

The Avaya Server Availability Management Processor User Guide

for SAMP Commands
Addendum 1

03-300619
Issue 1
May 2005

Password protection

The SAMP's default configuration includes two logins - craft and rasaccess. Prior to loading Remote Feature Access' (RFAs) authentication file; these may be used by either Avaya Services or BusinessPartners. The remote access password is used when accessing the card via the modem to establish a PPP session. The SAMP uses a password strategy similar to Remote Supervisor Adapter's (RSAs) for the craft login. Unlike the S8500, the S8500B also utilizes a static password for rasaccess. This is because the S8500B uses a single modem that terminates into the SAMP, but the SAMP does not support Access Security Gateway (ASG.)

Upon installing the RFA authentication file, the S8500B's default static passwords are changed automatically for security reasons. Services personnel should be aware that the rasaccess password changes every time an authentication file is loaded. Since the process relies on the Automatic Registration Tool (ART) to manually train Avaya's connect tool when the rasaccess password has been changed, it is imperative that the technician rerun ART whenever a new authentication is loaded.

BusinessPartners must create an alternate system login. The recommended system login is dadmin, with a password of the BusinessPartner's choice. The BusinessPartner may choose to create a PPP login for themselves. They must be cautious about utilizing modem access, however, as doing so blocks product alarming and also blocks Avaya Services from remotely fixing problems. If the BusinessPartner forgets to create logins or loses their login/password, they will not be able to access the SAMP nor remotely access the S8500B. Upon request, the BusinessPartner's login/password can be reset for a fee by Avaya's Technical Consulting - System Support team (U.S.-based BusinessPartners at 1-800-225-7585) or Regional Service Centers (non-U.S.).

Host commands

Host commands are divided into two groups:

- those commands that affect the SAMP card itself
- other commands that affect alarms, environment, product ID, and so forth

All commands are entered from the host (the S8500B Media Server), not the SAMP.

CAUTION:
Be careful when changing passwords.

Remote maintenance board commands

CAUTION:

Do not change the craft or rasaccess passwords. If these are changed, a service call is necessary to reset the passwords.

Note:

You can use the **-?** option to display a command syntax for each command.

The remote maintenance board (RMB) commands

- *loadpwd* - loads the new authentication file onto the host server and the SAMP.
- *rmbuseradd* - adds modem and SAMP user logins on the SAMP (creates remote/local logins).
- *rmbusermod* - changes existing logins on the SAMP (modifies existing logins).
- *rmbuserdel* - deletes customer-created logins from the SAMP (craft and rasaccess cannot be deleted by this command). It also deletes existing logins on the SAMP.
- *rmbpasswd* - changes (modifies) customer-created passwords.

Adding logins

For additional information on using SAMP commands, see Using the SAMP commands on page 6.

Remote (modem) logins

To create a remote login for use over a modem:

1. On the host, type **rmbuseradd -P y *login*** and press **Enter** where ***login*** is the unique login name.
2. Type **rmbpasswd *login*** and press **Enter** where ***login*** is the unique login name.

   The system responds with `Enter password`.
3. Type the new password and press **Enter**.

   The system responds with `Re-enter the password`.
4. Type the new password again and press **Enter**.

Local logins (SAMP login)

To create a local login for use on the SAMP:

1. On the host, type **rmbuseradd *login*** and press **Enter** where ***login*** is the unique login name.
2. Type **rmbpasswd *login*** and press **Enter** where ***login*** is the unique login name.

   The system responds with `Enter password`.
3. Type the new password and press **Enter**.

   The system responds with `Re-enter the password`.
4. Type the new password and press **Enter**.

Changing a local login to a remote login

To change a local login to a remote login:

1. On the host, type **rmbusermod -P y *login*** and press **Enter** where ***login*** is the unique login name.

Changing a remote login to a local login

To change a remote login to a local login:

1. On the host, type **rmbusermod -P n *login*** and press **Enter** where ***login*** is the unique login name.

Removing a login from the SAMP

To remove a login from the SAMP:

1. On the host, type **rmbuserdel *login*** and press **Enter** where ***login*** is the unique login name.

Common options for commands

All commands used on the SAMP have options. These options include:

- [-u uid] - specifies a unique user ID (login ID). This option can be used on *rmbuseradd* or *rmbusermod* commands. If this option is not used, the system assigns the next available UID.
- [-o] - creates a user ID that is already in the system (for example, two users with the same UID). This option can be used on *rmbuseradd* or *rmbusermod* commands.

- [-d home] - this is the home directory for a particular login on the SAMP. The default is /home/***login*** where ***login*** is the unique user name. This option can be used on *rmbuseradd* or *rmbusermod* commands.
- [-s shell] - this is the login shell you want to use. This option can be used on *rmbuseradd* and *rmbusermod* commands. If this option is not used, the system default of /bin/sh is used.

  Note:

  The next option must be an encrypted password as returned by the crypt system call and should only be used by automated scripts. To manually add/change a password, use the *rmbpasswd* command.
- [-p passwd] - This option sets the login password to *passwd*. This option can be used on *rmbuseradd* and *rmbusermod* commands.
- [-P y/n] - specifies that the login is used for establishing a PPP session through the modem. This option can be used on *rmbuseradd* and *rmbusermod* commands. If this option is not used, the system assigns the default of n (non-modem access).

  For example, to add a login to the SAMP that lets you log in to the host through the modem on the SAMP, type **rmbuseradd -P *y login*** where ***login*** is the unique user name, ***y*** is connect through the modem, and press **Enter**.

Using the SAMP commands

loadpwd

This command changes the craft and rasaccess passwords on the SAMP. Normally this is accomplished during the installation by the Installation Wizard and by the periodic update tools. It does not affect the passwords or any other logins.

rmbuseradd

This command adds logins on the SAMP (creates remote/local logins on the SAMP).

To add user IDs on the SAMP:

1. Type **rmbuseradd *login*** where ***login*** is the unique user name and press Enter.

   The system adds the user name.

rmbusermod

This command changes user IDs on the SAMP (modifies existing logins on the SAMP).

To change user IDs on the SAMP:

1. Type **rmbusermod *options login*** where ***options*** is the login parameter you want to change and ***login*** is the unique user name and press **Enter**.

   The system changes the user ID.

rmbuserdel

This command deletes logins from the SAMP (and also restricts the user from deleting the craft and rasaccess logins).

To delete a user ID on the SAMP:

1. Type **rmbuserdel *login*** where ***login*** is the unique user name and press **Enter**.

   The system deletes the login. There is no confirmation notice.

rmbpasswd

This command changes the passwords (modifies the passwords).

To change the password:

1. Type **rmbpasswd *login*** where ***login*** is the user ID name and press **Enter**.

   The system responds with `Enter password`.

2. Type in the password and press **Enter**.

   The system responds with `Re-enter password`.

3. Type in the password again and press **Enter**.

   The password is changed.

SAMP commands

There are two categories of SAMP commands. Some are run from the host and some are run by logging into the SAMP. The ones that have the same names do similar things with similar syntax.

To get assistance on the host for a particular command:

Type **info *command*** and press **Enter** where ***command*** is one of the below listed commands

SAMP commands run on the host

These commands are run on the host. They affect both how the host is administered and also how the SAMP is administered (assuming the host can communicate with the SAMP).

- *almcall* - This command is used to display and set the dial-up numbers on the modem for placing alarms.
- *testinads* - This command is used to generate a test alarm and sends it to INADS so the phone number administration can be exercised.
- *testmodem* - This command is used to test the connection to the SAMP modem and for exercising the communication path to the modem.
- *almenable* - This command is used to turn alarms on and off.
- *almsuppress* - This command is used to disable alarms while the user is logged in.
- *almdisplay* - This command is used to display outstanding host alarms.
- *productid* - This command is used to set the product ID for INADS alarms.
- *environment* - This command is used to display the environment sensors such as temperature, fan speed, and voltage values.
- *date* - This command is used to display or change the clock. For more information on this option, type **`man date`**.
- *sampcmd* - This command is used to log into the SAMP or run a command on the SAMP. If this command is followed by a command on the host, it elicits a response from the SAMP. For example, **`sampcmd date`** and press **Enter** requests the time from the SAMP to display.
- *sampdiag* - This command is used to test the communication path to the SAMP and performs simple repairs on the 'host-server to samp' virtual connection.
- *sampupdate* - This command is used to update the firmware on the SAMP. This requires that only one SAMP firmware file is resident in the /var/home/ftp/pub directory. The SAMP firmware has an extension of .tbz. Before running sampupdate, use the command from the host: **`ls/var/home/ftp/pub/*.tbz`**.
- *inventory* - This command displays the manufacturing information on the SAMP and verifies the SAMP is connected and working correctly.

SAMP commands run on the SAMP

The below listed commands are run on the SAMP, itself. There are two ways to run them, both from the user login. First, you can type **sampcmd**. This will log you into a shell on the SAMP. Second, if you want to run a single command, enter **sampcmd *command***.

- /opt/alarming/bin/almcall
- /opt/alarming/bin/testinads
- /opt/alarming/bin/almenable
- /opt/alarming/bin/almsuppress
- /opt/alarming/bin/productid
- date

Troubleshooting

All communication between host and the SAMP are via an internal, dedicated LAN. Three major channels (ports) are used in that LAN for host to SAMP software communications. The SAMP forwards traffic on all other channels between its LAN or modem connections and the host. The three channels are for:

- ssh sessions (logging into the SAMP)
- HPI traffic (environment and control traffic)
- NTP (time updates)

The way to determine if the SAMP is working is to see if any of these channels is working. If any one is and another is not, then the problem is with the channel that is working. If none is working, then the problem is with the SAMP or the internal LAN.

sampdiag

The place to start is to test the internal LAN. As user “craft” in a command line shell, run the **`sampdiag -v`** command. If you see the following

```
chintan-8500: sampdiag -v
The SAMP is using the Avaya IP address.
SAMP HWaddress: 00:0F:29:00:01:5C
SAMP IPaddress: 192.11.13.2
HOST IPaddress: 192.11.13.1
SSH port: 10022
SSH OK
HPI OK

SAMP OK
```

then everything is configured correctly and working.

Should you see failures due to permission problems, then you can try to run this command as an administrator. However, set the execution path properly before doing so:

PATH=$PATH:/opt/ecs/rmb/samp

The **`sampdiag`** command tries to fix the internal LAN configuration. If there was a problem in how the host internal LAN was configured, then sampdiag may have fixed the problem. If sampdiag did change the IP addresses, HPI will have to be restarted. It restarts the next time the host reboots. It can be forced to restart by someone with administrator privileges. An administrator can run the **`killall bridgeip`** command. After a moment, the HPI process recreates itself and the HPI channel should be working. You can run **`sampdiag –v`** again and see if HPI is recognized.

There are several things to look for in the response from sampdiag.

- The HWaddress line tells you if a SAMP was detected where the host configuration says that it is (eth2 or eth4). If no HWaddress was detected, then either the ecs.conf file is incorrect or the SAMP is not working.
- If the IPaddresses are similar to 10.221.248.1 (or .2), then an administration step was skipped or failed when the host software was installed. You should be sure the SAMP software is up to date.
- This command will test HPI and ssh configuration for you. If both are failing, but the IP address is reported, than the host software is probably not set up correctly.
- If sampdiag cannot determine the IP address, then there could be a problem with the SAMP, itself.

The next sections are tests targeted at specific components in the SAMP communication path.

Detecting the SAMP card

As an administrator, run the **lspci** command. The result should look something like:

```
chintan-8500: lspci
00:00.0 Host bridge: Intel Corp.: Unknown device 2578 (rev 02)
00:03.0 PCI bridge: Intel Corp.: Unknown device 257b (rev 02)
00:1c.0 PCI bridge: Intel Corp.: Unknown device 25ae (rev 02)
00:1d.0 USB Controller: Intel Corp.: Unknown device 25a9 (rev 02)
00:1d.1 USB Controller: Intel Corp.: Unknown device 25aa (rev 02)
00:1d.4 System peripheral: Intel Corp.: Unknown device 25ab (rev 02)
00:1d.5 PIC: Intel Corp.: Unknown device 25ac (rev 02)
00:1d.7 USB Controller: Intel Corp.: Unknown device 25ad (rev 02)
00:1e.0 PCI bridge: Intel Corp. 82801BA/CA/DB PCI Bridge (rev 0a)
00:1f.0 ISA bridge: Intel Corp.: Unknown device 25a1 (rev 02)
00:1f.2 IDE interface: Intel Corp.: Unknown device 25a3 (rev 02)
00:1f.3 SMBus: Intel Corp.: Unknown device 25a4 (rev 02)
02:01.0 Ethernet controller: Intel Corp.: Unknown device 1075
03:01.0 Ethernet controller: Intel Corp. 82559ER (rev 10)
04:02.0 VGA compatible controller: ATI Technologies Inc Radeon VE QY
04:03.0 Ethernet controller: Intel Corp.: Unknown device 1076
```

Look for “03:01.0 Ethernet controller: Intel Corp. 82559ER (rev 10)”. The “03” indicates the PCI card that the SAMP is plugged into and the 82559 is the NIC on the host side of the internal bus. If that line is missing, replace the SAMP.

Testing the internal LAN

As craft login, run the **ifconfig eth2** command (without the dual NIC) or **ifconfig eth4** (with the dual NIC). The results should look something like:

```
eth2      Link encap:Ethernet  HWaddr 00:0F:29:00:01:5C
          inet addr:192.11.13.1  Bcast:192.11.13.3  Mask:255.255.255.252
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:86930 errors:0 dropped:0 overruns:0 frame:0
          TX packets:89315 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:10273485 (9.7 Mb)  TX bytes:15627789 (14.9 Mb)
          Interrupt:11 Base address:0x3000 Memory:d0220000-d0220038
```

The things to look for are:

- The inet addr should be 192.11.13.1. If it is 10.221.248.2, then the host was not configured properly when software was installed or the SAMP needs to be updated.
- Both RX packets and TX packets should be non-zero. If RX packets is 0, then the SAMP is not sending anything to the host. This is a strong indication that the SAMP should be replaced.

Testing the host LAN administration

This test is performed by the **sampdiag** command, but can be run independently. With the craft login, run the **ping my-samp** command. You should see

```
chintan-8500: ping my-samp
PING my-samp (192.11.13.2) from 192.11.13.1 : 56(84) bytes of data.
64 bytes from my-samp (192.11.13.2): icmp_seq=1 ttl=64 time=0.401 ms
64 bytes from my-samp (192.11.13.2): icmp_seq=2 ttl=64 time=0.290 ms
64 bytes from my-samp (192.11.13.2): icmp_seq=3 ttl=64 time=0.299 ms
```

If my-samp is not found, then /etc/hosts is not set up correctly (sampdiag should fix this problem). If you see `destination unreachable`, then the host NIC is not configured correctly (sampdiag should fix this problem, as well).

Testing the SAMP through ssh

As user “craft”, enter the **sampcmd** command from a command line. If the SAMP is working, the first time this is done, you will be asked to add a security key. Answer **yes**. After the SAMP and host exchange keys and if everything is working, you will see something like the following:

```
            .
           .M
         .MM       _ _
       .MM  M     | (_)
     .MM    M     | |_ _ __  _   ___  __
    MMM  MMMMMMM  | | | '_ \| | | \ \/ /
  MMM       M     | | | | | | |_| |>  <
 MMMM       M     |_|_|_| |_|\__,_/_/\_\


BusyBox v1.00-pre10 (2005.03.09-16:48+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

craft@STA04310083:~$
```

This is a Linux banner and prompt from the SAMP.

Enter **exit** to log out of the SAMP.

If you do not see the above, then test HPI.

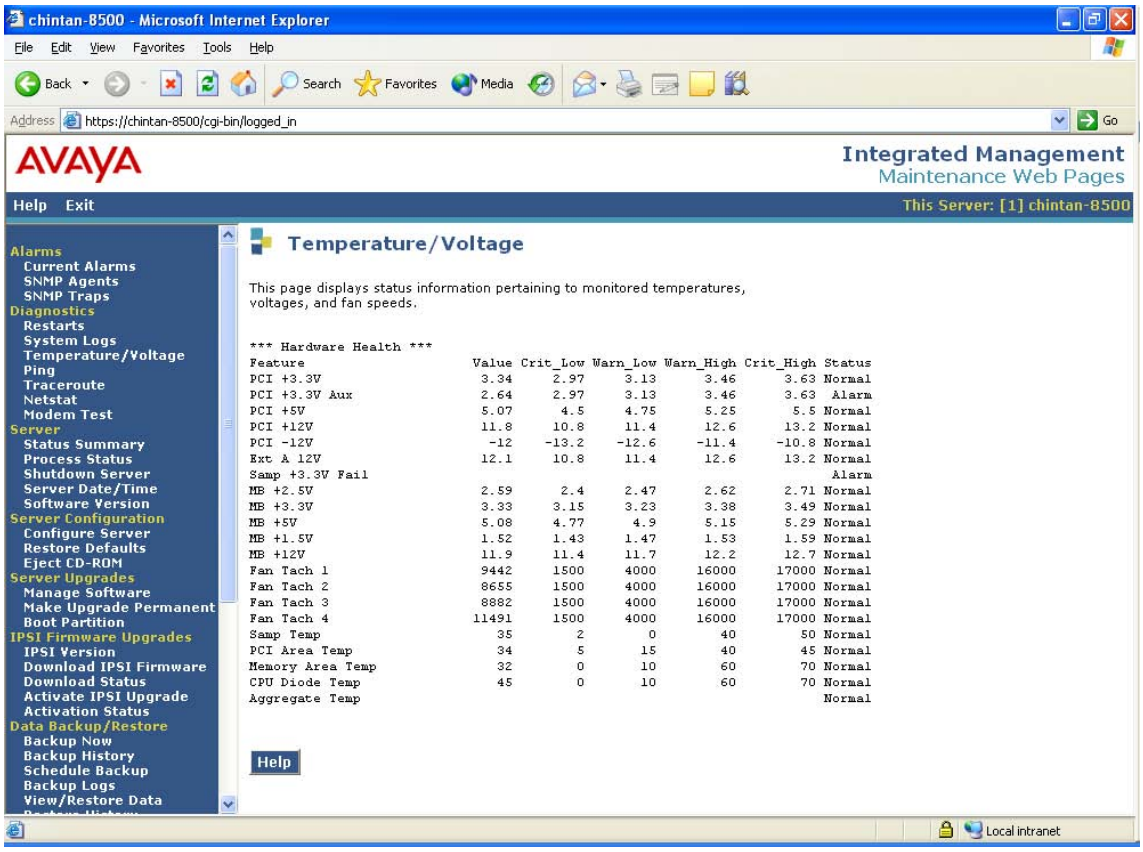
Testing HPI

There are several ways to test if the HPI (Hardware Platform Interface) is working, select the one most convenient for your situation:

- As user “craft”, from a command line, enter the **`inventory`** command. If everything is working, you will see something like

```
chintan-8500: inventory
2       Avaya S8500B    Chassis information     Asset Tag is    5000111222
2       Avaya S8500B    Board Information       Product is      Server Availabil
ity Management Card
2       Avaya S8500B    Board Information       Manufactured by Augmentix Corpor
ation
2       Avaya S8500B    Board Information       Product Version is      Avaya S8
500B
2       Avaya S8500B    Board Information       Manufactured on 2004-08-13T08:42
:29-06:00
2       Avaya S8500B    Board Information       Part Number is  10321 REV.B00
2       Avaya S8500B    Board Information       Serial Number is        STA04310
083
2       Avaya S8500B    Board Information       Product Version is      AVAYA_S8
500_1_0_SP1_BUILD_11
2       Avaya S8500B    Board Information       Product Version is      INP Firm
ware AVAYA1 1.18 Mar 2 2005
2       Avaya S8500B    Board Information       Custom is       MAC host 00:0F:2
9:00:01:5C
2       Avaya S8500B    Board Information       Custom is       MAC eth0 00:0F:2
9:00:01:5D
2       Avaya S8500B    Board Information       Custom is       MAC eth1 00:0F:2
9:00:01:5E
2       Avaya S8500B    Board Information       Custom is       MAC eth2 00:0F:2
9:00:01:5F
```

- From the Maintenance web pages, select **Temperature/Voltage**. If everything is working, you will see a page like:



- If you do not see anything like the above, log in with administrator privileges to a command line. Enter the **`/opt/desahpi/bin/hpisensors`** command. If everything is working, you should see something like:

```
chintan-8500: /opt/desahpi/bin/hpisensors
Opened Session to Domain 1

Resource 306  Avaya S8500B
Sens Num  EvtState         Reading                IdString
--------  --------  --------------------         --------
     1     0x0001                                 PCI Reset
     2     0x0000                3.344            PCI +3.3V
     3     0x0007                2.672            PCI +3.3V Aux
     4     0x0000                5.073            PCI +5V
     5     0x0000               11.776            PCI +12V
     6     0x0000              -11.992            PCI -12V
     7     0x0000               12.096            Ext A 12V
     9     0x0000                   35            Samp Temp
    10     0x0001                                 Samp +3.3V Fail
    50     0x0002                                 Server Power On
    51     0x0001                                 System Reset
   101     0x0000             2.59098             MB +2.5V
```

```
102     0x0000              3.33486             MB +3.3V
103     0x0000               5.0778             MB +5V
104     0x0000              1.52295             MB +1.5V
105     0x0000               11.875             MB +12V
106     0x0000                   34             PCI Area Temp
107     0x0000                   32             Memory Area Temp
108     0x0000                   45             CPU Diode Temp
110     0x0000                10306             Fan Tach 1
111     0x0000                 8655             Fan Tach 2
112     0x0000                 8767             Fan Tach 3
113     0x0000                 8941             Fan Tach 4
201     0x0000                    0             Alarm Total
202     0x0000                    0             Alarm Retries
203     0x0000                    0             Alarms Active
204     0x0000                                  Modem Status
258     0x0000                                  Aggregate Temp
257     0x0000                                  Aggregate Power
256     0x0000                                  Operational Status
```

- Finally, from a command line, run the **`ps –C bridgeip`** command. You should see a response like

```
chintan-8500: ps -C bridgeip
  PID TTY          TIME CMD
  317 ?        00:00:00 bridgeip
```

Testing NTP

The SAMP tries to get the date and time from the host once an hour. The date may off immediately after installation is complete, but should be synchronized after the next SAMP reboot or within the hour.

It is difficult to directly test that NTP is working. If the first test (testing ssh) worked, then as user “craft”, run the **`sampcmd date`** command. You should see something like

```
chintan-8500: sampcmd date
Fri Apr  8 08:19:34 MDT 2005
```

Where the response is the same time and date as the host. If this is not working, then NTP is not set up correctly on the host.

Rebooting the SAMP

To reboot the SAMP as craft login, perform the following step:

- Type **`sampcmd sudo reboot`** and press **Enter**.

  The SAMP then reboots and is unavailable for about a minute.