



# Using IP Office System Monitor

Release 12.0  
Issue 13  
April 2024

## Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

## Documentation disclaimer

"Documentation" means information published in varying media which may include product information, subscription or service descriptions, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End user agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End user.

## Link disclaimer

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

## Warranty

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

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

## Hosted Service

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

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

## Licenses

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

## Copyright

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

## Virtualization

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

## Third Party Components

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

## Service Provider

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

## **Compliance with Laws**

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

## **Preventing Toll Fraud**

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

## **Avaya Toll Fraud intervention**

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, please contact your Avaya Sales Representative.

## **Security Vulnerabilities**

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

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

## **Trademarks**

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya LLC.

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

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

## **Downloading Documentation**

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

## **Contact Avaya Support**

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

# Contents

<b>Chapter 1: System Monitor</b> .....	9
What's New.....	9
Default Logging.....	10
Installing System Monitor.....	10
System Status Report.....	11
The Alarm Log.....	14
Monitor Icons.....	14
Keyboard Shortcuts.....	15
<b>Chapter 2: Starting System Monitor</b> .....	18
Connecting to a System using UDP.....	18
Connecting to a System using TCP.....	19
Connecting to a System using HTTP.....	20
Connecting to a System using HTTPS.....	21
Closing System Monitor.....	22
<b>Chapter 3: IP Office Security Configuration</b> .....	23
Setting the Monitor Password.....	23
Disabling UDP/TCP/HTTP Access.....	23
Configuring a Service User for Monitor Access.....	24
Adjusting the HTTP Service.....	25
<b>Chapter 4: Using the Screen Log</b> .....	26
Pausing the Screen Log.....	27
Starting the Screen Log.....	27
Clearing the Screen Log.....	27
Filtering the Screen Log.....	28
Searching the Screen Log.....	28
Converting IP Address Hex Values.....	29
Selecting the System to Monitor.....	29
Reconnecting to the Monitored System.....	30
Setting the Trace Options.....	30
Viewing the System Alarms.....	30
Viewing the Status Menus.....	31
Emailing the Screen Log.....	31
Opening a Log File.....	32
Copying Screen Log Information.....	32
Saving the Screen Log as a Log File.....	33
Setting the Screen Font.....	33
Setting the Screen Background Color.....	33
Setting the Trace Colors.....	34
Setting the Indenting.....	34

Showing the Date and Time.....	35
<b>Chapter 5: Logging to a File.....</b>	<b>36</b>
Setting the Log Preferences.....	36
Starting File Logging.....	37
Stopping File Logging.....	38
Switching Between Binary and Text Logging.....	38
Adding Log Stamps.....	38
Opening a Log File.....	39
Saving the Screen Log as a Log File.....	40
Manually Rolling Over the Log File.....	40
Converting a Binary Log to a Text Log.....	40
<b>Chapter 6: Setting the Trace Options.....</b>	<b>42</b>
Setting the Trace Options.....	42
Saving Trace Options as a File.....	42
Loading trace options from a file.....	43
Coloring Individual Trace Options.....	43
Coloring Tab Trace Options.....	44
Clearing a Trace Options Tab.....	44
Setting a Trace Options Tab.....	45
Clearing All the Trace Options.....	45
Defaulting the Trace Options.....	45
<b>Chapter 7: Trace Option Menus.....</b>	<b>47</b>
ATM Trace Options.....	48
Call Trace Options.....	49
CTI Trace Options.....	51
Directory Trace Options.....	52
DTE Trace Options.....	53
EConf Trace Options.....	54
Frame Relay Trace Options.....	54
GOD Trace Options.....	55
H.323 Trace Options.....	56
Interface Trace Options.....	57
ISDN Trace Options.....	58
Jade Trace Options.....	60
<b>Key/Lamp Trace Options.....</b>	<b>61</b>
Media Trace Options.....	61
PPP Trace Options.....	62
R2 Trace Options.....	63
Routing Trace Options.....	64
SCN Trace Options.....	65
Services Trace Options.....	66
SIP Trace Options.....	67
SSI Trace Options.....	68

T1 Trace Options.....	69
System Trace Options.....	69
VComp Trace Options.....	71
VPN Trace Options.....	72
WAN Trace Options.....	74
<b>Chapter 8: Syslog Tracing.....</b>	<b>75</b>
Enabling Syslog Monitor Output.....	76
Configuring the Syslog Trace Options.....	76
Default Syslog Trace Options.....	77
Downloading a Syslog Archive from Web Control.....	78
Downloading a Syslog Archive from Cloud-based Systems.....	79
Downloading a Syslog Archive from Subscription Systems.....	80
Extracting the Syslog zip files.....	80
Converting Syslog Files.....	81
<b>Chapter 9: Status Screens.....</b>	<b>83</b>
Alarms.....	84
Blacklisted Extensions.....	84
Blacklisted IP Addresses.....	86
Buffer Data.....	88
Conference Status.....	89
DECT Line Status.....	90
DHCP Data.....	90
DSS Status.....	91
Equinox Sessions.....	92
H323 Phone Status.....	92
IPO-SNet.....	93
IPv6 Config.....	94
Jade Queue Status.....	94
Logging.....	95
Map Status.....	96
Memory Data.....	96
NAPT Status.....	97
Network View.....	98
Outdialer Status.....	99
Partner Sessions.....	100
Performance Data.....	101
Quarantined Phone Status.....	102
SCN Licence.....	104
SIP Phone Status.....	105
SIP TCP User Data.....	106
Small Community Networking.....	106
[S]RTP Sessions.....	107
TCP Streams Data.....	107

US PRI Trunks.....	108
Voicemail Sessions.....	108
Voice Compression.....	109
Voice Compression (TI).....	109
<b>Chapter 10: Example Monitor Settings.....</b>	<b>110</b>
J100 Phone Troubleshooting.....	110
Analog Trunk Caller ID.....	111
ISDN Trunk Caller ID.....	112
ISDN Calls Disconnecting.....	113
System Rebooting.....	115
ISDN Problems (T1 or E1 PRI Connections).....	116
ISP & Dial-Up Data Connection Problems.....	116
Remote Site Data Connection over Leased (WAN) Lines.....	117
Frame Relay Links.....	117
Problems Involving Non-IP Phones.....	118
Problems Involving IP Phones.....	118
Locating a Specific PC Making Calls to the Internet.....	118
Firewall Not Working Correctly.....	119
Calls Answered/Generated by IP Office Applications.....	120
Message Waiting Indication.....	120
Speech Calls Dropping.....	121
<b>Chapter 11: IP Office Ports.....</b>	<b>123</b>
Ports.....	123
Protocols.....	125
IP Office System Ports.....	125
Voicemail Pro Ports.....	133
one-X Portal Server and Client Ports.....	135
Media Manager Ports.....	137
Customer Operations Manager (COM).....	138
Port Changes Between Releases.....	138
Port Changes from 8.1 FP1 to 9.0.....	139
Port Changes from 9.0 to 9.0.3.....	140
Port Changes from 9.0.3 to 9.1.....	140
Port Changes from 9.1 to 10.0.....	141
Port Changes from 10.0 to 10.1.....	142
Port Changes from 10.1 to 11.0.....	143
Port Changes from 11.0.0 to 11.1.0.....	144
Port Changes from 11.1.0 to 11.1.1.....	144
Port Changes from 11.1.1 to 11.1.2.....	144
<b>Chapter 12: Addendum.....</b>	<b>146</b>
Cause Codes (ISDN).....	146
Cause codes and definition.....	146
Decoding FEC Errors.....	149

Miscellaneous.....	151
<b>Chapter 13: Additional Help and Documentation.....</b>	<b>152</b>
Additional Manuals and User Guides.....	152
Getting Help.....	152
Finding an Avaya Business Partner.....	153
Additional IP Office resources.....	153
Training.....	154



# Chapter 1: System Monitor

SysMonitor can assist in the detailed diagnosis of system problems. Through configuration of its trace options, it displays information on specific areas of a system's operation. It can also record that information as log files for later analysis.

- SysMonitor is also known as System Monitor, Monitor or SysMon.
- SysMonitor is intended primarily for use by Avaya support and development staff. The application settings and the information shown frequently change between software releases.
- Analysis of the information shown can require detailed data and telecommunications knowledge and so is not intended for general users. For general purpose monitoring of the status of a system and calls, use the System Status Application. System Status Application provides much easier to interpret data and information and is suitable for use by system maintainers and advanced system users.
- Despite the above, all persons maintaining systems need to be able to run SysMonitor in order to capture logs for submission with fault reports, even if they cannot interpret those logs themselves.

## Related links

[What's New](#) on page 9

[Default Logging](#) on page 10

[Installing System Monitor](#) on page 10

[System Status Report](#) on page 11

[The Alarm Log](#) on page 14

[Monitor Icons](#) on page 14

[Keyboard Shortcuts](#) on page 15

---

## What's New

For IP Office Release 11.1 FP1, the application has the following enhancements:

- **Access Through Customer Operations Manager for Subscription Mode Systems**

SysMonitor access to IP Office subscription mode systems is supported via Customer Operations Manager acting as a proxy for the connection. The address to use is shown within the system details within Customer Operations Manager. Refer to [Using Customer Operations Manager for IP Office Subscription Systems](#).

## Related links

[System Monitor](#) on page 9

---

## Default Logging

The following options apply for the monitoring of new or defaulted IP Office systems:

- **\*55 Log Stamp Short Code:**

All new and defaulted systems have the short code \*55 added. When the user dials the code, it inserts a log stamp (see [Adding Log Stamps](#) on page 38) into any traces running against the system. This allows users to indicate in the trace when an event has occurred.

- **Default Syslog Monitor Tracing:**

The default configuration of Linux-based servers automatically adds a monitor Syslog output to the system configuration. The entry is configured to store the records on the server using the 127.0.0.1 address. This provides hourly Syslog files which are retained for 3–days. See [Configuring the Syslog Trace Options](#) on page 76.

- **Cloud Edition Systems:**

For these system, the system's monitor Syslog output is automatically directed to the **Cloud Diagnostic Agent** service run by the cluster hosting the system. Those logs are kept for up to 3-days and can be downloaded through the cluster's Customer Operations Manager.

- **Subscription Systems:**

These systems can be monitored and managed through Customer Operations Manager running on the cluster providing the system subscriptions. In that case, the system Syslog files can also be collected using Customer Operations Manager.

### Related links

[System Monitor](#) on page 9

---

## Installing System Monitor

### About this task

Monitor is a Windows application. It runs in English only but does not require any licenses. Avaya supplies SysMonitor as part of the IP Office administrator suite DVD. This is available from a number of sources:

- Avaya supply the suite on the IP Office Applications DVD made available for each IP Office release. You can download an ISO file of the DVD from the Avaya support at <https://support.avaya.com>.
- Users of Customer Operations Manager can download the installer from the **Applications | IP Office Admin** menu.
- Users of Server Edition web manager can download the installer from the **Platform View | App Center** menu.

The default installation process also installs the System Status Application and IP Office Manager applications. However, if necessary, you can install just SysMonitor.

Minimum PC requirements	
RAM	128 MB
Hard disk free space	10 GB

Processor	
Pentium	PIII 800MHz
Celeron	Celeron 3 800Mhz
AMD	Athlon B 650MHz

- Any Ethernet speed mismatch between the PC running monitor and the system being monitored increases the likelihood of dropped packets. The PC port must match or exceed the speed of the system being monitored. The same problem may also arise from speed differences in any intermediate devices between the PC and the monitored system.

### Procedure

1. Insert the DVD into the PC's DVD drive. This starts the installation wizard.
2. Select the required language and click **Next**.
3. Select the file path for the installed files and click **Next**.
4. From the list of available applications, check that **System Monitor** is selected for installation. Be careful about de-selecting any other options as that triggers their removal if already installed.
5. Click **Next**.
6. Click **Install**.

### Related links

[System Monitor](#) on page 9

---

## System Status Report

The status report is output whenever monitor connects to a system. The information included varies depending on the type of system and the equipment installed with it.

In addition, when monitor starts, the initial output may include the system's alarm log. See [Alarms](#) on page 84.

### IP500 V2 System Example

The example below is a typical output for an IP500 system. The first few lines include the time, date plus the IP address of the system and up time of the monitored system.

```
***** SysMonitor v6.2 (4) *****
***** contact made with 192.168.42.1 at 10:45:17 22/7/2008 *****
***** System (192.168.42.1) has been up and running for 1day, 2hrs and
19secs (93619928mS) *****
93619928mS PRN: System Monitor Started IP=192.168.42.203 IP 500 4.2(4) IP500 Site A
```

## System Monitor

```
(IP Office: Supports Unicode, System Locale is eng)
93619928mS PRN: LAW=A PRI=0, BRI=4, ALOG=4, ADSL=0 VCOMP=64, MDM=0, WAN=0, MODU=0
LANM=0 CkSRC=5 VMAIL=1 (VER=3 TYP=1) CALLS=0 (TOT=3)
93623929mS PRN: ++++++
93623929mS PRN: + loader: 0.0
93623929mS PRN: + cpu: id 2 board a0 pld 17 type c10 options 802
93623929mS PRN: + fpga: id 1 issue 0 build 5e
93623929mS PRN: ++++++
93623929mS PRN: ++++++ LIST OF MODULES ++++++
93623930mS PRN: +-----
93623930mS PRN: + Slot 1: Base DIGSTA8 Board=0xc0 PLD=0x05
93623930mS PRN: + Mezzanine NONE
93623930mS PRN: +-----
93623930mS PRN: + Slot 2: Base VCM64 Board=0x01 PLD=0x10
93623930mS PRN: + Mezzanine BRI8 Board=0x01 PLD=0x07
93623930mS PRN: +-----
93623930mS PRN: + Slot 3: Base PHONE8 Board=0x01 PLD=0x03
93623931mS PRN: + Mezzanine ATM4 Board=0x00 PLD=0x06
93623931mS PRN: +-----
93623931mS PRN: + Slot 4: Base NONE
93623931mS PRN: + Mezzanine NONE
93623931mS PRN: +-----
93623931mS PRN: ++++++ END OF LIST OF MODULES ++++++
```

The next line gives information about various aspects of the system. This line is output at regular intervals, set through the [Logging to a file](#) on page 36.

```
93619928mS PRN: LAW=A PRI=0, BRI=4, ALOG=4, ADSL=0 VCOMP=64, MDM=0, WAN=0, MODU=0
LANM=0 CkSRC=5 VMAIL=1 (VER=3 TYP=1) CALLS=0 (TOT=3)
```

Output	Description
<b>LAW</b>	A-Law or U-law system.
<b>PRI</b>	Number of PRI channels
<b>BRI</b>	Number of BRI channels
<b>ALOG</b>	Number of Analog Trunk Channels
<b>ADSL</b>	Not used
<b>VCOMP</b>	Number of voice compression channels installed.
<b>MDM</b>	Size of Modem Card Fitted
<b>WAN</b>	Number of WAN Ports configured.
<b>MODU</b>	Number of external expansion modules (excluding WAN3 modules) attached.
<b>LANM</b>	Number of WAN3 external expansion modules attached.
<b>CKSRC</b>	The current clock source being used for PRI/BRI trunks (0 = Internal Clock Source).
<b>VMAIL</b>	Indicates whether the voicemail server is connected. 1 if connected, 0 if not connected.
<b>VER</b>	The software version of the voicemail server if obtainable.

*Table continues...*

Output	Description
<b>TYP</b>	The type of Voicemail Server: 0 = None. 1 = Voicemail Lite/Pro. 2 = Centralized Voicemail Pro. 3 = Embedded Voicemail. 4 = Group (3rd party) voicemail. 5 = Remote Audix Voicemail
<b>CALLS</b>	Number of current calls
<b>TOT</b>	Total number of calls made to date since last system reboot.

### IP Office Server Edition System Example

The example below is for an primary server in a IP Office Server Edition system. It shows details of the server and lists the core services running on the server.

```
Monitor Started IP=192.168.0.6 S-Edition Primary 9.1.0.0 build 87 ServerEdition (Server
Edition(P))
(Supports Unicode, System Locale is default)
PRN: Linux Whoo
8147790mS LIC: Processing token (serial number = 1342837622)
8147790mS LIC: Processing token (serial number = 2749693813)
8147790mS LIC: Processing token (serial number = 1351209077)
8147791mS LIC: Processing token (serial number = 3748848757)
8147791mS LIC: Processing token (serial number = 197602678)
8147791mS LIC: Processing token (serial number (big) = 611926526051)
8147791mS LIC: ProcessToken (Serial number (big) = 611926526051)
8148673mS PRN: IPOKeepaliveTask::Main sending keepalives at 5000 ms
8150830mS PRN: ++++++
8150864mS PRN: + hardware id: Generic
8150864mS PRN: + virtualized: no
8150864mS PRN: + ova: no
8150864mS PRN: + hosted: no
8150864mS PRN: + cpu: Intel(R) Pentium(R) 4 CPU 3.20GHZ
8150864mS PRN: + ram: 1868MB
8150864mS PRN: + hdd: WDC
8150864mS PRN: + hdd size: 73579MB
8150864mS PRN: + inventory code:
8150864mS PRN: + model info:
8150864mS PRN: + serial number:
8150864mS PRN: ++++++
8150864mS PRN: ++++++
8150864mS PRN: ++++++ LIST OF SERVICES ++++++
8150864mS PRN: +-----+
8150864mS PRN: + Service 1: IPO-Linux-PC
8150864mS PRN: +-----+
8150864mS PRN: + Service 2: IPO-MediaServer
8150864mS PRN: +-----+
8150864mS PRN: + Service 3: one-X Portal
8150864mS PRN: +-----+
8150864mS PRN: + Service 4: Voicemail Pro
8150864mS PRN: +-----+
8150864mS PRN: + Service 5: Contact Recorder
8150864mS PRN: +-----+
8150864mS PRN: + Service 6: WebLM
8150864mS PRN: +-----+
```

```
8150864mS PRN: + Service 7: Web RTC Gateway
8150864mS PRN: +-----
8150864mS PRN: + Service 8: Authentication Module
8150864mS PRN: +-----
8150864mS PRN: + Service 9: Web Collaboration
8150864mS PRN: +-----
8150864mS PRN: ++++++ END OF LIST OF SERVICES ++++++
8150964mS RES: Mon 1/9/2014 11:46:26 UsedMem=16302080 MemObjs=0(Max 0) CMMsg=5(5)
Buff=5000 20000 30000 49694 500 Links=111938(160000) BTree=14819 CPU=01.05%
8150964mS RES2: (SE-P) S-Edition Primary 9.1.0.0 build 87 Tasks=36 RTEngine=0
CMRTEngine=0 ExRTEngine=0 Timer=61 Poll=0 Ready=0 CMReady=0 CMQueue=0 VPNNQueue=0
Monitor=2 SSA=0 TCP=26(TLS=6) TAPI=1
```

## Related links

[System Monitor](#) on page 9

---

# The Alarm Log

## About this task

This menu displays the alarms records in the connected system's alarms log. When monitor connects to a system, the trace automatically includes the system's current alarm log at its start.

The alarms cannot be interpreted in the field. However, if a site experiences the same repeated problem, Avaya may request the alarm log details.

The presence of alarms is not necessarily critical as each system keeps a record of the first 8 alarms since the alarm log was last cleared. However, once the alarm log is full, the system ignores additional alarms.

```
3003mS PRN: +++ START OF ALARM LOG DUMP +++
3019mS PRN: ALARM: 18/03/2004 13:07:56 IP 412 2.1(8) CRIT RAISED addr=00000000 d=5
pc=00000000 0082eef0 0094d780 00a13250 00a13638 00a0cb3c
3019mS PRN: ALARM: 22/04/2004 07:26:44 IP 412 2.1(11)CRIT RAISED addr=00000000 d=5
pc=00000000 0095dfe0 0095e278 008b0570 008b0734 008b07b8
3019mS PRN: ALARM: 22/04/2004 07:26:46 IP 412 2.1(11)CRIT RAISED addr=00000000 d=0
pc=00000000 01e75750 01f983d4 0095e278 00000001 01e757f8
3004mS PRN: +++ END OF ALARM LOG DUMP +++
```

## Procedure

1. Click **Status** and select **Alarms**. Monitor displays the alarm records in a separate window.
2. To clear the alarm log, click **Clear Alarms**.















## Related links

[System Monitor](#) on page 9

---

# Monitor Icons

The system monitor window contains a number of icons:

Icon	Uses
 <b>Open File</b>	Open a previous saved monitor log file, see <a href="#">Opening a Log File</a> on page 32. Can also be used to open a Syslog file that has been produced by a system. See <a href="#">Converting Syslog Files</a> on page 81.
 <b>Save Screen Log As</b>	Save the current monitor log to a text file. See <a href="#">Saving the Screen Log as a Log File</a> on page 33.
 <b>Rollover Log</b>	Force the current log file to rollover. Monitor adds the date and time to the log file name and then starts a new log file. See <a href="#">Manually Rolling Over the Log File</a> on page 40.
 <b>Stop Logging</b>	Stop logging to a file. See <a href="#">Stopping File Logging</a> on page 38.
 <b>Start Logging</b>	Start logging to a file. See <a href="#">Starting File Logging</a> on page 37.
 <b>Text Log Files</b>	This icon indicates that monitor is currently set to text or binary file logging. Clicking the icon changes the mode and forces a rollover of the current log file. See <a href="#">Switching Between Binary and Text Logging</a> on page 38.
 <b>Binary Log Files</b>	
 <b>Clear Display</b>	Clear the current log shown in the display.
 <b>Run Screen Display</b>	Show the live monitor log in the display.
 <b>Freeze Screen Logging</b>	Pause the live monitor log in the display. This does not stop the logging to file.
 <b>Reconnect</b>	Connect to the system specified in the <b>Select Unit</b> options. See <a href="#">Reconnecting to the monitored system</a> on page 30.
 <b>Trace Options</b>	Set the filter options for what should be included in the logs.
 <b>Log Preferences</b>	Set the format and destination for the monitor log file.
 <b>Select Unit</b>	Set the details of the system to monitor. See <a href="#">Selecting the system to monitor</a> on page 29.

**Related links**

[System Monitor](#) on page 9

---

## Keyboard Shortcuts

You can use the following keyboard shortcuts with system monitor:

Function	Shortcut
<b>Select Unit</b> See <a href="#">Selecting the system to monitor</a> on page 29.	Ctrl+U
<b>Reconnect</b> See <a href="#">Reconnecting to the monitored system</a> on page 30.	Ctrl+E

*Table continues...*

Function	Shortcut
<b>Open File</b> See <a href="#">Opening a log file</a> on page 32 and <a href="#">Converting syslog files</a> on page 81.	Ctrl+O
<b>Save Screen Log As</b> See <a href="#">Saving the screen log as a log file</a> on page 33.	Ctrl+S
<b>Send to mail recipient</b> See <a href="#">Emailing the screen log</a> on page 31	Ctrl+M
<b>Send to mail recipient as attachment</b> See <a href="#">Emailing the screen log</a> on page 31	Ctrl+H
<b>Rollover Log</b> See <a href="#">Manually rolling over the log file</a> on page 40.	Ctrl+R
<b>Log Preferences</b> See <a href="#">Setting the log preferences</a> on page 36.	Ctrl+L
<b>Clear Display</b> See <a href="#">Clearing the screen log</a> on page 27.	Ctrl+X
<b>Copy the screen log</b> See <a href="#">Copying screen log information</a> on page 32	Ctrl+C
<b>Select All</b> See <a href="#">Copying screen log information</a> on page 32	Ctrl+A
<b>Find</b> See <a href="#">Serching the screen log</a> on page 28	Ctrl+F
<b>IP Calculated (Selected Hex)</b> See <a href="#">Converting IP address hex values</a> on page 29	Ctrl+D
<b>Log to screen (start/pause)</b> See <a href="#">Pausing the screen log</a> on page 27.	Ctrl+G
<b>Start/Stop File Logging</b>	Ctrl+W
<b>Trace Options</b> See <a href="#">Setting a trace options</a> on page 45	Ctrl+T
<b>US PRI Trunk status</b> See <a href="#">US PRI Trunks</a> on page 108	Ctrl+I
<b>Filter screen log</b> See <a href="#">Filtering the screen log</a> on page 28.	F4
<b>Exit</b> See <a href="#">Closing system monitor</a> on page 22	Alt+F4



**Related links**

[System Monitor](#) on page 9

# Chapter 2: Starting System Monitor

When starting monitor, you can select the protocol to be used for the connection. Use of unwanted protocols can be disabled if required for security.

Protocol	Description
<b>UDP</b>	<p>This protocol has a low impact on the system of sending records, especially when a large number of records are being sent.</p> <ul style="list-style-type: none"><li>• This is the preferred protocol if there are no security or bandwidth concerns between the monitor PC and the system being monitored.</li><li>• To capture system resets, <b>UDP</b> is recommended to ensure maximum trace capture necessary to help diagnose the cause of the reset.</li></ul>
<b>TCP</b>	<p>This protocol is supported for IP Office Release 9.0 or higher systems. For low volumes of traffic, this protocol is more reliable for routing across networks than <b>UDP</b>.</p> <ul style="list-style-type: none"><li>• This is the required protocol when using monitor remotely through an Avaya SAL connection.</li></ul>
<b>HTTP/HTTPS</b>	<p>These protocols are supported for IP Office Release 9.1 or higher systems. They are more secure than <b>UDP</b> and <b>TCP</b>. Rather than using the target system's monitor password, these protocols use the name and password of an IP Office service user account configured for monitor use.</p> <ul style="list-style-type: none"><li>• For cloud systems and subscription systems being accessed via Customer Operations Manager, <b>HTTPS</b> on port 8433 must be used.</li></ul>

---


## Connecting to a System using UDP

### About this task

This protocol reduces the impact on the system of sending records, especially when a large number of records are being sent. However, this protocol is not secure. Use of **UDP** can be disabled through the system security settings, see [Disabling UDP/TCP/HTTP Access](#) on page 23.

- To capture system resets, **UDP** is recommended to ensure maximum trace capture necessary to help diagnose the cause of the reset.
- Any Ethernet speed mismatch between the PC running monitor and the system being monitored increases the likelihood of dropped packets. The PC port must match or exceed the speed of the system being monitored. The same problem may also arise from speed differences in any intermediate devices between the PC and the monitored system.

## Procedure

1. Go to **Start > IP Office > Monitor**.
2. If **Monitor** has been previously run, it will attempt to automatically connect with the previous monitored system. Details of the connection are shown in the title bar. If otherwise or if you want to monitor another system, use the steps below.
3. Click on  or select **File > Select Unit**. The **Select System to Monitor** dialog box is displayed.
4. Enter the system details:
  - a. Enter the system's IP address or FQDN without any protocol prefix.
  - b. Set the **Protocol** to **UDP**.
  - c. The **Port**, **Certificate** and **Username** are not used.
  - d. Enter the system's monitor password. See [Setting the Monitor Password](#) on page 23.
  - e. If you want monitor to start with a previously saved set of trace options, use the **Trace Log Settings Filename** browse button to select the trace options file. See [Saving Trace Options as a File](#) on page 42.
5. Click **OK**.
6. Once **Monitor** has connected with a system, it displays the system's status report (see [System Status Report](#) on page 11) and alarm log (see [Alarms](#) on page 84).

---


## Connecting to a System using TCP

### About this task

**TCP** connection is supported for IP Office release 9.0 and higher. In order to use monitor remotely through Avaya SAL, select **TCP**.

However, this protocol is not secure. Use of **TCP** can be disabled through the system's security settings, see [Disabling UDP/TCP/HTTP Access](#) on page 23.

### Procedure

1. Go to **Start > IP Office > Monitor**.
2. If **Monitor** has been previously run, it will attempt to automatically connect with the previous monitored system. Details of the connection are shown in the title bar. If otherwise or if you want to monitor another system, use the steps below.
3. Click on  or select **File > Select Unit**. The **Select System to Monitor** dialog box is displayed.

4. Enter the system details:
  - a. Enter the system's IP address or FQDN without any protocol prefix.
  - b. Set the **Protocol** to **TCP**.
  - c. The **Port**, **Certificate** and **Username** are not used.
  - d. Enter the system's monitor password. See [Setting the Monitor Password](#) on page 23.
  - e. If you want monitor to start with a previously saved set of trace options, use the **Trace Log Settings Filename** browse button to select the trace options file. See [Saving Trace Options as a File](#) on page 42.
5. Click **OK**.
6. Once **Monitor** has connected with a system, it displays the system's status report (see [System Status Report](#) on page 11) and alarm log (see [Alarms](#) on page 84).

---

## Connecting to a System using HTTP


### About this task

**HTTP** and **HTTPS** connections are supported for IP Office Release 9.1 and higher. Using these protocols is more secure.

This type of connection uses the name and password of an IP Office service user who has been configured for monitor access, see [Configuring a service user for monitor access](#) on page 24. By default, only the **Administrator** account is configured for such access.

Use of **HTTP** and **HTTPS** access can be disabled through the system's security settings. See [Disabling UDP/TCP/HTTP Access](#) on page 23.

### Procedure

1. Go to **Start > IP Office > Monitor**.
2. If **Monitor** has been previously run, it will attempt to automatically connect with the previous monitored system. Details of the connection are shown in the title bar. If otherwise or if you want to monitor another system, use the steps below.
3. Click on  or select **File > Select Unit**. The **Select System to Monitor** dialog box is displayed.
4. Enter the system details:
  - a. Enter the system's IP address or FQDN without any protocol prefix.
  - b. Set the **Protocol** to **HTTP**.
  - c. The **Port** defaults to **80**. Change this if a different port is configured in the IP Office system's security settings.
  - d. The **Certificate** field is not used for **HTTP** connections.

- e. In the **Username** field enter the name of the service user account configured for monitor access to the system. In the **Password** field, enter the password for that service user account. Incorrect entry does not disable the account in the same way as for access from IP Office Manager. However, more than 10 incorrect login attempts in a 10 minute period will block further monitor access attempts for a minute.
  - f. If you want monitor to start with a previously saved set of trace options, use the **Trace Log Settings Filename** browse button to select the trace options file. See [Saving Trace Options as a File](#) on page 42.
5. Click **OK**.
  6. Once **Monitor** has connected with a system, it displays the system's status report (see [System Status Report](#) on page 11) and alarm log (see [Alarms](#) on page 84).

---

## Connecting to a System using HTTPS


### About this task

**HTTP** and **HTTPS** connections are supported for IP Office Release 9.1 and higher. Using these protocols is more secure.

This type of connection uses the name and password of an IP Office service user who has been configured for monitor access, see [Configuring a service user for monitor access](#) on page 24. By default, only the **Administrator** account is configured for such access.

Use of **HTTP** and **HTTPS** access can be disabled through the system's security settings. See [Disabling UDP/TCP/HTTP Access](#) on page 23.

### Procedure

1. Go to **Start > IP Office > Monitor**.
2. If **Monitor** has been previously run, it will attempt to automatically connect with the previous monitored system. Details of the connection are shown in the title bar. If otherwise or if you want to monitor another system, use the steps below.
3. Click on  or select **File > Select Unit**. The **Select System to Monitor** dialog box is displayed.
4. Enter the system details:
  - a. Enter the system's IP address or FQDN without any protocol prefix. For subscription systems being accessed via Customer Operations Manager, use the address shown in the system's details in Customer Operations Manager.
  - b. Set the **Protocol** to **HTTPS**.
  - c. The **Port** defaults to **443** (use **8443** for cloud based systems and systems being accessed via Customer Operations Manager). Change this if a different port is configured in the IP Office system's security settings.

- d. Select the **Certificate** that should be used for the connection. To select a certificate, click on the browse button , select the certificate to use and click **OK**. If you do not select a certificate, monitor will auto-generate a self-signed certificate file.
  - e. In the **Username** field enter the name of the service user account configured for monitor access to the system. In the **Password** field, enter the password for that service user account. Incorrect entry does not disable the account in the same way as for access from IP Office Manager. However, more than 10 incorrect login attempts in a 10 minute period will block further monitor access attempts for a minute.
  - f. If you want monitor to start with a previously saved set of trace options, use the **Trace Log Settings Filename** browse button to select the trace options file. See [Saving Trace Options as a File](#) on page 42.
5. Click **OK**.
  6. Once **Monitor** has connected with a system, it displays the system's status report (see [System Status Report](#) on page 11) and alarm log (see [Alarms](#) on page 84).

---

## Closing System Monitor

Closing monitor ends screen and file logging.

1. Click the **X** icon at the top-right of the window. Alternatively, press `Alt+F4` or select **File > Exit**.
2. The application closes and all logging stops.

# Chapter 3: IP Office Security Configuration

Use of monitor to access an IP Office system is configured through that system's security settings. Monitor can use a range of protocols for the connection with a balance between security and performance depending on the protocol chosen.

HTTPS is recommended for security. UDP is recommended for low performance impact but requires leaving an unsecure port open on the system. For full details, refer to the [Avaya IP Office™ Platform Security Guidelines](#) document.



---

## Setting the Monitor Password

### About this task

For UDP/TCP access, monitor uses the **Monitor Password** setting in the target system's security configuration. If no password is set, it uses the **System Password** setting in the same security configuration.

### Procedure

1. Using IP Office Manager, access the IP Office system's security settings.
2. Click  **System** and select the **Unsecure Interfaces** tab.
3. Next to the **Monitor Password**, click **Change**.
  - The **Use Service User Credentials** option can be used to disable the **Monitor Password**. When selected, UDP and TCP access uses the password of any service user configured for monitor access. See [Configuring a service user for monitor access](#) on page 24
4. Enter the existing password, then enter the new password and click **OK**. The default password for a system is blank.
5. Click on the  icon to save the security changes.

---

## Disabling UDP/TCP/HTTP Access



### About this task

UDP/TCP/HTTP access to the IP Office using monitor can be disabled.

 **Important:**

Note that this also disables the interface used by some legacy third-party applications and so also disables their access.

**Procedure**

1. Using IP Office Manager, access the IP Office system's security settings.
2. Click  **System** and select the **Unsecure Interfaces** tab.
3. In the **Application Controls** section, clear **DevLink** check box.
4. Click **OK**.
5. Click on the  icon to save the security changes.

---

## Configuring a Service User for Monitor Access



**About this task**

HTTP or HTTPS access uses the name and password of a service user configured specifically for monitor access. Configuring such a user is done in two parts:


- A security rights group is configured with monitor access.
- Selected service users are made members of that rights group.

**Procedure**


**To configure rights group access:**

1. Using IP Office Manager, access the IP Office system's security settings.
2. Click  **Rights Groups** and then select the rights group that you want to configure. By default the **System Status Group** has monitor access enabled.
3. Select the **System Status** tab.
4. The **SysMonitor Access** option is used to set for the service users who are the members of the rights group and can access a system using System Monitor.
5. Click **OK**.
6. Click on the  icon to save the security changes.

**To configure rights group membership:**

7. Using IP Office Manager, access the IP Office system's security settings.
8. Click  **Service Users** and select the service user.
9. In the **Rights Group Membership** section, ensure that the rights group configured for monitor access is selected.
10. Click **OK**.



- Click on the  icon to save the security changes.

## Adjusting the HTTP Service


### About this task

You can edit the level of security used for HTTP/HTTPS access.


#### Important:

The HTTP service is also used by other IP Office applications.

### Procedure

- Using IP Office Manager, access the IP Office system's security settings.
- Click  **Services** and select **HTTP**.
- The **Service Security Level** is the only setting that can be changed. It controls the unsecure (HTTP) and or secure (HTTPS) access depending on the usage.

Service Security Level	Usage
<b>Disabled</b>	The service and corresponding Transmission Control Protocol (TCP) ports are inactive.
<b>Unsecure Only</b>	Allows only unsecured access to the service. The service's secure TCP port is disabled.
<b>Unsecure + Secure</b>	Allows both unsecured and secure (Low) access.
<b>Secure, Low</b>	Allows secure access to the service using Transport Layer Security (TLS), and demands weaker (for example 3 DES) encryption and authentication or higher.  The service's unsecured TCP port is disabled.
<b>Secure, Medium</b>	Allows secure access to that service using TLS, and demands moderate (for example AES-128) encryption and authentication or higher.  The service's unsecured TCP port is disabled.
<b>Secure, High</b>	Allows secure access to that service using TLS and demands stronger (for example AES-256) encryption and authentication, or higher. In addition, a certificate is required from the client.  The service's unsecured TCP port is disabled.

- Click **OK**.
- Click on the  icon to save the security changes.

# Chapter 4: Using the Screen Log

System Monitor uses its main display area to show records received from the connected system. Alternatively, it can display a previously saved logged file for study.

## Important:

The screen log is limited to approximately 5000 records. If you anticipate logging for a long period or selecting a lot of trace options, you should log to file and then display the file. Large log files can be displayed in a separate text editor.

The records displayed in the screen log are not the raw records as received from the system, instead that are interpreted records. System Monitor applies various changes to aid the interpretation of the records. For example, a record containing the raw entry *pcol=6* is interpreted and displayed as *pcol=6 (TCP)*.


## Related links

- [Pausing the Screen Log](#) on page 27
- [Starting the Screen Log](#) on page 27
- [Clearing the Screen Log](#) on page 27
- [Filtering the Screen Log](#) on page 28
- [Searching the Screen Log](#) on page 28
- [Converting IP Address Hex Values](#) on page 29
- [Selecting the System to Monitor](#) on page 29
- [Reconnecting to the Monitored System](#) on page 30
- [Setting the Trace Options](#) on page 30
- [Viewing the System Alarms](#) on page 30
- [Viewing the Status Menus](#) on page 31
- [Emailing the Screen Log](#) on page 31
- [Opening a Log File](#) on page 32
- [Copying Screen Log Information](#) on page 32
- [Saving the Screen Log as a Log File](#) on page 33
- [Setting the Screen Font](#) on page 33
- [Setting the Screen Background Color](#) on page 33
- [Setting the Trace Colors](#) on page 34
- [Setting the Indenting](#) on page 34
- [Showing the Date and Time](#) on page 35

---

## Pausing the Screen Log

When displaying the trace from a system, you can pause the trace to inspect it. Pausing the screen log does not affect logging to file if that is also running.

1. Click on the  icon. Alternatively, press `Ctrl+G` or select **View > Freeze Screen Logging**.
2. The message `Logging to Screen Stopped` is shown as part of the log.
3. To restart the screen log, see, [Starting the screen log](#) on page 27.

### Related links


[Using the Screen Log](#) on page 26

---

## Starting the Screen Log

The screen log can be paused (see [Pausing the screen log](#) on page 27) . If so, use the following options to restart displaying records received.

When you load a log file for display, any screen logging from a connected system is automatically paused. Restarting the screen log, adds records from the connected system when it is received.

1. Click the  icon at the top-right of the window. Alternatively, press `Ctrl+G` or select **View > Log to Screen**.
2. The warning `Logging to Screen Started` is shown in the log.

### Related links

[Using the Screen Log](#) on page 26

---

## Clearing the Screen Log

You can clear the currently displayed trace:

- Clearing the trace does not affect any trace records logged to a file.
- If the screen log was loaded from a previously saved log file, clearing the trace clears the screen log but does not erase records from the log file.

### To clear the screen log:

1. Click the  icon. Alternatively, press `Ctrl+X` or select **Edit > Clear Display**.

### Related links

[Using the Screen Log](#) on page 26

---

## Filtering the Screen Log

### About this task

The System Monitor displays a filtered summary of the current screen log. You can apply the filter on any selected part of the existing screen log, for example an IP address or on extension number. The System Monitor displays the filtered log as a separate window and you can save to a text file.

### Procedure

#### To display a filtered screen log:

1. Using the cursor, highlight the part of the current screen log that you want use as filter. If necessary, pause the screen to select (see [Pausing the Screen Log](#) on page 27).
2. Press **F4**. Monitor displays a separate window containing the records that match to the filter.

#### To save a filtered screen log:

3. In the filtered log window, click **File** and select **Save As**.
4. Enter a file name or select an existing file to overwrite.
5. Click **Save**.

#### To copy the filtered screen log:

6. In the filtered log window, select the filter records that you want to copy.
7. Click **File** and select **Copy**.

### Related links

[Using the Screen Log](#) on page 26

---

## Searching the Screen Log

### About this task

You can search the screen log for records that contain text that match the search string you specify.

#### **Tip:**

Selecting a piece of text in the screen log before starting a search, automatically makes the selected text the search string.

### Procedure

1. Click **Edit** and select **Find**. Alternatively, press **Ctrl+F**.
2. Enter the search string for that you want to search on the screen log.

3. Click **Find Next** to find the first match.
4. Click **Find Next** again to find the next match.

#### Related links

[Using the Screen Log](#) on page 26

---

## Converting IP Address Hex Values

### About this task

Some values displayed in the screen log are hex values. These are indicated by a `0x` prefix to the number. Typically these are IP addresses. Monitor can display the converted value. For example, `0xff` becomes `0.0.0.255`.

### Procedure

1. In the screen log, select and highlight the value to be converted. You can include the `0x` prefix in the selection.
2. Press `Ctrl+D`. Alternatively, select **Edit > IP Calculated (Selected Hex)**.

#### Related links

[Using the Screen Log](#) on page 26


---

## Selecting the System to Monitor

### About this task

While monitoring a system or viewing a log file, you can switch to receiving and displaying the log records from another system.

### Procedure

1. Click on the  icon. Alternatively, press `Ctrl+U` or select **File > Select Unit**.
2. Follow the methods of connection you want to use:
  - [Connecting to system using UDP](#) on page 18
  - [Connecting to system using TCP](#) on page 19
  - [Connecting to system using HTTP](#) on page 20
  - [Connecting to system using HTTPS](#) on page 21


#### Related links

[Using the Screen Log](#) on page 26

---

## Reconnecting to the Monitored System

Monitor automatically attempts to reconnect to a system when it detects that the connection has been lost. However, if necessary you can manually select to reconnect.

1. Click on the  icon. Alternatively, press `Ctrl+E` or select **File > Reconnect**.
2. When reconnected with the system, its [Status Report](#) on page 11 and [Alarms](#) on page 84 reports are displayed.

### Related links

[Using the Screen Log](#) on page 26

---

## Setting the Trace Options

The output received from a system can include records of almost all system activity. This can make it difficult to find just those details needed to diagnose a particular issue. Therefore, monitor allows you to select which types of records to include in the current screen log and file logging. See [Setting the Trace Options](#) on page 42.

### Related links

[Using the Screen Log](#) on page 26

---

## Viewing the System Alarms

### About this task

This menu displays the alarms records in the connected system's alarms log. When monitor connects to a system, the trace automatically includes the system's current alarm log at its start.

The alarms cannot be interpreted in the field. However, if a site experiences the same repeated problem, Avaya may request the alarm log details.

The presence of alarms is not necessarily critical as each system keeps a record of the first 8 alarms since the alarm log was last cleared. However, once the alarm log is full, the system ignores additional alarms.

```
3003mS PRN: +++ START OF ALARM LOG DUMP +++
3019mS PRN: ALARM: 18/03/2004 13:07:56 IP 412 2.1(8) CRIT RAISED addr=00000000 d=5
pc=00000000 0082eef0 0094d780 00a13250 00a13638 00a0cb3c
3019mS PRN: ALARM: 22/04/2004 07:26:44 IP 412 2.1(11)CRIT RAISED addr=00000000 d=5
pc=00000000 0095dfe0 0095e278 008b0570 008b0734 008b07b8
3019mS PRN: ALARM: 22/04/2004 07:26:46 IP 412 2.1(11)CRIT RAISED addr=00000000 d=0
pc=00000000 01e75750 01f983d4 0095e278 00000001 01e757f8
3004mS PRN: +++ END OF ALARM LOG DUMP +++
```

### Procedure

1. Click **Status** and select **Alarms**. Monitor displays the alarm records in a separate window.

2. To clear the alarm log, click **Clear Alarms**.

**Related links**

[Using the Screen Log](#) on page 26

---

## Viewing the Status Menus

In addition to the screen log, monitor can display a number of different status screens for different aspects of system operation.

1. Click **Status** and select the status screen required. See [Status Screens](#) on page 83.

**Related links**

[Using the Screen Log](#) on page 26

---

## Emailing the Screen Log

**About this task**

You can use the default email application configured on the PC to send an email copy of the current screen log. You can send an email with the screen log either automatically pasted into the email text or attached as a separate `txt` file. Attaching it as a file allows the recipient to easily load the file back into their copy of monitor.

**Procedure**

1. Click **File > Send To** and then
2. Selection either:
  - Select **Mail Recipient**. The default email application displays a new email with the screen log pasted into the message text.
  - Select **Mail Recipient as Attachment**. The default email application displays a new email with the screen log pasted into the message text.
3. Complete the email details and click **Send**.

**Related links**

[Using the Screen Log](#) on page 26


---

## Opening a Log File

### About this task

You can open and view an existing log file. Opening a log file automatically pauses the display of the screen log from any connected system.

### Procedure

1. Click on the  icon. Alternatively, press `Ctrl+O` or select **File > Open**.
2. Browse to select the log file.
  - You can select more than one file; the contents are concatenated in the monitor display.
  - Different file extensions are used for different types of log file. Either select the file from the files shown or use the **Files of type** drop-down list to filter the files shown to a particular type:
    - **Text Log Files** – A `.txt` file containing plain text logging.
    - **Binary Log Files** – A `.mon` file containing binary logging.
    - **Syslog Files** – A `.log` file containing Syslog monitor records. See [Syslog tracing](#) on page 75.
    - **Zipped Files** – A `.zip` zipped file containing multiple log files.
3. Click **Open**.
4. For a `.zip` file, you are prompted for a password. Enter the password if one was set and click **OK**.

### Related links

[Using the Screen Log](#) on page 26

[Logging to a File](#) on page 36

---

## Copying Screen Log Information

### About this task

You can copy and paste the information shown in the screen log using the standard Windows methods.

### Procedure

1. Using the cursor, select the section of the screen log to copy or press `Ctrl+A` to select the whole screen log.
2. Press `Ctrl+C` to copy the selected portion of the screen log.

### Related links

[Using the Screen Log](#) on page 26



---


## Saving the Screen Log as a Log File

### About this task

You can save the screen log as a text log file.

To open a binary log file and then save it as a plain text log file can be problematic if the file contains a very large number of records. If a plain text copy of a binary log file is required, see [Converting a Binary Log to a Text Log](#) on page 40.

### Procedure

1. Click on the  icon. Alternatively, press `Ctrl+S` or select **File > Save Screen Log As**.
2. Enter a file name for the file.
3. Click **Save**.

### Related links

[Using the Screen Log](#) on page 26

[Logging to a File](#) on page 36

---

## Setting the Screen Font

### About this task

You can select the default font used for displaying the logs.

### Procedure

1. Click **View** and select **Font** .
2. Select the required font settings.
3. Click **OK**.

### Related links

[Using the Screen Log](#) on page 26

---

## Setting the Screen Background Color

### About this task

You can select the color used for the background of the screen log.

### Procedure

1. Click **View** and select **Background Colour** .
2. Select the color required.

3. Click **OK**.

#### Related links

[Using the Screen Log](#) on page 26


---

## Setting the Trace Colors

### About this task

When applying trace options, you can select a particular color for the options to make them easier to spot in the screen log.

### Procedure

1. Click on the  icon. Alternatively, press `Ctrl+T` or select **Filters > Trace Options**.
2. Select the tab showing the trace option for which you want a specific color applied.
3. Right click on the name of the trace option.
4. Select the required color.
5. Click **OK**.

#### Related links

[Using the Screen Log](#) on page 26

---

## Setting the Indenting

### About this task

To support the reading of the monitor trace and to import into other applications, you can adjust the indentation applied to the records.

### Procedure

1. Click **View** and select **Formatting**.
2. Use the controls to adjust the indentation applied to the packets of information shown on each line.
3. Click **OK**.

#### Related links

[Using the Screen Log](#) on page 26


---

# Showing the Date and Time

## About this task

Every record shown in the screen trace and recorded in the a log is prefixed with the number of milliseconds since the system last rebooted. You can also prefix it with the current system date and/or time.

## Procedure

1. Click on the  icon. Alternatively, press `Ctrl+T` or select **Filters > Trace Options**.
2. Select **System** tab.
  - To add the date, select **Prefix YYYY-M-DD**.
  - To add the time, select **Prefix hh:mm:ss**.
3. Click **OK**.

## Related links

[Using the Screen Log](#) on page 26

# Chapter 5: Logging to a File

In addition to displaying records in the screen log, monitor can copy records into a log file. You can view log files at a later time or send them for analysis by another person.

## Related links

- [Setting the Log Preferences](#) on page 36
- [Starting File Logging](#) on page 37
- [Stopping File Logging](#) on page 38
- [Switching Between Binary and Text Logging](#) on page 38
- [Adding Log Stamps](#) on page 38
- [Opening a Log File](#) on page 32
- [Saving the Screen Log as a Log File](#) on page 33
- [Manually Rolling Over the Log File](#) on page 40
- [Converting a Binary Log to a Text Log](#) on page 40


---


## Setting the Log Preferences

### About this task

These settings set where monitor stores log files and checks for a new log file.

### Procedure

1. Click on the  icon. Alternatively, press `Ctrl+L` or select **File > Log Preferences**.
2. Select the required **Log Mode**. This setting controls how often monitor saves the current log file and starts a new file.

Log Mode option	Description
<b>Periodic</b>	Only rollover the log when the  icon is pressed. See <a href="#">Manually Rolling Over the Log File</a> on page 40.
<b>Daily</b>	Rollover the log automatically at the end of each day.
<b>Every 'n' hours</b>	Rollover the log automatically every few hours. When selected, the settings includes an <b>Hours Interval</b> box to set the number of hours between rollovers.

Log Mode option	Description
Every 'n' MBytes	Rollover the log automatically when it reaches a set size. When selected, the settings includes a <b>MBytes Interval</b> box to set the size limit.

3. Browse to set the log file location. The default location is the application program folder (by default C:\Program Files (x86)\Avaya\IP Office\Monitor). Each time file logging stops or rolls over, monitor adds the date and time to the log file name.
4. Select the log format required by selecting **Binary Logging** or not:
  - **Binary Log Files** – This is the raw format of records as received from the system. The records are not processed in any way by monitor other than being added to the log file. The file extension used is `.mon`.
  - **Text Log Files** – This is the interpreted format of records. Monitor adds additional information, for example, a record containing the raw entry `pcol=6` is changed to `pcol=6 (TCP)`. The file extension used is `.txt`.
    - When logging in text format or running the screen log, it is possible for some records to be lost due to the high number of packets that monitor has to interpret. Running a binary log and pausing the screen log reduces the chances of such lost packets.
5. You can select whether you want the log file zipped into a password protected `.zip` file. To do that, select **Enable Zip** and enter a password of at least four characters.
6. To start logging to file immediately, select **Log to File**. If not selected, you can start logging to file manually when required, see [Starting File Logging](#) on page 37.
7. Click **OK**.



#### Related links

[Logging to a File](#) on page 36

---

## Starting File Logging

You can manually start logging to file if file logging is not already running.

1. Click the  icon. Alternatively, press `Ctrl+W`.
  - The records are logged to file using the settings defined for the log preferences. See [Setting the Log Preferences](#) on page 36.
  - The icon changes  that can be used to stop logging. See [Stopping File Logging](#) on page 38.



#### Related links

[Logging to a File](#) on page 36

---

## Stopping File Logging

You can stop the file logging at any time. When logging is stopped, the log file is saved in the folder specified in the log preferences with the date and time appended to the file name.

1. Click the  icon. Alternatively, press `Ctrl+W`.
  - The icon changes to  that can be used to start logging. See [Starting File Logging](#) on page 37.

### Related links

[Logging to a File](#) on page 36

---



## Switching Between Binary and Text Logging

### About this task

You can switch logging between using binary or text formats. Switching format automatically rolls over the current log file.

- **Binary Log Files** – This is the raw format of records as received from the system. The records are not processed in any way by monitor other than being added to the log file. The file extension used is `.mon`.
- **Text Log Files** – This is the interpreted format of records. Monitor adds additional information, for example, a record containing the raw entry `pcol=6` is changed to `pcol=6 (TCP)`. The file extension used is `.txt`.
  - When logging in text format or running the screen log, it is possible for some records to be lost due to the high number of packets that monitor has to interpret. Running a binary log and pausing the screen log reduces the chances of such lost packets.

### Procedure

1. The  icon indicates that binary logging is being used, the  icon, text logging.
2. To change the mode, click on the icon.
3. The current file logging is stopped and a new log file started using the new format.

### Related links

[Logging to a File](#) on page 36

---

## Adding Log Stamps

Using their phone, system users can access a log stamp function. This allows them to insert a log stamp event into the system's monitor records. They can use these to indicate when an issue that you are trying to capture has occurred.

The log stamp record is prefixed with **LSTMP: Log Stamped** and a log stamp number. It also the date and time plus the user name and extension of the user who triggered the log stamp function.

The log stamp number starts from 000 whenever the system is restarted. Each time the log stamp function is used, the number is incremented in a cycle from 000 to 999. However, a specific log stamp number can be assigned to a button or short code used to trigger the function. When triggered, the user's phone briefly displays the log stamp number.

A default system short code, \*55, is automatically added to new systems. For users with appropriate telephones, the log stamp function can also be assigned to a programmable button on the phone using the **Advanced > Miscellaneous > Stamp Log**.

- When the event to be marked occurs, dial \*55. If already on a call, put that call on hold and then dial \*55.

#### Related links

[Logging to a File](#) on page 36


---

## Opening a Log File

### About this task

You can open and view an existing log file. Opening a log file automatically pauses the display of the screen log from any connected system.

### Procedure

1. Click on the  icon. Alternatively, press **Ctrl+O** or select **File > Open**.
2. Browse to select the log file.
  - You can select more than one file; the contents are concatenated in the monitor display.
  - Different file extensions are used for different types of log file. Either select the file from the files shown or use the **Files of type** drop-down list to filter the files shown to a particular type:
    - **Text Log Files** – A `.txt` file containing plain text logging.
    - **Binary Log Files** – A `.mon` file containing binary logging.
    - **Syslog Files** – A `.log` file containing Syslog monitor records. See [Syslog tracing](#) on page 75.
    - **Zipped Files** – A `.zip` zipped file containing multiple log files.
3. Click **Open**.
4. For a `.zip` file, you are prompted for a password. Enter the password if one was set and click **OK**.

#### Related links

[Using the Screen Log](#) on page 26

[Logging to a File](#) on page 36

---


## Saving the Screen Log as a Log File

### About this task

You can save the screen log as a text log file.

To open a binary log file and then save it as a plain text log file can be problematic if the file contains a very large number of records. If a plain text copy of a binary log file is required, see [Converting a Binary Log to a Text Log](#) on page 40.

### Procedure

1. Click on the  icon. Alternatively, press `Ctrl+S` or select **File > Save Screen Log As**.
2. Enter a file name for the file.
3. Click **Save**.

### Related links


[Using the Screen Log](#) on page 26

[Logging to a File](#) on page 36

---

## Manually Rolling Over the Log File

You can force monitor to rollover the current log file at anytime. You can do this even if it is already set to automatically rollover the file.

1. Click on the  icon. Alternatively, press `Ctrl+R` or select **File > Rollover Log**.
2. Monitor saves the existing log file by adding the time and date to its file name and then starts a new log file.

### Related links

[Logging to a File](#) on page 36

---

## Converting a Binary Log to a Text Log







### About this task

You can use monitor to view binary log files (`.mon` files). However, it may sometimes be necessary to create a plain text copy of the log file so that it can be viewed in other applications.

Whilst you can save the current screen log to a text file at any time, this can be potentially problematic if a very large number of records have been displayed. Even if the procedure to convert a binary log to a text log is complex, it ensures that no records are lost.



## Procedure

1. Click on the  icon. Alternatively, press `Ctrl+G` or select **View > Freeze Screen Logging**.
2. Clear any existing contents in the screen log by clicking the  icon.
3. Configure monitor to a non-existent IP address.
  - a. Click the  icon or press `Ctrl+U`.
  - b. Enter an IP address that is not used.
  - c. Click **OK**.
4. Set monitor to capture the screen log records as they appear into a plain text log file.
  - a. Click on the  icon. Alternatively, press `Ctrl+L` or select **File > Log Preferences**.
  - b. Set the **Log Mode** to **Daily**.
  - c. Ensure the **Binary Logging** is not selected.
  - d. Select the **Log to File** option.
  - e. Click **OK**.
5. Open the binary log file:
  - a. Click on the  icon. Alternatively, press `Ctrl+O` or select **File > Open**.
  - b. Browse to and select the log file.
  - c. Click **Open**.
6. The file opens in the screen log. Due to the log preferences selected, as monitor adds each binary log file record to the screen log, it also writes the record into the plain text log file.
7. Once the binary log file has been fully loaded, rollover the log file. Click on the  icon. Alternatively, press `Ctrl+R` or select **File > Rollover Log**.

## Related links

[Logging to a File](#) on page 36

# Chapter 6: Setting the Trace Options

The trace options settings affect what type of records are included in both the screen log and logging to file.


## Related links

- [Setting the Trace Options](#) on page 42
- [Saving Trace Options as a File](#) on page 42
- [Loading trace options from a file](#) on page 43
- [Coloring Individual Trace Options](#) on page 43
- [Coloring Tab Trace Options](#) on page 44
- [Clearing a Trace Options Tab](#) on page 44
- [Setting a Trace Options Tab](#) on page 45
- [Clearing All the Trace Options](#) on page 45
- [Defaulting the Trace Options](#) on page 45

---

## Setting the Trace Options

### Procedure

1. Click on the  icon. Alternatively, press `Ctrl+T` or select **Filters > Trace Options**.
2. Click the setting to enable or disable it.
3. Click **OK**.

## Related links

- [Setting the Trace Options](#) on page 42

---

## Saving Trace Options as a File


### About this task

The current set of trace options settings can be exported to an `.ini` file. You can then reload the settings from the file or send the file to another user to set the saved trace options settings for their application. See [Loading trace options from a file](#) on page 43.

**\* Note:**

Monitor does not save trace option color settings as part of the trace options file.

**Procedure**

1. Click on the  icon. Alternatively, press `Ctrl+T` or select **Filters > Trace Options**.
2. Select **Save File**.
3. Enter the name for the file and select the location or select an existing file to overwrite.
4. Click **Save**.

**Related links**

[Setting the Trace Options](#) on page 42


---

## Loading trace options from a file

**About this task**

You can import a previously saved set of trace options settings as a file. See [Saving Trace Options as a File](#) on page 42.

**Procedure**

1. Click on the  icon. Alternatively, press `Ctrl+T` or select **Filters > Trace Options**.
2. Select **Load File**.
3. Locate and select the file to load.
4. Click **Open**.

**Related links**

[Setting the Trace Options](#) on page 42


---

## Coloring Individual Trace Options

**About this task**

You can select a color for a particular type of trace option. Monitor then applies the selected color to any matching records shown in the screen log.

**Procedure**

1. Click on the  icon. Alternatively, press `Ctrl+T` or select **Filters > Trace Options**.
2. Select the tab displaying the trace option for which you require a specific color.
3. Right-click on the name of the trace option.

4. Select the required color.
5. Click **OK**.

**Related links**

[Setting the Trace Options](#) on page 42


---

## Coloring Tab Trace Options

### About this task

For some tabs (**Call**, **H.323** and **System**), rather than applying colors to individual trace options (see [Coloring Individual Trace Options](#) on page 43), a single color selection can be applied for all options on the tab.

### Procedure

1. Click on the  icon. Alternatively, press `Ctrl+T` or select **Filters > Trace Options**.
2. Select the required tab.
3. Click on **Trace Colour**.
4. Select the required color.
5. Click **OK**.

**Related links**

[Setting the Trace Options](#) on page 42


---

## Clearing a Trace Options Tab

### About this task

You can clear all the currently selected trace options on the currently displayed tab.

### Procedure

1. Click on the  icon. Alternatively, press `Ctrl+T` or select **Filters > Trace Options**.
2. Select the tab that you want to clear.
3. Click **Tab Clear All**.

**Related links**

[Setting the Trace Options](#) on page 42


---

## Setting a Trace Options Tab

### About this task

You can set all the options on the currently displayed trace options tab.

### Procedure

1. Click on the  icon. Alternatively, press `Ctrl+T` or select **Filters > Trace Options**.
2. Select the tab on which you want to set all the options.
3. Click **Tab Set All**.

### Related links

[Setting the Trace Options](#) on page 42


---

## Clearing All the Trace Options

### About this task

You can clear all selected trace options.

### Procedure

1. Click on the  icon. Alternatively, press `Ctrl+T` or select **Filters > Trace Options**.
2. Click **Clear All**.
3. To continue, click **Yes**.

### Related links

[Setting the Trace Options](#) on page 42


---

## Defaulting the Trace Options

### About this task

You can set the trace options to store default settings. This enables you to set selected trace options and the trace option color settings to default.

### Procedure

1. Click on the  icon. Alternatively, press `Ctrl+T` or select **Filters > Trace Options**.
2. Click **Default All**.
3. To continue defaulting the trace options, click **Yes**. The defaults are listed below. Tabs not listed default to all options off.

Tab	Default Selected Trace Options
Call	Call, Call Delta, Call Logging, Extension, Targeting, ARS, LRQ, Extension Send, Extension Receive, Extension TxP, Extension RxP, Line Send, Line Receive, Sort IEs.
Frame Relay	Frame Relay Events, Management Events.
H.323	H.232 (Also automatically colored pink).
Interface	Interface Queue, TCP, UDP, ARP, MultiCast.
ISDN	Layer 1, Layer 2, Layer 3.
Media	Map.
PPP	Err Msg.
R2	CAS, Channel, Dialler, DSP, Line.
SIP	STUN, SIP Rx, SIP Tx.
System	Error, Print, Prefix hh:mm:ss, Resource Status Prints, Licensing.
VPN	Security Engine: Regs on H/W Cmd Error. SSL VPN: Session and Session State.
WAN	WAN Events.

**Related links**

[Setting the Trace Options](#) on page 42

# Chapter 7: Trace Option Menus

The trace options are grouped onto the following tabs:

Menu	Description
<b>ATM</b>	Monitor analog trunk traffic and events.
<b>Call</b>	Monitor extensions and calls.
<b>Directory</b>	Monitor LDAP traffic and events.
<b>DTE</b>	Monitor the system's DTE port.
<b>EConf</b>	Monitor IP Office Conferencing Center events.
<b>Frame Relay</b>	Monitor Frame Relay traffic and events.
<b>GOD</b>	Monitor messages between the modules in a system.
<b>H.323</b>	Monitor H.323 VoIP calls.
<b>Interface</b>	Monitor IP data interfaces such as NAT and the Firewall.
<b>ISDN</b>	Monitor ISDN traffic and events.
<b>Jade</b>	For Linux-based systems, monitor the call media services.
<b>Key/Map</b>	Monitor appearance functions.
<b>Media</b>	Monitor the media support provided by the system.
<b>PPP</b>	Monitor PPP traffic and events.
<b>R2</b>	Monitor R2 trunk traffic and events.
<b>Routing</b>	Monitor IP traffic and events.
<b>SCN</b>	Monitor Small Community Network traffic and information.
<b>Services</b>	Monitor traffic and events for IP Office services like DHCP, DNS, HTTP, TAPI, Telnet, Time, TFTP, SMTP, SNMP, Web Services.
<b>SIP</b>	Monitor SIP trunks and connections.
<b>SSI</b>	Monitor the system's SSI connections.
<b>System</b>	Monitor internal events.
<b>T1</b>	Monitor T1 traffic and events.
<b>VComp</b>	Monitor the system's voice compression channels.
<b>VPN</b>	Monitor VPN events.
<b>WAN</b>	Monitor WAN traffic and events.

## Related links

[ATM Trace Options](#) on page 48

- [Call Trace Options](#) on page 49
- [CTI Trace Options](#) on page 51
- [Directory Trace Options](#) on page 52
- [DTE Trace Options](#) on page 53
- [EConf Trace Options](#) on page 54
- [Frame Relay Trace Options](#) on page 54
- [GOD Trace Options](#) on page 55
- [H.323 Trace Options](#) on page 56
- [Interface Trace Options](#) on page 57
- [ISDN Trace Options](#) on page 58
- [Jade Trace Options](#) on page 60
- [Key/Lamp Trace Options](#) on page 61
- [Media Trace Options](#) on page 61
- [PPP Trace Options](#) on page 62
- [R2 Trace Options](#) on page 63
- [Routing Trace Options](#) on page 64
- [SCN Trace Options](#) on page 65
- [Services Trace Options](#) on page 66
- [SIP Trace Options](#) on page 67
- [SSI Trace Options](#) on page 68
- [T1 Trace Options](#) on page 69
- [System Trace Options](#) on page 69
- [VComp Trace Options](#) on page 71
- [VPN Trace Options](#) on page 72
- [WAN Trace Options](#) on page 74

---

## ATM Trace Options

This tab provides trace options for monitoring the system's analog trunks.

Option	Description
<b>Channel</b>	Log information relating to the Analog Trunk state machine.
<b>CM Line</b>	Log information relating to the interaction between the line handler and the Call Manager (CM).
<b>I/O</b>	Log events on the line or in the DSP.

### Default Settings

None of the trace options are enabled by default. See [Defaulting the Trace Options](#) on page 45.



**Related links**

[Trace Option Menus](#) on page 47

---

## Call Trace Options

This tab provides trace options for monitoring the system's calls including the use of voicemail.

**Events**

Events	Description
<b>Call</b>	Log changes of state for the call (Aend and Bend).
<b>Call Delta</b>	Log information on general call state changes.
<b>Call Delta 2</b>	Log information on additional call state changes.
<b>Call Logging</b>	Log <b>ACD</b> status messages, <b>CALL</b> message giving statistics of call and <b>SERVICE</b> message giving statistics of service.
<b>Extension</b>	Log changes of state for the extension plus console print on setting bchan.
<b>Extension Cut</b>	Log changes of cut state for the extension (mapping connections).
<b>Line</b>	Currently this option does not provide any trace messages. It is included for possible future use only.
<b>MonCM</b>	Log all received call control messages (NOT Short Code messages) and some additional console print messages such as <code>adjustcount</code> and <code>ringback</code> .
<b>MonIVR</b>	Log update information on the messages in a user's voicemail box.
<b>Targeting</b>	Log information concerning call routing (targeting).
<b>ARS</b>	–
<b>LQR</b>	–
<b>ACD</b>	–
<b>IP Dect</b>	–
<b>Call Detail Records</b>	–
<b>CDR Extra Diganostics</b>	–

**Packets**

Packets	Description
<b>Call</b>	Log all received call control messages and contents.
<b>Extension Send</b>	Log all call control messages and contents transmitted to an extension.
<b>Extension Receive</b>	Log all call control messages and contents received from an extension.

*Table continues...*

Packets	Description
<b>Extension TxC</b>	Log all call control messages and contents transmitted to the call object. This message is actually received from the extension.
<b>Extension RC</b>	Log all call control messages and contents received from the call object. This message is actually sent to the extension.
<b>Extension TxP</b>	Log all call control messages and contents transmitted to a partner application (for example SoftConsole). Also enables <code>CMExtnCopyProcessMsg</code> <code>CMExtnCopyProcessCallMsg</code> <code>CMExtnConfCopyProcessCallMsg</code> <code>CMExtnCopySendCallMsg</code> and <code>CMExtnCopyCallLostMsg</code> and messages.
<b>Extension RxP</b>	Log all call control messages and contents received from a partner application such as IP Office SoftConsole.
<b>Line Send</b>	Log all call control messages and contents sent to a line. Also enables <code>CMCallReleaseStart</code> <code>CMCallReleaseEnd</code> and <code>CMCallLostRecord</code> Timeout and messages.
<b>Line Receive</b>	Log all call control messages and contents received from a line. Also enables Incoming Call Waiting CallRefused Incoming Blocked and CallRefused and because channels are in use messages.
<b>Short Code Msgs</b>	Log short code messages associated with the selected <b>Extension Send</b> , <b>Extension Receive</b> and <b>MonCM</b> trace options.
<b>Supplementary services</b>	–
<b>IP Dect Msgs</b>	–
<b>Sort IEs</b>	If selected, sort the order of line alerting and connected events when displayed in the screen log. The order of line alerting and connected events varies depending on whether the system is transmitting or receiving. That makes it difficult to compare side by side traces of calls between two systems. This settings only affects those events that are sorted when displayed in the screen log and does not affect the order of the recorded log file.

### Embedded voicemail

Option	Description
<b>Voicemail Client</b>	–
<b>Audio Response</b>	–
<b>Message Recorder</b>	–
<b>Housekeeping</b>	–
<b>Flash Storage</b>	–
<b>Silence</b>	–
<b>Email</b>	–

## PC voicemail

Option	Description
Voicemail Events	–
Voicemail Messaging	–

### Trigger string detection

These options are only available when the **Development Tracing** option is selected in the **Filters > Trace Options > System** menu, see [System Trace Options](#) on page 69. They are not covered by this document as they are used by Avaya for product trials and are subject to frequent changes.

These options should only be used under the guidance of an authorized Avaya development engineer.

Option	Description
Call Log	–
Print	–
Auto Rollover	–
Allow Multiple Rollovers	–

### Trace Color

This option allows selection of a color that is then applied to all options in the menu, see [Coloring Tab Trace Options](#) on page 44. This selection overrides any previous color selected for individual options. However, it does not prevent subsequent individual option coloring, see [Coloring Individual Trace Options](#) on page 43.

### Default settings

The following trace options are enabled by default. See [Defaulting the Trace Options](#) on page 45.

- **Call, Call Delta, Call Logging, Extension, Targeting, ARS, LRQ, Extension Send, Extension Receive, Extension TxP, Extension RxP, Line Send, Line Receive, Sort IEs.**

### Related links

[Trace Option Menus](#) on page 47

---

## CTI Trace Options

This tab provides trace options for monitoring various external application services provided by the system.

Option	Description
<b>TAPI</b>	Log TAPI (Telephony Application Programming Interface) messages. <ul style="list-style-type: none"> <li>• <b>TAPI Call Log</b>: If selected, this option logs TAPI Call Log messages.</li> <li>• <b>TAPI Line</b>: If selected, this option logs TAPI Line messages.</li> <li>• <b>TAPI Onex Resiliency</b></li> <li>• <b>TAPI Raw Tx</b></li> <li>• <b>TAPI Raw Rx</b></li> </ul>
<b>WebRTC SDP Tx</b>	
<b>WebRTC SDP Rx</b>	
<b>MTCTI Tx</b>	
<b>MTCTI Rx</b>	
<b>MTCTI Events</b>	
<b>CTI1</b>	
<b>CTI3</b>	

### Default Settings

None of the trace options are enabled by default. See [Defaulting the Trace Options](#) on page 45.

### Related links

[Trace Option Menus](#) on page 47

---

## Directory Trace Options

This tab provides trace options settings to monitor the system's directory requests.

### Events

Events	Description
<b>LDAP Events</b>	Log information on the status of the system's LDAP software state machine and associated events.
<b>Directory Events</b>	

### Packets

Use the following options with caution as they produce a prolific amount of records. For both, if **Packets In** (see [Interface](#) on page 57) is also selected, monitor also adds the packet information to the end of the record.

Events	Description
<b>LDAP Tx</b>	Log a breakdown of any transmitted LDAP data packets.
<b>LDAP Rx</b>	Log a detailed breakdown of any received LDAP data packets.

## Default Settings

None of the trace options are enabled by default. See [Defaulting the Trace Options](#) on page 45.

### Related links

[Trace Option Menus](#) on page 47

---

## DTE Trace Options

This tab provides trace options for monitoring the system's DTE port.

### Events

Events	Description
<b>DTE Events</b>	Log the status of Flow Control, Modem Controls (Data Terminal Ready (DTR), Data Carrier Detect (DCD)), baud rate changes on the DTE port, and so on.

### Packets

Packets	Description
<b>DTE Command Tx</b>	Log the Hayes AT commands send out of the DTE interface.
<b>DTE Command Rx</b>	Log the Hayes AT commands received from the DTE interface.
<b>DTE Filter Tx</b>	Log serial data transmitted out of the DTE interface once connected.
<b>DTE Filter Rx</b>	Log serial data received from the DTE interface once connected.
<b>DTE PPP Tx</b>	Log Framed Point-to-Point Protocol (PPP) packets Transmitted to the DTE interface if the Hayes ATB0 option is set on the port.
<b>DTE PPP Rx</b>	Log Framed PPP packets received from the DTE interface if the Hayes ATB0 option is set on the port.
<b>DTE V110 Tx</b>	Log Framed V.110 packets received from the DTE interface if the Hayes ATB3 option is set on the port.
<b>DTE V110 Rx</b>	Log Framed V.110 packets received from the DTE interface if the Hayes ATB3 option is set on the port.
<b>DTE V120 Tx</b>	Log Framed V.120 packets received from the DTE interface if the Hayes ATB2 option is set on the port.
<b>DTE V120 Rx</b>	Log Framed V.120 packets received from the DTE interface if the Hayes ATB2 option is set on the port.

## Default Settings

None of the trace options are enabled by default. See [Defaulting the Trace Options](#) on page 45.

### Related links

[Trace Option Menus](#) on page 47

---

## EConf Trace Options

This tab provides trace options for monitoring the IP Office conferencing services.

### Events

Option	Description
<b>Session</b>	Log incoming and outgoing messages to/from the conferencing server. It also shows the session being established between the system and the conferencing server.
<b>Api</b>	Log state changes of the various EConf resources used.
<b>Targets</b>	Log the targeting information, as calls try to enter an enhanced conference.
<b>Conf</b>	Log events happening to <i>CMConference</i> object. It displays information on the creation/deletion of conferences, as well as calls being added or removed.
<b>Vmail</b>	Log information on the call as it arrives at the system from the voicemail server. It displays the GUID's that the server has given for the calls transfer into the conference and it shows the voicemail server making announcements into the conference.

### Packets

Option	Description
<b>Vmail Tx</b>	Log messages which show the contents of IP packets transmitted to the voicemail server that are specifically associated with the IP Officeconferencing centre.
<b>Vmail Rx</b>	Log messages which show the contents of IP packets received from the voicemail server that are specifically associated with the IP Officeconferencing centre.

### Report

The **Report** button gives details of the state of all the resources in the **EConf** system. It displays the states of all the **EConferences**, **EChannels**, **CMConferences** and **CMCalls** that are associated with at that time. It also displays the number of free reserved resources that are available.

When the **Report** button is clicked, a series of PRN traces are output to the log. Note that the **Print** option (see, [System Trace Options](#) on page 69) must be enabled.

### Default Settings

None of the trace options are enabled by default. See [Defaulting the Trace Options](#) on page 45.

### Related links

[Trace Option Menus](#) on page 47

---

## Frame Relay Trace Options

This tab provides trace options for monitoring the system's frame relay services.

## Events

Option	Description
<b>Frame Relay Events</b>	Log Frame Relay events be it data in, data out, management, status and so on.
<b>Management Events</b>	Log Management events/packets, that is SE/FSE packets and management status.

## Packets

Option	Description
<b>Tx Data</b>	Log transmitted packets on a Frame Relay link - both data and management.
<b>Rx Data</b>	Log received packets on a Frame Relay link - both data and management.

## Default Settings

The following trace options are enabled by default. See [Defaulting the Trace Options](#) on page 45.

- **Frame Relay Events, Management Events.**

### Related links

[Trace Option Menus](#) on page 47

# GOD Trace Options

This tab provides trace options for monitoring the system's communications between individual modules.

Option	Description
<b>Client Tx</b>	Log Inter-Unit protocol messages sent by the unit, other those from the Gatekeeper.
<b>Client Rx</b>	Log Inter-Unit protocol messages received by the unit, other those to the Gatekeeper.
<b>Server Tx</b>	Log Inter-Unit protocol messages sent by the Gatekeeper
<b>Server Rx</b>	Log Inter-Unit protocol messages received by the Gatekeeper.

## Default Settings

None of the trace options are enabled by default. See [Defaulting the Trace Options](#) on page 45.

### Related links

[Trace Option Menus](#) on page 47

## H.323 Trace Options

This tab provides trace options for monitoring H.323 and H.245 events related to VoIP calls. The Computing Center Management System (CCMS) options can also be used for tracing Session Initiation Protocol (SIP) telephones that uses the interface, for example the J169 and J179 telephones.

### Events

Option	Description
H.323	Log the state changes of the H.323 call.
Summary Tracing	–

### Packets

Option	Description
H.245 Send	Log H.245 messages sent to an H.323 endpoint (IP phone or IP trunk).
H.245 Receive	Log H.245 messages received from an H.323 endpoint (IP phone or IP trunk).
H.323	Log the state changes of the H.323 call.
H.323 Send	Log the H.323 messages sent to an H.323 endpoint (IP phone or IP trunk).
H.323 Receive	Log H.323 messages received from an H.323 endpoint (IP phone or IP trunk).
H.323 Fast Start	Log H.323 fast-start messages send to/received from an H.323 endpoint (IP phone or IP trunk).
RAS Send	Log RAS (registration, admission and status) messages sent to an IP phone.
RAS Receive	Log RAS messages received from an IP phone.
CCMS Send	Log the CCMS (Control Channel Message Set) messages sent to a VoIP endpoint (H.323/SIP phone or IP trunk).
CCMS Receive	Log CCMS messages received from an VoIP endpoint (H.323/SIP phone or IP trunk).
View Whole Packet	Decoded the full H.323 message and included in the trace. If not selected, the trace only includes the first two lines of the H.323 message.

### Trace Color

This option allows selection of a color that is then applied to all options in the menu, see [Coloring Tab Trace Options](#) on page 44. This selection overrides any previous color selected for individual options. However, it does not prevent subsequent individual option coloring, see [Coloring Individual Trace Options](#) on page 43.

### Default Settings

The following trace options are enabled by default. See [Defaulting the Trace Options](#) on page 45.

- H.232 (Also automatically colored pink).

### Related links

[Trace Option Menus](#) on page 47



## Interface Trace Options

This tab provides trace options for monitoring the system's data network interfaces. An interface can be a physical interface like a LAN port or a configuration interface, like a data connection to a remote system or a Dial-In User.

### Packets

The following trace options provide information on either the whole system or on the specific interface specified in the **Interface Name** field.

Option	Description
<b>Interface Remote</b>	Log traffic tunneled through to any externally connected WAN3 modules.
<b>Interface Queue</b>	Log packets being queued at an interface. Especially useful for determining what packet, and therefore which IP address on the internal network, caused an outgoing data call to be made.
<b>Interface Packets In</b>	Log all packets received.
<b>Interface Packets Out</b>	Log all packets transmitted.
<b>NAT Fail In</b>	Log all NAT (Network Address Translation) packets received that have failed to pass through the firewall.
<b>NAT Fail Out</b>	Log all NAT (Network Address Translation) packets transmitted that have failed to pass through the firewall.
<b>NAT In</b>	Log all NAT (Network Address Translation) packets received.
<b>NAT Out</b>	Log all NAT (Network Address Translation) packets transmitted.
<b>Firewall Allowed In</b>	Log all packets received that have successfully passed through the firewall.
<b>Firewall Allowed Out</b>	Log all packets transmitted that have successfully passed through the firewall.
<b>Firewall Fail In</b>	Log all packets received that have failed to pass through the firewall.
<b>Firewall Fail Out</b>	Log all packets transmitted by the system that have failed to pass through the firewall.
<b>Firewall Generic In</b>	Log all packets received (except UDP, TCP and ICMP) that have successfully passed through the firewall.
<b>Firewall Generic Out</b>	Log all packets transmitted (except UDP, TCP and ICMP) that have successfully passed through the firewall.
<b>Firewall TCP Allowed In</b>	Log all TCP packets received that have successfully passed through the firewall.
<b>Firewall TCP Allowed Out</b>	Log all TCP packets transmitted that have successfully passed through the firewall.
<b>Firewall UDP Allowed In</b>	Log all UDP packets received that have successfully passed through the firewall.

*Table continues...*

Option	Description
<b>Firewall UDP Allowed Out</b>	Log all UDP packets transmitted that have successfully passed through the firewall.
<b>Interface Name</b>	This option can be used to limit the information shown for the fields above to those associate with a selected service. A blank entry matches all services.

### Filters

These options are used in conjunction with the other options on the tab to limit the number of packets displayed or to display packets from a range of devices.

Option	Description
<b>IP Address 1</b>	If set, only packets to and from the IP address are logged.
<b>IP Address 2</b>	If set, this field is used in conjunction with IP Address 1 to display only packets between the pair of addresses.
<b>MAC Address 1</b>	If set, only packets to and from the MAC are logged.
<b>MAC Address 2</b>	If set, this field is used in conjunction with MAC Address 1 to display only packets between the pair of MAC addresses.
<b>TCP</b>	<ul style="list-style-type: none"> <li>• Src Port</li> <li>• Dst Port</li> </ul>
<b>UDP</b>	<ul style="list-style-type: none"> <li>• Src Port</li> <li>• Dst Port</li> </ul>
<b>Broadcast</b>	If set, this option logs all broadcast packets except ARP broadcasts.
<b>WAN3 chat</b>	This option allows you to filter out the continuous dialogue which takes place between an system's control unit and an associated WAN3 module.
<b>ARP</b>	Log ARP packets.
<b>Multicast</b>	Log MultiCast packets (i.e. packets with either a source or destination address of 224.0.0.0).
<b>Payload Display Size</b>	This option limits the size of the IP packet displayed. Displayed payload can be set to anything between 0 and 1500 bytes. The default setting is 32 bytes.

### Default Settings

The following trace options are enabled by default. See [Defaulting the Trace Options](#) on page 45.

- **Interface Queue, TCP, UDP, ARP, MultiCast.**

### Related links

[Trace Option Menus](#) on page 47

---

## ISDN Trace Options

This tab provides trace options for monitoring the system's Integrated Services Digital Network (ISDN) digital trunks (Basic Rate Interface (BRI) and Primary Rate Interface (PRI)).

## Events

Option	Description
<b>Layer 1</b>	Log information on the status of the system's ISDN Layer 1 software state machine and associated events.
<b>Layer 2</b>	Log information on the status of the system's ISDN Layer 2 software state machine and associated events.
<b>Layer 3</b>	Log information on the status of the system's ISDN Layer 3 software state machine and associated events.

## Packets

Option	Description
<b>Layer 1 Send</b>	Log the data packets transmitted at the ISDN Layer 1 level.
<b>Layer 1 Receive</b>	Log the data packets received at the ISDN Layer 1 level.
<b>Layer 2 Send</b>	Log the data packets transmitted at the ISDN Layer 2 level.
<b>Layer 2 Receive</b>	Log the data packets received at the ISDN Layer 2 level.
<b>Layer 3 Send</b>	Log the data packets transmitted at the ISDN Layer 3 level.
<b>Layer 3 Receive</b>	Log the data packets received at the ISDN Layer 3 level.

## Layer 1 Event Messages

The following messages are output when Layer1 events are selected:

ISDNL1Evt: v=[line\_no.] peb=[hardware device no.], [new state] [old state] where the state values shown are:

State Values	Definition
F1	Inactive
F2	Sensing
F3	Deactivated
F4	Awaiting signal
F5	Identifying input
F6	Synchronised
F7	Activated
F8	Lost framing

ISDNL1Evt: v=[line\_no.] peb=[hardware device no.], [message] where message values are:

Message Values	Definition
PHAI	Physical Activate Indication (i.e. Line is UP)
PHDI	Physical Deactivate Indication (Line is DOWN)
T3TO	T3 timeout has occurred

*Table continues...*

Message Values	Definition
TxErr	A Transmit error has occurred
UnLocked	The system is not able to lock its clock to this line
Locked	The system and the clock extracted from this line are locked together.

### Default Settings

The following trace options are enabled by default. See [Defaulting the Trace Options](#) on page 45.

- **Layer 1, Layer 2, Layer 3.**

### Related links

[Trace Option Menus](#) on page 47

## Jade Trace Options

This tab provides trace options for monitoring the jade service used by Linux base systems.

### Events

The drop-down is used to select the level of detail to include. The options are **Terse**, **Standard** or **Verbose**.

- **Mapper**
- **Remote Mapper**
- **SIP Handler**
- **MSML**

### Voicemail Pro

- **Rx from Jade**
- **Tx to Jade**
- **Rx from VmPro**
- **Tx to VmPro**

### Packets

- **MSML Rx**
- **MSML Tx**
- **Internal SIP Filter**
- **UDP**
- **TCP**

### Default Settings

None of the trace options are enabled by default. See [Defaulting the Trace Options](#) on page 45.

**Related links**

[Trace Option Menus](#) on page 47

---

## Key/Lamp Trace Options

This tab provides trace options for monitoring the events for T3 Series telephones.

**T3**

- **API Events**
- **API Messages**
- **Phone Model**

**Default Settings**

None of the trace options are enabled by default. See [Defaulting the Trace Options](#) on page 45.

**Related links**

[Trace Option Menus](#) on page 47

---

## Media Trace Options

This tab provides trace options for monitoring the system's media service.

**Media Events**

- **Extension Cut:** When selected, it logs changes of 'cut' state for the extension (mapping connections).
- **Media handlers**
- **Connection handle**
- **Map:** The drop-down is used to select the level of detail to include. The options are **Terse**, **Standard** or **Verbose**.

**VoIP Events**

- **VoIP:** The drop-down is used to select the level of detail to include. The options are **Terse**, **Standard** or **Verbose**.
- **Primitives:** The drop-down is used to select the level of detail to include. The options are **Terse**, **Standard** or **Verbose**.

**RTP Info Monitoring**

For each record type, the **Clear Stats** button can be used to reset the values.

- **RTP Filter Info**
- **Priority Queue Info**

- **FEC Interrupt Info**

### VoIP Packets

- **Fast Start Info**
- **Primitives**

### Default Settings

The following trace options are enabled by default. See [Defaulting the Trace Options](#) on page 45.

- **Map.**

### Related links

[Trace Option Menus](#) on page 47

---

## PPP Trace Options

This tab provides trace options for monitoring the system's Point-to-Point Protocol (PPP) service events.

### Events

Option	Description
<b>Err Msg</b>	Currently this option does not provide any trace messages. It is included for possible future use only.
<b>Stack</b>	Log interface utilisation and bandwidth allocation increase or decrease messages.
<b>Include LCP Echo</b>	Log all LCP Echo and LCP Echo Reply packets received and transmitted.

### Packets

Option	Description
<b>LCP Tx</b>	Log all LCP (Link Control Protocol) packets transmitted.
<b>LCP Rx</b>	Log all LCP (Link Control Protocol) packets received.
<b>Security Tx:</b>	Log all PAP (Password Authentication Protocol) and/or CHAP (Control Handshake Authentication Protocol) packets transmitted.
<b>Security Rx:</b>	Log all PAP (Password Authentication Protocol) and/or CHAP (Control Handshake Authentication Protocol) packets received.
<b>M LCP Tx</b>	Log all MLCP (Multilink Layer Control Protocol messages) packets transmitted.
<b>M LCP Rx</b>	Log all MLCP (Multilink Layer Control Protocol messages) packets received.
<b>IPCP Tx</b>	Log all IPCP (Internet Protocol Control Protocol) packets transmitted.
<b>IPCP Rx</b>	Log all IPCP (Internet Protocol Control Protocol) packets received.
<b>BACP Tx</b>	Log all BACP (Bandwidth Allocation Control Protocol) packets transmitted.
<b>BACP Rx</b>	Log all BACP (Bandwidth Allocation Control Protocol) packets received.

*Table continues...*

Option	Description
CCP Tx	Log all CCP (Compression Control Protocol) packets transmitted.
CCP Rx	Log all CCP (Compression Control Protocol) packets received.
CRTP Tx	Log all CRTP (Compressed Real Time Protocol) packets transmitted.
CRTP Rx	Log all CRTP (Compressed Real Time Protocol) packets received.
IPHC Tx	Log all IPHC (IP Header compression) packets transmitted.
IPHC Rx	Log all IPHC (IP Header compression) packets received.
IP Tx	Log all IP (Internet Protocol) packets transmitted.
IP Rx	Log all IP (Internet Protocol) packets received.
Link Tx	Log all packets transmitted.
Link Rx	Log all packets received.
Interface Name	This option can be used to limit the information shown for the fields above to those associate with a selected service. A blank entry matches all services.

### Default Settings

The following trace options are enabled by default. See [Defaulting the Trace Options](#) on page 45.

- Err Msg.

### Related links

[Trace Option Menus](#) on page 47

---

## R2 Trace Options

This tab provides trace options for monitoring the system's E1-R2 trunks.

Option	Description
CAS	Log the common-channel Channel Associated Signaling (CAS) being transmitted and received on all of the channels.
Channel	Log the events, messages and status changes on the lower level signaling handlers being used on each channel.
Dialler	Log Dialler events and state changes on all channels. This includes outgoing and incoming digits, MFC dialer state transitions and translations of transmitted and received MFC tones into the correct meanings.
DSP	Log all significant events, digits and MFC tones being processed by the DSP on the R2 card.
Line	Log the events, messages and status changes on the line in general, and of "upper level" channel events, messages and status changes, which are independent of the lower level signaling handler being used on each channel.

## Default Settings

The following trace options are enabled by default. See [Defaulting the Trace Options](#) on page 45.

- **CAS, Channel, Dialler, DSP, Line.**

## Related links

[Trace Option Menus](#) on page 47

---

# Routing Trace Options

This tab provides trace options for monitoring the system's IP data routing events for data and for voice.

## Data

The event options under the **Data** are used to display information pertinent to the IP Routing activities on the system. It provides information on the system's route cache, routing table, and any RIP updates it receive or transmits.

## Events

Option	Description
<b>Route Cache Events</b>	Log information on the current state of the system's route cache.
<b>Routing Table</b>	Log information on the system's Routing table.
<b>Routing Table Changes</b>	Log changes made to the system's Routing Table.
<b>RIP In</b>	Log received RIP packets.
<b>RIP Out</b>	Log transmitted RIP packets.
<b>IGMP</b>	Log IGMP packets.

## Voice

The options under the **Voice** are used to display event information pertinent to the Small Community Networking (SCN) Voice Routing activities on the system. These activities include information on SCN messages sent between Adjacent Nodes, and the actual information contained within those message packets.

## Messages

Option	Description
<b>Received AVRIP</b>	Log the received AVRIP messages which are sent every 10 seconds during user activity and stop after 11 when idle. They can be used to check what nodes are active in a network. (If you want to see the actual messages then enable Voice/Packets/AVRIP Tx).
<b>Inter Node</b>	Log general Small Community Networking (SCN) messages which may help in the diagnosis of problem networks.

*Table continues...*



Option	Description
<b>Remote Node</b>	Log information on the establishment (or breakdown) of remote nodes in a SCN. These messages can be used to check what nodes are active in a network (note that a remote node is 2 or more hops away).
<b>Node Forwarding</b>	Log information about how this node is forwarding information about adjacent nodes to other adjacent nodes. Note that in a star network, the central node receives a large number of forwarding messages.

### Packet Contents

An AVRIP packet contains information about the voicemail status of that node and information about what other nodes can be reached (IP address and number of hops and voicemail status). VPN TFTP packets contain information on the nodes of User configuration data, User VoiceMail message counts, extension BLF status, and call information.

Option	Description
<b>AVRIP Tx</b>	Log all transmitted SCN AVRIP packets from the Node being monitored.
<b>AVRIP Rx</b>	Log all received SCN AVRIP packets from Nodes adjacent to the one being monitored.
<b>VPN TFTP Tx</b>	Log all transmitted SCN TFTP packets from the Node being monitored.
<b>VPN TFTP Rx</b>	Log all received SCN TFTP packets from Nodes adjacent to the one being monitored.

### Default Settings

None of the trace options are enabled by default. See [Defaulting the Trace Options](#) on page 45.

### Related links

[Trace Option Menus](#) on page 47

---

## SCN Trace Options

This tab allows the logging of SCN messages.

### Events

- **DHG Call Routing**
- **DHG Membership**
- **DHG Service Change**
- **SCN Resilience**

### Messages

- **Control Stream Tx**
- **Control Stream Rx**

### Events

These options are only available when the **Development Tracing** option is selected in the **Filters > Trace Options > System** menu, see [System Trace Options](#) on page 69. They are

not covered by this document as they are used by Avaya for product trials and are subject to frequent changes.

These options should only be used under the guidance of an authorized Avaya development engineer.

- **DHG Longest Idle Info**
- **DHG Config Change**
- **SCN User Events**
- **SCN Dump**

### Default Settings

None of the trace options are enabled by default. See [Defaulting the Trace Options](#) on page 45.

### Related links

[Trace Option Menus](#) on page 47

---

## Services Trace Options

This tab provides trace options for monitoring various services provided by the system.

### SNMP Events

Option	Description
<b>Received Message Processing</b>	Log Simple Network Management Protocol (SNMP) requests (Get, Get-Next, Set) received by the system and the responses if valid or associated errors if invalid.
<b>Trap Generation</b>	Log SNMP trap events sent by the system.
<b>Var Bind Processing</b>	This option is available when either of the above SNMP trace options are selected. If selected, log a decode of SNMP Var Binds processed in received requests, returned Var Bind for Get-Next requests, and Var Binds sent out in Traps.

### Others

Option	Description
<b>FileSys</b>	Log file requests received by the system.
<b>Memory Card</b>	Log memory card commands and actions.
<b>TFTP</b>	Log Trivial File Transfer Protocol (TFTP) file requests to the system and by the system. <ul style="list-style-type: none"> <li>• <b>TFTP Warnings:</b> If selected, this option logs TFTP warnings that occur in response to file requests.</li> <li>• <b>TFTP Download:</b> If selected, this option logs the progress of TFTP downloads.</li> </ul>
<b>HTTP</b>	Log HTTP requests. <ul style="list-style-type: none"> <li>• <b>Websocket Ping Pong</b></li> </ul>

*Table continues...*

Option	Description
DHCP	Log Dynamic Host Configuration Protocol (DHCP) requests.
DNS	Log Domain Name System (DNS) requests.
Telnet	Log Telnet activity.
Time	Log time and date requests and responses to the system and between the system and its configured time server.
SMTP	Log Simple Mail Transfer Protocol (SMTP) activity on the system.
Outdialer	Log messages between the system and the outdialing server. System Monitor can also display a status summary of the current outdialer session, see <a href="#">Outdialer status</a> on page 99.
Syslog	Log Syslog messages and responses.
SCEP	
ReferredAuth	
Firewall	
IP Filter	The value in this field can be used to only show only messages to and from the specified IP address. The filter is applied to all the other selected trace options on the tab.
Web Services	Log web service messages.

### Default Settings

None of the trace options are enabled by default. See [Defaulting the Trace Options](#) on page 45.

### Related links

[Trace Option Menus](#) on page 47

---

## SIP Trace Options

This tab provides trace options for monitoring the system's SIP events.

### \* Note:

For SIP phones that uses Control Channel Message Set (CCMS) signalling. The H.323 trace options menu are used.

### Events

Option	Description
SIP	Log state changes for SIP calls. The drop-down is used to select the level of detail to include. The options are <b>Terse</b> , <b>Standard</b> or <b>Verbose</b> .
STUN	Log Session Traversal Utilities for NAT (STUN) server information.
SIP Dect	Log state changes for SIP DECT calls.

## Packets

Option	Description
<b>SIG Reg/Opt Tx</b>	Log the SIP Registration and Option messages sent by SIP endpoints.
<b>SIP Reg/Opt Rx</b>	Log the SIP Registration and Option messages received by SIP endpoints.
<b>SIP Call Tx</b>	Log the SIP Call messages sent by SIP endpoints.
<b>SIP Call Rx</b>	Log the SIP Call messages received by SIP endpoints.
<b>SIP Misc Tx</b>	Log the SIP Miscellaneous messages sent by SIP endpoints.
<b>SIP Misc Rx</b>	Log the SIP Miscellaneous messages received by SIP endpoints.
<b>Cm Notify Tx</b>	Log the SIP Notify messages sent by SIP endpoints.
<b>Cm Notify Rx</b>	Log the SIP Notify messages received by SIP endpoints.
<b>Sip Tx</b>	Log all SIP messages sent from SIP endpoints.
<b>Sip Rx</b>	Log all SIP messages received by SIP endpoints

### Default Settings

The following trace options are enabled by default. See [Defaulting the Trace Options](#) on page 45.

- **STUN, SIP Rx, SIP Tx.**

### Related links

[Trace Option Menus](#) on page 47

## SSI Trace Options

This tab provides trace options for monitoring the system's SSI connections. SSI is used for the IP Office Customer Call Reporter and System Status Application applications.

These options are only available when the **Development Tracing** option is selected in the **Filters > Trace Options > System** menu, see [System Trace Options](#) on page 69. They are not covered by this document as they are used by Avaya for product trials and are subject to frequent changes.

These options should only be used under the guidance of an authorized Avaya development engineer.

- **SSI Request Messages**
- **SSI Reply and Event Messages**
- **SSI Object Event Messages**
- **Decode SSI**

### Default Settings

None of the trace options are enabled by default. See [Defaulting the Trace Options](#) on page 45.

### Related links

[Trace Option Menus](#) on page 47

## T1 Trace Options

This tab provides trace options for monitoring the system's T1 trunks.

### Events

Option	Description
<b>CAS</b>	Log the robbed-bit Channel Associated Signaling (CAS) being transmitted and received on all of the channels.
<b>Channel</b>	Log the events, messages and status changes on the lower level signaling handlers being used on each channel.
<b>Dialler</b>	Log "Dialler" events and state changes on all channels. This includes outgoing and incoming digits.
<b>DSP</b>	Log all significant events and digits being processed by the DSP on the T1 card.
<b>Line</b>	Log the events, messages and status changes on the T1 line in general, and "upper level" channel events, messages and status changes, which are independent of the lower level signaling handler being used on each channel.

### Loop-back

These options are used to set loop-back operation. First select the line on which loop-back is required and then the type of loop-back. Click **OK** to apply the settings.

### Loop-back Type

Option	Description
<b>Line Loop-back</b>	This loop-back type loops back the entire received signal to the far end of the line without the signal entering the system at all.
<b>Payload Loop-back</b>	This loop-back type allows the received signal into the line driver chip-set. The signal payload is extracted from the incoming framed signal and transmitted back to the line with new framing.
<b>Loop-Back Off</b>	This option disables any loop-back operation currently applied to the selected line.

### Loop-back Line Selection

- **Loop-back Line Selection:** These settings are used to select the lines to which the selected **Loop-back Type** are applied.

### Default Settings

None of the trace options are enabled by default. See [Defaulting the Trace Options](#) on page 45.

### Related links

[Trace Option Menus](#) on page 47

## System Trace Options

This tab provides general trace options.

Option	Description
<b>Error</b>	Log all messages that are tagged with [ERROR:].
<b>Print</b>	Log all messages that are tagged with [PRN:]. These are messages relating to major events or changes in status of the software modules running.
<b>Prefix YYYY-MM-DD</b>	When selected, each record is prefixed with the current date.
<b>Prefix hh:mm:ss</b>	When selected, each record is prefixed with the current time.
<b>Resource Status Prints</b>	When selected, once every 20 seconds, the trace includes a summary of the system memory resources and the number of connections. The messages are tagged with [RES:].
<b>Date/Time Periodic Prints</b>	When selected, once a minute the trace includes a record prefixed with DTM of the date and time plus details of the connected system name and IP address. This is useful in a trace if the <b>Prefix YYYY-MM-DD hh:mm:ss</b> trace option is not selected. For example: DTM: 29/05/2015 11:28:06 (Tue 30 June 2015) [192.168.0.1 (SystemA)]
<b>Licensing</b>	Log messages relating to the verification of system licenses. Licensing messages are tagged with [LIC:].
<b>Development Tracing</b>	This option should only be selected when advised to do so by Avaya. Log additional trace option for <a href="#">SSI</a> on page 68 and <a href="#">VComp</a> on page 71 and a number of additional status screens, see <a href="#">Status screen</a> on page 83.
<b>Copy Logging to Main Window</b>	This option is only available if <b>Development Tracing</b> is selected.
<b>SNMP Periodic Status Traps</b>	This option is only available if <b>Development Tracing</b> is selected. When selected, the system outputs a periodic SNMP trap containing a summary of the current system status (memory usage, alarms count, channel available and in uses, etc). The trap information is sent to the SNMP destination configured in the IP Office system's System Alarms configuration. The frequency of sending is configurable between 20 to 7200 seconds. Status element is not included is both values would be 0.
<b>Copy Trap data to log</b>	If selected, the SNMP periodic status trap information is also included in the monitor logs.

## SNMP Period Status Trap

The following is an example of a status trap. The table below explains each field.

```
CP:1/2.67% ME:72014/22034 AL:4/1 VC:74/0 DC:48/1 VM:40/0 CC:128/0/0 N(1/R:162/T:651 2/R:98/T:99)N E(10/10 S:1/1 H:1/1 D:6/6 P:2/2)E CA:1 VR:10.0.0.0(9601)
```

Status	Description
<b>CP</b>	CPUs: Number of CPUs , % use.
<b>ME</b>	Memory: total memory/used memory (KB).
<b>AL</b>	Alarm counts: SSA alarm count , system log hw alarm count.
<b>VC</b>	VCM Channels: total/used.
<b>DC</b>	Data Channels: total/used.
<b>VM</b>	Voicemail Channels: total/used.

*Table continues...*

Status	Description
MC	Modem Channels: total/used.
CC	Conference Channels: total/used/HQ used.
N	Network interface stats: interface/Rx/Tx. (Rx and Tx are average for previous 3 seconds).
E	Extension stats: total/connected, SIP registered/logged in, digital extensions/logged in, analog extensions/logged in, IP DECT extensions/logged in.
CA	Calls active count.
VR	Version: IP Office software version.

### Trace Color

This option allows selection of a color that is then applied to all options in the menu, see [Coloring Tab Trace Options](#) on page 44. This selection overrides any previous color selected for individual options. However, it does not prevent subsequent individual option coloring, see [Coloring Individual Trace Options](#) on page 43.

### Default Settings

The following trace options are enabled by default. See [Defaulting the Trace Options](#) on page 45.

- **Error, Print, Prefix hh:mm:ss, Resource Status Prints, Licensing.**

### Related links

[Trace Option Menus](#) on page 47

---

## VComp Trace Options

This tab provides trace options for monitoring the system's voice compression channels. Note that these options produce a large amount of trace records and so should be used with caution.

These options are only available when the **Development Tracing** option is selected in the **Filters > Trace Options > System** menu, see [System Trace Options](#) on page 69. They are not covered by this document as they are used by Avaya for product trials and are subject to frequent changes.

These options should only be used under the guidance of an authorized Avaya development engineer.

### General VCM Trace Options

Option	Description
Command Send	Log details of commands transmitted to the voice compressor chip.
Command Receive	Log details of commands received from the voice compressor chip.
Data Send	Log details of data transmitted to the voice compressor chip (additional detail from the Command Send option).

*Table continues...*

Option	Description
<b>Data Receive</b>	Log details of data received from the voice compressor chip (additional detail from the Command Receive option).
<b>Print on Stuck</b>	Log a summary trace if the system detects a severe problem.
<b>Summary Trace</b>	Log the commands to and from all the voice compressor chips (multiple occurrences are counted to reduce output) and the output is controlled so as not to swamp the system. Care should be exercised when selecting this option - especially if multiple VoIP calls are in progress.

### Fax Specific VCM Trace Options

Option	Description
<b>Development Test</b>	Used when debugging private variations of Development software.
<b>Fax Summary</b>	Log the V.21 and T.30 messages.
<b>Show all fax packet contents</b>	Log the contents of ALL fax packets - including the actual fax data (only when connected to a Definity).
<b>Show T.30 V.21 packet contents</b>	Log the contents of T.30 and V.21 packet (only when connected to a Definity).

### TI-VCM Trace Options

- **Command Trace**
- **Fax Debug**
- **DIM Spy Level**
- **CCU Spy Level**

### Default Settings

None of the trace options are enabled by default. See [Defaulting the Trace Options](#) on page 45.

### Related links

[Trace Option Menus](#) on page 47

---

## VPN Trace Options

This tab provides trace options for monitoring the systems Virtual Private Network (VPN) connections.

These options should only be used under the guidance of an authorized Avaya development engineer.



## IPSec Events

Option	Description
<b>IPSec Events</b>	Log primary events when bringing up and tearing down IPSec tunnels. It also indicates when packets are being discarded, and so on.
<b>Decode</b>	Log the decrypted IKE packets.
<b>IPO-SNet</b>	Not currently used.
<b>Data Events</b>	Log when packets are encrypted into and out of tunnel. It does not display the actual packet contents, they can be logged using the <a href="#">Interface</a> on page 57 tab options <b>Interface Packets In</b> and <b>Interface Packets Out</b> .
<b>Warnings</b>	Log information relating to faults in the IPSec processing.
<b>Debug</b>	Log special engineering trace information.

## IPSec Packets

Option	Description
<b>Rx Data</b>	Log the content of received ESP encrypted packets before decryption.
<b>Tx Data</b>	Log the content of sent ESP encrypted packets after encryption.

## L2TP Events

- **L2TP Events:** If selected, this option logs the establishment of the L2TP tunnel (the stage underneath the PPP). You really need to include the appropriate PPP tracing additionally to this to see the complete picture.

## L2TP Packets

- **Rx Data:** Currently not used.
- **Tx Data:** Currently not used.

## Security Engine

- **Events**
- **Measurements**
- **Stack Trace**
- **Regs on H/W Cmd Init**
- **Regs on H/W Cmd Done**
- **Regs on H/W Cmd Error**

## SSL VPN

- **Configuration**
- **Session**
- **Session State**
- **Fsm**
- **Socks**
- **SocksState**

- **Heartbeat**
- **Keepalive**
- **SignalingPktRx**
- **SignalingPktTx**
- **DataPktRx**
- **DataPktTx**
- **TunnelInterface**
- **TunnelRoutes**

### Default Settings

The following trace options are enabled by default. See [Defaulting the Trace Options](#) on page 45.

- Security Engine: **Regs on H/W Cmd Error**. SSL VPN: **Session** and **Session State**.

### Related links

[Trace Option Menus](#) on page 47

---

## WAN Trace Options

This tab provides trace options for monitoring the system's WAN ports.

### Events

**WAN Events:** When selected, log messages that are associated with changes to the software state machine controlling the WAN link on the selected unit.

### Packets

Option	Description
<b>WAN Tx</b>	Log all IP data packets transmitted on the WAN ports of the selected unit.
<b>WAN Rx</b>	Log all IP data packets received on the WAN ports of the selected unit.

### Default Settings

The following trace options are enabled by default. See [Defaulting the Trace Options](#) on page 45.

- **WAN Events.**

### Related links

[Trace Option Menus](#) on page 47

# Chapter 8: Syslog Tracing

For IP Office Release 9.0 and higher, in addition to the existing Syslog output of alarms and events, IP Office systems can also output System Monitor events to Syslog. To view the `Syslog` files containing monitor events in monitor, they need to be converted to monitor log file. This task is done using monitor.

- Activation of Syslog monitor events output is done through IP Office Manager.
- Configuration of which trace options to include in the output is done using System Monitor.
- **Default Syslog Monitor Tracing:**

The default configuration of Linux-based servers automatically adds a monitor Syslog output to the system configuration. The entry is configured to store the records on the server using the `127.0.0.1` address. This provides hourly Syslog files which are retained for 3–days. See [Configuring the Syslog Trace Options](#) on page 76.

- **Cloud Edition Systems:**

For these system, the system's monitor Syslog output is automatically directed to the **Cloud Diagnostic Agent** service run by the cluster hosting the system. Those logs are kept for up to 3-days and can be downloaded through the cluster's Customer Operations Manager.

- **Subscription Systems:**

These systems can be monitored and managed through Customer Operations Manager running on the cluster providing the system subscriptions. In that case, the system Syslog files can also be collected using Customer Operations Manager.

## Related links

[Enabling Syslog Monitor Output](#) on page 76

[Default Syslog Trace Options](#) on page 77

[Downloading a Syslog Archive from Web Control](#) on page 78

[Downloading a Syslog Archive from Cloud-based Systems](#) on page 79

[Downloading a Syslog Archive from Subscription Systems](#) on page 80

[Extracting the Syslog zip files](#) on page 80

[Converting Syslog Files](#) on page 81

---

## Enabling Syslog Monitor Output

### About this task

The Syslog output from cloud edition systems is automatically configured. The Syslog output from non-cloud edition systems is configured using IP Office Manager.

- While an IP Office system can have several Syslog outputs, only one output can include System Monitor events.

### Procedure

1. Using IP Office Manager, receive the configuration from the IP Office system.
2. Select **System** and then select the **System Events** tab.
3. Click **Add** and set the **Destination** to **Syslog**.
4. Enter the details for the destination server for the output.
  - For Linux-based IP Office servers you can use `127.0.0.1` to specify that the server should store the records itself.
  - On Linux-based IP Office servers, the logs are stored in `/var/log/sysmon`. This stores hourly Syslog monitor files a maximum of 3 days. However, the maximum total log files capacity per day is 4 Gigabyte (GB).
5. The recommended protocol is **UDP**.
6. Set the **Format** to **Enterprise**.
7. From the list of **Events** select **System Monitor**.
8. Click **OK** and save the configuration back to the IP Officesystem.

### Next steps

You can now customize the monitor trace options to include in the Syslog output. See [Configuring the syslog trace options](#) on page 76.

### Related links

[Syslog Tracing](#) on page 75

---

## Configuring the Syslog Trace Options

### About this task

The system's Syslog output includes the events and the default monitor trace options. However, you can alter the trace options used.

### Procedure

1. Using monitor, connect to the IP Office system. See [Selecting the System to Monitor](#) on page 29.

2. Set the trace options required. See [Setting the Trace Options](#) on page 42.
3. Save the trace options as a file so that you can reload them at a later date if you need to reapply or amend them. See [Saving Trace Options as a File](#) on page 42.
4. Select **Filters** and click **Send to Syslog**.
5. The trace option settings are sent as a file to the connected system. The settings are applied to the monitor events and included in the system's Syslog output.

---

## Default Syslog Trace Options

The following Syslog trace options are enabled by default on systems.

### All systems

Release 9.0 and higher	Release 10 and higher
<ul style="list-style-type: none"> <li>• <b>System</b></li> <li>- <b>Print</b></li> <li>- <b>Error</b></li> <li>- <b>Resource Status Prints</b></li> <li>- <b>Licensing</b></li> </ul>	<ul style="list-style-type: none"> <li>• <b>System</b></li> <li>- <b>Print</b></li> <li>- <b>Error</b></li> <li>- <b>Resource Status Prints</b></li> <li>- <b>Licensing</b></li> <li>- <b>Date/Time Periodic Prints</b></li> <li>• <b>Service</b></li> <li>- <b>Time</b></li> </ul>

### Additional options for Linux-based systems

<ul style="list-style-type: none"> <li>• <b>Call</b> <ul style="list-style-type: none"> <li>- <b>Call Logging</b></li> <li>- <b>Targeting</b></li> <li>- <b>ARS</b></li> <li>- <b>Extension</b></li> <li>- <b>Extension Send</b></li> <li>- <b>Extension Receive</b></li> <li>- <b>Line Send</b></li> <li>- <b>Line Receive</b></li> <li>- <b>Call Delta</b></li> <li>- <b>Voicemail Events</b></li> <li>- Voicemail Messaging</li> </ul> </li> <li>• <b>Media</b> <ul style="list-style-type: none"> <li>- <b>Map (Standard)</b></li> </ul> </li> <li>• <b>H.323</b> <ul style="list-style-type: none"> <li>- <b>Events</b></li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• <b>SIP</b> <ul style="list-style-type: none"> <li>- <b>SIP (Standard)</b></li> <li>- <b>SIP Rx</b></li> <li>- <b>SIP Tx</b></li> </ul> </li> <li>• <b>Services</b> <ul style="list-style-type: none"> <li>- <b>TAPI</b></li> <li>- <b>TAPI Call Log</b></li> <li>- <b>TAPI Line</b></li> <li>- <b>TAPI Onex Resiliency</b></li> </ul> </li> <li>• <b>Jade</b> <ul style="list-style-type: none"> <li>- <b>Mapper (Standard)</b></li> <li>- <b>Remote Mapper (Standard)</b></li> <li>- <b>MSML Tx</b></li> </ul> </li> </ul>
---	--

**Related links**

[Syslog Tracing](#) on page 75

## Downloading a Syslog Archive from Web Control

### About this task

Linux-based IP Office servers can store their own **Syslog** monitor records by using the destination 127.0.0.1. When doing this, you can download the records from the server's web management menus.

### Procedure

1. Using a browser, login to the server's web management menus.
2. Click **SolutionSolution**.
3. Click on the ☰ icon next to the required server and select **Platform View**.
4. Select **Log** and then click **Download**.
5. Click **Create Archive** in the **Logs** section. The button remains greyed out while the server creates an compressed archive file for each of the different types of log files it is storing. Each file contains all the logs that have not been previously archived.

6. The Syslog monitor file is prefixed with `sysmon_logs` followed by the date and time.
7. To download the file, click on the file name and follow the normal download options for your browser.

**To extract the System Monitor Syslog files:**

8. Open the `sysmon_logs tar.gz` file using a suitable tool such as 7-Zip.
9. Browse to the required folder. The default is the `127.0.0.1` folder.
10. Extract the individual `.zip` files to your PC.

**Next steps**

The download file is a `.tar.gz` format archive file which can contain a number of `.zip` files. See [Extracting the Syslog zip files](#) on page 80.

**Related links**

[Syslog Tracing](#) on page 75

## Downloading a Syslog Archive from Cloud-based Systems

**About this task**

For these system, the system's monitor Syslog output is automatically directed to the **Cloud Diagnostic Agent** service run by the cluster hosting the system. Those logs are kept for up to 3-days and can be downloaded through the cluster's Customer Operations Manager.

**Procedure**

1. Within Customer Operations Manager, select the system in the customer list.
2. Click **Action** and select **Log Management**.
3. To create an archive of any existing logs:
  - a. Select **Archives**.
  - b. Select **System Monitor**.
  - c. Click **System Monitor**.
4. To download an archive:
  - a. Select **Downloads**.
  - b. The existing archives are listed. Click on a file to download it.

**Next steps**

The download file is a `.tar.gz` format archive file which can contain a number of `.zip` files. See [Extracting the Syslog zip files](#) on page 80.

**Related links**

[Syslog Tracing](#) on page 75

---

## Downloading a Syslog Archive from Subscription Systems

### About this task

These systems can be monitored and managed through Customer Operations Manager running on the cluster providing the system subscriptions. In that case, the system Syslog files can also be collected using Customer Operations Manager.

### Procedure

1. Within Customer Operations Manager, select the system in the customer list.
2. Click **Action** and select **Log Management**. Any log files already fetched from the system are shown. By default, Customer Operations Manager retains files for 30-days.

#### To fetch any existing logs from a system:

3. Click **Fetch New Logs**.
4. It can take several minutes before the archive file is shown

#### To download log archives:

5. Click the checkbox next to the required logs.
6. Click **Download**.

### Next steps

The download file is a `.tar.gz` format archive file which can contain a number of `.zip` files. See [Extracting the Syslog zip files](#) on page 80.

### Related links

[Syslog Tracing](#) on page 75

---

## Extracting the Syslog zip files

### Before you begin

An archive of Syslog files held by a server can be download from the server:

- [Downloading a Syslog Archive from Web Control](#) on page 78
- [Downloading a Syslog Archive from Cloud-based Systems](#) on page 79
- [Downloading a Syslog Archive from Subscription Systems](#) on page 80

### About this task

Having downloaded a syslog `.tar.gz` file, the individual `.zip` files need to be extracted from it. These `.zip` files can then be processed and viewed by monitor.

### Procedure

1. Open the `sysmon_logs tar.gz` file using a suitable tool such as 7-Zip.



2. Browse to the required folder. The default is the 127.0.0.1 folder.
3. Extract the individual .zip files to your PC.

### Next steps

See [Converting Syslog Files](#) on page 81.

### Related links

[Syslog Tracing](#) on page 75

---

## Converting Syslog Files


### About this task

Using monitor, you can convert the **Syslog** monitor files to System Monitor log files. These can then be viewed in monitor.


- You can convert multiple files in a single operation.
- Zipped .zip monitor Syslog files can be converted without extracting the files.


### Procedure

#### To configure the logging options for file conversion:

1. Start monitor.
2. Click  **Log Preferences**.
3. Set the **Log Mode** setting to **Every 'n' MBytes**. The current .txt file is rolled over to start a new file when necessary. Otherwise, a new file is started each time the current log file reaches 100MB.
4. Set the log file name and location in the **Log Filename** field. The default location is the monitor program folder (C:\Program Files (x86)\Avaya\IP Office\Monitor). Each time a new log file is started, monitor adds the date and time to the log file name.
  - One monitor .txt file is created for each Syslog file being converted.
  - If the **Every 'n' MBytes** setting is set, a new file is started if it is reached during the conversion of a file.
5. Do not select **Binary Logging** and **Enable Zip**.
6. Select **Log to File**.
7. Click **OK**.

#### To convert the Syslog monitor files:

8. Configure the logging options for file conversion.
9. If converting a large file or numerous files, click  to pause the screen trace display. This speeds up the conversion process.

10. Click .
11. Browse to and select the `.zip` file containing the monitor Syslog files. You can select more than one file if required. Or select the `.log` file or files if they have already been extracted from the archive file.
12. You are prompted for a password, click **OK**.
13. Click **Open**.

The file or files are converted to monitor `.txt` log files using the logging settings.

**Related links**

[Syslog Tracing](#) on page 75

# Chapter 9: Status Screens

In addition to screen logging, System Monitor can display a number of status screens that show additional information about the connected system. Click **Status** to access and select the required status menu.

## Related links

- [Alarms](#) on page 84
- [Blacklisted Extensions](#) on page 84
- [Blacklisted IP Addresses](#) on page 86
- [Buffer Data](#) on page 88
- [Conference Status](#) on page 89
- [DECT Line Status](#) on page 90
- [DHCP Data](#) on page 90
- [DSS Status](#) on page 91
- [Equinox Sessions](#) on page 92
- [H323 Phone Status](#) on page 92
- [IPO-SNet](#) on page 93
- [IPv6 Config](#) on page 94
- [Jade Queue Status](#) on page 94
- [Logging](#) on page 95
- [Map Status](#) on page 96
- [Memory Data](#) on page 96
- [NAPT Status](#) on page 97
- [Network View](#) on page 98
- [Outdialer Status](#) on page 99
- [Partner Sessions](#) on page 100
- [Performance Data](#) on page 101
- [Quarantined Phone Status](#) on page 102
- [SCN Licence](#) on page 104
- [SIP Phone Status](#) on page 105
- [SIP TCP User Data](#) on page 106
- [Small Community Networking](#) on page 106
- [\[S\]RTP Sessions](#) on page 107
- [TCP Streams Data](#) on page 107
- [US PRI Trunks](#) on page 108

[Voicemail Sessions](#) on page 108

[Voice Compression](#) on page 109

[Voice Compression \(TI\)](#) on page 109

---

## Alarms

### About this task

This menu displays the alarms records in the connected system's alarms log. When monitor connects to a system, the trace automatically includes the system's current alarm log at its start.

The alarms cannot be interpreted in the field. However, if a site experiences the same repeated problem, Avaya may request the alarm log details.

The presence of alarms is not necessarily critical as each system keeps a record of the first 8 alarms since the alarm log was last cleared. However, once the alarm log is full, the system ignores additional alarms.

```
3003mS PRN: +++ START OF ALARM LOG DUMP +++
3019mS PRN: ALARM: 18/03/2004 13:07:56 IP 412 2.1(8) CRIT RAISED addr=00000000 d=5
pc=00000000 0082eef0 0094d780 00a13250 00a13638 00a0cb3c
3019mS PRN: ALARM: 22/04/2004 07:26:44 IP 412 2.1(11)CRIT RAISED addr=00000000 d=5
pc=00000000 0095dfe0 0095e278 008b0570 008b0734 008b07b8
3019mS PRN: ALARM: 22/04/2004 07:26:46 IP 412 2.1(11)CRIT RAISED addr=00000000 d=0
pc=00000000 01e75750 01f983d4 0095e278 00000001 01e757f8
3004mS PRN: +++ END OF ALARM LOG DUMP +++
```

### Procedure

1. Click **Status** and select **Alarms**. Monitor displays the alarm records in a separate window.
2. To clear the alarm log, click **Clear Alarms**.

### Related links

[Status Screens](#) on page 83

---

## Blacklisted Extensions

This menu displays extensions that have attempted to register using the wrong password.

Extn Num	Blocked	Current Failures	Max Failures	Last Failure	Time To Be Removed	Time To Be Unblocked	Avaya Phone

Page 1

Buttons: Save Page, Log To Sysmon, Remove Entries, Cancel

- Extensions are blocked after five failed registration attempts within a 10 minute period.
- The extensions are blocked for 10 minutes.
- Whilst blocked, further registration attempts are ignored even if correct password details are entered.
- For non-Avaya phones, if the extension continues to attempt to register during this period its blocking time is extended.
- When an extension becomes blocked, the system also generates an alarm in System Status Application application and adds an entry to the audit log. A system alarm is also generated and can be output using any of the configurable system alarm routes.
- The IP address of a phone attempting to register can also blocked, see, [Blacklisted IP addresses](#) on page 86. A phone can also be blocked from registering if it becomes quarantined, see [Quarantined Phone Status](#) on page 102.

## Columns

<b>Extn Num</b>	The extension number.
<b>Blocked</b>	Indicates whether the extension is now blocked having exceeding the number of allowed registration failure.
<b>Current Failures</b>	The number of registration attempt failures.
<b>Max Failures</b>	The number of registration failures at which the extension was blocked.
<b>Last Failure</b>	The date and time of the last failed registration attempt.
<b>Time To Be Removed</b>	The date and time at which the extension, if not blocked, and removed from the blacklist if there are no further failed registration attempts.
<b>Time To Be Unblocked</b>	<p>The date and time at which a blocked extension will be unblocked and removed from the list.</p> <ul style="list-style-type: none"> <li>• For non-Avayaphones, this time is extended if the extension continues attempting to re-register before the time is reached.</li> </ul>
<b>Avaya Phone</b>	Indicates whether the extension is a recognized Avaya phone.

**Button**

<b>Save Page</b>	Saves the current status menu data to a text file in comma separated format.
<b>Log To Sysmon</b>	When selected, the information is added to the Syslog monitor log. A comma separated row is added to the log output for each current entry.
<b>Remove Entries</b>	Removes the current blacklist entries. This allows to attempt to reregister again without having to wait for the expiry of their previous blacklisting.
<b>Cancel</b>	Close the status menu.

**Related links**

[Status Screens](#) on page 83

---

## Blacklisted IP Addresses

This menu displays IP addresses that are currently blacklisted by the system. Blacklisting is typically applied after 10 failed access attempts. The IP address remains blacklisted for 10 minutes from the last failed access attempt.

Ip Address	Blocked	Current Failures	Max Failures	Last Failure	Time To Be Removed	Time To Be Unblocked	Avaya Phone
212.83.128.121	YES	10	10	26/10/2016 15:05:01	26/10/2016 15:15:01	26/10/2016 15:15:01	
212.83.137.201	YES	10	10	26/10/2016 15:03:23	26/10/2016 15:13:23	26/10/2016 15:13:23	
212.129.27.34	YES	10	10	26/10/2016 15:05:02	26/10/2016 15:15:02	26/10/2016 15:15:02	

When an address becomes blocked, the system generates an alarm in System Status Application application and adds an entry to its audit log. A system alarm is also generated and can be output using any of the configurable system alarm routes (Simple Mail Transfer Protocol (SMTP), Simple Network Management Protocol (SNMP), Syslog).

An IP address can become blacklisted for the following reasons:

<b>Extension registration blacklisting</b>	<p>An extension that has repeatedly attempted to register a non-existing extension or to register an existing extension with the wrong password. When blacklisted, further registration attempts are ignored even if they use the correct parameters. Note that the extension number of a phone attempting to register can also become blocked, see <a href="#">Blacklisted extensions</a> on page 84</p> <ul style="list-style-type: none"> <li>The use of IP address blacklisting can be disabled through the addition of the NoUser Source Number <code>B_DISABLE_HTTP_IPADDR</code>.</li> </ul>
<b>Application blacklisting</b>	<p>An application trying to connection on port 443 or 8443 has repeatedly entered the wrong password. That can apply, for example, to web manager, system status and system monitor connections. When blacklisted, further connected attempts are ignored.</p> <ul style="list-style-type: none"> <li>The use of IP address blacklisting can be disabled through the addition of the NoUser Source Number <code>B_DISABLE_HTTP_IPADDR</code>.</li> </ul>
<b>Session Initiation Protocol (SIP) Invite blacklisting</b>	<p>Repeated SIP invites to an unregistered extension.</p> <ul style="list-style-type: none"> <li>The use of SIP Invite blacklist can be disabled through the addition of the NoUser source number <code>B_DIS_UNREG_SIP_INVITE</code>.</li> </ul>
<b>Excessive SIP traffic blacklisting</b>	<p>IP address blacklisting can be applied when the number of SIP messages (all types) from the same address exceeds a set rate. The default rate is 100,000 messages in 100 milliseconds. Unlike the other blacklistings, this blacklisting can only be manually removed.</p> <ul style="list-style-type: none"> <li>The following NoUser source numbers can be used to alter the use of SIP traffic blacklisting: <ul style="list-style-type: none"> <li><code>B_RATE_DISABLE</code> disables the functionality (by default it is enabled).</li> <li><code>B_RATE_HIGH_LIMIT=X</code> where X is the number of SIP messages allowed within the time threshold. The default limit is 500, where minimum is 1 and maximum is 100,000.</li> <li><code>B_RATE_HIGH_THRESH=Y</code> where Y is the time threshold in milliseconds. The default limit is 100, where minimum is 100, and maximum is 300,000 (which is 5 minutes).</li> </ul> </li> </ul>

## Columns

<b>IP Address</b>	The IP address
<b>Blocked</b>	Indicates whether the extension is now blocked from registering for exceeding the number of failed registration attempts.
<b>Current Failures</b>	The number of registration attempt failures.
<b>Max Failures</b>	The number of registration failures at which the extensions can be blocked.
<b>Last Failure</b>	The date and time of the last failed registration attempt.
<b>Time To Be Removed</b>	The date and time at which the extension, if not blocked, it is removed from the blacklist if there are no further failed registration attempts.

*Table continues...*

<b>Time To Be Unblocked</b>	The date and time at which the blocked extension is unblocked and removed from the blacklist. For non-Avaya phones this will extend if the extension attempts to re-register again before this time.
<b>Avaya Phone</b>	Indicates whether the extension is recognized as being an Avaya phone.
<b>Protocol</b>	The connection protocol being used by the phone or application that is now blocked. For example; H. 323, SIP or HTTP.  <ul style="list-style-type: none"> <li>SIP-Message Limiter is displayed for SIP message blacklisting. In this case, the blacklisting is not automatically removed but can be removed manually.</li> </ul>
<b>Client Name</b>	The client name of the blocked application.

**Table 1: Button**

Save Page	Save the current status menu data to a text file in comma separated format.
Log To Sysmon	When selected, the information is added to the Syslog monitor log. A comma separated row is added to the log output for each current entry.
Remove Entries	Remove the current blacklist entries. This allows to attempt to reregister again without having to wait for the expiry of their previous blacklisting.
Cancel	Close the status menu.

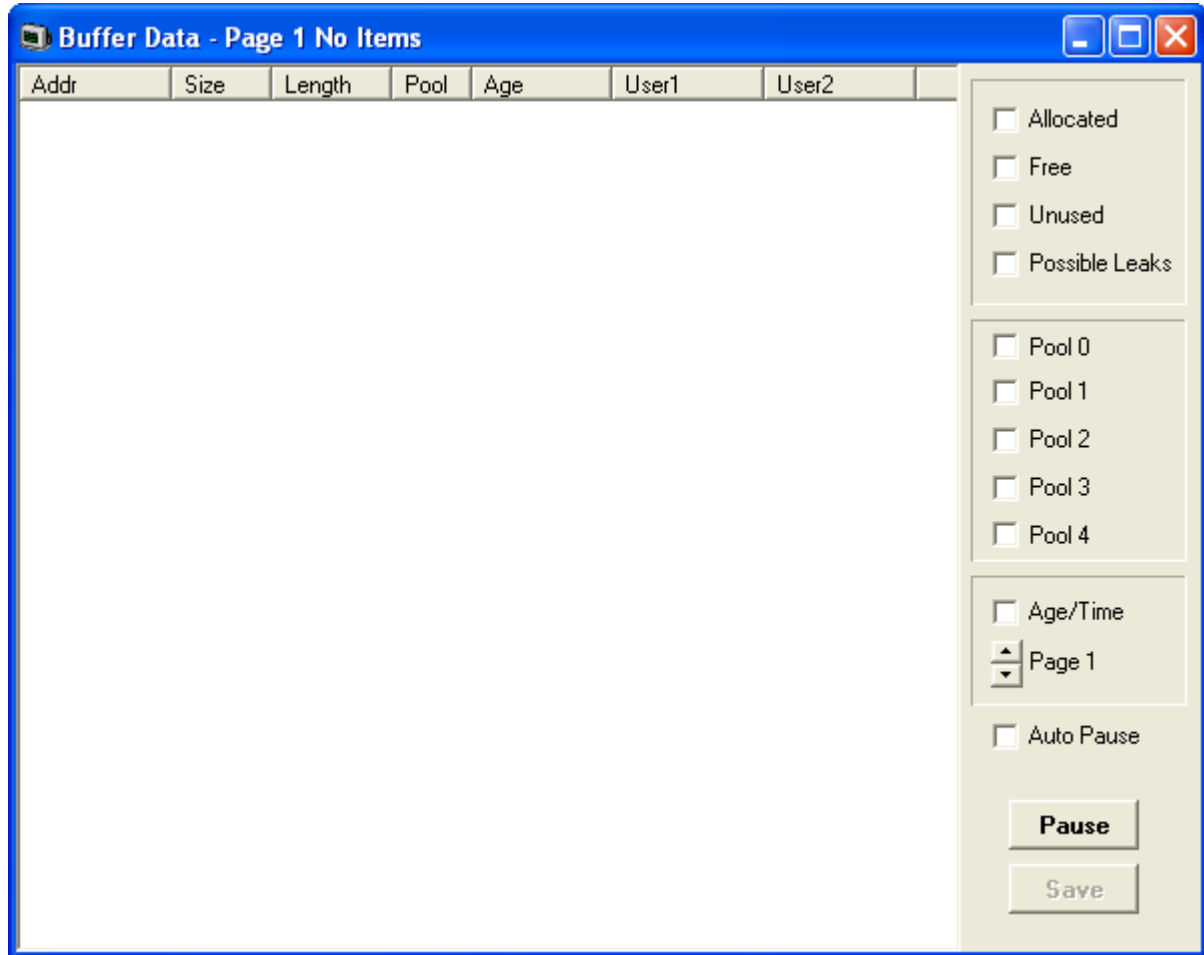
**Related links**

[Status Screens](#) on page 83

## Buffer Data

This menu displays data about the system's memory buffers.





These options are only available when the **Development Tracing** option is selected in the **Filters > Trace Options > System** menu, see [System Trace Options](#) on page 69. They are not covered by this document as they are used by Avaya for product trials and are subject to frequent changes.

These options should only be used under the guidance of an authorized Avaya development engineer.

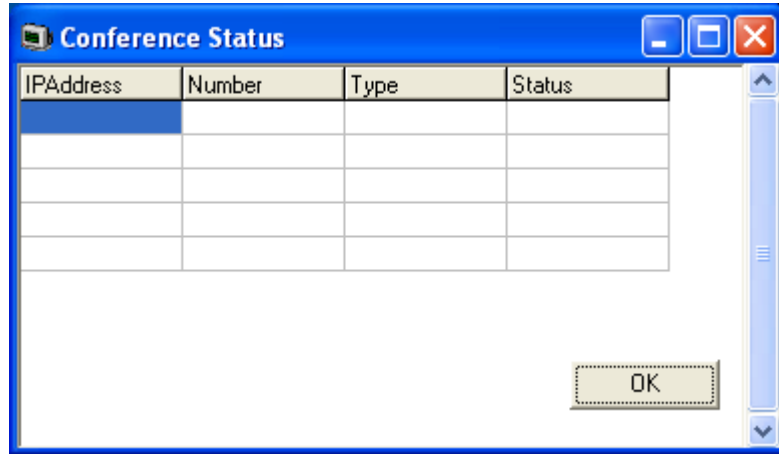
#### Related links

[Status Screens](#) on page 83

---

## Conference Status

This menu displays the status of conference's being supported by the system.



**Related links**

[Status Screens](#) on page 83

---

## DECT Line Status

This menu displays the status of the Internet Protocol (IP) Digital Enhanced Cordless Telecommunications (DECT) lines used by the system. When DECT line resilience is being used multiple lines are displayed with the current status of each line indicated.

**Related links**

[Status Screens](#) on page 83

---

## DHCP Data

This menu displays details of the system's DHCP server settings and the DHCP clients being supported by the system.

The screenshot shows the DHCPStatus window with the following configuration:

- DHCP LAN1:** Mode: Disabled, Number Of Pools: 0, Base IP Address: 0.0.0.0, Number Of IP Addresses: 0, Subnet Mask: 0.0.0.0, Default Route: 0.0.0.0
- DHCP LAN2:** Mode: Disabled, Number Of Pools: 0, Base IP Address: 0.0.0.0, Number Of IP Addresses: 0, Subnet Mask: 0.0.0.0, Default Route: 0.0.0.0
- RESILIENCE:** Mode: Idle,  Select, Number Of IP Addresses: 0

Below the configuration is a checked checkbox for "Filter To Selected Pools" and a table with the following columns: IP Address, Mac Address, Preallocated, LAN / Pool, State, Client Type, and Timer Expiry (ms). The table is currently empty.

At the bottom of the window are buttons for: Force Backup, Erase Backup, Free Address, Fire Timer, Print, and Cancel.

These options are only available when the **Development Tracing** option is selected in the **Filters > Trace Options > System** menu, see [System Trace Options](#) on page 69. They are not covered by this document as they are used by Avaya for product trials and are subject to frequent changes.

These options should only be used under the guidance of an authorized Avaya development engineer.

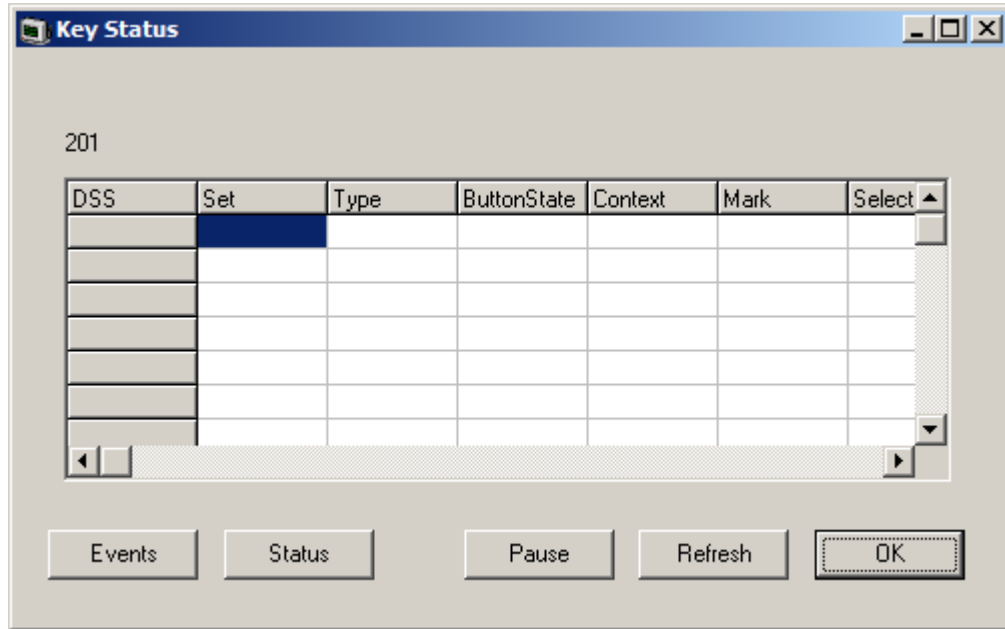
#### Related links

[Status Screens](#) on page 83

---

## DSS Status

This menu displays details of an extension's programmable DSS keys. When selected, the menu prompts for the extension first. The status of that extension's DSS keys are then displayed.



These options are only available when the **Development Tracing** option is selected in the **Filters > Trace Options > System** menu, see [System Trace Options](#) on page 69. They are not covered by this document as they are used by Avaya for product trials and are subject to frequent changes.

These options should only be used under the guidance of an authorized Avaya development engineer.

**Related links**

[Status Screens](#) on page 83

## Equinox Sessions

This menu displays details of equinox client connections to the system.

**Related links**

[Status Screens](#) on page 83

## H323 Phone Status

This menu displays details of the H.323 end points known by the system.

For phones using NAT traversal, the private IP address is shown in the Private Address field. The **IP Address** field displays either the public IP address or, if no NAT Traversal is being used, the IP address. If the phone requires DTMF signaling is shown in the **ReqDTMF** field.

Extn Num	User Num	Phone Type	Licensed	Security	Behind NAT	IP Address	Mac...	Version Id	EP identifier	Status	Registra...	TimeoutV...	TimeLast...	Avera...	Rf
650	650	Unknown	No Licence	disable		0.0.0.0	00-00...	V?	EP?	RAS: UnRe...	0	0s		0secs	0
680		Unknown	No Licence	disable		0.0.0.0	00-00...	V?	EP?	RAS: UnRe...	0	0s		0secs	0
857	857	Unknown	No Licence	disable		0.0.0.0	00-00...	V?	EP?	RAS: UnRe...	0	0s		0secs	0
7501	7501	Unknown	No Licence	disable		0.0.0.0	00-00...	V?	EP?	RAS: UnRe...	0	0s		0secs	0
244	244	1616	Avaya IP	disable		192.168.0.2...	00-07...	1.350B	System_C_5425...	RAS: Regist...	1	240s	26/09/20...	54secs	0

- **Reset Phones** - Cause the phones to restart and reregister.
- **Reregister Phones** - Cause the phones to reregister without restarting.

### Related links

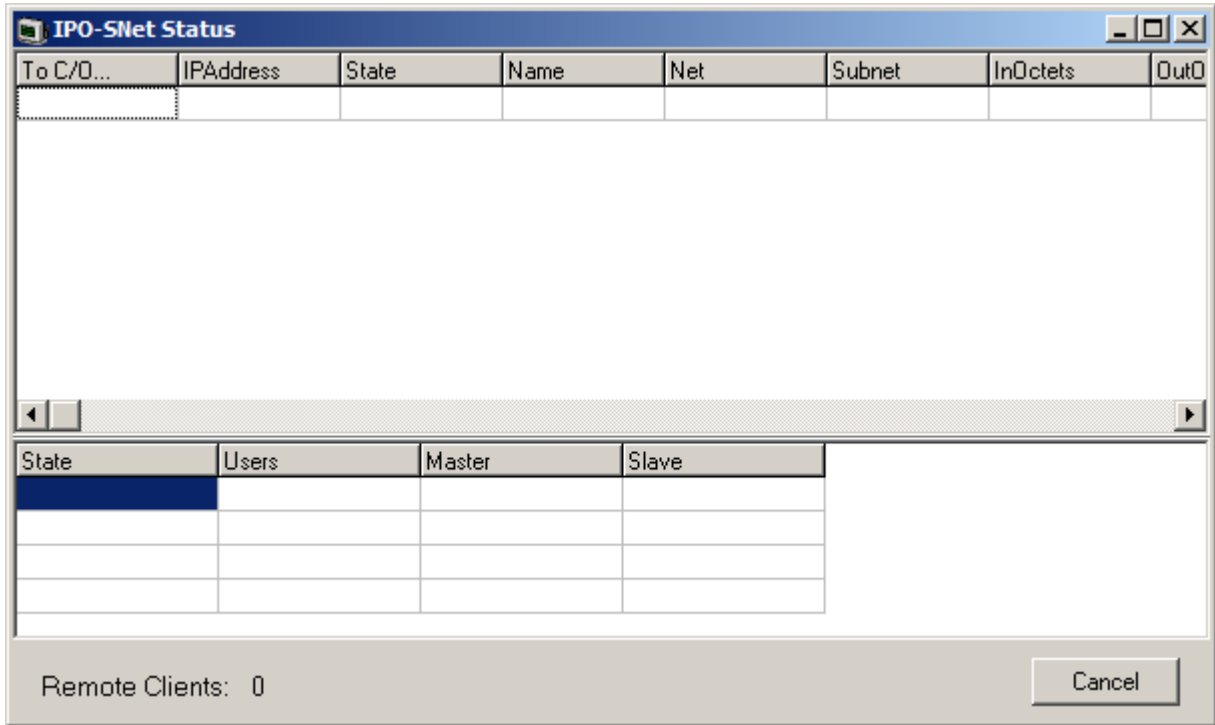
[Status Screens](#) on page 83

---

## IPO-SNet

These options are only available when the **Development Tracing** option is selected in the **Filters > Trace Options > System** menu, see [System Trace Options](#) on page 69. They are not covered by this document as they are used by Avaya for product trials and are subject to frequent changes.

These options should only be used under the guidance of an authorized Avaya development engineer.



**Related links**

[Status Screens](#) on page 83

## IPv6 Config

This status menu is not currently used.

**Related links**

[Status Screens](#) on page 83

## Jade Queue Status

These options are only available when the **Development Tracing** option is selected in the **Filters > Trace Options > System** menu, see [System Trace Options](#) on page 69. They are not covered by this document as they are used by Avaya for product trials and are subject to frequent changes.

These options should only be used under the guidance of an authorized Avaya development engineer.

The screenshot shows the 'JadeQueueStatus' application window. It features four main sections of metrics:

- Live:** Ports: 0, Streams: 0, Queueing: 0
- Counters:** Queued: 0, NotQueued: 0, QLongWait: 0, QAbandoned: 0, LearnedRA: 0, LearnedRP: 0
- Max Counters:** MaxAssigned: 0, MaxLearning: 0, MaxPaging: 0, MaxBusy: 0, MaxWaiting: 0, MaxLWaiting: 0
- Timings (ms):** AvgQTime Assign: 0, AvgQTime Abandon: 0, Queue Longest: 0, Slowest Learn: 0, Avg Learn: 0, Longest LAbandon: 0

Below these sections, it indicates 'Waiting 69 secs for update'. A table with the following columns is present: Lport, Status, Streams, VStreams, RxPackets, TxPackets, RxDiscards, Assigned, VAssigned, Guards. The table is currently empty. At the bottom, there are buttons for 'Log To Sysmon', 'Reset Stats', 'Reset Stream Stats', 'Print', and 'Cancel'.

**Related links**

[Status Screens](#) on page 83

## Logging

These options are only available when the **Development Tracing** option is selected in the **Filters > Trace Options > System** menu, see [System Trace Options](#) on page 69. They are not covered by this document as they are used by Avaya for product trials and are subject to frequent changes.

These options should only be used under the guidance of an authorized Avaya development engineer.

**Related links**

[Status Screens](#) on page 83

# Map Status

	TDM0	TDM1	TDM2	TDM3	TDM4	TDM5	TDM6	TDM7	TDM8	TDM9	TDM10	TDM11	TDM12	TDM13	TDM14	TDM15	TDM16	TDM17	TDM18	TDM19	TDM20	TDM21	
CH:0																							
CH:1									21.1	21.33	21.2	21.34	21.3	21.35	21.4	21.36						8.1	
CH:2																							10.1
CH:3																							12.1
CH:4																							14.1
CH:5																							
CH:6																							
CH:7																							
CH:8																							
CH:9																							
CH:10																							
CH:11																							
CH:12																							
CH:13																							
CH:14																							
CH:15																							
CH:16																							
CH:17																							
CH:18																							
CH:19																							
CH:20																							
CH:21																							
CH:22																							
CH:23																							
CH:24																							
CH:25																							
CH:26																							
CH:27																							
CH:28																							
CH:29																							
CH:30																							
CH:31																							
CH:32																							
CH:33																							9.1
CH:34																							11.1

**Related links**

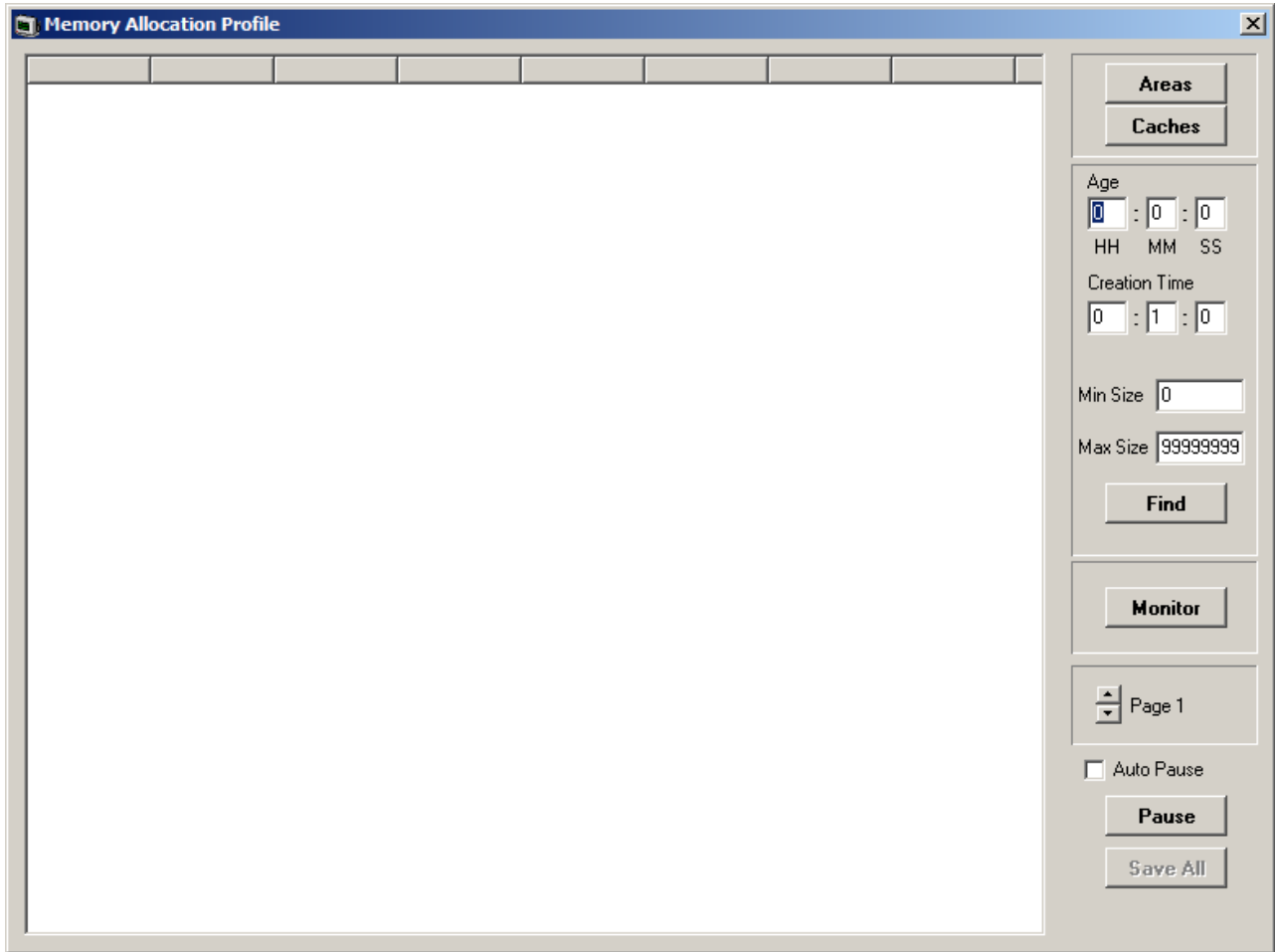
[Status Screens](#) on page 83

# Memory Data

These options are only available when the **Development Tracing** option is selected in the **Filters > Trace Options > System** menu, see [System Trace Options](#) on page 69. They are not covered by this document as they are used by Avaya for product trials and are subject to frequent changes.

These options should only be used under the guidance of an authorized Avaya development engineer.





### Related links

[Status Screens](#) on page 83

---

## NAPT Status

These options are only available when the **Development Tracing** option is selected in the **Filters > Trace Options > System** menu, see [System Trace Options](#) on page 69. They are not covered by this document as they are used by Avaya for product trials and are subject to frequent changes.

These options should only be used under the guidance of an authorized Avaya development engineer.

## Status Screens

The screenshot shows the 'NAPT Status' window. At the top, there is a summary table with the following data:

Interface	Protocol	Session Count	Session Displayed
LAN1		0	0
Internet01	Static NAT	0	0

Below this summary are 'Pause' and 'Quit' buttons. To the right, under 'Filter Options', there are checkboxes and text input fields for filtering by IP Address 1, IP Address 2, Port 1, and Port 2.

The main part of the window is a large table with the following headers:

Remote IP	Remote Port	Inbound IP	Inbound Port	Outbound IP	Outbound Port	Type	Session TTL (ms)	Age (ms)	Max Age (ms)	Last Used

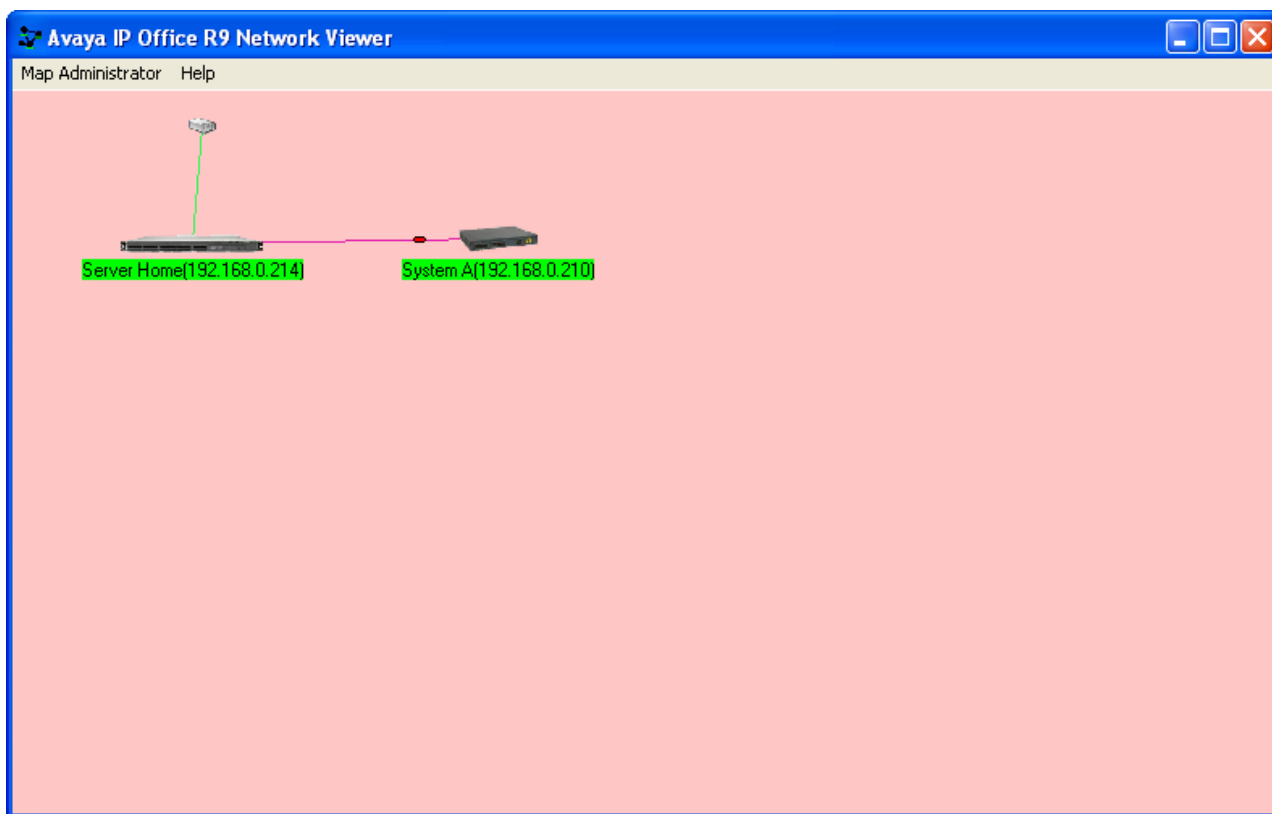
### Related links

[Status Screens](#) on page 83

---

## Network View

This menu displays a view of the multi-site network of which the system is a part. It displays calls between the sites. This menu is not supported when using TCP, HTTP or HTTPS to connect.



### Related links

[Status Screens](#) on page 83

---

## Outdialer Status

This menu shows a summary of the activity of the outdialing server supported by the system.

**Outdialer Status**

**Campaign**

- Calls: 0
- Answered: 0
- ConnAgt: 0
- Timeout: 0
- Managed: 0
- Failed: 0

**Current**

- Idle%: 0.00
- Ring %: 0.00
- Conn %: 0.00
- Talk%: 0.00
- OnCall%: 0.00

**Trunks**

#	state	call	agent

**Agents**

agent	state

**Domains**

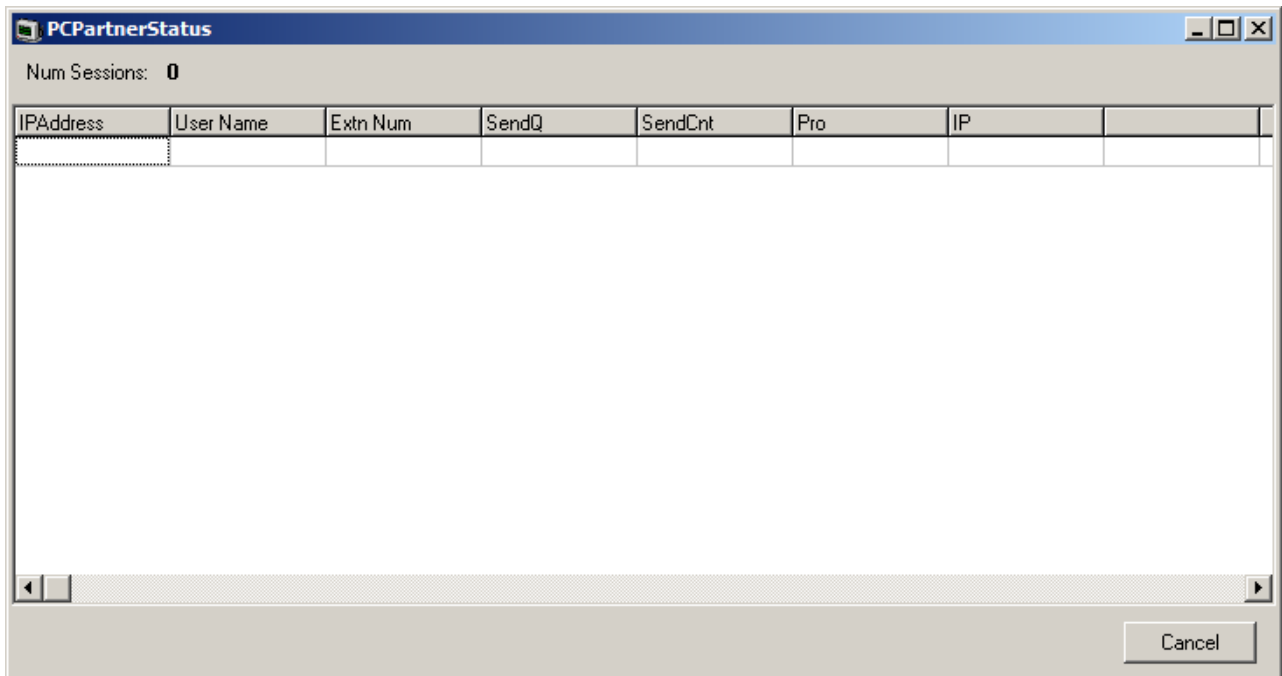
Domain

Cancel

**Related links**  
[Status Screens](#) on page 83

## Partner Sessions

This menu displays details of the connections for IP Office PCPartner applications (SoftConsole) to the system.



PCPartnerStatus

Num Sessions: 0

IPAddress	User Name	Extn Num	SendQ	SendCnt	Pro	IP		

Cancel

#### Related links

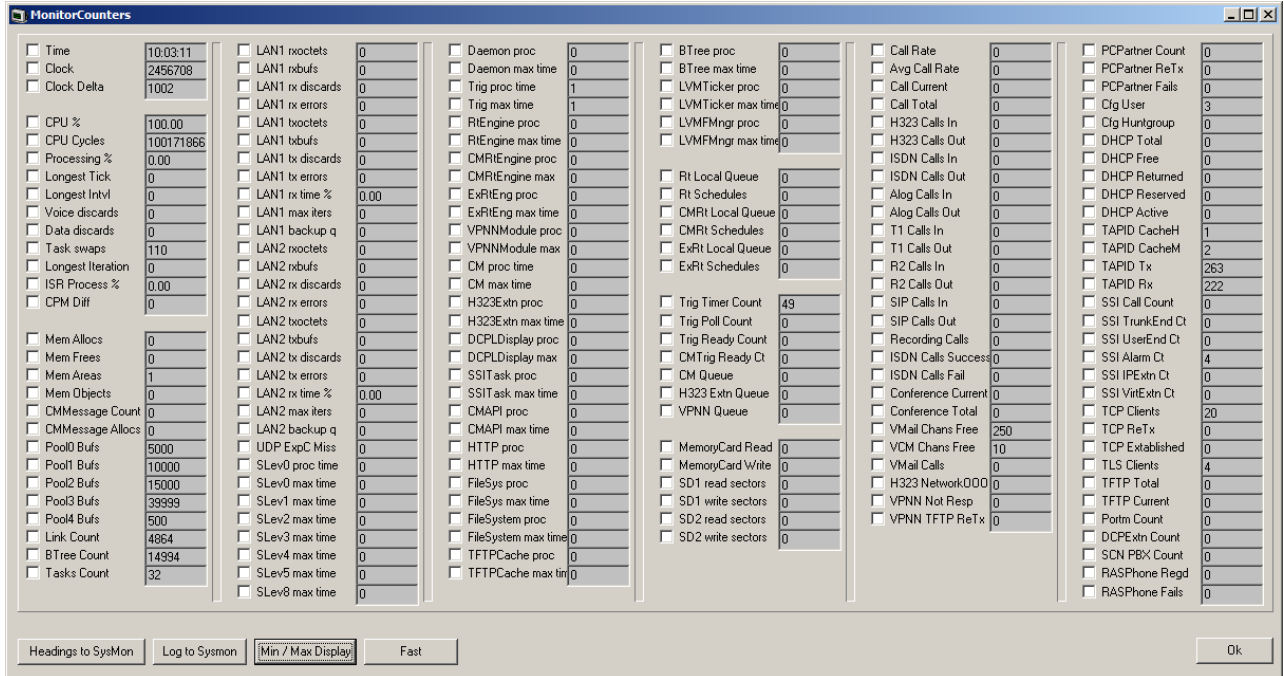
[Status Screens](#) on page 83

---

## Performance Data

These options are only available when the **Development Tracing** option is selected in the **Filters > Trace Options > System** menu, see [System Trace Options](#) on page 69. They are not covered by this document as they are used by Avaya for product trials and are subject to frequent changes.

These options should only be used under the guidance of an authorized Avaya development engineer.



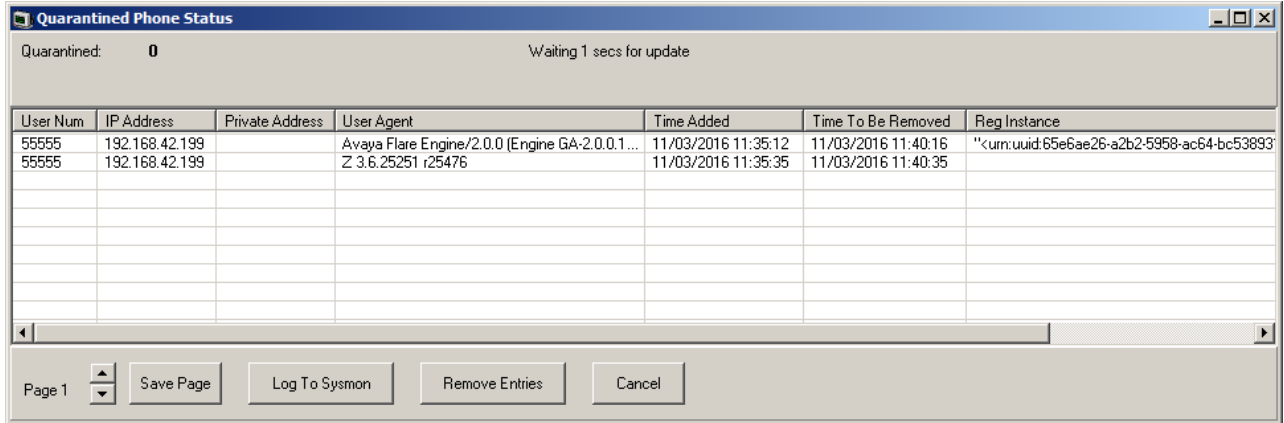
**Related links**

[Status Screens](#) on page 83

## Quarantined Phone Status

This menu displays phones that have previously been registered but are now blocked from re-registering because another phone has subsequently registered using the same registration parameters. This blocked state is called quarantined.

- For example: When a user who has an already registered on one phone then registers on another phone using the same parameters, the previous phone may automatically attempt to reregister itself. In that case, even though the previous phone is presenting correct registration details, its registration is blocked and it is quarantined.



- The default quarantine time is five minutes. However, if the phone keeps on trying to reregister, its quarantine time is extended. Most phones eventually cease attempting to automatically re-register.
- Quarantining is treated separately from blacklisting since the phone has been previously registered with correct authentication parameters.
- Quarantining honors the restrictions for simultaneous telephony device use by users. For example, such users can simultaneously register one physical deskphone (including SIP, H.323 and DECT), one desktop PC VoIP client, one mobile VoIP client and one WebRTC client.

**Columns**

<b>User Num</b>	The extension number.
<b>IP Address</b>	The phone's public IP address.
<b>Private Address</b>	The phone's private IP address.
<b>User Agent</b>	The device type string. This can help identify the phone type.
<b>Time Added</b>	The date and time when phone was added to the quarantined phones list.
<b>Time To Be Removed</b>	The current date and time when the phone will be removed from the quarantined phones list. This will extend if the phone attempts to re-register again before this time.
<b>Reg Instance</b>	For SIP phones, the protocol parameter used during registration. This can be useful to distinguish between simultaneous phones where whilst 'roaming' and changing the IP address the instance remains fixed.
<b>Reg ID</b>	N.A

**Buttons**

<b>Save Page</b>	Save the current status menu data to a text file in comma separated format.
------------------	---

*Table continues...*

<b>Log To Sysmon</b>	When selected, the information is added to the <a href="#">Syslog tracing</a> on page 75. A comma separated row is added to the log output for each current entry.
<b>Remove Entries</b>	Remove the current quarantined entries. This allows them to attempt to reregister again.
<b>Cancel</b>	Close the status menu.

**Related links**

[Status Screens](#) on page 83

## SCN Licence

The menu displays details of the available and those used in a Server Edition network.

The screenshot shows a window titled "SCN Licence status" with the following sections:

**Server Data:**

PBX	dongle	Server Edition req	Alloc	Power User req	Alloc	Avaya Phones req	Alloc	3pty Phones req	Alloc	Office Worker req	Alloc	SIP Channels req	Alloc
Self	--NA--	0R8.1	0	0	0	0+0	0	0+0	0	0	0	0	0
Totals		0	0	0	0	0+0	0	0+0	0	0	0	0	0
Available		0		0		0		0		0		0	

**Client Data:**

- Licence Server: <unset>
- Last Refresh: <unset>
- Max Software Upgrade: <unset>
- Upgrade Licence Deficiency: <unset>

Licence	Allocated	Reserved Need	UnReserved Need

Buttons: Cancel

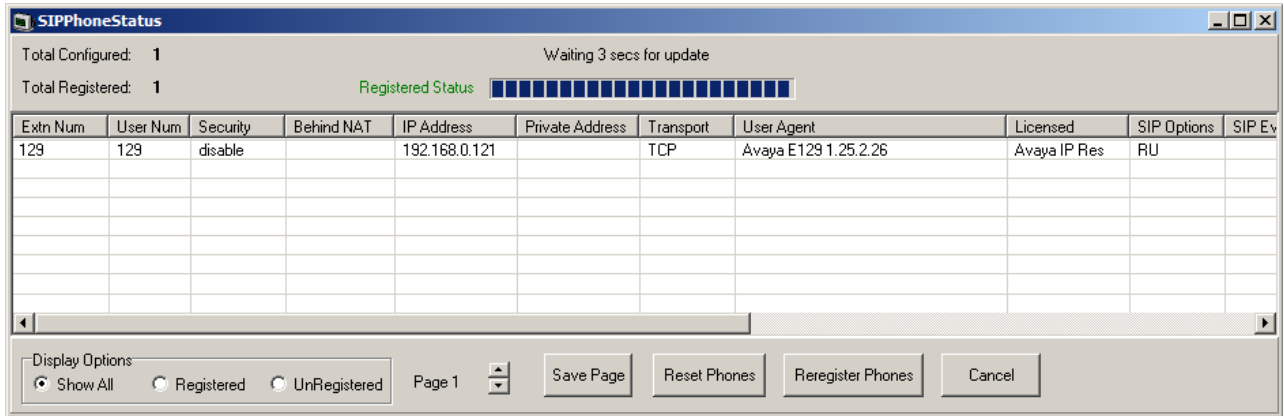
**Related links**

[Status Screens](#) on page 83



## SIP Phone Status

This menu displays the status of the SIP end points known by the system.



For IP OfficeRelease 10, for phones using Network Address Translator (NAT) traversal, the private IP address is shown in the **Private Address** field. The **IP Address** field displays either the private IP address or if not NAT traversal is being used it displays public IP address.

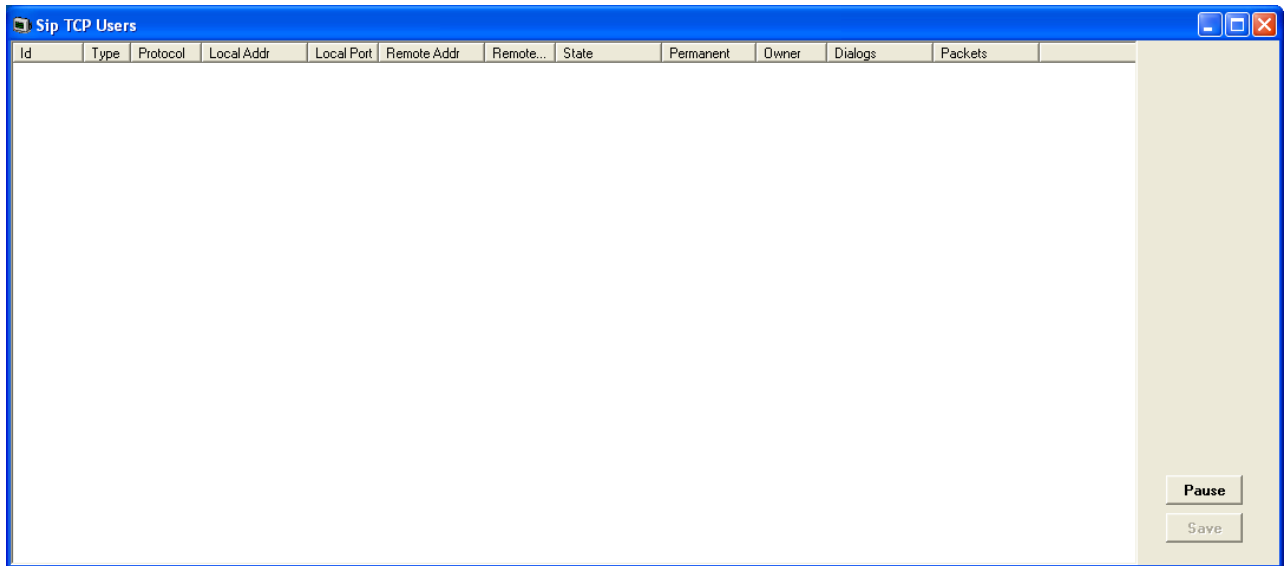
Whether the phone requires Dual-tone Multi Frequency (DTMF) signalling is shown in the **ReqDTMF** field.

<b>Save Page</b>	Save the current status menu data to a text file in comma separated format.
<b>Reset Phones</b>	Cause the registered SIP phones to restart and subsequently re-register. Only supported with Avaya SIP phones.
<b>Reregister Phones</b>	De-register all SIP phones from the system. Those phones that support the <i>REGISTER</i> event are informed, which causes them to re-register with the system. This action also clears the list of <a href="#">Quarantined phones status</a> on page 102 and allows them to reregister if present.

### Related links

[Status Screens](#) on page 83

## SIP TCP User Data

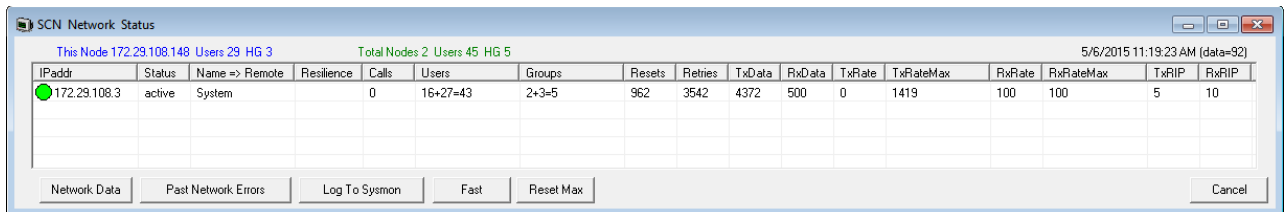


**Related links**

[Status Screens](#) on page 83

## Small Community Networking

This menu displays the status of the system's multi-site network connections.



<b>Network Data</b>	Display a summary of the known details of the other network nodes.
<b>Past Network Errors</b>	
<b>Log To Sysmon</b>	When selected, the menu information is added to the <b>Syslog Monitor</b> output every 5 seconds. The button changes to <b>Stop Log</b> and is used to stop the logging output. A comma separated row is added to the log output for each SCN link.
<b>Fast</b>	When selected, it changes the menu update rate from every 8 seconds to every second.

*Table continues...*

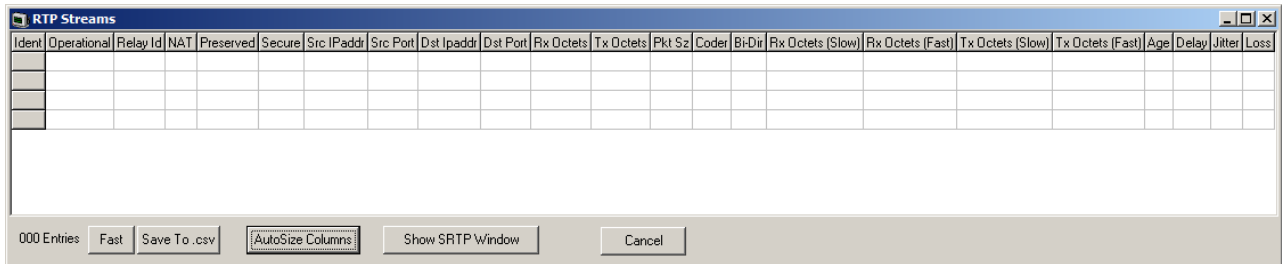
<b>Slow</b>	When selected, it changes the menu update rate from every second to every 8 seconds
<b>Reset Max</b>	The <b>TxRateMax</b> and <b>RxRateMax</b> columns show the maximum values whilst the menu is running. This button resets the values.

**Related links**

[Status Screens](#) on page 83

## [S]RTP Sessions

This status menu displays details of the Real-Time Transport Protocol (RTP) and Secure Real-time Transport Protocol (SRTP) sessions being supported by the system.

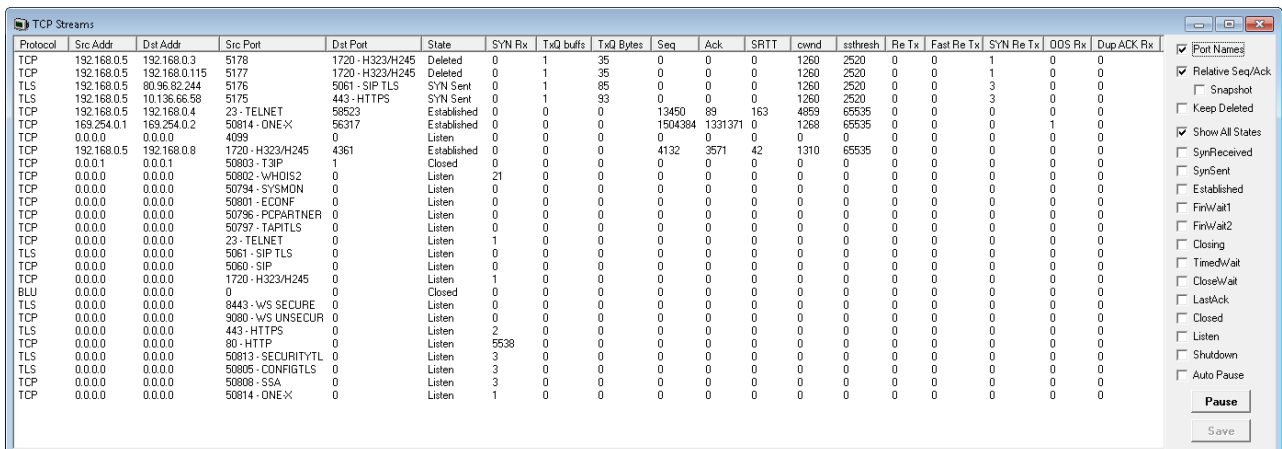


- **Fast** - Changes the menu update rate from every eight seconds to every second.
- **Slow** - Changes the menu update rate from every second to every eight seconds.

**Related links**

[Status Screens](#) on page 83

## TCP Streams Data



**Related links**

[Status Screens](#) on page 83

---

## US PRI Trunks

This menu displays the status of the system's US PRI trunk channels.

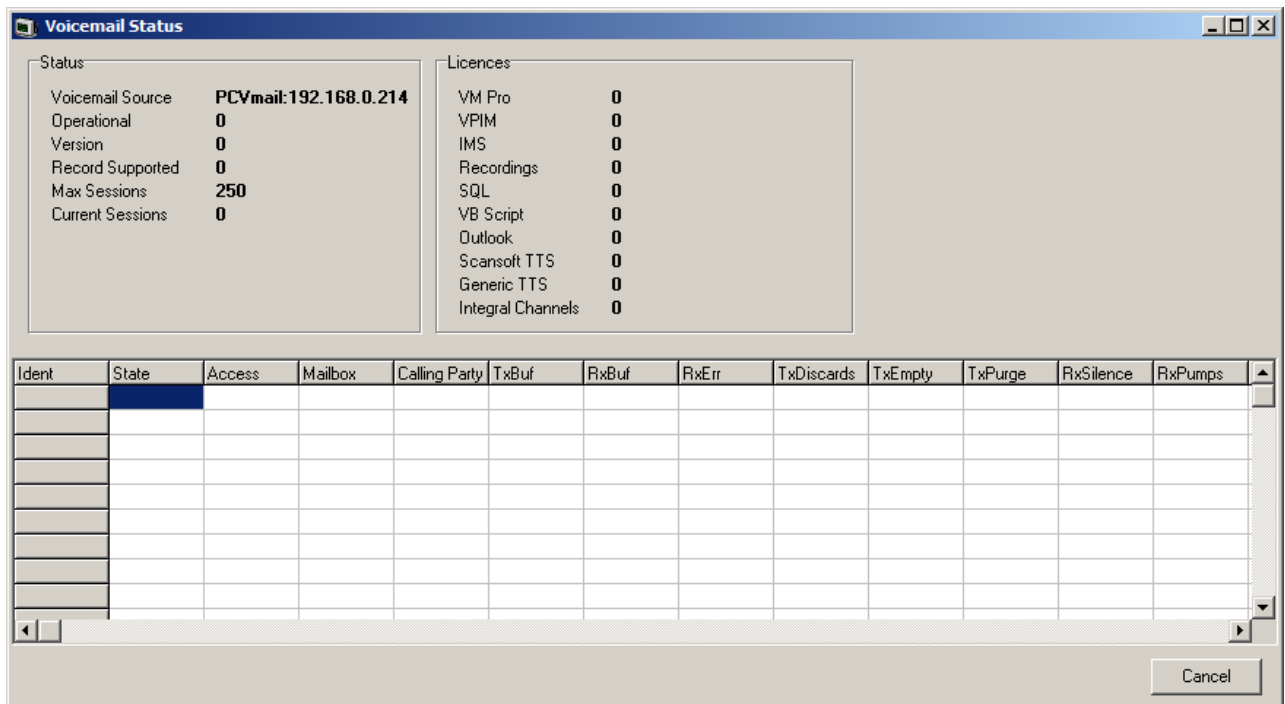
**Related links**

[Status Screens](#) on page 83

---

## Voicemail Sessions

The status screen displays a summary of the voicemail service connections.



**Related links**

[Status Screens](#) on page 83

## Voice Compression

These options are only available when the **Development Tracing** option is selected in the **Filters > Trace Options > System** menu, see [System Trace Options](#) on page 69. They are not covered by this document as they are used by Avaya for product trials and are subject to frequent changes.

These options should only be used under the guidance of an authorized Avaya development engineer.

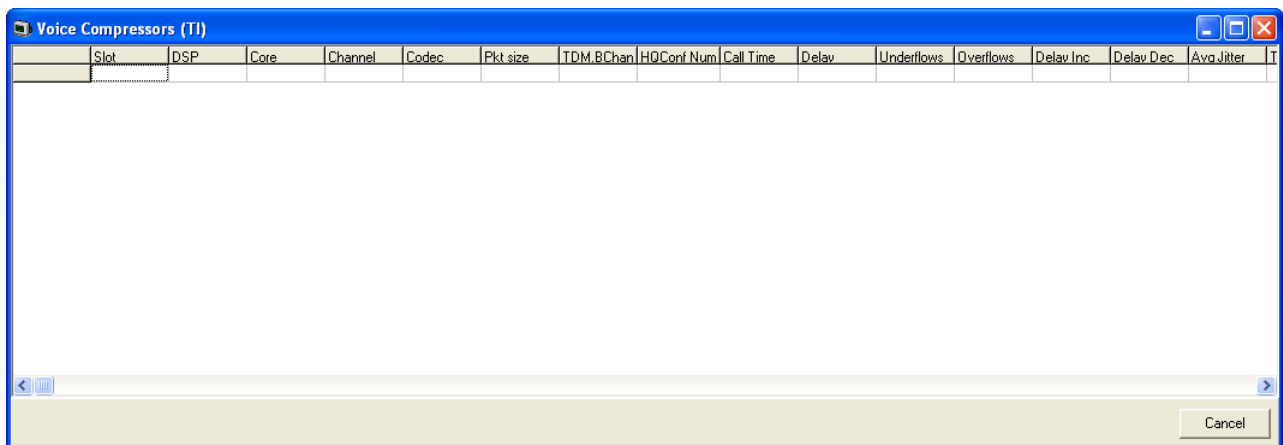
### Related links

[Status Screens](#) on page 83

## Voice Compression (TI)

These options are only available when the **Development Tracing** option is selected in the **Filters > Trace Options > System** menu, see [System Trace Options](#) on page 69. They are not covered by this document as they are used by Avaya for product trials and are subject to frequent changes.

These options should only be used under the guidance of an authorized Avaya development engineer.



Slot	DSP	Core	Channel	Codec	Pkt size	TDM.BChan	HQConf Num	Call Time	Delay	Underflows	Overflows	Delay Inc	Delay Dec	Avg Jitter	TI

### Related links

[Status Screens](#) on page 83

# Chapter 10: Example Monitor Settings

The typical monitor settings to provide useable traces in different test and diagnosis scenarios is explained. With depth data and telecoms experience the interpretation of the resulting traces can be explained.

## Related links

- [J100 Phone Troubleshooting](#) on page 110
- [Analog Trunk Caller ID](#) on page 111
- [ISDN Trunk Caller ID](#) on page 112
- [ISDN Calls Disconnecting](#) on page 113
- [System Rebooting](#) on page 115
- [ISDN Problems \(T1 or E1 PRI Connections\)](#) on page 116
- [ISP & Dial-Up Data Connection Problems](#) on page 116
- [Remote Site Data Connection over Leased \(WAN\) Lines](#) on page 117
- [Frame Relay Links](#) on page 117
- [Problems Involving Non-IP Phones](#) on page 118
- [Problems Involving IP Phones](#) on page 118
- [Locating a Specific PC Making Calls to the Internet](#) on page 118
- [Firewall Not Working Correctly](#) on page 119
- [Calls Answered/Generated by IP Office Applications](#) on page 120
- [Message Waiting Indication](#) on page 120
- [Speech Calls Dropping](#) on page 121

---

## J100 Phone Troubleshooting

### IP Office

- SysMonitor
  - Enable the default tracing: **Filters > Trace Options > Default All.**
  - **SysMonitor > Filters > Trace Options > H.323 > CCMS Send/CCMS Receive.**
  - **SysMonitor > Filters > Trace Options > SIP > Verbose, SIP Stim Rx, SIP Stim Tx, SIP Rx, SIP Tx.**
- IP Office configuration file

- Wireshark traces

## Phone

- Phone Log level set to Debug, Log categories : ALSIP, CCMS, IPODATA, SIP, MEDIA, SECURITY, CERTMGMT, HTTP.
- Remote Syslog server
- When log categories are checked, phone performance may be degraded due to hardware limitation. After capturing logs clear the log categories

## Related links

[Example Monitor Settings](#) on page 110

---

# Analog Trunk Caller ID

The following is an example trace from an analogue trunk that supports Incoming Call Line Identification (ICLID) or Calling Line Identification (CLI).

```

108691mS PRN: AtmTrunk1: StateChange CLIPossibleIncoming->Idle
108692mS PRN: AtmIO1: Block Forward OFF
108692mS PRN: AtmIO1: CLI Detection ON Equaliser ON
109703mS PRN: AtmTrunk1: CLI Message Rx'd:
109703mS PRN: 0x4500
109704mS PRN: 0x3031
109704mS PRN: 0x3134
109704mS PRN: 0x3136
109704mS PRN: 0x3035
109705mS PRN: AtmTrunk1: CLI Message Rx'd:
109705mS PRN: 0x4980
109706mS PRN: 0x3031
109706mS PRN: 0x3730
109706mS PRN: 0x372d
109706mS PRN: 0x3339
109706mS PRN: 0x3033
109707mS PRN: 0x3931
109707mS PRN: AtmTrunk1: CLI Message Rx'd:
109707mS PRN: 0x5800
09708mS PRN: AtmIO1: CLI Detection OFF Equaliser OFF
109708mS PRN: AtmTrunk1: StateChange CLIAwaitData->CLIDataSettle
109911mS PRN: AtmTrunk1: StateChange CLIDataSettle->CLIAwaitSecondRing
110191mS PRN: AtmTrunk1: StateChange CLIAwaitSecondRing->PossibleIncoming

```

## Explanation:

108691mS PRN: AtmTrunk1: StateChange CLIPossibleIncoming->Idle	The Line interface is primed ready for the possibility of an incoming ICLID/CLI message.
108692mS PRN: AtmIO1: Block Forward OFF	AtmIO1 = Line Number 1.
108692mS PRN: AtmIO1: CLI Detection ON Equaliser ON	CLI detection is enabled for trunk 1.
109703mS PRN: AtmTrunk1: CLI Message Rx'd:	The first part of a ICLID message on trunk 1 is detected.

*Table continues...*

## Example Monitor Settings

109703mS PRN: 0x4500	4500 = Date and time information. The info then follows in the 4 byte words.
109704mS PRN: 0x3031 109704mS PRN: 0x3134 109704mS PRN: 0x3136 109704mS PRN: 0x3035	The call date and time is 16:05 on 14th January. <ul style="list-style-type: none"> <li>Month: 30 (hex) = 0 (ASCII), 31 (hex) = 1 (ASCII) &gt; 01 (January)</li> <li>Day: 31 (hex) = 1 (ASCII), 34 (hex) = 4 (ASCII) &gt; 14th.</li> <li>Hours: 31 (hex) = 1 (ASCII), 36 (hex) = 6 (ASCII) &gt; 16:00.</li> <li>Minutes: 30 (hex) = 0 (ASCII), 35 (hex) = 5 (ASCII) &gt; 00:05.</li> </ul>
109705mS PRN: AtmTrunk1: CLI Message Rx'd:	The second part of the ICLID message on trunk 1 is detected.
109705mS PRN: 0x4980	4980 = Calling Party Number information.
109706mS PRN: 0x3031 109706mS PRN: 0x3730 109706mS PRN: 0x372d 109706mS PRN: 0x3339 109706mS PRN: 0x3033 109707mS PRN: 0x3931	The Calling Party Number is 01707-390391 <ul style="list-style-type: none"> <li>30 (hex) = 0 (ASCII), 31 (hex) = 1 (ASCII) &gt; 01</li> <li>37 (hex) = 7 (ASCII), 30 (hex) = 0 (ASCII) &gt; 70</li> <li>37 (hex) = 7 (ASCII), 2d (hex) = - (ASCII) &gt; 7-</li> <li>33 (hex) = 3 (ASCII), 39 (hex) = 9 (ASCII) &gt; 39</li> <li>30 (hex) = 0 (ASCII), 33 (hex) = 3 (ASCII) &gt; 03</li> <li>39 (hex) = 9 (ASCII), 31 (hex) = 1 (ASCII) &gt; 91</li> </ul>
109707mS PRN: AtmTrunk1: CLI Message Rx'd:	The third part of the ICLID message on trunk 1 is detected.
109707mS PRN: 0x5800	5800 = End of ICLID.
09708mS PRN: AtmIO1: CLI Detection OFF Equaliser OFF	ICLID detection is disabled.
109708mS PRN: AtmTrunk1: StateChange CLIAwaitData->CLIDataSettle 109911mS PRN: AtmTrunk1: StateChange CLIDataSettle->CLIAwaitSecondRing 110191mS PRN: AtmTrunk1: StateChange CLIAwaitSecondRing->PossibleIncoming	Line state changes from receiving ICLID to awaiting the incoming audio call.

### Related links


[Example Monitor Settings](#) on page 110

## ISDN Trunk Caller ID

### Procedure

1. Go to **Start > Programs > IP Office > Monitor**.



2. On the **System Monitor**, click  **Trace Options** to select the trace settings.
3. In **Call** tab, select **Line Receive** check box.
4. Click **OK**.

In the System Monitor window, look for trace codes similar to the following:

```
22984658mS ISDNL3Rx: v=5 peb=5
ISDN Layer3 Pcol=08(Q931) Reflen=2 ref=272F(Remote)
Message Type = Setup
InformationElement = BearerCapability
0000 04 03 80 90 a2 .....
InformationElement = CHI
0000 18 03 a1 83 95 .....
InformationElement = CallingPartyNumber
0000 6c 0c 21 83 36 31 38 37 30 39 33 39 39 31 1.!.6187093991
InformationElement = CalledPartyNumber
0000 70 08 c1 36 34 36 37 31 33 31 p..6467131
InformationElement = HigherLayerCompat
0000 7d 02 91 81 }...
```

- The Calling Party Number is (6187093991)
- The Called Party Number is (6467131)

#### Related links

[Example Monitor Settings](#) on page 110

---

## ISDN Calls Disconnecting

Enable the following trace option settings:

Tab	Trace Options
<b>ISDN</b>	Layer 1, Layer 2, Layer 3, Layer 1 Send, Layer 1 Receive, Layer 2 Send, Layer 2 Receive, Layer 3 Send and Layer 3 Receive.
<b>Call</b>	Extension Send, Extension Receive, Extension TxP, Extension RxP, Line Send, Line Receive, Targetting and Call Logging.
<b>System</b>	Error, Print and Resource Status Prints.

The following is a sample trace of an Primary Rate Interface (PRI) line going down, cutting off the calls in progress and then the line coming back up:

```
1072151mS ISDNL1Evt: v=0 peb=5,F2 F1
1072651mS ISDNL1Evt: v=0 peb=5,PHDI ?
1072651mS ISDNL3Evt: v=0 p1=0,p2=1001,p3=5,p4=127,s1=
1072651mS ISDNL3Evt: v=0 stacknum=0 State, new=NULLState, old=Active id=4
1072652mS ISDNL3Evt: v=0 stacknum=0 State, new=NULLState, old=Active id=24
1072653mS ISDNL3Evt: v=0 p1=0,p2=1001,p3=5,p4=0,s1=
1072656mS CMLineRx: v=5
CMReleaseComp
Line: type=Q931Line 5 Call: lid=5 id=4 in=1
Cause=38, Network000
1072658mS CALL:2000/11/2408:40,00:00:17,033,01732464420,I,300,027624,,,,,0
1072682mS CMLineRx: v=5
CMReleaseComp
```

## Example Monitor Settings

```
Line: type=Q931Line 5 Call: lid=5 id=24 in=1
Cause=38, Network000
1072684mS CALL:2000/11/2408:36,00:04:12,004,01689839919,I,300,027624,,,,,0
1075545mS ISDNLEvt: v=0 peb=5,F1 F2
1075595mS ISDNLEvt: v=0 peb=5,PHAI ?
```

### Explanation:

1072151mS ISDNLEvt: v=0 peb=5,F2 F1	PRI Line 5 (peb is 5) has gone from the F1 state (normal Operational state) to the F2 state (Fault condition 1 state - receiving RAI or receiving CRC errors).
1072651mS ISDNLEvt: v=0 peb=5,PHDI ?	Line 5 (peb is 5) is now in the Disconnected state (PHDI – Physical Deactivate Indication).
1072651mS ISDNLEvt: v=0 p1=0,p2=1001,p3=5,p4=127,s1=	ISDN Layer 3 event which gives current status of line 5 (p3 is 5) <ul style="list-style-type: none"> <li>• P1 is 0: ISDN Stacknum is 0.</li> <li>• P2 is 1001: Line Disconnecting.</li> <li>• P3 is 5: Internal reference number.</li> <li>• P4 is 127: TEI is 127 and S1 is not used.</li> </ul>
1072651mS ISDNLEvt: v=0 stacknum=0 State, new=NULLState, old=Active id=4	ISDN Layer 3 event which indicates that call with id 4 (id is 4) on the first ISDN stack (stacknum is 0) has changed from being Active (old is Active) to No Call exists (new is NULLState).
1072652mS ISDNLEvt: v=0 stacknum=0 State, new=NULLState, old=Active id=24	ISDN Layer 3 event which indicates that call with id 24 (id is 24) on the first ISDN stack (stacknum is 0) has changed from being Active (old is Active) to No Call exists (new is NULLState).
1072653mS ISDNLEvt: v=0 p1=0,p2=1001,p3=5,p4=0,s1=	ISDN Layer 3 event which gives current status of line 5 (p3 is 5) <ul style="list-style-type: none"> <li>• P1 is 0: ISDN Stack number is 0.</li> <li>• P2 is 1001: Line Disconnecting.</li> <li>• P3 is 5: Internal reference number.</li> <li>• P4 is 0: TEI is 0.</li> <li>• S1 is not used.</li> </ul>
1072656mS CMLineRx: v=5 CMReleaseComp Line: type=Q931Line 5 Call: lid=5 id=4 in=1 Cause=38, Network000	The incoming call (in is 1) on line 5 (lid is 5), with an internal call id of 4 (id is 4) has been dropped. Clear code is 38 – Network Out Of Order (refer to ISDN Clear codes on our web site). There is no ISDNLEvt trace information as the call is dropped by the PBX NOT by the local exchange (due to the fact that we are no longer in communication with the Local Exchange!).
1072658mS CALL:2000/11/2408:40,00:00:17,033,017 32464420,I,300,027624,,,,,0	The Incoming call from 01732464420 to [02083]027624 (Extn 300) has been disconnected.

*Table continues...*

1072682mS CMLineRx: v=5 CMReleaseComp Line: type=Q931Line 5 Call: lid=5 id=24 in=1 Cause=38, Network000	The incoming call (in is 1) on line 5 (lid is 5), with an internal call id of 24 (id is 24) has been dropped. Clear code is 38 – Network Out Of Order (refer to ISDN Clear codes on our web site). Again there is no ISDNL3RX trace information as the call is dropped by the PBX NOT by the local exchange (due to the fact that we are no longer in communication with the Local Exchange!).
1072684mS CALL:2000/11/2408:36,00:04:12,004,016 89839919,I,300,027624,,,,0	The incoming call from 01689839919 to [02083]027624 (Extn300) has been disconnected.
1075545mS ISDNL1Evt: v=0 peb=5,F1 F2	Line 5 (peb is 5) has gone from the F2 state (Fault condition 1 state i.e. receiving RAI or receiving CRC errors) to the F1 state (normal Operational state).
1075595mS ISDNL1Evt: v=0 peb=5,PHAI ?	Line 5 (peb is 5) has now fully recovered and is in the Connected state (PHAI – Physical Activate Indication).

### Related links

[Example Monitor Settings](#) on page 110

---

## System Rebooting

Enable the following trace option settings:

Tab	Trace Options
Call	Line Send, Line Receive, Extension Send, Extension Receive, Extension RxP, Extension TxP, Call Delta, Map, Targeting and Call Logging
System	Error, Print and Resource Status Prints.

It is necessary to capture the data that is output of the Data Terminal Equipment (DTE) port placed on the back of the system control unit. The unit sends information to the DTE port during a reboot that is not seen by **System Monitor** as it cannot make contact with the unit via the LAN until the reboot is completed.

If you are experiencing a rebooting problem then it is very important that both traces are provided in order to make an effective investigation into the problem. Both traces should cover the period before and after the reboot occurs.

A reboot can be easily seen in the System Monitor application by the following:

```
== 25/4/2000 14:27 contact lost - reselect = 1
*****
***** From: 192.168.27.1 (13597) *****
== 25/4/2000 14:27 contact made
```

The **System Reboot** can be easily located, search for the trace (contact lost).

### Related links

[Example Monitor Settings](#) on page 110

## ISDN Problems (T1 or E1 PRI Connections)

Enable the following trace option settings. These provide information about the ISDN line itself and any calls in progress.

Tab	Trace Options
<b>ISDN</b>	Layer 1, Layer 2, Layer 3, Layer 1 Send, Layer 1 Receive, Layer 2 Send, Layer 2 Receive, Layer 3 Send and Layer 3 Receive.
<b>Call</b>	Extension Send, Extension Receive, Extension TxP, Extension RxP, Line Send, Line Receive, Targetting and Call Logging.
<b>System</b>	Error, Print and Resource Status Prints.

If the problem is with a specific ISDN line then the System Monitor can record info for a specific line by entering an ISDN line number in the **Port Number** field. ISDN line numbers range from 0 to 8. The line number is displayed in the **Configuration Lines List**. A blank entry indicates that all ISDN lines are monitored.

### Related links

[Example Monitor Settings](#) on page 110

## ISP & Dial-Up Data Connection Problems

Enable the following trace option settings:

Tab	Trace Options
<b>ISDN</b>	Later3 Tx and Layer3 Rx.
<b>Call</b>	Line Send, Line Receive, Targetting and Call Logging
<b>Interface</b>	Interface/Interface Queue
<b>PPP</b>	LCP Tx, LCP Rx, Security Tx, Security Rx, IPCP Tx and IPCP Rx.
<b>System</b>	Error, Print and Resource Status Prints.

If the problem is to a specific destination then **System Monitor** can record information pertinent to that connection only. This is done by entering the appropriate service name in the **Interface Name** field in the **PPP** trace option settings. A blank entry means monitor all data connections.

You should also look for things like Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP) password failure. This indicates that the *Service* configuration is not correct.

Note that the WAN Tx and WAN Rx information is in raw hex format only. An in-depth knowledge of the IP Packet make-up is required to manually decode these messages and it is not done automatically.

### Related links

[Example Monitor Settings](#) on page 110

## Remote Site Data Connection over Leased (WAN) Lines

Enable the following trace option settings:

Tab	Trace Options
<b>WAN</b>	WAN Tx, WAN Rx and Events.
<b>PPP</b>	LCP Tx, LCP Rx, Security Tx, Security Rx, IPCP Tx, IPCP Rx, IP Tx and IP Rx.
<b>System</b>	Error, Print and Resource Status Prints.

- If the line is connected via the WAN port on the system's control unit, **System Monitor** should be configured to monitor the IP address of the system.
- If the line is connected via a WAN port on a WAN3 module, **System Monitor** should be configured to monitor the IP address of the WAN3 unit.

If the leased line problem is to a specific destination, then **System Monitor** can record information pertinent to that connection only. By entering the appropriate service name in the **PPP** trace option settings **Interface Name** field. A blank entry means all the data connections (Services) are monitored.

Check for any PAP/CHAP password failure. This indicates that the `Service` configuration is not correct.

Note that the WAN Tx and WAN Rx information is in raw hex format only. An in-depth knowledge of the IP Packet make-up is required to manually decode these messages which is not done automatically.

### Related links

[Example Monitor Settings](#) on page 110

## Frame Relay Links

Enable the following trace option settings:

Tab	Trace Options
<b>Frame Relay</b>	Events, Tx Data, Tx Data Decode, Rx Data, Rx Data Decode, Tx Data and Mgmt Events (if Management enabled on link)

Please note that the following Point-to-Point Protocol (PPP) options may also be required if using PPP over Frame Relay as the connection method:

Tab	Trace Options
<b>PPP</b>	LCP Tx, LCP Rx, Security Tx, Security Rx, IPCP Tx, IPCP Rx, IP Tx and IP Rx

### Related links

[Example Monitor Settings](#) on page 110

## Problems Involving Non-IP Phones

Enable the following trace option settings:

Tab	Trace Options
Call	Line Send, Line Receive, Extension Send, Extension Receive, Extension RxP, Extension TxP, Short Code Msgs, Call Delta, Targetting and Call Logging.

The **Call** tab provides details on Call Setup, Call Proceeding, Alerting, Call Connected, and Call Disconnected is provided. A step by step trace of the process that the call has gone through and all information relating directly to the setup of the call is displayed in the **Call** tab.

### Related links

[Example Monitor Settings](#) on page 110

## Problems Involving IP Phones

Enable the following trace option settings:

Tab	Trace Options
H.323	H.323, H.323 Send, H.323 Receive, H.323 Fast Start, H.245 Send, H.245 Receive, RAS Send, RAS Receive and View Whole Packet.

The **H.323** tab provides details on Call Setup, Call Proceeding, Alerting, Call Connected, and Call Disconnected is provided. A step by step trace of the process that the call has gone through and all information relating directly to the setup of the call is displayed in the **H.323** tab.

### Related links

[Example Monitor Settings](#) on page 110

## Locating a Specific PC Making Calls to the Internet

Enable the following trace option settings:

Tab	Trace Options
ISDN	Layer3 Tx and Layer3 Rx.
Interface	Interface Queue
Call	Line Send, Line Receive, Targeting and Call Logging
System	Error, Print and Resource Status Prints.

If Network address translation (NAT) is not being used on the connection this produces:

```
Interface Queue: v=UKIP WAN 1 1
IP Dst=194.217.94.100 Src=212.46.130.32 len=48 id=043e ttl=127 off=4000 pcol=6 sum=017c
TCP Dst=80 (0050) Src=4105 (1009) Seq=338648156 Ack=0 Code=02 (SYN )
```

```
Off=112 Window=8192 Sum=6aae Urg=0
0000 02 04 05 b4 01 01 04 02
```

- The source (Src) of this packet is 212.46.130.32.
- The destination (IP Dst) is 194.217.94.100,
- The protocol is TCP (pcol is 6)
- The destination socket is 80 (80 is World Wide Web HTTP is, a PC is trying to access a web page)
- The source socket is 4105 (unassigned means it is free to be used by any program)
- The packet is a TCP SYN.

You need to locate the PC with address 212.46.130.32. To locate, type the IP Dst in the address bar of the web browser and it takes the specific page.

If NAT is being used, you can trace by observing in System Monitor traces, example:

```
PRN: ~NATranslator d40190dc 00000000
PRN: ~UDPNATSession in=c0a84d01 out=d40190dc rem=d401809c in_port=0035 out_port=1000
rem_port=0035
PRN: ~TCPNATSession in=c0a84d02 out=d40190dc rem=c2ed6d49 in_port=0423 out_port=1005
rem_port=0050
```

The Interface Queue trace is preceded by the following System Monitor output :

```
PRN: TCPNATSession in=c0a84d02 out=d40190dc rem=c2ed6d49 in_port=0423 out_port=1005
rem_port=0050
```

Where:

<b>in</b>	Is the IP address (in hex format) of the device on the LAN that is initiating the request.
<b>out</b>	Is the IP address of the PBX (i.e. the local IP address of the link) as allocated by the ISP/Remote Routing device.
<b>rem</b>	Is the requested destination IP address.
<b>in_port</b>	Is the port (socket) number used by the initiating device on the LAN
<b>out_port</b>	Is the outgoing port we use on the link (due to the NAT)
<b>rem_port</b>	Is the requested destination port (socket) number.

### Related links

[Example Monitor Settings](#) on page 110

---

## Firewall Not Working Correctly

Enable the following trace option settings:

Tab	Trace Options
<b>Interface</b>	Interface Queue, Firewall Fail In and Firewall Fail Out.
<b>System</b>	Error, Print and Resource Status Prints.

When monitoring starts, if you do not see any specified failing in the trace, then enable the following additional settings:

Tab	Trace Options
<b>Interface</b>	Interface Queue, Firewall Fail In and Firewall Fail Out.
<b>System</b>	Error, Print and Resource Status Prints.

This traces all the packets that are allowed in and out of the Private Branch Exchange (PBX) via the firewall.

 **Note:**

Use the **Interface Name** field available in the **Interface** trace option setting menu to enter the name of a particular service that you want to monitor.

**Related links**

[Example Monitor Settings](#) on page 110

## Calls Answered/Generated by IP Office Applications

Enable the following trace option settings:

Tab	Trace Options
<b>Call</b>	Line Send, Line Receive, Extension Send, Extension Receive, Extension TxP, Extension RxP, Short Code Msgs, Call Delta, Targetting and Call Logging.
<b>System</b>	Error, Print and Resource Status Prints.

**Related links**

[Example Monitor Settings](#) on page 110

## Message Waiting Indication

To determine if Voicemail Pro is transmitting message waiting indication Message Waiting Indication (MWI) information.

Enable the following trace option settings:

Tab	Table
<b>Call</b>	Extension Send, MonIVR and Targetting
<b>System</b>	Print

Whenever voicemail is accessed for a mailbox (message leaving or retrieval) voicemail sends a voicemail status update for that mailbox to the PBX. This is traced out within **System Monitor** with the **MonIVR** option and is an IVR Event type message.



The following is a trace example received with leaving a message to mailbox 206:

- **IVR Events** indicate the number of new, read, saved messages. If the new message count is zero then the PBX should extinguish the message waiting light, otherwise the message waiting light should be activated.

When the MWL indication is sent to the phone, the CMExtnTx event should indicate the transmission of the message **CMVoiceMailStatus** with the number of new messages being in the display field (may also be in the calling party field). The **UUI** field may also contain the information format (length of UUI, number of messages, unread messages, extension state).

```
7201633mS CMExtnTx: v=203, p1=1
CMVoiceMailStatus
Line: type=DigitalExtn 3 Call: lid=0 id=-1 in=0
Calling[00000001] Type=Default (100)
UUI type=Local [...] [0x03 0x01 0x01 0x00 ]
Display [Extn203 Msgs=1]
Timed: 06/05/05 12:26
7201634mS IVR Event: Voicemail message update for [Extn203]:- New=1,Read=1,Saved=0
```

### Related links

[Example Monitor Settings](#) on page 110

---

## Speech Calls Dropping

### ISDN or QSIG line

Enable the following trace option settings:

Tab	Trace Options
<b>ISDN</b>	Layer 1, Layer 3, Layer 1 Send, Layer 1 Receive, Layer 3 Send and Layer 3 Receive
<b>Call</b>	Line Send, Line Receive, Extension Send, Extension Receive, Extension RxP, Extension TxP, Short Code Msgs, Call Delta, Targeting and Call Logging
<b>System</b>	Error, Print and Resource Status Prints

### Analogue Line

Enable the following trace option settings:

Tab	Trace Options
<b>ATM</b>	Channel, I-O and CM Line
<b>Call</b>	Line Send, Line Receive, Extension Send, Extension Receive, Extension RxP, Extension TxP, Short Code Msgs, Call Delta, Targeting and Call Logging
<b>System</b>	Error, Print and Resource Status Prints

### VoIP Line

Enable the following System Monitor settings:

Tab	Trace options
<b>ISDN</b> <sup>[1]</sup>	Layer 3 Send <sup>[1]</sup> and Layer 3 Receive.
<b>ATM</b> <sup>[2]</sup>	Channel <sup>[2]</sup> , I-O2 and CM Line.
<b>T1</b> <sup>[3]</sup>	Line, Channel, Dialler, DSP and CAS.
<b>H.323</b>	H.323, H.323 Send, H.323 Receive, H.323 Fast Start <sup>[4]</sup> , H.245 Send, H.245 Receive and View Whole Packet.
<b>Call</b>	Line Send, Line Receive, Extension Send, Extension Receive, Extension RxP, Extension TxP, Short Code Msgs, Call Delta, Targeting and Call Logging.
<b>System</b>	Error, Print and Resource Status Prints

**\* Note:**

1. If VoIP call traverses a T1 ISDN, E1 ISDN, BRI ISDN or QSig line to get to its final destination.
2. If VoIP call traverses out over an Analogue Line to get to its final destination.
3. If VoIP call traverses out over a Channelized T1 Line to get to its final destination.
4. If in use by VPN Line or VoIP Extension.

**Channelized T1 Line**

Enable the following System Monitor settings:

Tab	Trace Options
<b>T1</b>	Line, Channel, Dialler, DSP and CAS.
<b>Call</b>	Line Send, Line Receive, Extension Send, Extension Receive, Extension RxP, Extension TxP, Short Code Msgs, Call Delta, Targeting and Call Logging.
<b>System</b>	Error, Print and Resource Status Prints

**Related links**

[Example Monitor Settings](#) on page 110

# Chapter 11: IP Office Ports

Full details of the range of ports used by different releases of IP Office and IP Office applications are found in the Port Matrix documents at [https://ipofficekb.avaya.com/businesspartner/ipoffice/mergedProjects/general/port\\_matrix/index.htm](https://ipofficekb.avaya.com/businesspartner/ipoffice/mergedProjects/general/port_matrix/index.htm).

## Related links

[Ports](#) on page 123

[Protocols](#) on page 125

[IP Office System Ports](#) on page 125

[Voicemail Pro Ports](#) on page 133

[one-X Portal Server and Client Ports](#) on page 135

[Media Manager Ports](#) on page 137

[Customer Operations Manager \(COM\)](#) on page 138

[Port Changes Between Releases](#) on page 138

---

## Ports

The port being used by a data packet is displayed as `src=` followed by a port number.

For the following ports, SysMonitor also adds the protocol name taken from <http://www.iana.org/assignments/port-numbers>. For example `src=23` is displayed as `src=23 (Telnet)`.

Number	Protocol
20	File Transfer [Default Data]
21	File Transfer [Control]
23	Telnet
25	Simple Mail Transfer
37	Time
43	Who Is
53	Domain Name Server
67	Bootstrap Protocol Server
68	Bootstrap Protocol Client
69	Trivial File Transfer

*Table continues...*

Number	Protocol
70	Gopher
79	Finger
80	World Wide Web-HTTP
115	Simple File Transfer Protocol
123	Network Time Protocol
137	NETBIOS Name Service
138	NETBIOS Datagram Service
139	NETBIOS Session Service
156	SQL Service
161	SNMP
162	SNMPTRAP
179	Border Gateway Protocol
1719	H.323Ras
1720	H.323/H.245
1764	NA Monitor
1765	NA BLF/TAPI
1766	NA PCPartner
1755	NA Who-Is response
3851	NA Voicemail
3852	NA Network DTE
3867	NA SoloMail
50791	IPO Voicemail
50792	IPO Network DTE
50793	IPO Solo Voicemail
50794	IPO Monitor
50795	IPO Voice Networking
50796	IPO PCPartner
50797	IPO TAPI
50798	IPO Who-Is response
50799	IPO BLF
50800	IPO License Dongle
54050	BT Fusion

**Related links**

[IP Office Ports](#) on page 123

## Protocols

The protocol being used by a data packet is shown as `pcol=` followed by a protocol number.

For the following common protocols, SysMonitor also adds the protocol name taken from <http://www.iana.org/assignments/protocol-numbers>. For example `pcol=1` is displayed as `pcol=1 (ICMP)`.

Number	Protocol	Monitor shows
1	Internet Control Message	ICMP
2	Internet Group Management	IGMP
6	Transmission Control	TCP
8	Exterior Gateway Protocol	EGP
9	Interior Gateway Protocol	IGP
17	User Datagram	UDP
41	Ipv6	IPV6
46	Reservation Protocol	PRSVIP
47	General Routing Encapsulation	GRE
58	ICMP for IPv6	IPV6-ICMP
111	IPX in IP	IPX-In-IP
115	Layer Two Tunneling Protocol	L2TP
121	Simple Message Protocol	SMP

### Related links

[IP Office Ports](#) on page 123

## IP Office System Ports

The tables lists the ports required for IP Office services and applications such as IP Office Manager, System Status Application, SysMonitor.

**Table 2: Ingress**

Port (Range)	Protocol	Switchable	External Device	Description
		<ul style="list-style-type: none"> <li>• Default</li> </ul>		<ul style="list-style-type: none"> <li>• Authenticated</li> </ul>
22	TCP/SSH	<ul style="list-style-type: none"> <li>No</li> <li>• Open</li> </ul>	Admin terminal or SAL Gateway	<ul style="list-style-type: none"> <li>Remote maintenance connection</li> <li>• Username + password</li> </ul>

*Table continues...*

Port (Range)	Protocol	Switchable • Default	External Device	Description • Authenticated
52	DNS	No • Open	DNS Client	IP Office acts as a DNS relay • None
67	UDP/DHCP	Yes • Open	DHCP clients such as IP Phones	IP Office DHCP service • None
67	UDP/BOOTP	Yes • Open	Manager	Manager BOOTP server for IP address and firmware for IP Office • None
69	UDP/TFTP	No • Open	Legacy Manager, Upgrade Wizard.	IP Office status, program data, UDP Whois. The information that is obtained can be controlled with security settings • Obfuscated password
80* (1-100)	TCP/HTTP	Yes • Open	File transfer Manager and phones, Web client, DECT R4 Provisioning, SoftConsole, WebSocket SCN, Voicemail Pro.	General purpose HTTP file and WebSocket server. Phone backup/restore and firmware download. • Some URIs RFC2617 Authenticated
123	NTP	No • Open	DECT R4, IP Office	NTP (RFC4330) Service - SNTP subset • None
161* (161, 1024-65535)	UDP/SNMP	Yes • Open	SNMP Agent	Read-only access to MIB entries • Community string
411	TCP/HTTPS	Yes • Open	H.232 phone	Phone settings files • None

*Table continues...*

Port (Range)	Protocol	Switchable • Default	External Device	Description • Authenticated
443* (1-65535)	TCP/HTTPS	Yes • Open	Manager and phones, Web client, DECT R4 Provisioning, SoftConsole, WebSocket SCN, Voicemail Pro. SIP, H.323 phones	General purpose HTTPS file and WebSocket server. Secure phone backup/restore • Shared secret (Softphone) X.509 certificate (IP Office)
520	UDP/RIP	Yes • Open	Router	Exchange routing information with adjacent IP routers or receive information • None
1300	TLS/H.323 signaling	Yes • Closed	H.323 Phone	Secure H.323 signaling from IP phones • None
1701	UDP/L2TP	Yes • Closed	Remote Network devices	From layer 2 tunnels to remote network devices • CHAP
1718	UDP/H.323 discovery	Yes • Filtered	H.323 phone	H.323 service to IP Phones • Shared secret (password) HMAC-SHA1-96
1719	UDP/H.323 status	Yes • Filtered	H.323 phone	H.323 service to IP Phones • Shared secret (password) HMAC-SHA1-96
1720	TCP/H.323 signaling	Yes • Filtered	H.323 phone	H.323 service to IP Phones • Shared secret (password) HMAC-SHA1-96
4097	TCP	No • Filtered	N/A	Debug (disabled) • None
5056* (1024- 64510)	UDP+TCP/SIP	Yes • Closed	SIP endpoint, SIP trunk, SIP Proxy	SIP extensions. • MD5 CHAP
5060* (1024-64510)	TCP+UDP/SIP	Yes • Closed	SIP endpoint, SIP trunk, SIP Proxy	SIP extensions • MD5 CHAP
5061* (1024-64510)	TLS/SIP	Yes • Closed	SIP endpoint, SIP trunk, SIP Proxy	SIP extensions • MD5 CHAP

*Table continues...*

Port (Range)	Protocol	Switchable • Default	External Device	Description • Authenticated
5443	TCP/HTTPS	Yes • Open	Backup/ Restore client, UC client upgrade.	Secure server for solution backup/restore. Secure URI for VM listen for UC client. Upgrade for Hosted Deployment. Applies only to IP Office Linux and Application Server • None
5480	TCP/HTTPS	Yes • Open	Web interface for Virtual Appliance Management Infrastructure (VAMI)	Virtual Linux-based IP Office servers. No firewall configuration needed • Authenticated
5488	TCP	Yes • Open	CIM client for VAMI	Linux-based IP Office servers. No firewall configuration needed. • Authenticated
5489	Yes • Closed	Yes • Open	CIM client for VAMI	Linux-based IP Office servers. No firewall configuration needed. • Authenticated
7070	TCP/HTTPS	Yes • Open	Web Management client	Linux-based IP Office servers. • Username + password
7071	TCP/HTTPS	Yes • Open	Web Management client	Linux-based IP Office servers. • Username + password
7147	TCP/HTTPS	No • Open	Collaboration Services/SMA	IP Office Application Server. • Internal. Token based authentication.
7444	TCP/HTTPS	No • Open	IP Office User Portal	IP Office Application Server. • Username + password
8000	TCP/HTTP	No • Closed	Web Management client, Upgrade.	Upgrade web service. Log download • Username + password
8411	TCP/HTTP	Yes • Closed	H.323 phone	Phone settings files. Firmware download • None
8443* (1-65535)	TCP/HTTPS	Yes • Closed	Web Management client	- • None
9080	TCP/HTTP	No • Closed	Web Management client	- • Username + password

*Table continues...*



Port (Range)	Protocol	Switchable • Default	External Device	Description • Authenticated
40750-50750	UDP/RTP UDP/RTCP	Yes • N/A	Media end points	IP Office Linux uses the port range 32768-61000 for RTP connections. IP500 V2 default 40750-50750 • None
40750-50750	UDP/SRTP UDP/SRTCP	Yes • N/A	Media end points	IP Office Linux uses the port range 32768-61000 for RTP connections. IP500 V2 default 40750-50750 • None
50780	UDP/ Proprietary	Yes • Open	Dongle application	Not used • None
50792	UDP/ Voicemail	Yes • Open	Voicemail server	Voicemail Pro media • None
50793	TCP/ Proprietary	Yes • Open	Solo Server	TAPI Wave Driver – audio stream interface for TAPI based applications • None
50794	UDP+TCP,Sy sMonitor	Yes • Open	System Monitor, DevLink.	Event, trace and diagnostics outputs • Password
50795	UDP, Voicenet	Yes • Open	SCN Trunks	Small Community Network peer to peer trunk signaling • None
50796	TCP/TLS	Yes • Open	IPOCC/ACCS	CTI link for Contact Center application • Password
50797	TCP/TAPI	Yes • Open	TAPI clients: CPA, PC Dialer, Web Agent	TAPI • None
50801	TCP/ Proprietary	Yes • Open	Voice Conferencing application	- • None
50802	TCP/ Proprietary	Yes • Open	IP Office Manager, Web Management	Whois #2 and Whois #3, TCP discovery • -
50804* (49152-65280)	TCP/ Proprietary	Yes • Open	IP Office Manager	IP Office configuration interface • HMAC SHA-1 challenge sequence

*Table continues...*

Port (Range)	Protocol	Switchable • Default	External Device	Description • Authenticated
50805* (49152-65280)	TCP/TLS	Yes • Open	IP Office Manager	IP Office configuration interface secure (encrypted) • HMAC SHA-1 challenge sequence X.509 Certificate
50808* (49152-65280)	TCP/ Proprietary	Yes • Open	System Status Application	IP Office status information • HMAC SHA-1 challenge sequence
50809* (49152-65280)	TCP/TLS	Yes • Open	System Status Application	IP Office status information secure (encrypted) • HMAC SHA-1 challenge sequence
50812* (49152-65280)	TCP/ Proprietary	Yes • Open	IP Office Manager	IP Office security settings • HMAC SHA-1 challenge sequence
50813* (49152-65280)	TCP/TLS	Yes • Open	IP Office Manager	IP Office security settings secure (encrypted) • HMAC SHA-1 challenge sequence X.509 Certificate
50814* (49152-65280)	TCP/ Proprietary	Yes • Open	one-X server	IP Office CTI control for one-X • HMAC SHA-1 challenge sequence
50823	TCP	No • Closed	N/A	Debug IP Office Linux (disabled) • None
52233	TCP/HTTPS	Yes • Closed	WebLM client	WebLM server for licensing • X.509 certificate
56000-58000	UDP/RTP	No • Open	WebRTC Media gateway	Media endpoints • None

**Egress**

Port (Range)	Protocol	Switchable • Default	External Device	Description • Authenticated
25	TCP/SMTP	Yes • N/A	SMTP email server	Email transmission from IP Office (TLS enforced) • None
37	UDP/TIME	Yes • N/A	Manager and VMPPro	TIME (RFC868) Service • None

*Table continues...*

Port (Range)	Protocol	Switchable • Default	External Device	Description • Authenticated
53	UDP/DNS	Yes • N/A	DNS server	Name Service • None
68	UDP/DHCP	Yes • N/A	DHCP server	IP Office obtaining DHCP address from a server • None
68	UDP/BOOTP	Yes • N/A	Manager	IP Office obtaining IP address and firmware • None
69	UDP/TFTP	Yes • N/A	Manager	IP Office obtaining firmware on behalf of phones • None
123	UDP/NTP	Yes • N/A	NTP server	NTP (RFC 4330) Service - SNTP • None
162*	UDP/SNMP	Yes • N/A	SNMP Receiver	Trap generation from IP Office • Community string
389	TCP/LDAP	Yes • N/A	LDAP service	Import of directory information from LDAP database • Kerberos 4 or simple password
443	TCP/HTTPS	Yes • N/A	SCEP server	SCEP to System Manager • Password
443	HTTPS	Yes • -	Google Cloud Storage	Subscription system backup, restore, and upgrade.
500	UDP/IKE	Yes • N/A	Remote device	Form IPsec association with remote security devices • Shared secret MD5 or SHA
514*	UDP+TCP/Syslog	Yes • N/A	Syslog server	- • None
520	-	Yes • Open	Router	Exchange routing information with adjacent IP routers or receive information • None
3478*	UDP	Yes • N/A	STUN Server	- • None
5060	UDP+TCP/SIP	Yes • N/A	c	- • MD5 CHAP

*Table continues...*

Port (Range)	Protocol	Switchable • Default	External Device	Description • Authenticated
5061	TLS/SIP	Yes • N/A	SIP trunk	- • MD5 CHAP
5443	TCP/HTTPS	Yes • N/A	HTTPS server	Solution backup/restore using HTTPS • Username + password
6514	TLS/Syslog	Yes • N/A	Syslog server	- • None
10162	UDP/SNMP	Yes • N/A	SNMP trap	SNMP trap to System Manager • None
40750-50750*	UDP/RTP-RTCP UDP/SRTPSRTCP	Yes • N/A	Media end points	IP Office Linux uses the port range of 32768-61000 for RTP connections with the media server. IP500 V2 default 46750-50750 • None
50791	UDP/Voicemail	Yes • N/A	Voicemail server	Voicemail Pro signaling/media • None
50795	UDP/Voicenet	Yes • N/A	SCN trunks	SCN peer to peer trunk signalling Legacy trunks only, WebSocket SCN uses 80/443 • None
50815	TCP/TLS	No • Open	one-X Portal	IP Office CTI control for one-X Portal • HMAC SHA-1 challenge sequence
52233	TCP/HTTPS	Yes • N/A	WebLM server	Used for WebLM licensing • X.509 certificate

### Intra-Device

Port (Range)	Protocol	Switchable • Default	External Device	Description • Authenticated
4096	TCP	Yes • Open	IP Office SNMP Agent	- • Internal.
4444	TCP/JMX	Yes • Open	WebRTC signaling gateway	Management port used by WebRTC signal gateway to communicate with media gateway • Internal.
4445	TCP/JMX	Yes • Open		Messaging port used by WebRTC signal gateway to communicate with media gateway • Internal.

*Table continues...*

Port (Range)	Protocol	Switchable • Default	External Device	Description • Authenticated
5005*	TCP	Yes • Open	RTCP monitoring	- • Internal.
5555	TCP	Yes • Open	WebRTC signaling gateway	Messaging port used by WebRTC signal gateway to communicate with media gateway • Internal.
5556	TCP/JMX	Yes • Open		Messaging port used by WebRTC signal gateway to communicate with media gateway • Internal.
6006	TCP	Yes • Open	QoS	- • Internal.
17777	TCP	Yes • Open	IP Office and Jade	Communication between IP Office and JADE • Internal.
42004*	TCP/SIP	Yes • Open	WebRTC signaling gateway	SIP client connections from IP Office • Internal.
42008*	TCP/SIP	Yes • Open		SIP trunk connections from IP Office • Internal.

\* Configurable.

#### Related links

[IP Office Ports](#) on page 123

---

## Voicemail Pro Ports

### Ingress

Port (Range)	Protocol	Switchable • Default	Default State	External Device	Description • Authenticated
25	TCP/ SMTP/TLS	Yes	Open	SMTP	Voicemail Pro client for SMTP operations - TLS enforced. • None
37	UDP/TIME	Yes	Open	IP Office	TIME (RFC868) Service for IP Office • None

*Table continues...*

Port (Range)	Protocol	Switchable • Default	Default State	External Device	Description • Authenticated
143	TCP/IMAP4	Yes	Open	IMAP4 client	Access to voicemails using IMAP4 over non-secure connection • None
993	IMAP4 – SSL	Yes	Open	IMAP4 client – SSL	Access to voicemails using IMAP4 over SSL connection • None
5443	TCP/HTTPS	No	Open	UC client, one-X Portal server	Secured share access to Voicemail Pro media files with one-X Portal server and UC clients. • None
50791	UDP/TCP/Voicemail	Yes	Open	Voicemail Pro client	Communication with IP Office and one-X Portal • None

### Egress

Port (Range)	Protocol	Switchable • Default	External Device	Description • Authenticated
22	TCP/FTP	Yes • N/A	Media Manager Backup file server	FTP or SFTP • None
25	TCP/SMTP/TLS	Yes • N/A	SMTP	Voicemail email integration - TLS enforced • None
443	TCP/HTTPS	Yes • N/A	Exchange server	Web service API client for Exchange integration • None
50792	UDP/Voicemail	Yes • N/A	IP Office	Voicemail Pro media • None
50792	SSL/Voicemail	Yes • N/A	Exchange MAPI proxy	Exchange MAPI proxy connector • None
50793	SSL/Voicemail	Yes • N/A	Exchange MAPI proxy	Exchange MAPI proxy connector • None
50802	TCP/Proprietary	No • N/A	IP Office	Whois • None

**Intra-Device**

Port (Range)	Protocol	Switchable • Default	External Device	Description • Authenticated
25	TCP/ SMTP/TLS	Yes • Open	SMTP	Messaging and configuration updates between Voicemail Pro servers - TLS enforced • None

**Related links**

[IP Office Ports](#) on page 123

**one-X Portal Server and Client Ports****Ingress**

Port (Range)	Protocol	Switchable • Default	External Device	Description • Authenticated
4560	TCP/Log4j	No • Open	Log4j appender	- • -
5222	TCP/XMPP	Yes • Open	XMPP client	Instant message clients • Username + password
5269	TCP/XMPP	Yes • Open	XMPP federation	Instant message federation • Username + password
7171	TCP/BOSH	Yes • Open	OpenFire for BOSH	- • Username + password
7443	TCP/BOSH	Yes • Filtered	OpenFire for BOSH	- • Username + password
8005	TCP/Tomcat shutdown	No • Closed	Tomcat shutdown listener	- • -
8080	TCP/HTTP	Yes • Open	Web Client	one-X Portal • Username + password
8666	TCP/JMX	Yes • Open	Java extension	- • Username + password
9092	TCP/JDBC	No • Open	Database client listener	- • Username + password

*Table continues...*

Port (Range)	Protocol	Switchable • Default	External Device	Description • Authenticated
9443	TCP/HTTPS	Yes • Open	Web Client, Media Manager client, WebRTC client	one-X Portal secure/ Media Manager/ WebRTC Gateway • Username + password X.509 Certificate
5433	TCP/JDBC	No • Open	one-X Portal	Geo-redundant one-X Portal server database sync. • Username + password
61615	TCP/Proprietary	No • Open	one-X Portal	Geo-redundant one-X Portal server database sync. • Username + password

### Egress

Port (Range)	Protocol	Switchable • Default	External Device	Description • Authenticated
80/8000	TCP/HTTP	Yes • N/A	Voicemail Pro	Voicemail Pro communication with one-X Portal • None
50791	TCP/Voicemail	yes • N/A	Voicemail Pro	Voicemail Pro communication with one-X Portal • None
50814 (49152-65280)	TCP/Proprietary	Yes • N/A	IP Office	IP Office CTI control for one-X Portal • HMAC SHA-1 challenge sequence
50815	TCP/TLS	No • Open	IP Office	
5433	TCP/JDBC	No • Open	one-X Portal	Geo-redundant one-X Portal server database sync. • Username + password
61615	TCP/Proprietary	No • Open	one-X Portal	Geo-redundant portal server status sync. • Username + password



**Intra-Device**

Port (Range)	Protocol	Switchable • Default	External Device	Description • Authenticated
8086	TCP/HTTP	No • Open	XMPP	Internal REST interface • Internal, no firewall configuration required.
8667	TCP	Yes • Open	one-X Portal (Openfire)	Used by XMPP service for JMX connection. • Accessed by manual script from same host to take Openfire heap and thread.

**Related links**

[IP Office Ports](#) on page 123

**Media Manager Ports****Ingress**

Port (Range)	Protocol	Switchable • Default	External Device	Description • Authenticated
49001	TCP/HTTP	Yes • Closed	Web client	HTTP Listener port. Used only during the one time Google authorization process. • None

**Egress**

Port (Range)	Protocol	Switchable • Default	External Device	Description • Authenticated
49001	TCP/HTTP	Yes • Closed	Web client	HTTP Listener port. Used only during the one time Google authorization process. • None

**Related links**

[IP Office Ports](#) on page 123

---

## Customer Operations Manager (COM)

### Ingress

Port (Range)	Protocol	Switchable • Default	External Device	Description • Authenticated
7080	HTTPS	No • Open	Web client	HTTP Listener port for COM admin client • Service User

### Egress

Port (Range)	Protocol	Switchable • Default	External Device	Description • Authenticated
7070	HTTPS	No • Open	IP Office Primary, IP Office Secondary	Status and management traffic between COM and IP Office Server Edition. • None

### Related links

[IP Office Ports](#) on page 123

---

## Port Changes Between Releases

The following sections summarize the port changes that have occurred between different releases.

### Related links

[IP Office Ports](#) on page 123

[Port Changes from 8.1 FP1 to 9.0](#) on page 139

[Port Changes from 9.0 to 9.0.3](#) on page 140

[Port Changes from 9.0.3 to 9.1](#) on page 140

[Port Changes from 9.1 to 10.0](#) on page 141

[Port Changes from 10.0 to 10.1](#) on page 142

[Port Changes from 10.1 to 11.0](#) on page 143

[Port Changes from 11.0.0 to 11.1.0](#) on page 144

[Port Changes from 11.1.0 to 11.1.1](#) on page 144

[Port Changes from 11.1.1 to 11.1.2](#) on page 144

## Port Changes from 8.1 FP1 to 9.0

Port: Default (Range)	Protocol	Switch On/Off	Default State	External Device	Description
21	TCP	Yes	Open	FTP	This port is used by FTP server for transferring VMPro recordings to Contact Store/ Contact Recorder.
22	TCP	Yes	Open	SFTP	This port is used by SFTP server for transferring VMPro recordings to Contact Store/ Contact Recorder.
7071	TCP/HTTPS	No	Open	Web Management client	Web control access IP Office Linux
8805	TCP/Tomcat shutdown	No	Open	Tomcat shutdown listener	This port is used by Contact Store/ Contact Recorder for internal activities.
9444	TCP/HTTPS	No	Open	Web client	This is the HTTP listener port.
9888	TCP/HTTP	No	Open	Web client	This is the HTTP listener port.
52233	TCP/HTTPS	Yes	N/A	Web LM server	WebLM licensing IP Office

### Related links

[Port Changes Between Releases](#) on page 138

## Port Changes from 9.0 to 9.0.3

Port: Default (Range)	Protocol	Switch On/Off	Default State	External Device	Description
<b>Changed</b>					
47000-54000 (Min start 1024, min end 2048)	UDP/RTP-RTCP	Yes	N/A	Media end points	IP Office Linux uses the port range 32768-61000 for RTP connections with the media server. Default range updated.

### Related links

[Port Changes Between Releases](#) on page 138

## Port Changes from 9.0.3 to 9.1

Port: Default (Range)	Protocol	Switch On/Off	Default State	External Device	Description
<b>Added</b>					
441	TCP/HTTPS	Yes	Open	H.323 phone	Phone settings, backup/restore
4443	TCP/JMX	yes	Open	WebRTC signaling gateway	Management port user by WebRTC signaling gateway to communicate with Media gateway
4444	TCP/JMX	Yes	Open	WebRTC signaling gateway	Messaging port user by WebRTC signaling gateway to communicate with Media gateway
7171	TCP/BOSH	Yes	Open	OpenFire for BOSH	-
8086	TCP/HTTP	No	Open	XMPP	Internal REST interface
52233	TCP/HTTPS	Yes	Closed	WebLM client	WebLM server for licensing
56000-58000 (Configurable)	UDP/SRTP	No	Open	WebRTC media gateway	Media endpoints
<b>Changed</b>					

*Table continues...*

Port: Default (Range)	Protocol	Switch On/Off	Default State	External Device	Description
<b>Added</b>					
40750-50750 (Min start 1024, min end 2048)	UDP/RTP-RTCP	Yes	N/A	Media end points	IP Office Linux uses the port range 32768-61000 for RTP connections with the media server. Default range updated.
Removed					
CCR Ingress					
80	TCP/HTTP	No	Open	Web client	
443	TCP/HTTPS	No	Open	Web client	
1433	TCP/MSSQL	No	Open	MSSQL	MSSQL server
1434	TCP/MSSQL	No	Open	MSSQL	MSSQL monitor
8135	TCP/Proprietary	No	Open	Wallboard	
8080	TCP/SOAP	No	Open	one-X Portal server	Communication with portal server
Removed					
CCR Egress					
25	TCP/SMTP	Yes	N/A	SMTP email server	Email transmission
50804	TCP/Proprietary	No	N/A	IP Office	SSI client (system status information)

**Related links**

[Port Changes Between Releases](#) on page 138

**Port Changes from 9.1 to 10.0**

Port: Default (Range)	Protocol	Switch On/Off	Default State	External Device	Description
<b>Added</b>					
<b>IP Office Ingress</b>					
1300	TCP/TLS	Yes	Closed	H.323 phone	Secure H.323 signalling to IP phones.
3478	UDP	Yes	N/A	STUN Server	Stun client in previous IP Office releases.

*Table continues...*

Port: Default (Range)	Protocol	Switch On/Off	Default State	External Device	Description
<b>Added</b>					
<b>IP Office Ingress</b>					
Portal Ingress					
9843	TCP/TLS	No	Open	Web Collaboration	Policy file check
Portal Intra					
5433	TCP/JDBC	No	Open	one-X Portal	Geo-redundant portal database sync.
61615	TCP/Proprietary	No	Open	one-X Portal	Geo-redundant portal status sync.
<b>Removed</b>					
8063	TCP/HTTPS	No	Open	Communication and portal plug-ins access to one-X Portal	-
8069	TCP/HTTP	No	Open	Communication and portal plug-ins access to one-X Portal	-
8444	TCP/Proprietary	Yes	Open	Mobility client	Mobility client authentication
9094	TCP/XMP RPC	No	Open	-	OpenFire XML Remote Procedure Call and Admin console
9095	TCP/HTTPS	No	Open	Administration console	OpenFire Admin Console

**Related links**

[Port Changes Between Releases](#) on page 138

**Port Changes from 10.0 to 10.1**

None

**Related links**

[Port Changes Between Releases](#) on page 138

## Port Changes from 10.1 to 11.0

Port: Default (Range)	Protocol	Switch On/Off	Default State	External Device	Description
<b>Added</b>					
<b>COM Ingress</b>					
7080	HTTPS	No	Open	Web client	HTTP Listener for COM admin client browser.
<b>COM Egress</b>					
7070	HTTPS	No	Open	IP Office Primary, IP Office Secondary	Status and management traffic between COM and IP Office Server Edition.
<b>Removed</b>					
<b>IP Office Ingress</b>					
5807 (5800-5899)	TCP	Yes	Open	VNC Server	Used for VNC viewer
<b>Contact Recorder Ingress</b>					
8805	TCP/Tomcat shutdown	No	Open	Tomcat shutdown listener	
9444	TCP/HTTPS	No	Open	Web client	HTTP Listener port
98888	TCP/HTTP	No	Open	Web client	HTTP Listener port
<b>Contact Recorder Egress</b>					
21	TCP	Yes	Open	FTP	FTP server for transferring Voicemail Pro recordings to Contact Recorder.

### Related links

[Port Changes Between Releases](#) on page 138

## Port Changes from 11.0.0 to 11.1.0

Port: Default (Range)	Protocol	Switch On/Off	Default State	External Device	Description
<b>Added</b>					
8667	TCP	Enabled	Open	one-X Portal	Used for XMPP server for JMX connection.
<b>Changed</b>					
443	TCP/HTTPS	Yes	N/A	Avaya Space	OAuth 2.0
443	TCP/HTTPS	Yes	N/A	Subscription license server WebSocket	Authenticated username/ password + SHA256 CHAP
8443	TCP/HTTPS	Yes	N/A		

### Related links

[Port Changes Between Releases](#) on page 138

## Port Changes from 11.1.0 to 11.1.1

Port: Default (Range)	Protocol	Switch On/Off	Default State	External Device	Description
<b>Added</b>					
50815	TCP/TLS	No	Open	one-X Portal	IP Office CTI control for one-X Portal.
443	HTTPS	Yes	-	Google Cloud Storage	Subscription system backup, restore, upgrade, etc.
50815	TCP/TLS	No	Open	IP Office	IP Office CTI control for one-X Portal.

### Related links

[Port Changes Between Releases](#) on page 138

## Port Changes from 11.1.1 to 11.1.2

Port: Default (Range)	Protocol	Switch On/Off	Default State	External Device	Description
<b>Ports Added</b>					

*Table continues...*



Port: Default (Range)	Protocol	Switch On/Off	Default State	External Device	Description
7444	TCP/HTTPS	No	Open	User Portal	IP Office Application Server
7147	TCP/HTTPS	No	Open	Collaboration Services/SMA	
<b>Ports Changed</b>					
8000	TCP/HTTP	Yes	Now Closed by default.	Web Management client upgrade	Upgrade web service. Log download.
8411	TCP/HTTP	Yes		SIP/H323 Phone	Phone settings files, firmware download, backup/restore.
9080	TCP/HTTP	Yes		Web Management client	

**Related links**

[Port Changes Between Releases](#) on page 138

# Chapter 12: Addendum

This section covers additional information.

## Related links

[Decoding FEC Errors](#) on page 149

[Miscellaneous](#) on page 151

---

## Cause Codes (ISDN)

When a call is ended, a cause code may be shown in the system monitor trace. The cause code is not an error as cause codes are shown at the end of normal calls.

- Cause codes 0 to 102 are standard Integrated Services Digital Network (ISDN) cause codes. Causes codes 103 upwards are system specific codes.

To display cause codes, ensure that the **System Monitor > Call > Extension > Send** option is enabled. The cause code is displayed as part of `CMExtnTx:` events within the monitor trace. For example:

```
10185mS CMExtnTx: v=100, p1=1
CMReleaseComp
Line: type=DigitalExtn 3 Call: lid=0 id=-1 in=0
UUI type=Local [....] [0x03 0x00 0x00 0x00 ]
Cause=16, Normal call clearing
Timed: 12/07/05 11:00
```

## Cause codes and definition

Cause Code	Definition
0	Unknown.
1	Unallocated (unassigned) number.
2	No route to specific transit network/(5ESS)Calling party off hold.
3	No route to destination / (5ESS) Calling party dropped while on hold.
4	Send special information tone / (NI-2) Vacant Code..
5	Misdialed trunk prefix.
6	Channel unacceptable.

*Table continues...*

Cause Code	Definition
7	Call awarded and being delivered.
8	Preemption/(NI-2)Prefix 0 dialed in error.
9	Preemption, cct reserved / (NI-2) Prefix 1 dialed in error.
10	(NI-2) Prefix 1 not dialed.
11	(NI-2) Excessive digits received call proceeding.
16	Normal call clearing.
17	User busy.
18	No user responding / No response from remote device.
19	No answer from user.
20	Subscriber absent (wireless networks).
21	Call rejected.
22	Number changed.
23	Redirection to new destination.
25	Exchange routing error.
26	Non-selected user clearing.
27	Destination Out Of Order.
28	Invalid number format.
29	Facility rejected.
30	Response to STATUS ENQUIRY.
31	Normal, unspecified.
34	No cct / channel available.
38	Network out of order.
39	Permanent frame mode connection out of service.
40	Permanent frame mode connection is operational.
41	Temporary failure.
42	Switching equipment congestion.
43	Access information discarded
44	Requested cct / channel not available
45	Pre-empted
46	Precedence blocked call
47	Resources unavailable/(5ESS)New destination
49	Quality of service unavailable
50	Requested facility not subscribed
52	Outgoing calls barred.

*Table continues...*

Cause Code	Definition
54	Incoming calls barred
57	Bearer capability not authorised.
58	Bearer capability not presently available.
63	Service or option not available, unspecified.
65	Bearer capability not implemented.
66	Channel type not implemented.
69	Requested facility not implemented.
70	Only restricted digital bearer capability is available.
79	Service or option not implemented, unspecified.
81	Invalid call reference.
82	Identified channel does not exist.
83	A suspended call exists, but this id does not.
84	Call id in use.
85	No call suspended.
86	Call having the requested id has been cleared.
87	User not a member of Closed User Group.
88	Incompatible destination.
90	Non-existent Closed User Group.
91	Invalid transit network selection.
95	Invalid message, unspecified.
96	Mandatory information element missing.
97	Message type non-existent/not implemented.
98	Message not compatible with call state, non-existent or not implemented.
99	Information element non-existent or not implemented.
100	Invalid information element contents.
101	Message not compatible with call state / (NI-2) Protocol threshold exceeded.
102	Recovery on timer expiry.
IP Office Specific Cause Codes	
103	Parameter not implemented.
110	Message with unrecognised parameter
111	Protocol error, unspecified
117	Parked (Internal system code).
118	UnParked (Internal system code).
119	Pickup (Internal system code).

*Table continues...*

Cause Code	Definition
120	Reminder (Internal system code).
121	Redirect (Internal system code).
122	Call Barred (Internal system code).
123	Forward To Voicemail (Internal system code).
124	Answered By Other (Internal system code).
125	No Account Code (Internal system code).
126	Transfer (Internal system code).
129	Held Call (Internal system code).*
130	Ring Back Check (Internal system code).*
131	Appearance Call Steal (Internal system code).*
132	Appearance Bridge Into (Internal system code).*
133	Bumped Call (Internal system code).*
134	Line Appearance Call (Internal system code).+
135	Unheld Call (Internal system code).+
136	Replace Current Call (Internal system code).+
137	Glare (Internal system code).+
138	R21 Compatible Conf Move (Internal system code).+
139	RingBack Answered (Internal system code).+
140	Transfer Request Failed (Internal system code).+
141	HuntGroup Drop (Internal system code).+

---

## Decoding FEC Errors

This section describes about decoding the Fast Ethernet Controller (FEC) receiver error (PRN) statements that appear in the log. These Fast Ethernet Controller error messages are shown when the **System/Print** option is enabled.

For example: PRN: IP403\_FEC::ReceiverError 844

The message format is: PRN: PLATFORM\_FEC::ReceiverError ABCD

Where:

- PRN: Indicates that message was output as the result of having the **System/Print** option enabled.
- PLATFORM: Indicates the type of system control unit reporting the error. The possible values are IP401NG (Small Office Edition), IP403, IP406, IP406V2 (shows as IP405 in Version 2.1(27)) and IP412.

- ABCD: This is the actual error code. It is a decode of the *Ethernet Receive Buffer Descriptor* packet. Note that if the most significant byte (A) is 0 (zero) it is not printed and the error code is only three characters long (BCD).

FEC: *ReceiverError Codes* are derived from the *Ethernet Receive Buffer Descriptor (RxB D)*. The table shows the bits within the RxB D that are used to generate the error codes. The **N/U** labeled options are not used in the FEC error decoding mechanism although they may be non zero.

Byte	Bit	Value	Option	Description
A	0	8	N/U	May be non-zero but not used for FEC decode.
	1	4	N/U	
	2	2	N/U	
	3	1	N/U	
B	4	8	L	Last in frame. • 0: The buffer is not the last in the frame. • 1: The buffer is the last in the frame.
	5	4	0	Always zero
	6	2	0	Always zero
	7	1	N/U	May be non-zero but not used for FEC decode.
C	8	8	N/U	May be non-zero but not used for FEC decode.
	9	4	N/U	
	10	2	LG	Length Error: Rx frame length violation. The frame length exceeds the value of <code>MAX_FRAME_LENGTH</code> in the bytes. The hardware truncates frames exceeding 2047 bytes so as not to overflow receive buffers This bit is valid only if the <b>L</b> bit is set to <b>1</b> .
	11	1	NO	Non-Octet: A frame that contained a number of bits not divisible by 8 was received and the CRC check that occurred at the preceding byte boundary generated an error. <b>NO</b> is valid only if the <b>L</b> bit is set and <b>CR</b> bit is not set.
D	12	8	SH	Short Frame: A frame length that was less than the minimum defined for this channel was recognized.
	13	4	CR	CRC Error: This frame contains a CRC error and is an integral number of octets in length. This bit is valid only if the <b>L</b> bit is set.
	14	2	OV	Overrun Error: A receive FIFO overrun occurred during frame reception. If <b>OV</b> is set to <b>1</b> , the other status bits, <b>LG</b> , <b>NO</b> , <b>SH</b> , <b>CR</b> , and <b>CL</b> lose their normal meaning and are cleared. This bit is valid only if the <b>L</b> bit is set.
	15	1	TR	Truncate Error: Set if the receive frame is truncated ( $\geq 2$ Kilobytes)

PRN: IP403\_FEC::ReceiverError 844

The error code in the above example is 844. You can decode the message produced using information given in table.

- Byte A is 0 and so was not shown.
- Byte B is 8, which is 1000 in binary, so bit 4 (L) is set.
- Byte C is 4, which is 0100 in binary, so bit 9 (N/U) is set.
- Byte D is 4, which is 0100 in binary, so bit 13 (CR) is set.

#### Related links

[Addendum](#) on page 146

---

## Miscellaneous

- What does the message *PRN: FEC::ReceiverError* mean?

FEC stands for Fast Ethernet Controller (100mb LAN). The **ReceiverError** line is followed by a number that denotes the exact problem.

Basically it is stating that the system received a packet that it considers wrong or corrupt in some way or perhaps there was a collision so it threw it away, the packet would then have been re-sent. This does not normally indicate a problem and is nothing to worry about unless the error's are streaming in the trace. See [Decoding FEC errors](#) on page 149.

- What does the message *PRN: UDP: Sending from indeterminate address to 0a000003 3851* mean?

The port number 3851 at the end indicates that the system is looking for an IP Office Voicemail Server.

If your system is not using voicemail, remove the entry in the **Voicemail IP Address** field, found on the **Voicemail** tab of the **System** form in the system configuration.

#### Related links

[Addendum](#) on page 146

# Chapter 13: Additional Help and Documentation

The following pages provide sources for additional help.

## Related links

[Additional Manuals and User Guides](#) on page 152

[Getting Help](#) on page 152

[Finding an Avaya Business Partner](#) on page 153

[Additional IP Office resources](#) on page 153

[Training](#) on page 154

---

## Additional Manuals and User Guides

The [Avaya Documentation Center](#) website contains user guides and manuals for Avaya products including IP Office.

- For a listing of the current IP Office manuals and user guides, look at the [Avaya IP Office™ Platform Manuals and User Guides](#) document.
- The [Avaya IP Office Knowledgebase](#) and [Avaya Support](#) websites also provide access to the IP Office technical manuals and users guides.
  - Note that where possible these sites redirect users to the version of the document hosted by the [Avaya Documentation Center](#).

For other types of documents and other resources, visit the various Avaya websites (see [Additional IP Office resources](#) on page 153).

## Related links

[Additional Help and Documentation](#) on page 152

---

## Getting Help

Avaya sells IP Office through accredited business partners. Those business partners provide direct support to their customers and can escalate issues to Avaya when necessary.



If your IP Office system currently does not have an Avaya business partner providing support and maintenance for it, you can use the Avaya Partner Locator tool to find a business partner. See [Finding an Avaya Business Partner](#) on page 153.

#### Related links

[Additional Help and Documentation](#) on page 152

---

## Finding an Avaya Business Partner

If your IP Office system currently does not have an Avaya business partner providing support and maintenance for it, you can use the Avaya Partner Locator tool to find a business partner.

#### Procedure

1. Using a browser, go to the [Avaya Website](#) at <https://www.avaya.com>
2. Select **Partners** and then **Find a Partner**.
3. Enter your location information.
4. For IP Office business partners, using the **Filter**, select **Small/Medium Business**.

#### Related links

[Additional Help and Documentation](#) on page 152

---

## Additional IP Office resources

In addition to the documentation website (see [Additional Manuals and User Guides](#) on page 152), there are a range of website that provide information about Avaya products and services including IP Office.

- [Avaya Website](#) (<https://www.avaya.com>)

This is the official Avaya website. The front page also provides access to individual Avaya websites for different regions and countries.

- [Avaya Sales & Partner Portal](#) (<https://sales.avaya.com>)

This is the official website for all Avaya business partners. The site requires registration for a user name and password. Once accessed, you can customize the portal to show specific products and information type that you want to see.

- [Avaya IP Office Knowledgebase](#) (<https://ipofficekb.avaya.com>)

This site provides access to an online, regularly updated version of IP Office user guides and technical manual.

- [Avaya Support](#) (<https://support.avaya.com>)

This site provide access to Avaya product software, documentation and other services for Avaya product installers and maintainers.

- [Avaya Support Forums](https://support.avaya.com/forums/index.php) (<https://support.avaya.com/forums/index.php>)

This site provides forums for discussing product issues.

- [International Avaya User Group](https://www.iuag.org) (<https://www.iuag.org>)

This is the organization for Avaya customers. It provides discussion groups and forums.

- [Avaya DevConnect](https://www.devconnectprogram.com/) (<https://www.devconnectprogram.com/>)

This site provides details on APIs and SDKs for Avaya products, including IP Office. The site also provides application notes for third-party non-Avaya products that interoperate with IP Office using those APIs and SDKs.

- [Avaya Learning](https://www.avaya-learning.com/) (<https://www.avaya-learning.com/>)

This site provides access to training courses and accreditation programs for Avaya products.

#### Related links

[Additional Help and Documentation](#) on page 152

---

## Training

Avaya training and credentials ensure our Business Partners have the capabilities and skills to successfully sell, implement, and support Avaya solutions and exceed customer expectations. The following credentials are available:

- Avaya Certified Sales Specialist (APSS)
- Avaya Implementation Professional Specialist (AIPS)
- Avaya Certified Support Specialist (ACSS)

Credential maps are available on the [Avaya Learning](#) website.

#### Related links

[Additional Help and Documentation](#) on page 152

# Index

## Numerics

443 .....	<a href="#">21</a>
8443 .....	<a href="#">21</a>
9600 .....	<a href="#">15</a>

## A

access service	
monitor .....	<a href="#">24</a>
adding log	
log stamps .....	<a href="#">38</a>
Address	
blacklist .....	<a href="#">86</a>
Administrator .....	<a href="#">152</a>
Alarm Log .....	<a href="#">14</a>
alarms .....	<a href="#">84</a>
analog	
analog line .....	<a href="#">111</a>
answer .....	<a href="#">120</a>
APIs .....	<a href="#">153</a>
Application Notes .....	<a href="#">153</a>
applications .....	<a href="#">120</a>
archive	
extract .....	<a href="#">80</a>
syslog .....	<a href="#">78–80</a>
ATM .....	<a href="#">48</a>

## B

background color .....	<a href="#">33</a>
binary	
logging .....	<a href="#">38</a>
text .....	<a href="#">40</a>
blacklisted	
IP address .....	<a href="#">84, 86</a>
buffer	
trace options .....	<a href="#">88</a>
business partner locator .....	<a href="#">153</a>

## C

call	
detection .....	<a href="#">49</a>
embedded voicemail .....	<a href="#">49</a>
events .....	<a href="#">49</a>
packets .....	<a href="#">49</a>
PC voicemail .....	<a href="#">49</a>
caller	
caller line .....	<a href="#">111</a>
ID .....	<a href="#">112</a>
calls	

calls ( <i>continued</i> )	
disconnect .....	<a href="#">113</a>
making .....	<a href="#">118</a>
calls answered	
generated .....	<a href="#">120</a>
calls dropping .....	<a href="#">121</a>
cause .....	<a href="#">146</a>
code .....	<a href="#">146</a>
changes	
port .....	<a href="#">138–144</a>
clearing log .....	<a href="#">27</a>
clearing option .....	<a href="#">44, 45</a>
clearing trace .....	<a href="#">44, 45</a>
client	
ports .....	<a href="#">135</a>
close	
system .....	<a href="#">22</a>
closing system .....	<a href="#">22</a>
code	
cause .....	<a href="#">146</a>
definition .....	<a href="#">146</a>
color	
trace options .....	<a href="#">34</a>
coloring	
individual .....	<a href="#">43</a>
tab .....	<a href="#">44</a>
COM .....	<a href="#">138</a>
community	
networking .....	<a href="#">106</a>
compression .....	<a href="#">109</a>
T1 .....	<a href="#">109</a>
conference .....	<a href="#">89</a>
configuration .....	<a href="#">94</a>
security .....	<a href="#">23</a>
configuring service .....	<a href="#">24</a>
configuring syslog trace .....	<a href="#">76</a>
connecting system	
HTTP .....	<a href="#">20</a>
HTTPS .....	<a href="#">21</a>
TCP .....	<a href="#">19</a>
UDP .....	<a href="#">18</a>
connection	
problems .....	<a href="#">116</a>
site data .....	<a href="#">117</a>
connections	
PR1 .....	<a href="#">116</a>
converting binary .....	<a href="#">40</a>
converting files	
syslog .....	<a href="#">81</a>
converting IP Address .....	<a href="#">29</a>
copy	
screen log .....	<a href="#">32</a>
correct	

correct ( <i>continued</i> )		File	40
working	119	file log	37, 38
courses	153	files	81
CTI	51	filter	28
Customer Operations Manager	21, 138	firewall	
		working	119
<b>D</b>		font	
data	90, 96, 101, 106, 107, 116	select	33
connection	117	forums	153
system	88	frame	
Data terminal equipment (DTE)	53	relay	54, 117
date and time	35	<b>G</b>	
decoding FEC		generated calls	120
errors	149	GOD	55
default		<b>H</b>	
logging	10	H.323	56, 92
options	45	Help	152
system monitor	10	hex	
default syslog trace		values	29
options	77	HTTP	20, 23, 25
defaulting the trace	45	HTTPS	21
dial-up		<b>I</b>	
connection	116	icons	14
Digital Enhanced Cordless Telecommunications (DECT)	90	ID	
Direct Station Selection (DSS)	91	ISDN	112, 146
Directory	52	Identification ID	111
disabling access	23	indenting	34
disconnecting calls	113	indication	
downloading syslog	78–80	waiting	120
drop		installing system monitor	10
speech calls	121	Integrated Services Digital Network (ISDN)	58, 146
Dynamic Host Configuration Protocol (DHCP)	90	Interface	57
<b>E</b>		internet	118
EConf	54	Internet Service Provider (ISP)	
email		connection	116
screen log	31	IP	86
enabling syslog	76	phones	118
equinox		IP address	29
status	92	IP office	
errors		applications	120
decoding	149	IP Office	23
example settings	110	ports	123
extensions	84	security	23
blacklisted	84	system	125
extract syslog	80	IPO	93
<b>F</b>		IPV6	94
Fast Ethernet Controller (FEC)	149	ISDN	112, 146
file	33, 40	calls	113
loading	43	problem	116
logging	36		
save	42		

<b>J</b>		
J100		
phone .....	<a href="#">110</a>	
Jade .....	<a href="#">60, 94</a>	
<b>K</b>		
key .....	<a href="#">61</a>	
keyboard .....	<a href="#">15</a>	
<b>L</b>		
lamp .....	<a href="#">61</a>	
leased		
over .....	<a href="#">117</a>	
license .....	<a href="#">104</a>	
line		
status .....	<a href="#">90</a>	
loading trace .....	<a href="#">43</a>	
locating		
calls .....	<a href="#">118</a>	
log		
add .....	<a href="#">38</a>	
clear .....	<a href="#">27</a>	
convention .....	<a href="#">40</a>	
file .....	<a href="#">40</a>	
pause .....	<a href="#">27</a>	
screen .....	<a href="#">26</a>	
setting .....	<a href="#">36</a>	
log file .....	<a href="#">32, 39</a>	
logging .....	<a href="#">10, 37, 38</a>	
Logging .....	<a href="#">95</a>	
logging to a file .....	<a href="#">36</a>	
<b>M</b>		
manager		
ports .....	<a href="#">137</a>	
manually rolling		
file .....	<a href="#">40</a>	
Manuals .....	<a href="#">152</a>	
map .....	<a href="#">96</a>	
media .....	<a href="#">61</a>	
ports .....	<a href="#">137</a>	
memory		
data .....	<a href="#">96</a>	
message		
indication .....	<a href="#">120</a>	
miscellaneous .....	<a href="#">151</a>	
monitor .....	<a href="#">9</a>	
icons .....	<a href="#">14</a>	
install .....	<a href="#">10</a>	
password .....	<a href="#">23</a>	
settings .....	<a href="#">110</a>	
syslog output .....	<a href="#">76</a>	
monitor ( <i>continued</i> )		
system .....	<a href="#">18, 30</a>	
monitor access .....	<a href="#">24</a>	
<b>N</b>		
network .....	<a href="#">98, 106</a>	
Network address port translation (NAPT) .....	<a href="#">97</a>	
networking .....	<a href="#">106</a>	
<b>O</b>		
opening .....	<a href="#">32, 39</a>	
option		
trace .....	<a href="#">45</a>	
options .....	<a href="#">43, 47</a>	
trace .....	<a href="#">43, 44</a>	
outdialer .....	<a href="#">99</a>	
output .....	<a href="#">76</a>	
<b>P</b>		
paint .....	<a href="#">15</a>	
partner		
sessions .....	<a href="#">100</a>	
pause screen .....	<a href="#">27</a>	
PC		
internet .....	<a href="#">118</a>	
performance .....	<a href="#">101</a>	
phone .....	<a href="#">105</a>	
problems .....	<a href="#">118</a>	
status .....	<a href="#">92, 102, 105</a>	
troubleshooting .....	<a href="#">110</a>	
Point-to-Point Protocol (PPP) .....	<a href="#">62</a>	
port .....	<a href="#">138–144</a>	
portal .....	<a href="#">135</a>	
one .....	<a href="#">135</a>	
ports .....	<a href="#">123, 125, 137</a>	
Ports .....	<a href="#">133</a>	
PR1 .....	<a href="#">116</a>	
preferences		
log .....	<a href="#">36</a>	
Primary Rate Interface (PRI) .....	<a href="#">108</a>	
pro		
voicemail .....	<a href="#">133</a>	
problems		
dial-up .....	<a href="#">116</a>	
problems involved .....	<a href="#">118</a>	
protocols .....	<a href="#">125</a>	
<b>Q</b>		
quarantined		
phone .....	<a href="#">102</a>	
quarantined status .....	<a href="#">102</a>	
Quick Reference Guides .....	<a href="#">152</a>	

## R

R2	63
reboot	115
reconnect	
monitored system	30
system	30
relay	54
links	117
remote	
site data	117
Report	11
Reseller	152
roll over	
log file	40
Routing	64
RTP	
sessions	107

## S

sales	153
saving file	33, 40
saving screen log	
file	33, 40
saving trace option	
file	42
SCN	104
screen	83
background color	33
clear log	27
filter	28
font	33
log	26
screen log	27, 33, 40
copy	32
email	31
pause	27
search	28
SDKs	153
search	
screen log	28
selecting system	
monitor	29
server	
ports	135
service	25
services	66
session	100
Session Initiation Protocol (SIP)	67, 105, 106
sessions	107, 108
setting	
monitor examples	110
option	45
setting log	
preferences	36
setting password	23

setting trace	
option	45
options	42
shortcuts	15
small community	106
SNet	93
specific	
call	118
speech calls	
dropping	121
SRTP	
sessions	107
SSI	68
stamps	
log	38
starting	18
starting file	
logging	37
starting screen	
log	27
starting systemmonitor	18
status	83, 89, 91, 92, 96, 97, 99
alarm	30
H.323	92
menu	31
Status	11
stopping file	
logging	38
streams	
data	107
Subscription	21
support	153
Sustainable Communities Network (SCN)	65
switching binary and text	38
switching logging	38
syslog	75
archive	78–80
extract	80
monitor	76
trace options	77
Syslog	
files	81
syslog trace	
options	76
system	9
connection	20, 21
monitor	10, 22, 29
ports	125
rebooting	115
System	11, 69
System Administrator	152
system monitor	
selection	29

## T

T1	69
----	----

T1 ( <i>continued</i> )	
connections .....	<a href="#">116</a>
EI .....	<a href="#">116</a>
tab	
options .....	<a href="#">44</a> , <a href="#">45</a>
Tab coloring .....	<a href="#">44</a>
TCP .....	<a href="#">23</a> , <a href="#">107</a>
Technical Bulletins .....	<a href="#">153</a>
text	
logging .....	<a href="#">38</a>
trace	
options .....	<a href="#">43–45</a> , <a href="#">47</a>
trace menu	
options .....	<a href="#">47</a>
trace option	
file saving .....	<a href="#">42</a>
tab .....	<a href="#">45</a>
trace options	
color .....	<a href="#">34</a>
coloring .....	<a href="#">43</a> , <a href="#">44</a>
setting .....	<a href="#">42</a>
tracing .....	<a href="#">75</a>
training .....	<a href="#">153</a> , <a href="#">154</a>
Transmission Control Protocol (TCP) .....	<a href="#">19</a> , <a href="#">106</a>
Trigger string detection .....	<a href="#">49</a>
troubleshooting .....	<a href="#">110</a>
trunk .....	<a href="#">111</a>
caller ID .....	<a href="#">112</a>
trunks	
PRI .....	<a href="#">108</a>

## U

UDP .....	<a href="#">23</a>
US .....	<a href="#">108</a>
user	
data .....	<a href="#">106</a>
User Datagram Protocol (UDP) .....	<a href="#">18</a>
User Guides .....	<a href="#">152</a>
using screen log .....	<a href="#">26</a>

## V

VComp .....	<a href="#">71</a>
view	
alarm .....	<a href="#">30</a>
menu .....	<a href="#">31</a>
network .....	<a href="#">98</a>
viewing status alarm .....	<a href="#">30</a>
viewing status menu .....	<a href="#">31</a>
Virtual Private Network VPN .....	<a href="#">72</a>
voice .....	<a href="#">109</a>
voicemail .....	<a href="#">108</a>
ports .....	<a href="#">133</a>

## W

wating .....	<a href="#">120</a>
websites .....	<a href="#">153</a>
What's new .....	<a href="#">9</a>
Wide Area Network (WAN) .....	<a href="#">74</a>
lines .....	<a href="#">117</a>
work	
correctly .....	<a href="#">119</a>