61700544G1-29.4A
March 2010

ADTRAN

Configuration Guide

Configuring Desktop Auditing in AOS

This guide provides an overview of the desktop auditing feature and its operation in ADTRAN Operating System (AOS) products. Included in this guide are an overview of the desktop auditing functionality and how to configure desktop auditing using both the Web-based graphical user interface (GUI) and the command line interface (CLI). Also, included in this guide are desktop auditing configuration examples and troubleshooting information.

This guide includes the following information:

- *Desktop Auditing Overview on page 2*
- *Desktop Auditing in AOS on page 2*
- *Hardware and Software Requirements and Limitations on page 3*
- *Configuring Desktop Auditing Using the GUI on page 4*
- *Viewing Client NAP Information Using the GUI on page 9*
- *Configuring Desktop Auditing Using the CLI on page 13*
- *Viewing Client NAP Information Using the CLI on page 16*
- *Example Desktop Auditing Configuration on page 20*
- *Configuration Command Summary on page 21*
- *Troubleshooting on page 24*

Desktop Auditing Overview

Desktop auditing is an AOS feature that uses Dynamic Host Configuration Protocol (DHCP) in conjunction with the Microsoft® Network Access Protection (NAP) Protocol to monitor the health of client computers connected to an AOS network. The two protocols work together to ensure that systems connected to the network are using appropriate corporate policies, such as appropriate firewall settings, antivirus settings, and other client health information. This information is exchanged between clients and servers in statement of health (SoH) and statement of health response (SoHR) messages.

SoH messages include the state of the firewall, antivirus, and other health- and security-related information from a client computer. This information is collected on the client computer by the Microsoft Windows Security Health Agent (WSHA). Once the information is collected into an SoH message, if a client is configured to do NAP over DHCP the SoH message is encapsulated in DHCP messages sent between the client and the server. An AOS product within the network can monitor these messages to determine the SoH information included within the packet.

SoHR messages are server responses to client SoH messages. SoHR messages are created by a Windows Security Health Validator (WSHV) on the server when it receives the SoH messages from a client on the network. The WSHV contains configurable policies that determine the minimum allowed state for health- and security-related features on clients within the network. Based on the client's SoH messages and the policies held by the WSHV, a SoHR message is generated, indicating compliance or noncompliance with the policies for each health- and security-related feature.

Desktop Auditing in AOS

In AOS, desktop auditing functions by using DHCP as the carrier of SoH and SoHR messages so that NAP information can be collected. When desktop auditing is enabled, the AOS switch collects the NAP information of clients by monitoring DHCP messages exchanged between the server and the client. If the AOS product is also the DHCP server, it can be configured to advertise its NAP capability so that clients on the network will include SoH information in the DHCP messages. Figure 1 describes the exchange of SoH and SoHR messages using DHCP between the client and the server.

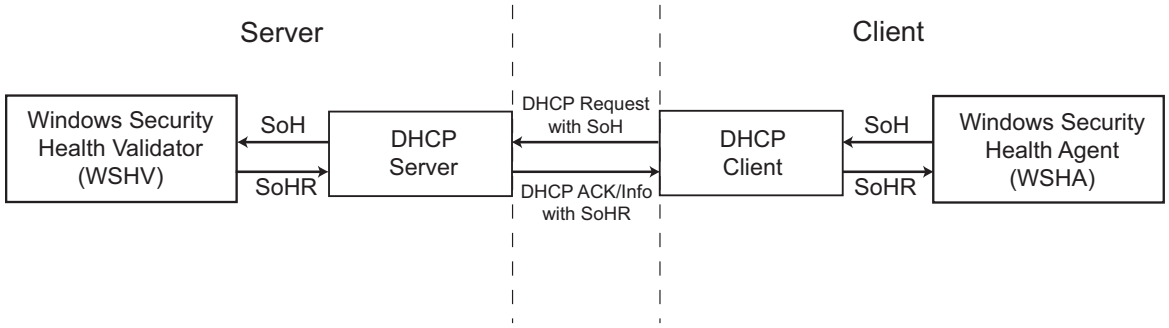


Figure 1. SoH and SoHR Messages Using DHCP Exchange

Desktop auditing is configured on AOS products by enabling the feature and by configuring filters to limit the output of the collected NAP information. When desktop auditing is enabled, the AOS product collects DHCP information, such as the medium access control (MAC) and IP addresses, virtual local area network (VLAN) ID, host name, and source port, as well as the MAC and IP addresses of the server and the date

and time of the last DHCP information update. The NAP information collected by desktop auditing includes the client's OS version and service pack, processor architecture, firewall name and state, antivirus name and state, antispyware name and state, automatic update configuration, security update information, and the NAP state (enabled or disabled) of both the server and the client.

NOTE *Not all clients provide all informational fields.*

The NAP information is collected and indexed by MAC addresses, to avoid multiple inputs for the same client, and up to 2000 NAP entries can be stored. Once the 2000 entry limit is reached, each new entry overwrites the older entries.

If the AOS product is acting as the DHCP server, the NAP DHCP server support can be configured on a per-pool basis. When NAP is enabled on a server pool and if a client's DHCP exchange includes a message indicating NAP support, then the AOS product will reply with NAP support indication in the DHCP offer message. If NAP is disabled on a server pool or a client's DHCP exchange does not indicate NAP support, then the AOS product will operate as normal without including any NAP information in its offer messages.

NOTE *Properly configured NAP-capable DHCP clients will not provide any SoH messages indicating the client's system health if the responding DHCP server does not indicate NAP support in its messages to the client.*

Hardware and Software Requirements and Limitations

Desktop auditing functions by monitoring DHCP exchanges. Only the NetVanta 1534 and NetVanta 1544 running AOS firmware release 17.08.01 or later are able to collect client NAP information through DHCP exchanges.

NAP capability is available on clients running Microsoft® Windows XP Service Pack 3 or later. ADTRAN does not provide customer support for NAP configuration on client PCs. For information on how to configure your PC to support NAP over DHCP, refer to your operating system manual.

AOS DHCP servers do not react to clients with invalid security settings. The AOS DHCP server can only advertise NAP capability to enable clients to provide SoH messages, indicating their system health and security.

Desktop auditing-capable AOS switches also do not react to clients with invalid security settings. Desktop auditing-capable switches only monitor exchange messages for SoH information and identify clients that have invalid security settings.

There is a storage limit of 2000 NAP entries. When the limit has been reached, new entries overwrite the oldest entries.

Desktop auditing collects both NAP and DHCP information for clients connected to the network. If you only want to collect DHCP information for connected clients, you have that option using the network forensics feature. For more information on this feature, refer to the *Configuring Network Forensics in AOS* configuration guide available online at http://kb.adtran.com.

Configuring Desktop Auditing Using the GUI

Desktop auditing can be configured using either the GUI or the CLI. To configure desktop auditing using the GUI, complete the following tasks:

- Enable desktop auditing.
- Specify the desktop auditing information timeout.
- Define the local policy for determining client health violations (optional).
- Enable NAP advertisements on DHCP server pools (if the AOS unit is acting as the network's DHCP server).

Enabling and Configuring Desktop Auditing

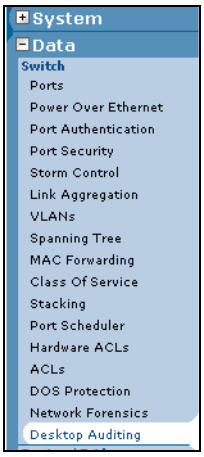
To begin configuring desktop auditing, you must first connect to the GUI. To connect to the GUI, follow these steps:

1. Open a new Web page in your Internet browser.
2. Enter your AOS product's IP address in the Internet browser's address field in the following form: **http://***<ip address>*.

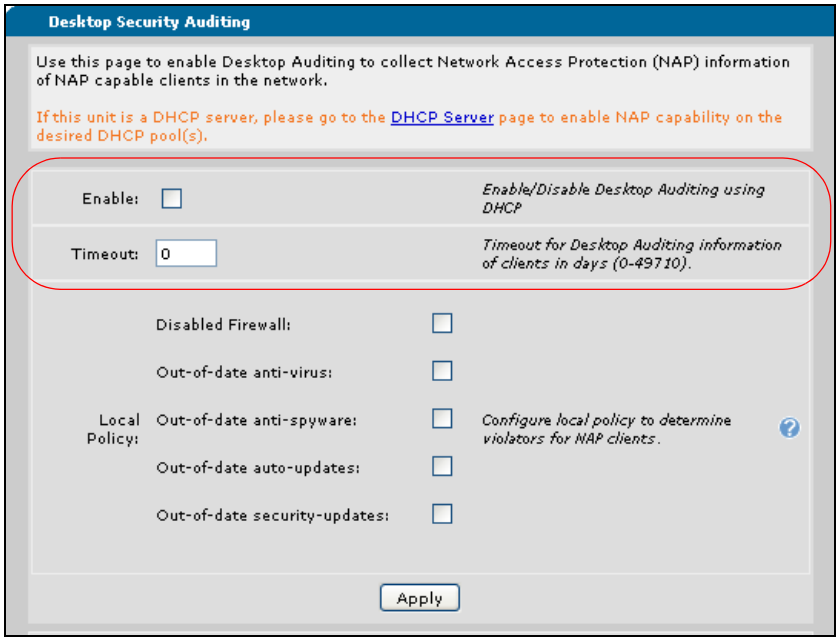
   For example: **http://65.162.109.200**
3. At the prompt, enter your user name and password and select **OK**.

NOTE *The default user name is **admin** and the default password is **password**.*

4. Navigate to **Data** > **Switch** > **Desktop Auditing**.



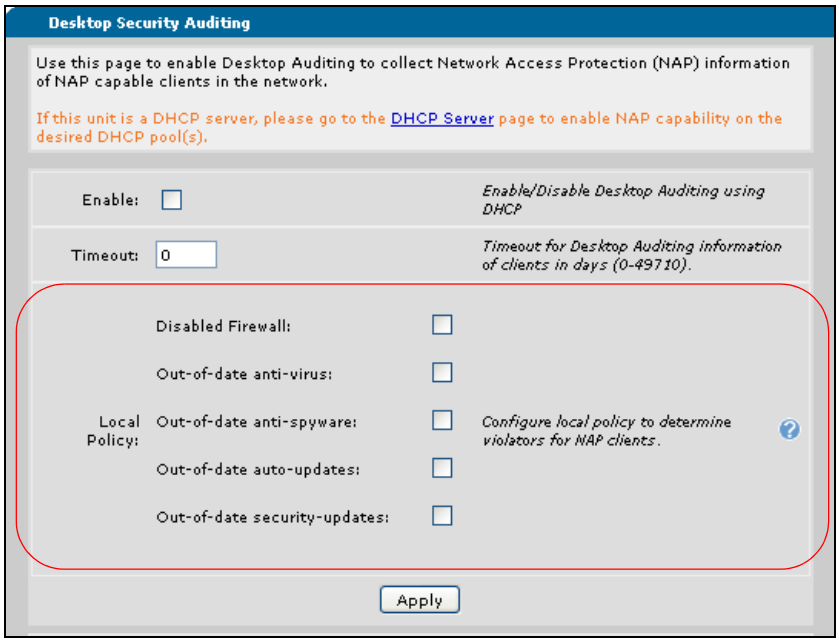
5. Enable desktop auditing by checking the box next to **Enable** (by default, desktop auditing is disabled). Next, specify the desktop auditing information timeout in the appropriate field. This parameter specifies the number of days that desktop auditing information is stored. The range is **0** to **49710** days, and the value of **0** indicates the information will be stored indefinitely.



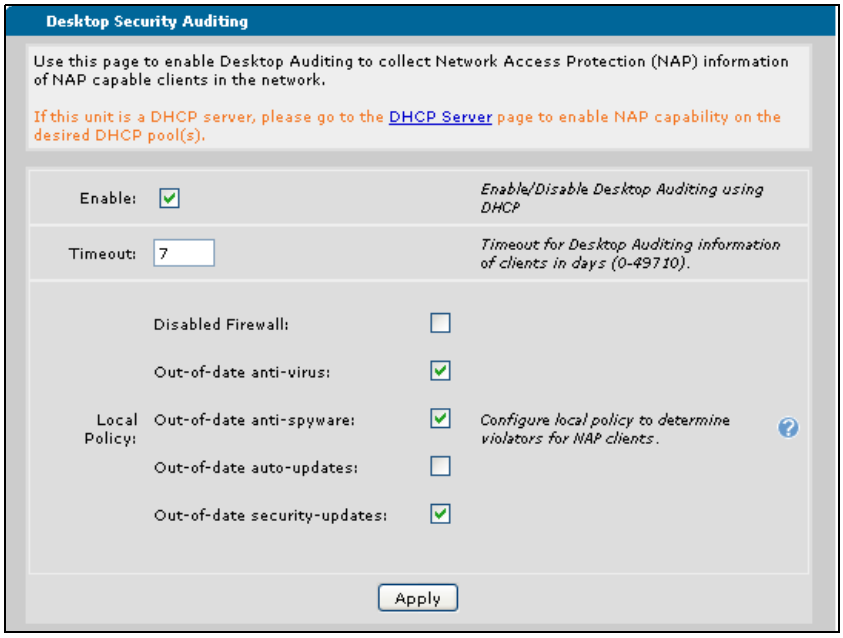
NOTE *Remember that there is a storage limit of 2000 NAP entries. When this limit is reached, new entries overwrite the old entries.*

6. Next, optionally specify the local policy for determining client health violations. These policies determine and show when a NAP client is in violation by collecting NAP information for the connected clients and comparing them to the policies configured here. You can choose violations based on the client's firewall state, antivirus status, antispyware status, auto-update status, and security update status. Selecting these policies filters the collected client information.

   Select the settings you wish to apply by checking the box next to each policy. When you have made your selections, enabled desktop auditing, and specified the timeout period, select **Apply** to apply the settings.



   For example, in the following image desktop auditing has been enabled, the timeout period has been set for **7** days, and the antivirus, antispyware, and security updates for each NAP client are being monitored.

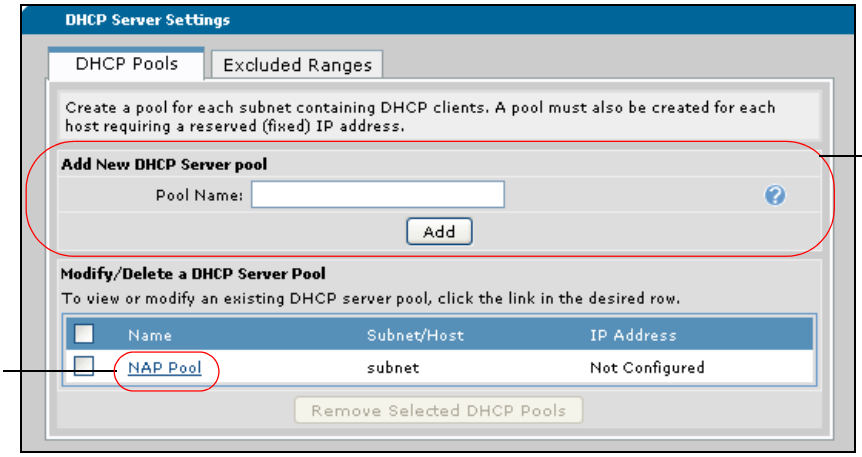


Desktop auditing is now enabled and configured, and begins to monitor the specified NAP information from each client.

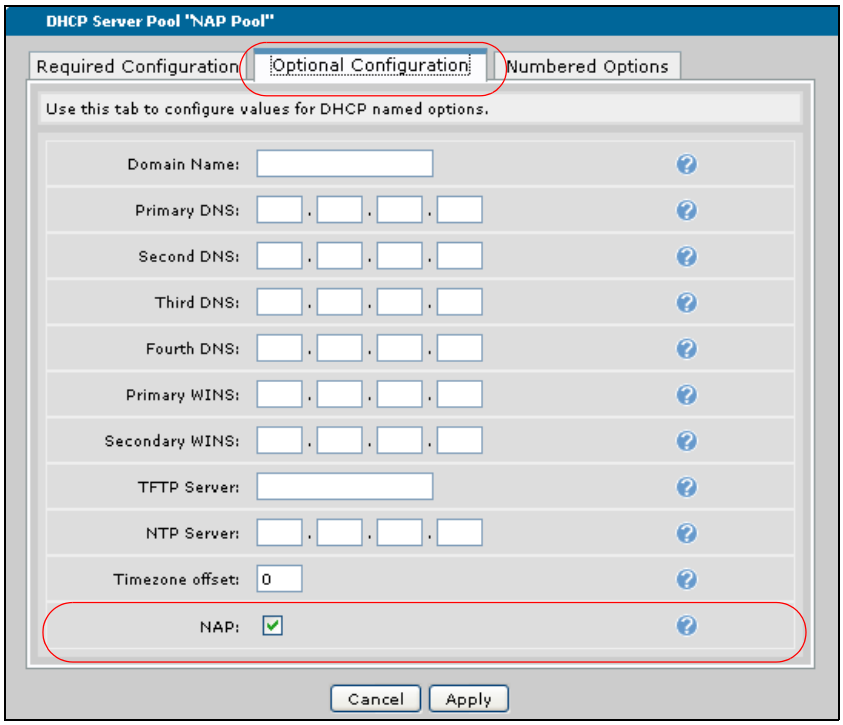
Enabling NAP Advertisements on DHCP Server Pools

If your AOS unit is functioning as a DHCP server and you want DHCP server pools to advertise that they are NAP compatible, you must enable NAP in the DHCP server pool's configuration. To do so, follow these steps:

1. Navigate to **System** > **DHCP Server**. If you have not already created a DHCP server pool, enter the server pool's name in the appropriate field and select **Add**. If you have DHCP pools already configured, you can select from the list the name of the DHCP pool on which you want to enable NAP advertisements.



2. Once you have selected a new or existing pool, navigate to the **Optional Configuration** tab for that pool. Enable NAP advertisements by checking the **NAP** check box and selecting **Apply**.



*These instructions do not include all the other settings that are necessary for DHCP server pool configuration and operation. You should also include these configurations and the necessary information for your network operation if you are creating a new server pool (or updating an existing pool) before selecting **Apply**. For more information about configuring your DHCP server, refer to the **Configuring DHCP in AOS** technical note available online at http://kb.adtran.com (article number 2149).*

3. The DHCP pool is now configured to include NAP advertisements.

If an existing DHCP server pool is updated using this method, the client will need to obtain another lease from the AOS product for the updates to take effect.

Viewing Client NAP Information Using the GUI

Once desktop auditing is enabled and configured, the AOS unit gathers NAP information from each connected client. Desktop auditing collects two types of information: DHCP and NAP.

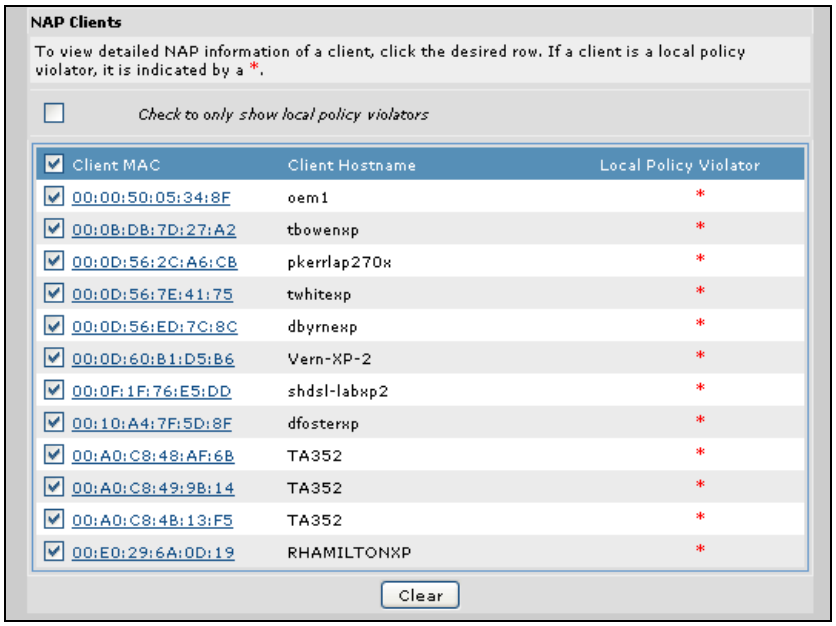
DHCP information collected by desktop auditing includes the following:

- Client MAC address
- Client IP address
- Client VLAN ID
- Client host name
- Client source port
- Server MAC address
- Server IP address
- The date and time the SoH information was last updated

The NAP information collected by desktop auditing includes the following:

- Client NAP state (enabled or disabled)
- Client operating system version
- Client operating system service pack
- Client processor architecture
- Client firewall name and state
- Client antivirus name and state
- Client antispyware name and state
- Client automatic updates state and configuration
- Client security updates server, last update time, and state

To view the DHCP and NAP information collected for clients on the network, navigate to **System** > **Data** > **Desktop Auditing**. The NAP clients detected on the system are listed at the bottom of the screen.



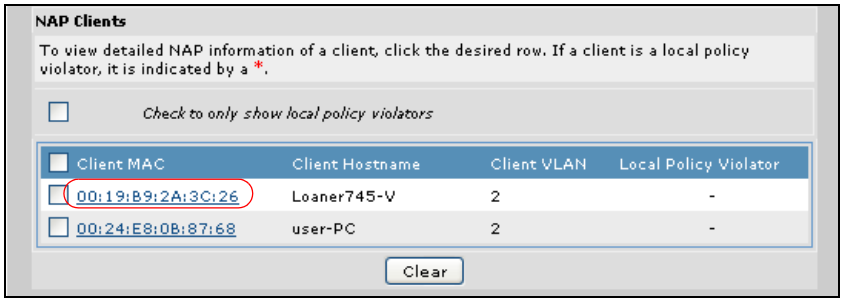
The red * in the client NAP information indicates the client is a violator of one of the local policies specified in ***Step 6*** *on page 6*.

Limiting the Client Information Displayed

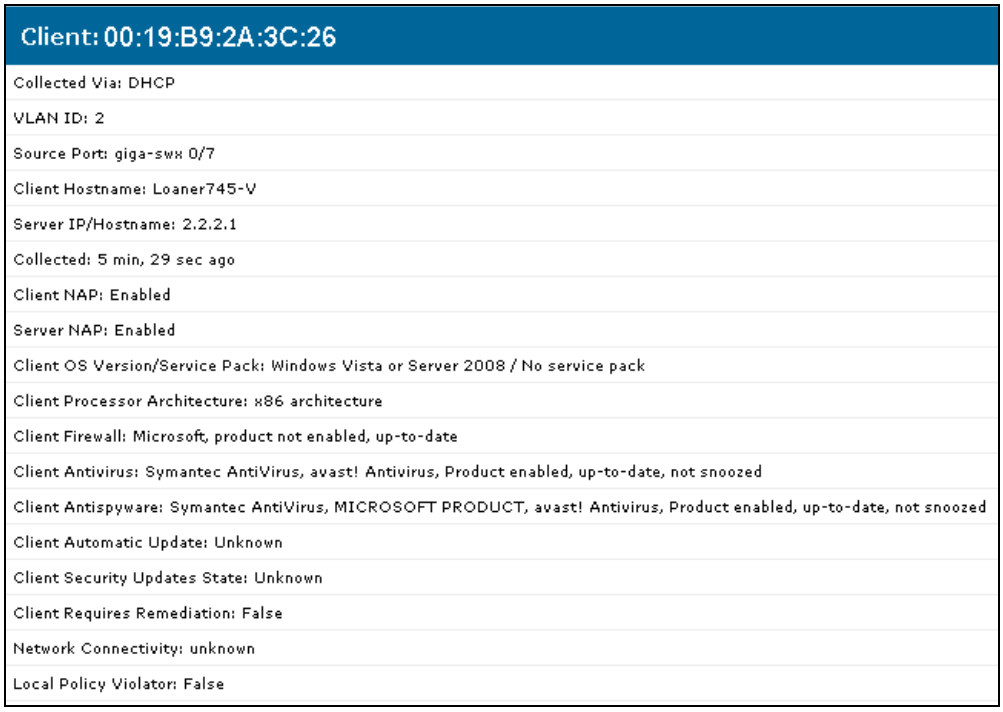
You can limit the types of clients displayed in the NAP clients list by checking the **Check to only show local policy violators** check box located above the NAP clients list. Checking this box limits the clients listed by only showing local policy violators.

Viewing Information for a Specific Client

You can view NAP information for specific clients by selecting the MAC address of the client in the list.

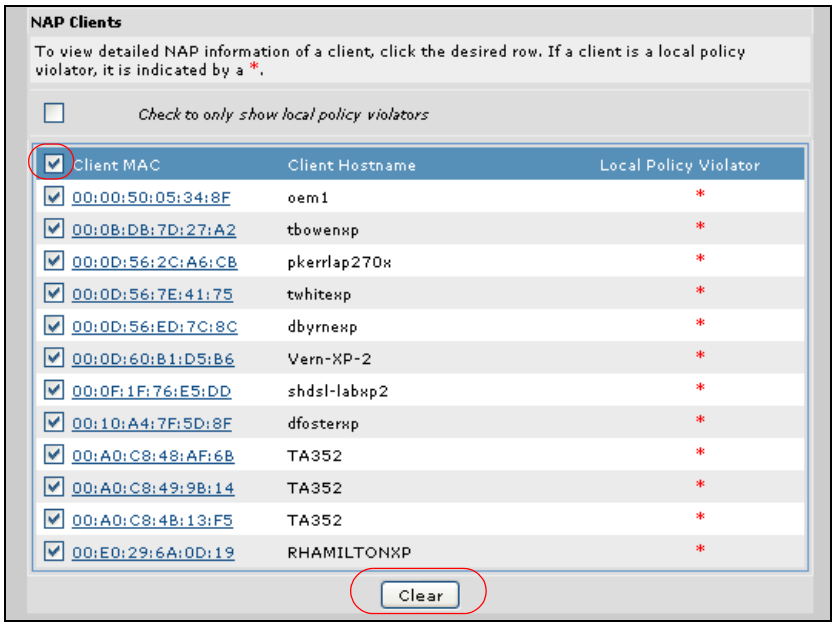


Once the client is selected, the specific information collected for that client is displayed.



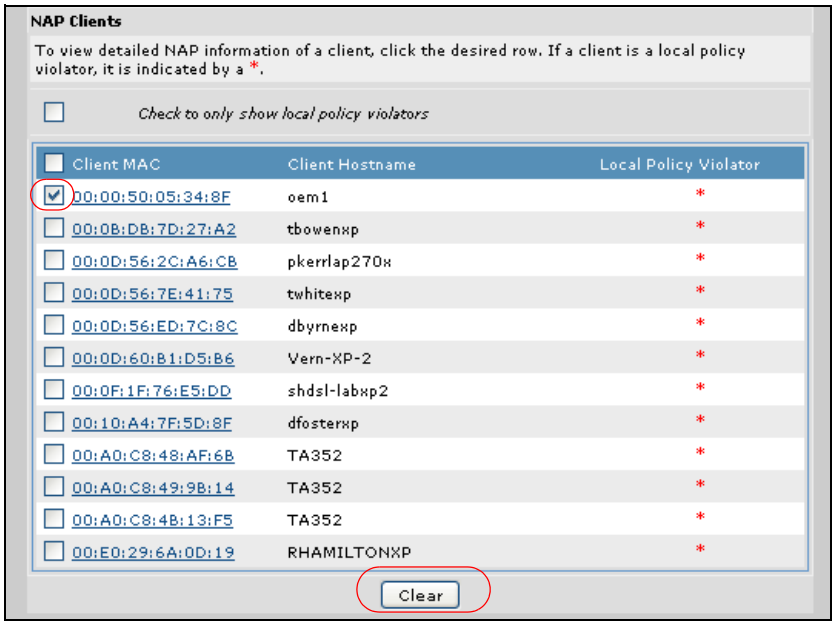
Clearing Client Information

You can clear the collected NAP information by either clearing all the collected NAP statistics, or by clearing the NAP information for specific clients. To clear the information for all NAP statistics, check all statistics by checking the check box next to **Client MAC** and select **Clear** at the bottom of the client NAP statistics.



> **NOTE** *NAP information for a particular client will not be repopulated until the client requests a new IP address via DHCP.*

To clear the NAP statistics for a specific client, select the check box next to the client MAC address and select **Clear**.



Configuring Desktop Auditing Using the CLI

To configure desktop auditing using the CLI, complete the following tasks:

- Enable desktop auditing.
- Specify the desktop auditing information timeout.
- Define the local policy for determining client health violations (optional).
- Enable NAP advertisements on DHCP server pools (if the AOS unit is acting as the network's DHCP server).

Enabling Desktop Auditing

Desktop auditing is enabled using the **desktop-auditing dhcp** command. The command specifies that the AOS unit will monitor DHCP information to collect NAP information. By default, desktop auditing is not enabled. Using the **no** form of this command disables desktop auditing. To enable desktop auditing, enter the **desktop-auditing dhcp** command from the Global Configuration mode prompt as follows:

(config)**#desktop-auditing dhcp**

Specifying the Desktop Auditing Timeout

You can specify the amount of time (in days) that the AOS unit will store NAP information using the **desktop-auditing timeout** <*days*> command. The range is **0** to **49710** days and the value of **0** (default) indicates the information will be stored indefinitely. Using the **no** form of this command returns the timeout period to the default value. To specify the timeout period, enter the command from the Global Configuration mode prompt as follows (in this example, the timeout period is set to **7** days):

(config)**#desktop-auditing timeout 7**

Remember that there is a storage limit of 2000 NAP entries. When this limit is reached, new entries overwrite the old entries.

Creating a Local Policy

The local policy determines when a NAP client is in violation by collecting NAP information for the connected clients and comparing them to the policies configured here. These policies are optional, and display the violators. You can choose violations based on the client's firewall state, antivirus status, antispyware status, auto-update status, and security update status. Selecting these policies filters the collected client information.

Policies are created using the **desktop-auditing local-policy** command. This command creates a local policy and enters the policy's configuration mode. Using the **no** form of this command removes the policy from the unit's configuration. To create a local policy, enter the command from the Global Configuration mode prompt as follows:

(config)**#desktop-auditing local-policy**
(config-desktop-audit-policy)#

Once you have entered the local policy configuration mode, you can specify whether the policy will be monitoring the firewall, antivirus status, antispyware status, auto-update status, and the security-update status of the connected clients. As you specify the information to be monitored, you also specify the state (enabled, current, etc.) of the features you are monitoring.

To specify that the policy monitors the firewall status of connected clients, enter the **firewall enable** command from the local policy configuration mode prompt. This command specifies that the local policy will monitor connected clients to verify the client firewall is enabled and active. Using the **no** form of this command removes the firewall information from the local policy. Enter the command as follows:

(config)**#desktop-auditing local-policy**
(config-desktop-audit-policy)**#firewall enable**

To specify that the policy monitors the antivirus status of connected clients, enter the **anti-virus current** command from the local policy configuration mode prompt. This command specifies that the local policy will monitor connected clients to verify the client antivirus protection is enabled, active, and up-to-date. Using the **no** form of this command removes the antivirus information from the local policy. Enter the command as follows:

(config)**#desktop-auditing local-policy**
(config-desktop-audit-policy)**#anti-virus current**

To specify that the policy monitors the antispyware status of connected clients, enter the **anti-spyware current** command from the local policy configuration mode prompt. This command specifies that the local policy will monitor connected clients to verify the client antispyware protection is enabled, active, and up-to-date. Using the **no** form of this command removes the antispyware information from the local policy. Enter the command as follows:

(config)**#desktop-auditing local-policy**
(config-desktop-audit-policy)**#anti-spyware current**

To specify that the policy monitors the auto-update status of connected clients, enter the **auto-update current** command from the local policy configuration mode prompt. This command specifies that the local policy will monitor connected clients to verify the client auto-updates settings are configured to check for updates, download them, and install them automatically (as needed). Using the **no** form of this command removes the auto-update information from the local policy. Enter the command as follows:

(config)**#desktop-auditing local-policy**
(config-desktop-audit-policy)**#auto-update current**

To specify that the policy monitors the security update status of connected clients, enter the **security-update current** command from the local policy configuration mode prompt. This command specifies that the local policy will monitor connected clients to verify the client security updates are current. Using the **no** form of this command removes the security update information from the local policy. Enter the command as follows:

(config)**#desktop-auditing local-policy**
(config-desktop-audit-policy)**#security-update current**

Sample Policy Configuration

In the following example, a local desktop auditing policy is created to monitor the status of the firewall, antivirus, antispyware, and security updates on connected clients.

```
(config)#desktop-auditing local-policy
(config-desktop-audit-policy)#firewall enable
(config-desktop-audit-policy)#anti-virus current
(config-desktop-audit-policy)#anti-spyware current
(config-desktop-audit-policy)#security-update current
```

Once the desktop audit local policy is defined, desktop auditing is configured. You can view violators of the defined policies by using the **show** commands described in *Viewing Client NAP Information Using the CLI on page 16*. The only other configuration requirement is to specify that the DHCP server pools will advertise NAP capability. This is only necessary if your AOS unit is functioning as a DHCP server.

Enabling NAP Advertisements on DHCP Server Pools

If your AOS unit is functioning as a DHCP server and you want DHCP server pools to advertise that they are NAP compatible, enable NAP in the DHCP server pool's configuration by entering the **nap** command from the DHCP server pool configuration mode prompt. Using the **no** form of this command disables NAP advertisements on the DHCP server pool. By default, NAP advertisements are disabled. To enable NAP advertisements, enter the command as follows:

```
(config)#dhcp-server pool MyPool
(config-dhcp)#nap
```

The specific pool (**MyPool**) is now enabled to advertise NAP capability.

*These instructions do not include all the other settings that are necessary for DHCP server pool configuration and operation. You should also include these configurations and the necessary information for your network operation if you are creating a new server pool (or updating an existing pool) before selecting **Apply**. For more information about configuring your DHCP server, refer to the **Configuring DHCP in AOS** technical note available online at http://kb.adtran.com (article number 2149).*

If an existing DHCP server pool is updated using this method, the client will need to obtain another lease from the AOS product for the updates to take effect.

Viewing Client NAP Information Using the CLI

Once desktop auditing is enabled and configured, the AOS unit gathers NAP information from each connected client. Desktop auditing collects two types of information: DHCP and NAP.

DHCP information collected by desktop auditing includes the following:

- Client MAC address
- Client IP address
- Client VLAN ID
- Client host name
- Client source port
- Server MAC address
- Server IP address
- The date and time the DHCP information was last updated

The NAP information collected by desktop auditing includes the following:

- Client NAP state (enabled or disabled)
- Client operating system version
- Client operating system service pack
- Client processor architecture
- Client firewall name and state
- Client antivirus name and state
- Client antispyware name and state
- Client automatic updates state and configuration
- Client security updates server, last update time, and state

The **show desktop-auditing dhcp** command displays the collected NAP information along with some DHCP information for the connected client. This command can display information for all connected clients, or for a specific client only. This command displays a large amount of information, so it is possible to filter the output using the following keywords:

- **server-violators**: This parameter limits the output to only display clients that are status violators indicated by the DCHP server.
- **server-restricted**: This parameter limits the output to only display clients that have restricted network access as indicated by the DHCP server.
- **local-violators**: This parameter limits the output to only display clients that violate the desktop auditing local policy (as configured in *Creating a Local Policy on page 13*).
- **firewall [disabled | 3rd-party | snoozed]**: This parameter limits the output to only display clients with either disabled, third party, or inactive firewall states.
- **antivirus [disabled | out-of-date | 3rd-party | snoozed]**: This parameter limits the output to only display clients with disabled, out-of-date, third party, or inactive antivirus states.
- **antispyware [disabled | out-of-date | 3rd-party | snoozed]**: This parameter limits the output to only display clients with disabled, out-of-date, third party, or inactive antispyware states.

- **auto-updates [disabled | not-checking | not-downloading | not-installing]**: This parameter limits the output to only display clients with disabled auto-updates, or clients that are not checking, not downloading, or not installing the updates.
- **brief**: This parameter compresses the collected information into a table format.

For example, to view client statistics for all clients that are local policy violators, enter the command from the Enable mode prompt as follows:

```
#show desktop-auditing dhcp local-violators
```

To view client statistics for all clients that are not installing auto-updates, enter the command as follows:

```
#show desktop-auditing dhcp auto-updates not-installing
```

The show output can also be limited to specific clients. Clients are specified using their MAC address, IP address, host name, or the interface they are using. To specify output for a specific client using the client MAC address, use the **show desktop-auditing dhcp mac** <*mac address*> command. MAC addresses are specified in HH:HH:HH:HH:HH format. To specify output for a specific client using the client IP address, use the **show desktop-auditing dhcp ip** <*ip address*> command. IP addresses are specified in dotted decimal notation, for example, **10.10.10.1**. To specify output for a specific client using the client host name, use the **show desktop-auditing dhcp hostname** <*hostname*> command. To specify output for a specific client using the client interface, use the **show desktop-auditing dhcp interface gigabit-switchport** <*slot/port*> command.

For example, to specify only desktop auditing output from the client at IP address **10.200.1.68**, enter the command from the Enable mode prompt as follows:

```
#show desktop-auditing dhcp ip 10.200.1.68
```

*The output for the **show desktop-auditing dhcp** command can be limited either by naming a specific client, or by only showing specific types of results, but not both.*

Show Desktop-Auditing DHCP Output

The following is sample output from the **show desktop-auditing dhcp** command.

```
#show desktop-auditing dhcp
Client MAC/IP: 00:E0:29:0E:D5:E3 / 10.23.220.1 / xpsp3-host
    Collected: DHCP
    VLAN ID: 100
    Source Port: gigabit-switchport 0/2
    Date/Time Collected: 2009.08.25 10:33:42
    Client NAP: Enabled
    Server NAP: Enabled
    Client OS Version: Windows XP
    Client OS Service Pack: 3
    Client Processor Architecture: x86 architecture
    Client Firewall:  Microsoft
                      Disabled but Up-To-Date
    Client Antivirus: Symantec Antivirus Corporate Edition
                      Enabled & Up-To-Date
    Client Antispyware: None Installed
    Client Automatic Security Updates: Enabled, Download, but Don't Install
    Client Security Updates: From 10.10.10.3
                             Up-To-Date (2009.08.25 10:33:42)
    Client Requires Remediation: False
    Network Connectivity: Not restricted
```

The preceding output is for one client. This same information will be displayed for all connected clients unless one of the filtering parameters is used in conjunction with the ***show desktop-auditing dhcp*** *command.*

The following is sample output from the **show desktop-auditing dhcp brief** command. Because of the **brief** keyword, the results are displayed in table format.

#show desktop-auditing dhcp brief

```
Columns:        E = Enabled, U = Up-to-date, 3 = 3rd party (not MS), S = Snoozed
                C = Check for Updates, D = Download Updates, I = Install Updates
                ! = Error (not installed, other)
Indicators:     + = True, - = False, ? = Unknown State
                ! = Attention
Server
Response        R = Client Requires Remediation, N = Client Network Restricted
Codes:          . = No Server Response

Client           FireWall   AntiVir    AntiSpy    AutoUpd    SecUpd     Server
                    E3S!     EU3S!      EU3S!      ECDI!      Severity   Response
   ------------------------------------------------------------------------------
00:E0:29:0E:D5:E3  +--      +++-       +++-       ++--       Important
00:E0:29:0E:D5:E4  ---      +-+-       ----!      ++++       Low        RN
```

Clearing NAP Client Information

The collected NAP client information can be cleared using the **clear desktop-auditing** command from the Enable mode prompt. The information can be cleared for all clients or for a specific client. Clients are specified using their MAC address, IP address, host name, or interface. To clear information for a specific client using the client MAC address, use the **clear desktop-auditing mac** <*mac address*> command. MAC addresses are specified in HH:HH:HH:HH:HH format. To clear information for a specific client using the client IP address, use the **clear desktop-auditing ip** <*ip address*> command. IP addresses are specified in dotted decimal notation, for example, **10.10.10.1**. To clear information for a specific client using the client host name, use the **clear desktop-auditing host** <*hostname*> command. To clear information for a specific client using the client interface, use the **clear desktop-auditing interface gigabit-switchport** <*slot/port*> command. To clear information for a specific client using the client's VLAN interface, use the **clear desktop-auditing vlan** <*vlan id*> command. VLAN ID range is **1** to **4096**.

For example, to clear NAP information for all clients, enter the **clear desktop-auditing** command as follows:

#clear desktop-auditing

To clear information for the specific client at MAC address **00:E0:29:0E:D5:E3**, enter the command as follows:

#clear desktop-auditing mac 00:E0:29:0E:D5:E3

Example Desktop Auditing Configuration

The following is sample configuration of desktop auditing on a NetVanta 1544. This scenario is provided for example purposes only and only includes the information necessary for configuring desktop auditing on the unit. Example configurations should be modified to fit your specific configuration needs.

In this example, a NetVanta 1544 is acting as a DHCP server with the server pool **MyPool**. The unit is configured to collect NAP information of the clients in the network, and uses a local policy that defines any NAP client with a disabled firewall and out-of-date antivirus protection to be a policy violator.

```
!
ip domain-proxy
ip name-server 65.162.109.202
!
desktop-auditing dhcp
desktop-auditing timeout 1
desktop-auditing local-policy
    firewall enable
    anti-virus current
!
ip dhcp-server pool MyPool
    network 192.168.1.0 255.255.255.0
    dns-server 192.168.1.1
    netbios-node-type h-node
    default-router 192.168.1.1
    nap
!
interface eth 0/1
    ip address 192.168.1.1 255.255.255.0
    no shutdown
!
```

ADTRAN does not provide customer support for NAP over DHCP configuration or for WSHA configuration for client PCs. For information about how to configure NAP or WSHA for clients, refer to your client's operating system manual.

Configuration Command Summary

The following table includes configuration and **show** commands necessary for configuring the desktop auditing feature. **Debug** troubleshooting commands are summarized in *Troubleshooting on page 24*.

Table 1. Configuration Command Summary

Prompt	Command	Description
(config)#	**[no] desktop-auditing dhcp**	Enables desktop auditing. Using the **no** form of this command disables desktop auditing.
(config)#	**[no] desktop-auditing timeout** <*days*>	Specifies the period (in days) that the AOS unit will store the NAP information. Range is **0** to **49710** days. By default, the timeout period is set to **0**, which means information is kept indefinitely. Using the **no** form of this command returns the timeout to the default value.
(config)#	**[no] desktop-auditing local-policy**	Creates a local policy to determine when clients are violators of that policy. This command enters the local policy's configuration mode. Using the **no** form of this command removes the policy.
(desktop-audit-policy)#	**[no] firewall enable**	Defines the local policy to monitor clients' firewall states. If the firewall is inactive or disabled, the client is a violator. Using the **no** form of this command removes firewall monitoring from the policy.
(desktop-audit-policy)#	**[no] anti-virus current**	Defines the local policy to monitor clients' antivirus status. If the antivirus is inactive, disabled, or not up-to-date, the client is a violator. Using the **no** form of this command removes antivirus monitoring from the policy.

Table 1. Configuration Command Summary *(Continued)*

Prompt	Command	Description
(desktop-audit-policy)#	**[no] anti-spyware current**	Defines the local policy to monitor clients' antispyware status. If the antispyware is inactive, disabled, or not up-to-date, the client is a violator. Using the **no** form of this command removes antispyware monitoring from the policy.
(desktop-audit-policy)#	**[no] auto-update current**	Defines the local policy to monitor clients' auto-update status. If the auto-update is not configured to check for, download, and automatically install updates the client is a violator. Using the **no** form of this command removes auto-update monitoring from the policy.
(desktop-audit-policy)#	**[no] security-update current**	Defines the local policy to monitor clients' security update status. If the security updates are not current, the client is a violator. Using the **no** form of this command removes security update monitoring from the policy.
(config-dhcp)#	**[no] nap**	Enables NAP advertisements on a DHCP server pool. Using the **no** form of this command disables NAP advertisements. NAP advertisements are disabled by default.
#	**show desktop-auditing dhcp [mac** <*mac address*> **| ip** <*ip address*> **| hostname** <*hostname*> **| interface gigabit-switchport** <*slot/port*> **| brief]**	Displays the client information collected by desktop auditing. This output can be for all clients, or limited to specific clients by indicating the client MAC address, IP address, host name, or interface. The keyword **brief** indicates the output is displayed in table format. Output can be limited by specific client, or by specific criteria, but not both.

Table 1. Configuration Command Summary *(Continued)*

Prompt	Command	Description
#	**show desktop-auditing dhcp [local-violators | server-violators | server-restricted | firewall [disabled | 3rd-party | snoozed] | antivirus [disabled | out-of-date | 3rd-party | snoozed] | antispyware [disabled | out-of-date | 3rd-party | snoozed] | auto-updates [disabled | not-checking | not-downloading | not-installing] | brief]**	Displays client information collected by desktop auditing. This output can be for all clients, or limited to specific clients by feature criteria. The **server-violator** parameter specifies that only clients violating server policies are displayed. The **server-restricted** parameter specifies that only clients that have restricted network access are displayed. The **local-violators** parameter specifies that only clients violating the local desktop auditing policy are displayed. The **firewall**, **antivirus**, **antispyware**, and **auto-updates** parameters specify that only clients whose information matches the specific feature criteria are displayed. These criteria can only be used one at a time. The **brief** keyword indicates the output is displayed in table format.
#	**clear desktop-auditing [mac** <*mac address*> **| ip** <*ip address*> **| host** <*hostname*> **| interface gigabit-switchport** <*slot/port*> **vlan** <*vlan id*>**]**	Clears the collected information for either all clients or a specific client. Clients are specified by MAC address, IP address, host name, interface, or VLAN.

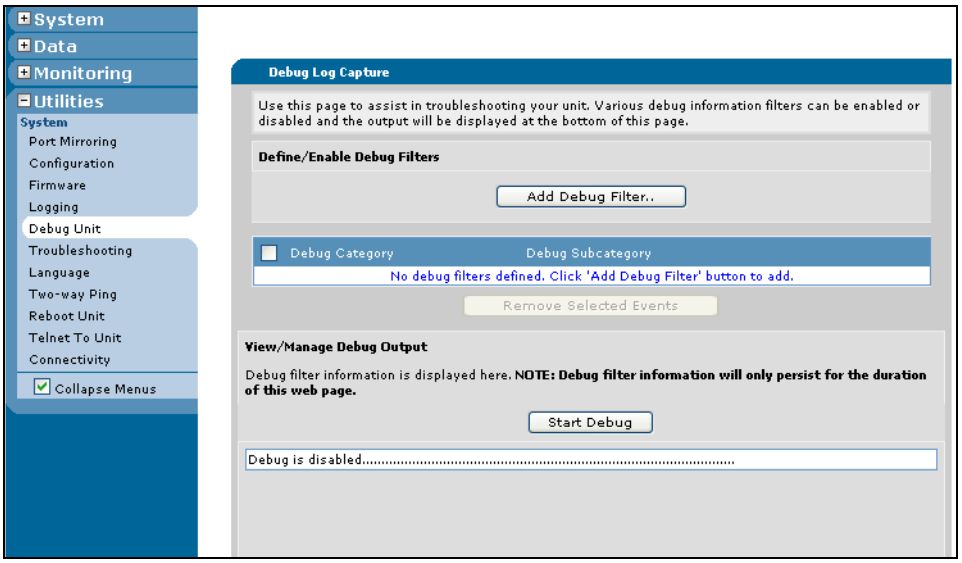
Troubleshooting

There are two methods for troubleshooting desktop auditing. Troubleshooting can be done from either the GUI or the CLI. Both methods are described in the following sections.

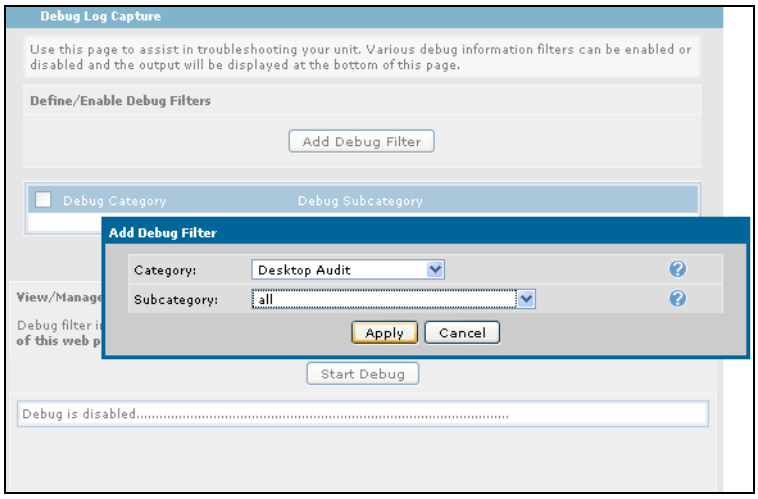
Troubleshooting Using the GUI

Debug messaging can be enabled for desktop auditing using the GUI. To access GUI debugging abilities, follow these steps:

1. Navigate to **Utilities** > **System** > **Debug Unit** menu.

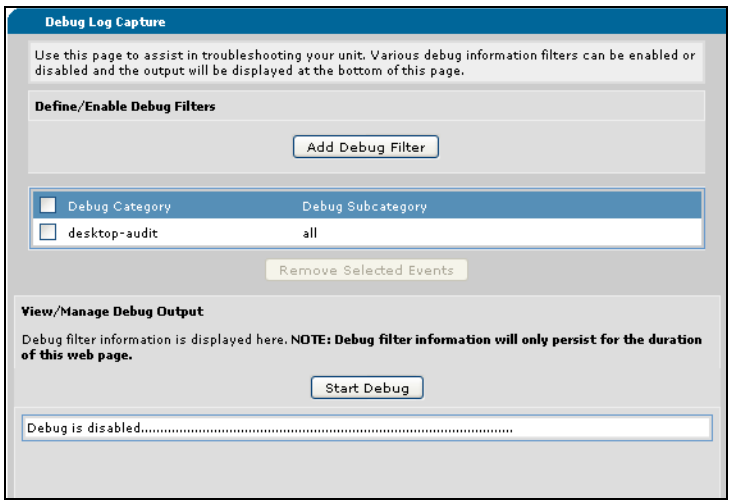


2. Select the **Add Debug Filter** button and select **Desktop Audit** from the **Category** drop-down menu. Then select whether you want debug information for all connected clients or a specific client by choosing the appropriate subcategory from the drop-down menu. Select **Apply**.



The item you have selected to debug will appear in the **Debug Category** tab in the middle of the menu.

3. Select **Start Debug** to begin receiving debug information for the item you selected.



Troubleshooting Using the CLI

The **debug desktop-auditing** command can be beneficial in verifying the desktop auditing configuration. The command is issued from the Enable mode in the CLI to assist in troubleshooting, and can specify if debug information for all clients is displayed or if information for a specific client is displayed. Clients can be specified by MAC address, IP address, host name, or interface. The information contained in the debug output includes the NAP messages transferred within the DHCP packets between the client and the server. This information can be beneficial in verifying that the configuration of desktop auditing is providing the necessary information for your network, as well as in viewing the client NAP information collected.

NOTE *Using **debug** commands can be very processor intensive, and should be used with caution.*

To view debug information for all clients connected to the network, enter the command as follows:

#debug desktop-auditing

2009.08.31 14:30:30 DESKTOP_AUDITING.DHCP.giga-swx 0/5 from 00:E0:29:0E:D5:E3 NAP Capable client

2009.08.31 14:30:31 DESKTOP_AUDITING.DHCP.giga-swx 0/24 from 00:E0:29:0E:D5:E5 to 00:E0:29:0E:D5:E3 NAP Capable Server

2009.08.31 14:30:31 DESKTOP_AUDITING.DHCP.giga-swx 0/5 from 00:E0:29:0E:D5:E3 to 00:E0:29:0E:D5:E5 NAP SoH: Firewall is 3rd-Party, AutoUpdates not downloading or installing

2009.08.31 14:30:31 DESKTOP_AUDITING.DHCP.giga-swx 0/24 from 00:E0:29:0E:D5:E5 to 00:E0:29:0E:D5:E3 NAP SoHR: OK

To specify only the output for a specific client is displayed, using the client MAC address, enter the **debug desktop-auditing mac** <*mac address*> command as follows:

#debug desktop-auditing mac 00:E0:29:0E:D5:E3

To specify only the output for a specific client is displayed, using the client IP address, enter the **debug desktop-auditing ip** <*ip address*> command as follows:

#debug desktop-auditing ip 10.200.25.659

To specify only the output for a specific client is displayed, using the client host name, enter the **debug desktop-auditing hostname** <*hostname*> command as follows:

#debug desktop-auditing hostname Desktop1

To specify only the output for a specific client is displayed, using the client interface, enter the **debug desktop-auditing interface gigabit-switchport** <*slot/port*> command as follows:

#debug desktop-auditing interface gigabit-switchport 0/1