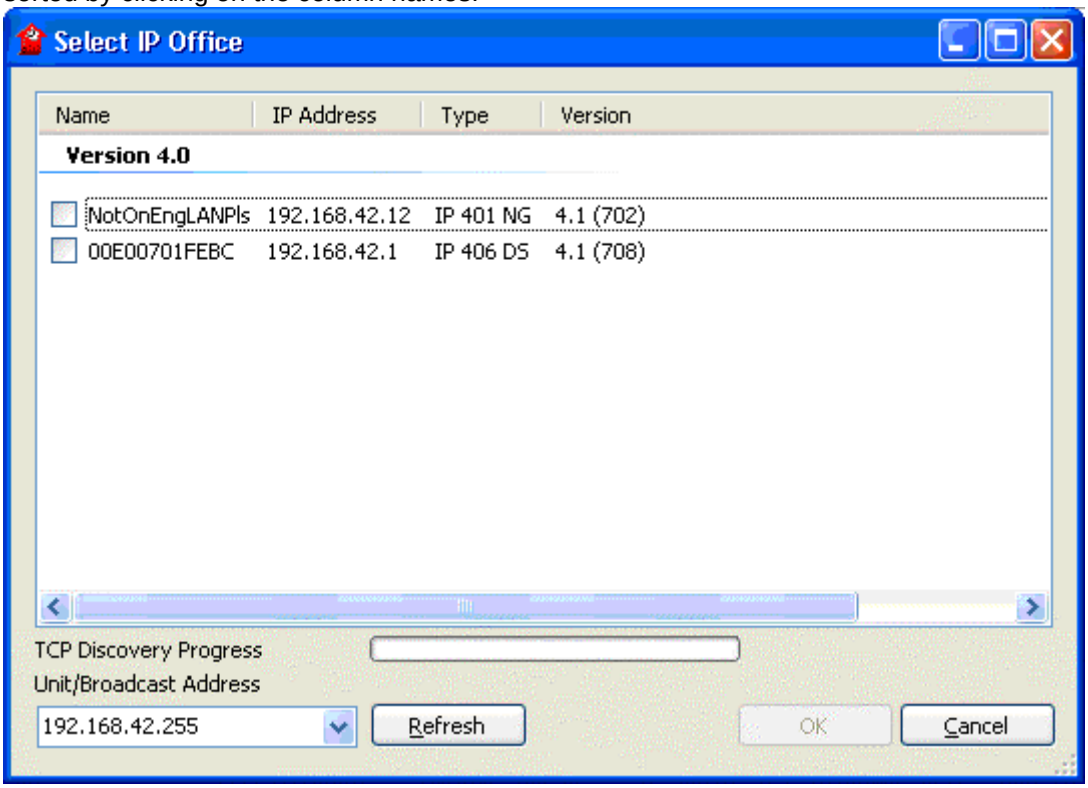
Saving Security Settings

1. Click in the Main Toolbar or select **File | Save Security Settings** from the menu bar. These options are only available when some change has been made.
2. The user name and password request for the system is then displayed. Enter the required details and click **OK**. By default this is a different user name and password from those that can be used for configuration access.

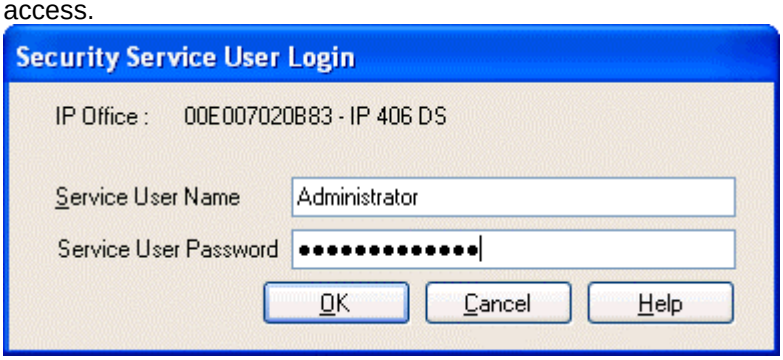
Resetting An IP Office's Security Settings

This option is only supported by IP Office 4.1 and higher systems. For other systems the method of resetting security settings requires is through the IP Office's DTE port, refer to the IP Office Installation manual for details.

1. Select **File | Reset Security Settings** (if in security mode), or **File | Advanced | Erase Security Settings** (if in configuration mode).
2. The **Select IP Office** window appears, listing those IP Office systems that responded. The list can be sorted by clicking on the column names.



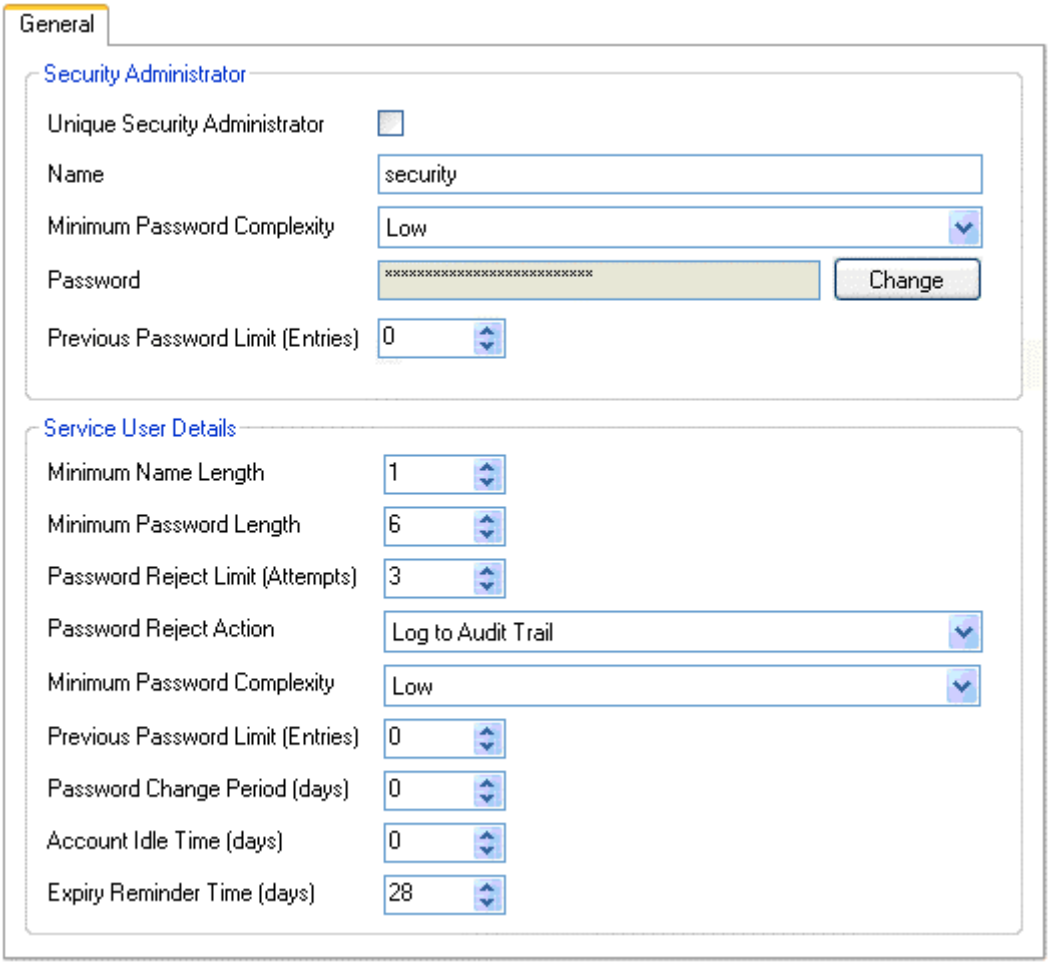
3. When the system required is located, check the box next to the system and click **OK**.
4. The user name and password request for the system is then displayed. Enter the required details and click **OK**. By default this is a different user name and password from those that can be used for configuration access.



5. Manager will indicate if the security settings are reset successfully.

General Settings

These settings are displayed when **General** is selected in the navigation pane.



- **Security Administrator**
  The Security Administrator is a special Service User who does not belong to any Rights Groups. The Administrator is able to access the IP Office system's security settings but cannot access its configuration settings. By default it is the only Service User able to access to the security settings.
  - **Unique Security Administrator:** *Default = Off*
    When selected, only the Security Administrator is able to access the IP Office system's security settings. When this is selected, the security options for Rights Groups are disabled. When not selected, the ability to access security settings can also be assigned to Rights Groups.
  - **Name:** *Default = 'security'. Range = 6 to 31 characters.*
    The name for the Security Administrator.
  - **Minimum Password Complexity:** *Default = Low, Software level = 4.1+.*
    The password complexity requirements for the Security Administrator. 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.

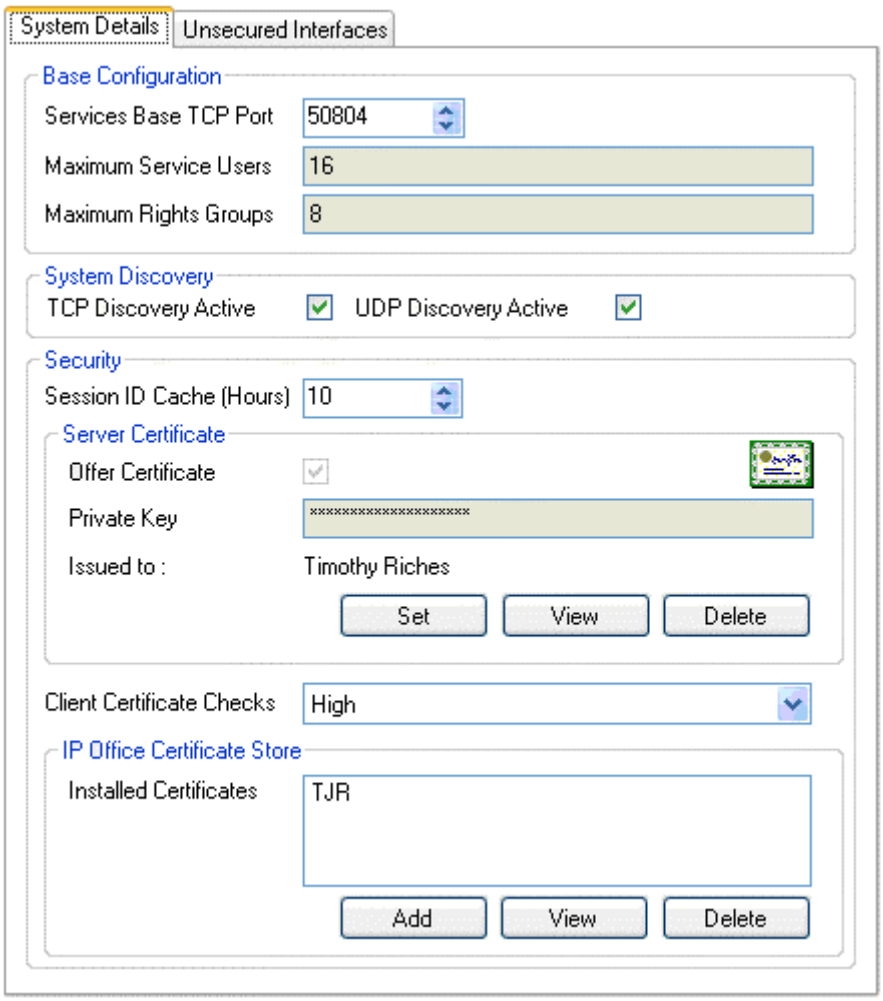
- **Password:** *Default = 'securitypwd'. Range = 6 to 31 characters.*
  The password for the Security Administrator. In order to change the Security Administrator password, the current password must be known.
- **Previous Password Limit:** *Default = 0. Range = 0 (Off) to 10 entries, Software level = 4.1+.*
  The number of previous password 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**
  These settings control Service User names and password/account policies.
  - **Minimum Name Length:** *Default = 6, Range 1 to 31 characters.*
    This field sets the minimum name length for Service User names.
  - **Minimum Password Length:** *Default = 6, Range 1 to 31 characters.*
    This field sets the minimum password length for Service User passwords.
  - **Password Reject Limit:** *Default = 3, Range 0 to 255 failures.*
    Sets how many times an invalid name or password is allowed within a 10 minute period before the **Password Reject Action** is performed. Selecting ***0*** indicates never perform the **Password Reject Action**.
  - **Password Reject Action:** *Default = Log to Audit Trail*
    The action performed when a user reaches the **Password Reject Limit**. Current options are:
    - ***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, Software level = 4.1+.*
    The password complexity requirements for all Service Users. 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.
  - **Password Change Period:** *Default = 0 (Off), Range 0 to 999 days, Software level = 4.1+.*
    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 a **Expiry Reminder Time** (see below).
    - 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, Software level = 4.1+..*
  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.
    - 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, Software level = 4.1+.*
  Sets the period before password or account expiry during which a reminder indication 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 (see **Service User** setting) – whichever is the sooner. It is up to the IP Office application to display this reminder. Currently IP Office Manager displays reminders but SSA does not.

Security | System Details

This tab is accessible when **System** is selected in the navigation pane.



- **Base Configuration**
  - **Base TCP Port:** *Default = 50804, Range = 49152 to 65526.*
    This is the base TCP port for services provided by IP Office 3.2+ systems. It sets the ports on which the IP Office listens for requests to access those services, using its LAN1 IP address. Each service uses a port offset from the base port value. If this value is changed from its default, the Manager application must be set to the same Base TCP Port through its **Services Base TCP Port** setting (**File | Preferences**).

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+

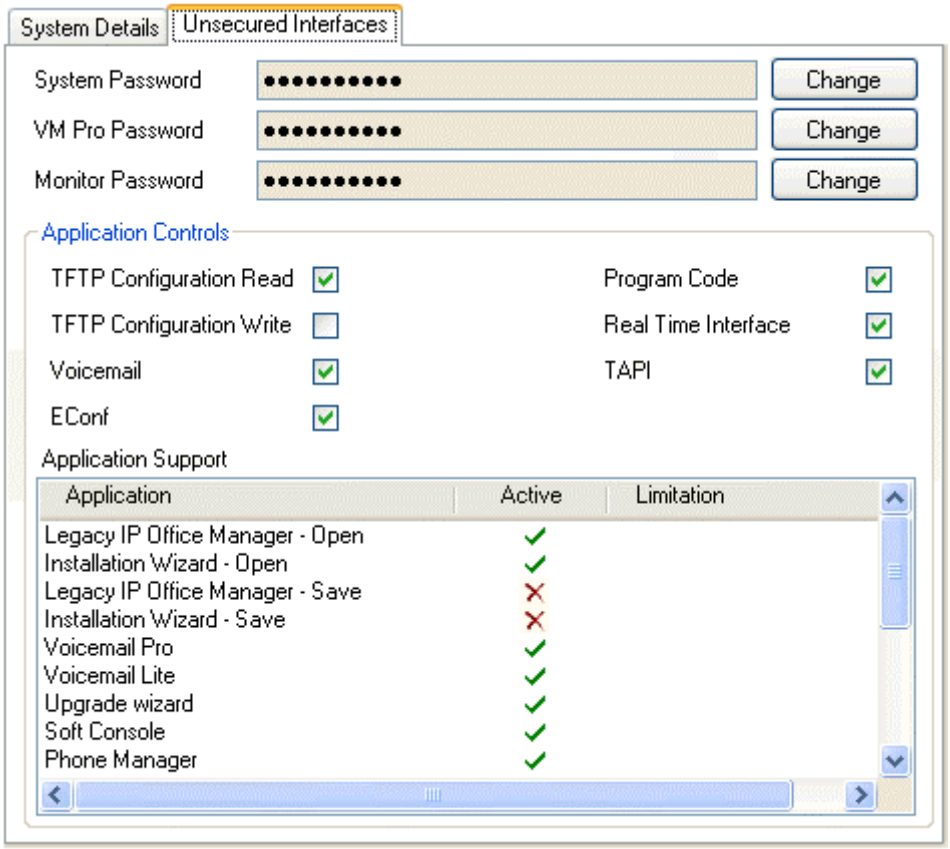
    - When changing the base port, exercise caution that the selected port and those offset from it do not conflict with any ports already in use by other applications.
  - **Maximum Service Users:** *Default = 16.*
    This is a fixed value for indication purposes only. This value is the maximum number of Service Users that can be stored in an IP Office system's security settings.
  - **Maximum Rights Groups:** *Default = 8.*
    This is a fixed value for indication purposes only. This value is the maximum number of Rights Groups that can be stored in an IP Office system's security settings.

- **System Discovery**
  System discovery is the processes used by IP Office applications to locate and list available IP Office systems. The IP Office can be disabled from responding to this process if required. If this is done, access to the IP Office requires its specific IP address to be used.
    - **TCP Discovery Active:** *Default = On.*
      TCP is the discovery method supported by Manager 5.2+ and IP Office 3.2+ systems. Selecting **TCP Discovery Active** allows the IP Office system to respond to those requests.
    - **UDP Discovery Active:** *Default = On.*
      UDP is the discovery method used by previous versions of Manager and by other IP Office applications. Selecting **UDP Discovery Active** allows the IP Office system to respond to those requests.
- **Security:** *Software level = 4.1+.*
  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 indicate 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 Level** is 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. For general information on security policy and application see Appendix: IP Office Secure Administration. 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.

Security | Unsecured Interfaces

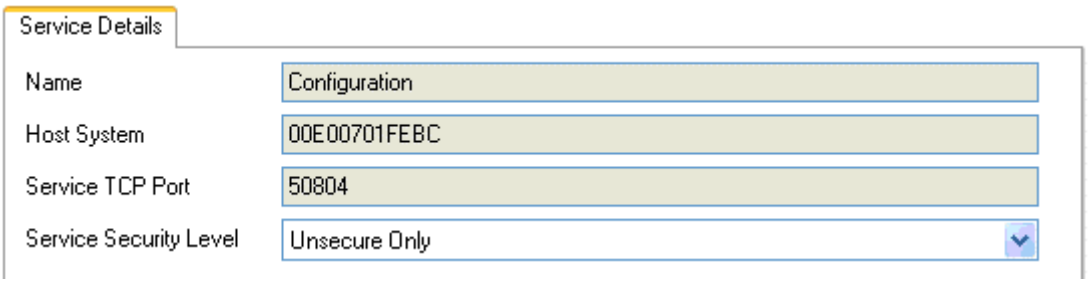
This tab is accessible when **System** is selected in the navigation pane. These features relate to IP Office applications that also access the IP Office configuration settings but still use the pre-IP Office 3.2 security methods. Currently this includes all 3.2+ applications except Manager and System Status Application.



- **System Password:** *Default = 'password', Range = 0 to 31 characters.*
  This password is required by some legacy applications such as Monitor and Call Status. It is also used for IP Office control unit software upgrades.
- **VM Pro Password:** *Default = '', Range = 0 to 31 characters.*
  This password is required if a matching password is also set through the Voicemail Pro client application. Typically no password is set.
- **Monitor Password:** *Default = '', Range = 0 to 31 characters.*
  This password, if set, is used by the IP Office Monitor and Call Status applications. If this password is not set, those applications use the system password.
- **Applications Controls:** *Default = All selected except TFTP Configuration Write.*
  These check boxes control which actions the IP Office will support for legacy applications. Different combinations are used by the different applications. A summary of the applications affected by changes is listed in the **Application Support** list.
- **Application Support**
  This panel is shown for information only. It indicates the effect on various IP Office applications of the **Application Controls** selections.

Security Services Settings

This tab is accessible when **Service** is selected in the navigation pane. It shows details of the services that the IP Office runs to which Service Users can communicate. Currently three services exist. The **Configuration** service is used for accessing IP Office configuration settings. The **Security Administration** service is used for accessing IP Office security settings. The System Status Interface service is used by the **System Status Application**.



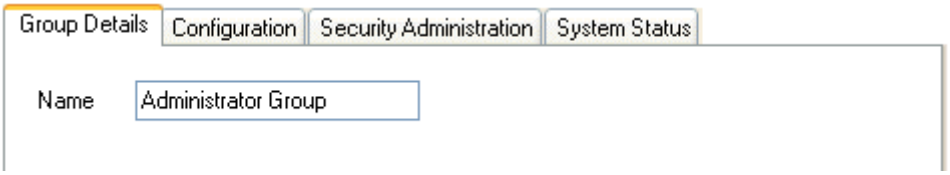
- **Name**
  The name of the service. This is a fixed value for indication purposes only.
- **Host System**
  This field shows the IP Office system's name. This is a fixed value for indication purposes only.
- **TCP Base Port**
  This is the TCP port on which the IP Office system listens for attempts to access the service. The routing of traffic to this port may need to be enabled on firewalls and network devices between the Service Users and the IP Office. The TCP Base Port for each service is offset by a fixed amount from the Base TCP Port set in **System Settings**.

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+

- **Service Security Level:** *Default = 'Unsecure Only', Software level = 4.1+.*
  Sets the minimum security level the service will support. See **File | Preferences | Security** for the corresponding Manager application setting, which must be changed to match the appropriate service access security settings. **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 while the IP Office generates a unique security certificate.
  - ***Unsecure Only***
    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). See **System Details | Client Certificate Checks** for tests made on the received certificate. The service's unsecured TCP port is disabled.

Rights Group | Group Details

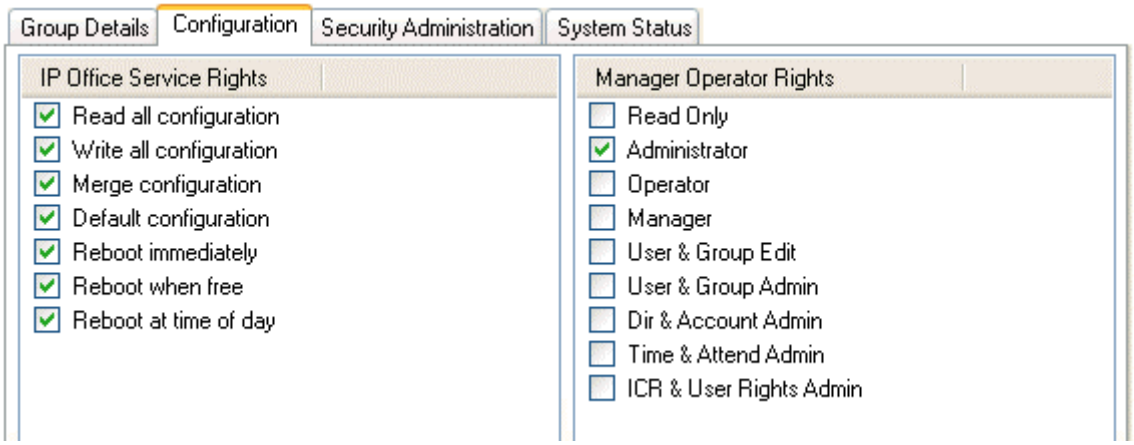
These settings are displayed when **Rights Groups** is selected in the navigation pane. This tab sets the name of the Rights Group.



- **Name:** *Range = Up to 31 characters*
  The name for the Rights Group should be unique.

Rights Group | Configuration

These settings are displayed when **Rights Groups** is selected in the navigation pane. This tab sets the configuration settings access for Service User's who are members of this Rights Group.

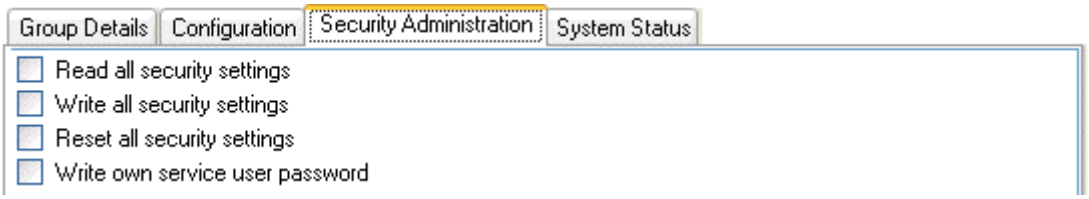


- **IP Office Service Rights**
  This setting controls what action on the IP Office system can be performed by members of the Rights Group.
- **Manager Operator Rights**
  This setting controls what types of configuration entries Manager will allow members of the Rights Group to viewed and what actions they can perform with those types of entries.

Operator	View/Edit/ New/Delete	Configuration Entry Types
Administrator	All	View, edit create and delete all configuration entries.
Manager	View	View all except **WAN Port**.
	Edit	**Extension**, **User**, **Hunt Group**, **Short Code**, **Service**, **RAS**, **Incoming Call Route**, **Directory**, **Time Profile**, **Firewall Profile**, **IP Route**, **Least Cost Route**, **Account Code**, **ARS, E911 System**.
	New	
	Delete	As edit except **Short Code**.
Operator	View	View all except **WAN Port**.
	Edit	**Extension, User**, **Hunt Group**, **Short Code**, **Service, RAS**, **Incoming Call Route**, **Time Profile**, **Firewall Profile**, **IP Route**, **Least Cost Route**, **Account Code**, **Licence, ARS**, **E911 System**.
	New	None.
	Delete	Delete **Incoming Call Route** and **Directory**.
User & Group Edit	View	**User** and **Hunt Group** entries only.
	Edit	
	New	None
	Delete	
User & Group Admin	All	**User** and **Hunt Group** entries only.
Dir & Account Admin	All	**Directory** and **Account Code** entries only.
Time & Attendant Admin	All	**Time Profile** and **Auto Attendant** entries only.
ICR & User Rights Admin	All	**Incoming Call Route** and **User Rights** entries only.
Read Only	View	View all configuration entries.
	Edit	None.
	New	
	Delete	

Rights Group | Security Administration

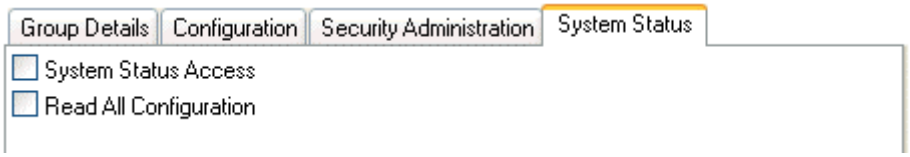
These settings are displayed when **Rights Groups** is selected in the navigation pane. This tab sets the security settings access for Service user's who are members of this Rights Group. These settings are ignored and greyed out if a **Unique Security Administrator** has been enabled in **General Settings**.



- **Read all security settings**
  Members of the Rights Group can view the IP Office system's security settings.
- **Write all security settings**
  Members of the Rights Group can edit and return changes to the IP Office system's security settings.
- **Reset all security settings**
  For systems prior to IP Office 4.1 this option was not used. For IP Office 4.1+, if selected, members of the Rights Group can reset the security settings to default values.
- **Write own service user password:** *Software level = 4.1+.*
  If selected, members of the Rights Group can change their own password. This option must be enabled if a **Password Change Period** is enabled on the **General Settings** tab.

Rights Group | System Status

These settings are displayed when **Rights Groups** is selected in the navigation pane. This tab sets whether members of the group can access the IP Office system using the IP Office System Status Application (SSA). That application is only supported by IP Office 4.0 and higher systems.

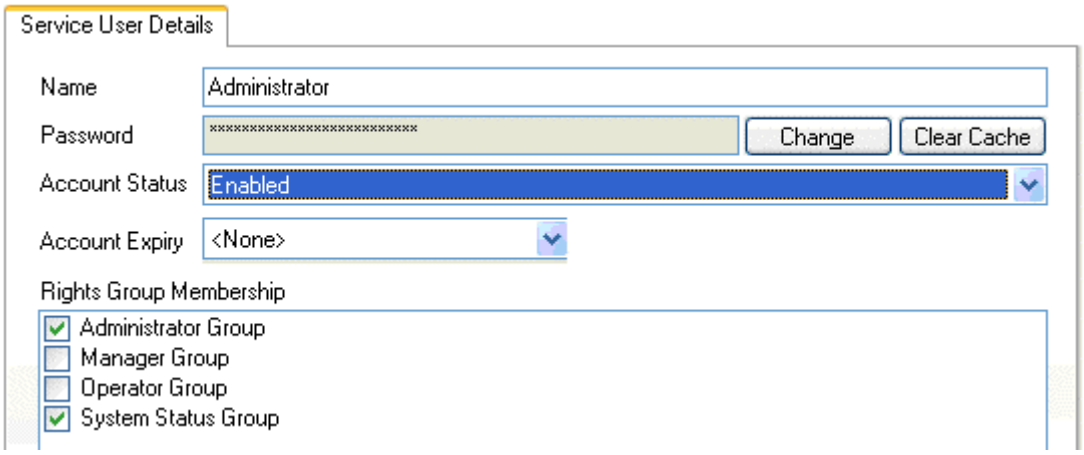


- **System Status Access**
  If selected, members of the Rights Group can view the IP Office system's current status and resources using the System Status Application (SSA).
- **Read all configuration**
  The System Status application includes tools to take a snapshot of the system for use by Avaya for diagnostics. That snapshot can include a full copy of the IP Offices configuration settings. This setting must be enabled for the SSA user to include a copy of the configuration in the snapshot.

Security Service User Settings

These settings are displayed when **Service Users** is selected in the navigation pane and a particular Service User is selected in the group pane.

Users can be created and deleted using the and icons at the top-right of the details pane. The maximum number of Service Users is 16.



- **Name:** *Range = Up to 31 characters.*
  Sets the Service User's name. The minimum name length is controlled through **General** settings.
- **Password:** *Range = Up to 31 characters.*
  Sets the Service User's password. The minimum password length and complexity is controlled through **General** settings.
- **Account Status:** *Default = 'Enabled', Software level = 4.1+.*
  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), Software level = 4.1+.*
  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.

- **Rights Group Membership**
  The check boxes are used to set the Rights Groups to which the user belongs. The user's rights will be a combination of the rights assigned to the groups to which they belong.

Menu Bar Commands

Menu Bar Commands

The commands available through the Manager's menu bar change according to whether Manager is running in configuration or security mode. Commands may also be grayed out if not useable.

The following sections outline the functions of each command. The **Edit** and **Help** menus are not included.

Configuration Mode

File Menu	View Menu	Tools Menu
Open Configuration...	Toolbars	Extension Renumber
Close Configuration	Navigation Pane	Line Renumber
Save Configuration	Group Pane	MSN Configuration
Save Configuration As	Details Pane	
Change Working Directory...	Error Pane	
Preferences	TFTP Log	
Offline | Create New Config		
Offline | Open File...		
Offline | Send Config...		
Offline | Receive Config...		
Advanced | Erase Configuration (Default)		
Advanced | Reboot		
Advanced | Upgrade..		
Advanced | Audit Trail...		
Advanced | Security Settings...		
Advanced | Erase Security Settings (Default)		
Advanced | System Status		
Advanced | LVM Greeting Utility		
Backup/Restore | Backup Binaries and Configurations		
Backup/Restore | Restore Binaries and Configurations		
Import/Export | Import		
Import/Export | Export		
Exit		

Security Mode

File	View
File | Open Security Settings	Toolbars
File | Close Security Settings	Navigation Pane
File | Save Security Settings	Group Pane
File | Reset Security Settings	Details Pane
File | Preferences	
File | Configuration	
File | Exit	

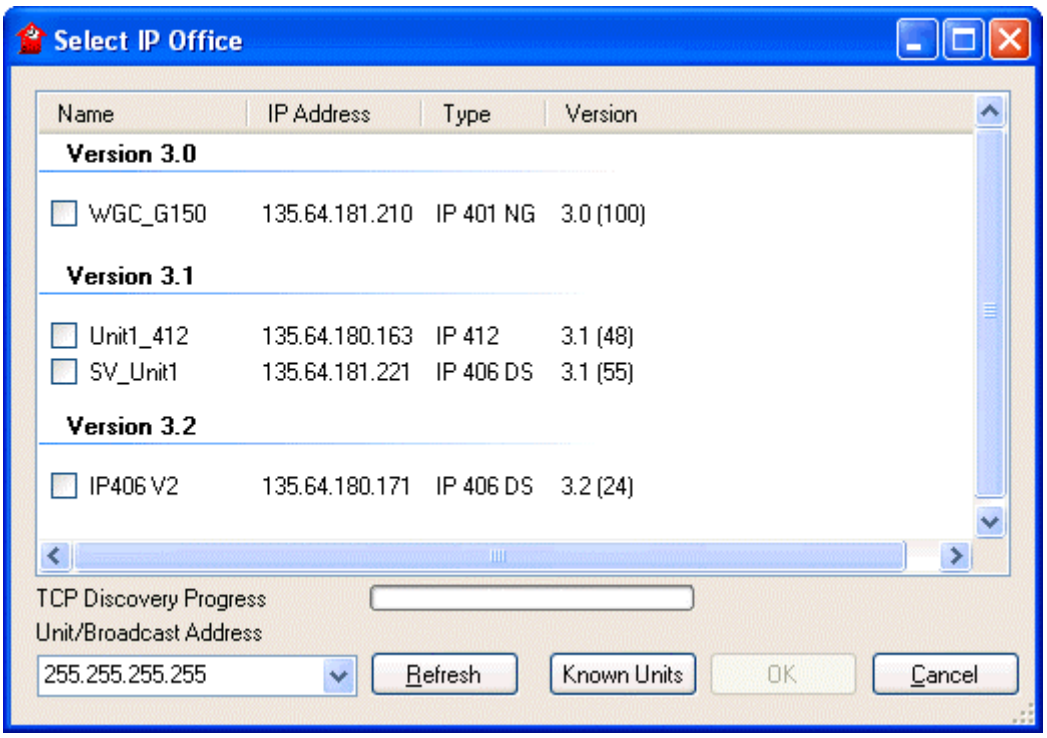
Configuration Mode

File Menu

File | Open Configuration

This command displays the Select IP Office menu used to receive an IP Office systems configuration settings. See **Loading a Configuration**.

The same action is performed by the icon in the Main Toolbar.



The Select IP Office menu is also used for other actions such as reboot and sending a configuration. If the unit required is not found, the **Unit/Broadcast Address** can be changed and then **Refresh** clicked. To change the TCP addresses scanned, select **File | Preferences | Discovery** and enter the required addresses in the **IP Search Criteria**.
Known Units is not available unless configured, see **Known IP Office Discovery**.

File | Close Configuration

This command closes the currently loaded configuration without saving it.

File | Save Configuration

The **File | Save** command saves the amended configuration.

If the configuration has been received from an IP Office, the **Send Config** menu is displayed. See **Sending a Configuration**.

If the configuration file has been opened offline or created from new, the file is saved to disk only.

File | Save Configuration As

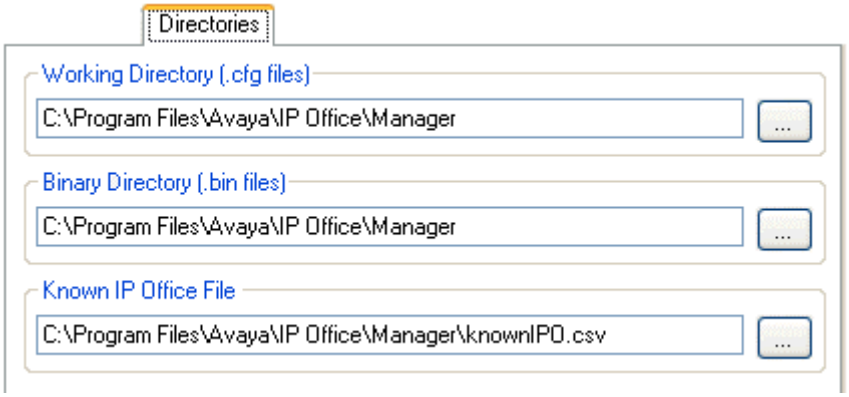
The **File | Save As** command allows you to save a configuration offline. The command displays the **Save File As** dialog box. You can enter the new file name, including the drive and directory.

Configurations saved onto the PC in this way can be reopened using the icon or the **File | Offline | Open File** command.

Note that dynamic configuration data, for example advertised hunt groups, is not included in a configuration file saved onto PC and then reopened.

File | Change Working Directory

This command allows you to change the default locations where Manager looks for and saves offline configuration (.cfg) files and IP Office equipment binary (.bin) files.



- **Working Directory (.cfg files)**
  Sets the directory into which Manager saves .cfg files. By default this is the Manager application's program directory.
- **Binary Directory (.bin files)**
  Sets the directory in which the Manager upgrade, TFTP and BOOTP functions look for .bin files. By default this is the Manager application's program directory.
- **Known IP Office File:** *Software level = 4.0 Q2 2007 maintenance release+.*
  Sets the file and directory into which Manager can record details of the IP Office systems it has discovered. Once a file location has been specified, a **Known Units** button becomes available on the discovery menu used for loading IP Office configuration. Pressing that button displays the known units file as a list from which the required IP Office system can be selected. It also allows sorting of the list and entries to be removed.

File | Preferences

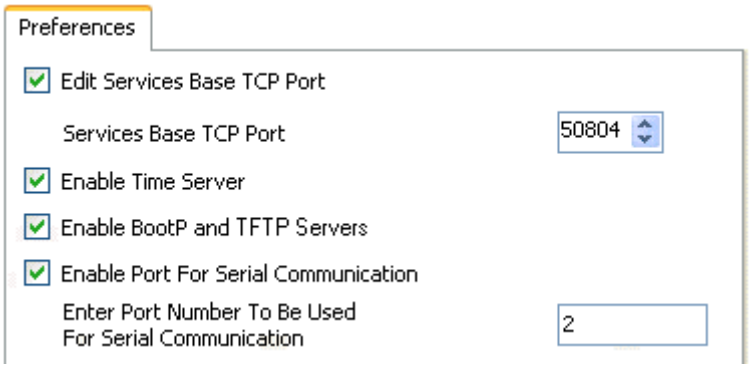
This command displays a menu for configuring various aspects of Manager's operation. The menu is divided into a number of tabs.

- **Preferences**
- **Directories**
- **Visual Preferences**
- **Discovery**
- **Validation**
- **Security**

Preferences | Preferences

This tab is accessed through **File | Preferences** and then selecting the **Preferences** sub-tab.

- Note: For IP Office Manager 6.1+, a number of option have been moved from this sub-tab to the **Security** sub-tab. Those options are **Request Login on Save**, **Close Configuration/Security Settings After Send**, **Save Configuration File After Load**, **Backup Files on Send**.

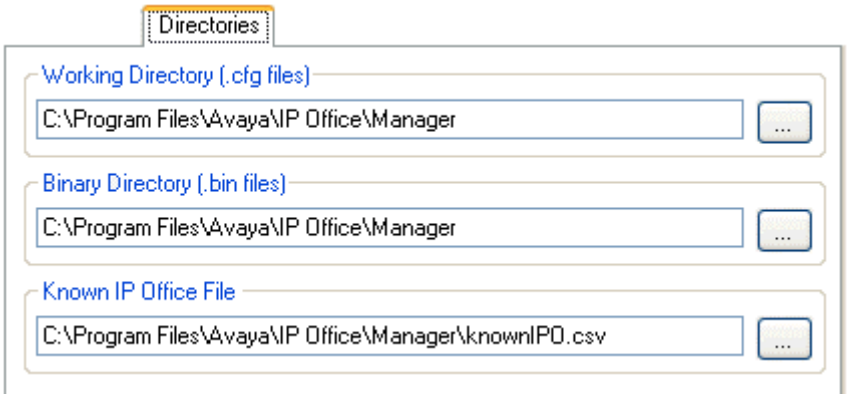


- **Edit Services Base TCP Port:** *Default = On.*
  This field shows or hides the Service Base TCP Port setting.
  - **Service Base TCP Port:** *Default = 50804*
    Access to the configuration and security settings on an IP Office 3.2+ system requires Manager to send its requests to specific ports. This setting allows the TCP Base Port used by Manager to be set to match the TCP Base Port setting of the IP Office system. The IP Office system's TCP Base Port is set through its security settings.
- **Enable Time Server:** *Default = On.*
  This setting allows Manager to respond to time requests from IP Office systems.
- **Enable BootP and TFTP Servers:** *Default = On.*
  This setting allows Manager to respond to BOOTP request from IP Office systems for which it also has a matching BOOTP entry. It also allows the IP Office to respond to TFTP requests for files. Note that IP Office Manager is not recommended as a permanent TFTP server.
- **Enable Port for Serial Communication**
  Not used. This is a legacy feature for some older control units that were managed via the serial port rather than the LAN.
  - **Enter Port Number to be used for Serial Communication**
    Used with the setting above to indicate which serial port Manager should use.

Preferences | Directories

This tab is accessed through **File | Preferences** and then selecting the **Directories** sub-tab.

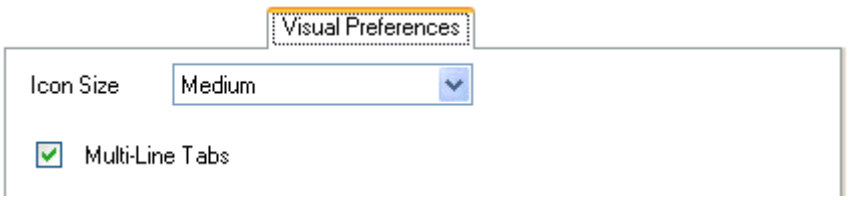
These fields set the default location where Manager will look for and save files. This tab is also accessed by the **File | Change Working Directory** command.



- **Working Directory (.cfg files)**
  Sets the directory into which Manager saves .cfg files. By default this is the Manager application's program directory.
- **Binary Directory (.bin files)**
  Sets the directory in which the Manager upgrade, TFTP and BOOTP functions look for .bin files. By default this is the Manager application's program directory. Note that in the Upgrade Wizard, right-clicking and selecting **Change Directory** also changes this setting.
- **Known IP Office File:** *Software level = 4.0 Q2 2007 maintenance release+.*
  Sets the file and directory into which Manager can record details of the IP Office systems it has discovered. Once a file location has been specified, a **Known Units** button becomes available on the discovery menu used for loading IP Office configuration. Pressing that button displays the known units file as a list from which the required IP Office system can be selected. It also allows sorting of the list and entries to be removed.

Preferences | Visual Preferences

This tab is accessed through **File | Preferences** and then selecting the **Visual Preferences** sub-tab.



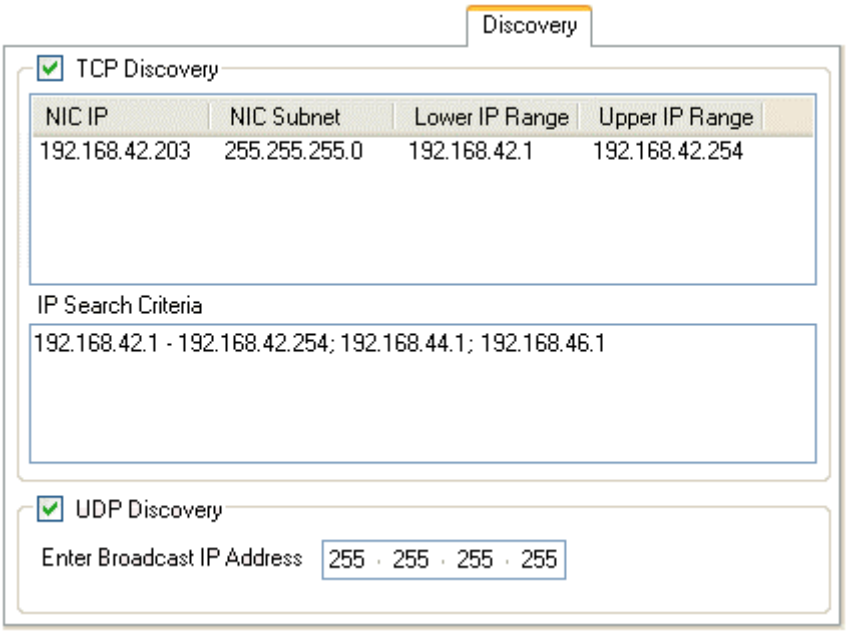
- **Icon size**
  Sets the size for the new look icons between ***Small***, ***Medium*** or ***Large***.
- **Multi-Line Tabs:** *Default = Off.*
  In the details pane, for entry types with more than two tabs, Manager can either use  buttons to scroll the tabs horizontally or arrange the tabs in multiple rows. This setting allows selection of which method Manager uses.

Preferences | Discovery

This tab is accessed through **File | Preferences** and then selecting the **Discovery** sub-tab.

When  is clicked, the **Select IP Office** form appears and Manager attempts to discovery any IP Office systems. Within Preferences, the **Discovery** tab sets the IP addresses and methods used for the discovery process.

By default IP Office 3.2 systems respond to both UDP and TCP discovery. Pre-3.2 IP Office systems only support UDP discovery.



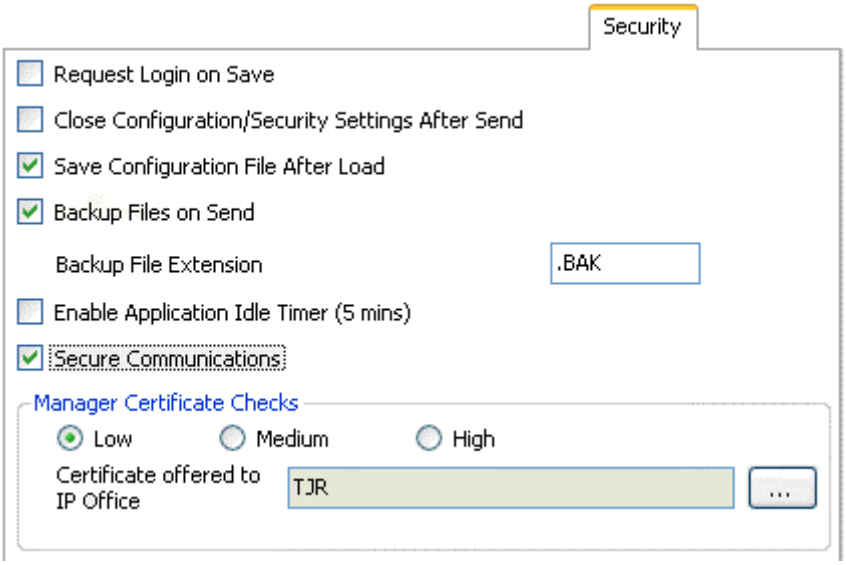
- **TCP Discovery:** *Default = On*
  This setting controls whether Manager uses TCP to discover IP Office systems. Only IP Office 3.2 and higher systems can respond to TCP discovery. The addresses used for TCP discovery are set through the **IP Search Criteria** field below.
  - **NIC IP/NIC Subnet**
    This area is for information only. It shows the IP address settings of the LAN network interface cards (NIC) in the PC running Manager. Double-click on a particular NIC to add the address range it is part of to the **IP Search Criteria**. Note that if the address of any of the Manager PC's NIC cards is changed, the Manager application should be closed and restarted.
  - **IP Search Criteria**
    This tab is used to enter TCP addresses to be used for the discovery process. Individual addresses can be entered separated by semi-colons, for example ***135.164.180.170; 135.164.180.175***. Address ranges can be specified using dashes, for example ***135.64.180.170 - 135.64.180.175***.
- **UDP Discovery:** *Default = On*
  This settings controls whether Manager uses UDP to discover IP Office systems. Pre-3.2 IP Office systems only respond to UDP discovery. By default IP Office 3.2 and higher systems also respond to UDP discovery but that can be disabled through the IP Office system's security settings.
  - **Enter Broadcast IP Address:** *Default = 255.255.255.255*
    The broadcast IP address range that Manager should used during UDP discovery. Since UDP broadcast is not routable, it will not locate IP Office systems that are on different subnets from the Manager PC unless a specific address is entered.

Preferences | Security

This tab is accessed through **File | Preferences** and then selecting the **Security** sub-tab.

Controls the various security settings of Manager. To control the security settings of the IP Office, see **Security Mode**.

All settings except Secure Communications can only be changed when a configuration has been opened using a user name and password with Administrator rights or security administration rights.



- **Request Login on Save:** *Default = On*
  By default a valid user name and password is required to receive a configuration from an IP Office and also to send that same configuration back to the IP Office. Deselecting this setting allows Manager to send the configuration back without having to renter user name and password details. This does not apply to a configuration that has been saved on PC and then reopened. 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.
- **Close Configuration/Security Settings After Send:** *Default = On.*
  When selected, the open configuration file or security settings are closed after being sent back to the IP Office system.
- **Save Configuration File After Load:** *Default = On.*
  When selected, a copy of the configuration is saved on the Manager PC when the configuration is received from the IP Office. The copy is given the IP Office system name followed by .cfg. The saved location is set by the Working Directory setting on the preferences Directories tab (see below). 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.
- **Backup Files on Send:** *Default = On.*
  When selected, whenever a copy of the configuration is saved, if an configuration of that name already exists, the existing file is renamed using the suffix set below. The date and a version number is also added to the backup file name. 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.
- **Backup File Extension:** *Default = .BAK*
  Sets the file extension to use for backup copies of system configurations generated by the **Backup Files on Send** option above.
- **Enable Application Idle Timer (5 minutes):** *Default = Off, Software level = 4.1+.*
  When enabled, no keyboard or mouse activity for 5 minutes will cause the Manager to grey out the application and re-request the current service user password. 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.

- **Secure Communications:** *Default = Off, Software level = 4.1+.*
  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 Office's 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. See Security Administration.
  - When Secure Communications set to On, a  padlock icon is displayed at all times in the lower right Manager status field.
- **Manager Certificate Checks:** *Software level = 4.1+.*
  When the **Secure Communications** option above 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 previously 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 cause 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. Use the Set button to change the selected certificate. Any certificate selected must have an associated private key held within the store:
    - Select from Current User certificate store - Display certificates currently in the currently logged-in user store.
    - Select from Local Machine certificate store.
    - Remove Selection – do not offer a Manager certificate.

Security – Registry Settings

- **WARNING: Changing Windows Registry Settings**
  Avaya accept no liability for any issues arising from the editing of a PC's registry settings. If you are in any doubt about how to perform this process you should not proceed. It is your responsibility to ensure that the registry is correctly backed up before any changes are made.

NOTE: Before manually editing any registry entry, the following Microsoft support articles should be read:

- http://support.microsoft.com/kb/256986
- http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/regedit_permit_key.mspx

Manager stores it's security preferences in the Windows Registry. The following key affects manager security operation; it's values may only be changed by a configuration or security administrator:

- HKEY_CURRENT_USER\Software\Avaya\IP400\Manager\Security\

In order to prevent circumvention by manual editing of the Windows Registry, Regedt32.exe, the native registry editor, allows an operator user (with Full Control permissions) to edit permissions on a per key basis.

To prevent a user from manually editing the security preferences, the HKEY_USERS\User GUID\Software\Avaya\IP400\Manager\Security key permission should be set to 'Read' only for that user. Ensure that all child object permissions are replaced as well by using the 'Advanced' button.

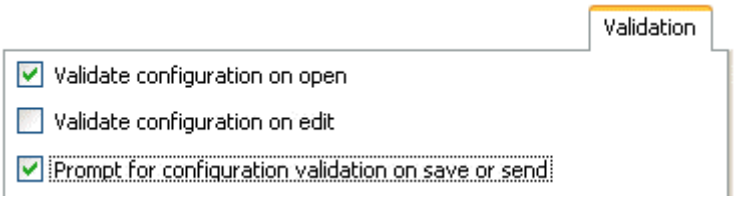
To allows the security policy of all local PC users to be fixed, a set of values in the key HKEY_CURRENT_USER\Software\Avaya\IP400\Manager\Security\ may be created. This is tested and used in preference to any value found under HKEY_CURRENT_USER\Software\Avaya\IP400\Manager\Security\.

This key is not created by the manager application.

Preferences | Validation

This tab is accessed through **File | Preferences** and then selecting the **Validation** sub-tab.

By default Manager validates the whole configuration when it is loaded and individual fields whenever they are edited. This tab allows selection of when automatic validation should be applied to configuration files loaded into Manager.



- **Validate configuration on open**
  Automatically validate configuration files when they are opened in Manager.
- **Validate configuration on edit**
  Validate the whole configuration when OK is clicked after editing a record. For large configurations, disabling this option removes the delay caused by revalidating the configuration after every edit.
- **Prompt for configuration validation on save or send**
  If selected, when saving or sending a configuration, a prompt is displayed asking whether the configuration should be validated. If validation is selected and error are found, the send or save process is cancelled. This option is disabled if **Validate configuration on edit** is selected.

File | Offline | Create New Config

This command starts a dialog that allows you to create a default offline configuration by specifying the system locales, the type of IP Office control unit and expansion modules and the trunk cards fitted. See **Creating a New Configuration**.

The same action is performed by the icon in the Main Toolbar.

File | Offline | Open File

This command allows a configuration file stored on PC to be opened in Manager.

File | Offline | Send Config

This command is used to send an offline configuration to an IP Office system. See **Sending a Configuration**.

File | Offline | Receive Config

This command displays the Select IP Office menu used to receive an IP Office systems configuration settings. See **Loading a Configuration**.

Once the configuration has been received, you are prompted to save it on the PC.

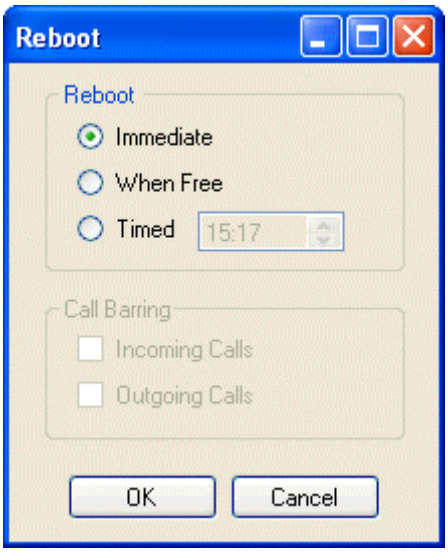
File | Advanced | Erase Configuration (Default)

This command returns the configuration settings of an IP Office system back to their default values. This action does not affect the IP Office system's security settings or audit trail record.

When this command is used, the **Select IP Office** menu is displayed. Once an IP Office system is selected, a valid user name and password are required to complete the action.

File | Advanced | Reboot

When this command is used, the **Select IP Office** menu is displayed. Once an IP Office system is selected, a valid user name and password are required. The type of reboot can then be selected.

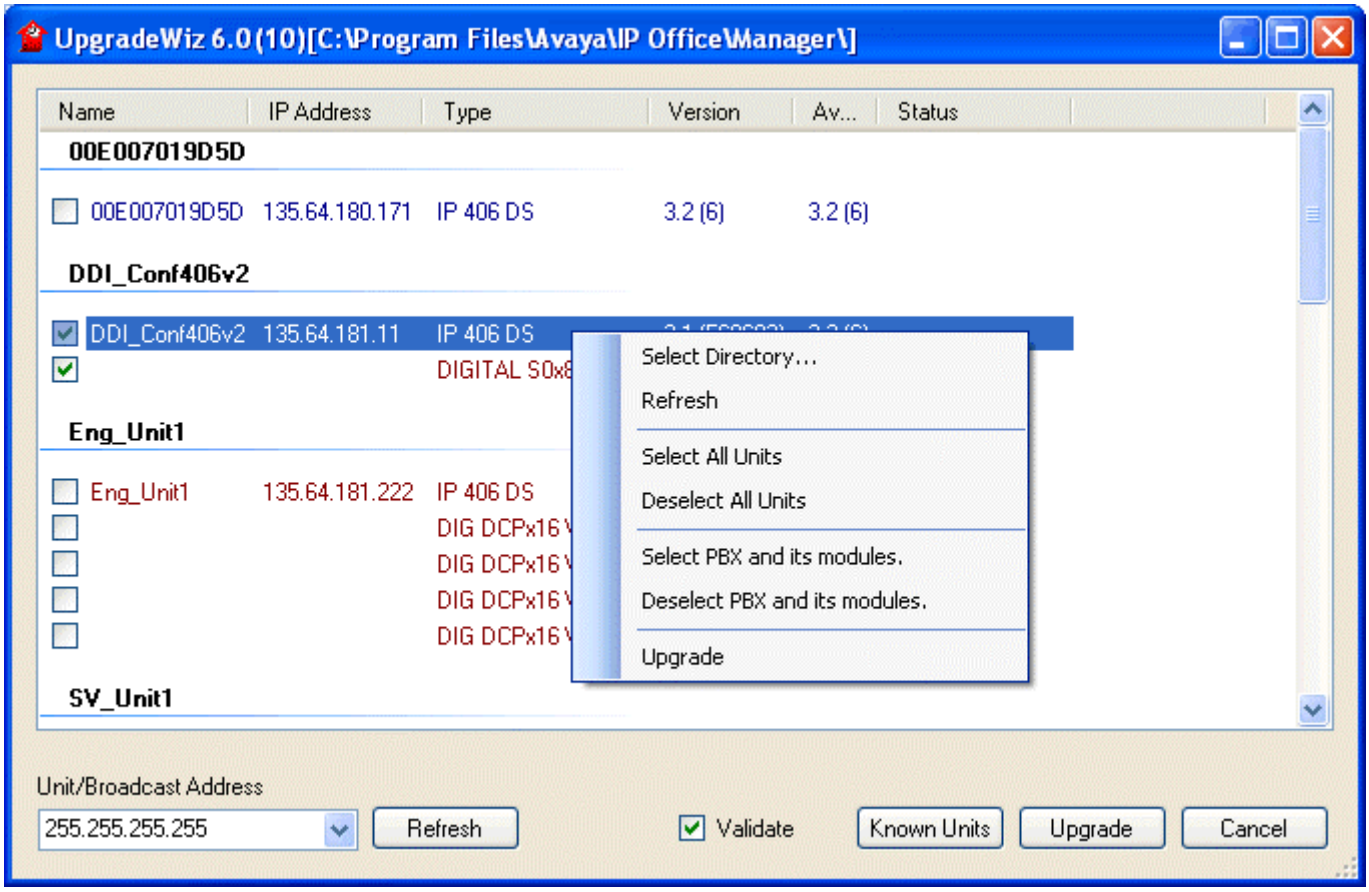


File | Advanced | Upgrade

This command starts the Upgrade Wizard tool. This tool is used to compare the software level of the control unit and expansion modules within IP Office systems against the software level of the .bin binary files Manager has available. The Upgrade Wizard can then be used to select which units to upgrade.

⚠WARNING

- Incorrect use of the upgrade command can halt IP Office operation and render units in the system unusable. You must refer to the IP Office Technical Bulletins for a specific release for full details of performing software upgrades to that release.
- Performing any other actions on a system during an upgrade or closing the upgrade wizard and Manager during an upgrade may render systems unusable.
- During an upgrade the IP Office system may restrict calls and services. It will reboot and disconnect all current calls and services.
- The **Validate** option must remain selected wherever possible. Use of unvalidated upgrades is subject to a number of conditions outlined in the IP Office Installation Manual and Technical Bulletins.



The list area shows details of IP Office systems found by the Upgrade Wizard. The **Version** column details the current software each unit in the systems is running whilst the **Available** column shows the version of .bin file Manager has available for that type of unit (a – indicates no file available).

The check boxes are used to select which units should be upgraded. Upgrading will require entry of a valid name and password for the selected IP Office system.

The **Validate** option should remain selected wherever possible. When selected, the upgrade process is divided as follows: transfer new software, confirm transfer, delete old software, restart with new software. If **Validate** is not selected, the old software is deleted before the new software is transferred.

Sorting the List

1. To sort list of IP Office systems click on the Name or IP Address column headings.

Search for Particular Systems

The default address used by the Upgrade Wizard is the address shown in the Manager title bar, which is selected through **File | Preferences**. If the unit required is not found, the address used can be changed.

1. Enter or select the required address in the **Unit/Broadcast Address** field.
2. Click **Refresh** to perform a new search.

Changing the .bin File Directory Used

The directory in which the Upgrade Wizard looks for .bin files is set through Manager's **Binary Directory** setting. This can be changed using **Files | Change Working Directory** or **File | Preferences | Directories**. It can also be changed directly from the Upgrade Wizard as follows.

1. Right-click on the list area.
2. Select **Select Directory**.
3. Browse to and highlight the folder containing the .bin files. Click **OK**.
4. The list in the **Available** column will be updated to show the .bin files in the selected directory that match IP Office units or modules listed.

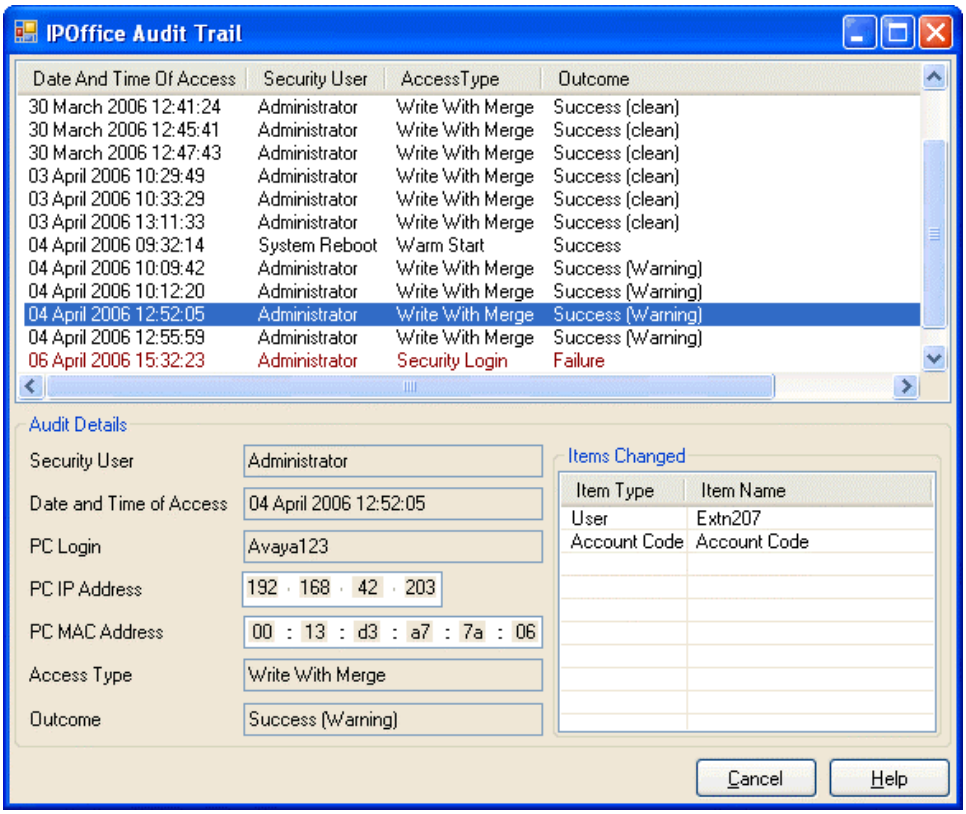
File | Advanced | Audit Trail

The audit trail lists the last 16 actions performed on the system from which the configuration loaded into Manager was received. It includes actions by Service Users such as getting the configuration, sending a configuration back, reboots, upgrades and default the system. The audit trail is not available for systems running pre-3.2 IP Office software.

For IP Office 4.1+ systems, audit trail events can be output to a Syslog server through the IP Office's System | System Events settings.

The last failed action is always recorded and shown in red. It is kept even if there have been 16 subsequent successful actions.

- Note: The Audit Trail is part of the IP Office configuration file received from the IP Office system. If the configuration is kept open between send and reboot operations (ie. if **Close Configuration/Security Setting After Send** is not selected), the Audit Trail will not show details of those operations. It will only show details of operations since the configuration was received if the configuration is closed and then a new copy of the configuration is received from the IP Office.



- **Audit Details**
  When a specific access event is selected from the list, the following information is shown in the Audit Details section:
  - The **Security User** shows the service user name used for the access action.
  - The **Data and Time of Access** indicate the local IP Office time when the recorded event occurred.
  - The **PC Login** is the computer name of the PC used for the access.
  - The **PC IP Address** and **PC MAC Address** are the IP address and MAC address of the PC used for access.
  - The **Access Type** details the type of action that was performed.
  - The Outcome shows the IP Office's response to the access. The outcome **Success (Warning)** refers to the sending of a configuration that contains fields marked as errors or warnings by Manager's validation function. **Success (Clean)** refers to the sending of a configuration that does not contain any validation errors or warnings.
- **Items Changed**
  The **Items Changed** area summarizes the changes contained in a sent configuration. Where changes to a single entry of a particular type are made, the Item Name field lists the individual entry changed. Where changes are made to several entries of the same type, the **Item Name** field displays ***Multiple items***.

File | Advanced | Security Settings

This command is used to switch the Manager application to security mode. In that mode, Manager is used to edit the security settings of an IP Office system (3.2 or higher only). Refer to the section **Security Mode**.

File | Advanced | Erase Security Settings (Default)

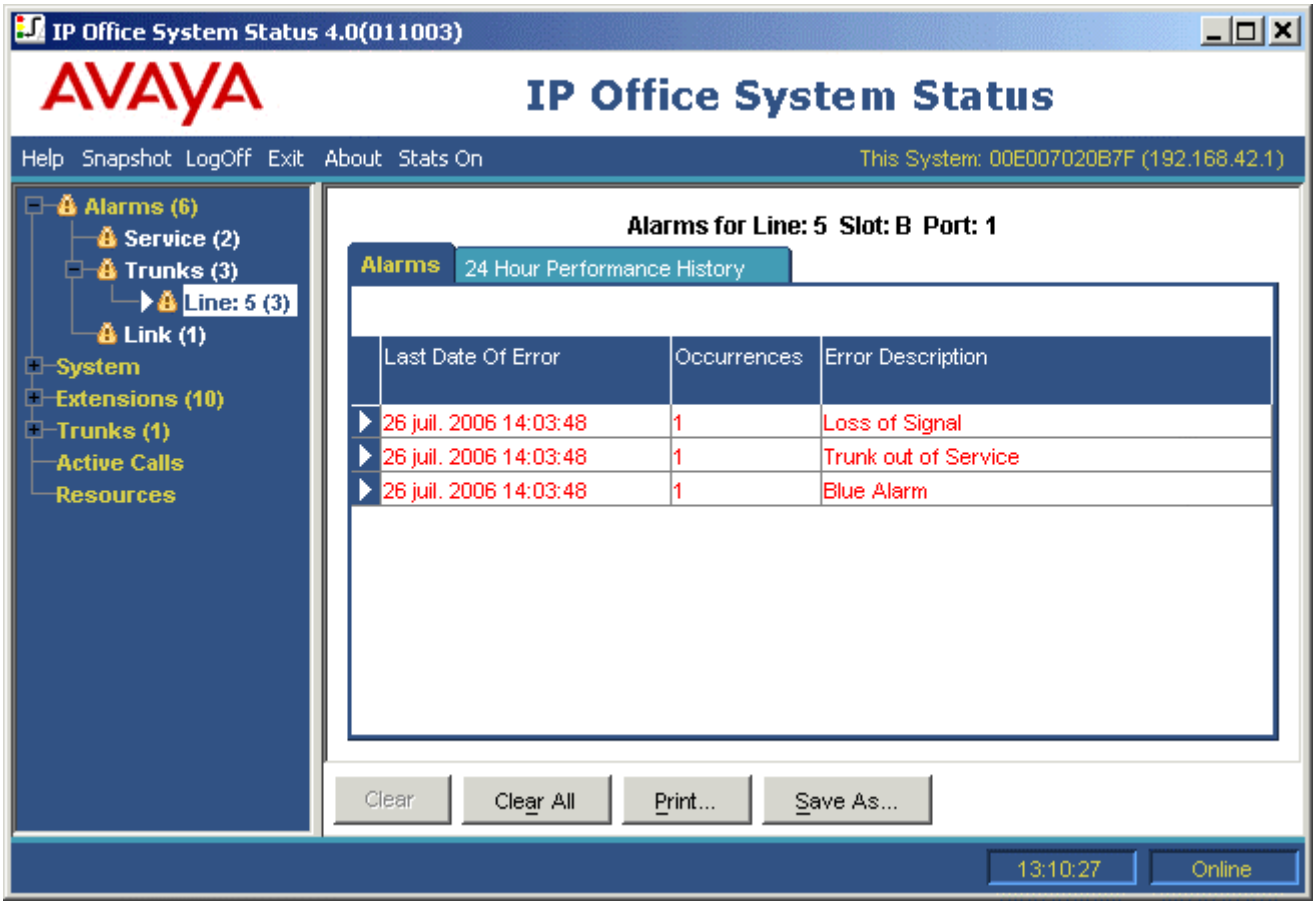
Added in IP Office Manager 6.1 and supported for IP Office 4.1+ systems.

This command returns the security settings of an IP Office system back to their default values. This action does not affect the IP Office system's configuration or audit trail record.

When this command is used, the Select IP Office menu is displayed. Once an IP Office system is selected, a valid user name and password are required to complete the action.

Advanced | System Status

IP Office System Status is an application that can be used to monitor and report on the status of an IP Office system. This application is supported by IP Office systems running IP Office 4.0 or higher.



This is a separate application from IP Office Manager but if installed on the same PC, it can be started using the **File | Advanced | System Status** link within Manager. Use of the application requires a service user name and password configured on the IP Office system for **System Status Access** within the IP Office's security settings.

File | Backup/Restore | Backup Binaries and Configurations

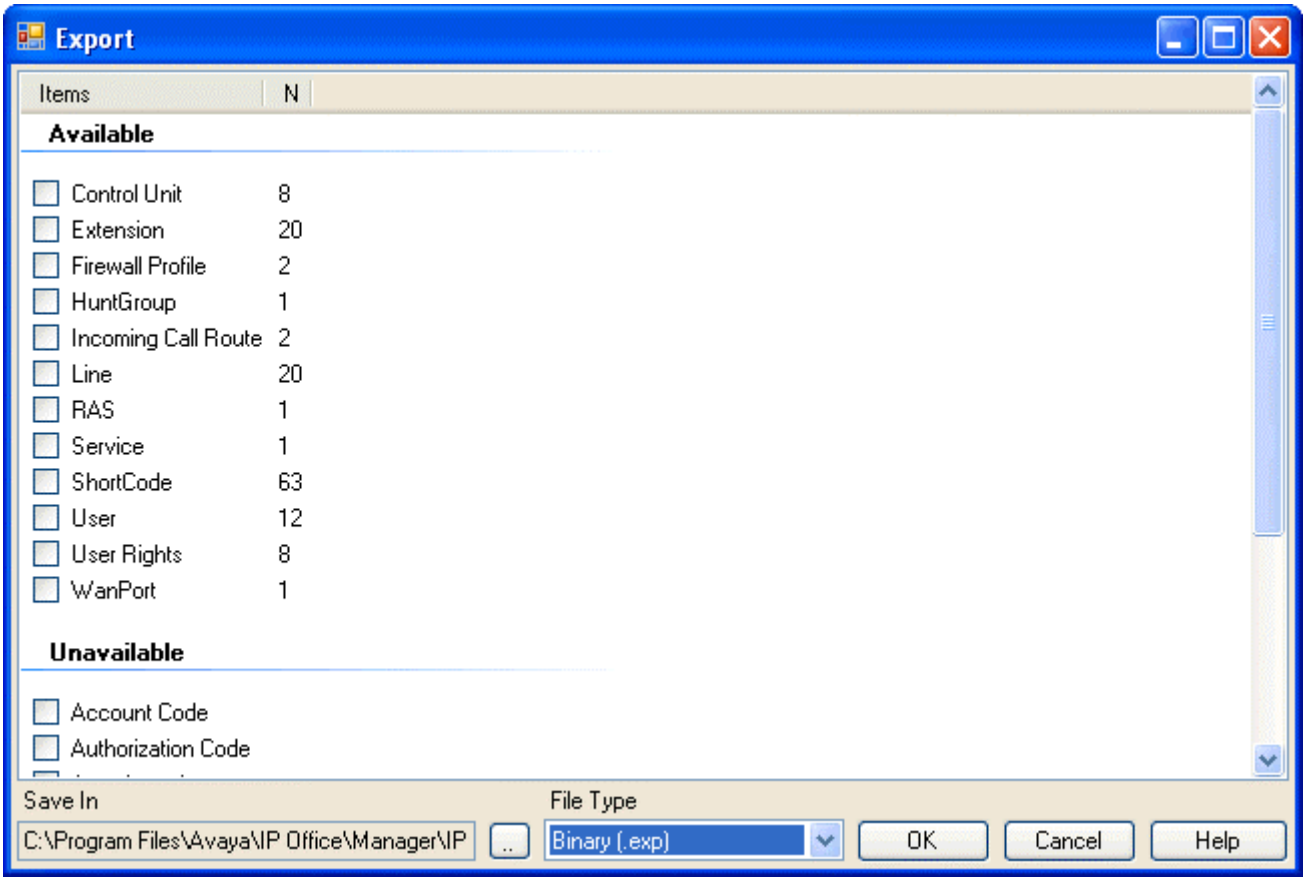
This command copies of all configuration files (***.cfg***) and software files (***.bin***) stored in Manager's working directory to a selected folder.

File | Backup/Restore | Restore Binaries and Configurations

This command copies all configuration files (***.cfg***) and software files (***.bin***) stored in a selected folder to the Manager's working directory.

File | Import/Export | Export

This command allows you to export the selected parts of the configuration to either a set of CSV text files (.csv) or a single binary file (.exp). See Importing and Exporting Settings.

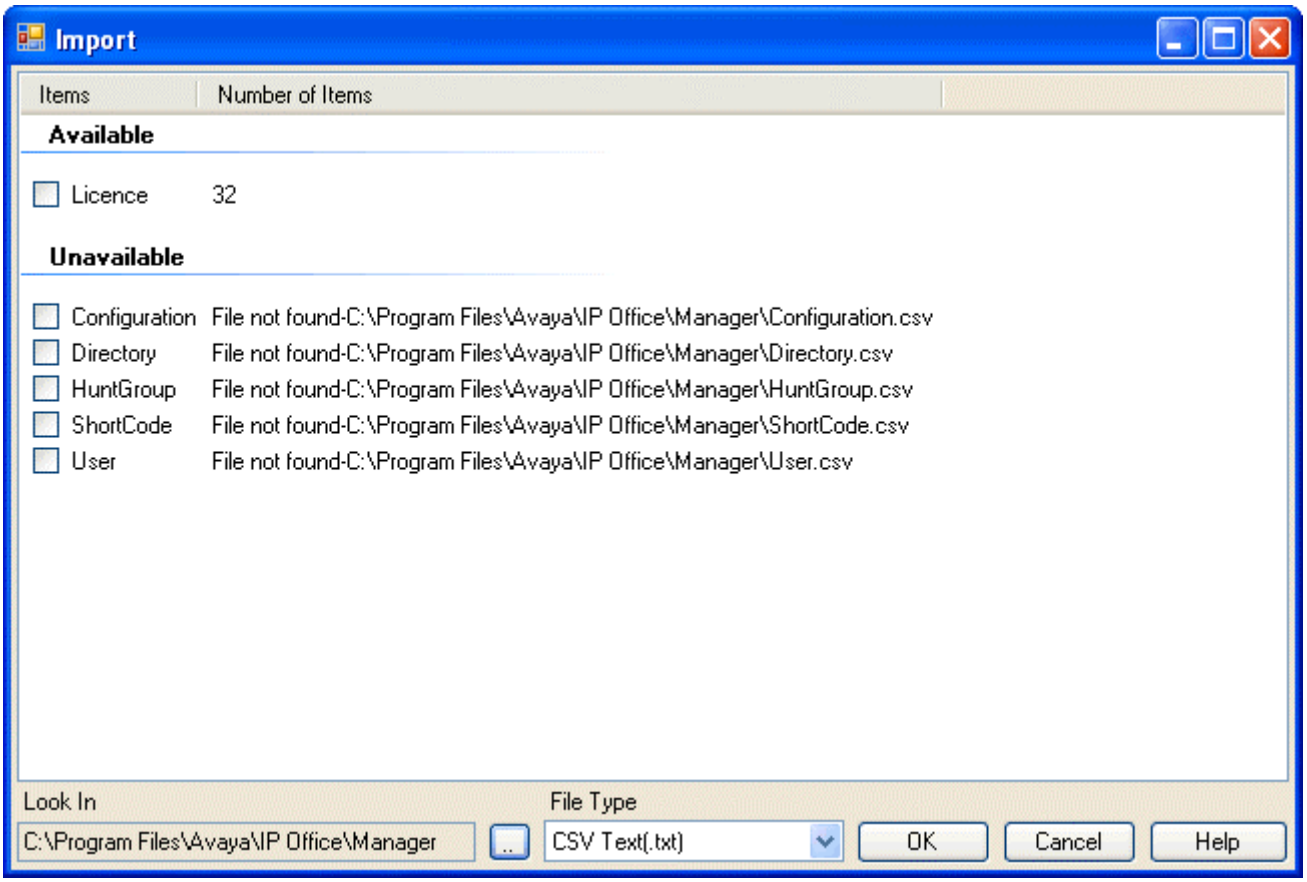


The display shows those exportable entry types for which the configuration contains entries. The **File Type** and the **Save In** path can be selected at the base. The default location used is sub-directory of the Manager application directory based on system name of the currently loaded IP Office system.

Manager imports and exports CSV files using UTF8 character encoding which uses a double byte to support characters with diacritic marks such as ä. Other applications such as Excel, depending on the user PC settings, may use different single-byte encoding which will cause such characters to be removed. Care should be taken to ensure that any tool used to create or edit a CSV supports all the characters expected and is compatible with UTF8.

File | Import/Export | Import

This command allows you to import configuration settings. Two formats are supported. Binary files (.exp) are settings previously exported from an IP Office system using **File | Import /Export | Export**. CSV text files (.csv) can also be exported from an IP Office system or can be created using a plain text editor. See Importing and Exporting Settings.



For the selected **File Type** and the **Look In** path, the window displays the file or files found. The default location used is sub-directory of the Manager application directory based on system name of the currently loaded IP Office system.

Manager imports and exports CSV files using UTF8 character encoding which uses a double byte to support characters with diacritic marks such as ä. Other applications such as Excel, depending on the user PC settings, may use different single-byte encoding which will cause such characters to be removed. Care should be taken to ensure that any tool used to create or edit a CSV supports all the characters expected and is compatible with UTF8.

File | Exit

The **File | Exit** command exits the Manager application.

View

View | Toolbars

This command allows selection of which toolbars should be shown or hidden in configuration mode. A tick mark is displayed next to the name of those toolbars that are currently shown.

View | Navigation Pane

This command shows or hides the Navigation Pane. A tick mark appears next to the command when the pane is shown.

View | Group Pane

This command shows or hides the Group Pane. A tick mark appears next to the command when the pane is shown.

View | Details Pane

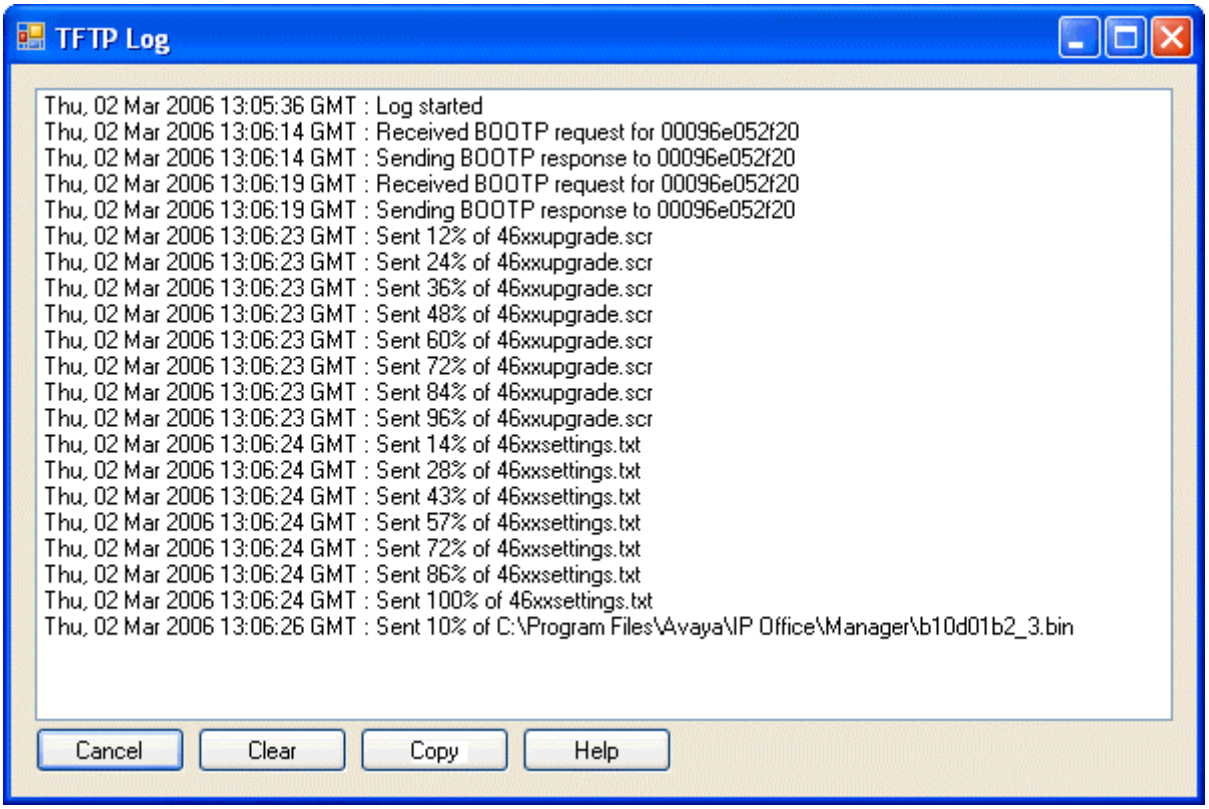
This command set the location of the Details Pane when the Group Pane is also shown. The Details Pane can be placed either below or to the right of the Group Pane.

View | Error Pane

This command shows or hides the Error Pane. A tick mark appears next to the command when the pane is shown.

View | TFTP Log

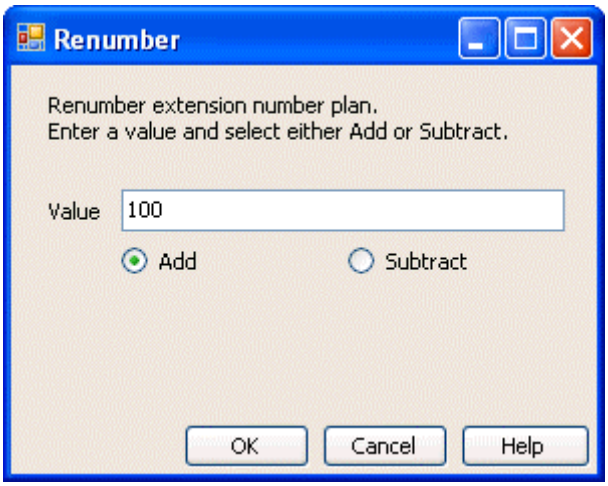
This command displays the TFTP Log window. This window shows TFTP traffic between Manager and devices that uses TFTP to send and receive files. For example, the TFTP Log below shows an Avaya IP phone requesting and then being sent its software files.



Tools Menu

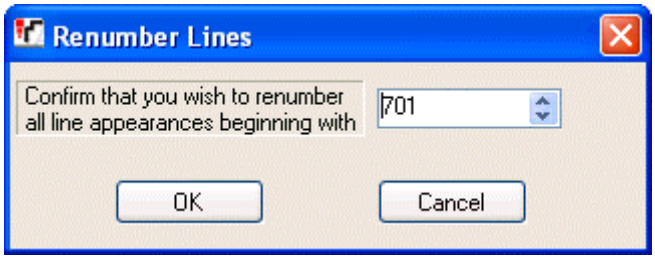
Tools | Extensions Renumber

This command allows the extension numbering of user extensions to be raised or lowered by a specified amount. The command does not alter the extension number used for hunt groups but does adjust the extension numbers of hunt group members.



Line Renumber

On external trunks Line appearance ID numbers can be assigned to each channel supported in order to allow that channel or line to be associated with a Line Appearance button on phones that support button programming. By default all lines are automatically numbered from 701 upwards when added to the IP Office system. This command allows the lines to be renumbered from a different starting point.



Busy on Held Validation

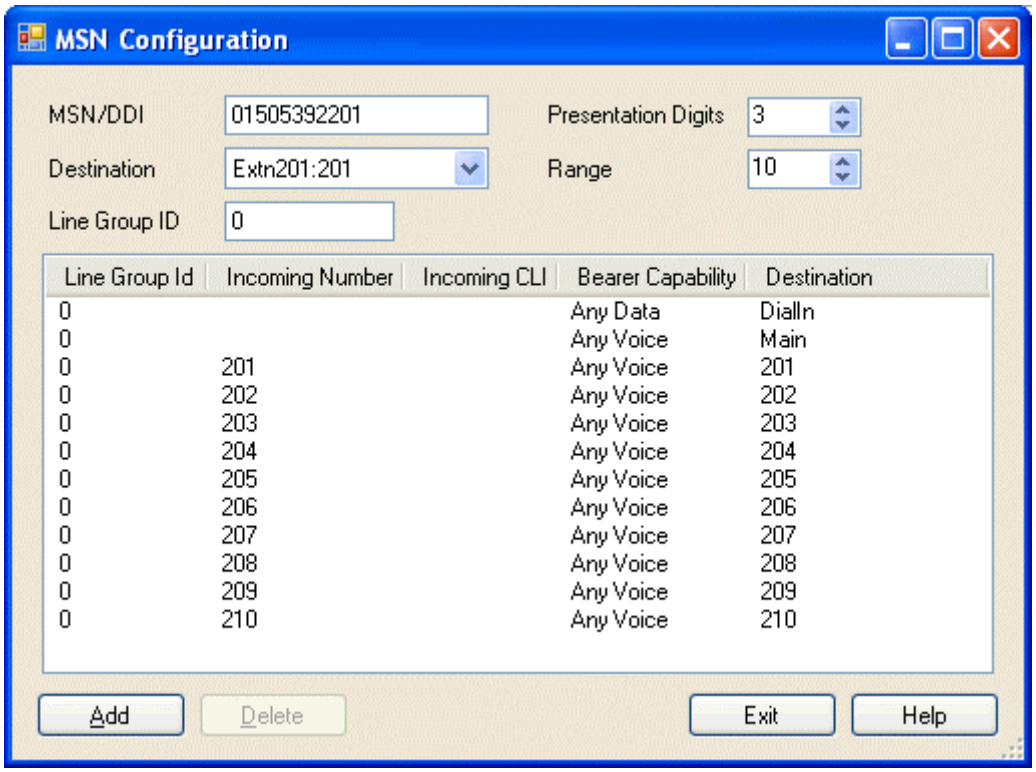
Busy on Held is a user feature where, when the user has a call on hold, the system indicate the user as being busy to any further calls.

The use of **Busy on Held** in conjunction with multiple call appearance buttons is deprecated. This command can be used to identify those users who have multiple call appearance buttons and for whom Busy on Held is currently set.

When run, it shows a list of the users affected and if selected their Busy on Held setting will be switched off.

MSN Configuration

This menu can be used to populate the **Incoming Call Route** table with a range of MSN or DID numbers.



In the example above, the customer has ten DID numbers starting at 01505392201 with the central office exchange passing through 3 digits for each. Having selected the number of presentation digits (3), set the range (10) and selected the first destination (201); clicking **Add** created the ten incoming call routes (201 to 210).

Settings

- **MSN/DID**
  The first number in the set of MSN numbers for which you have subscribed. Note: If you require to find an exact match between the MSN numbers and the destination numbers, enter a minus (-) sign before the first MSN number.
- **Destination**
  Where incoming calls with matching digits should be routed. The drop-down list contains the extensions and groups on the IP Office system.
- **Line Group ID**
  Specifies the incoming line group ID of the trunks to which the DID routing is applied.
- **Presentation Digits**
  Set to match the number of digits from the MSN number that the central office exchange will actually present to the IP Office system.
- **Range**
  How many MSN or DID number routes to create in sequence using the selected MSN/DID and Destination as start points. Only routing to user extensions is supported when creating a range of entries.
- **Add**
  Adds the appropriate entries to the Incoming Call Route table using the value entered above.
- **Delete**
  Removes a specific entry.

File | Advanced | LVM Greeting Utility

This command launches a utility that can be used to convert ***.wav*** files to the formats used by embedded voicemail (***.c711*** for Small Office Edition and ***.c723*** for others). The source file must be in the standard format used for all IP Office applications: PCM, 8kHz 16-bit, mono.

The resulting named greeting files can then be transferred to the embedded voicemail memory card and selected as auto attendant greetings in the **Recording Name** field on the **Auto Attendant | Auto Attendant** tab. The same named greeting file can be used in several auto attendants.

The utility can be run separately using the file ***LVMGreeting.exe*** found in the **LVMGreeting** sub-folder of the Manager application.

Security Mode

File | Open Security Settings

This command displays the **Select IP Office** menu to select and load a system's security settings. This requires entry of a user name and password with rights to access security settings of the selected system.

This behavior changes when configuration settings have already be received from a system using a Service User name and password that also has security access rights for that system. In that case, the system's security settings are automatically loaded without requiring name and password entry.

File | Close Security Settings

Close the currently open set of security settings received from an IP Office system without saving those settings.

File | Save Security Settings

Send edited security settings back to the IP Office. Requires re-entry of a Service User name and password with access rights for security settings.

File | Reset Security Settings

Added in IP Office Manager 6.1 and supported for IP Office 4.1+ systems.

Reset the security settings of the selected IP Office to defaults. Requires entry of a Service User name and password with access rights for resetting the security settings. This option is not useable while a set of security configuration settings is loaded.

The command **File | Advanced | Erase Security Settings (Default)** performs the same action from IP Office Manager configuration mode.

File | Preferences

See **Preferences** in the **Menu Bar Commands | Configuration Mode | File Menu section**.

File | Configuration

This command returns the Manager application to configuration mode.

File | Exit

This command closes Manager.

Index

10
  account, 107
16-bit High Color, 25
200MB
  Manager, 25
20DT Analog DECT, 17
255.255.255.255
  UDP Broadcast, 30
256KB, 73
256MB, 25
3.2
  having, 30
3DES, 97, 114
600MB, 25
600MHz Pentium, 25
64-bit, 25
800MB, 25
800MHz Pentium, 25
802.11a, 15
802.11b, 15
802.11g, 15
8kHz 16-bit, 141
96dpi, 25
access
  Configuring, 42
  IP Office, 30, 42, 54, 76, 92, 97, 107, 110, 113, 114, 118
  IP Office 3.2, 30, 54, 92
  IP Office 3.2 Configuration, 30
  IP Office 4.1, 30
  Service, 117
  Service User's, 116
  Time, 134
Access Control, 97
Access Denied, 76, 88, 104
Access Type, 134
according, 110
  Client Certificate Checks, 110
account, 76, 107
  10, 107
  Service User, 76
Account Admin, 54, 92, 116
Account Code, 44, 49, 54, 72, 73, 92, 116
Account Expiry, 76, 107, 119
  passing, 119
  resetting, 119
Account Idle Time, 107, 119
  set, 119
Account Locked, 76
Account Status, 119
account', 97
Adding, 17, 25, 43, 62, 65, 140
  clicking, 140
  IP Office, 43
  IP500 Upgrade Standard, 17
  Manager Start Dialogue, 25
  New Entry, 62, 65
Additional B-channels, 9
Additional Channels, 9
Addressing, 74
administrating, 97
  IP Office 4.1, 97
Administration | Preferences, 9
Administrator Rights Group, 42
  belonging, 42
Advanced, 51, 90, 91, 95, 104, 131, 132, 134, 135
Advanced | Erase Security Settings, 121
Advanced Networking License, 17
Advanced Small Community Networking, 17
Advanced' button, 127
Advertised Hunt Groups, 17
AES-128, 97
AES-256, 97
affect
  IP Office, 131, 135
Afternoon, 48
Agent Status on No Answer, 17
AIM, 9, 15, 39, 40, 42, 43, 76
  IP Office, 39
  Refer, 39, 40
AIM Applications, 39, 40
AIM Network Management Console, 39, 40
AIM NMC, 39, 44
AIM Provisioning, 40
AIM Secure Access Administration, 40
AIM Secure Admin Access, 42
AIM Software Update Manager, 39, 40
AIMAdmin, 42
All, 67
All Network Alchemy, 17
All Programs, 28
allocating, 90
  IP, 90
Allow, 48
  WAV file, 48
Altering, 58, 68
  Configuration Interface, 68
  Toolbars, 58
AMD Athlon XP, 25
AMD Athlon64, 25
AMD Opteron, 25
An IP Office's Security Settings, 104
  Resetting, 104
Analog, 65
and/or unsecure, 9
Announcements, 17
Answer Pre-Select, 17
Answer Time, 17
AOC, 17
AOC-D, 17
AOC-E, 17
appears, 15
  Embedded Voicemail, 15
Appendix, 62, 110
Application Support list, 113
Applications Controls, 113
ARS, 17, 49, 54, 72, 92, 116
Assisted Transfer, 9
Attendant Admin, 54, 92, 116
Audit Details, 134
Audit Trail, 87, 97, 107, 134
  include, 87
  Log, 107
authorities', 97
Authorization Code, 72
Auto Attendant, 9, 47, 48, 54, 72, 92, 116
Auto Attendant Template, 48
auto-attendants, 9
Automatically Saving Sent Configurations, 87
Available Columns list, 62
Avaya, 5, 9, 15, 17, 97, 118, 127
  interlinking, 9
Avaya Integrated Management, 15, 39, 76
Avaya IP, 138
  shows, 138
Avaya IP DECT, 15, 17
Avaya SES, 9
AVRIP, 30
back, 5, 71, 127, 142
  IP Office, 5, 71, 127, 142
Backup Binaries, 135
Backup File Extension, 127
Backup Files on Send, 124, 127
Backup/Restore, 135
Backward Compatibility, 37
BAK, 127
Bar Commands, 121
Base Configuration, 110
Base TCP Port, 110, 114
B-channels, 9
behaviour, 17
belonging, 42
  Administrator Rights Group, 42
Binary Directory, 123, 125
Binary Files, 84
BLF, 30
BOOTP, 5, 17, 60, 70, 123, 124, 125
  matching, 124
BOOTP Entries, 17
BOOTP Server, 5
Border Between, 60, 62, 68
  Moving, 60, 62, 68
Branch Prefix, 9
Brazilian Portuguese, 25, 29
Break Out, 17
Broadcast, 84
Broadcast IP Address, 126
browsers', 97
Busy
  contains, 17
Busy on Held, 139
Busy Subscriber, 17
  Call Completion, 17
Busy Tone Detection, 72
c711, 141
  Small Office Edition, 141
c723, 141
CA, 97
Call Barring, 88
Call Completion, 17
  Busy Subscriber, 17
Call Data Tagging on Transfer Actions, 9
Call Presentation, 17
Call Route, 47, 48, 54, 72, 73, 92, 116
Call Routing, 17
  Outgoing, 17
Call Sender, 17
Call Status, 17, 25, 113
Call Status Application, 17
Call Transfer Announcements, 9
Call Waiting, 17
Calling, 9
Cancel, 9, 25, 28, 65
Cancel button, 80
  Selecting, 80
Castelle Fax Server Support, 9
cause, 65, 67, 82, 114, 127
  IP Office, 65, 67, 82, 114
  login, 127
  Manager, 127
CBC, 17, 38
CCBS, 17
CCC, 17, 38
CD, 25
  Insert, 25
  open, 25
CDR, 72
Centralized Voicemail, 9
cer, 110
Certificate Authorities, 97
Certificate Checks, 127
Certificate Import Wizard, 97
Certificate MMC, 97
Certificate Offered, 127
  IP Office, 127
Certificate Store Export, 97
Certificates, 97
Certificates – Current User Folder, 97
CFG, 87, 123, 125, 127, 135

cfg file, 87
Manager PC, 87
Chain Store Mangement, 39
Change Directory, 125
selecting, 125
Change Passwords, 94
Change Universal PRI Card Line Type, 9
Change Working Directory, 80, 123, 125, 132
Changing, 25, 29, 30, 60, 62, 65, 68, 72, 74, 76, 104, 117, 122, 127
Column Widths, 62
Companding LAW, 72
How, 65, 68
Initial Discovery Settings, 74
Installed Applications, 25
IP Office, 117
IP Office 4.1, 76, 104
Locale, 72
Manager Language, 29
Position, 65, 68
Services Base TCP, 30
Size, 60, 62, 68
TCP, 122
Unit/Broadcast Address, 30
Voicemail Type, 72
Windows Registry Settings, 127
Channel Reservation, 17
Charge, 17
CLI, 9, 15
CLI Routing, 9
existing, 9
CLI Routing Action, 9
replaces, 9
clicking, 140
Add, 140
Client Certificate Checks, 110
according, 110
Client IP Office Certificate Store, 110
Close Configuration, 122
Close Configuration/Security Settings After Send, 124, 127
Close Security Settings, 142
closing, 9
Manager, 9
Code, 9, 17, 46, 48, 72
Code, Telephone Number, 84
codecs, 17
Colors, 25
Column Widths, 62
Changing, 62
Columns Displayed, 62
Customizing, 62
Comma Separated Variable Text Files, 84
Compact Business Center, 38
Compact Contact Center, 38
Compact DECT, 17
Companding LAW, 72
Changes, 72
compared, 17
LCR, 17
computer', 97
Conference Center, 17, 25, 38
Conference Meet Me button, 9
Conferences, 17
Ending, 17
config, 76
Configuration
Erasing, 90
Loading, 76
Saving, 87
Sending, 88
Configuration Icons, 60, 62, 68
Configuration Interface, 68
Altering, 68
Configuration Mode, 51, 95, 142
Configuration Mode Interface, 52
Configuration Mode Screen Elements, 52
Configuration onto PC, 87
Saving, 87
Configuration Received, 87
Saving, 87
Configuration Settings, 67, 87
Revalidating, 67
Configuration Stored, 76
Loading, 76
Configurations, 135
configuring, 42, 43, 80
Access, 42
IP Office, 43
Manager, 80
Connecting, 5, 9, 17, 30, 82
IP Office, 5, 82
IP Office 3.2, 17, 30
Manager, 30
SES, 9
Contact Information Check, 76
ContactStore, 38
contains, 17
Busy, 17
Line Renumber, 17
Contains ARS, 44
Contains Auto Attendant, 44
Contains Control Unit, 44
Contains User, 44
Continue, 9, 25, 28
control, 42, 71
IP Office, 71
IP Office's System Password, 42
Control Unit, 46, 72, 73
Control Unit's LAN1, 90
copy, 76, 87, 97, 118
IP Office Manager, 76
IP Offices, 118
Manager, 97
corresponding, 97, 114
Manager application, 114
Managers, 97
Create Configuration tool, 82
Create New Config, 82, 131
Create New Configuration, 58
Create New Record, 58
Create Offline Configuration Wizard, 44, 46
during, 46
started, 44
Creating, 29, 42, 82
IP Office Service User, 42
New Configuration, 82
Windows, 29
CSV, 84, 136, 137
set, 136
CSV file, 15, 80, 84
CSV File Formats, 84
Current Configuration, 76
Loading, 76
Current User, 97, 127
Current User Certificate Store, 110
Currently IP Office Manager, 107
Custom Firewall Entry, 73
Customize Columns, 62
Customizing, 15, 62
Columns Displayed, 62
Data, 134
Data Settings, 90
D-channels, 9
DDI, 9
DDI Numbers, 9
DDI System, 9
DECT, 17
de-DE, 29
define, 44, 48
DTMF key, 48
IP Office, 44
Delayed Ring Preference, 17
Delete Contact Information, 76
Delete Entry, 58
Delete Incoming Call Route, 54, 92, 116
Deleting, 62, 65, 80
Entry, 62, 65
Delta Server, 17, 38
DER, 97, 110
DES_40, 114
DES_56, 114
DES-40, 97
DES-56, 97
describes, 28
Manager, 28
Deselecting, 127
deskers, 17
desking, 17, 62
Destinations, 140
Details Pane, 65, 68, 95, 138
Details Pane Actions, 65
Details Toolbar, 58
Device Manager menu, 40
Device Profile, 44
PIM, 44
Device Version Numbers, 9
DHCP, 90
DHCP Client, 30
DHCP Server, 30, 90
DHCP/BOOTP, 30
DID, 140
Digital Trunk Clock Source Change Alarm, 9
Dir, 54, 92, 116
Direct Media, 15, 17
Directories, 44, 54, 92, 116, 123, 125, 127, 132
selecting, 125
Working, 123, 125
Directory Entry, 73
Disable Account, 97, 107, 119
Disable Speakerphone, 9
Disconnect Tone, 17
discover, 74
IP Office, 74
Discovery, 30, 74, 110, 126
selecting, 126
Discovery Addresses, 74
Display, 127
Distributed Hunt Groups, 17
DNS, 30, 72
DO, 9
Domain Name Service, 30
dongle, 17, 25
drivers', 97
DS, 90
DSS Button, 73
DTE, 73
DTMF key, 48
defines, 48
during, 30, 126
Create Offline Configuration Wizard, 46
IP Office, 30
UDP, 126
Dutch, 25, 29
E1, 9
E1-R2 PRI, 9
E911, 44, 46, 60
E911 System, 54, 72, 92, 116
e-commerce, 97
including, 97
Edit menu, 87
Editing, 5, 65, 71, 87, 104, 121, 127
Entry, 65
IP Office, 5, 71
PC's, 127
Security Settings, 104
Windows Registry, 127
Email, 9, 97
Embedded Voicemail, 9, 15, 17, 38, 47, 48
appears, 15
running, 48

Embedded Voicemail Auto Attendant Short Codes, 9
Embedded Voicemail Memory, 48
Emulation, 9
Enable Application Idle Timer, 127
Enable BootP, 124
Enable Port, 124
Serial Communication, 124
Enable Time Server, 124
Enabled', Software, 119
enabled/disabled, 9
Enabling, 17, 43, 119
IP, 17
SNMP, 43
End, 17
Conferences, 17
English, 25
Enhanced Conference Meet Me, 9
Entry
Deleting, 62, 65
Editing, 65
Validating, 62, 65
Entry Types, 54, 92, 116
en-US, 29
Erase Configuration, 90, 131
Erase Security Settings, 104, 135
Erasing, 90
Configuration, 90
IP Office Configuration, 90
Error, 67
Jumping, 67
Error Pane, 58, 67, 138
hides, 138
Show/Hide, 58
Error Pane Actions, 67
es-MX, 29
etcissue.txt, 25
Ethernet LAN, 5
ethernet LAN/WAN, 17
Evening, 48
Events, 72
Excel, 84, 136, 137
except, 9, 43
IP500, 43
Legacy Card Carrier, 9
exchange, 30
IPSec, 30
excluding, 9, 25, 82
Home Editions, 25
T3, 9
WAN3, 82
exe file, 29
existing, 9, 43, 44, 95
CLI Routing, 9
IP Office, 43
Rights Groups, 95
Service Users, 95
Short Code, 44
Exit, 137, 142
Manager application, 137
exp, 84, 136, 137
expiry, 9, 76, 107, 119
Expiry Reminder Time, 107, 119
set, 107, 119
Exporting, 84, 136
Settings, 84
Exporting Settings, 84
Extension, 9, 44, 84
Extension Number, 15
Extension, User, 54, 92, 116
extension/VCM, 82
Extensions Renumber, 139
External, 15
place, 15
External Expansion Modules, 38
Extn201, 90
Extn202, 90
Fast Forward, 17
Favor RIP Routes, 72
Fax, 17
includes, 17
Feature Key dongle, 17
FIFO, 9
File
selecting, 51, 91, 104
File Directory Used, 132
File Menu, 142
File Sizes, 73
File Type, 136, 137
Files, 65, 82, 97, 122, 124, 126, 130, 135
Filters, 80
Finish, 82
FIPS 140-2, 97
Firewall, 44, 47, 49
Firewall IP Office Service Controls, 17
Firewall Profile, 54, 72, 73, 92, 116
firewalls, 30, 114
First In-First Out, 9
order, 9
Fixed Length Numbering, 82
flash, 71
following, 17, 30, 58, 127
IP Office, 30
ISDN, 17
Microsoft, 127
toolbars, 58
Force New Password, 119
Form, 97
ID, 97
Forwarding, 30
UDP, 30
FR, 73
Free, 88
French, 25, 29
fr-FR, 29
Full Control, 127
G723, 17
G729a, 17
GAP, 17
General, 9, 107, 119
General Availability, 37
General IP Office Features, 9
General Manager Changes, 9
General Settings, 107
General Template, 49
German, 25, 29
Get, 95
Security Settings, 95
greyed, 44, 46, 47, 117
Group Admin, 54, 92, 116
Group Details, 115
Group Edit, 54, 92, 116
Group Listen, 9
Group Listen Off, 9
Group Listen On, 9
Group Listen On/Off, 9
Group Membership, 94, 119
Group Operation, 9
Group Pane, 62, 95, 138
hides, 138
right, 138
Show/Hide, 95
Group Pane Actions, 62
Group/Account Code Call Recording Destination, 9
Guest, 76
H.323, 9, 30
H.323 Discovery, 30
H.323 Gatekeeper, 72
H.323 Signalling, 30
H.323 Status, 30
H.323 Trunk Support, 9
H323, 17, 38
H323 IP, 17, 38
handsfree, 9
Hard Disk Space, 25
Hardware, 44
Hardware Support, 17
Hardware Template, 46, 48
Having, 30
3.2, 30
HEADSET, 9
Headset Force Feed, 9
Held, 139
Held Validation, 17, 139
hide, 124, 138
Error Pane, 138
Group Pane, 138
Navigation Pane, 138
Service Base TCP Port, 124
Hide/Show Error Pane, 68
Hide/Show Group Pane, 68
Hide/Show Navigation Pane, 68
Hiding Panes, 60, 62, 67, 68
Hiding Toolbars, 58, 68
High, 97, 107, 110
set, 110
Set IP Office Minimum Password Complexity, 97
Higher Software, 43
HKEY_CURRENT_USER/Software/Avaya/IP400/Manager/Security, 127
HKEY_USERS/User GUID/Software/Avaya/IP400/Manager/Security key, 127
Home Editions, 25
excluding, 25
Host System, 114
hosting, 25
IP Office, 25
Hot Desking, 17
hot-swappable, 15
Housekeeping, 9
How
Changing, 65, 68
Hunt Group, 44, 54, 92, 116
HuntGroup, 84
ICLID, 15, 49
match, 49
ICMP, 30
sends, 30
ICR, 54, 92, 116
ID
forms, 97
ID Numbers, 17
identifies, 97, 110
IP Office, 97, 110
Manager, 97
ID's, 17
ie, 17, 134
IKE, 30
Immediate, 88
Implementing, 97
IP Office Administration Security, 97
Import/Export, 84, 136, 137
IMPORTANT, 5
Importing, 84, 137
Settings, 84
include, 17, 30, 87, 97
Audit Trail, 87
e-commerce, 97
Fax, 17
IP, 17
IP Office, 30
Incoming Call Route, 17, 44, 47, 54, 92, 116, 140
individual', 97
Initial Discovery Settings, 74
Changing, 74
Insert, 25
CD, 25
Installation Manager, 40
Installed Applications, 25
Changing, 25
Installing, 25
Manager, 25
Insufficient, 88
Integrated Management, 76
interlinking, 9
Avaya, 9
Internal Twinning, 15

Internet Time, 5
internet-based, 97
Intranet, 65
Intranet Service, 73
Intuity, 17
IP, 9, 17, 30, 43, 46, 74, 80, 82, 90, 110, 126, 134
  allocates, 90
  Enabling, 17
  including, 17
  sets, 126
  shows, 126
  uses, 90
IP Address, 30, 80, 132
IP DECT, 15, 17, 46
IP DECT Extension, 58
IP DECT Trunks, 38
IP Extensions, 73
IP Mask 255.255.255.0, 90
IP Mask 255.255.255.0., 90
IP Office
  access, 30, 42, 54, 76, 92, 97, 107, 110, 113, 114, 118
  adding, 43
  affect, 131, 135
  AIM, 39
  back, 5, 71, 127, 142
  cause, 65, 67, 82, 114
  Certificate Offered, 127
  changes, 117
  Configuring, 43
  connecting, 82
  connects, 5
  control, 71
  copy, 118
  define, 44
  discover, 74
  During, 30
  editing, 5, 71
  existing, 43
  following, 30
  hosting, 25
  identifies, 110
  identify, 97
  including, 30
  level, 37, 56
  loading, 123, 125
  Manager, 127
  match, 30, 70, 76, 82
  online, 104
  Opens, 58
  present, 140
  prevents, 104
  rebooting, 88
  relate, 113
  render, 5, 94
  requests, 5
  reset, 9
  responding, 30
  restore, 40
  returns, 90
  running, 76
  selects, 30
  send, 97
  set, 9, 42
  shows, 114
  take, 76
  type, 46, 82, 131
  upgrade, 43
  Voicemail Pro, 9
IP Office 2.1, 5, 37, 39
  IP Office 3.2, 39
IP Office 2.1., 43
  level, 43
IP Office 3.1, 15
IP Office 3.2
  Access, 30, 54, 92
  connect, 30
  connects, 17
  IP Office 2.1, 39
IP Office 3.2 Configuration, 30
  Accessing, 30
IP Office 4.0, 15, 17, 25, 38, 39, 94, 118, 135
  release, 15
  running, 135
  Service Users, 94
IP Office 4.0 General Availability, 17
IP Office 4.0 Q2 20007, 9
IP Office 4.0 Q2 2007, 74, 80
IP Office 4.0., 17, 43
  level, 43
IP Office 4.1, 9, 30, 37, 38, 54, 76, 82, 92, 94, 97, 104, 117, 134, 135, 142
  access, 30
  administrating, 97
  change, 76, 104
IP Office 4.1 Admin, 5
IP Office 4.1., 9, 97
IP Office 500, 9, 38, 39
IP Office 500 PRI Trunk Card, 9
IP Office 500 System Unit, 17
IP Office Admin, 17, 25
IP Office Admin Suite, 25
  selecting, 25
IP Office Administration Security, 97
  Implementing, 97
IP Office Administrator Applications CD, 25
IP Office Analog DECT, 17
IP Office application, 107, 110
  re-connecting, 110
IP Office Audit Trail, 9
IP Office Auto-Attendant Template, 40
IP Office Certificate Stores, 97
IP Office Configuration, 90
  Erasing, 90
IP Office Date, 9
IP Office Delta Server, 17
IP Office DVD, 25
IP Office Embedded Voicemail, 25
IP Office Embedded Voicemail Installation, 9
  refer, 9
IP Office File, 123, 125
IP Office firewall, 17
IP Office Functions, 5
IP Office General Template, 40
IP Office Hardware Template, 40
IP Office Installation, 104
  refer, 104
IP Office Installation Manual, 25, 90, 132
  refer, 25
IP Office LAN1 IP, 30
  traffic, 30
IP Office Manager
  copy, 76
  starting, 9
IP Office Manager application, 29
IP Office Manager Language, 29
IP Office Manager PC, 9
IP Office Manager Use, 97
IP Office menu, 30
IP Office Monitor, 113
IP Office Phone Manager, 47
IP Office Professional Edition, 17, 38
IP Office Secure Administration, 110
IP Office Service Rights, 116
IP Office Service User, 42
  creates, 42
IP Office Setting, 42
IP Office Small Office Edition, 46, 48
IP Office SNMP, 40
IP Office Standard, 38
IP Office Standard Edition, 17, 38
IP Office System Discovery, 74
IP Office System Status, 135
IP Office System Status Application, 17, 25, 30, 118
IP Office Systems, 42, 43, 48, 76
IP Office TAPI, 30, 38
IP Office Technical Bulletins, 15, 132
  refer, 132
IP Office Time Profiles, 9
IP Office Unique System Administrator, 42
IP Office Unsecured Interfaces, 97
IP Office User Template, 40
IP Office's DTE, 104
IP Office's Flash, 71
IP Office's IP, 30
IP Office's Security Settings, 104
  Loading, 104
IP Office's System Password, 42
  control, 42
IP Route, 54, 72, 73, 92, 116
IP Search Criteria, 30, 74, 122, 126
  Preferences, 30
IP400, 82
IP403, 17, 73
IP406 V1, 17, 73
IP406 V2, 9, 17, 48, 73
IP412, 73, 90
IP500, 9, 17, 38, 43, 48, 73, 82, 90
  except, 43
IP500 Licences, 38
IP500 PRI Trunk Channels, 38
IP500 PRI Universal, 9
IP500 PRI-U, 9, 38
IP500 Universal PRI, 9
IP500 Upgrade Standard, 17, 38
  adding, 17
  Professional, 17, 38
IP500 VCM 32, 17
IP500 VCM 64, 17
IP500 VCM Channels, 17
IP500 Voice Networking, 9, 17, 38
IPO TAPI, 30
IPO User, 42, 43
  match, 42
IPO User TFTP, 42
IPO User TFTP Password, 42
  match, 42
IPO Voice Networking, 30
IPSec, 30, 73
  exchange, 30
ISDN, 17
  following, 17
  outgoing, 17
it’s, 127
Italian, 25, 29
  Target, 29
Item Name, 134
Items Changed, 134
it-IT, 29
Java, 25
Java application, 25
Jobs, 44
Jumping, 67
  Error, 67
Key Dongle Serial Number, 17
Key Server, 25
key’, 97
Know System Discovery, 80
Know Units, 80

Known IP Office File, 80
Known IP Office Systems, 80
Known System Discovery, 80
Known Systems CSV file, 80
Known Units button, 15, 80
Known Units file, 80
L2TP, 30, 73
Lamp Operation, 9
LAN, 30, 90, 124, 126
LAN1, 30, 90
LAN1 IP, 110
LAN1 IP Address, 30
LAN1/LAN2, 72
LAN2, 9, 90
Language Support, 25
Large, 60, 62, 68, 125
Last In-First Out, 9
Latin Spanish, 25
LCR, 17
  compared, 17
LDAP, 72
Least Cost Route, 17, 54, 72, 92, 116
Legacy Card Carrier, 9
  except, 9
level, 37, 43, 56, 97
  IP Office, 37, 56
  IP Office 2.1., 43
  IP Office 4.0., 43
  Secure, 97
Licence, 54, 92, 116
License, 84
License Keys, 73
License Server IP Address, 72
License, License Key, 84
LIFO, 9
LIFO/FIFO Mailbox Operation, 9
Line Appearance button, 139
Line Appearance ID, 15
Line Appearance ID's, 17
Line Appearances, 15
Line Renumber, 17
  contains, 17
Line Renumber tool, 17
List
  Sorting, 62, 132
Listen, 30
  TCP, 30
  UDP, 30
Lite, 38
Loading, 76, 104, 123, 125
  Configuration, 76
  Configuration Stored, 76
  Current Configuration, 76
  IP Office, 123, 125
  IP Office's Security Settings, 104
Local Computer, 97
Local Machine, 97, 127
Local Machine Certificate Store, 110
Local Number Length, 9
Locales, 15, 72, 82
  Changes, 72
Locate IP Office Admin Suite, 25
Locked - Expired, 119
Locked - Idle, 119
Locked – Password Error, 119
Locked – Password Expired, 119
Locked - Temporary, 119
Locked Setting, 65
Log, 17, 97, 107, 119
  Audit Trail, 107
  Out, 17
  Set IP Office Service User Password Reject Action, 97
Logical LAN, 72, 73
login, 9, 17, 76, 119, 127
  cause, 127
  set, 17
long, 110
  TLS, 110
Longest Waiting, 84
Look In, 84, 137
Low, 97
  Set IP Office Minimum Password Complexity, 97
Low, Software, 107
LVM Greeting, 141
LVMGreeting, 9, 141
LVMGreeting.exe, 9, 141
MAC, 134
Main, 90
Main Toolbar, 58, 95, 104, 122, 131
make/receive, 9
Malicious Call Identification, 17
Manager
  copy, 39, 97
  describes, 28
  match, 76
  Overview, 5
  Starting, 28
  Switching, 51, 95
Manager 1st, 97
Manager 2nd, 97
Manager 5.2, 110
Manager application
  corresponding, 114
  exits, 137
  returns, 142
  switch, 135
Manager Back, 95
  Switching, 95
Manager Certificate Checks, 97, 127
Manager Certificate Stores, 97
Manager Language, 29
  Changing, 29
Manager Operator Rights, 54, 92
Manager PC, 30, 60, 74, 87, 97, 126, 127
  cfg file, 87
Manager PC's NIC, 126
Manager Preferences menu, 74
Manager Security Preferences, 97
Manager Start Dialogue, 25
  Adding, 25
Manager toolbars, 58, 68
  position, 58, 68
Manager Window, 68
  Resizing, 68
Manager's
  200MB, 25
  cause, 127
  closing, 9
  Configuring, 80
  Connecting, 30
  corresponding, 97
  identify, 97
  Installing, 25
  IP Office, 127
  offer, 127
  order, 97
Manager's Binary Directory, 132
Manager's menu bar, 121
Manager's Select IP Office menu, 30, 74
Manager's Working Directory, 87
Managing, 30
  Multiple Remote IP Offices, 30
Marks_Test, 70
match
  BOOTP, 124
  ICLID, 49
  IP Office, 30, 70, 76, 82
  IPO User, 42
  IPO User TFTP Password, 42
  Manager, 76
  PC's, 25, 29
  Service User, 76
Maximum Configuration, 73
Maximum Rights Groups, 110
Maximum Security, 97
Maximum Service Users, 110
May 2007, 15
MCID, 17
MD5, 97, 114
Medium, 60, 62, 68, 97, 107, 125
  Set IP Office Minimum Password Complexity, 97
Medium Security, 97
Meet-me conferencing, 17, 38
Menu Bar, 57
Menu Bar Commands, 142
Menu Options, 48
Merge, 88
Message Authentication, 97
Mexican Spanish, 29
Microsoft, 127
  following, 127
Microsoft Management Console, 97
Minimum Name Length, 107
Minimum Password Complexity, 107
Minimum Password Length, 107
Minimum Security, 97
misconfiguration, 9, 65, 67
MMC, 97
Monitor, 17, 25, 113
Monitor Password, 113
Morning, 48
Moving, 58, 60, 62, 65, 68
  Border Between, 60, 62, 68
  Previous, 58, 65
  Toolbars, 58, 68
MS-CRM, 9, 17, 38
MSN, 140
  set, 140
MSN Configuration, 58, 140
MSN/DID, 140
Multi-Line Tabs, 65, 68, 125
Multiple, 134
Multiple IP Offices, 42
Multiple Remote IP Offices, 30
  Managing, 30
name/password, 76, 104
Names, 15
Navigation Pane, 60, 95, 138
  hides, 138
  Show/Hide, 95
Navigation Pane Actions, 60
Navigation Toolbar, 58
need, 104
  OK button, 104
Negligible Security, 97
NET, 25
New Configuration, 82
  Creating, 82
New Entry, 62, 65
  Adding, 62, 65
New/Delete, 54, 92, 116
Next Entry, 58, 65
NIC, 126
NIC IP/NIC Subnet, 126
nl-NL, 29
NMC, 39, 40, 43
No Account Expiry, 119
No Answer Time, 17
None, 82, 97
  Set IP Office Service User Password Reject Action, 97
non-mergeable, 71
North American, 15
NOTE, 97, 127
NotFound, 70
Notify, 9
  Pots Extension, 9
NoUser, 15, 17

NoUser User, 17
offer, 127
  Manager, 127
Offer Server Certificate, 110
offline
  send, 131
OK button, 104, 107
  need, 104
online, 25, 104
  IP Office, 104
open
  CD, 25
  IP Office, 58
Open Configuration, 58, 76, 80, 122
Open File, 58, 76, 122, 131
Open Security Settings, 104, 142
Opened Offline/Newly Created Configuration, 88
Operating, 25
  System, 25
Operator Rights, 116
Order, 9, 15, 84, 97
  First In-First Out, 9
  Manager, 97
  remove/replace, 15
Other People, 97
Otherwise, 119
Out
  Logging, 17
Outcome, 134
Outgoing, 17
  Call Routing, 17
  ISDN, 17
Overview, 5, 91
  Manager, 5
  Security Settings, 91
Panes, 60, 62, 68
Partial Rerouting, 17
Particular Systems, 132
passcode, 71
passing, 119
  Account Expiry, 119
Password, 42, 104, 113
  Updating, 42
Password - Pre-3.2 Systems Only, 88
Password Administration, 42
Password Change Period, 107, 117, 119
Password Change Required, 5
Password Lockout, 17
Password Reject Action, 76, 107, 119
  perform, 107
Password Reject Limit, 76, 107
password/account, 107
Pasting, 87
PC IP Address, 134
PC Login, 134
PC MAC Address, 134
PC Requirements, 25
PC's, 127
  editing, 127
PCM, 141
PCPartner, 30
PC's, 25, 29
  match, 25, 29
PEM, 97, 110
perform, 74, 107
  Password Reject Action, 107
  UDP, 74
Personal, 97
Personal | Certificates, 97
pfx, 110
pfx file, 97
Phone Manager application, 9
Phone Manager Installation Manual, 9
Phone Manager Lite/Pro, 17
Phone Manager Pro, 9
Phone Manager Pro 4.1, 9
Phone Manager Type, 9
Phone Manager User Guide, 9
  refer, 9
Physical Extensions, 73
PIM, 40, 43, 44, 48
  Device Profile, 44
PIM IP Office Templates, 44
PKCS#12, 97, 110
place, 15, 97
  External, 15
Port Number, 124
Port Used, 110, 114
position, 58, 65, 68
  Changing, 65, 68
  Manager toolbars, 58, 68
Pots Extension, 9
  Notify, 9
PPP, 73
PR, 17
pre-2.1 IP Office, 37
Pre-3.2 IP Office Software, 43
pre-4.0, 25
pre-4.0 IP Office, 17, 25
Preferences
  IP Search Criteria, 30
  selecting, 124
Preferences menu, 17, 74
pre-IP Office 3.2, 94, 113
pre-IP Office 4.0, 17
Present, 140
  IP Office, 140
Presentation Digits, 140
pressing, 9
  Transfer, 9
prevents, 104
  IP Office, 104
Previous, 58, 65
  Moving, 58, 65
Previous Password Limit, 107
PRI, 9
PRI-U, 9
Private Call, 17
Pro, 9, 17, 38
Professional, 17, 38
  IP500 Upgrade Standard, 17, 38
Professional Edition, 9, 17, 38
Profile, 47, 48, 49, 54, 72, 73, 92, 116
Profile Entry, 73
Program, 28
Programming, 9
Properties, 29
pt-Br, 29
Q2 2007, 15, 123, 125
QSIG, 9, 17, 38
Queue Threshold, 9
Queued, 9, 17
Queuing On, 84
RAM, 25, 71
RAS, 47, 54, 72, 90, 92, 116
RAS Service, 73
RC4-128, 97
Read All Configuration, 54, 92
Read All Security Settings, 94
Read Configuration, 94
Read Only, 54, 92, 116
Read', 97, 127
Reboot Immediately, 94
Reboot Mode, 88
Reboot Time, 88
Reboot When Free, 94
Reboot/Merge Configuration List, 71
rebooting, 88, 131
  IP Office, 88
Receive Config, 131
Received BOOTP, 70
Received Configuration, 88
Received TFTP Error, 70
recognised, 97
re-connecting, 110
  IP Office application, 110
Recording Name, 9, 48
refer, 9, 25, 39, 40, 104, 132
  AIM, 39, 40
  IP Office Embedded Voicemail Installation, 9
  IP Office Installation, 104
  IP Office Installation Manual, 25
  IP Office Technical Bulletins, 132
  Phone Manager User Guide, 9
  Vista Business Ultimate, 9
Refresh, 30, 76, 80, 104, 122, 132
Regedt32.exe, 127
relating, 113
  IP Office, 113
release, 15
  IP Office 4.0, 15
Remote Hot Desking, 17
Remove, 25
Remove Programs, 25
Remove Selection, 127
remove/replace, 15
  order, 15
render, 5, 94
  IP Office, 5, 94
Renumber, 17, 139
replace, 9
  CLI Routing Action, 9
Request Login on Save, 124, 127
requests, 5
  IP Office, 5
Reserve Last CA, 17
Reset All Security Settings, 94
Reset Security Settings, 104, 121, 142
resetting, 9, 42, 104, 119
  Account Expiry, 119
  An IP Office's Security Settings, 104
  IP Office, 9
  Unique System Administrator, 42
Resizing, 68
  Manager Window, 68
respond, 30, 126
  IP Offices, 30
  TCP, 126
  UDP, 30, 126
restore, 40
  IP Office, 40
Restore Binaries, 135
Retry, 76
return, 90, 142
  IP Office, 90
  Manager application, 142
Revalidating, 67
  Configuration Settings, 67
RFC868, 5
RFT, 25
right, 47, 72, 138
  Group Pane, 138
Rights Groups
  existing, 95
  set, 119
Ringing Line Preference, 17
RIP, 30
RJ45 Ethernet LAN, 9
RJ45 Ethernet WAN, 90
Rotary, 84
routable, 30, 74, 126
RTF, 25
RTP, 17
RTP Relay, 17
running, 9, 48, 76, 135
  Embedded Voicemail, 48
  IP Office, 76
  IP Office 4.0, 135
  VPNremote, 9
S0, 15
SAA, 40, 42, 43
SAA AIMAdmin, 42
SAA IPO User, 42
SAA Setting, 42

Save, 87, 95, 104, 122
Configuration, 87
Configuration onto PC, 87
Configuration Received, 87
Security Settings, 95, 104
Save As, 122
Save Configuration, 58, 87, 88, 122
Save Configuration As, 122
Save Configuration File After Load, 124, 127
Save File As dialog, 122
Save In, 84, 136
Saving Security Settings, 104, 142
SCN, 17
SCN Distributed Hunt Groups, 17
Secondary Dial Tone, 17
Secure, 97, 114
level, 97
Secure Communications, 76, 104, 127
Secure, High, 114
Secure, Low, 114
Secure, Medium, 114
Security, 97, 104, 110, 113, 127
selecting, 127
Security – Registry Settings, 127
Security Administration, 97, 110, 114, 117
Security Administrator, 5, 54, 92, 94, 97, 107
Security Enhancements, 9
Security Manager, 107
Security Manager Service User, 107
Security Mode, 95, 121
Security Mode Interface, 95
Security Mode Screen Elements, 95
Security Service User Settings, 119
Security Services Settings, 114
Security Settings
Editing, 104
Get, 95
Overview, 91
Save, 95
Saving, 104
Security Settings Pane, 95
Security User, 94, 134
securitypwd, 94, 107
Select Directory, 132
selecting
Cancel button, 80
Change Directory, 125
Directories, 125
Discovery, 126
File, 51, 91, 104
IP Office, 30
IP Office Admin Suite, 25
Preferences, 124
Security, 127
Tab, 65
TCP Discovery Active, 110
UDP Discovery Active, 110
Validation, 130
Visual Preferences, 125
Yes, 25
Self Administer button, 9
self-signed', 97
send, 30, 88, 97, 131
Configuration, 88
ICMP, 30
IP Office, 97
offline, 131
TCP, 30
Send Config, 88, 131
Send Config menu, 122
Send Configuration, 82
Send Configuration menu, 72, 88
Serial Communication, 124
Enable Port, 124
Server, 5
Server Certificate, 110
Server Private Key, 110
Service, 54, 73, 92, 114, 116, 117
access, 117
Service Security Level, 110, 114
Service Short Codes, 17
Set Hunt Group Out, 17
Service User
access, 116
account, 76
existing, 95
IP Office 4.0, 94
match, 76
Sets, 119
Service User Details, 107
Services Base TCP, 30
change, 30
Services Base TCP Port, 110, 124
hides, 124
SES, 9
connect, 9
SES Trunks, 38
Session ID Cache, 110
Session Initiation Protocol, 30
set
Account Idle Time, 119
CSV, 136
Expiry Reminder Time, 107, 119
High, 110
IP, 126
IP Office, 9, 42
Login, 17
MSN, 140
Rights Groups, 119
Service User's, 119
TCP, 74
UDP, 74
Set button, 127
Set Certificate, 97
Set Hunt Group Night Service, 17
Set Hunt Group Out, 17
Service Short Codes, 17
Set IP Office Account Idle Time, 97
Set IP Office Client Certificate Checks, 97
Set IP Office Configuration, 97
Set IP Office Minimum Password Complexity, 97
High, 97
Low, 97
Medium, 97
Set IP Office Minimum Password Length, 97
Set IP Office Password Change Period, 97
Set IP Office Previous Password Limit, 97
Set IP Office Security Administration, 97
Set IP Office Service User Password Reject Action, 97
Log, 97
None, 97
Set IP Office Session ID Cache, 97
Set Manager Certificate Checks, 97
Settings
Exporting, 84
Importing, 84
setup.exe, 25
SHA-1, 97, 114
Short Code
existing, 44
ShortCode, 84
Shortcut Locale Setting, 29
Show In Groups, 62
Show Previous/Next Entry, 58
Show/Hide, 58, 95
Error Pane, 58
Group Pane, 95
Navigation Pane, 95
SHOW_LINEID_NOT_OUTSIDE, 15
shows, 114, 126, 138
Avaya IP, 138
IP, 126
IP Office, 114
Since UDP, 126
SIP, 9, 15, 17, 30, 46
SIP Enablement Service, 9
SIP Trunk Channels, 9, 17
SIP Trunks, 38
Size, 60, 62, 68, 73
Changing, 60, 62, 68
Small, 60, 62, 68, 125
Small Community Network, 9, 17, 30, 38
Small Office Edition, 60, 73, 82, 90, 141
c711, 141
Smart Card, 17
SMTP email, 9
snap-in', 97
SNMP, 9, 30, 39, 40, 43
enabling, 43
SoftConsole, 17, 30, 38
Software, 107, 114, 127
Solomail, 30
Sorting, 62, 132
List, 62, 132
SP2, 25
SP4, 25
SPEAKER key on Avaya DS, 9
SSA, 9, 17, 107, 118
SSA on IP Office 3.2, 97
Standard Edition, 9, 17, 38
Standard Edition Mode, 9
started, 9, 28, 44
Create Offline Configuration Wizard, 44
IP Office Manager, 9
Manager, 28
Static, 72
Status, 17, 30, 54, 92
Status Access, 54, 92, 118
Status Application, 9, 17, 25
Status Bar, 70, 95
Status Group, 94
Status Interface, 110, 114
Still Queued, 9, 17
store', 97
Strong', 97
subnet, 30, 74
subnets, 74, 126
Success, 134
SUM, 39, 40, 43
support.microsoft.com/kb/256986, 127
supporting, 113
Switching, 51, 95, 135
Manager, 51, 95
Manager application, 135
Manager Back, 95
Syslog, 9, 134
Sysmonitor, 30
SysMonitor application, 17
System Alarms, 9
System Details, 110
System Discovery, 80
System Events, 9
System Monitor, 25
System Password, 43
System Phone, 9
System Preferences, 9
System Settings, 114
System Status, 17, 118, 135
System Status Access, 135

System Status Application, 9, 25, 113, 114, 118
System Status Interface, 114
Systems, 15, 17, 25, 30, 43, 44, 72, 76, 110, 113
  Operating, 25
T1, 9, 15
T246, 15
T3, 9, 15, 17
  excluding, 9
T3 Direct Media Support, 15
T3 IP, 9, 15, 17
Tab, 65
  Selecting, 65
Tabs Display, 65, 68
take, 76
  IP Office, 76
TAPI, 17
TAPI Wave Driver, 30
Target, 29
  Italian, 29
TCP, 30, 74, 80, 110, 114, 122, 126
  change, 122
  listens, 30
  respond, 126
  sends, 30
  set, 74
TCP Base Port, 114, 124
TCP Discovery, 126
TCP Discovery Active, 110
  Selecting, 110
TCP Discovery Address Ranges, 74
Technical Bulletins, 132
telecoms, 25
Telephony, 9, 17, 72
Telephony Settings, 90
Template, 47
Template Records, 46, 47, 48, 49
Temporary Disable, 107, 119
Terminal Support, 17
TFTP, 5, 30, 42, 70, 123, 124, 125, 138
TFTP Configuration Write, 113
TFTP Log, 138
TFTP Log window, 138
TFTP Server, 5, 124
Those toolbars, 58, 68
Though Manager, 51
Through Manager, 30
TIME
  Access, 134
Time on System Variables, 9
Time Profile, 44, 54, 92, 116
timeout, 9
TimeQueued, 9
TimeSystem, 9
Title Bar, 52, 56
TLS, 9, 30, 70, 97, 110, 114, 127
  long, 110
Toolbars, 58, 68, 138
  Altering, 58
  following, 58
  Moving, 58, 68
Tools, 9, 40, 139, 141
Tools -> Device Manager, 44
Tools menu, 17, 57, 121
traffic, 30
  IP Office's LAN1 IP, 30
Transfer, 9
  pressing, 9
TRANSFER button, 9
Transport Layer Security, 97
Transtalk 9040, 17
Trusted Root Certification Authorities, 97
Tunnel, 30
type, 46, 82, 131
  IP Office, 46, 82, 131
UDP, 30, 74, 80, 110, 126
  during, 126
  forward, 30
  listens, 30
  performs, 74
  respond, 30, 126
  set, 74
UDP Broadcast, 30
  255.255.255.255, 30
UDP Discovery, 126
UDP Discovery Active, 110
  Selecting, 110
UDP/TCP, 30
UK English, 29
Unblock, 28
Under UDP Discovery, 74
unencrypted, 97
Unique Security Administrator, 42, 43, 107, 117
Unique Security Control Unit, 94
Unique System Administrator, 42
  reset, 42
Unit/Broadcast Address, 30, 74, 76, 104, 122, 132
  changes, 30
United States, 46
Units, 76, 122
unparked, 17
unsecure, 5, 94, 114
Unsecure Only, 110, 114
Unsecure Only', 114
Unsecured Interfaces, 113
unvalidated, 132
Updating, 42
  Passwords, 42
Upgrade, 43, 132
  IP Office, 43
Upgrade Wizard, 5, 125, 132
Upgrade Wizard tool, 132
US, 60
US English, 29
USB, 17, 25
Use Port, 9, 90
User Restriction/Rights, 84
User Rights, 44, 47, 54, 65, 92, 116
User Rights Admin, 54, 92, 116
uses, 90
  IP, 90
UTF8, 84, 136, 137
v1.0, 97
Validate Configuration, 58
Validate Entry, 58
Validating, 62, 65, 130, 132
  Entry, 62, 65
Validation, 130
  selecting, 130
Validation Control, 17
Variable Routing, 9
VCM, 9
Version, 9, 132
Very strong', 97
View/Edit, 54, 92, 116
Viewing, 58, 60, 65, 67, 68, 94
Vista, 9
Vista Business Ultimate, 9
  refers, 9
Vista Enterprise, 9
Vista Home Basic, 9
Vista Home Premium, 9
Visual Preferences, 60, 62, 65, 68, 125
  selecting, 125
Visual Voice, 17
VM Pro Password, 113
Voice Mail Lite, 25
Voice Recording, 17
Voicemail Email, 84
Voicemail Lite, 17
Voicemail Lite/Pro, 17
Voicemail On, 84
Voicemail Pro, 9, 17, 25, 113
  IP Office, 9
Voicemail Pro 4.0, 17
Voicemail Pro 4.1, 9
Voicemail Type, 72
  Changes, 72
VoIP, 9
VoIP Extension, 58
VPN IP Extensions, 9
VPN IP Extensions Licenses, 9
VPN Phone Allowed, 9
VPNremote, 9
  running, 9
WAN, 5, 65
WAN Port, 54, 72, 73, 92, 116
WAN Service, 73
WAN3, 17, 82
  excluding, 82
WAN3 10/100, 17
wav, 44, 48, 141
WAV file, 48
  allow, 48
What's New, 9, 15, 17
When Free, 88
wildcards, 9
Windows, 25, 28, 29, 87, 97, 127
  Create, 29
Windows 2000 Professional, 25
Windows 2000 Server, 25
Windows 2003 SBS, 25
Windows 2003 Server, 25
Windows Certificate Store Import, 97
Windows Certificate Store Organisation, 97
Windows Certificate Store Usage, 97
Windows Control Panel, 25
Windows Notepad, 25
Windows Operating System Support, 9
Windows PC, 5
Windows Registry, 127
  editing, 127
Windows Registry Settings, 127
  Changing, 127
Windows Security Alert, 28
Windows Server 2003, 97
Windows Vista, 9, 25, 97
Windows XP, 28
Windows XP Pro, 9
Windows XP Professional, 25, 97
Wireless, 44, 60
Wireless IP Phones, 15
Within Preferences, 126
Within SAA, 42
WordPad, 25, 84
Working, 123, 125
  Directory, 123, 125
Working Directory, 127
Write, 119
Write All Security Settings, 94
Write Configuration, 94
X.509 v3, 97
X.509v3, 110
X509, 97
xxxx, 88
Yes
  Selecting, 25

Avaya
Unit 1, Sterling Court
15 - 21 Mundells
Welwyn Garden City
Hertfordshire
AL7 1LZ
England

Tel: +44 (0) 1707 392200
Fax: +44 (0) 1707 376933

Web: http://www.avaya.com/ipoffice/knowledgebase