

Getting Started with the Web Client

The OmniVista Web Client for OmniVista 3.3 provides users access to basic versions of the OmniVista Locator, Notifications, and Topology applications through a web application residing on the OmniVista Server. The following functionality is available:

- **Locator** - Search for an end station by either IP or MAC address and browse to locate an end station
- **Notifications** - View traps sent to OmniVista by the switches
- **Topology** - View information for all switches managed by OmniVista.

Requirements

The Web Client is installed on the OmniVista Server and can be accessed through the following web browsers:

- Internet Explorer, version 6.0 for Windows
- Mozilla Firefox, version 1.5 for Solaris.

Your browser preferences (or options) should be set up as follows:

- Cookies should be enabled. Typically, this is the default.
- JavaScript must be enabled/supported.
- Java must be enabled.
- Style sheets must be enabled; that is, the colors, fonts, backgrounds, etc., of web pages should always be used (rather than user-configured settings).
- Checking for new versions of pages should be set to "Every time" your browser opens.

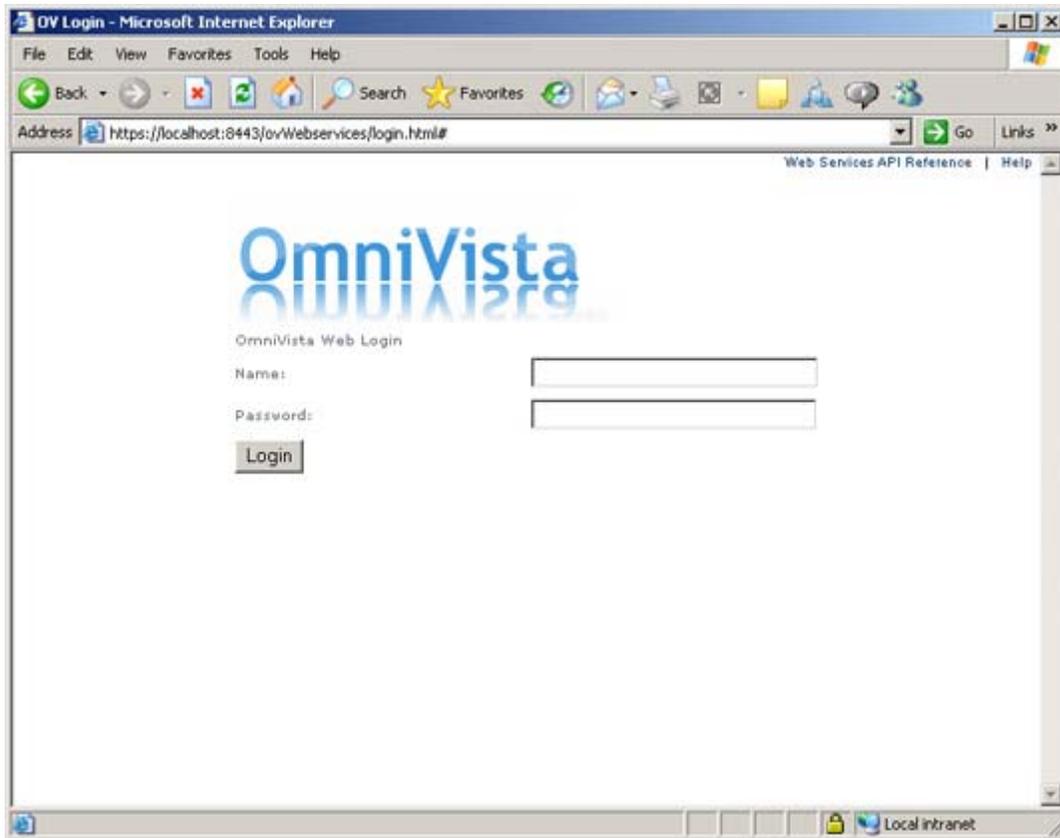
Note: Typically, many of these settings are configured as the default. Different browsers (and different versions of the same browser) may have different dialogs for these settings. Check your browser help pages if you need help.

Logging Into OmniVista Web Client

To access the OmniVista Web Client:

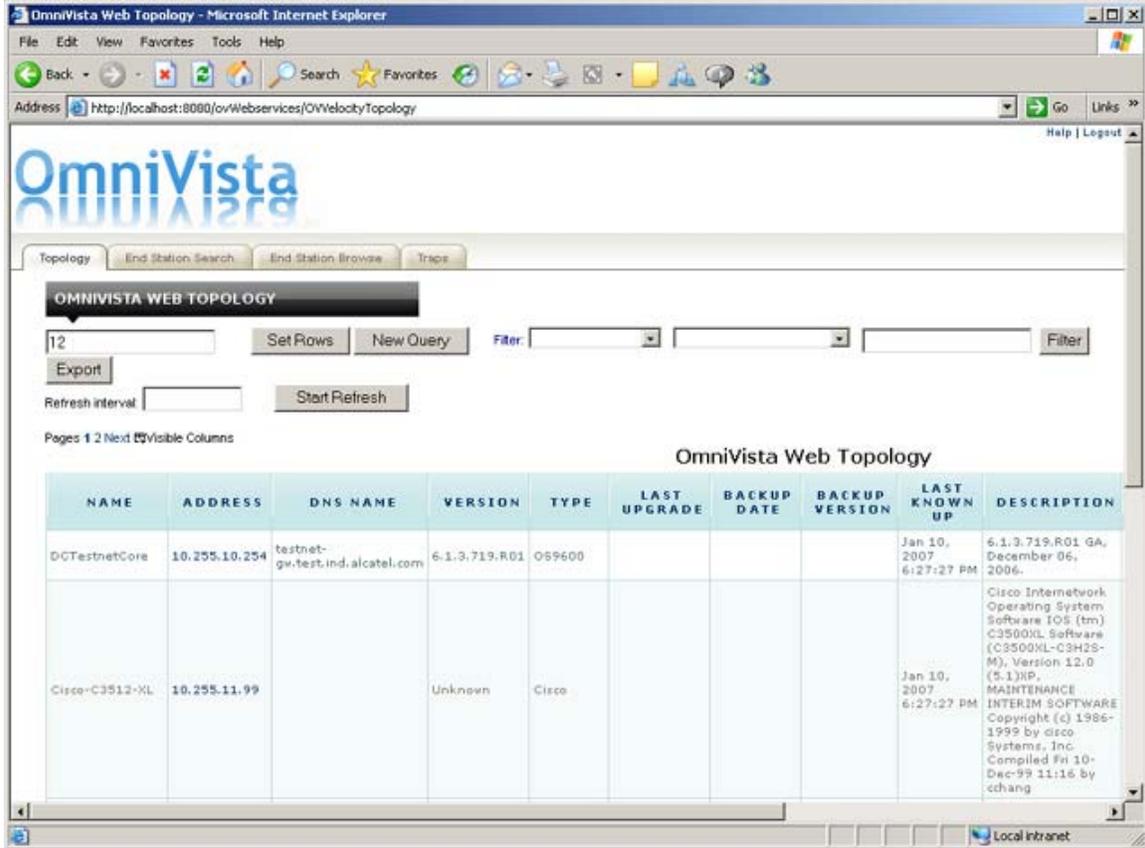
1. Open an Internet browser and enter **http://OmniVista Server IP Address:8080** in the address line, then press **ENTER**. The Login Screen will appear.

Note: If the client and server are installed on the same machine, you can enter **http://localhost:8080**.



Note: The **Web Services API Reference** link at the top of the page brings up the OmniVista Web Services API Guide.

2. Enter the OmniVista user name and password and click **Login**. The following screen will appear.



The Web Client Topology screen provides a listing and description of all discovered switches. From here, you can perform OmniVista Topology functions. You can also click on the End Station Search or End Station Browse tabs to access Locator functions; or click on the Traps tab to access Notifications Functions.

Locator

The OmniVista **Locator** application within the OmniVista Web Client is a search tool that enables you to search for end stations connected to switches in the network. The End Station Search tab enables you to locate a switch that is directly connected to a user-specified end station. The End Station Browse tab enables you search in the "opposite direction". Instead of entering an end station's address to locate the switch and slot/port to which the end station is connected, you can search for and list ALL end stations connected to user-specified switch ports. The end stations are located by searching the historical database.

The search results display a list of devices in a table that provides basic information for each device. You can customize the table display, sort the information in the table by column, and create filters to view specific information. You can also export the information to a .CSV file.

End Station Search Tab

The **End Station Search** tab enables you to locate a switch that is directly connected to a user-specified end station. You can enter the end station's IP address or MAC address to locate the switch and slot/port to which the end station is connected.

Although you can enter an end station's IP address or MAC address to locate the switch and slot/port that is directly connected to the end station, Locator actually searches for the end station's MAC address. If you enter an IP address, the first thing Locator does is find the corresponding MAC address. This MAC address is displayed in the **OmniVista Web Service Locator** table with a time stamp indicating when the information was obtained (last time the device was polled).

Searching for a Specific End Station

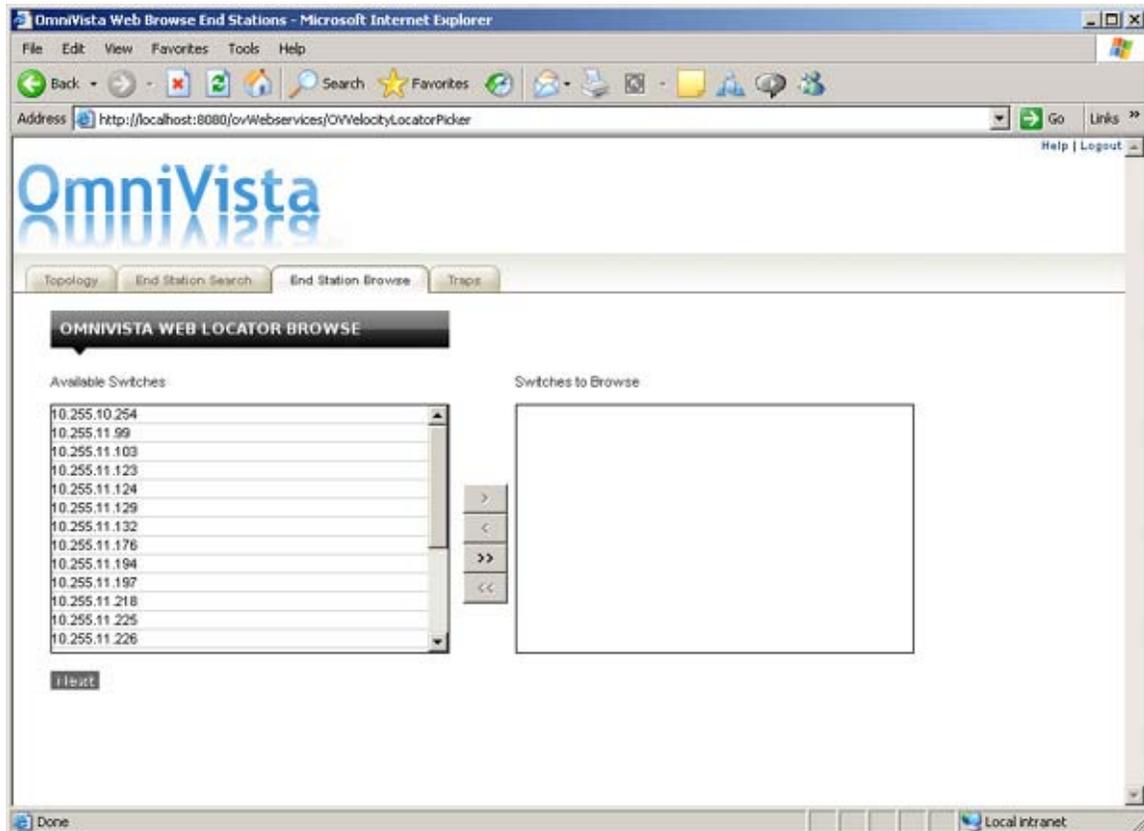
To search for a specific switch:

1. In the **Address Type** field, select IP to search by IP address or MAC to search by MAC address.
2. In the **Address** field, enter the IP or MAC address. If searching by MAC address, you must enter the address in 000000:000000 format.
3. Click the **Set Address** button.

The results will appear in the **OmniVista Web Service Locator** table. You can sort the data by column heading or apply filters to the table to display specific information. You can also export the information to a .CSV file. Click here for column heading definitions.

End Station Browse Tab

The **End Station Browse** tab enables you search in the "opposite direction" of the End Station Search tab. Instead of entering an end station's address to locate the switch and slot/port to which the end station is connected, you can search for and list ALL end stations connected to user-specified switch ports.



To browse for end stations select the switch(es) in which you are interested, then click the **Next** button. To select multiple switches, use the **Shift** or **Ctrl** keys. The results will appear in the **OmniVista Web Service Locator Browse** table. You can sort the data by column heading or apply filters to the table to display

specific information. You can also export the information to a .CSV file. Click here for column heading definitions.

OmniVista Web Service Locator Browse

12 Set Rows Filter

New Query Export

Pages 1 2 3 4 5 6 7 8 9 10 Next | Next 10 Visible Columns

SEARCHED IP ADDRESS	SEARCHED MAC ADDRESS	SEARCHED DNS NAME	DEVICE IP ADDRESS	DEVICE DNS	DEVICE NAME	SLOT/PORT	PORT STATUS
	00a098:048dc7		10.255.10.254	testnet-gv.test.ind.alcatel.com	DCTestnetCore	1/10	up
10.255.10.107	0003ba:2c93fa		10.255.10.254	testnet-gv.test.ind.alcatel.com	DCTestnetCore	1/22	up
10.255.10.105	0003ba:2ca082		10.255.10.254	testnet-gv.test.ind.alcatel.com	DCTestnetCore	1/24	up
10.255.10.160	0003ba:d389a2		10.255.10.254	testnet-gv.test.ind.alcatel.com	DCTestnetCore	1/21	up
10.255.10.100	0003ba:e40a64		10.255.10.254	testnet-gv.test.ind.alcatel.com	DCTestnetCore	1/23	up
10.255.10.9	00a098:048eab		10.255.10.254	testnet-gv.test.ind.alcatel.com	DCTestnetCore	1/8	up

Done Local Intranet

Table Display

You can set the number of rows that you want displayed on each page by entering the number of rows you want to display (e.g., 12), then clicking the **Set Rows** button. If a table spans several pages, click **Next** or a specific page number at the top left corner of the table to page through the table.

Note: A maximum row setting of 100 is advised. Larger row settings can increase the time it takes to populate the table.

You can also configure the columns you want to display. Click on **Visible Columns** and select all of the columns you want to display. De-select any columns you want to hide. The new settings will remain in effect until you log out of the session. By default, all columns are displayed.

Column Definitions

Searched IP Address: The IP address of the end station connected to the selected device.

Searched MAC Address: The MAC address of the end station connected to the selected device.

Searched DNS Name: The DNS name of the end station connected to the selected device.

Device IP Address: The IP address of the device connected to the end station.

Device DNS: The DNS of the device connected to the end station.

Device Name: The name of the device connected to the end station.

Slot/Port: The slot/port of the device connected to the end station.

Port Speed: The port speed of the device connected to the end station.

Port Status: The port status of the device connected to the end station.

Duplex Mode: The duplex mode (half duplex, full duplex, or auto duplex) of the selected device connected to the end station.

VLAN ID: The VLAN ID associated with the device connected to the end station.

Timestamp: The time the information was gathered.

Sorting Information

You can sort the Locator Browse Table in ascending or descending order by clicking on a column heading.

Filtering Information

You can filter the information in the table to display specific switch information.

1. Select a column heading from the first **Filter** drop-down menu (e.g., Device IP Address, Device DNS).
2. Select an operator from the second **Filter** drop-down menu (e.g., Equals, Starts With).
3. Enter a value in the last **Filter** field (e.g., "9600").

For example, to view a list of devices in the Test Network, you would select "Device DNS", "Contains", and enter "testnet" in the last field).

4. When you have entered all of the filter criteria, click the **Filter** button. The results will be displayed in the Locator Table. To refine the filter, enter a new set of filtering criteria and click the **Refine Filter** button to display a list of devices matching both sets of filters.

Note: You can display the results of previous filters by clicking the browser's **Back** button. The OmniVista Web Client will display up to eight (8) previous results in a single login session.

To start over click the **New Query** button.

Exporting Information

To export the table to a .CSV file, use the browse function to locate the devices and populate the Locator Browse Table, filter the information (if applicable), then click the **Export** button. Click **Yes** at the Security prompt, then select the directory in which you want to save the file.

Notifications

The **Notifications** application within the OmniVista Web Client is used to monitor switch activity through the **OmniVista Web Traps** Table. The table, available under the **Traps** tab, displays information on all alarms and traps received by the OmniVista Server. You can customize the table display, sort the information in the table by column, and create filters to view specific information. You can also export the information to a .CSV file.

Note: If the table is not displaying any notifications, it may be that none of your discovered switches have been configured to send traps to the OmniVista server.

NAME	SYNOPSIS	AGENT	AGENT NAME	DATE/TIME	SEVERITY	ACKNOWLEDGMENT
alaOvSwitchUp	Switch has resumed responding to OmniVista. Last up time: 0 hours, 2 minutes, 50 seconds.	10.255.73.12	vxTarget	Jan 10, 2007 6:23:32 PM	Normal	false
alaOvSwitchDown	Switch has STOPPED responding to OmniVista: Couldn't send SNMP message (Timeout or Authentication Problem). Last up time: 0 hours, 15 minutes, 27 seconds.	10.255.73.12	vxTarget	Jan 10, 2007 6:22:27 PM	Normal	false
alaOvSwitchUp	Switch has resumed responding to OmniVista. Last up time: 0 hours, 2 minutes, 31 seconds.	10.255.73.12	vxTarget	Jan 10, 2007 6:03:38 PM	Normal	false

Table Display

You can set the number of rows that you want displayed on each page by entering the number of rows you want to display (e.g., 12), then clicking the **Set Rows** button. If a table spans several pages, click **Next** or a specific page number at the top left corner of the table to page through the table.

You can also configure the columns you want to display. Click on **Visible Columns** and select all of the columns you want to display. De-select any columns you want to hide. The new settings will remain in effect until you log out of the session. By default, all columns are displayed.

By default, up to 1,000 traps are displayed. However, you can configure the display by entering a number in the **Traps Limit** field, and clicking the **Set The Max Number of Traps** button. When the configured maximum number is reached, the newest traps overwrite the oldest traps.

The refresh function is disabled by default. To enable it, enter a value (in seconds) in the **Refresh Interval** field, and click the **Start Refresh** button (the refresh function will be enabled and the **Start Refresh** button will change to **Stop Refresh**). To disable the refresh function, click the **Stop Refresh** button. The default refresh interval is 30 seconds (this is also the minimum refresh interval).

Column Definitions

Name: The name of the trap as defined in the MIB.

Synopsis: A brief description of the trap.

Agent: The IP address of the switch that generated the trap.

Agent Name: The name of the switch that generated the trap.

Date/Time: The date and time the trap was received by the OmniVista server, using the OmniVista server's system clock.

Severity: The severity level assigned to the trap in the Notifications Application's Trap Definitions Window:

- Normal
- Warning
- Minor
- Major
- Critical.

Acknowledged: Indicates whether or not the trap has been acknowledged. "true" indicates an acknowledged trap. "false" indicates that the trap has yet been acknowledged, or the acknowledgement has been renounced.

Sorting Information

You can sort the **OmniVista Web Traps** Table in ascending or descending order by clicking on a column heading.

Filtering Information

You can filter the information in the table to display specific switch information.

1. Select a column heading from the first **Filter** drop-down menu (e.g., Name, Severity).
2. Select an operator from the second **Filter** drop-down menu (e.g., Equals, Starts With).
3. Enter a value in the last **Filter** field (e.g., "OS9600").

For example, to view a list of all traps with a Severity Level of "Major", you would select "Severity" in the first field, "Equals" in the second, then enter "Major" in the last field).

4. When you have entered all of the filter criteria, click the **Filter** button. The results will be displayed in the OmniVista Web Traps Table. To further refine the filter, enter a new set of filtering criteria and click the **Refine Filter** button to display a list of devices matching both sets of filters.

Note: You can display the results of previous filters by clicking the browser's **Back** button. The OmniVista Web Client will display up to eight (8) previous results in a single login session.

To start over and create a new filter, click the **New Query** button and repeat Steps 1 - 4.

Exporting Information

To export the table to a .CSV file, filter the information (if applicable), then click the **Export** button. Click **Yes** at the Security prompt, then select the directory in which you want to save the file.

Topology

The **Topology** application within the OmniVista Web Client is used to access the OmniVista "List of All Discovered Devices". The table, available under the **Topology** tab, provides basic information for all physical devices in the network, including all devices discovered by OmniVista, as well as any devices that were added manually. You can customize the table display, sort the information in the table by column, create filters to view specific information and export the information to a .CSV file. You can also access web-based management tools (e.g., WebView) for individual AOS switches listed in the Topology Table.

NAME	ADDRESS	DNS NAME	VERSION	TYPE	LAST UPGRADE	BACKUP DATE	BACKUP VERSION	LAST KNOWN UP	DESCRIPTION
DCTestnetCore	10.255.10.254	testnet-gw.test.ind.alcatel.com	6-1-3-719-R01	OS9600				Jan 10, 2007 6:27:27 PM	6.1.3.719.R01 GA, December 06, 2006.
Cisco-C3512-XL	10.255.11.99		Unknown	Cisco				Jan 10, 2007 6:27:27 PM	Cisco Internetwork Operating System Software IOS (tm) C3500XL Software (C3500XL-C3H2S-M), Version 12.0 (S1)NP, MAINTENANCE INTERIM SOFTWARE Copyright (c) 1986-1999 by Cisco Systems, Inc. Compiled Fri 10-Dec-99 11:16 by cchang

Table Display

You can set the number of rows that you want displayed on each page by entering the number of rows you want to display (e.g., 12), then clicking the **Set Rows** button. If a table spans several pages, click **Next** or a specific page number at the top left corner of the table to page through the table.

Note: A maximum row setting of 100 is advised. Larger row settings can increase the time it takes to populate the table.

You can also configure the columns you want to display. Click on **Visible Columns** and select all of the columns you want to display. De-select any columns you want to hide. The new settings will remain in effect until you log out of the session. By default, all columns are displayed.

The refresh function is disabled by default. To enable it, enter a value (in seconds) in the **Refresh Interval** field, and click the **Start Refresh** button (the refresh function will be enabled and the **Start Refresh** button will change to **Stop Refresh**). To disable the refresh function, click the **Stop Refresh** button. The default refresh interval is 30 seconds (this is also the minimum refresh interval).

Column Definitions

Address: The IP address of the device.

DNS Name: The name of the device, if applicable.

Version: The version number of the device firmware. Version numbers are not displayed for certain non-XOS devices.

Type: The type of the device chassis.

Last Upgrade Status: The status of the last firmware upgrade on the switch:

- "Successful" - Successful BMF and Image upgrade performed.
- "Successful (BMF)" - Successful BMF upgrade performed.
- "Successful (Image)" - Successful Image upgrade is performed.
- "Failed (BMF, Image)" - BMF and Image upgrade failed.
- "Failed (BMF)" - BMF upgrade failed.
- "Failed (Image)" - Image upgrade failed.

In all "Failed" cases, "Reload From Working" will be disabled on the switch until a successful upgrade is performed.

Backup Date: The date that the device's configuration and/or image files were last backed-up to the OmniVista server.

Backup Version: The firmware version of the configuration and/or image files that were last backed-up to the OmniVista server.

Last Known Up At: The date and time when the last poll was initiated on the device.

Description: A description of the device, usually the vendor name and model.

Status: This field displays the operational status of the device.

- **Up** - Device is up and responding to polls.
- **Down** - Device is down and not responding to polls.
- **Warning** - Device has sent at least one warning or critical trap and is thus in the warning state.

Traps: This field indicates the status of trap configuration for the device.

- **On** - Traps are enabled.
- **Off** - Traps are disabled.
- **Not Configurable** - Traps for this device are not configurable from OmniVista. (Note that traps may have been configured for such devices outside of OmniVista.)

- **Unknown** - OmniVista does not know the status of trap configuration on this switch. OmniVista will read the switch's trap configuration when traps are configured for the switch via the Configure Traps Wizard.

Seen By: This field lists the Security Groups that are allowed to view the device. (The Security Groups that are allowed to view a device can be defined when devices are auto-discovered, added manually, or edited.) The default Security Groups shipped with OmniVista are as follows:

- **Default Group** - This group has read-only access to switches in the list of All Discovered Devices that are configured to grant access to this group.
- **Writers Group** - This group has both read and write access to switches in the list of All Discovered Devices that are configured to grant access to this group. However, members of this group cannot run auto-discovery nor can they manually add, delete, or modify entries in the list of All Discovered Devices.
- **Network Administrators Group** - This group has full administrative access rights to all switches on the network. Members of this group can run autodiscovery and can manually add, delete, and modify entries in the list of All Discovered Devices. Members of this group also have full read and right access to entries in the Audit application and the Control Panel application. Members of this group can do everything EXCEPT make changes to Security Groups.
- **Administrators Group** - This group has all administrative access rights granted to the Network Administrators group AND full administrative rights to make changes to Security Groups.

Note that other Security Group names may display in this field if custom Security Groups were created. Refer to help for the Security application Users and Groups for further information on Security Groups.

Running From: For AOS devices, this field indicates whether the switch is running from the certified directory or from the working directory. This field is blank for all other devices. For AOS devices, the directory structure that stores the switch's image and configuration files in flash memory is divided into two parts:

- The Certified Directory contains files that have been certified by an authorized user as the default configuration files for the switch. When the switch reboots, it will automatically load its configuration files from the certified directory if the switch detects a difference between the certified directory and the working directory. (Note that you can specifically command a switch to reboot from either directory.)
- The Working Directory contains files that may or may not have been altered from those in the certified directory. The working directory is a holding place for new files to be tested before committing the files to the certified directory. You can save configuration changes to the working directory. You cannot save configuration changes directly to the certified directory.

Note that the files in the certified directory and in the working directory may be different from the running configuration of the switch, which is contained in RAM. The running configuration is the current operating parameters of the switch, which are originally loaded from the certified or working directory but may have been modified through CLI commands, WebView commands, or OmniVista. Modifications made to the running configuration must be saved to the working directory (or lost). The working directory can then be copied to the certified directory if and when desired.

Changes: For AOS devices, this field indicates the state of changes made to the switch's configuration. This field is blank for all other devices. This field can display the following values:

- **Unsaved.** Changes have been made to the running configuration of the switch that have not been saved to the working directory.

- **Uncertified.** Changes have been saved to the working directory, but the working directory hasn't been copied to the certified directory. The working directory and the certified directory are thus different.
- **Blank.** When this field is blank for an AOS device, the implication is that OmniVista knows of no unsaved configuration changes and assumes that the working and certified directories in flash memory are identical.

OmniVista is now capable of tracking AOS configuration changes made through CLI commands or WebView, and so will reflect configuration changes made outside of OmniVista through these two interfaces in the Changes field. Information in the Changes field will be accurate as long as OmniVista has polled the switch since the last change was made (through any interface).

Note that it is possible a switch could be in a state where it is both Unsaved and Uncertified. In this situation Unsaved displays in the Changes field. Whenever an AOS device is in the Unsaved or Uncertified state, a blue exclamation mark displays on its icon ().

Sorting Information

You can sort the Discovered Devices Table in ascending or descending order by clicking on a column heading.

Filtering Information

You can filter the information in the table to display specific switch information.

1. Select a column heading from the first **Filter** drop-down menu (e.g., Address, DNS Name).
2. Select an operator from the second **Filter** drop-down menu (e.g., Equals, Starts With).
3. Enter a value in the last **Filter** field (e.g., "9600").

For example, to view a list of 9600 devices, you would select "Type", "Equals", and enter "9600" in the last field).

4. When you have entered all of the filter criteria, click the **Filter** button. The results will be displayed in the OmniVista Web Topology Table. To further refine the filter, enter a new set of filtering criteria and click the **Refine Filter** button to display a list of devices matching both sets of filters.

Note: You can display the results of previous filters by clicking the browser's **Back** button. The OmniVista Web Client will display up to eight (8) previous results in a single login session.

To start over and create a new filter, click the **New Query** button and repeat Steps 1 - 4.

Exporting Information

To export the table to a .CSV file, filter the information (if applicable), then click the **Export** button. Click **Yes** at the Security prompt, then select the directory in which you want to save the file.

Web-Based Management

You can also access web-based management tools (e.g., WebView) for individual AOS switches listed in the Topology Table by clicking on the switch's IP address in the Topology Table. If a switch has web-based management capabilities, the login screen for the switch will appear. A WebView Login Screen is shown below.

