TECHNICAL WHITE PAPER

Avaya Endpoints logs collection guide

Date: 22nd June, 2015
Authors: Jiang, Ping (Sawyer); Ivan Proença

Abstract

This document explains how-to collect logs from various Avaya Endpoints. It is applicable to the below listed Avaya Endpoints (hard-phone and soft-client models):

- 96x0 (9610, 9620, 9630, 9640, 9650, 9670)
- 96x1 (9608, 9611, 9621, 9641)
- Avaya one-X® Communicator soft-client
- Avaya one-X® Agent soft-client
- Avaya one-X® Attendant soft-client
- Avaya Flare Experience
- Avaya IP Softphone 2050

AVAYA
The Power of We™

Contents

1. Hard-phone syslog

System logs are written to a volatile memory and containing information mainly regarding performance and related code explanation for troubleshooting.

H.323 Syslog is already included in Phone Report (will be introduced in later **section 3.1**). It should be provided independently in case the relevant scenario is missing in the phone report. It could also be sent to an external server.

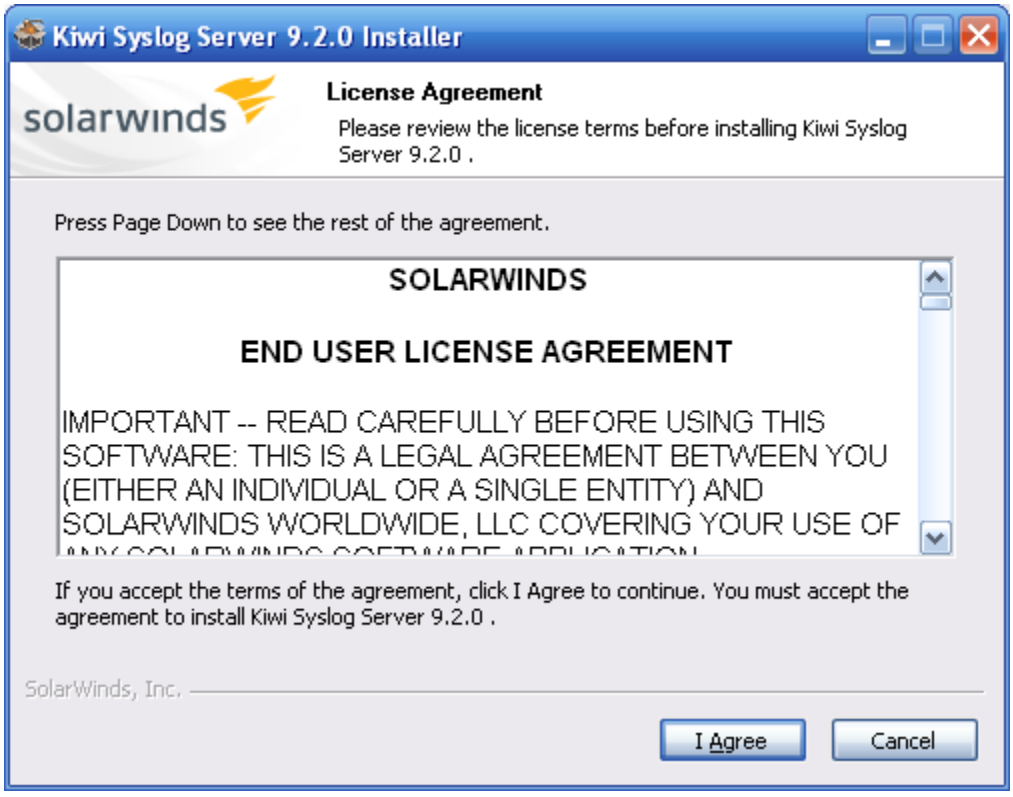
1.1 External software installation

Syslog software can be found on the internet, from licensed to freeware. We shall use **Kiwi syslog**, as an example in this document.

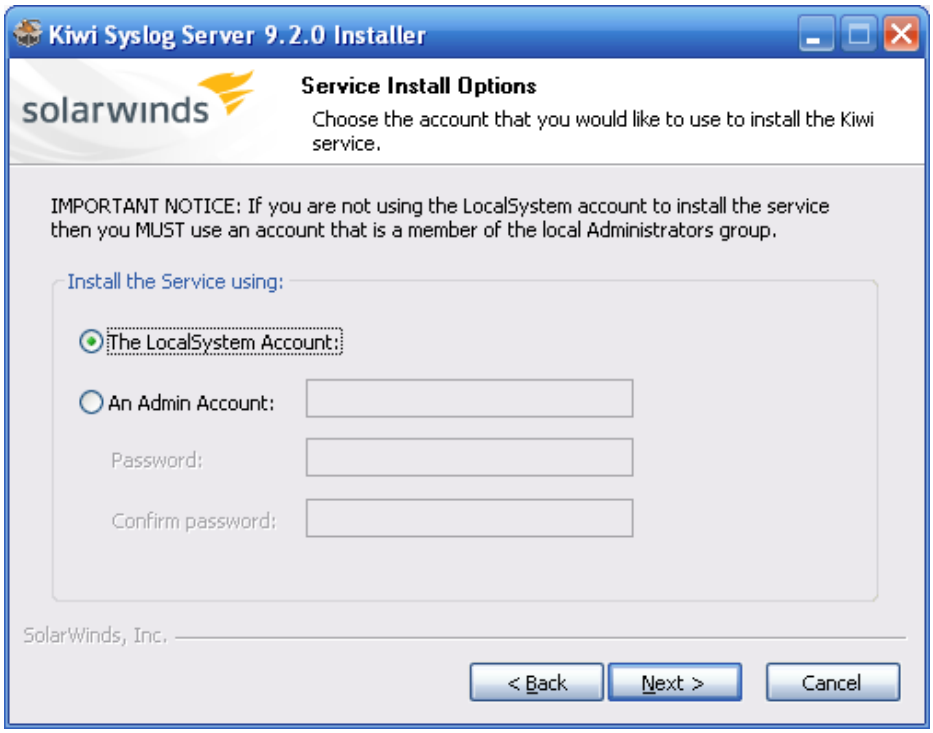
Please download Kiwi syslog from the below link (free version available):

http://www.kiwisyslog.com/products/kiwi-syslog-server/product-overview.aspx/

Once downloaded, install using the '***Kiwi_Syslog_Server_9.2.0.setup.exe***':

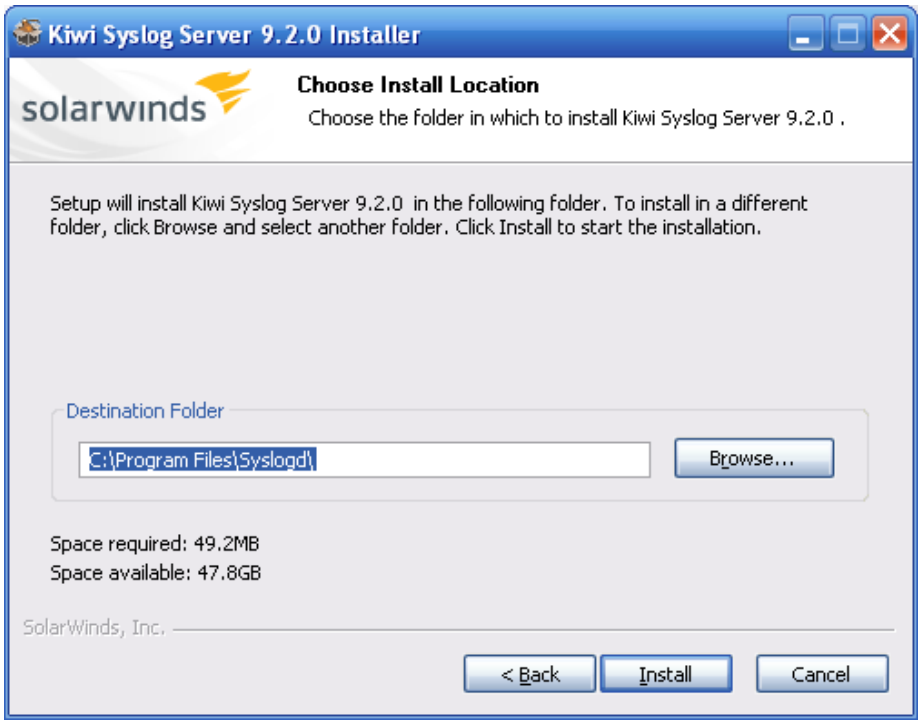



Kiwi Syslog Server 9.2.0 Installer
solarwinds
Choose Operating Mode
The program can be run as a Service or Application
Install Kiwi Syslog Server as a Service
This option installs Kiwi Syslog Server as a Windows service, allowing the program to run without the need for a user to login to Windows. This option also installs the Kiwi Syslog Server Manager which is used to control the service.
Install Kiwi Syslog Server as an Application
This option installs Kiwi Syslog Server as a typical Windows application, requiring a user to login to Windows before running the application.
SolarWinds, Inc.
< Back
Next >
Cancel

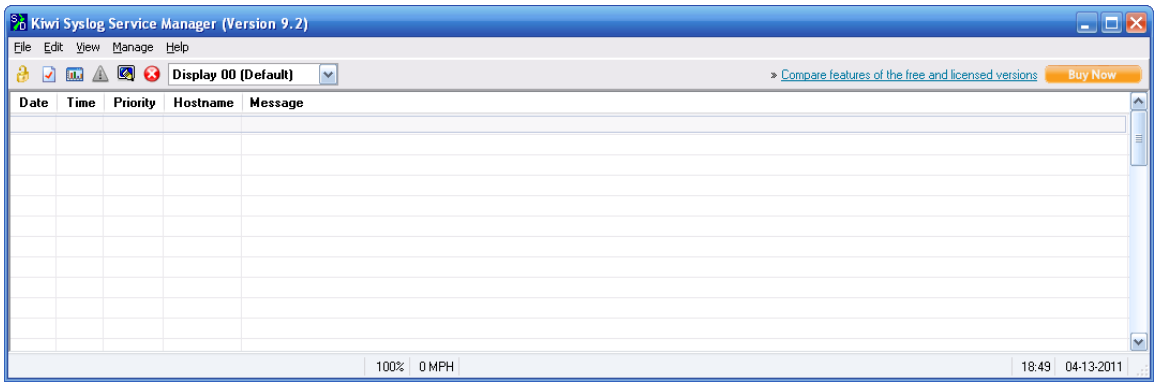

Kiwi Syslog Server 9.2.0 Installer
solarwinds
Service Install Options
Choose the account that you would like to use to install the Kiwi service.
IMPORTANT NOTICE: If you are not using the LocalSystem account to install the service then you MUST use an account that is a member of the local Administrators group.
Install the Service using:
The LocalSystem Account:
An Admin Account:
Password:
Confirm password:
SolarWinds, Inc.
< Back
Next >
Cancel


Kiwi Syslog Server 9.2.0 Installer
solarwinds
Install Kiwi Syslog Web Access
Remote viewing, filtering and highlighting of Syslog events...
Install Kiwi Syslog Web Access
Create a new Web Access logging rule in Kiwi Syslog Server
Kiwi Syslog Web Access can only be enabled in the licensed or evaluation versions of Kiwi Syslog Server.
SolarWinds, Inc.
< Back
Next >
Cancel


Kiwi Syslog Server 9.2.0 Installer
solarwinds
Choose Components
Choose which features of Kiwi Syslog Server 9.2.0 you want to install.
This will install Kiwi Syslog Server version 9.2.0
Select the type of install:
Normal
Or, select the optional components you wish to install:
Program files (required)
Shortcuts apply to all users
Add Start menu shortcut
Add Desktop shortcut
Add QuickLaunch shortcut
Add Start-up shortcut
Description
Position your mouse over a component to see its description.
Space required: 49.2MB
SolarWinds, Inc.
< Back
Next >
Cancel


Kiwi Syslog Server 9.2.0 Installer
solarwinds
Choose Install Location
Choose the folder in which to install Kiwi Syslog Server 9.2.0 .
Setup will install Kiwi Syslog Server 9.2.0 in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.
Destination Folder
C:\Program Files\Syslogd\
Browse...
Space required: 49.2MB
Space available: 47.8GB
SolarWinds, Inc.
< Back
Install
Cancel

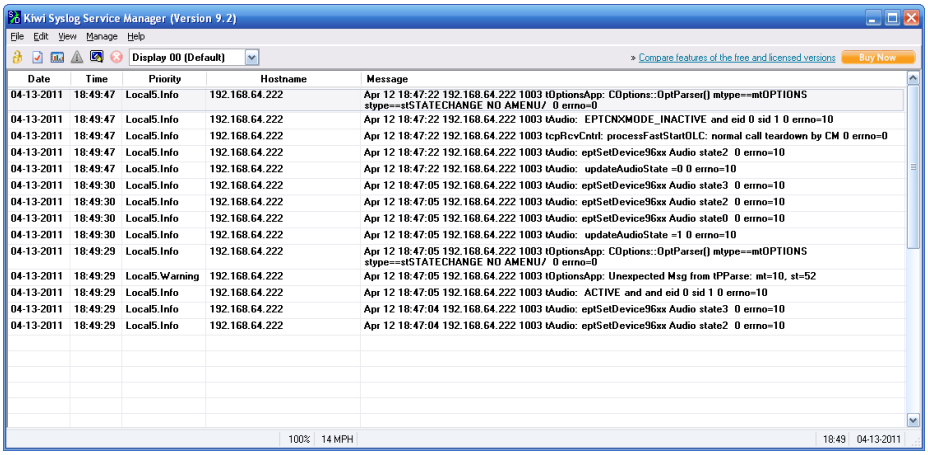

Kiwi Syslog Server 9.2.0 Installer
Completing the Kiwi Syslog Server 9.2.0 Setup Wizard
Kiwi Syslog Server 9.2.0 has been installed on your computer.
Click Finish to close this wizard.
Run Kiwi Syslog Server 9.2.0
solarwinds
Visit the SolarWinds website
< Back
Finish
Cancel



1.2 Enable syslog from endpoint

To begin capturing activities of the phone on the syslog, you need to do the followings:

1. In the '***46xxsettings.txt***' file, uncomment parameter and configure ***SET LOGSRVR*** *X.X.X.X* (where X.X.X.X is the IP address of the Syslog Server/PC, you already setup, per above. Make sure that the syslog server and phones are reachable in the Network)
2. In the '***46xxsettings.txt***' file, uncomment parameter and configure ***SET LOGLOCAL 8*** (For debug level).
3. Reboot the phones to pick up the updated '***46xxsettings.txt***' file.
   - Make sure that the Syslog Server is up and running at this time to capture any event on the phones
4. Once rebooted, you should see logs on the syslog server window, similarly as it is seen in the below capture:



Note: 96X1 SIP phones performance can slowdown, if all the categories are enabled

1.3 Additional Info to collect, when collecting syslog

This is only being done if problem is reported as phone hang/freeze. Make sure to check phone firmware related information, prior to collecting logs.

a) Date and time the phone freezes

b) What is the call flow when the phone freezes, confirm with end-user on what is seen happening on the phone's display.

c) Request end-user not to reboot the impacted phone, yet. Go to Communication Manager (CM) and issue command '***status station*** *xxxx*' and capture all pages where xxxx is the extension # of the phone that hangs

d) Also take the command '***list registered-ip-stations ext*** *xxxx*' where xxxx is the extension # of the phone, that hangs

e) Once all details have been collected, end-user can reboot the phone

f) Note down the date and time, when the phone is rebooted

Note: This is applicable only to H.323 phones.

2. Hard-phone MIB log

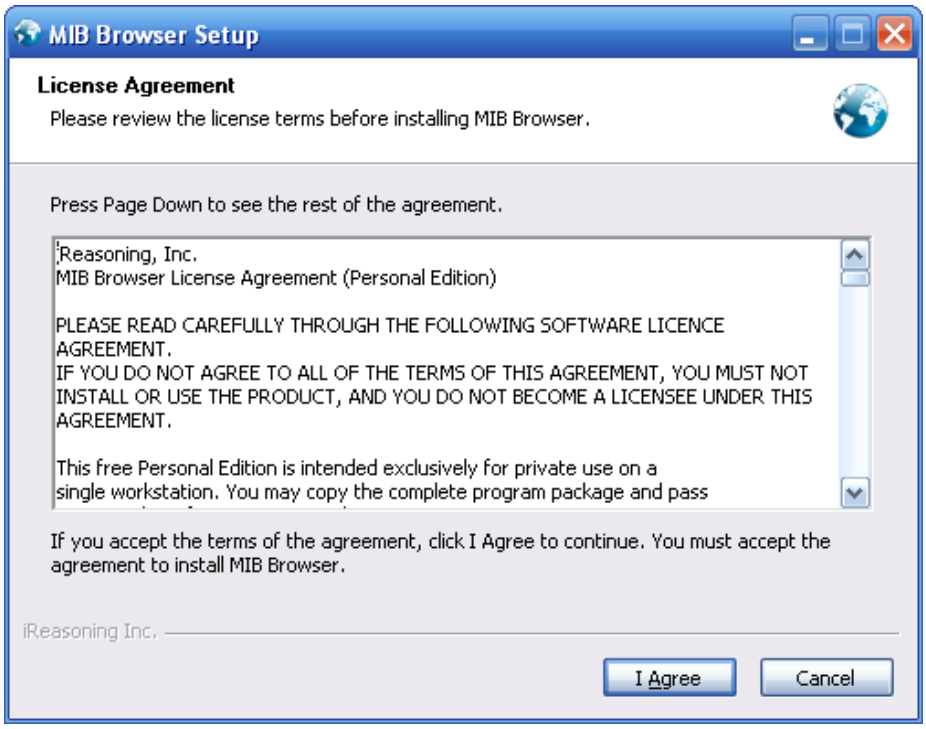
Simple Network Management Protocol (SNMP) is a vehicle for managing network devices. An SNMP network element is a device (i.e., router, switch, IP phone) that has a management information base (MIB), which is a tree of objects. Some objects contain data. For example, the object sysUpTime contains a value stating how long the device has been up since last reboot.

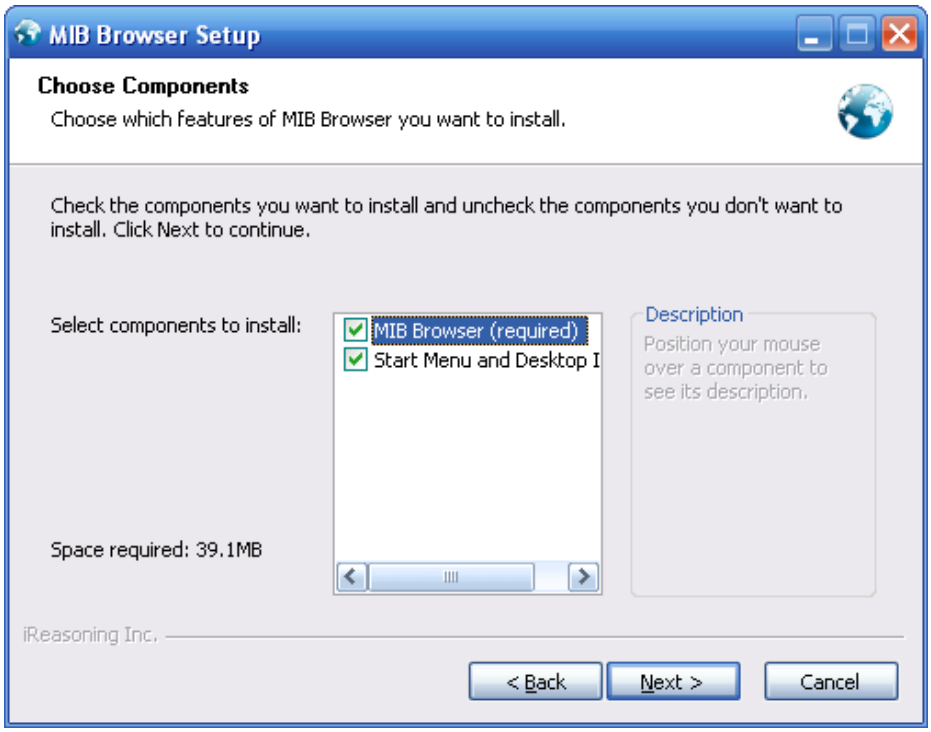
Some objects have other objects branching out from them. For example, sysContact, sysName, sysLocation and sysServices branching out from it.
An object like this is also called a sub tree.

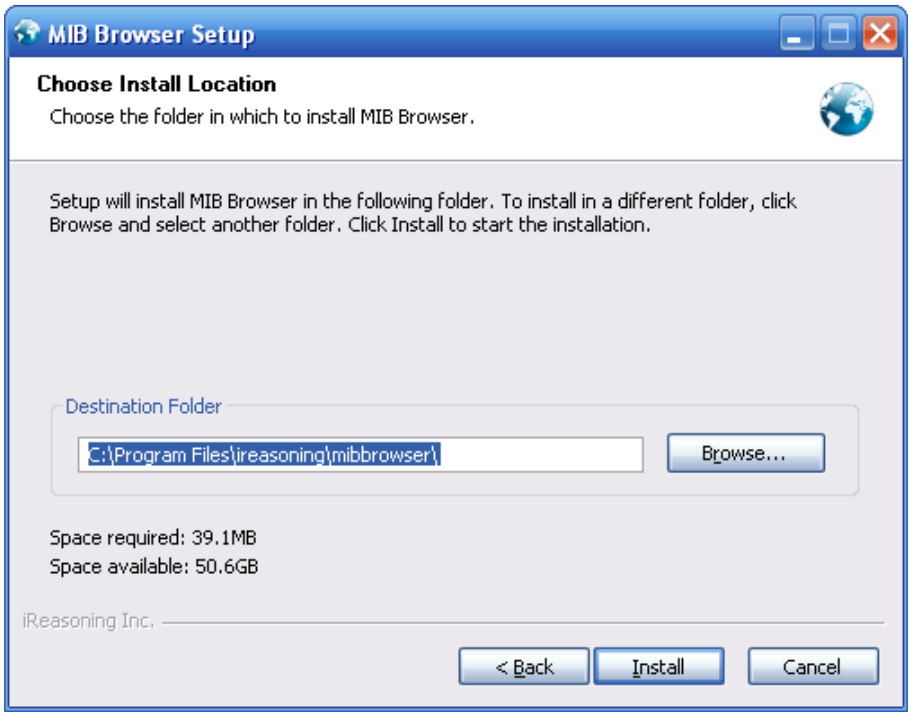
Avaya endpoint also can send related SNMP information to SNMP receiver; we will cover two approaches and introduce how to collect SNMP information.

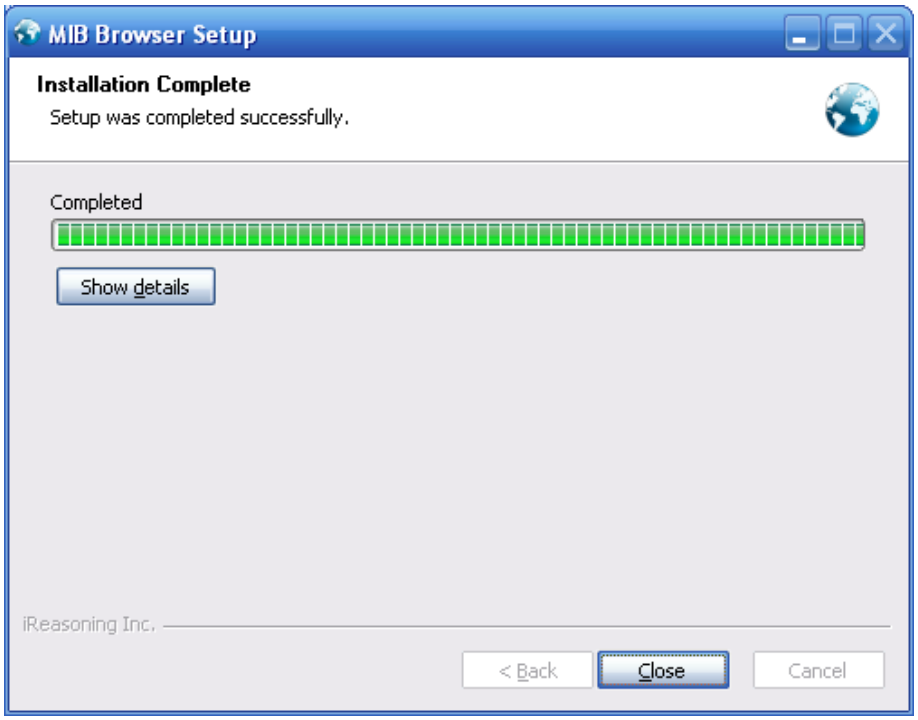
2.1 SNMP client software

Download MIB Browser from the below link, download the free personal edition and then install:
http://ireasoning.com/mibbrowser.shtml

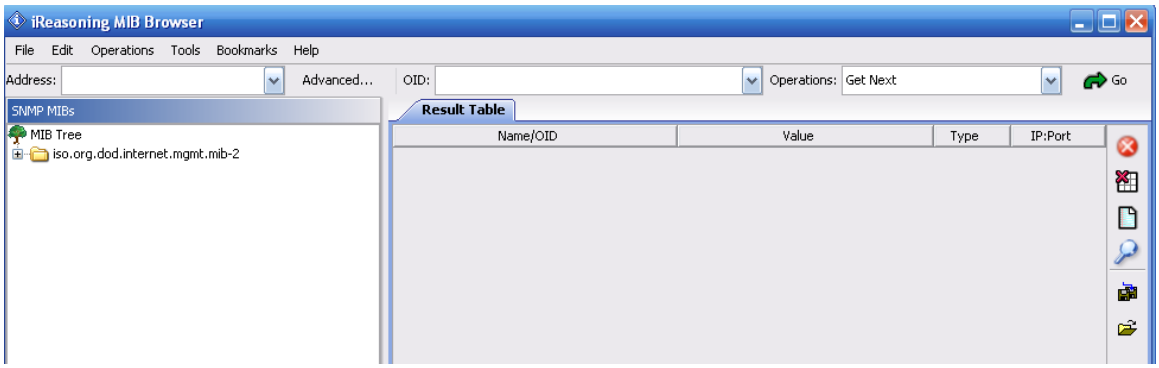

MIB Browser Setup
License Agreement
Please review the license terms before installing MIB Browser.
Press Page Down to see the rest of the agreement.
Reasoning, Inc.
MIB Browser License Agreement (Personal Edition)
PLEASE READ CAREFULLY THROUGH THE FOLLOWING SOFTWARE LICENCE AGREEMENT.
IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, YOU MUST NOT INSTALL OR USE THE PRODUCT, AND YOU DO NOT BECOME A LICENSEE UNDER THIS AGREEMENT.
This free Personal Edition is intended exclusively for private use on a single workstation. You may copy the complete program package and pass
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install MIB Browser.
iReasoning Inc.
I Agree
Cancel


MIB Browser Setup
Choose Components
Choose which features of MIB Browser you want to install.
Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.
Select components to install:
MIB Browser (required)
Start Menu and Desktop I
Description
Position your mouse over a component to see its description.
Space required: 39.1MB
iReasoning Inc.
< Back
Next >
Cancel


MIB Browser Setup
Choose Install Location
Choose the folder in which to install MIB Browser.
Setup will install MIB Browser in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.
Destination Folder
C:\Program Files\ireasoning\mibbrowser\
Browse...
Space required: 39.1MB
Space available: 50.6GB
iReasoning Inc.
< Back
Install
Cancel


MIB Browser Setup
Installation Complete
Setup was completed successfully.
Completed
Show details
iReasoning Inc.
< Back
Close
Cancel

Then you should see the following screen:



2.2 MIB files

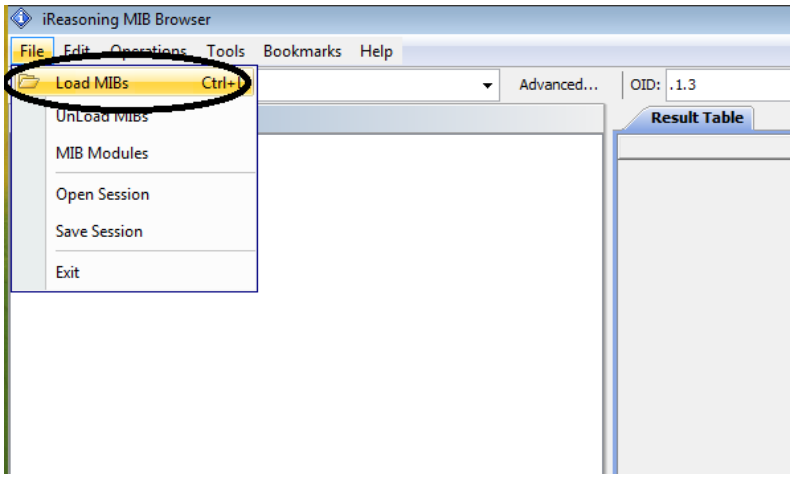
Avaya supply different MIB files for different endpoints. Customer and business partners should download respective MIB files corresponding to their endpoint type.

Here are the links to different phone models (latest can be found from support.avaya.com)

- 4600 MIB: ftp://ftp.avaya.com/incoming/Up1cku9/tsoweb/ip_telephone/46xxmib24.txt
- 9600 MIB: http://support.avaya.com/elmodocs2/MIB/96xxmib.txt
- 96x1 6.3 MIB: https://support.avaya.com/downloads/download-details.action?contentId=C2013922185185600_7&productId=P0553&releaseId=H.323%206.3.x
- 16X0 1.2 MIB: https://support.avaya.com/downloads/download-details.action?contentId=C20090710164240184625489&productId=P0468&releaseId=1.2.x

2.2.1 How-to load MIB files

Open your MIB browser and load the files from ***section 2.2***, into your browser:

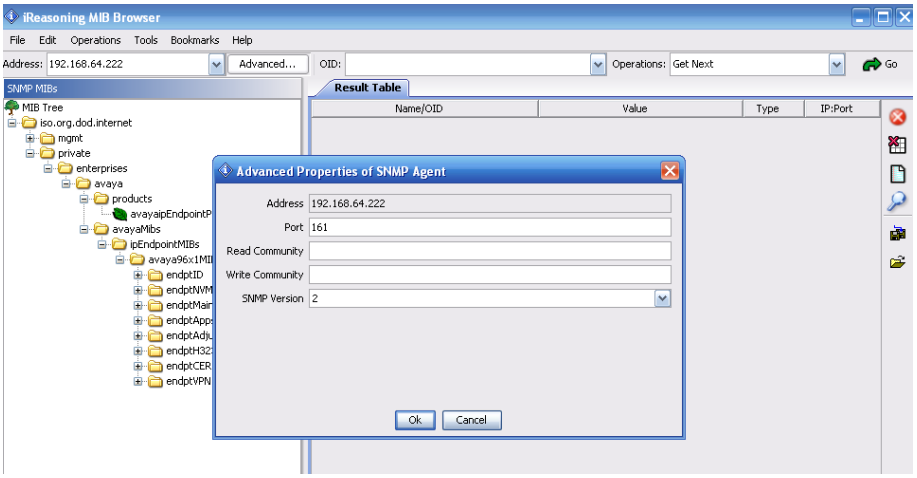


2.3 Enable SNMP from endpoint

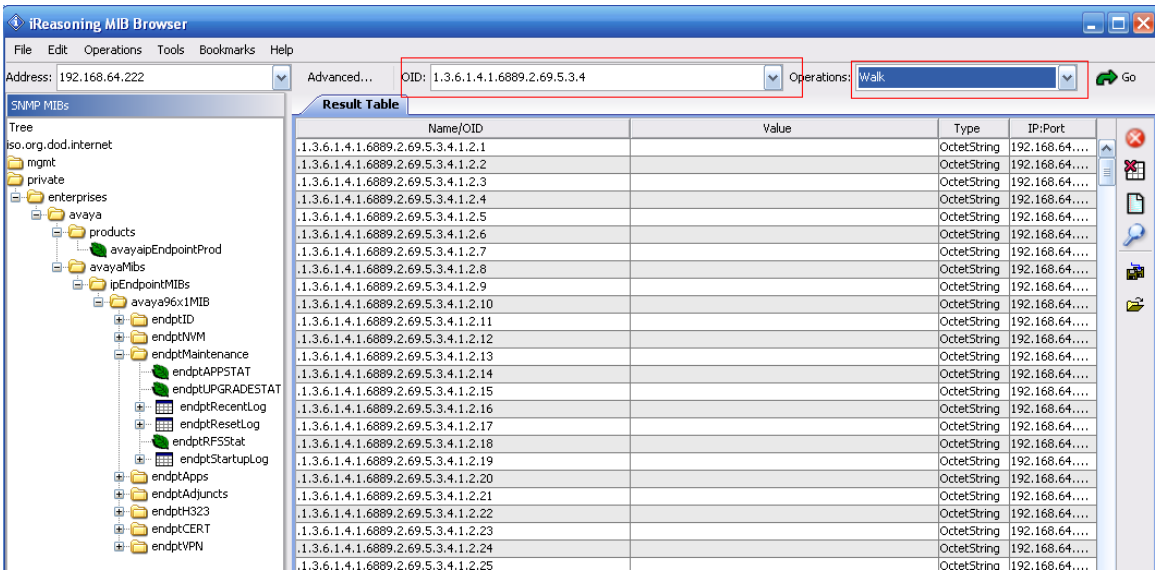
- In the '***46xxsettings.txt***' file, uncomment parameter and configure '***SET SNMPSTRING public***'.
- In the '***46xxsettings.txt***' file, uncomment parameter and configure ***SET SNMPADD*** *x.x.x.x,y.y.y.y* (where x.x.x.x,y.y.y.y is the IP address of the MIB Browser)

2.4 How-to collect SNMP data

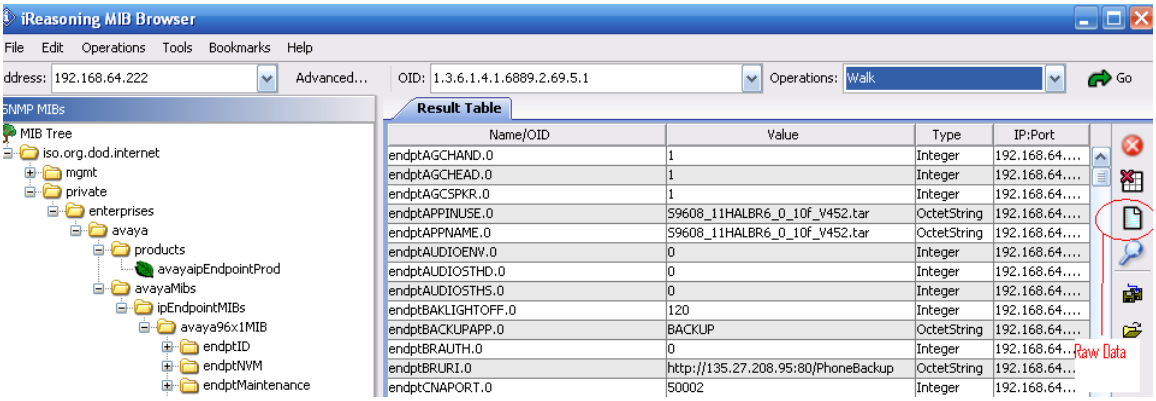
For '***Address***' field, put the ip-address of the IP phone that experiences hang issue, then set the '***SNMP version***' field to '***2***', as seen in the below capture:



Click ok then put the OID value '***.1.3.6.1.4.1.6889.2.69***' and then, under ***Operations*** → select '***Walk***' and you should receive results, as seen in the below capture:



Once done, on the right-hand side, there is a link to click on Raw Data, as highlighted below:



Then copy all the output from the raw result to a notepad make a filename of the result to the same OID.

2.5 Other document reference, to set SNMP

Here is a link to the IP Telephone SNMP Security document detailing instructions on how to configure SNMP for Avaya IP Phones:
http://support.avaya.com/elmodocs2/security/ipphone_snmp_secv7.pdf

3. Other logs for hard-phones

Other logs cover 96x1 phone types only, those of 96x0 phones have to be taken from serial adapter and most of our customers and business partners, do not have this tool kit.

Regarding debug, from endpoint firmware 6.2 and later version, please note the following:

The DEBUG option is available for use only for non-default passwords (different than '***CRAFT***'). To set a new password for the craft menu, change '***PROCPSWD***' parameter in the settings file.

The new value of the PROCPSWD parameter must be 4 to 7 numeric digits, '0000' through '9999999'. However, if value of PROCPSWD is less than 4 digits, the value will be changed back to the default value of '***27238***' ('***CRAFT***').

3.1 Phone Report

This report can be generated any time, per user request, and it includes information regarding a phone's last events and a "snapshot" of registers and parameters values. The report can be simply opened by WinZip (*.tgz* file) and includes standard viewable text files inside. Generating and extracting the phone report, can be done by two ways:

3.1.1 Phone Report via phone menu

(H323 sets only and not possible during a call)

1. Press '***Mute***', '***C***', '***R***', '***A***', '***F***', '***T***', '#'
2. Scroll down and select '***DEBUG***'
3. Select '***Phone Report***'
4. The report file (named: [ext]_***report.tgz***) will be uploaded to the http location, mentioned at '***BRURI***' parameter in the phone's settings file (backup/restore server).

Note: When there is no BRURI parameter in the settings file, the menu will display "Create" instead of "Send" and the report will be saved in the RAM, and can be collected via shell.

We should set our laptop's ip-address, at the BRURI parameter in the phone's settings file, then we can use 'MV_IPTEL' to get phone report. MV_IPTEL is one small tool supplied by Avaya, we shall not cover the usage of this tool, in this document.

3.1.2 Phone Report via shell menu

One can enable shell access, using telnet or SSH connection. We recommend using SSH.

a) Using telnet connection (for 96x1 phones only, not for 96x0)

1. Open 'PUTTY', 'SecureCRT' or any other terminal program
2. Select '***telnet***' and connect via port '***23***' (for telnet)

In case of connection failure:

i) Verify that the '***Serial Port***' is active, Otherwise, set it to '***CLI***'
ii) Connect via Serial interface
iii) Verify that '***telnetd***' process is running by typing the command '***ps –x***'
iv) If '***telnetd***' is not running, invoke '***telnetd &***' and try to connect telnet again (goto #1)

Press '***Alt***' ***+ Left Arrow*** keys, to return back to previous view

Setting '***Logging Mode***' parameter to '***On***'

1. Press '***Mute***', '***C***', '***R***', '***A***', '***F***', '***T***', '#'
2. Scroll down and select '***DEBUG***' (please note **section 3**)
3. Change '***Log to files***' to '**On**'
4. Press '***Save***' (the phone will reboot after saving).

Note: Due to a known issue, when upgrading/downgrading 6.2.3 from/to 6.2.4, ***LOGTOFILE*** value might be undesirably changed. In this case a manual reconfiguration might be required.

b) Open an SSH connection

1. Ensure '***SSH_ALLOWED***' parameter is set to '***1***', in the '***46xxsettings.txt***' file
2. Open 'PUTTY', 'SecureCRT' or any other terminal program
3. Select '***SSH2***' at the terminal application (port 22 is used for ssh connection)
4. Login as '***craft***' user. The terminal will then display a product ID and a challenge code.
5. Contact Avaya Services, to receive a response code for the challenge code.

Notes:

i) Since r6.2 SP1, SSH phone reports contain full information.
ii) SSH does not require any special debugging mode state.

3.1.2a Phone report generation (for 96x1 phones only, not for 96x0)

Once shell has been enabled, run the following command:

- For H323 and SIP root users: ***/AvayaDir/lib/phone-report***
- For SIP SSH craft users: ***/AvayaDir/lib/phone-report-user***

This will generate the phone report at folder '***/tmp***' or '***/var/log***' (for SIP root users)

The report name is '***phone_report.tar.gz***' or '***phone_report_craft.tar.gz***' (for craft users)

3.1.3 Download phone report

We can copy files to USB or PC

a) Copying report files to USB

On 9611 and 9641 phones, core dump files and phone report can be copied to a USB device.

Note: This capability works for H323 phones only.

1. Open shell
2. Connect a storage device to the USB socket.
3. The phone should recognize the USB device and make it accessible under '***/mnt/h323_usb***'

To see all mounted paths type the command: ***mount***

Note: The phone might display an error of "Not enough power…". In this case, unplug any other devices or turn up the power, by the switch on the back panel.

4. Copy all desired files to the above USB mounted directory.
5. Before disconnecting the USB device, type the command: ***umount /mnt/h323_usb***

b) Uploading a file to the PC or remote server

Below are three methods that can be used:

1) TFTP:

- Run a TFTP server, on the PC
- From shell, use the command: ***tftp -p –l <file name> <PC- IP>***

2) FTPPUT:

ftpput -u <username> -p <password> <server IP> <destination file> <local file>

3) SCP (Copy a file from local to remote server. For directory use flag ***[-r]***):

scp <local file name> <username>@<remote_server_name>:/<remote_path>

3.2 Crash Report

Most of crash report is also included in phone report, except for the below core files:

Extracting steps:

1. Check via shell whether core files (.core) are available, using command: ***ls /data/crash***
2. Optional: compress core files before uploading, using the following command:

gzip /data/crash/<core filename>.core

3. Please DO NOT change core files names, as it contains valuable information.
4: Download files to PC or USB (covered in **section 3.1.3**)

3.3 Audio Report (for h.323 phone, also for 96x1 SIP Audio recording)

This report includes the full phone report and additional audio information.

Available only when '***AUDIOREPORT***' is set to '***1***', in the '***46xxsettings.txt***' file.

Creation and extraction steps:

1. Verify via the phone menu that the '***Logging Mode***' is '***On***'. If it is not enabled, set it to '***On***'.
   - Logging may be enabled also on multiple phones, via settings file by: '***SET LOGTOFILE 1***'.

   Note: When Logging Mode is 'OFF', the audio report will include only partial information.
2. Press '***Home***' (A-Menu)
3. Only in touch phones: Select '***Settings***'
4. Select '***Network Information***' and then select '***Report***' Soft key
5. The output is generated at: '***/tmp/Audio_Report.tar.gz***'
   Note: User can expect slowness when accessing phone, during report collection.
6. Upload the output file to the PC or copy it to a USB device

To generate this report via shell, run the command: ***/AvayaDir/lib/phone-report -a***

3.4 Sniffer / Ethereal / Wireshark / Packet trace

This whitepaper shall not cover details on how-to collect sniffer / ethereal / wireshark / packet trace, it being commonly used in data-networking.

Avaya recommends capturing bookend trace, for endpoints issue.

For examples:

- For phone registration issue, one should sniff at:
  - BOTH, controller end (PE/CLAN) and at the endpoint

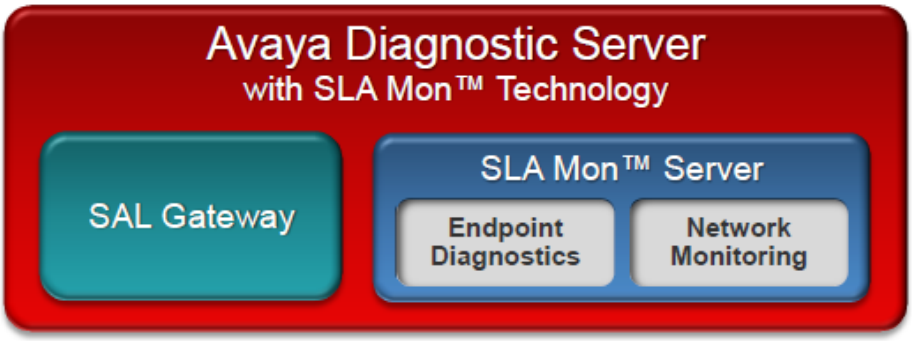
  Or
  - BOTH, Session Manager and at the endpoint

- For voice quality issue, sniffer should be taken at:
  - BOTH, Medpro/MG-VoIP and at the endpoint

4. Avaya Diagnostic Server (ADS) – with SLA Mon™ technology

Avaya offers Avaya Diagnostic Server - SLA Mon Server for endpoints log collection.

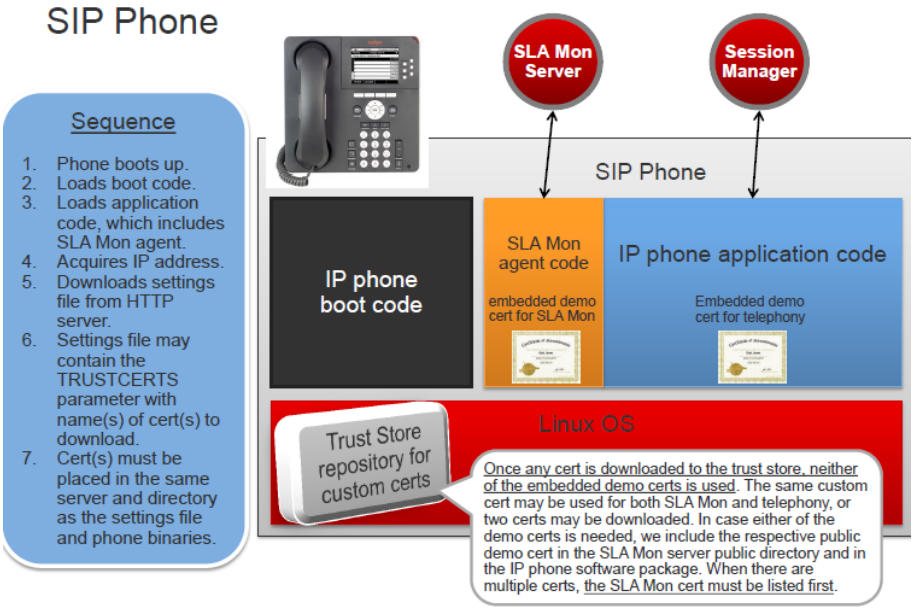
4.1 Introduction

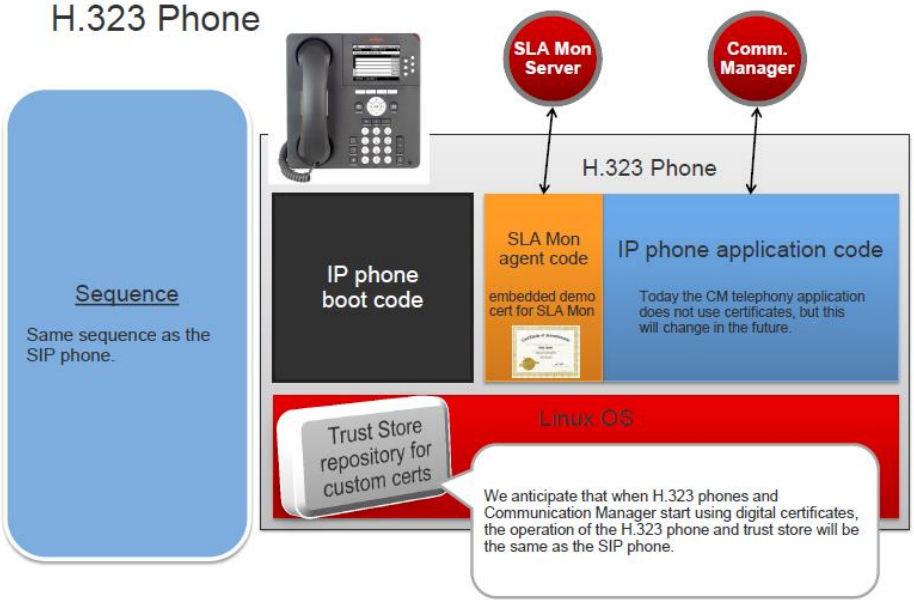


Advanced diagnostic capabilities differentiate the Avaya solution and Avaya maintenance

- SAL gateway – available to all Avaya maintenance customers
  - Secure connection between Avaya and the enterprise
  - Gateway for Avaya services delivery

- SLA Mon™ server – available to Support Advantage Preferred and Avaya Networking GE maintenance customers
  - Endpoint Diagnostics
  - Network Monitoring





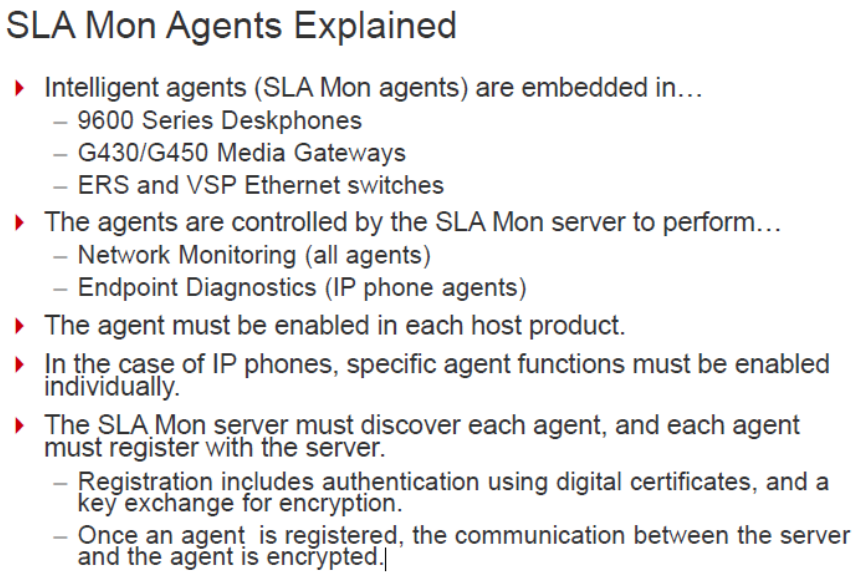
The latest 96x0/96x1 H.323 MIBs and latest 96x1 SIP MIB contain the following object:

endptTRUSTCERTS

- 96x0/96x1 H.323 MIB description:
  "Trusted Certificates list. This variable returns the current trusted certificates to be downloaded; 0-255 ASCII characters, 0 or more filenames or URLs separated by commas."

- 96x1 SIP MIB description:
  "Trusted Certificate URLs. This variable returns the URLs of certificate files that are considered as trusted certificates and requested to download into the endpoint at boot-time."

4.2 How an endpoint works with SLA Mon Server



4.2.1 Supported products and their versions (Compatibility Matrix)

Refer to the "Supported Products Interoperability List for Avaya Diagnostic Server SLA Mon™" document at https://downloads.avaya.com/css/P8/documents/100180195

4.2.2 Configuration at the endpoint end

Enable the Agent in IP Phones

46xxsettings file parameters	
SLMSTAT 1	Enable the agent. This also enables the network monitoring function.
SLMSRVR <a.b.c.d>	Set IP address of the SLA Mon server. Agent will only talk to this server (for security and control).
SLMCTRL 1, 2	Enable agent function – IP phone remote control (Agent Remote GUI). 1 = enable 2 = see below for 96x1 H.323 R6.4 local control function
SLMPERF 1	Enable agent function – IP phone events monitoring (Agent Remote GUI).
SLMCAP 1, 2	Enable agent function – IP phone remote packet capture. 1 = packet capture without RTP payload 2 = packet capture with RTP payload (see below for 96x1 H.323 R6.4)

Craft DEBUG Menu for 96x1 H.323 R6.4

- If SLMCTRL=2
  - then SLA Mon remote control can be enabled/disabled locally (disabled by default).
- If SLMCAP=2
  - then SLA Mon packet capture with RTP payload can be enabled/disabled locally (disabled by default)
- Values for both local parameters are: "Disabled," "Enabled," and "Active."
- DEBUG menu configuration requires PROCPSWD to be configured to non default value (27238).

- The latest 96x1 H.323 and SIP MIBs contain the following object:

  endptSLMSTAT

- 96x1 H.323 MIB description:

  "SLA Monitor permission flag. This variable returns 1 if the Avaya Service Level Agreement (SLA)_Monitor is enabled, else 0."

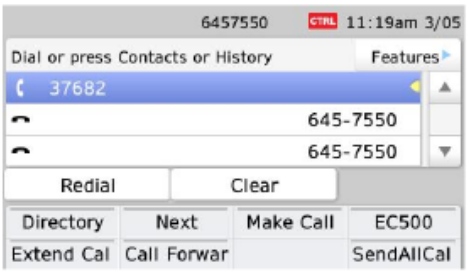
- 96x1 SIP MIB description:

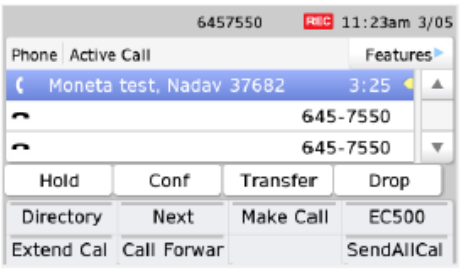
  "Indicates whether the SLA monitor agent is enabled or disabled. This variable returns a 0 if the monitor is disabled (default) and 1 if the monitor is enabled."

4.2.3 User Interface

User Prompts – 96x1 H.323 R6.4

- If IP phone remote control or packet capture is activated, the phone will display the CTRL & REC icons respectively, alerting the user that someone is controlling the phone.
- If these occur during a call, there will be “beeps” on the call every few seconds.
- Note that REC also appears when tcpdump is running using SSH connection.





4.3 SLA Mon Functionalities and Features

SLA Mon consists of primarily 2 functionalities:

1. Endpoint Diagnostics
2. Network Monitoring

4.3.1 Endpoint Diagnostics

The Endpoint diagnostics gives the capability to remotely diagnose Avaya 96xx and 96x1 IP deskphones by reducing the need for onsite technician and time-consuming deployment of sniffers and other tools

4.3.1a Features:

Phone Remote control:

The phone remote control feature is useful in troubleshooting Avaya endpoints remotely. Through this feature, service professional from Avaya, Partners, and customer can remotely access and control Avaya endpoints that the phone remote control feature enabled. You can perform remote activities on the endpoints, such as the following:

• Press buttons or perform touch events.

• Trigger calls between Avaya endpoints remotely and observe the events occurring on the remote endpoint.

• Monitor the overlay of the actual phone screen on the SLA Mon web interface to verify events displayed on the phone screen.

Event monitoring:

You can use the event monitoring feature to monitor events occurring on Avaya endpoints, such as button presses or touch events.

Phone screen capture:

Through the SLA Mon server command line interface (CLI), you can retrieve the real-time screen capture of the phone display area. Service personnel can use the screen capture feature to verify user comments and monitor the screen of the endpoints.

Bulk calls:

Through the SLA Mon server CLI, you can make bulk calls to stress test the communication system and the network. For example, if a branch location has to support 50 simultaneous calls to the central office, you can use the bulk calls feature to simulate the requirement.

Packet capture:

The packet capture feature captures the network traffic flowing in and out of Avaya endpoints. You can configure the SLA Mon agent on an endpoint to capture a copy of the network traffic. You can analyze the packets to identify issues with the device.

4.3.2 Network Monitoring

The network monitoring features provide vendor agnostic, end-to-end network insight into conditions that might have an impact on your voice, video, and data applications. The feature provides an easy-to-understand visual representation of your network performance data. Using the network-performance and the call-trace data, you can proactively identify and troubleshoot network issues.

The network monitoring feature displays the results of the network performance tests using colored grids and graphs.

The test pattern can be configured and run through the SLA Mon web interface controls the nature of the test calls.

Based on the Quality of Service (QoS) levels or thresholds that you configure for each traffic type, the SLA Mon server analyzes the test results for each source-destination

pair. Based on the analysis, the Network Monitoring feature presents the network performance information using colored grids and graphs.

For additional information on the features and implementation details, refer to the Best Practices guide: https://downloads.avaya.com/css/P8/documents/100181590

5. Softclients Log – Avaya Softlients Log Collector (ASLC) tool

We recommend our entitled end-users, to collect soft client product logs, utilizing the '***Avaya Softclients Log Collector*' *(ASLC)*** tool.

Our Entitled Clients and Partners should download this tool, using their respective FL #s.

Click on "**Diagnostics & Tools**", at our support site → search/scroll-down and click on "**Softclients Log Collector**".

Alternatively, click on:
https://secureservices.avaya.com/adp-softclients/menus/landingPage.xhtml

- Download the executable (.exe) file to your local hard-disk (hdd).
- Run the executable file to open the ASLC tool application

5.1 Prerequisites

To use the Avaya Softclients Log Collector tool, ensure that you have the following:

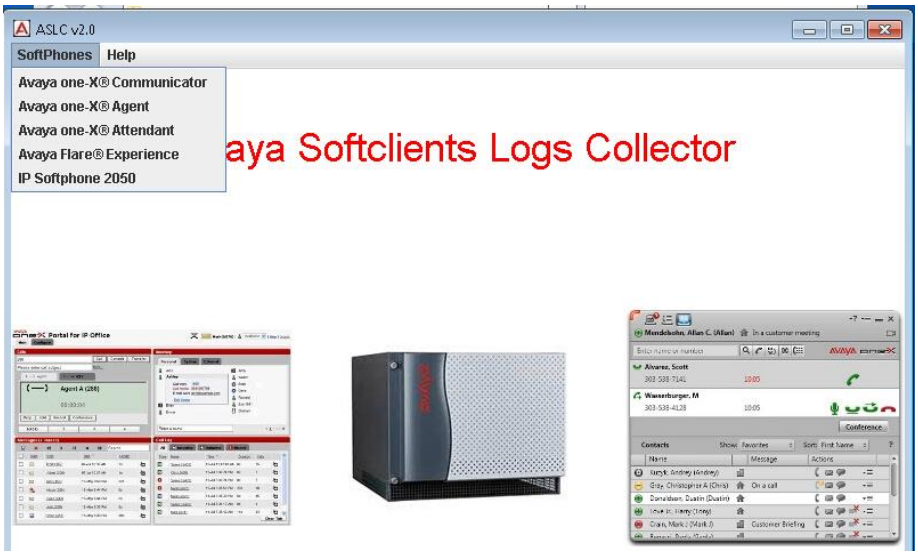
- ✓ Access to the Avaya Support site
- ✓ An Avaya single sign-on (SSO) account
- ✓ Access to the Product Licensing and Delivery System (PLDS) portal
- ✓ Java Runtime Environment (JRE) version 1.7.0_0 or higher

5.2 Supported soft-client models and their versions

Below is list of currently supported soft-clients and their respective versions, for the ASLC tool:

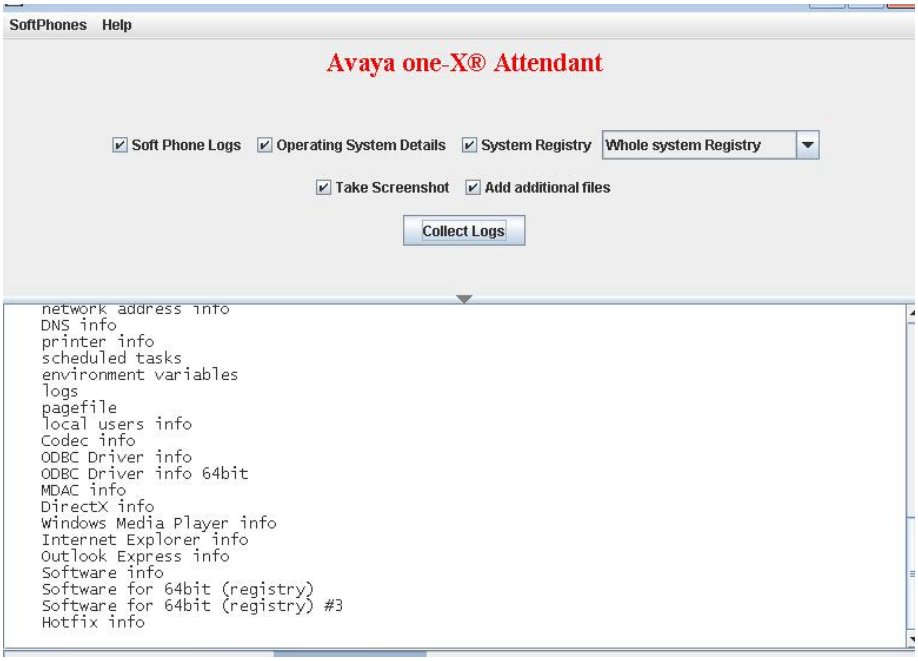
SUPPORTED PRODUCTS	SUPPORTED VERSIONS
One-X Communicator	6.0/6.1/6.2
One-X Agent	1.0/2.0/2.5
One-X Attendant	3.0+
Avaya Flare Experience	1.1
IP Softphone 2050	4.3+

5.3 User Interface of the ASLC tool



Choose the desired soft-client product, for log collection.

We shall take 'Avaya one-X® Attendant' product, as an example in this whitepaper.

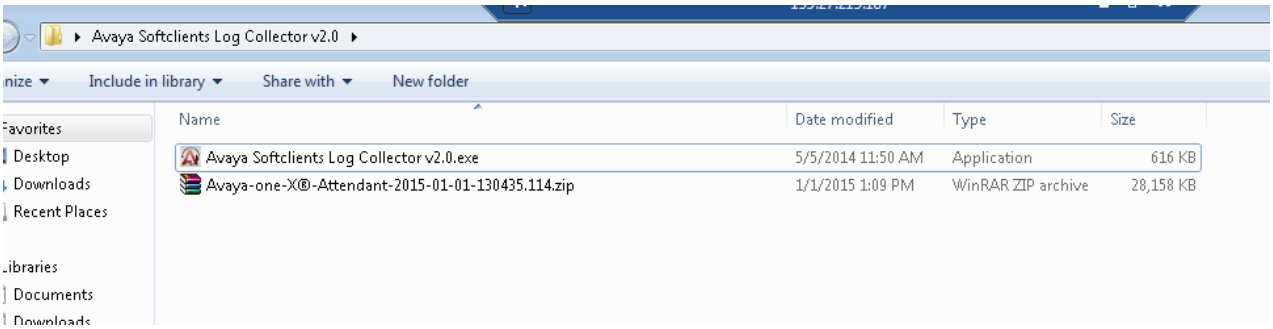


Choose the needed options and click on the "Collect Logs" button.

Best is to have all options enabled (as seen in the above capture), if unsure of what options are needed for a particular scenario.

Alternatively, contact Avaya Services for quick consultation, should support be needed on what logs to collect for a particular issue scenario.

ASLC software client will start to collect data and generate a ZIP file under the software folder:



The ASLC tool will collect the supported product-specific logs, in the following format:

Avaya-one-X®-Attendant*-2015-01-28-172630.282.zip*
Avaya-one-X®-Communicator*-2015-01-28-175400.987.zip*
Avaya-one-X®-Agent*-2015-01-28-172119.163.zip*
IP-Softphone-2050*-2015-01-28-173502.965.zip*

i.e., the product's name will be added, at the beginning of the collected zip-filename (followed by Year-Month-Date-Timestamp).

5.4 References for ASLC tool

- ✓ "Using Softclients Log Collector Tool": https://downloads.avaya.com/css/P8/documents/100178444
- ✓ KB #: ADMN111977