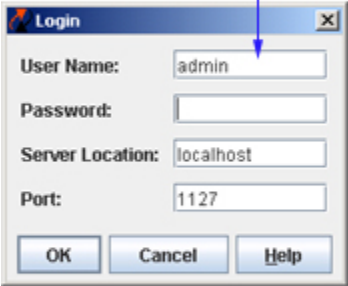


# Quick Start Guide

This Quick Start guide will get you up and running OmniVista. It provides instructions for logging into OmniVista and performing automatic discovery of the switches in your network. It also describes tasks you should perform after devices have been discovered. Follow the steps below to get OmniVista up and running quickly.

## Step 1. Log Into OmniVista

When you execute OmniVista for the first time, the **Login** window is displayed, as shown below. (Note that in the single-user version of OmniVista, the Login window does not include the **Server Location** or **Port** fields.) The user name and password with which you log into OmniVista determine the administrative rights available to you. For this reason, it is recommended that you log in as user **admin** the first time. The password for user **admin** is **switch**. Each field in the Login window is explained below.



**User Name**  
The default user is **admin**. User **admin** has full administrative rights to all switches in the network AND full administrative rights to define security permissions for OmniVista users. It is recommended that you log in as **admin** the first time.

**Password**  
Enter the default password for user **admin**. The default password is **switch**.

**Server Location**  
The default server location is **localhost** if you are running the OmniVista server and the OmniVista client on the same machine. If you are running the OmniVista server on a different machine, enter that machine's name or IP address in this field.

**Port**  
The default server port used for communications with the client is **1127**. If you are using a different port, enter the port number in this field.

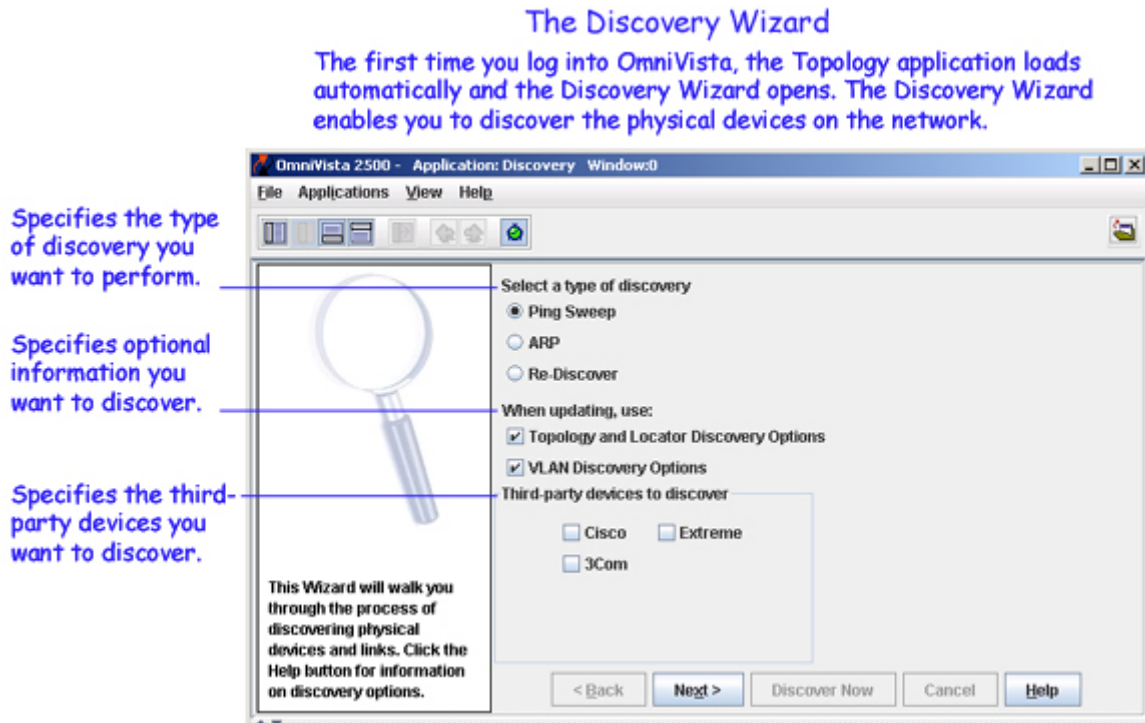
Click the **OK** button when you have completed the fields in the Login window. The Topology application will load automatically and the Discovery Wizard will open. The Discovery Wizard makes it possible to automatically discover the devices in your network.

**Note:** If you are running OV as a service on Linux and you want to change the server location, you need to edit the following installation base directory files:

- properties.conf
- openldap/privaterun.sh
- classes/com/alcatel/ov1/ldap/server/resource/NetscLdapConfig.xml

## Step 2. Discover Network Devices

After your initial login as user **admin**, the Topology application loads automatically and the Discovery Wizard opens, as shown below. The Discovery Wizard guides you through the process of discovering the physical Alcatel devices in the network. Optionally, it also enables you to discover network links, additional link information required for the OmniVista's Locator application, information on network VLANs required by OmniVista's VLANs application, and third-party physical devices by Cisco, Extreme, and 3Com.



The first page of the Discovery Wizard, shown above, enables you to specify the type of discovery you want to perform and the types of additional information you want to discover. You can select one of the following types of discovery:

- A **Ping Sweep** discovery enables you to discover all switches with an IP address that falls within user-specified ranges of IP addresses. If you enable this button, the Discovery Wizard will display a window that enables you to enter the ranges of IP addresses you want discovered.
- An **ARP** discovery enables you to connect to a gateway device, which uses ARP to return a list of all subnets known to the gateway. Each subnet is then discovered. If you enable this button, the Discovery Wizard will display a window that enables you to enter the gateway devices you want discovered.

**Note:** The **Re-Discover** selection is not appropriate for your initial discovery. The **Re-Discover** selection makes it possible to learn information about selected devices that was not learned during a previous discovery. For example, you might wish to rediscover a device to learn VLAN information that was not gathered during the first discovery. You might also wish to rediscover a device if that device was reconfigured outside of OmniVista.

You can specify that you want to learn the following types of optional information during the discovery:

- **Locator and Topology Discovery Options.** Enable this checkbox if you wish to learn information about network links. Link information is maintained by proprietary protocols that are active by default in each switch. Information about network links is necessary to display the links between devices when the network and its regions are displayed. This option also enables you to learn additional link information required by the Locator application. If you enable this checkbox, the Discovery Wizard will later display a window that allows you to specify the precise link information you want learned.
- **VLAN Discovery Options.** Enable this checkbox if you wish to learn VLAN information required by the VLANs application. If you enable this checkbox, the Discovery Wizard will later display a window that allows you to specify the precise VLAN information you want to learn.

By default, the Discovery Wizard will discover third-party devices in the network built by Cisco, Extreme, and 3Com. If you do not have such devices in the network, or you do not wish OmniVista to discover them, click the respective third-party device checkbox to disable it.

Click the Discovery Wizard's **Next** button when you have selected the desired discovery options. Click the **Help** button at the bottom of each page of the Discovery Wizard for information on using that page. The discovery will be performed when you click **Finish** on the last page of the Wizard.

## Viewing Discovered Devices

When the discovery is complete, all devices discovered display in the list of **All Discovered Devices**. Select **Switches** in the Tree to view the list of All Discovered Devices, as shown below. Each discovered device also displays in the Tree. Click **Switches** and **Physical Network** open as shown below to view the individual subnets discovered. Click a subnet open to view individual devices on the subnet. Note that you can connect to any switch by selecting it in the Tree.

Click on Switches to display the list of All Discovered Devices.

Discovered devices display here.

Name	Address	DNS Name	Type	Version
DCTestnetCore	10.255.10.3		OS7700	5.1.6.86.R02
Kite_59	10.255.11.59		OS6800-48	6.1.2.88.R01
Kite_60	10.255.11.60		OS6800-48	6.1.2.37.R01
vxTarget	10.255.11.61		OS6800-24	6.1.2.119.R01
vxTarget	10.255.11.63		OS6800-24	6.1.2.116.R01
vxTarget	10.255.11.97		OS9700	6.1.1.631.R01
NMS_HAWK_102	10.255.11.102		OS6624	5.1.6.147.R02
nms-test-103	10.255.11.103		OmniSIR-9	4.5.1
no-name	10.255.11.104		OS6800-48	6.1.1.502.R01
vxTarget	10.255.11.111		OS9700	6.1.1.615.R01
Kite	10.255.11.112		OS6800-24	6.1.2.120.R01
no-name-119	10.255.11.119		OmniSIR-5	4.5.2
no-name	10.255.11.120		OmniSIR-3	4.4.5
no-name	10.255.11.121		OS9700	6.1.1.632.R01
VW_HAWK_122	10.255.11.122		OS6648	5.4.1.148.R01
USS_Blue_Ridge_4	10.255.11.123		OS6648	5.1.5.133.R04
NMS_125	10.255.11.125		OS6300-24	2.2.0.10
VW_FUJII_126	10.255.11.126		OS9700	6.1.1.631.R01
BS0001s	10.255.11.127		OS7800	5.1.6.125.R02
VW_FUJII_129	10.255.11.129		OS9800	6.1.1.631.R01

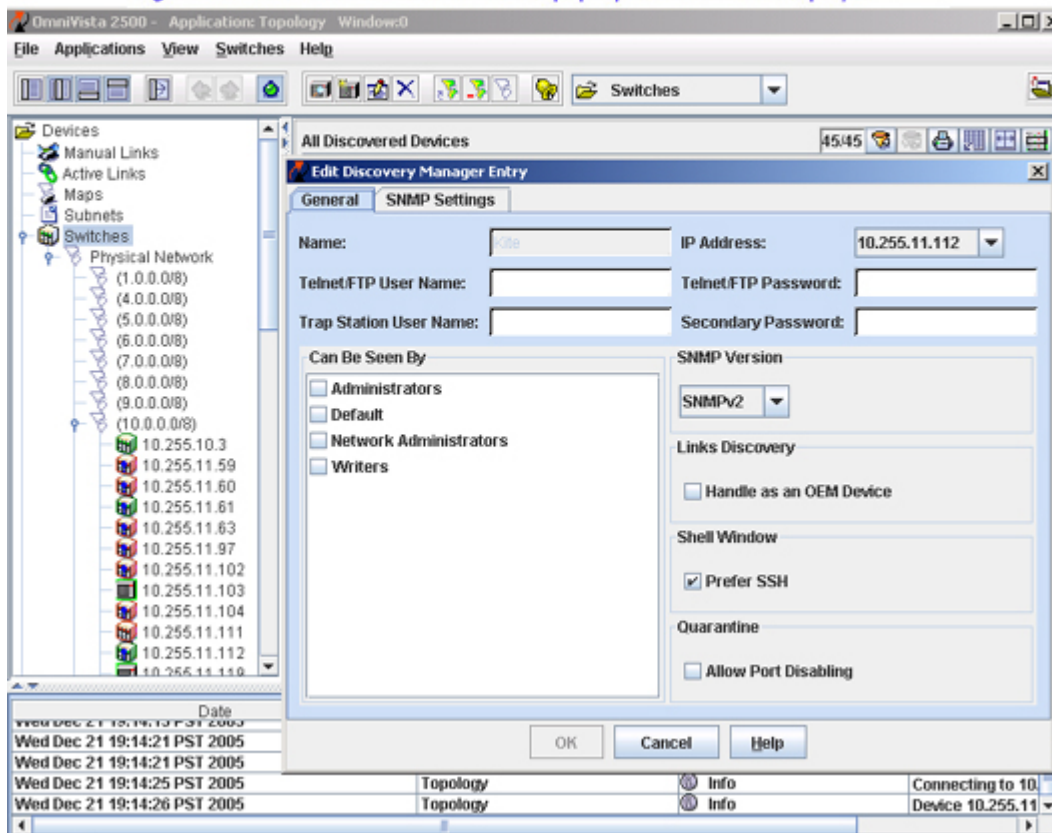
### Step 3. Edit Discovered Devices

Once switches are discovered, you may want or need to edit entries in the list of All Discovered Devices. The reasons for editing discovered devices are discussed in the section below, *Why Edit a Discovered Device?*.

To edit a discovered device, double click the device's entry in the list of All Discovered Devices to display the **Edit Discovery Manager Entry** window, shown below. You can also edit multiple entries at one time. To do this, select the desired entries in the list of All Discovered Devices, click right, and select **Edit** from the pop-up menu that displays. Your edits will then apply to all selected devices.

#### The Edit Discovery Manager Entry Window

Double-click any entry in the list of All Discovered Devices to display the Edit Discovery Manager Entry Window. Or, select multiple entries, right-click, and select Edit from the pop-up window that displays.



## Why Edit a Discovered Device?

### To Redefine the Primary IP Address

When switches are auto-discovered via a Ping Sweep or ARP discovery, each IP address in a range or subnet is pinged. OmniVista uses the first IP address that responds to a ping as that device's primary IP address. However, if multiple VLANs exist in the device, additional IP addresses in the device will also respond to pings. The Edit Discovery Manager Entry window's **IP Address** field combo box lists these additional IP addresses and enables you to select any address listed as the device's primary IP address. The device's primary IP address will display as the device's address in the list of All Discovered Devices.

### To Specify the Correct Write Community Name

All devices that are discovered are initially specified to have the default write community name, **public**. If any discovered devices in your network have a non-default write community name, use the Edit Discovery Manager Entry window's SNMP Settings tab to specify the correct community name to OmniVista. If the correct write community name is not specified to OmniVista, you will not be able to write configuration changes to the switch.

**Please Note:** Switches' SNMP write (set) community names are not configurable from OmniVista. SNMP read (get) and write (set) community names can only be configured by logging onto the switch.

### To Specify the Telnet or FTP User Name and Password

#### *XOS and AOS Devices*

Firmware configuration files for XOS and AOS devices can be saved to the OmniVista server and restored when desired. When files are saved, they are FTPed from the switch to the OmniVista server. When files are restored, they are FTPed from the server to the switch. New configuration files can also be installed via FTP. In order to FTP files, OmniVista must know the FTP login name and password that is defined on the switch. The **Telnet/FTP User Name** and **Telnet/FTP Password** fields on the Edit Discovery Manager Entry window enable you to specify this information to OmniVista.

**Please Note:**

- If you do not define the FTP login names and passwords for XOS and AOS devices, and you attempt to save, restore, or update configuration files for these devices, you will be individually queried for the FTP login name and password of each individual switch for which configuration files are being saved, restored, or updated.
- For XOS and AOS devices, the user names and passwords entered in these fields are used for FTP ONLY. They are not used for Telnet. When you Telnet to an XOS or AOS device, you will be queried for a user name and password.

#### *OmniCore Devices*

If you defined a non-default Telnet user name and password for an OmniCore device, the **Telnet/FTP User Name** and **Telnet/FTP Password** fields on the Edit Discovery Manager Entry window enable you to specify this information to OmniVista. The non-default Telnet user name and password will be passed to the TrackView Element Manager automatically whenever TrackView is invoked.

**Please Note:**

- For OmniCore devices, the user names and passwords entered in these fields are used for Telnet communications via TrackView ONLY.
- If an OmniCore device is using the default Telnet user name and password, leave these fields blank. The default user name admin and a null password will be passed to TrackView automatically.

## To Redefine Switch Access

The **Can Be Seen By** parameter specifies the OmniVista security group that has access to the device. The Edit Discovery Manager Entry window enables you to redefine the security group or to specify that all security groups have access. OmniVista is shipped with the following pre-configured security groups:

- **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 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 discovery 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 Server application. Members of this group can do everything EXCEPT edit the groups and users defined in the Security application.
- **Administrators** group. This group has all administrative access rights granted to the Network Administrators group AND full administrative rights to edit the groups and users defined in the Security application.

## To Redefine the SNMP Version or SNMP Parameters

The Edit Discovery Manager Entry window enables you to redefine the SNMP version that OmniVista uses to communicate with AOS devices. You can also redefine SNMP parameters. The SNMP version or parameter settings that OmniVista uses cannot be changed until OmniVista has connected to the switch. XOS devices support SNMP version 1 only. AOS devices support SNMP version 1, SNMP version 2 or SNMP version 3.

## Step 4. Configure Traps

It is necessary to configure the switches in the network to send OmniVista the traps that are needed by different applications. To configure traps for one or more devices, select the device(s) in the list of All Discovered Devices, click right, and select **Configure Traps** from the pop-up menu. The Configure Traps window displays. The traps OmniVista needs for each application are listed below.

### AOS Traps

#### Traps Needed for Topology

coldStart, warmStart, linkUp, linkDown

**Note:**For proper link display in Topology, linkUp and linkDown traps must be enabled for each individual port.

**Traps Needed for PolicyView QoS**  
policyEventNotification

## XOS Device Traps

**Traps Needed for Topology**  
coldStart, warmStart, linkUp, linkDown, portLinkUpEvent, portLinkDownEvent

**Traps Needed for PolicyView QoS**  
policyEvent

## Step 5. Redefine Default Passwords

The Security application *Users and Groups* utilizes security groups, defined users, and passwords to control access to OmniVista. OmniVista is shipped with four default security groups and four default users. The default password for each user is **switch**. At a minimum, you should redefine the passwords assigned to each user. You can also create new security groups and new users. OmniVista is shipped with the following default users, groups, and passwords:

**user**. This user belongs to the **Default** group and thus has read-only access to switches that are configured to grant access to this group. The default password for this user is **switch**.

**writer**. This user belongs to the **Writers** group and thus has both read and write access to switches that are configured to allow access to this group. This user can view and modify switch information. The default password for this user is **switch**.

**netadmin**. This user belongs to the **Network Administrators** group and thus has full administrative rights to all switches on the network. Members of this group can do everything EXCEPT edit the groups and users defined in the Security application *Users and Groups*. The default password for this user is **switch**.

**admin**. This user belongs to the **Administrators** group and thus has full administrative rights to all switches on the network AND full administrative rights to the Security application *Users and Groups*. The default password for this user is **switch**.

For further information, refer to the help for the Security application *Users and Groups*.

## Step 6. AOS Devices Only: Save Changes

### Overview

The directory structure that stores AOS 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 load 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 memory. The running configuration is the current operating parameters of the switch, which are originally loaded from the certified or working directory. Modifications made to the running configuration of the switch must be saved to the working directory (or lost). The working directory can then be copied to the certified directory if and when desired.

When changes are made to the configuration of an AOS device -- such as configuring the traps the switch should transmit -- the change is written to the running configuration of the switch. However, if the switch is powered off, the running configuration will be lost. To make changes to the running configuration persistent, you must save the running configuration to the working directory of the switch. You should also then copy the working directory to the certified directory, so the changes will be persistent when the switch is booted from the certified directory.

**Note:** When a change is written to the running configuration of an AOS device that has not been saved to the working directory, the Changes column in the list of All discovered Devices displays **Unsaved**. When the working directory has changes saved to it that are not in the certified directory, the Changes column in the list of All discovered Devices displays **Uncertified**. Icons for AOS devices display a blue exclamation mark (  ) when the switch configuration is in the Unsaved state or the Uncertified state.

## How to Save Changes

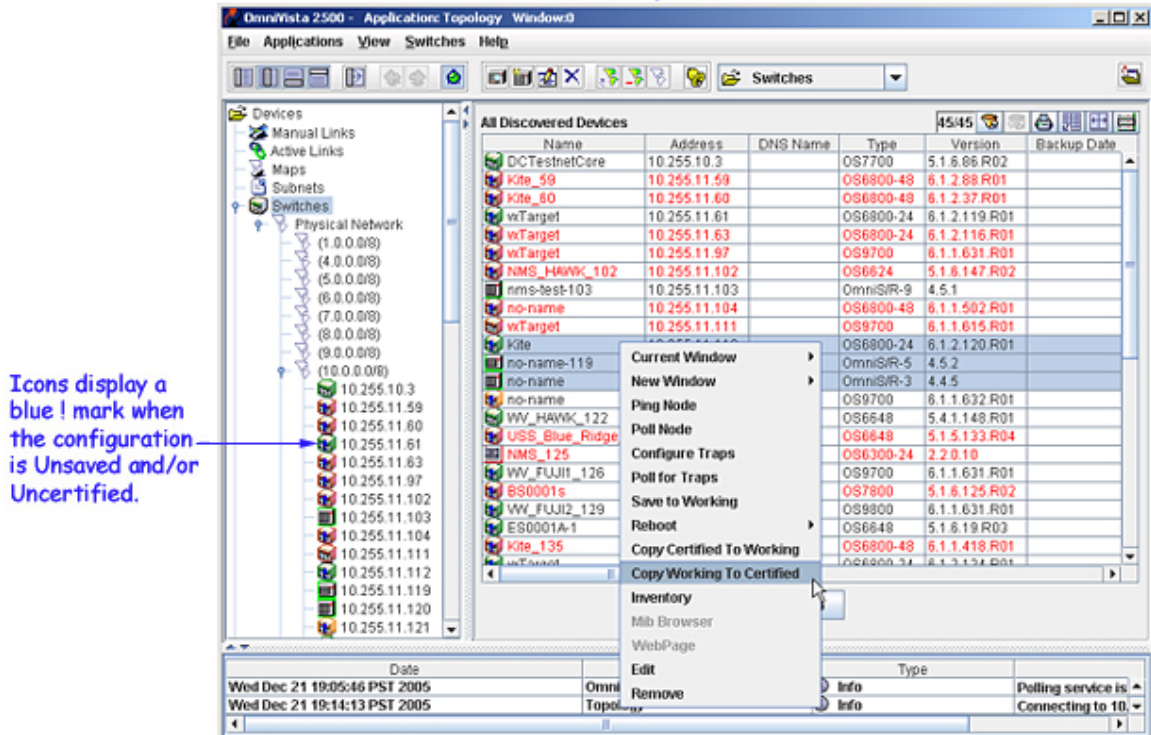
You can save configuration changes for multiple switches simultaneously by following the steps below.

1. Select **Switches** in the Tree to display the list of All Discovered Devices. Click on the Changes column to sort the list according to the switch configuration state.
2. Select all switches with Unsaved changes and click right. Select **Copy Working to Certified** from the pop-up menu that displays. The configuration is first saved to the working directory and then the working directory is saved to the certified directory for each selected switch. The Changes field will display **Uncertified** when the changes are saved to the working directory and will go blank when the working directory is saved to the certified directory. Note that it may take a few moments for the Changes field to update.



### Saving OmniSwitch 6000/7000/8000 Configuration Changes

Select all switches with unsaved changes and right-click. Select **Copy Working to Certified** from the pop-up menu. Configuration changes will be saved to the Working directory and the working directory will be saved to the Certified directory for each selected switch.



### If you Installed PolicyView QoS....

When PolicyView QoS is executed, it writes the address of the LDAP server to each QoS-enabled switch in the list of All Discovered Devices. (All AOS devices are QoS-enabled.) In the case of AOS devices, the LDAP address is written to the running configuration of the switch. For this reason, once PolicyView QoS has executed, all AOS devices will be left with their running configuration in the **Unsaved** state (indicating that the running configuration has changes that have not been saved to the working directory). It is important to save the running configuration to the working directory and then the certified directory after PolicyView QoS has executed. To do this, follow the steps in *How to Save Changes* directly above.