CHAPTER 15

Management, Logging and Troubleshooting

This chapter describes the following:

- SNMP Configuration
- System Logging

SNMP Configuration

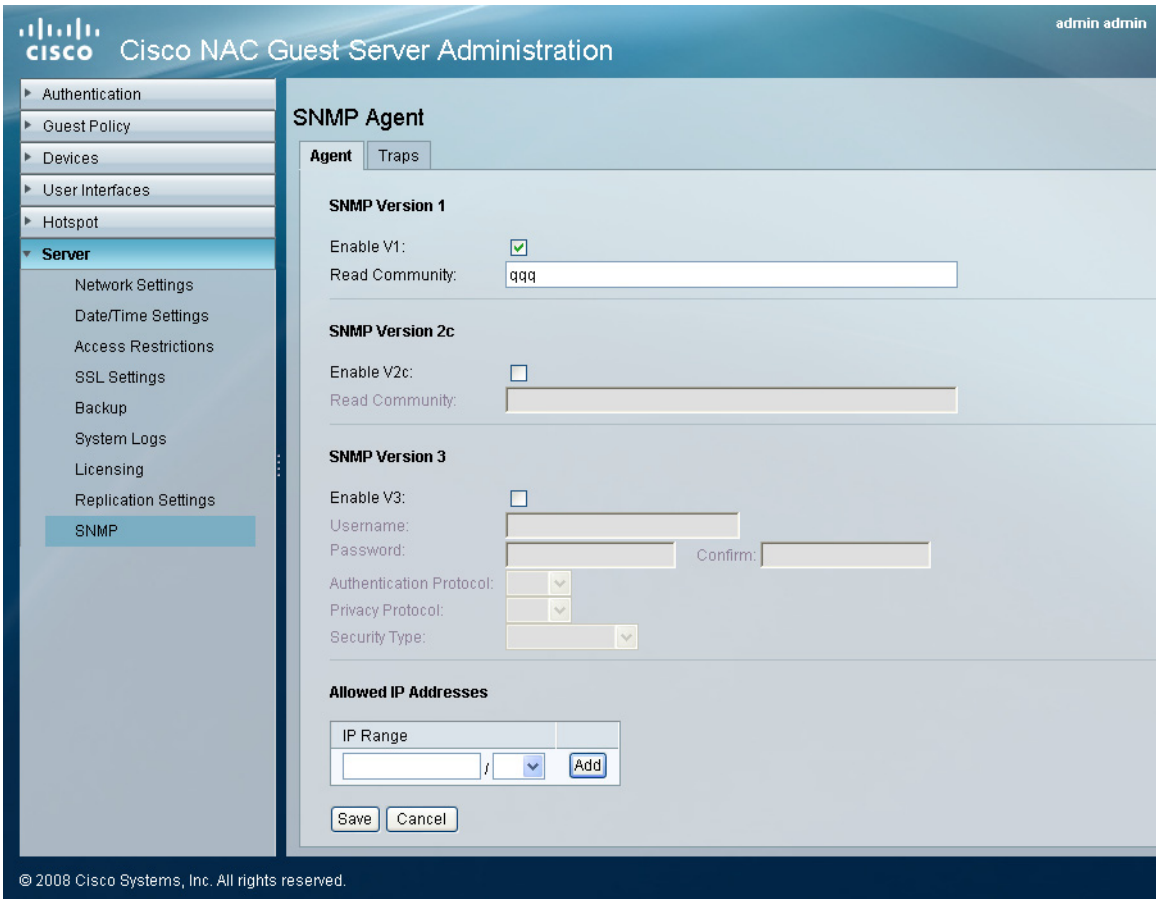
Cisco NAC Guest Server supports management applications monitoring the system over SNMP (Simple Network Management Protocol). SNMP Versions 1, 2c and 3 are supported.

The appliance can also send SNMP traps and informs when certain settings exceed a defined value.

SNMP Agent Configuration

From the administration interface, select **Server > SNMP** as shown in Figure 15-1.

Figure 15-1 SNMP Configuration



You can configure the following options:

- Configuring SNMP Version 1
- Configuring SNMP Version 2c
- Configuring SNMP Version 3
- Configuring SNMP Allowed Addresses

Configuring SNMP Version 1

Step 1 To enable SNMP Version 1, check the **Enable V1** checkbox.

Step 2 Enter an SNMP Read Community name to be used for read access.

Step 3 Configure the Allowed IP Addresses allowed to access the appliance using SNMP by following the instructions in Configuring SNMP Allowed Addresses, page 15-3.

Step 4 Click **Save**.

Configuring SNMP Version 2c

Step 1 To enable SNMP Version 2c, check the **Enable V2c** checkbox.

Step 2 Enter an SNMP Read Community name to be used for read access.

Step 3 Configure the Allowed IP Addresses allowed to access the appliance using SNMP by following the instructions in Configuring SNMP Allowed Addresses, page 15-3.

Step 4 Click **Save**.

Configuring SNMP Version 3

Step 1 To enable SNMP Version 3, check the **Enable V3** checkbox.

Step 2 Enter a Username to be used for read access.

Step 3 Enter the Password and confirm it to make sure it has been entered correctly.

Step 4 Select an Authentication Protocol from the dropdown menu: **MD5** (HMAC-MD5-96) or **SHA** (HMAC-SHA-96).

Step 5 Select a Privacy Protocol from the dropdown menu: DES or AES.

Step 6 Select the Security Type to use from the dropdown menu: Authentication or Encryption.

Step 7 Configure the Allowed IP Addresses allowed to access the appliance using SNMP by following the instructions in Configuring SNMP Allowed Addresses, page 15-3.

Step 8 Click **Save**.

Configuring SNMP Allowed Addresses

Step 1 Enter an IP Address Range made up of an IP Address and a prefix length. For example:

- 0.0.0.0/0 to allow any address to access the appliance by SNMP.
- 192.168.1.0/24 to allow any address from the 192.168.1.0-255 to access the appliance.
- 172.16.45.2/32 to allow only the host 172.16.45.2 to access the appliance.

Step 2 Click the **Add** button.

Step 3 You can repeat Step 1 and Step 2 for as many addresses as you like.

Step 4 Click **Save**.

SNMP Trap Support

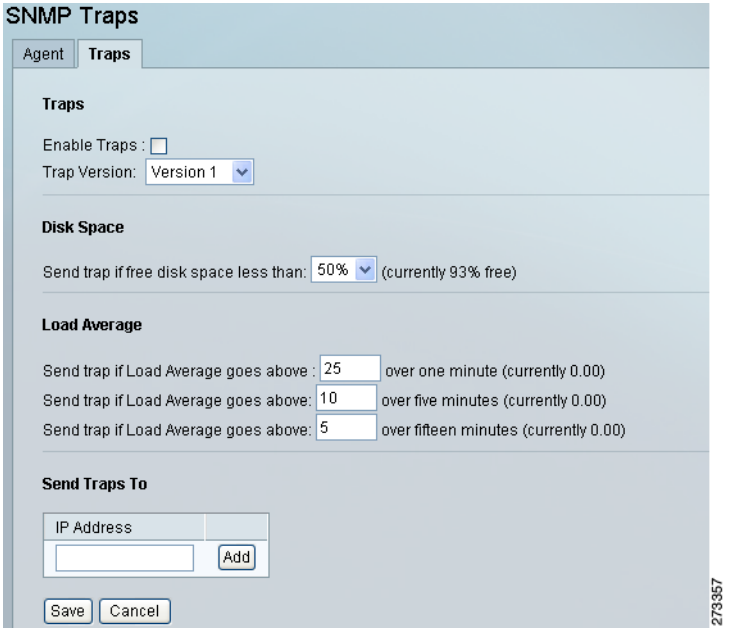
The NAC Guest Server can be configured to send SNMP Traps to an SNMP Manager based upon certain system events.

Configuring SNMP Traps

Note SNMP Traps are sent with the community string set to "traps". Cisco NAC Guest Server is not supporting authentication / warmstart traps.

Step 1 From the administration interface, select **Server > SNMP > Traps** as shown in Figure 15-2.

Figure 15-2 SNMP Trap Configuration



Step 2 Check the **Enable Traps** checkbox if you want to enable traps.

Step 3 Select the Trap Version from the dropdown: Version 1, Version 2c or Informs.

Step 4 The NAC Guest Server sends a trap if the disk space goes below a specified value. Enter the value you want the trap to be sent at in the Disk Space dropdown field.

Step 5 Specify the Load Average that you want a trap to be sent if it exceeds the value over 1 minute, 5 minutes or 15 minutes. Load Average is calculated using the standard Linux formula and can be seen from the command line with the **uptime** command.

Step 6 Enter each IP Address that you want to send a SNMP trap to and click the Add button.

Step 7 Click the **Save** button to save the changes.

SNMP MIB Files

The MIBs that the NAC Guest Server supports are located at /usr/share/snmp/mibs. The MIBfiles can only be obtained through an SFTP connection to the Guest Server. For Windows platforms, you can get a free SFTP client from http://winscp.net.

Step 1 Open an SFTP connection to the Cisco NAC Guest Server. The authentication credentials are the same as for the command line. Login with the root username and password you assigned for this account in the initial setup.

Step 2 Change to the **/usr/share/snmp/mibs** directory and download the files.

System Logging

All actions within the Cisco NAC Guest Server are logged into the database. This enables you to:

- View any action that occurred as part of the normal operating process of the application
- Log administrator and sponsor actions
- Create system logs

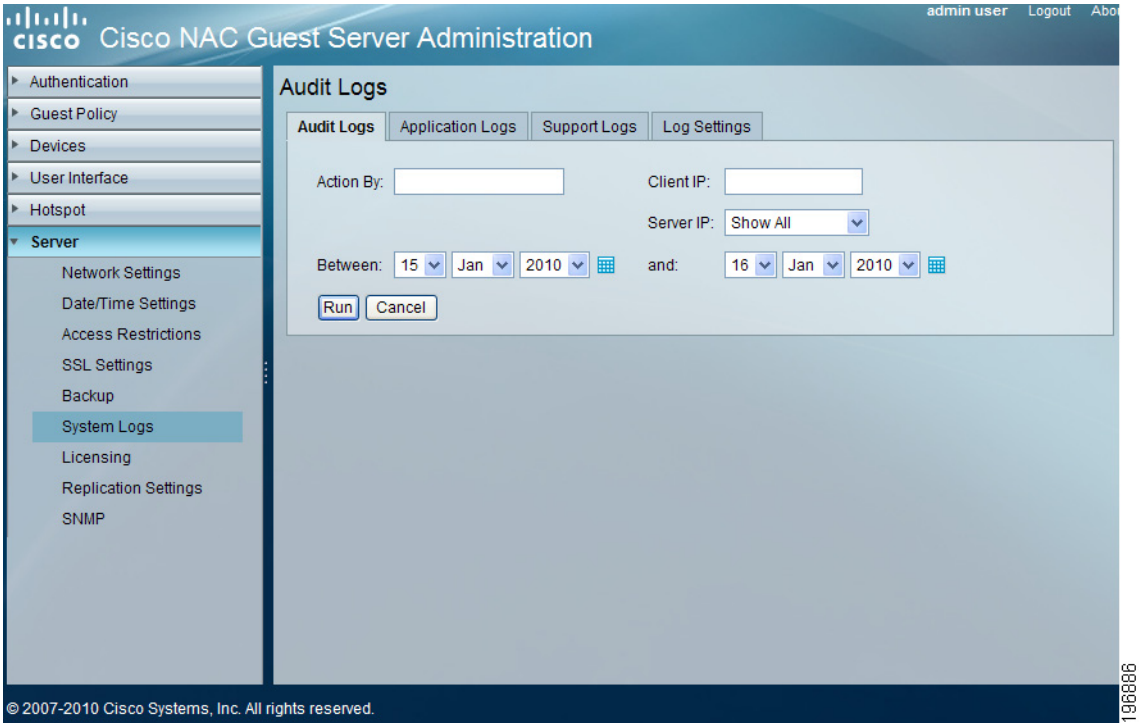
Note It is important to create and constantly maintain logging levels. Refer Log Settings, page 15-9 for details.

Audit Logs

Audit logs create a record of administrator and sponsor actions and can be created using four different methods.

Step 1 To access the audit log functions from the administration interface, select **Server > System Logs** as shown in Figure 15-3 and click the **Audit Logs** tab.

Figure 15-3 System Log



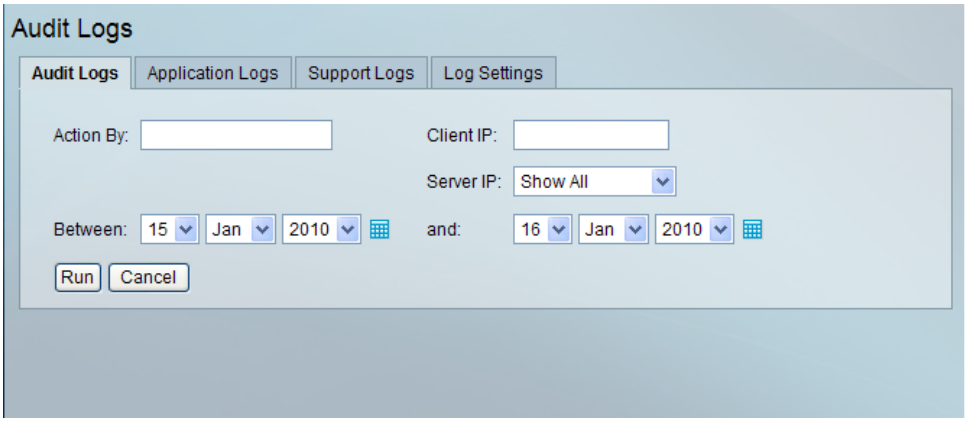
Step 2 Audit log reports can be run using four different categories as shown in Figure 15-4:

- **Action by**—Displays logs using admin/sponsor user name as its search criteria.
- **Client IP**—Displays logs using Client IP address as its search criteria.
- **Server IP**—Displays logs using Server IP as its search criteria.

You can run log reports for a single category, multiple categories, or all categories at the same time.

Step 3 Select a time duration for your search criteria using the date pickers provided, then click the **Run** button.

Figure 15-4 Audit Logs

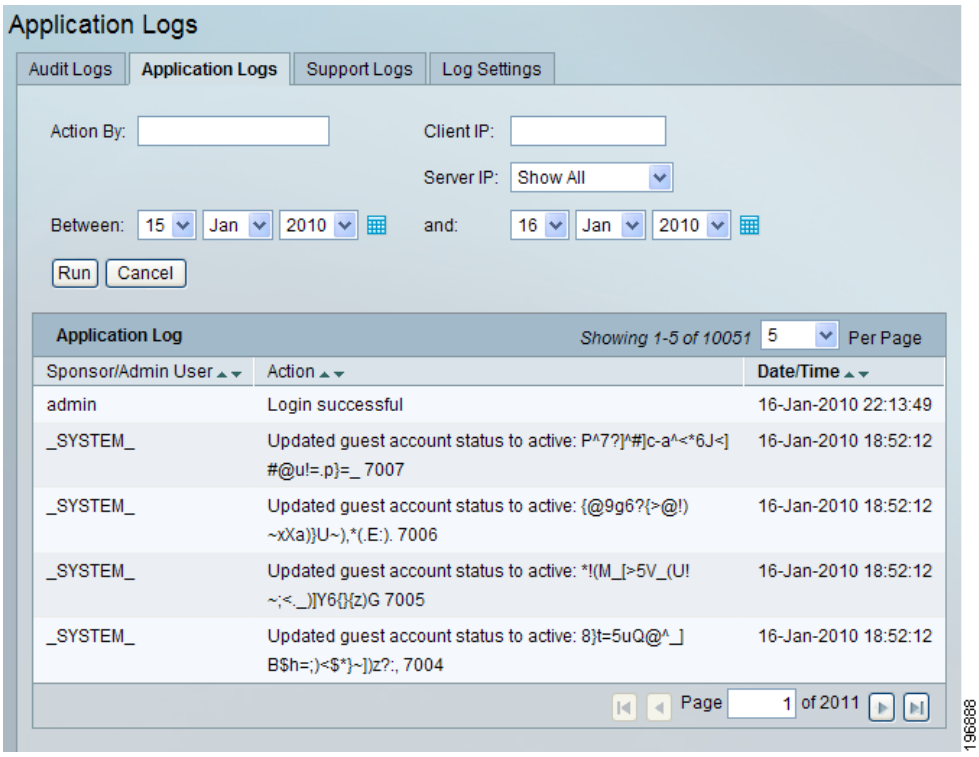


Application Logs

Application Logs shows the application log containing application debugs.

Step 1 To access the Application Logs function from the administration interface, select **Server > System Logs** and click the **Application Logs** tab as shown in Figure 15-5.

Figure 15-5 Application Logs



Step 2 Application Log reports can be run using four different categories:

- **Action by**—Displays logs using admin/sponsor user name as its search criteria.
- **Client IP**—Displays logs using Client IP address as its search criteria.
- **Server IP**—Displays logs using Server IP as its search criteria.

You can run log reports for a single category, multiple categories, or all categories at the same time.

Step 3 Select a time duration for your search criteria using the date pickers provided then click the **Run** button.

Note Cisco recommends disabling debugging immediately after use so as not to potentially disrupt any other NAC Guest Server functionality.

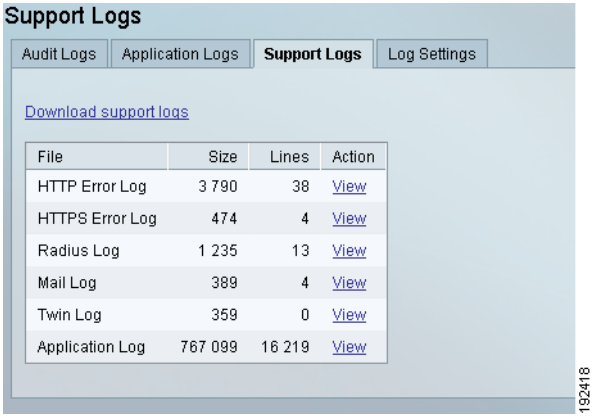
Support Logs

Support Logs provide an area that stores:

- HTTP error logs
- RADIUS logs
- Mail logs
- Twin (Replication logs only applicable if running replication between NAC Guest Servers)
- Debug logs
- Audit logs
- Application logs
- An XML file

Step 1 To access the Support Logs function from the administration interface, select **Server > System Logs** and click the **Support Logs** tab as shown in Figure 15-6.

Figure 15-6 Support Logs



Step 2 You can view or download the logs listed by clicking the underlined **Action** links.

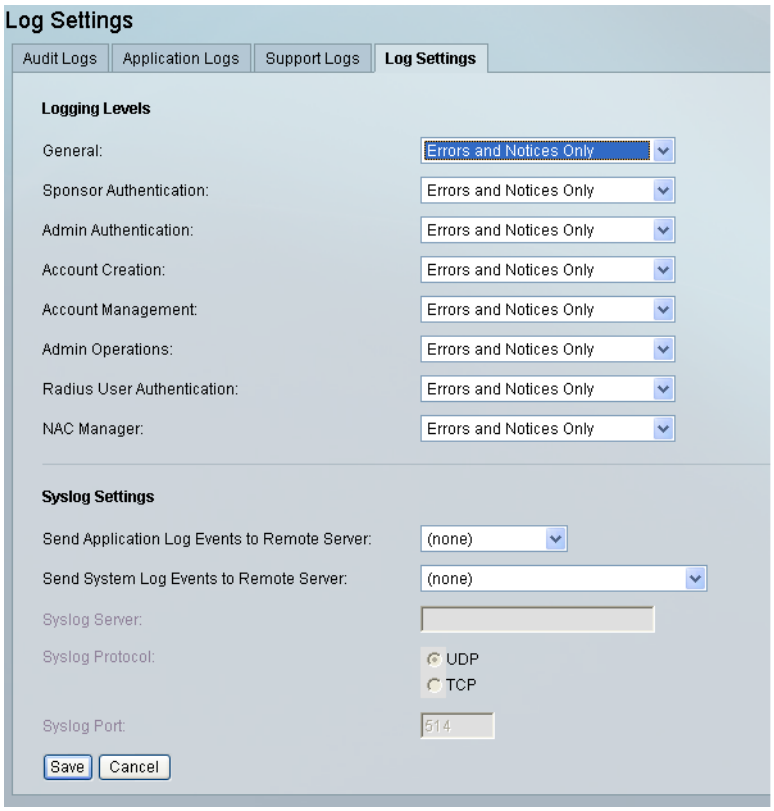
Note The Support Logs page only displays the latest details of each available log. However, clicking View or Download retrieves and displays ALL logs for that category.

Log Settings

The Log Settings page allows an administrator to set the level of logging and administer syslog settings.

Step 1 To access the Log Settings page from the administration interface, select **Server > System Logs** and click the **Log Settings** tab as shown in Figure 15-7.

Figure 15-7 Log Settings Page



Step 2 **Logging Levels** allow an administrator to choose the level of logging for multiple criteria:

- **General**—Allows an administrator to set logging of Errors and Notices only, Errors Notices and Info, or Errors Notices Info and Debugs.
- **Sponsor Authentication**—Allows an administrator to set logging of Errors and Notices only, Errors Notices and Info, or Errors Notices Info and Debugs.
- **Admin Authentication**—Allows an administrator to set logging of Errors and Notices only, Errors Notices and Info, or Errors Notices Info and Debugs.
- **Account Creation**—Allows an administrator to set logging of Errors and Notices only, Errors Notices and Info, or Errors Notices Info and Debugs.
- **Account Management**—Allows an administrator to set logging of Errors and Notices only, Errors Notices and Info, or Errors Notices Info and Debugs.
- **Admin Operations**—Allows an administrator to set logging of Errors and Notices only, Errors Notices and Info, or Errors Notices Info and Debugs.

- **Radius User Authentication**—Allows an administrator to set logging of Errors and Notices only, Errors Notices and Info, or Errors Notices Info and Debugs.
- **NAC Manager**—Allows an administrator to set logging of Errors and Notices only, Errors Notices and Info, or Errors Notices Info and Debugs.

Step 3 **Syslog Settings** allows an administrator to determine what log events are sent to a predefined syslog server.

- **Send Application Log Events to Remote Server—**This determines what type of application errors are logged and sent to the server. The administrator can decide on none, Audit, Errors or Audit and Errors.
- **Send System Log Events to Remote Server—**This determines what type of system errors are logged and sent to the server. The administrator can decide on Emergency, Emergency and Alerts, Emergency Alerts and Critical, or Emergency Alerts Critical and Errors.
- **Syslog Server—**Enter the DNS or IP Address of the syslog server to which the logs to be sent.
- **Syslog Protocol—**Choose between UDP and TCP protocols.
- **Syslog Port—**Define a port for your syslog server.

Step 4 Click the **Save** button to save your settings.

Note To test basic syslog functionality, go to the Log Settings page and click **Save**. This sends a test message to the syslog server with priority info (6).