CHAPTER 11

Monitoring and Troubleshooting Agent Sessions

This chapter provides information on compiling and accessing various Cisco NAC Appliance Agent reports and log files and troubleshooting Agent connection and operation issues:

- Viewing Agent Reports, page 11-1
- Create Agent Log Files Using the Cisco Log Packager, page 11-6
- Manage Certified Devices, page 11-10
- Report Settings, page 11-18
- Online Users list, page 11-29
- Agent Troubleshooting, page 11-37

Viewing Agent Reports

The administrator Agent Reports page (under Device Management > Clean Access > Clean Access Agent > Reports > Report Viewer) gives you detailed information about user Agent sessions. The information includes user access attempts and system check results.

Using the Reports page, administrators can log and search Agent reports to facilitate information gathering and export compiled report data to aid statistical analysis and Agent connection issue troubleshooting. The Reports page presents Agent report entry information using the following column headings:

- **Status**—Green or red flag indicates successful or unsuccessful Agent connection
- **User**—The user ID used to establish the session from the client machine
- **Agent**—Specifies the type of Cisco NAC Appliance Agent used to initiate the client session
- **Type**—Specifies whether the report has been generated due to Login posture or Passive Re-assessment
- **IP**—The client machine IP address
- **MAC**—The client machine interface MAC address
- **OS**—The operating system detected on the client machine
- **Time**—The date and time the user attempted to initiate the Agent session

**Note**

Report List entries with a red background indicate clients who failed system checking.
The Reports page also enables you to filter the list of user session reports by activating and defining additional client report display criteria. For example, if you have a very large user access base where users log in every day (even multiple times per day) and you want to limit the number of reports to a more manageable total, you can choose to display user session information for a single user ID or all user sessions from a specific device. The filter parameters available in the dropdown menu are:

- **Status**—Allows you to list either successful or unsuccessful, or both types of user sessions
- **Username**—Allows you to specify all or part of a specific user ID to display in the client report list
- **Agent**—Allows you to select the type of Cisco NAC Appliance Agent
- **Type**—Allows you select the type of the posture by which the client has got access to the NAC Appliance (Login or Passive Re-assessment)
- **IP**—Allows you to limit the list of client reports to match all or part of a specified IP address (you could use this parameter to limit the user list to only IP addresses in the 10.12.4.<x> range by specifying “starts with” “10.12.4.”, for example)
- **MAC**—Allows you to limit the list of client reports to match all or part of a specified source MAC address
- **OS**—Allows you to display client reports based on the operating system detected on the client machine
- **Time**—Allows you to display client report entries either since or before a point in time (like within the last hour or before the last day, for example)
- **Software**—Allows you to display client reports for specific installed AntiVirus, Antispyware, and/or any Unsupported AV/AS software
- **Requirement**—Allows you to display only client reports associated with a specific Agent requirement
- **Requirement Status**—Allows you to display client reports for successful or unsuccessful Agent requirements for the specified Requirement (above)
- **System Name**—Allows you to display client reports associated with all or part of a specific client system name
- **System User**—Allows you to display client reports associated with a specific system user (that is, the user logged in to the client machine at the time the actual user session was initiated, which is not necessarily the same ID as the Username, above)
- **System Domain**—Allows you to display only client reports based on the system domain into which the client machine has been logged in

- **User Domain**—Allows you to display only client reports based on the user domain with which client **System User ID** is associated

Click the **Filter** button after selecting and defining parameters for any of the search options to display a summary of all client report entries that match the criteria as well as the detailed administrator report for each client.

For example, you can use the **OS** filter option to refine the Agent report display to a smaller number of report entries by selecting one of the options from the dropdown list (Figure 11-2).

**Figure 11-2  Agent Administrator Report—OS Filter Option**

You can click **Reset** to negate any of the optional search criteria from the filter dropdown menu and return the client report display list to default settings.

Click the **View** icon (far-right magnifying glass icon) to see an individual user report, as shown in Figure 11-3.
Figure 11-3  Example Agent Report

System Name: VU  System Domain: n/a
System User: User Domain: VU

1. req_microsoft_updates (Mandatory)
   - Passed Checks:
     - pc_K9961971_MS09-029_Vista
     - pc_K960863_MS09-013_Vista
     - pc_K954593_MS08-052_Vista
     - pc_Windows-Vista-SP1
     - pc_Vista_RE972600_MS09-034_IE7
     - pc_KB999499_MS08-075_Vista
     - pc_KB956662_MS08-071_Vista
     - pc_Vista64_IE851696_MS08-033
   - Failed Checks:
     - pc_Windows-Vista-SP2 Registry Check [HKKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Windows\SDD\Version] v12
     - pc_Windows-Vista-SP2 Registry Check [HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Windows\SDD\Version] contains Service Pack 2
     - pc_Vista64 Registry Check [HKKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Version: start with 2]
     - pc_IE8_0 Registry Check [HKKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Version: start with 2]
   - Not executed Checks:
     - pc_KB925993_MS07-017_Vista
     - pc_KB929123_MS07-034_Vista
     - pc_MS25MS08-069_Vista
     - pc_KB929016_MS07-040_Vista
     - pc_Vista_RE972500_MS09-034_IE8
     - pc_KB929123_MS07-034_Vista
     - pc_MS25MS08-069_Vista
     - pc_KB929016_MS07-040_Vista
     - pc_Windows-Vista-SP1 Registry
     - pc_KB46026_MS08-007_Vista
     - pc_KB940178_MS07-021_Vista
     - pc_KB938127_MS07-050_Vista
     - pc_KB925992_MS07-017_Vista
     - pc_KB44026_MS08-007_Vista
     - pc_KB90178_MS07-021_Vista

2. req any av_win (Optional)
   - Passed Checks:
     - pc_av_win ANY_vendor

3. req any av_win (Optional)
   - Passed Checks:
     - pc_av_win ANY_vendor

4. req any av def win (Optional)
   - Failed Checks:
     - pc_av_def ANY, Anti-Spyware Check [Any supported AV software up-to-date] see Client AV Info for details

5. req any av def win (Optional)
   - Passed Checks:
     - pc_av_def ANY, Anti-Spyware Check [Any supported AS software up-to-date] see Client AS Info for details

Client AV Info
Product ID: E-BEDV
Product Name: Anti-Virus Personal – Free Antivirus
Product Version: 8.2.0.354
Virus Definition File Version: 7.0.0.00 97
Virus Definition File Date: 1/1/2009

Client AS Info
Product ID: MicrosoftAS
Product Name: Windows Defender Vista
Product Version: 1.1.1400.0
Spyware Definition File Version: 1.0.0.0
Spyware Definition File Date: 07/13/2006

Close
In addition to user, operating system, Agent version, and domain information, the Agent report lists the
requirements applicable for the user role (both mandatory and optional). Requirements that the user met
are listed in green, and failed requirements are listed in red. The individual checks making up the
requirement are listed by status of Passed, Failed, or Not executed. This allows you to view exactly which
check a user failed when a requirement was not met.

**Not Executed** checks are checks that were not applied, for example because they apply to a different
operating system. **Failed** checks may be the result of an “OR” operation. To clear the reports, click the
**Delete** button. The button clears all the report entries that are currently selected by the filtering criteria.

### Exporting Agent Reports

You can use the **Export** and **Export (with text)** buttons to save CSV files containing Agent report data
to your local hard drive to search, view, and manipulate whenever needed for troubleshooting or
statistical analysis purposes.

1. **Step 1**
   Go to under **Device Management > Clean Access > Clean Access Agent > Reports > Report Viewer**
   (see **Figure 11-4**).

2. **Step 2**
   Click **Export** or **Export (with text)**.

   **Note**
   Due to limits native to the Microsoft Excel application, you can only export up to 65534 entries using
   this function.

   **Figure 11-4**  **Exporting Agent Reports**

   ![Figure 11-4 Exporting Agent Reports](https://example.com/figure11-4.png)

3. **Step 3**
   Do one of the following:
   - Click **Open** to view the resulting Agent report file.
• Click Save, navigate to a directory on your local machine where you want to save the Agent report file, enter a name for the file, and click Save in the navigation dialog so you can view the report at a later date.

Limiting the Number of Reports

You can limit the number of reports in the log under Device Management > Clean Access > Clean Access Agent > Reports > Report Setting. Specify the maximum number of reports as a value between 100 and 200000 (default is 30000).

Agent reports are stored in their own table and are separate from the general Event Logs.

Create Agent Log Files Using the Cisco Log Packager

When users download the Cisco NAC Agent, the installation process also adds the Cisco Log Packager utility to the client machine in the same relative Program File location as Agent files. The Log Packager utility compiles and saves a number of different types of Agent logs in a single .zip file (named CiscoSupportReport.zip) and saves it on the client machine’s desktop, so the user can access the information easily and forward on to network administrators to help troubleshoot Agent session login and/or operation issues.

Note

In Cisco NAC Appliance Release 4.6(1) and later, the Cisco Log Packager application is only available for English and Japanese Windows platforms.

To launch the Cisco Log Packager:

Step 1

On the Windows client machine, navigate to Start > Program Files > Cisco > Client Utilities > Cisco Log Packager (Figure 11-5).

Figure 11-5 Cisco Log Packager
Step 2 Click Collect Data and wait for the Cisco Log Packager to complete compiling the Agent log information. This step takes anywhere from several seconds to a couple of minutes or so. The process is complete when you see a “Log file has been archived” message in the Cisco Log Packager display window and the Copy to Clipboard and Locate Log File buttons become active (Figure 11-6).

Figure 11-6 Cisco Log Packager—Log File Archive Complete

Step 3 To automatically navigate to the location on the client machine where the log file has been compiled and saved, click Locate Log File. A Windows Explorer dialog box opens highlighting the location of the new CiscoSupportReport.zip log file on the client machine desktop (Figure 11-7).

Figure 11-7 Agent Log File Location
Use the **CiscoSupportReport.zip** log file to help diagnose and troubleshoot Agent login/operation issues. Users can send the .zip file to their respective Cisco NAC Appliance system administrator or, if performing local troubleshooting, extract and view the contents of the various Cisco Log Packager files on the client machine. For details on the files included in the **CiscoSupportReport.zip** log file and their purpose, see Figure 11-7.

### Table 11-1 Cisco Log Packager Files

<table>
<thead>
<tr>
<th>Agent Log File Name</th>
<th>Contents/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CiscoSupportReportLog.txt</td>
<td>This text file contains client machine system information, including CPU usage and memory allocation.</td>
</tr>
<tr>
<td>ipinfo.log</td>
<td>This log file contains network configuration and network connection status, including client machine IP interface status, IP statistics, and the client ARP table.</td>
</tr>
<tr>
<td>NACAgentLogPlugin.log</td>
<td>This user-inaccessible log is one of the modules in the LogPacker component that calls the NACAgentDiags function to generate the NACAgentDiagnosticLog.txt log report.</td>
</tr>
<tr>
<td>NACAgentDiagnosticsLog.txt</td>
<td>This user-inaccessible text file contains diagnostic messages used to help debug AV issues.</td>
</tr>
<tr>
<td>NACAgentDiagsLogMessages.txt</td>
<td>This text file contains other regular log messages not used in the diagnostics output.</td>
</tr>
<tr>
<td>NACAgentLogCurrent.log</td>
<td>This is an encrypted log file that contains the current Cisco NAC Agent messages from the active session and is used primarily to help debug Cisco NAC Agent issues. When the system reboots or services have been restarted, the existing NACAgentLogOld.log is erased, the active NACAgentLogCurrent.log becomes the new NACAgentLogOld.log, and a new NACAgentLogCurrent.log is created.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>You can configure the size of Agent log files using the LogFileSize parameter in the NACAgentCFG.xml Agent configuration XML file. If set to 0, no logging takes place. If set to non-zero, then the log file does not grow larger than the value (in Megabytes). The default is 5 MB. When NACAgentLogCurrent.log reaches the setting value, it is copied to NACAgentLogOld.log and a new NACAgentLogCurrent.log is created.</td>
</tr>
</tbody>
</table>
Users can open any of the .txt files on the client machine using a standard text editor application and view the report contents. Figure 11-8 shows the contents of a CiscoSupportReportLog.txt file opened using Microsoft Notepad on the client machine.

Table 11-1 Cisco Log Packager Files

<table>
<thead>
<tr>
<th>Agent Log File Name</th>
<th>Contents/Description</th>
</tr>
</thead>
</table>
| NACAgentLogOld.log      | This is an encrypted log file that contains output from the previous active Cisco NAC Agent session and is also used to help debug Cisco NAC Agent issues. This file is created in one of two ways:  
  - The “archived” log file from an active Cisco NAC Agent session that reached its maximum size (configured using the LogFileSize parameter in the NACAgentCFG.xml Agent configuration XML file).  
  - When the system reboots or services are restarted, the existing NACAgentLogOld.log is erased, the active NACAgentLogCurrent.log becomes the new NACAgentLogOld.log, and a new NACAgentLogCurrent.log is created. |
Manage Certified Devices

This section describes the following:

- **Add Exempt Device, page 11-12**
- **Clear Certified or Exempt Devices Manually, page 11-13**
- **View Reports for Certified Devices, page 11-13**
- **View Switch/WLC Information for Out-of-Band Certified Devices, page 11-13**
- **Configure Certified Device Timer, page 11-14**
- **Add Floating Devices, page 11-16**

The Clean Access Manager web console provides two important lists that manage users and their devices: the **Online Users list** (both In-Band and Out-of-Band) and **Certified Devices List**. The Online Users list displays logged-in users by IP address and login credentials (see Interpreting Event Logs, page 13-4). When a user device passes network scanning or meets Agent Requirements, the Clean Access Server automatically adds the MAC address of the device to the Certified Devices List (for users with Layer 2 proximity to the CAS).

Because the Certified Devices List is based on client MAC addresses, the Certified Devices List never applies to users in Layer 3 deployments. Web login users that are one or more Layer 3 hops away from the CAS are tracked by IP address only, unless the ActiveX/Java applet web client is enabled for the login page (to obtain the MAC address of the client). For further details on Layer 3 deployment, see “Enable L3 Deployment Support” in the **Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(1)**.

Dropping an In-Band user from the In-Band Online Users list does not remove the client device from the Certified Devices List. However, manually dropping an In-Band client from the Certified Devices List automatically removes the user from the network and the In-Band Online Users list.

Dropping an Out-of-Band user from the Out-of-Band Online Users list has different results depending on your Cisco NAC Appliance configuration:

- In a deployment where Out-of-Band Logoff has been enabled, the client machine is also automatically removed from the Certified Devices List.
- If Out-of-Band Logoff is not enabled and you kick the user from the Out-of-Band Online Users list, the client machine stays in the Certified Devices List just as with an In-Band deployment.

For more information on Out-of-Band logoff, see **Configure Out-of-Band Logoff, page 9-6**.

For network scanning, once on the Certified Devices List, the device does not have to be recertified as long as its MAC address is in the Certified Devices List, even if the user of the device logs out and accesses the network again as another user. Dropping a client from the Certified Devices List forces the user to repeat authentication and the device to repeat network scanning to be readmitted to the network. (Multi-user devices should be configured as floating devices to require recertification at each login.) You can make sure that a device is always removed from the Certified Devices List when a network scanning user logs off by enabling the option **Require users to be certified at every web login** in the **General Setup > Web Login** tab (see Client Login Overview, page 1-7).

For Agent users, devices always go through Agent Requirements at each login, even if the device is already on the Certified Devices List. In addition, the Certified Devices List only records the first user that logged in with the device. This helps to identify the authenticating user who accepted the User
Chapter 11  Monitoring and Troubleshooting Agent Sessions

Manage Certified Devices

Agreement Page (for web login users) or the Network Policy Page (for Agent users) if either page was configured for the role. See Table 1-2 “Web Login—General Setup Configuration Options” and Table 1-3 “Web Login User Page Summary” for details on these pages.

A certified device remains on the Certified Devices List until:

- The list is automatically cleared using a Certified Devices Timer.
- The administrator manually clears the entire list.
- The administrator manually drops the client from the list.
- The user logs out or is removed from the network, and the Require users to be certified at every web login option is checked for the role from the General Setup > Web Login page.

Devices automatically added to the Certified Devices List can be cleared manually or cleared automatically at specified intervals. Because the administrator must manually add exempt devices to the list, the administrator must also manually remove them. This means that an exempt device on the Certified Devices List is protected from being automatically removed when the global Certified Devices Timer form is used to clear the list at regularly scheduled intervals.

Clearing devices from the Certified Devices List (whether manually or automatically) performs the following actions:

- Removes IB clients from the In-Band Online Users list and logs them off the network.
- Removes OOB clients from the Out-of-Band Online Users list and bounces their port (unless port bouncing is disabled for OOB VGW; see Add Port Profile, page 3-34 for details).
- Forces client devices to repeat posture assessment at the next login.

Once off the Certified Devices List, the client must pass network scanning and meet Agent Requirements again to be readmitted to the network. You can add floating devices that are certified only for the duration of a user session. You can also exempt network scanning devices from Nessus Scanning altogether by manually adding them to the Certified Devices List.

If using a Certified Device timer, you can configure whether or not a user is removed when the list is cleared by enabling/disabling the Keep Online Users option for the timer. See Configure Certified Device Timer, page 11-14 for further details.

Note that logging an IB user off the network from Monitoring > Online Users > View Online Users does not remove the client from the Certified Devices List. This allows the user to log in again without forcing the client machine to go through posture assessment again. Note that for Agent users, devices always go through Agent Requirements at each login, even if the device is already on the Certified Devices List.

Because the Certified Devices List displays users authenticated and certified based on known L2 MAC address, the Certified Devices List does not display information for remote VPN/multihop L3 users tracked by IP address only. To view these authenticated remote VPN/multihop L3 users, see the In-Band Online Users list. The User MAC field for these user entries appears as “00:00:00:00:00:00.”

For further details on terminating active user sessions, see Interpreting Active Users, page 11-30 and Out-of-Band Users, page 3-70.

If a certified device is moved from one CAS to another, it must go through Nessus Scanning again for the new CAS unless it has been manually added as an exempt device at the global level for all Clean Access Servers. This allows for the case where one Clean Access Server has more restrictive posture assessment requirements than another.
Though devices can only be certified and added to the list per Clean Access Server, you can remove certified devices globally from all Clean Access Servers or locally from a particular CAS only (see the Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(1) for additional details.) For additional information, see also Out-of-Band Users, page 3-70.

Add Exempt Device

Designating a device as Exempt excludes the device from Network Scanning (Nessus scans) and no network scanning report is generated for the client. Exempting a device manually adds it to the Certified Devices List and allows it to bypass network scanning as long as its MAC address remains on the list.

Note
Adding a device as Exempt does not exempt the client machine from Agent posture assessment.

Note
For details on how to allow users/devices to bypass authentication, see Global Device and Subnet Filtering, page 2-10.

To add an exempt device:

Step 1  Go to Device Management > Clean Access > Certified Devices > Add Exempt Device.

Figure 11-9Add Exempt Device

Step 2  Type the MAC address in the Exempt Device MAC Address field. To add several addresses at once, use line breaks to separate the addresses.

Step 3  Click Add Exempt.

Step 4  The Certified Devices List page appears, highlighting the exempt devices (Figure 11-10).

Note
Exempt devices added with these forms are exempt for all Clean Access Servers. To designate an exempt device for only a particular Clean Access Server, see the Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(1).
Clear Certified or Exempt Devices Manually

To clear device MAC addresses, go to Device Management > Clean Access > Certified Devices > Certified Devices List and click:

- **Clear Exempt** to remove only the MAC addresses that were added manually with the Add Exempt button.
- **Clear Certified** to remove only the MAC addresses that were added automatically by the Clean Access Server.
- **Clear All** to remove MAC addresses of both exempt and certified devices.

Remove individual addresses individually by clicking Delete next to the MAC address.

View Reports for Certified Devices

You can view the results of previous Agent scans for certified devices under Device Management > Clean Access > Clean Access Agent > Reports. Click the View icon to see which requirements, rules, and checks succeeded or failed for an individual client. See View Scan Reports, page 12-17 for details.

You can view the results of previous network scans for certified devices at any time from Device Management > Clean Access > Network Scanner > Reports. Click the Report icon to see an individual scan report. See View Scan Reports, page 12-17 for details.

View Switch/WLC Information for Out-of-Band Certified Devices

For Out-of-Band users only, the Certified Devices List (Figure 11-10) populates the Location column with a the IP address and specific port on the Out-of-Band switch, or (in the case of a Wireless LAN controller) the IP address and SSID for the specific Out-of-Band WLC.

For further details on OOB clients, see:

- Chapter 4, “Wireless LAN Controller Management: Configuring Wireless Out-of-Band Deployment”
Configure Certified Device Timer

You can configure Certified Device Timers to automatically clear the Certified Device list at specified intervals. The Certified Devices List no longer needs to be cleared in its entirety each time the timer is applied. Administrators can now:

- Clear the Certified Devices List per Clean Access Server, User Role, or Authentication Provider, or a combination of all three.
- Clear certified devices without removing users from the network with the “Keep Online Users” option. When the “Keep Online Users” option is checked, user sessions are not immediately ended when clearing the list, but at user logout time (or at linkdown for OOB). Devices can re-enter the list after user authentication and device remediation.
- Clear the Certified Devices List all at once or in batches (to manage user re-login and certification during peak times). You can clear devices according to how long they have been on the list and/or in fixed time interval batches. This facilitates CAM database management when clearing large numbers of devices.
- Configure multiple independent timers. Administrators can create and save multiple instances of Certified Device Timers (similar to a Scheduled Job/Task). Each Timer is independent of the others and can be maintained separately. For example, if managing 6 CAS pairs, the administrator can create a different Timer for each pair of HA-CASs.

**Step 1** Go to Device Management > Clean Access > Certified Devices > Timer. The List page appears by default.

**Figure 11-11  Certified Devices Timer—List**

**Step 2** Click the New sublink to bring up the New Timer configuration form.
**Figure 11-12  New Certified Devices Timer**

- **Step 3** Type a **Timer Name** for the timer.
- **Step 4** Type an optional **Description** of the timer.
- **Step 5** Click the checkbox for **Enable this timer** to apply the timer right away after configuration.
- **Step 6** Click the checkbox for **Keep Online Users** if you only want to remove client devices from the Certified Devices List without removing the users from the network.
- **Step 7** Type the **Start Date and Time** for the timer, using format: `YYYY-MM-DD hh:mm:ss`. The **Start Date and Time** sets the initial date and time for this timer to clear the Certified Devices List.
- **Step 8** Type a **Recurrence** in days to set the repeat interval for this timer. For example, a **Recurrence** of 7 will clear the Certified Devices List 7 days after the initial clearing and at the same **Start Time** specified. Typing 0 will clear the Certified Devices List only once.
- **Step 9** Choose from any of the dropdown menus to apply this timer by the following **Criteria**:
  a. **Clean Access Server**: Apply this timer to **Any CCA Server** (default) or to a specific CAS by IP address.
  b. **User Role**: Apply this timer to **Any User Role** (default) or to a specific system user role
  c. **Provider**: Apply this timer to **Any Provider** (default) or to a specific system **Auth Provider** (Local DB or any other)
Step 10  Type a **Minimum Age** in days to only clear devices that have been on the Certified Devices List for the number of days specified. Typing 0 clears all devices regardless of how long they have been on the Certified Devices List.

Step 11  Choose a clearing **Method** for how much of the Certified Devices List (sorted by Criteria) this timer should clear at one time. Options are:

a. **Clear all matching certified devices.**

b. **Clear the oldest [ ] matching certified devices only.** (for example, “10” clears the ten oldest certified devices in the sort list)

c. **Clear the oldest [ ] certified devices every [ ] minutes until all matching certified devices are cleared.**

Step 12  When done, click **Update.** This saves the Timer in the Certified Devices Timer List.

**Note**  For additional information on terminating user sessions, see also **Configure User Session and Heartbeat Timeouts,** page 8-15.

---

**Add Floating Devices**

A floating device is certified only for the duration of a user session. Once the user logs out, the next user of the device needs to be certified again. Floating devices are useful for managing shared equipment, such as kiosk computers or wireless cards loaned out by a library.

In addition to session-length certification, you can configure devices that are never certified. This is useful for multi-user devices, such as dial-up routers that channel multi-user traffic from the untrusted side of the network. In this case, the Clean Access Server will see only that device’s MAC address as the source and destination of the network traffic. If the device is allowed to be certified, after the first user is certified, additional users would be exempt from certification. By configuring the router’s MAC address as a floating device that is never certified, you can ensure that each user accessing the network through the device is individually assessed for vulnerabilities/requirements met.

In this case, the users are distinguished by IP address. Users must have different IP addresses. If the router performs NATing services, the users are indistinguishable to the Clean Access Manager and only the first user will be certified.

**Figure 11-13** shows the **Floating Devices** tab.
To configure a floating device:

1. Go to Device Management > Clean Access > Certified Devices > Add Floating Device.
2. In the Floating Device MAC Address field, enter the MAC address. Type the entry in the form:

   `<MAC> <type> <description>`

   Where:
   - `<MAC>` is the MAC address of the device.
   - `<type>` is either:
     - 0 for session-scope certification, or
     - 1 if the device should never be considered certified
   - `<description>` is an optional description of the device.

   Include spaces between each element and use line breaks to separate multiple entries. For example:

   00:16:21:11:4D:67 0 LibCard1
   00:16:21:11:4D:67 0 LibCard2
   00:16:11:12:4A:71 1 Router1

3. Click Add Device to save the setting.

To remove a floating device, click the Delete icon for the MAC address.
Report Settings

The Monitoring > Reporting tab can be used to enable or disable the reporting and user activity logging, to view the current system information, to customize the reports, and to view the preset reports. This section contains the following topics:

- Dashboard, page 11-18
- Custom Reports, page 11-22
- Configuration, page 11-28

Dashboard

The current system information of the CAM and CAS can be viewed from Monitoring > Reporting > Dashboard tab.

The Dashboard page displays the system information, which is constantly monitored and updated. This page is enabled only when the Enable Dashboard and related tasks checkbox is checked in the Monitoring > Reporting > Configuration page.

**Note** Dashboard and related tasks check box is enabled by default when you upgrade from previous version of NAC release. The default landing page will be the dashboard summary page.

The current system information is displayed as different subtabs in this page. Click the appropriate tabs to view the following information:

- Current Status, page 11-18
- CCA Servers, page 11-20
- Managed Switches, page 11-20
- Authentication Servers, page 11-21
- User Statistics, page 11-22

Current Status

This tab displays the current status of the following:

- **System Summary**: Displays the details of the CAM along with the License details, NAC version installed, NAC Agent versions and so on.
  - Service Uptime: Time since the perfigo service started.
  - Active Uptime: Time since the perfigo service is active on the CAM.
- **Status Summary**: Displays the details of CAM, CAS, OOB Switches, Auth Server and so on.
- **Top 5 CASs**: Displays the CASs with maximum number of current online users in the system.
- **User Summary**: Displays a graphical summary of number of users in online status with reference to time. This graph displays details based on assigned user roles.
- **Recent Events**: Displays system events that happened in the last 5 days.
The **Current Status** tab displays the “last refreshed” date and time at the top-right corner of the page. The current system information is automatically refreshed every 10 minutes. You can also refresh the page manually by clicking the **Current Status** tab.
CCA Servers

The CCA Servers view displays the details of CASs added to the CAM. It displays the online status (green if online), location, current memory usage, number of users currently connected to the CAS and last access time. Last access time is always the last successful access time for CAS by the CAM. If the CAS status is down (it would be shown in red), but the last access time would be the time CAS was last reachable.

**Figure 11-15  Dashboard > CCA Servers**

The details icon displays the details of selected CCA Server.

**Figure 11-16  Dashboard > CCA Servers > Details**

Managed Switches

The OOB switches and OOB wireless LAN controllers managed by the CAM are under Managed Switches. You can view the switch and wireless LAN controller information like its IP address, device profile, number of ports managed by CAM, status (green if online) and last access time that is last successful access time.
Managed ports column for wireless LAN controllers will be empty as managed ports are applicable to switches only and not to WLAN controllers.

### Authentication Servers

The status and other details of the authentication servers used by NAC are under the Auth Servers view. NAC does not actively check the authentication servers for their reachability to display the status here. As and when a user request comes for authentication and NAC is able to communicate to the authentication server, status is marked as reachable and the time is set as the last access time.

Two types of authentication providers are supported - First, where CAM does the active authentication with the authentication server on behalf of the end users like Radius or LDAP servers. Second, the single sign-on (SSO) type like ADSSO or VPNSSO, where the user gets authenticated elsewhere first and an already authenticated user enters into the NAC system. In the case where the CAM does the active authentication for the end users, both the status (green if online) and the last access time is shown. In the SSO type auth providers case, CAM or NAC does not do any active authentication and hence it never tries to reach them. Accordingly, here the last access time shown is the time any user last entered into NAC using that provider. Additionally, it displays the status CAS wise that is more granular as SSO happens through CASs.
User Statistics

This tab displays the summary of current user statistics. Total number of users in the system is the total count of users currently in all roles in the systems. It includes users in temporary roles also (users undergoing posture assessment).

Number of users that failed login in the last 24 hrs is count of users who have failed login due to posture requirements only. It does not include other failures like invalid user or passwords entered by the users. Also, if the user is failing posture assessment more than once in the last 24 hrs, it is counted as one failure only.

User statistics shows the top five operating systems in current use in NAC system with respect to the number of users using those O/S(s). Click Refresh to get the latest data.

Figure 11-19 Dashboard > User Statistics

Note

When the Out-of-band devices list is large, the reporting page takes a longer time to display the reports. If this situation occurs, try deleting some of the unused devices in the Out-of-band devices list to view the reports.

Custom Reports

The Custom Reports tab can be used to generate customized and scheduled reports. You can save the customized settings as a template for future reference. This section contains the following topics:

- Generate New Reports, page 11-22
- View Saved Templates, page 11-27
- View Executive Summary, page 11-27

Generate New Reports

You can generate new reports, customize them by setting up filters, and schedule to generate a report in future.

Go to Monitoring > Reporting > Custom Reports > New Report.
Figure 11-20 Generate Reports

Monitoring > Reporting

Dashboard | Custom Reports | Configuration
New Report | Saved Templates | Executive Summary

New Report
Report Type: Compliant Machines
Report Format: html

Optional Fields:
- Role
- CAS
- User
- Sys User
- Sys Name
- O/S
- Report Time
- VLAN
- Switch IP

Filters
Add Filter... Generate Report Reset Save Template As

Schedule Future Report Generation
START DATE | TIME | FREQUENCY | NEXT SCHEDULED RUN
24-May-2011 | 5:51 | Monthly | Schedule

Report Type | Format | Frequency | NEXT SCHEDULED RUN
--- | --- | --- | ---
COMPLIANT MACHINES | html | OneTime | Thu Mar 25 06:34:00 PDT 2010
COMPLIANT MACHINES | html | Monthly | Wed Jun 08 06:04:00 PDT 2011
COMPLIANT MACHINES | html | Monthly | Wed Jun 08 06:04:00 PDT 2011
COMPLIANT MACHINES | html | Monthly | Wed Jun 08 06:04:00 PDT 2011
OS_INFO | html | Monthly | Fri Jun 10 06:10:00 PDT 2011

Reports Previously Generated
Report Type | Format | TIME REPORT RUN | DELETE
--- | --- | --- | ---
OS_INFO | html | 05-10-11 06:10-0700 | X
COMPLIANT MACHINES | html | 05-09-11 06:10-0700 | X
COMPLIANT MACHINES | html | 05-09-11 06:10-0700 | X
COMPLIANT MACHINES | html | 05-09-11 06:10-0700 | X
OS_INFO | html | 04-10-11 06:12-0700 | X
COMPLIANT MACHINES | html | 04-09-11 06:12-0700 | X
COMPLIANT MACHINES | html | 04-09-11 06:12-0700 | X
COMPLIANT MACHINES | html | 04-09-11 06:12-0700 | X
COMPLIANT MACHINES | html | 03-10-11 05:11-0860 | X
OS_INFO | html | 03-09-11 06:10-0860 | X
COMPLIANT MACHINES | html | 03-09-11 06:09-0860 | X
COMPLIANT MACHINES | html | 03-09-11 06:03-0860 | X

Note: Login Time and Report Time is not considered for the Scheduling Report and Save Template options.
Note: VID is available only for the VGW or IP Managed topologies.
Generating a Report

Under the New Report panel, you can select the Report Type and the required Report Format from the dropdown.

Report Type—Select the type of report from the drop-down list. For each type of the report, a set of fields are included in the report by default. You can include the other information to the report by checking the fields that are available under Optional Fields.

You can select a Filter from the dropdown and the report is filtered by the selected option. The Filter by option varies for each Report Type.

Table 11-2 lists the default, optional, and filter by fields available for each report type.

<table>
<thead>
<tr>
<th>Report Type</th>
<th>Mandatory Fields</th>
<th>Optional Fields</th>
<th>Filter-by Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliant Machines</td>
<td>IP Address, MAC Address, Login Time</td>
<td>Role, CAS, User, Sys User, Sys Name, O/S, Report Time, VLAN, Switch IP</td>
<td>All the default and optional fields</td>
</tr>
<tr>
<td>Non Compliant Machines</td>
<td>IP Address, MAC Address, Login Time</td>
<td>Role, CAS, User, Sys User, Sys Name, O/S, Report Time, VLAN, Switch IP</td>
<td>All the default and optional fields</td>
</tr>
<tr>
<td>Non Compliant Requirements</td>
<td>Requirement, MAC Address</td>
<td>User, Report time</td>
<td>All the default and optional fields</td>
</tr>
<tr>
<td>Non Compliant Users</td>
<td>MAC Address, User, Frequency</td>
<td>None</td>
<td>MAC address and User</td>
</tr>
<tr>
<td>A/V and A/S information</td>
<td>AV/AS Type, Product ID, User</td>
<td>Client IP, Sys Name, Software Version, Def Version, Def Date</td>
<td>All the default and optional fields</td>
</tr>
<tr>
<td>O/S Information</td>
<td>MAC Address, Sys Name, O/S, Report time</td>
<td>None</td>
<td>All the default fields</td>
</tr>
<tr>
<td>Missing A/V and A/S Requirements</td>
<td>User, Client IP, MAC Address, Report time</td>
<td>Software Version, Def Version, Def Date</td>
<td>Report time and all the optional fields</td>
</tr>
<tr>
<td>User Specific (Enter the User name in the text box that appears when you select this option)</td>
<td>Login time, Client IP, MAC Address, login success/failure flag</td>
<td>Role, Sys Name, Report time</td>
<td>All the default and optional fields</td>
</tr>
<tr>
<td>Requirement Specific (Select the Requirement from the dropdown that appears when you select this option)</td>
<td>Client IP, User Name, Success/Fail flag, Report time</td>
<td>MAC Address, Sys Name, Requirement Status</td>
<td>All the default and optional fields</td>
</tr>
</tbody>
</table>
Chapter 11  Monitoring and Troubleshooting Agent Sessions

Report Settings

Table 11-2  Report Types and the Fields Included (continued)

<table>
<thead>
<tr>
<th>Report Type</th>
<th>Mandatory Fields</th>
<th>Optional Fields</th>
<th>Filter-by Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role Specific Reports</td>
<td>Login status, User, Client IP, Requirement</td>
<td>Sys Name, Login Time, MAC Address, Requirement Status, Report time</td>
<td>All the default and optional fields</td>
</tr>
<tr>
<td>(Select the Role from the dropdown that appears when you select this option)</td>
<td>For each record, a link is available to view the failed and passed requirements, and the requirements in Audit / Mandatory / Optional mode.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Controlled Switch Ports 2</td>
<td>Switch IP, Port Name, User IP</td>
<td>Port Number, Port Description, Port Profile, User MAC Address, User Name</td>
<td>All the default and optional fields</td>
</tr>
</tbody>
</table>

1. Mandatory fields would always be part of the generated report.
2. The report is generated only when there is a maximum of 50 switches are available. If you have more than 50 switches in the network, filter the report by using the Switch IP field.

Format—Select the format of the output report file. The options available are HTML and PDF.

After selecting the Report Type, Report Format, and Filter, you can perform the following actions:

- Click Generate Report to generate and view the report immediately.
- Click Reset to remove the filters.
- Enter a name for the report and click Save Template As to save the current settings as a template.

Scheduling Report Generation

You can schedule to generate a report in future by setting up the date and time.

- Start Date—Enter the date on which the report generation has to start.
- Time—Enter the time at which the report generation has to start.
- Frequency—Select the frequency of the report generation from the drop-down list. The options available are: One Time, Hourly, Daily, Weekly, and Monthly.

Once you select the above parameters, click the Schedule button and the following are displayed:

- Report Type
- Format
- Frequency
- Next scheduled run

The reports are generated with the currently selected Report Type and the Report Format at the scheduled time. The previously generated reports are displayed at the bottom of the page.

Note

A maximum of 500 reports are displayed under the Reports Previously Generated section.
Note

Login Time and Report Time Start Date and End Date under report Filters are not considered for Scheduled Report and Saved Template.
View Saved Templates

You can view the saved templates by navigating to Monitoring > Reporting > Custom Reports > Saved Templates.

**Figure 11-21  Saved Templates**

<table>
<thead>
<tr>
<th>Template Name</th>
<th>Report Type</th>
<th>Format</th>
<th>Selected Fields</th>
<th>Filtered Fields</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rpt1</td>
<td>Compliant Machines</td>
<td>html</td>
<td>Role, User, OS, VLAN, ReportTime, SysUser, SysName, SwitchIP, CAS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>template1</td>
<td>Compliant Machines</td>
<td>html</td>
<td>User, Role, OS, VLAN, SysUser, CAS</td>
<td>IP, MAC, User, Role</td>
<td></td>
</tr>
</tbody>
</table>

Clicking the Template Name navigates to the New Report tab and the saved report settings are displayed.

View Executive Summary

It displays the current license usage - number of CASs in use versus the allowed license limit, peak user count in the last 24 hrs versus the allowed license limit. It also displays the role-wise compliance statistics summary - how many users failed login and how many passed login. Go to Monitoring > Reporting > Custom Reports > Executive Summary to view a report of the NAC License Utilization and Role-wise compliance statistics as shown in Figure 11-22.

**Figure 11-22  Executive Summary**
**Configuration**

Use the Monitoring > Reporting > Configuration tab to enable Dashboard and Custom Reports.

**Figure 11-23 Configuration**

- Check the **Enable Dashboard and related tasks** checkbox to enable the Dashboard page.
- Check the **Enable User Activity Logging** checkbox to save the user information in the User Activity Log (UAL) files.
  - Enabling **Include Posture Report** in UAL logging seriously impacts system performance.
- Role based user statistics collection: NAC periodically collects role-wise user count statistics. Choose the **Collection Span** and **Collection frequency** for role-wise statistics collection. Statistics collected by NAC is used to generate the user summary chart in the main dashboard (current status page).
  - Choose the period of time for the **Collection Span**. The User Statistics is displayed for the selected period. Choose the **Collection frequency** and the User Statistics is refreshed at the interval of the selected frequency.
- Check **Enable reports scheduling** to enable scheduling of reports in the Custom Reports tab. Click **Update** to save the settings.

**User Activity Log Files**

User Activity Log (UAL) Files are the log files that record user activities. This is an XML file stored in the location: `/perfigo/control/data/ual/`. The user information is stored in this file only when the **Enable User Activity Logging** checkbox is enabled in the Monitoring > Reporting > Configuration tab. The data is logged according to the period of interval set in the Current Status tab.
The UAL files are updated with the user information every day and the historical data for the past 90 days are available in the file.

The following details are stored in the UAL files:

- Username
- Activity Time—login time, logout time, or role change time
- Activity Reason—Reason for logout. The reasons may be “Logout”, “Timeout”, or “Admin Action”
- User Location—VPN, switch, port, VLAN, etc. (whatever is applicable)
- User Reports—Applicable for login and role change, not on logout
- Activity Result—The result is reported as success or failure. If activity fails, it means the login has failed. Activity Reason is supplied with the appropriate agent, authentication server, or switch management error
- MAC address
- Hostname
- IP address
- Role
- OS
- VLAN
- Session Length—For role change and logout only (applicable for only In-Band deployments). Session Length is a pre-configured value for the temporary role configured under User Management > User Roles> Schedule.

Note: Session Length will not be displayed in the Logout activity when the client is logged out from a Temporary Role after failing to satisfy a requirement.

Note: The UAL file is not updated when the Enable User Activity Logging checkbox is unchecked in the Monitoring > Reporting > Configuration tab.

---

**Online Users list**

Two Online Users lists are viewed from the Monitoring > Online Users > View Online Users tab:

- **In-Band Online Users**
  - Tracks In-Band authenticated users logged into the network. In-Band users with active sessions on the network are listed by characteristics such as IP address, MAC address (if available), authentication provider, and user role.
  - Removing a user from the In-Band Online Users list logs the user off of the In-Band network.

- **Out-of-Band Online Users**
  - Tracks all authenticated Out-of-Band users that are on the Access VLAN (trusted network). Out-of-Band users can be listed by switch IP address, port, and assigned Access VLAN, in addition to client IP address, MAC address (if available), authentication provider, and user role.
Removing a user from the Out-of-Band Online Users list causes the VLAN of the port to be changed from the Access VLAN to the Authentication VLAN. You can additionally configure the Port profile to bounce the port (for a Real-IP gateway). See Out-of-Band Users, page 11-32 and Out-of-Band Users, page 3-70 for details.

Both Online Users lists are based on the IP address of users. Note that:

- For Layer 2 deployments the User MAC address field is valid
- For Layer 3 deployments the User MAC address field is not valid (for example, 00:00:00:00:00:00)

Only the Certified Devices List is based on client MAC addresses, and therefore the Certified Devices List never applies to users in Layer 3 deployments.

For Out-of-Band deployments, OOB user entries always appear first in the In-Band Online Users list, then in the Out-of-Band Online Users list. When user traffic is coming from a controlled port of a managed switch, the user shows up first in the In-Band Online Users list during the authentication process, then is moved to the Out-of-Band Online Users list after the user is authenticated and moved to the Access VLAN.

Finally, the Display Settings tab let you choose which user characteristics are displayed on each respective Online Users page.

**Note**

When a user device is connecting to Cisco NAC Appliance from behind a VPN3000/ASA device, the MAC address of the first physical adapter that is available to the CAS/CAM is used to identify the user on the Online Users list. This may not necessarily be the adapter with which the user is connecting to the network. Users should **disable** the wireless interface of their machines when connecting to the network using the wired (Ethernet card) interface.

---

## Interpreting Active Users

Once logged onto the Cisco NAC Appliance network, an active user session persists until one of the following events occurs:

- The user logs out of the network through the browser logout page or Agent logout.
  
  Once on the network, users can remain logged on after a computer shutdown/restart. A user can log out of the network using the web logout page or Agent logout.

- The Agent user logs off Windows or shuts down Windows machine.
  
  You can configure the CAM and Agent to log off In-Band users only from the Clean Access system when the user logs off from the Windows domain (i.e. **Start > Shutdown > Log off current user**) or shuts down the machine (**Start > Shutdown > Shutdown machine**).

- An administrator manually drops the user from the network.
  
  The Monitoring > Online Users > View Online Users page (IB or OOB) can be used to drop users from the network, without deleting their clients from the Certified Devices List.

- The session times out using the Session Timer.
  
  The Session Timer works the same way for multi-hop L3 (IB) deployments as for L2 (IB or OOB) deployments and is set in User Management > User Roles > Schedule > Session Timer. It is set per user role, and logs out any user in the selected role from the network after the configured time has elapsed. For details, see Configure Session Timer (per User Role), page 8-17.

- The CAS determines that the user is no longer connected using the Heartbeat Timer and the CAM terminates the session.
The Heartbeat Timer applies to L2 IB deployments only and is set for all users regardless of role. It can be set globally for all Clean Access Servers using the form **User Management > User Roles > Schedule > Heartbeat Timer**, or for a specific Clean Access Server using the local form **Device Management > CCA Servers > Manage [CAS_IP] > Misc > Heartbeat Timer**. For details, see **Configure Heartbeat Timer (User Inactivity Timeout)**, page 8-18.

The Heartbeat Timer will not function in L3 deployments, and does not apply to OOB users. However, note that the HeartBeat Timer will work if the CAS is the first hop behind the VPN concentrator. This is because the VPN concentrator responds to the ARP queries for the IP addresses of its current tunnel clients.

- The Certified Device list is cleared (automatically or manually) and the user is removed from the network.

The Certified Devices List applies to L2 (IB or OOB) deployments only and can be scheduled to be cleared automatically and periodically using the global Certified Devices timer form (**Device Management > Clean Access > Certified Devices > Timer**). You can manually clear the certified devices for a specific Clean Access Server from the Certified Devices List using the local form **Device Management > CCA Servers > Manage [CAS_IP] > Filters > Clean Access > Certified Devices**, or manually clear the Certified Device list across all Clean Access Servers using the global form **Device Management > Clean Access > Certified Devices**. For details, see **Manage Certified Devices**, page 11-10.

Keep in mind that the Certified Devices List will not display remote VPN/L3 clients (since these sessions are IP-based rather than MAC address-based).

- SSO and Auto-Logout are configured for the VPN concentrator, and the user disconnects from the VPN.

With Auto Logout enabled, when the user disconnects from the VPN client, the user is automatically removed from the Online Users list (In-Band).

Note that when SSO is configured for multi-hop L3 VPN concentrator integration, if the user’s session on the CAS times out but the user is still logged in on the VPN concentrator, the user will be able to log back into the CAS without providing a username/password.

---

### Note

Whether the CAS or another server is used for DHCP, if a user’s DHCP lease expires, the user remains on the Online Users list (In-Band or Out-of-Band). When the lease expires, the client machine will try to renew the lease.

See also **Configure User Session and Heartbeat Timeouts**, page 8-15 and **Out-of-Band Users**, page 3-70 for additional details.

---

## View Online Users

The **View Online Users** tab provides two links for the two online users lists: **In-Band** and **Out-of-Band**.

By default, **View Online User** pages display the login user name, IP and MAC address (if available), provider, and role of each user. For information on selecting the column information to display, such as OS version, or for Out-of-Band users: switch port, see **Display Settings**, page 11-36.

A **green** background for an entry indicates a user device accessing the Clean Access network in a temporary role: either a Quarantine role or the Agent Temporary role.

A **blue** background for an entry indicates a user device accessing the Clean Access network in a restricted network access role.
A device listed on the **View Online Users** page but not in the Clean Access **Certified Devices List** generally indicates the device is in the process of certification.

### In-Band Users

Clicking the **In-Band** link brings up the **View Online Users** page for In-Band users ([Figure 11-24](#)). The In-Band Online Users list tracks the In-Band users logged into the Clean Access network.

The Clean Access Manager adds a client IP and MAC address (if available) to this list after a user logs into the network either through web login or the Agent.

Removing a user from the Online Users list logs the user off the In-Band network.

**Figure 11-24 View Online Users Page—In-Band**

Note For AD SSO users, the **Provider** field displays **AD_SSO**, and the **User/User Name** field lists both the username and domain of the user (for example, **user1@domain.name.com**.) on the **Online Users** and **Certified Devices** pages.

### Out-of-Band Users

Clicking the **Out-of-Band** link brings up the **View Online Users** page for Out-of-Band users ([Figure 11-25](#)).

The Out-of-Band Online Users list tracks all Out-of-Band authenticated users that are on the Access VLAN (on the trusted network). The CAM adds a user IP address to the Out-of-Band Online Users list after a client is switched to the Access VLAN.

Note The “**User IP**” of Out-of-Band online users will be the IP address of the user on the Authentication VLAN. By definition CCA does not track users once they are on the Access VLAN; therefore OOB users are tracked by the Auth VLAN IP address they have while in the CCA network.

When a user is removed from the Out-of-Band Online Users list, the following typically occurs:

1. The CAM bounces the switch port (off and on).
2. The switch resends SNMP traps to the CAM.
3. The CAM changes the VLAN of the port based on the configured Port Profile associated with this controlled port.
Removing an OOB user from the Certified Devices List also removes the user from Out-of-Band Online Users list and changes the port from the Access VLAN to the Auth VLAN.

When the “Remove Out-of-Band online user without bouncing port” option is checked for the Port Profile, for OOB Virtual Gateways, the switch port will not be bounced when:

- Users are removed from the Out-of-Band Online Users list, or
- Devices are removed from the Certified Devices list

Instead, the port Access VLAN will be changed to the Authentication VLAN (see Add Port Profile, page 3-34 for details).

**Figure 11-25  View Online Users Page—Out-of-Band**

For AD SSO users, the Provider field displays AD_SSO, and the User/User Name field lists both the username and domain of the user (for example, user1@domain.name.com) on the Online Users and Certified Devices pages.

For more details, see Chapter 3, “Switch Management: Configuring Out-of-Band Deployment.”

**Table 11-3** View Online Users Page Controls

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>The user name used for login is displayed.</td>
</tr>
</tbody>
</table>
Table 11-3  View Online Users Page Controls

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Criteria:</td>
<td></td>
</tr>
<tr>
<td>CCA Server</td>
<td>• Any Clean Access Server</td>
</tr>
<tr>
<td></td>
<td>• &lt;specific CAS IP address&gt;</td>
</tr>
<tr>
<td>Provider</td>
<td>• Any Provider</td>
</tr>
<tr>
<td></td>
<td>• &lt;specific authentication provider&gt;</td>
</tr>
<tr>
<td>Role</td>
<td>• Any Role</td>
</tr>
<tr>
<td></td>
<td>• Unauthenticated Role</td>
</tr>
<tr>
<td></td>
<td>• Temporary Role</td>
</tr>
<tr>
<td></td>
<td>• Quarantine Role</td>
</tr>
<tr>
<td></td>
<td>• &lt;specific Role&gt;</td>
</tr>
<tr>
<td>Location</td>
<td>• Any Switch or Wireless LAN Controller</td>
</tr>
<tr>
<td></td>
<td>• &lt;specific switch/WLC IP address&gt;</td>
</tr>
<tr>
<td>Select Field</td>
<td>• User Name</td>
</tr>
<tr>
<td></td>
<td>• IP Address</td>
</tr>
<tr>
<td></td>
<td>• MAC Address</td>
</tr>
<tr>
<td>Operator</td>
<td>equals: Search text value must be an exact match for this operator</td>
</tr>
<tr>
<td></td>
<td>starts with:</td>
</tr>
<tr>
<td></td>
<td>ends with:</td>
</tr>
<tr>
<td></td>
<td>contains</td>
</tr>
<tr>
<td>Search Text</td>
<td>Enter the value to be searched using the operator selected.</td>
</tr>
<tr>
<td>Controls:</td>
<td></td>
</tr>
<tr>
<td>View</td>
<td>After selecting the search criteria, click View to display the results.</td>
</tr>
<tr>
<td></td>
<td>You can view users by CAS, provider, user role, user name, IP address,</td>
</tr>
<tr>
<td></td>
<td>MAC address (if available), or switch (OOB only).</td>
</tr>
<tr>
<td>Reset View</td>
<td>Resets to the default view (with search criteria reset to “Any”)</td>
</tr>
<tr>
<td>Kick Users</td>
<td>Clicking Kick Users terminates all user sessions filtered through the</td>
</tr>
<tr>
<td></td>
<td>search criteria across the number of applicable pages. Users can be</td>
</tr>
<tr>
<td></td>
<td>selectively dropped from the network by any of the search criteria used to</td>
</tr>
<tr>
<td></td>
<td>View users. The “filtered users indicator” shown in Figure 11-25 displays</td>
</tr>
<tr>
<td></td>
<td>the total number of filtered users that will be terminated when Kick Users</td>
</tr>
<tr>
<td></td>
<td>is clicked.</td>
</tr>
<tr>
<td>Reset Max Users</td>
<td>Resets the maximum number of users to the actual number of users displayed</td>
</tr>
<tr>
<td></td>
<td>in the “Active users:” status field (Figure 11-25)</td>
</tr>
<tr>
<td>Delete Checked Entries</td>
<td>You can remove as many users as are shown on the page by selecting the</td>
</tr>
<tr>
<td></td>
<td>checkbox next to each user and clicking the Delete Checked Entries Icon.</td>
</tr>
<tr>
<td>Navigation:</td>
<td></td>
</tr>
<tr>
<td>First/Previous/Next/Last</td>
<td>These navigation links allow you to page through the list of online users.</td>
</tr>
<tr>
<td></td>
<td>A maximum of 25 entries is displayed per page.</td>
</tr>
</tbody>
</table>
View Users by Clean Access Server, Authentication Provider, or Role

1. From the View Online Users page, select a specific Clean Access Server, or leave the first field as Any CCA Server.
2. Select a specific authentication provider, or leave as Any Provider.
3. Select a specific user role, or leave as Any Role.
4. Click View to display users by Clean Access Server, provider, role or any combination of the three.

Search by User Name, IP, or MAC Address

1. In the Select Field dropdown menu next to Search For:, select User Name or IP Address or MAC Address.
2. Select one of the four operators: starts with, ends with, contains, exact match.
3. Enter the text to be searched in the Search For: text field. If using the exact match operator, only the exact match for the search text entered is returned.
4. Click View to display results.

Log Users Off the Network

Clicking Kick Users terminates all user sessions filtered through the search criteria across the number of applicable pages. (Note that a maximum of 25 entries is displayed per page.) You can selectively remove users from the network by any of the search criteria used to View users. The “filtered users indicator” shown in Figure 11-24 displays the total number of filtered user sessions that will be terminated when you click the Kick Users button.

1. Go to Monitoring > Online Users > View Online Users.
2. To terminate user sessions either:
   - Drop all users (filtered through search criteria) from the network by clicking Kick Users
   - Drop individual users by selecting the checkbox next to each user and clicking the Delete Checked Entries Icon.

Note that removing a user from the online users list (and the network) does not remove the user from the Certified Devices List. However, dropping a user from the Certified Devices List also logs the user off the network. See Clear Certified or Exempt Devices Manually, page 11-13 for further details.

---

Note

When there is a large number Out-of-Band Online Users, then the Kick User option takes a longer time to remove the online users. This happens when switches and CASs are not available to the CAM, resulting in a timeout for each communication failure. The Kick User is slow due to this timeout.
Display Settings

Figure 11-26 shows the Display Settings page for In-Band users.

**Figure 11-26  Display Settings—In-Band**

Select the online user information to be displayed:
- IP
- MAC
- Provider
- Role
- CCA Server
- VLAN
- OS
- Login Time

<table>
<thead>
<tr>
<th>IP address of the user</th>
<th>MAC address (ethernet address) of the user</th>
<th>Provider that authenticated the user</th>
<th>Role of the user</th>
<th>IP address of the Clean Access Server to which the user originally logged in</th>
<th>The user’s VLAN ID</th>
<th>Operating system of the user</th>
<th>Time when the user logged in</th>
<th>Green shading denotes a Clean Access quarantined user</th>
<th>Blue shading denotes a Clean Access restricted access user</th>
</tr>
</thead>
</table>

**Note**

Role—the role assigned to the user upon login.

Figure 11-27 shows the Display Settings page for Out-of-Band users.
Figure 11-27  Display Settings—Out-of-Band

To choose what information is displayed on the View Online Users page:

Step 1  Click the Display Settings tab.
Step 2  Select the check box next to an item to display it in the list.
Step 3  Click Update.
Step 4  Click the View Online Users tab to see the desired settings displayed.

Agent Troubleshooting

This section contains the following:

- Debug Logging for Cisco NAC Appliance Agents
- Client Cannot Connect/Login
- No Agent Pop-Up/Login Disabled
- Client Cannot Connect (Traffic Policy Related)
- AV/AS Rule Troubleshooting
- Cisco NAC Web Agent Status Codes
- Known Issue for Windows Script 5.6
- Known Issue for MS Update Scanning Tool (KB873333)
Debug Logging for Cisco NAC Appliance Agents

This section describes how to view and/or enable debug logging for Cisco NAC Appliance Agents. Refer to the following sections for steps for each Agent type:

- Generate Cisco NAC Agent Debug Logs
- Cisco NAC Web Agent Logs
- Generate Mac OS X Agent Debug Log

Copy these event logs to include them in a customer support case.

Generate Cisco NAC Agent Debug Logs

To generate Cisco NAC Agent logs using the Cisco Log Packager utility, refer to Create Agent Log Files Using the Cisco Log Packager, page 11-6.

Cisco NAC Web Agent Logs

The Cisco NAC Web Agent version 4.1.3.9 and later can generate logs when downloaded and executed. By default, the Cisco NAC Web Agent writes the log file upon startup with debugging turned on. The Cisco NAC Web Agent generates the following log files for troubleshooting purposes: `webagent.log` and `webagentsetup.log`. These files should be included in any Cisco Technical Assistance Center (TAC) support case for the Web Agent. Typically, these files are located in the user’s temp directory, in the form:

```
C:\Document and Settings\<user>\Local Settings\Temp\webagent.log
C:\Document and Settings\<user>\Local Settings\Temp\webagentsetup.log
```

If these files are not visible, check the TEMP environment variable setting. From a command-prompt, type “echo %TEMP%” or “cd %TEMP%”.

When the client uses Microsoft Internet Explorer, the Cisco NAC Web Agent is downloaded to the `C:\Documents and Settings\<user>\Local Settings\Temporary internet files` directory.

Generate Mac OS X Agent Debug Log

For Mac OS X Agents, the Agent `event.log` file and `preference.plist` user preferences file are available under `<username> > Library > Application Support > Cisco Systems > CCAAgent.app`. To change or specify the LogLevel setting, however, you must access the global `setting.plist` file (which is different from the user-level `preference.plist` file).

Because Cisco does not recommend allowing individual users to change the LogLevel value on the client machine, you must be a superuser or root user to alter the global `setting.plist` system preferences file and specify a different Agent LogLevel.

Note

For versions prior to 4.1.3.0, debug logging for the Mac OS X Agent is enabled under `<local drive ID> > Library > Application Support > Cisco Systems > CCAAgent.app > Show Package Contents > setting.plist`.

To view and/or change the Agent LogLevel:

Step 1
Open the navigator pane and navigate to `<local drive ID> > Applications.`
Step 2  Highlight and right-click the CCAAgent.app icon to bring up the selection menu.

Step 3  Choose Show Package Contents > Resources.

Step 4  Choose setting.plist.

Step 5  If you want to change the current LogLevel setting using Mac Property Editor (for Mac OS 10.5 and later), find the current LogLevel Key and replace the exiting value with one of the following:

- **Info**—Include only informational messages in the event log
- **Warn**—Include informational and warning messages in the event log
- **Error**—Include informational, warning, and error messages in the event log
- **Debug**—Include all Agent messages (including informational, warning, and error) in the event log

**Note**  The Info and Warn entry types only feature a few messages pertaining to very specific Agent events. Therefore, you will probably only need either the Error or Debug Agent event log level when troubleshooting Agent connection issues.

**Note**  Because Apple, Inc. introduced a binary-format .plist implementation in Mac OS 10.4, the .plist file may not be editable by using a common text editor such as vi. If the .plist file is not editable (displayed as binary characters), you either need to use the Mac Property List Editor utility from the Mac OS X CD-ROM or acquire another similar tool to edit the setting.plist file.

Property List Editor is an application included in the Apple Developer Tools for editing .plist files. You can find it at <CD-ROM>/Developer/Applications/Utilities/Property List Editor.app.

If the setting.plist file is editable, you can use a standard text editor like vi to edit the LogLevel value in the file.

You must be the root user to edit the file.

---

**Client Cannot Connect/Login**

The following client errors at login can indicate CAM/CAS certificate related issues (i.e. the CAS does not trust the certificate of the CAM, or vice-versa):

- Users attempting web login continue to see the login page after entering user credentials and are not redirected.
- Users attempting Agent login see the following error: “Clean Access Server could not establish a secure connection to the Clean Access Manager at <IPaddress or domain>.

To resolve these issues, refer to Troubleshooting Certificate Issues, page 14-21.

**No Agent Pop-Up/Login Disabled**

For L2 or L3 deployments, the Agent will pop up on the client if “Popup Login Window” is enabled on the Agent and the Agent detects it is behind the Clean Access Server. If the Agent does not pop up, this indicates it cannot reach the CAS.
Agent Troubleshooting

Chapter 11 Monitoring and Troubleshooting Agent Sessions

To Troubleshoot L2 Deployments:
1. Make sure the client machine can get a correct IP address. Open a command tool (Start > Run > cmd) and type `ipconfig` or `ipconfig /all` to check the client IP address information.
2. If necessary, type `ipconfig /release`, then `ipconfig /renew` to reset the DHCP lease for the client.

To Troubleshoot L3 Deployments:
1. Check whether the Discovery Host field is set to the IP address of the CAM itself under Device Management > Clean Access > Clean Access Agent > Installation | Discovery Host. This field must be the address of a device on the trusted side and cannot be the address of the CAS.
2. Uninstall the Agent from the client machine.
3. Change the Discovery Host field to the IP address of the CAM and click Update.
4. Reboot the CAS.
5. Re-download and re-install the Agent on the client.

Note
The Login option on the Agent is correctly disabled (greyed out) in the following cases:
- For OOB deployments, the Agent user is already logged in through the CAS and the client port is on the Access VLAN.
- For multi-hop L3 deployments, Single Sign-On (SSO) has been enabled and the user has already authenticated through the VPN concentrator (therefore is already automatically logged into Cisco NAC Appliance).
- MAC address-based authentication is configured for the machine of this user and therefore no user login is required.

Client Cannot Connect (Traffic Policy Related)

The following errors can indicate DNS, proxy or network traffic policy related issues:
- User can login via Agent, but cannot access web page/Internet after login.
- User cannot access web login page without typing in https://<CAS_IP_address> as the URL.

To troubleshoot these issues:
- Verify and/or change DNS Servers setting on the CAS (under Device Management > CCA Servers > Manage <CAS_IP> > Network > DNS)
- If enabling the CAS as a DHCP server, verify and/or change the DNS Servers field for the Subnet List (under Device Management > CCA Servers > Manage <CAS_IP> > Network > DHCP > Subnet List > List | Edit).
- If remediation sites cannot be reached after login, verify default host policies (Allowed Hosts) are enabled for the Temporary role (under User Management > User Roles > Traffic Control > Host).
- If using a proxy server, make sure a traffic policy allowing HTTP traffic to the proxy server is enabled for the Temporary role. Verify the proxy is correctly set in the browser (from IE go to Tools > Internet Options > Connections > LAN Settings | Proxy server).

See Troubleshooting Host-Based Policies, page 8-30 for additional details.
AV/AS Rule Troubleshooting

To view administrator reports for the Agent, go to Device Management > Clean Access > Clean Access Agent > Reports. To view information from the client, right-click the Agent taskbar icon and select Properties.

When troubleshooting AV/AS Rules, please provide the following information:

1. Version of CAS, CAM, and Agent.
2. Client OS version (e.g. Windows XP SP2)
3. Name and version of AV/AS vendor product.
4. What is failing—AV/AS installation check or AV/AS update checks? What is the error message?
5. What is the current value of the AV/AS def date/version on the failing client machine?
6. What is the corresponding value of the AV/AS def date/version being checked for on the CAM? (See Device Management > Clean Access > Clean Access Agent > Rules > AV/AS Support Info.)

Cisco NAC Web Agent Status Codes

Table 11-4 shows the status codes passed from the ActiveX or Java Applet downloader used to install the Cisco NAC Web Agent on the client machine.

<table>
<thead>
<tr>
<th>ActiveX/Java Applet Status Code</th>
<th>Value/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACTIVEX_FAILURE</td>
<td>-1 “unable to launch active-x control”</td>
</tr>
<tr>
<td>DL_FAILURE</td>
<td>-2 “failed to download the web agent executable”</td>
</tr>
<tr>
<td>EXE_FAILURE</td>
<td>-3 “there was an error running the web agent”</td>
</tr>
<tr>
<td>ACTIVEX_START</td>
<td>0</td>
</tr>
<tr>
<td>STATUS_DL_START</td>
<td>1</td>
</tr>
<tr>
<td>DL_IN_PROGRESS</td>
<td>2</td>
</tr>
<tr>
<td>EXE_IN_PROGRESS</td>
<td>3</td>
</tr>
</tbody>
</table>

Table 11-5 shows the status codes passed from the Cisco NAC Web Agent back to the Cisco NAC Appliance system during posture assessment and remediation.

<table>
<thead>
<tr>
<th>Cisco NAC Web Agent Status Code</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMPLIANT/SUCCESS</td>
<td>32</td>
</tr>
<tr>
<td>NON_COMPLIANT</td>
<td>33</td>
</tr>
<tr>
<td>REJECTED_AUP</td>
<td>34</td>
</tr>
<tr>
<td>REMEDIATION TIMEOUT</td>
<td>35</td>
</tr>
<tr>
<td>GENERAL ERROR</td>
<td>36</td>
</tr>
<tr>
<td>TEMPORARY/RESTRICTED ACCESS</td>
<td>37</td>
</tr>
<tr>
<td>WEB AGENT ALREADY RUNNING</td>
<td>38</td>
</tr>
</tbody>
</table>
Known Issue for Windows Script 5.6

Windows Script 5.6 is required for proper functioning of the Agent. Most older operating systems come with Windows Script 5.1 components. Microsoft automatically installs the new 5.6 component on performing Windows updates. Windows installer components 2.0 and 3.0 also require Windows Script 5.6. However, PC machines with a fresh install of Windows 2000 that have never performed Windows updates will not have the Windows Script 5.6 component. Cisco NAC Appliance cannot redistribute this component as it is not provided by Microsoft as a merge module/redistributable.

In this case, administrators will have to access the MSDN website to get this component and upgrade to Windows Script 5.6. For convenience, links to the component from MSDN are listed below:

Filename: scripten.exe

If these links change on MSDN, try a search for the file names provided above or search for the phrase “Windows Script 5.6.”

Known Issue for MS Update Scanning Tool (KB873333)

Background

KB873333 is a critical update that is required for Windows XP Professional and Home for SP1 and SP2. It fixes an OS vulnerability that can allow remote code to run. However, Microsoft had a bug in this hotfix which caused problems on SP2 editions (home/pro). This bug required another fix (KB894391), because KB873333 on SP2 caused a problem with displaying Double Byte Character Sets (DBCS). However, KB894391 does not replace KB873333, it only fixes the DBCS display issue.

Ideally, KB894391 should not be installed or shown in updates unless the user machine has KB873333. However, the MS Update Scanning Tool shows it irrespective of whether or not KB873333 is installed. In addition, if due to ordering of the updates, KB894391 is installed, the MS Update Scanning Tool does not show KB873333 as being installed, thereby leaving the vulnerability open. This could happen if the user does not install KB873333 and only selects KB894391 to install from the updates list shown or manually installs KB894391 without installing KB873333 first. In this case, the next time updates are run, the user will not be shown KB873333 as a required update, because the MS Update Scanning Tool (including MS Baseline Analyzer) will assume KB873333 is installed if KB894391 is installed, even if this is not true and the machine is still vulnerable.

Workaround

Because of this potential vulnerability, Cisco does not intend to remove the update check for KB87333 from the Clean Access ruleset and users should manually download and install KB873333 to protect their machines. This can be done in one of two ways:
Option 1 (Cisco Recommended Option)

Create a new Link requirement in the CAM web console to check for KB873333, using the following steps:

1. Create a rule to check for the presence of KB873333. To create this rule, go to the Rules section of the web console and click New Rule. Give the rule a name (e.g. “KB873333_Rule”), and for the rule expression, copy/paste the exact name of the KB873333 check from the list of checks displayed on that page (the list of available checks appear below the new rule creation section). Save the rule by clicking “Add Rule.”

2. Download the update executable for KB873333 from Microsoft’s website and host it on an available web server.

3. Create a Link Requirement on Cisco NAC Appliance, and enter the URL from step 2.

4. Create Requirement-Rules for this requirement by selecting the rule you created in step 1.

5. Finally, go to the Role-Requirements section, and associate the Requirement you just created with the role to which you want this to be applied.

Note
On the Requirements page, make sure that the KB873333 requirement is above the Windows Hotfixes requirement.

Option 2

Uninstall KB894391 from affected machines. After rebooting, go to the Windows Update page again. Windows Update should now display both the updates. Install KB873333 and KB894391 on the client machine. Note that this requires administrators to educate users or manually perform this task on the user machines.