



Avaya Solution & Interoperability Test Lab

Application Notes for Eastcom Systems Comprehensive Alarm Monitoring System with Avaya Communication Manager - Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Eastcom Systems Comprehensive Alarm Monitoring System (CAMS) to interoperate with Avaya Communication Manager.

Eastcom CAMS is designed to provide comprehensive centralized alarm monitoring within the most complex and mission-critical automation environments. With outstanding features such as built-in workflow escalation alerts, CAMS can be configured to send primary and secondary alarm notifications via SMS or email to an administrator for immediate acknowledgement.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

The objective of this interoperability compliance testing was to verify that Eastcom Systems Comprehensive Alarm Monitoring System (CAMS) can interoperate with Avaya Communication Manager 5.1.

Eastcom CAMS uses Avaya Site Administration to poll Avaya Communication Manager systems for active alarms. The alarms are then filtered based on severity and type, and notifications are sent to registered users via short message service (SMS).

Figure 1 illustrates the network configuration used to verify the Eastcom CAMS solution. Site A is comprised of an Avaya S8500 Server running Avaya Communication Manager, and has connections to the following: Avaya 9630 IP Telephones, Avaya 2400 Series Digital Telephones, and an ISDN-BRI trunk to the PSTN. Eastcom CAMS is installed on a server running Microsoft Windows Server 2003 with Service Pack 2. Site B is comprised of an Avaya S8300 Server with Avaya G350 Media Gateway, and has connections to Avaya 4621SW IP Telephones. The Avaya C364T-PWR Converged Stackable Switch provides Ethernet connectivity to the servers and IP telephones and Layer 3 IP routing between the two sites. An H.323 IP trunk is configured between Site A and B for the users to call between the two sites.

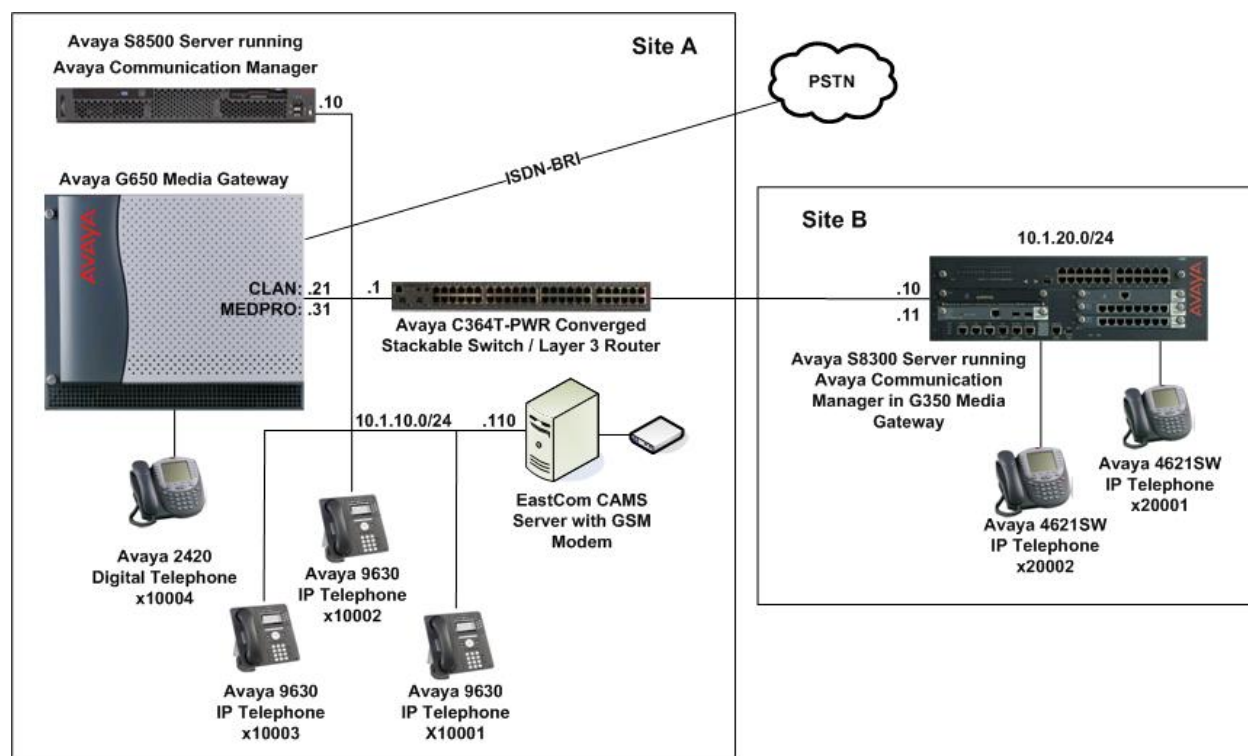


Figure 1: Test configuration

2. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment	Software
Avaya S8500 Server	Avaya Communication Manager 5.1 (Service Pack 01.0.414.3-15962)
Avaya G650 Media Gateway <ul style="list-style-type: none">- TN2312BP IP Server Interface- TN799DP C-LAN Interface- TN2302AP IP Media Processor- TN2214CP Digital Line- TN2793B Analog Line	- HW07, FW044 HW01, FW026 HW20, FW117 HW08, FW015 000013
Avaya S8300 Server	Avaya Communication Manager 5.1 (Service Pack 01.0.414.3-15962)
Avaya G350 Media Gateway	28.17.0
Avaya 4600 Series IP Telephones - 4621SW	2.8.8.7 (H.323)
Avaya 9600 Series IP Telephones - 9630	1.5 (H.323)
Avaya 2400 Series Digital Telephone	-
Avaya C364T-PWR Converged Stackable Switch	4.5.18
Avaya Site Administration	5.0.11 SP2.01
Eastcom CAMS	3.0

3. Configure Avaya Communication Manager

This section describes the steps needed to configure Avaya Communication Manager to interoperate with Eastcom CAMS. This section describes the steps to create a login account and a SAT User Profile for CAMS to access Avaya Communication Manager to retrieve the alarms. The steps are repeated for each Avaya Communication Manager system.


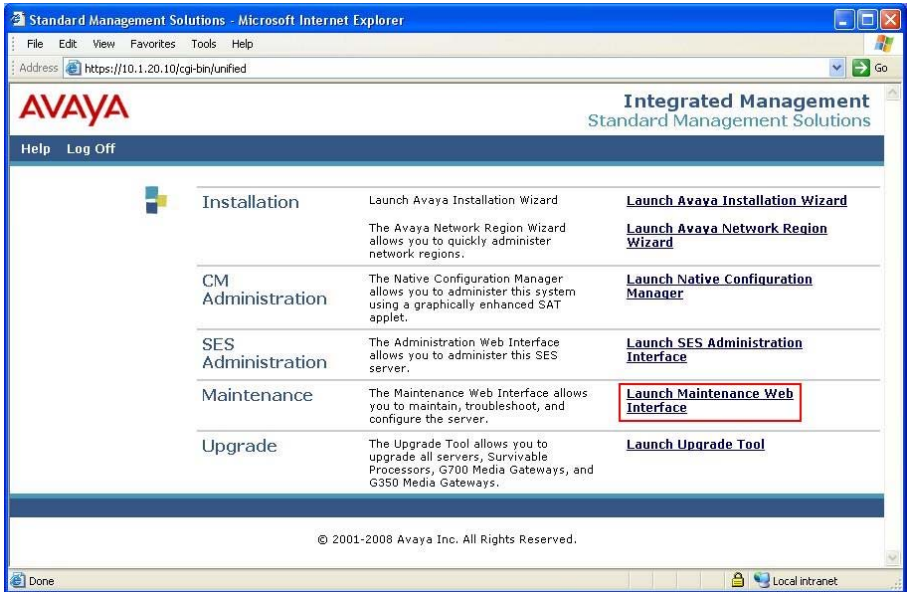
3.1. Configure SAT User Profile

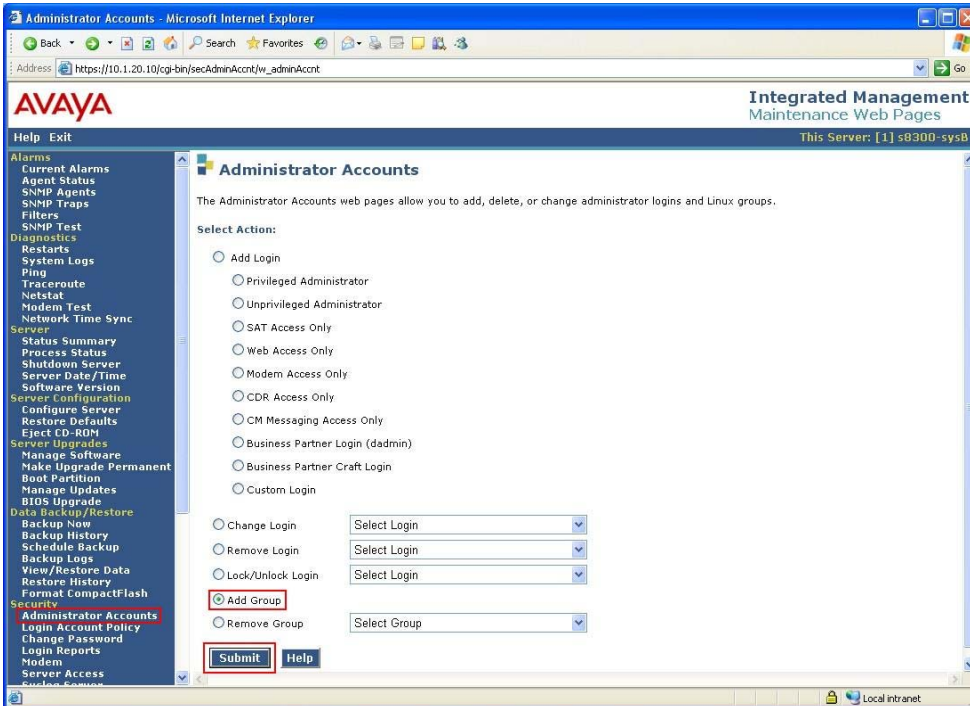
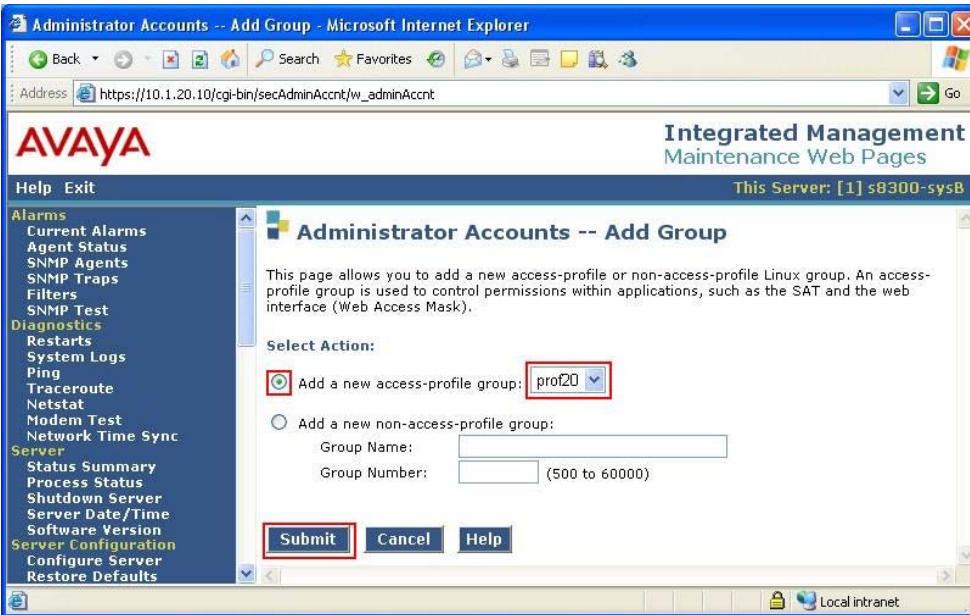
A SAT User Profile specifies which SAT screens may be accessed by the user assigned the profile and the type of access to each screen. As Eastcom CAMS does not modify any system configuration, create a SAT User Profile with limited permissions to assign to the CAMS login account.

Step	Description
1.	<p>Enter the add user-profile <i>n</i> command, where <i>n</i> is the next unused profile number. Enter a descriptive name for User Profile Name and enable Category H by setting the Enbl field to y. In this configuration, the user profile 20 is created.</p> <pre> add user-profile 20 USER PROFILE 20 Page 1 of 41 User Profile Name: CAMS This Profile is Disabled? n Shell Access? n Facility Test Call Notification? n Acknowledgement Required? n Grant Un-owned Permissions? n Extended Profile? n Name Cat Enbl Name Cat Enbl Adjuncts A n Routing and Dial Plan J n Call Center B n Security K n Features C n Servers L n Hardware D n Stations M n Hospitality E n System Parameters N n IP F n Translations O n Maintenance G n Trunking P n Measurements and Performance H y Usage Q n Remote Access I n User Access R n </pre>
2.	<p>To further restrict the permissions assigned to the CAMS login account, set the permissions of all objects in Category H to '--' (i.e. no permission) except for the alarms object, which is assigned the permission 'r-'. Submit the form to create the user profile.</p> <pre> add user-profile 20 USER PROFILE 20 Page 3 of 41 Set Permissions For Category: H To: -- Set All Permissions To: '-'=no access 'r'=list,display,status 'w'=add,change,remove+r 'm'=maintenance Name Cat Perm aesvcs link A -- aesvcs-server A -- agent B -- agent-loginID B -- alarms H r- alias station M -- alphanumeric-dial-table J -- alternate-fri C -- amw all G -- amw asai G -- amw audix G -- amw pms G -- analog-testcall board G -- </pre>

3.2. Configure Login Group

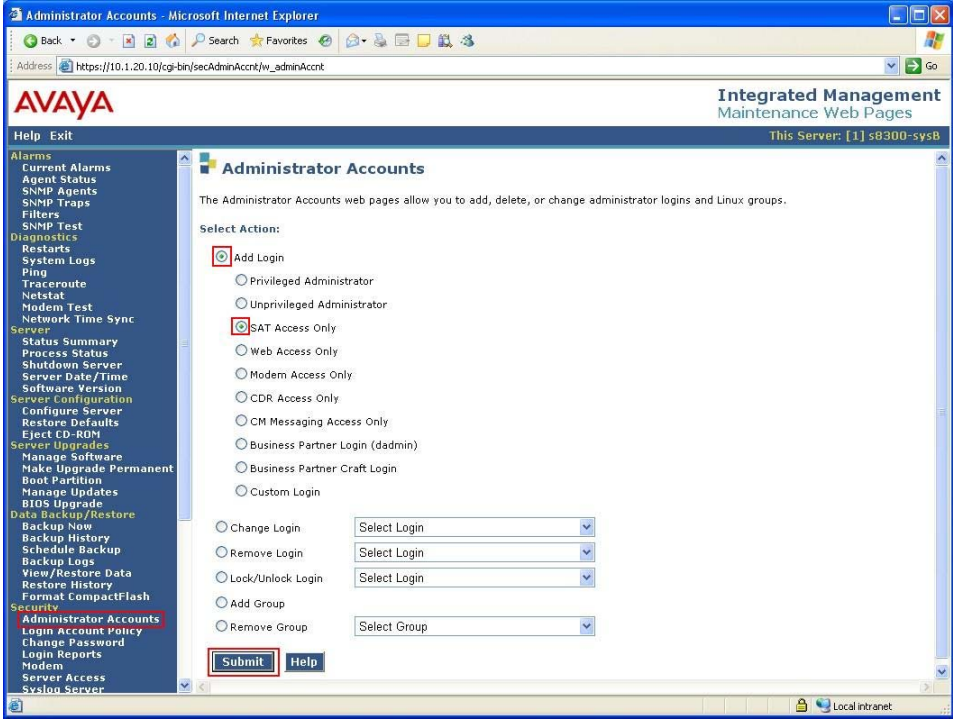
Create a Login Group to correspond to the SAT User Profile created in **Section 3.1**.

Step	Description
1.	<p>Using a web browser, enter https://<IP address of Avaya Server> to connect to the Avaya Server being configured and log in using appropriate credentials.</p> 
2.	<p>Click Launch Maintenance Web Interface. This will open up the Maintenance Web Pages in a new window that will allow the user to complete the configuration process.</p> 

Step	Description
3.	<p>From the navigation panel on the left side, click Administrator Accounts. Select Add Group and click Submit.</p> 
4.	<p>Select Add a new access-profile group and select prof20 from the drop-down box to match the user-profile created in Section 3.1 Step 1. Click Submit. This completes the creation of the login group.</p> 

3.3. Configure Login

Create a login account for Eastcom CAMS to access the SAT.

Step	Description
1.	<p>From the navigation panel on the left side, click Administrator Accounts. Select Add Login and SAT Access Only and click Submit.</p> 

Step	Description
2.	<p>On the Administrator Accounts -- Add Login: SAT Access Only page, configure the login as follows:</p> <ul style="list-style-type: none"> • Login name: Specify the login name to create. In this configuration, the login cams was created. • Primary group: users [Limits the permissions of the login] • Additional groups (profile): prof20 [Select the login group created in Section 3.2.] • Select type of authentication: Password [Uses a password for authentication.] • Enter password or key / Re-enter password or key [Define the password] <p>Click Submit to continue. This completes the configuration of the login.</p>

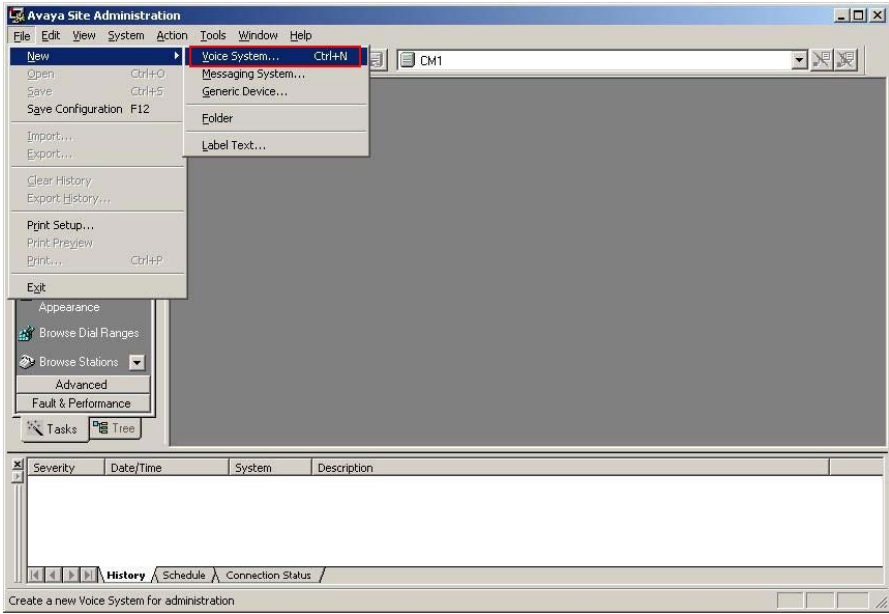

The screenshot shows the Avaya Integrated Management Maintenance Web Pages interface. The browser window title is "Administrator Accounts -- Add Login: SAT Access Only - Microsoft Internet Explorer". The address bar shows "https://10.1.20.10/cgi-bin/secAdminAcct/jw_adminAcct". The page header includes the Avaya logo and "Integrated Management Maintenance Web Pages". The sidebar on the left contains a list of navigation links under categories like Alarms, Diagnostics, Server, Server Configuration, Server Upgrades, Data Backup/Restore, Security, and Media Gateways. The main content area is titled "Administrator Accounts -- Add Login: SAT Access Only" and contains the following fields and options:

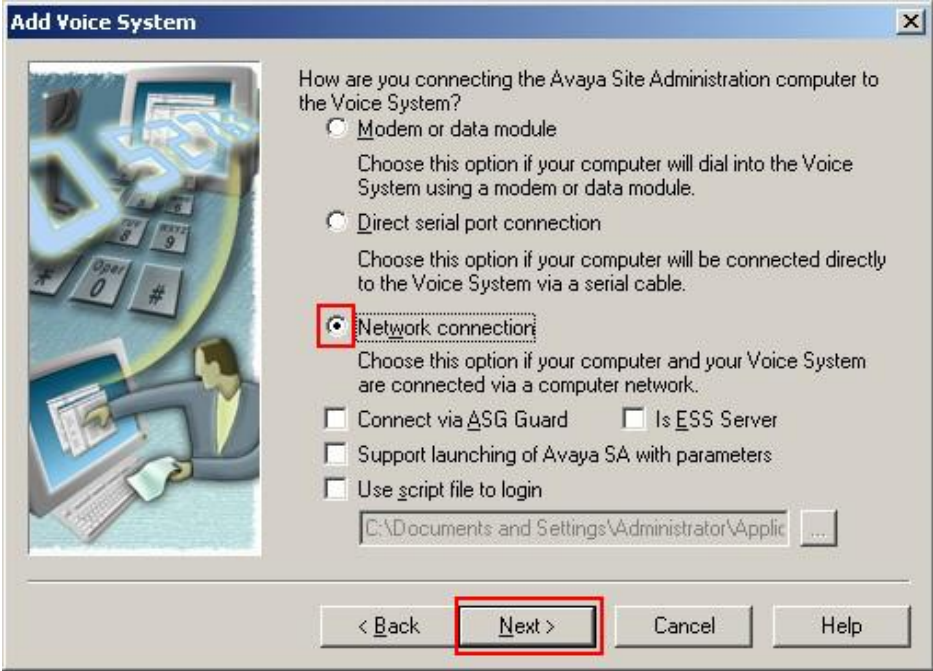
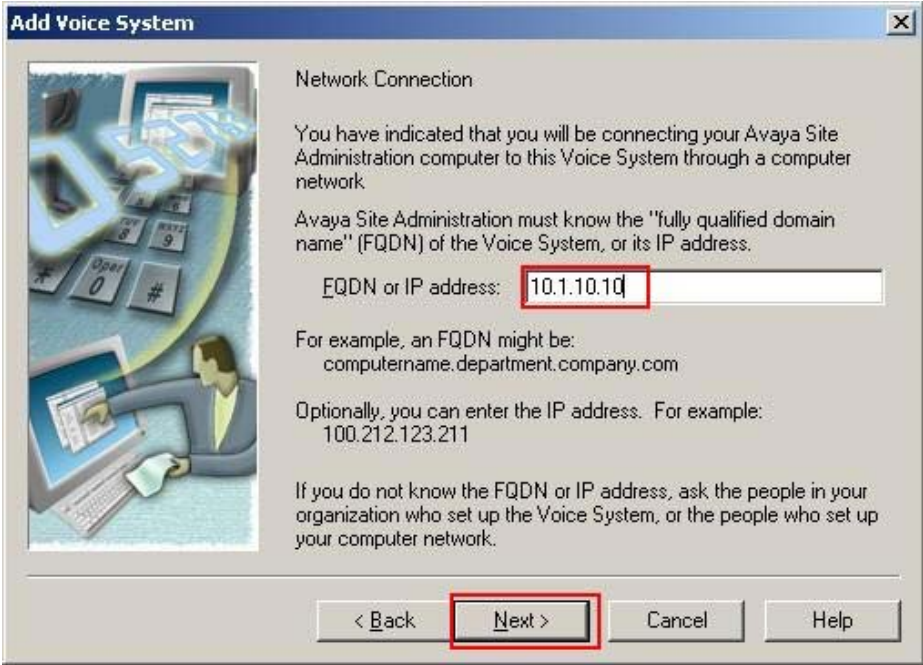
- Login name:**
- Primary group:** ☒ users
- Additional groups (profile):**
- Linux shell:**
- Home directory:**
- Lock this account:** ☐
- Date after which account is disabled-blank to ignore (YYYY-MM-DD):**
- Select type of authentication:** ☒ Password, ☐ ASG: enter key, ☐ ASG: Auto-generate key
- Enter password or key:**
- Re-enter password or key:**
- Force password/key change on next login:** ☐ Yes, ☒ No

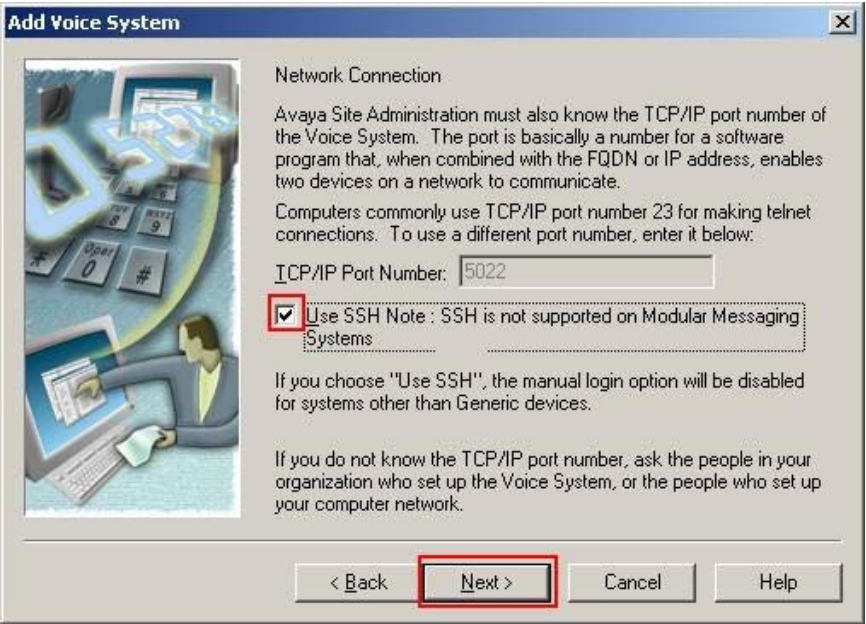
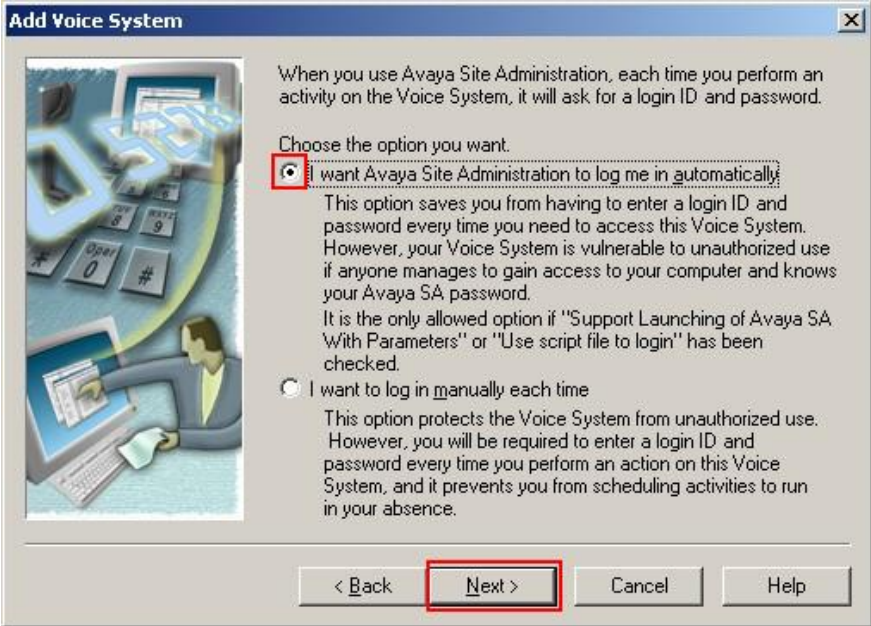
At the bottom of the form are three buttons: **Submit**, **Cancel**, and **Help**. The **Submit** button is highlighted with a red box. There are also two warning icons on the right side of the form.


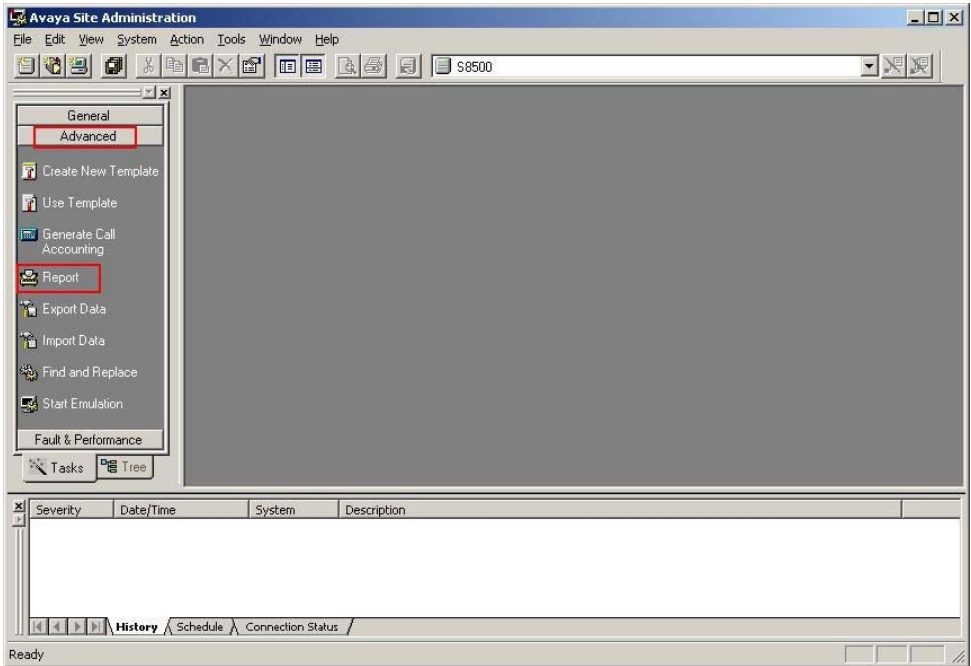
4. Configure Avaya Site Administration

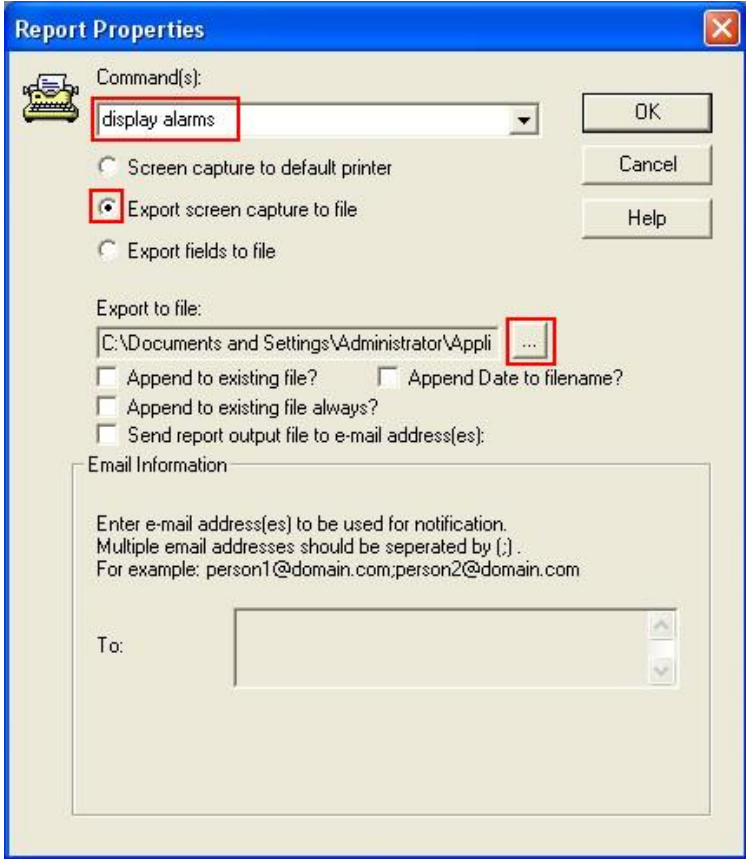
This section describes the steps needed to configure Avaya Site Administration to poll the alarms from the Avaya Communication Manager systems.

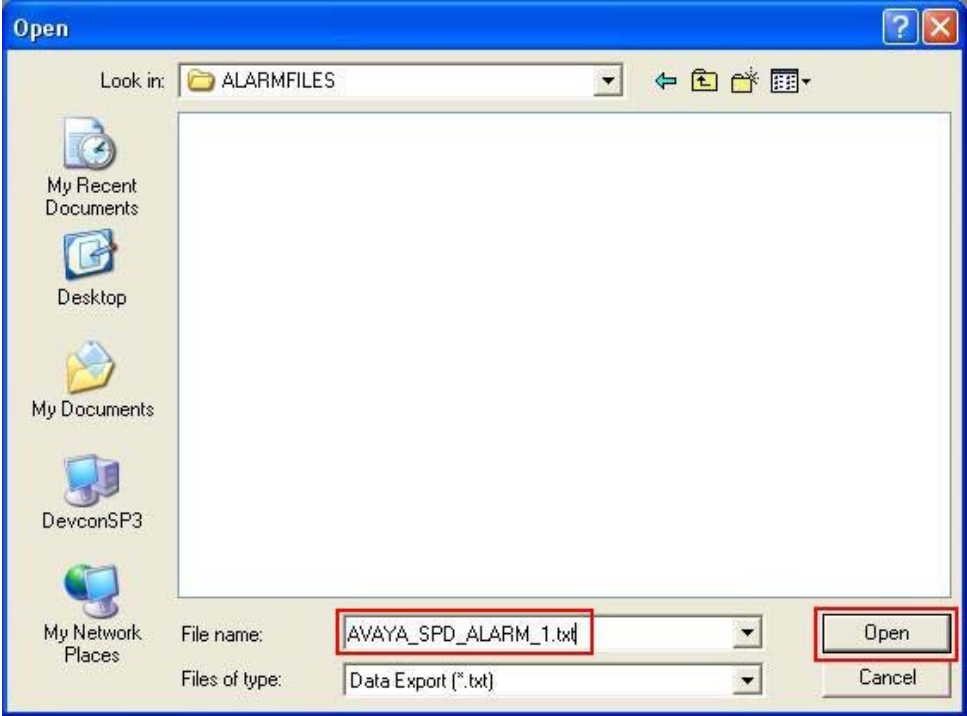
Step	Description
1.	<p>Start Avaya Site Administration by clicking on Start > All Programs > Avaya > Site Administration. From the menu, click File > New > Voice System to start the Add Voice System Wizard configure a new Avaya Communication Manager system.</p> 
2.	<p>Specify a name in the Voice System Name field and click Next.</p> 

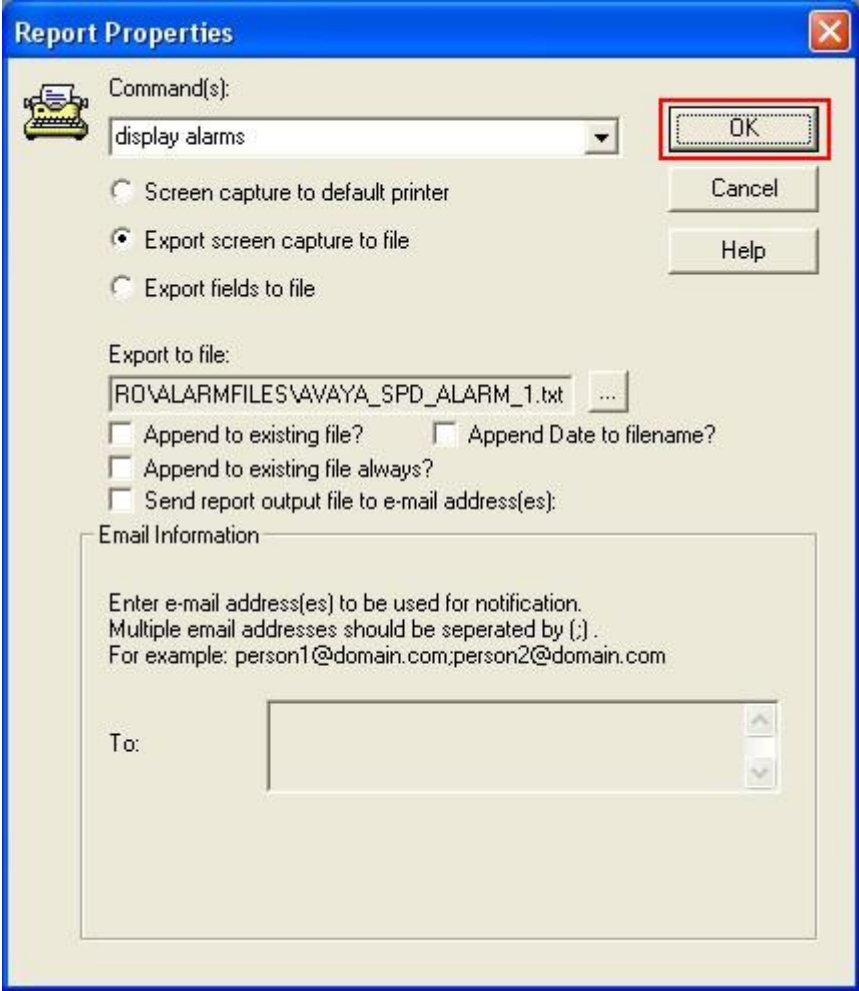
Step	Description
3.	<p>Select Network Connection and click Next.</p>  <p>The screenshot shows the 'Add Voice System' dialog box. On the left is an illustration of a person at a computer. The main text asks 'How are you connecting the Avaya Site Administration computer to the Voice System?'. There are three radio button options: 'Modem or data module', 'Direct serial port connection', and 'Network connection'. The 'Network connection' option is selected and highlighted with a red box. Below it are several checkboxes: 'Connect via ASG Guard', 'Is ESS Server', 'Support launching of Avaya SA with parameters', and 'Use script file to login'. At the bottom, there is a text field with a file path and a 'Next >' button which is highlighted with a red box. Other buttons include '< Back', 'Cancel', and 'Help'.</p>
4.	<p>Enter the IP address of the first Avaya Server for the field FQDN or IP address and click Next.</p>  <p>The screenshot shows the 'Add Voice System' dialog box, specifically the 'Network Connection' screen. On the left is the same illustration as before. The main text states: 'You have indicated that you will be connecting your Avaya Site Administration computer to this Voice System through a computer network. Avaya Site Administration must know the "fully qualified domain name" (FQDN) of the Voice System, or its IP address.' Below this is a text field labeled 'FQDN or IP address:' which contains the value '10.1.10.10' and is highlighted with a red box. Further text provides examples for FQDN and IP address. At the bottom, the 'Next >' button is highlighted with a red box. Other buttons include '< Back', 'Cancel', and 'Help'.</p>

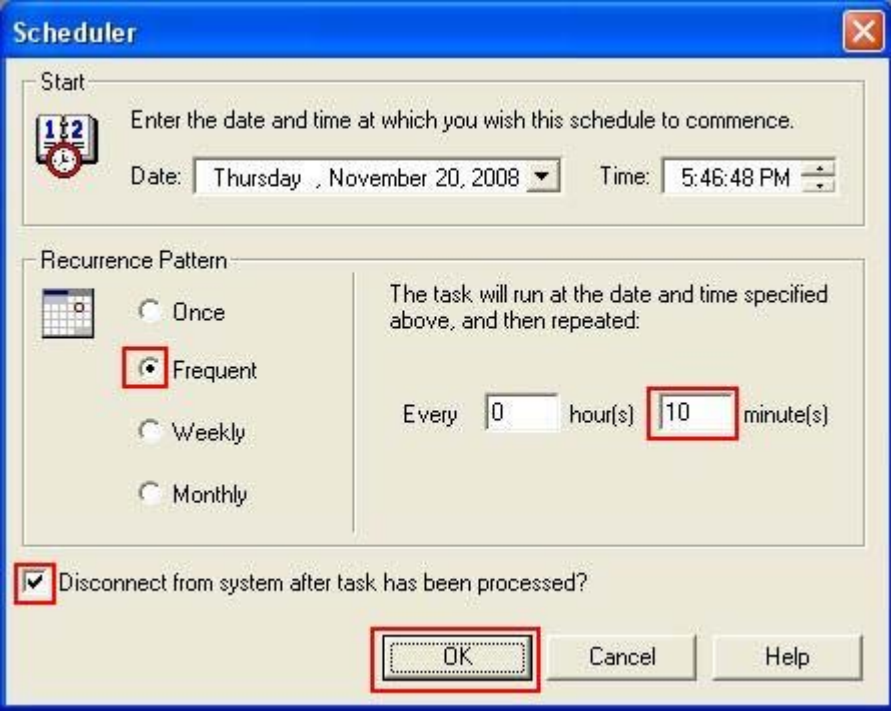
Step	Description
5.	<p>Check Use SSH and click Next. SSH is enabled by default on the Avaya Server. Click Next on the next screen (not shown) to accept the default values.</p>  <p>Add Voice System</p> <p>Network Connection</p> <p>Avaya Site Administration must also know the TCP/IP port number of the Voice System. The port is basically a number for a software program that, when combined with the FQDN or IP address, enables two devices on a network to communicate.</p> <p>Computers commonly use TCP/IP port number 23 for making telnet connections. To use a different port number, enter it below:</p> <p>TCP/IP Port Number: 5022</p> <p><input checked="" type="checkbox"/> Use SSH Note : SSH is not supported on Modular Messaging Systems</p> <p>If you choose "Use SSH", the manual login option will be disabled for systems other than Generic devices.</p> <p>If you do not know the TCP/IP port number, ask the people in your organization who set up the Voice System, or the people who set up your computer network.</p> <p>< Back Next > Cancel Help</p>
6.	<p>Select I want Avaya Site Administration to log me in automatically and click Next. This is required so that the display alarms reports can be scheduled to run at periodic intervals.</p>  <p>Add Voice System</p> <p>When you use Avaya Site Administration, each time you perform an activity on the Voice System, it will ask for a login ID and password.</p> <p>Choose the option you want.</p> <p><input checked="" type="radio"/> I want Avaya Site Administration to log me in automatically</p> <p>This option saves you from having to enter a login ID and password every time you need to access this Voice System. However, your Voice System is vulnerable to unauthorized use if anyone manages to gain access to your computer and knows your Avaya SA password.</p> <p>It is the only allowed option if "Support Launching of Avaya SA With Parameters" or "Use script file to login" has been checked.</p> <p><input type="radio"/> I want to log in manually each time</p> <p>This option protects the Voice System from unauthorized use. However, you will be required to enter a login ID and password every time you perform an action on this Voice System, and it prevents you from scheduling activities to run in your absence.</p> <p>< Back Next > Cancel Help</p>

Step	Description
7.	<p>Select Password for Authentication Methods and enter the login created for Eastcom CAMS in Section 3.3 for the fields Login, Password and Password (again). Click Next. On the next screen (not shown), click Next and then click Finish on the summary screen (not shown) to complete the wizard.</p> 
8.	<p>From the left panel, click Advanced > Report to create the display alarms report.</p> 

Step	Description
9.	<p>Enter display alarms for Command(s) and select Export screen capture to file. For the field Export to file, click ‘...’ to input the filename.</p> 

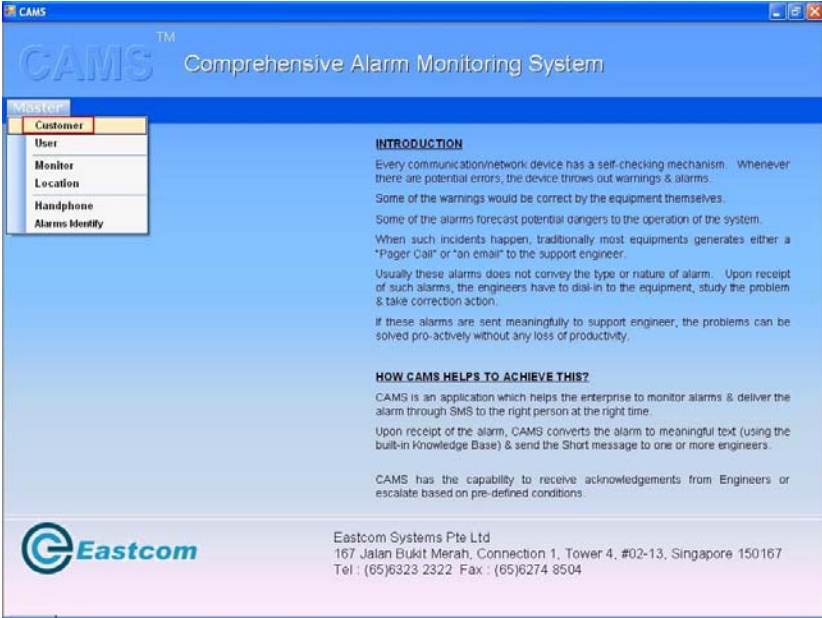
Step	Description
10.	<p>In the Open screen, browse to the folder D:\EASTCOM\CAMSPRO\ALARMFILES\ and enter the File name in the format <Customer ID>_<Location ID>_<Monitor ID>_<Alarm Ref#>.txt. See Section 5 for the configuration of the fields in Eastcom CAMS. The alarm file will be polled at periodic intervals by Eastcom CAMS. Click Open.</p> 



Step	Description
11.	<p>At the Report Properties screen, click OK.</p>  <p>The screenshot shows the 'Report Properties' dialog box. The 'Command(s):' field is set to 'display alarms'. The 'OK' button is highlighted with a red rectangle. The 'Export screen capture to file' radio button is selected. The 'Export to file' section shows a file path 'RO\ALARMFILES\AVAYA_SPD_ALARM_1.txt'. The 'Email Information' section is also visible.</p>

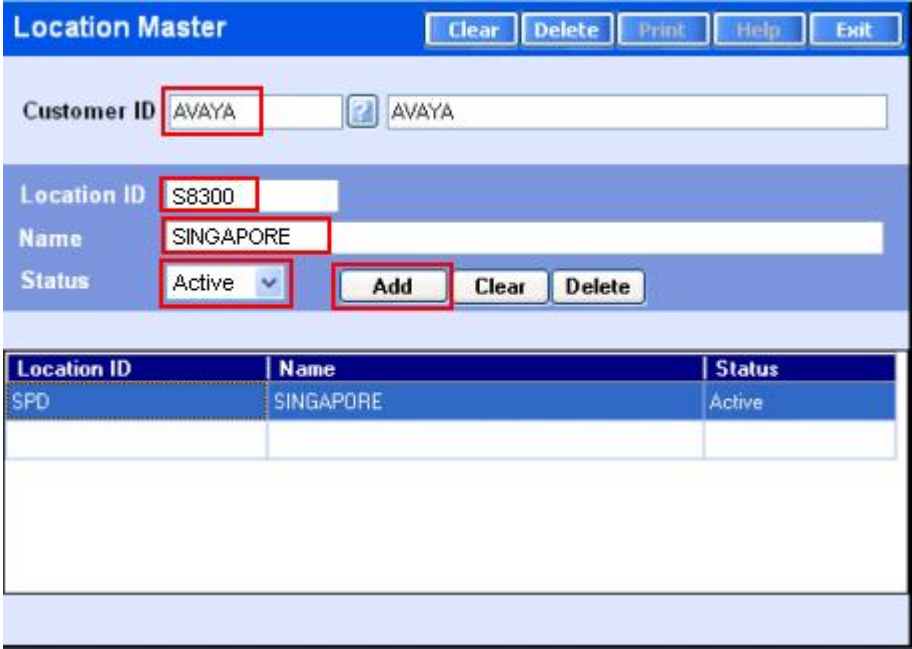
Step	Description
12.	<p>At the Scheduler screen, check Frequent for Recurrence Pattern and set the report to run every 10 minutes. Check Disconnect from system after task has been processed so that Avaya Site Administration will not permanently use up a SAT session. Click OK. Leave Avaya Site Administration running so that the reports will be run at the scheduled intervals.</p> 
13.	<p>Repeat Step 1 to Step 12 to configure Avaya Site Administration for the second system at Site B. This completes the creation of the display alarms report.</p>

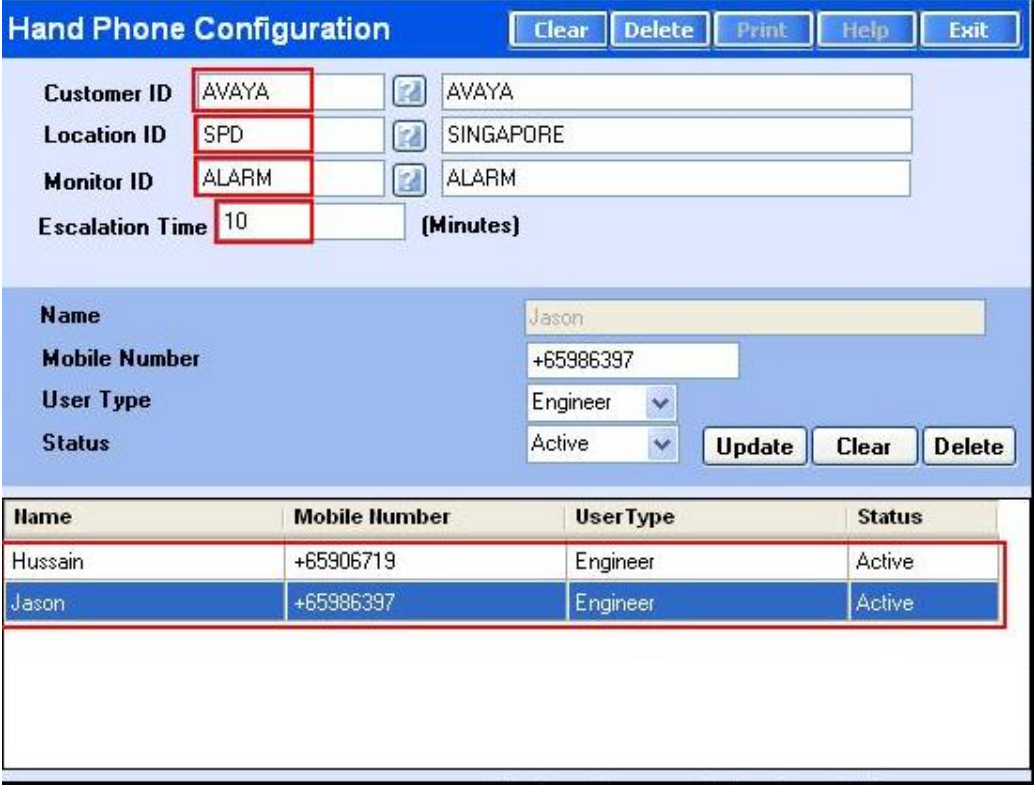
5. Configure Eastcom CAMS

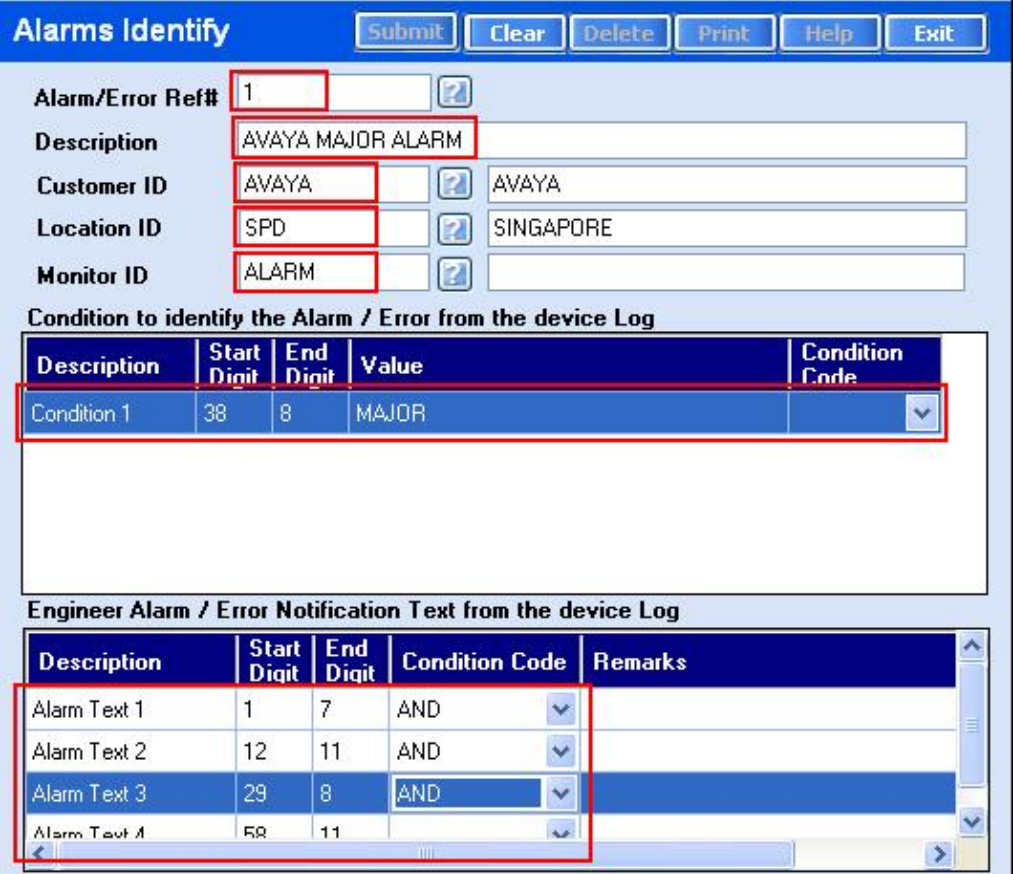
This section describes the configuration of Eastcom CAMS.

Step	Description
1.	<p>From the Eastcom CAMS server, click Start > All Programs > Eastcom > CAMS Manager (or click on the CAMS icon on the desktop) to launch the CAMS application and log in using a user ID with administrative privileges. From the CAMS window, click Master > Customer.</p> 

Step	Description
2.	<p>Enter the customer information in the fields provided. The following fields need to match the configuration for Avaya Site Administration in Section 4 Step 10.</p> <ul style="list-style-type: none"> • Customer Id • Alarm File Folder <p>Click Submit.</p> 
3.	<p>From the CAMS window, click Master > Monitor (not shown) to create a new monitor configuration. Specify a value for Monitor ID and Monitor Name. The field Monitor ID needs to match the configuration for Avaya Site Administration in Section 4 Step 10.</p> 

Step	Description
4.	<p>From the CAMS window, click Master > Location (not shown). Enter the Customer ID created in Step 2. Specify the Location ID and Name. Select Active for Status and click Add. The field Location ID needs to match the configuration for Avaya Site Administration in Section 4 Step 10. In this configuration, the Location IDs for the systems in Site A and Site B are SPD and S8300 respectively.</p> 

Step	Description
5.	<p>From the CAMS window, click Master > Handphone (not shown). Enter the following information:</p> <ul style="list-style-type: none"> • Customer ID: Set to the value defined in Step 2. • Location ID: Set to the value defined in Step 4. • Monitor ID: Set to the value defined in Step 3. • Escalation Time: The purpose of this field is to monitor the receipt of the alarm files to be received from the Avaya Site Administration. This should either match the value administered in Section 4 Step 12 or set to 5 or 10 minutes later than the file creation time set in the Avaya Site Administration. In the event that the alarm file is not received from the Avaya Site Administration, the CAMS system will automatically generate and send an SMS to notify the administrator. <p>Define the users that will receive the alarm notifications using the fields Name, Mobile Number, User Type and Status. In this configuration, the alarm notifications will be sent to two users for the system at Site A.</p> 

Step	Description
6.	<p>From the CAMS window, click Master > Alarms Identify (not shown). On this screen, the types of alarm (MAJOR, MINOR, WARNING) and the text to be sent out are defined. Enter the following information:</p> <ul style="list-style-type: none"> • Alarm/Error Ref#: Specify an alarm reference. This field needs to match the configuration for Avaya Site Administration in Section 4 Step 10. • Description: Provide a description for this alarm. • Customer ID: Set to the value defined in Step 2. • Location ID: Set to the value defined in Step 4. • Monitor ID: Set to the value defined in Step 3. <p>The sections that follow are customized by Eastcom engineers for each customer installation and will not be discussed in detail. In this configuration, any major alarms for the system in Site A will trigger an SMS notification to the engineers defined in Step 5. Multiple alarm types can also be specified through this screen.</p> 

6. Interoperability Compliance Testing

The interoperability compliance testing included feature and serviceability testing. The feature testing evaluated the ability of Eastcom CAMS to process the alarm reports retrieved by Avaya Site Administration and send out the alarms to the assigned users. The serviceability test introduced failure scenarios to see if Eastcom CAMS can resume operation after failure recovery.

6.1. General Test Approach

The general test approach was to manually cause various types of alarms to occur on the Avaya Communication Manager systems, and verify that Eastcom CAMS sends out the alarms accurately to the assigned users. For serviceability testing, the network connection on the Eastcom CAMS server was disconnected, and the Avaya S8500 servers and Eastcom CAMS server were also rebooted.

6.2. Test Results

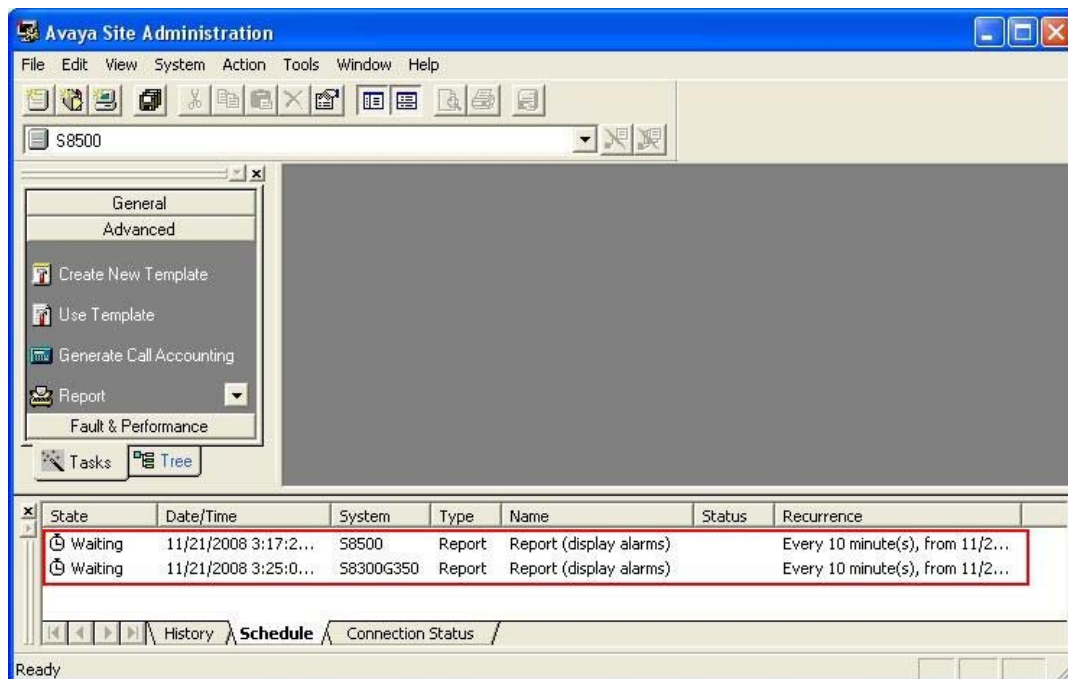
All feature and serviceability tests passed.

7. Verification Steps

The following steps may be used to verify the configuration:

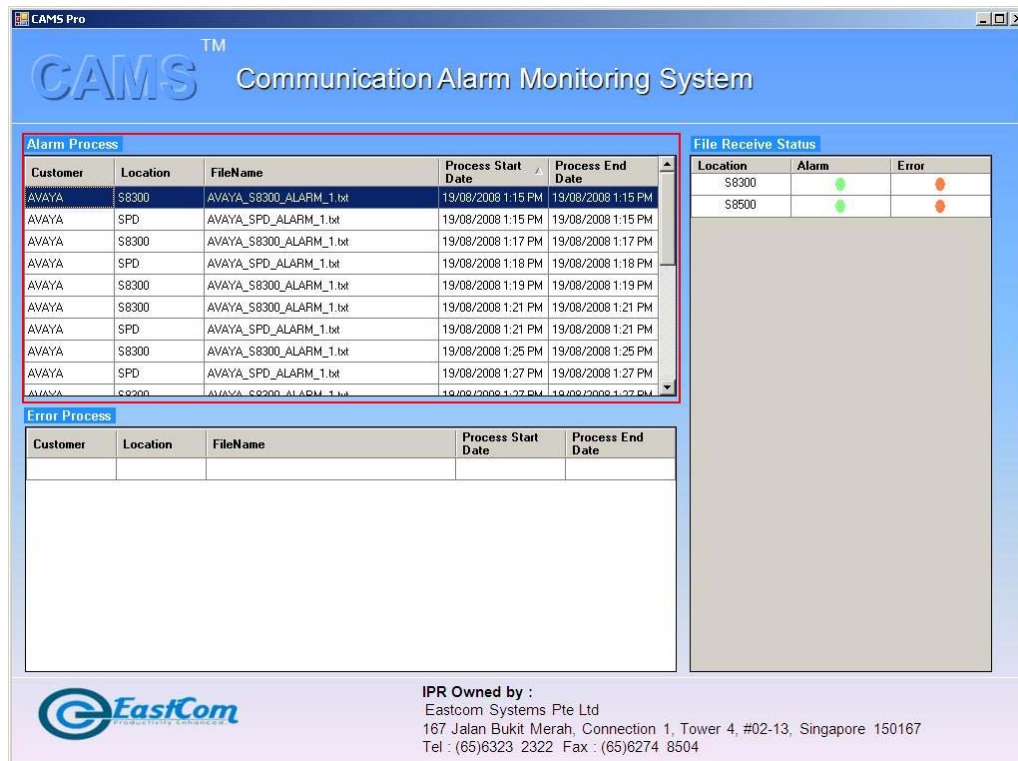
7.1. Verify Avaya Site Administration

In the **Schedule** tab at the bottom of the window, verify that the **display alarms** report is scheduled to run at the required interval.



7.2. Verify Eastcom CAMS

In the CAMS window, verify that the alarm reports from Avaya Site Administration are being processed. Verify that the assigned users received the alarm notifications on their mobile phones as SMS when there are alarms on the Avaya Communication Manager systems.



8. Support

Technical support for Eastcom CAMS can be obtained by contacting Eastcom's Support Desk at +65 63232822, or sending an e-mail to support@eastcom-systems.com.

9. Conclusion

These Application Notes describe the procedures for configuring the Eastcom CAMS to interoperate with Avaya Communication Manager. Eastcom CAMS successfully passed the compliance testing.

10. Additional References

This section references the Avaya documentation that is relevant to these Application Notes.

The following Avaya product documentation can be found at <http://support.avaya.com>.

[1] *Administrator Guide for Avaya Communication Manager*, Release 5.0, Issue 4.0, January 2008, Document Number 03-300509.

[2] *Avaya Site Administration Reference*, Issue 5, June 2008, Document Number 14-300610.

©2008 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.