



IPSWITCH

WhatsUp Log Management
v10.x
Syslog Device Wizard Guide

Using the Multiple Syslog Device Wizard

- Step 1: Defining Subnets to Scan 3
 - Adding a Network to the Multiple Syslog Device Wizard..... 4
 - Adjusting Settings for the WhatsUp Syslog Hostname Resolver Service 4
- Step 2: Choosing Discovered Syslog Devices 5
- Step 3: Adding Syslog Devices for Monitoring 6

Using the Multiple Syslog Device Wizard

In This Guide

Step 1: Defining Subnets to Scan.....	3
Step 2: Choosing Discovered Syslog Devices.....	5
Step 3: Adding Syslog Devices for Monitoring	6

The Multiple Syslog Device Wizard is designed to help you manage adding a large number of syslog-generating devices on your network. The Multiple Syslog Device wizard saves you the time of having to manually type information for all your syslog-generating devices by automatically discovering them for you. Using the wizard, specify subnets for your network that include syslog-generating devices that you want discovered. Once syslog-generating devices are discovered, information is sent to either WhatsUp Event Alarm or WhatsUp Event Archiver for processing.

You can access the Multiple Syslog Device Wizard from either of the following options:

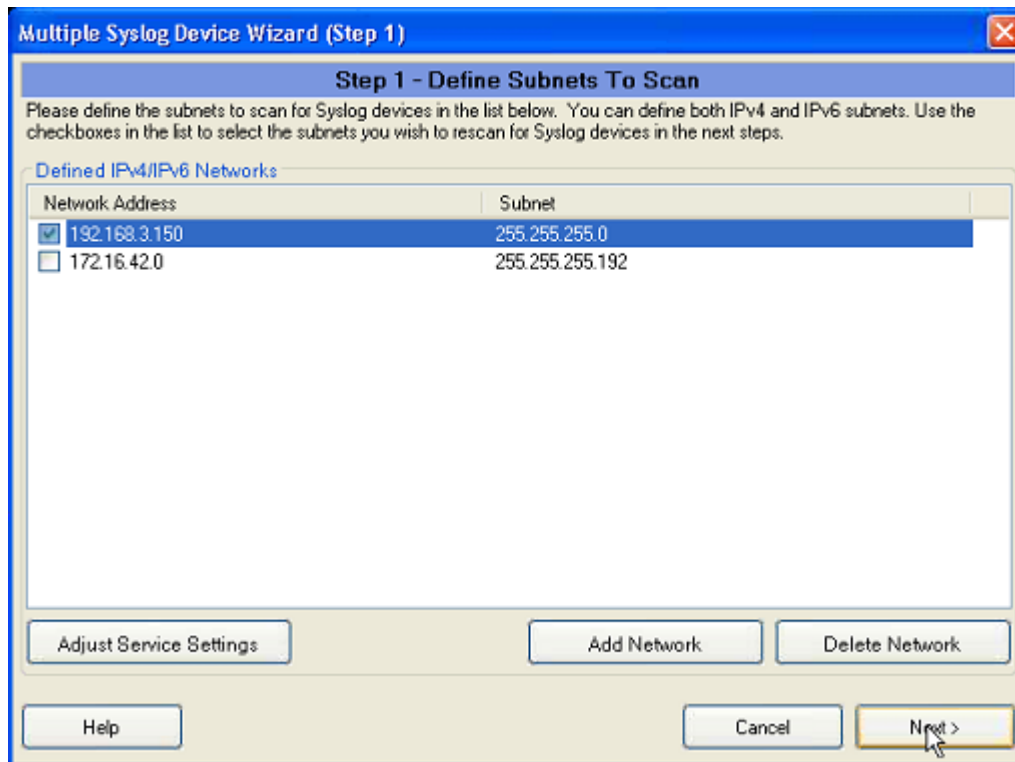
- From WhatsUp Event Archiver, click the **Syslog** menu, and then select **Add Multiple Syslog Devices by Subnet**.
- From WhatsUp Event Alarm, click the **Tools** menu, and then select **Step-By-Step Wizards**. From the list of wizards, select **Add Multiple Syslog Devices by Subnet**.

The steps involved in completing the wizard include:

- *Defining a network address and subnet mask containing syslog-generating devices you want monitored (on page 3).*
- *Selecting or choosing discovered syslog-generating devices for monitoring (on page 5).*
- *Adding syslog-generating devices for monitoring (on page 6).*

Step 1: Defining Subnets to Scan

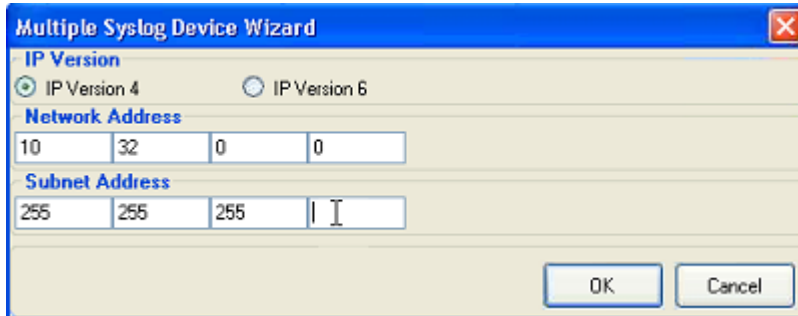
In Step 1, define the subnets you want to scan for syslog-generating devices. You can define a Class C network (255 devices or less), multiple Class C networks, or networks smaller than Class C. When setting networks you want scanned, ensure that the checkbox associated with the network you want to scan is checked. Unchecked networks are not scanned. When you are finished adding networks to scan, click **Next**.



- To delete a network, select the check box associated with the network you want to delete, and then click **Delete Network**.
- To adjust settings for the *WhatsUp Syslog Hostname Resolver Service* (on page 4), click **Adjust Service Settings**.

Adding a Network to the Multiple Syslog Device Wizard

To add a network to the Multiple Syslog Device Wizard, click **Add Network** from Step 1 of the wizard.



As the figure above indicates, you can type information for either IPv4 or IPv6 networks. Also, from the Subnet Address octets, the network being added is an example of a Class C network. In the last Subnet address octet, you can type a smaller number than 255 as a CIDR specification if your network does not follow standard class conventions.

Adjusting Settings for the WhatsUp Syslog Hostname Resolver Service

The WhatsUp Syslog Hostname Resolver Service scans devices on your network and updates any changes to DNS names. The service accesses the DNS server, and if a hostname has changed, that change is noted by the WhatsUp Syslog Hostname Resolver Service and updated in the database. A benefit of this service is that if DNS names change, the change does not have to be manually updated in the product. Instead, the service automates the process for you.



Use the drop down list to set how often you want the service to run automatically. You can set it to run Nightly (every twenty-four hours from the time the service is first started), Weekly (every seven days from the time the service is first started), or Monthly (every 30 days from the time the service is first started). In addition, the service starts a new resolver scan every time it is started anew.

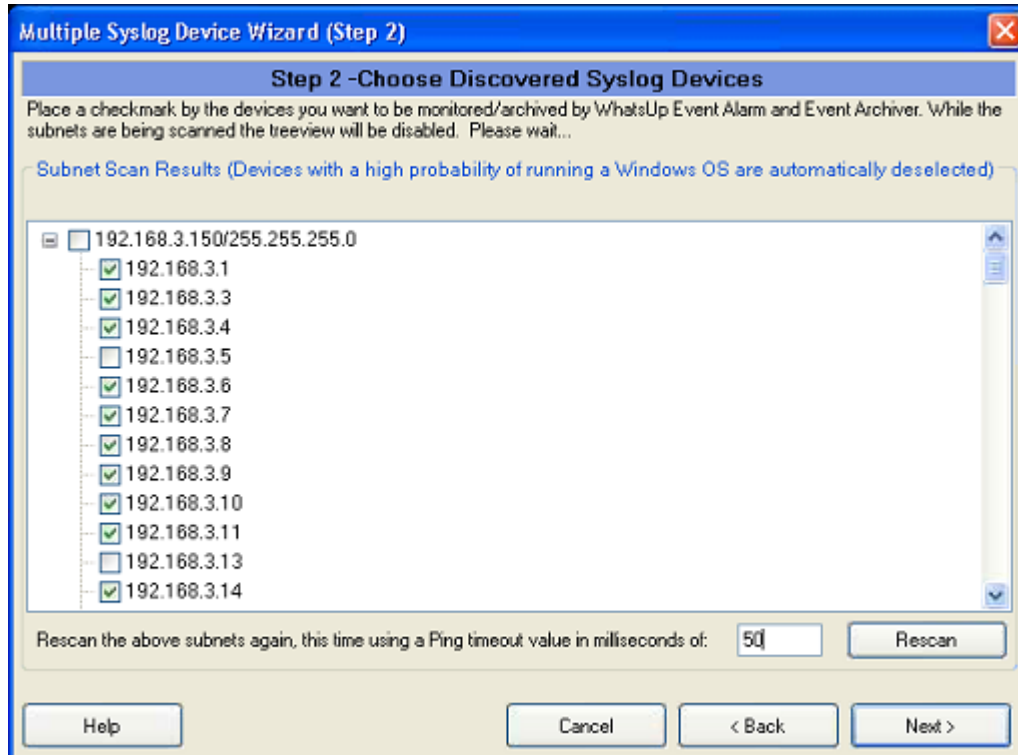
Multiple Syslog Device Wizard

To run the lookup service to resolve or update hostnames, click **Resolve/Update Hostnames Now**.

When you are finished, click **OK** to return to the Defining Subnets to Scan dialog.

Step 2: Choosing Discovered Syslog Devices

In Step 2, you choose which syslog devices you want to monitor. After clicking Next in Step 1, the Step 2 dialog displays with a progress bar at the top indicating that the system is scanning for any devices in the specified subnet on the network. The system is also differentiating between Windows devices and non-Windows syslog-generating devices. After the scan completes, a list of all devices found displays. The list of devices indicates devices that answered a Ping command. Any Windows devices found during the scan have cleared checkboxes, indicating that they will not be added for syslog monitoring. If a device you want monitored is not checked, check the associated checkbox to add the device for monitoring.



If you have a slow network or if you believe that devices are missing from the list, you can increase the millisecond value for a Ping timeout. For example, the default value for this field is 50 milliseconds. If you would like to rescan the network with a longer Ping timeout value, increase the number in this field, and then click **Rescan**. Note that if you increase the Ping timeout value, it could substantially increase the amount of time it takes to scan your network.

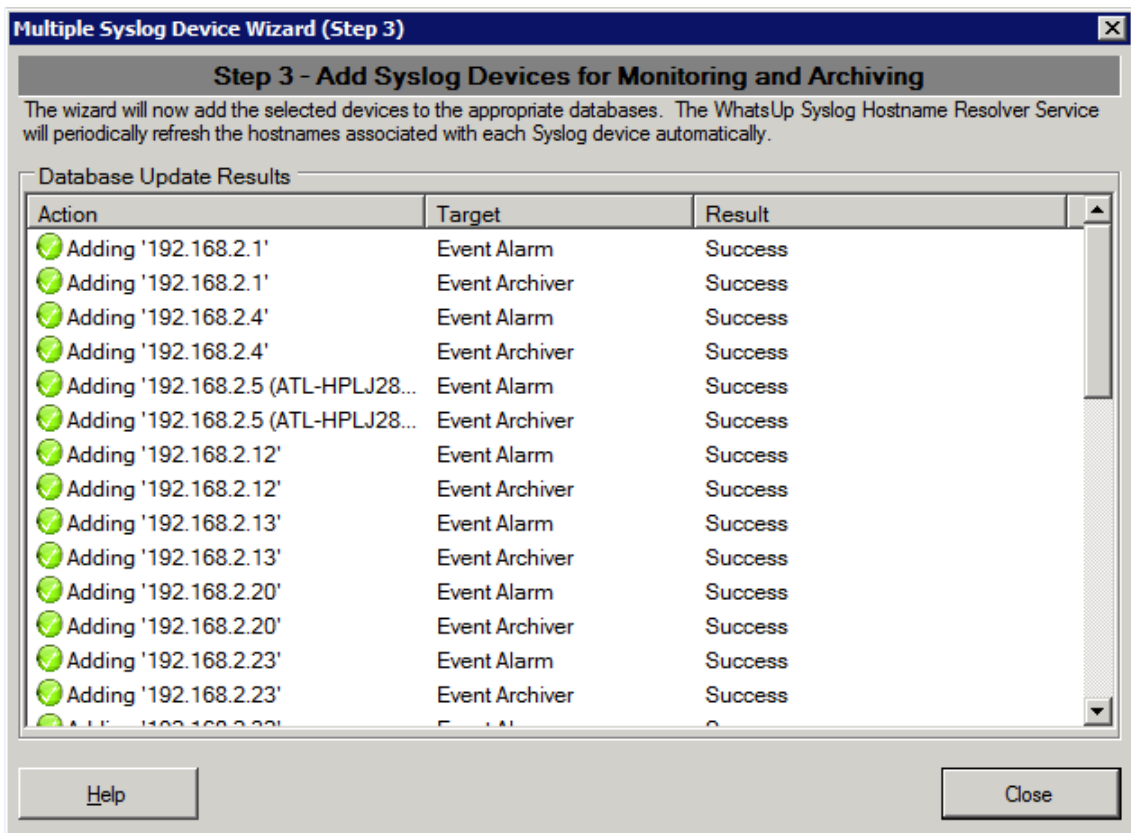
Multiple Syslog Device Wizard

Any syslog devices found with DNS names will include the DNS name in parenthesis. This is performed by the *WhatsUp Syslog Hostname Resolver Service* (on page 4). If the DNS names are changed, those changes are updated and noted by the service.

When you are finished, click **Next**.

Step 3: Adding Syslog Devices for Monitoring

In Step 3, a list of the devices added for monitoring displays. The database update results have 3 possible statuses: the device(s) are added to the database successfully, the devices already exist in the database, or adding this device exceeds the number allowed for your license. If you receive an error associated with licensing, you can make room on the database by removing Windows devices and other non-syslog generating devices, or contact Ipswitch to update licensing.



Multiple Syslog Device Wizard

After your devices are added, you can close the Multiple Syslog Device Wizard and return to either WhatsUp Event Archiver or WhatsUp Event Alarm to see your list of syslog devices in the application. The figure below displays a list of syslog devices associated with WhatsUp Event Archiver. Note that devices can have a blue or green screen icon to the left of the device name. Devices with a blue screen icon indicates that they were added manually. Devices with a green screen icon indicates that they were added using the wizard. Devices added manually are not subject to the WhatsUp Syslog Hostname Resolver Service; therefore, DNS names are not resolved by reverse lookup.

